MTHSC 852: Modules

1. Preliminaries

Motivation: A module is like a "vector space over a ring."

Throughout, let R be a ring, and M an additive abelian group.

Def: M is a (left) R-module if there is scalar multiplication

$(r,x) \longmapsto rx \in M$ satisfying

(i) $r(x+y) = rx + ry$

(ii) $(r+s)x = rx + sy$

(iii) $(rs)x = r(sx)$

for all $r,s \in R$, $x,y \in M$.

Note: It is easy to check that $r.0 = 0.x = 0$, and $(-r)x = r(-x) = -rx$.

Right R-modules are defined similarly.

Recall: $\mathrm{End}(M)$ is a ring.

Exercise: If M is an R-module, then $\exists$ ring homomorphism

$\phi : R \longrightarrow \mathrm{End}(M)$, $\phi : r \longmapsto \phi_r$, where $\phi_r(x) = rx$.

Conversely, for any homomorphism $\phi : R \longrightarrow \mathrm{End}(M)$, defining

$rx = \phi_r(x)$ makes M into an R-module.

This can be made into an alternative and equivalent

definition of R-modules.

Examples:

1. If V is a vector space over a field F, then V is an F-module.
2. Any abelian group G is a $\mathbb{Z}$-module, since for any $r \in \mathbb{Z}^+$, $x \in G$, $rx = x + x + \dots + x$ (n times).
3. Any left-ideal $I \subseteq R$ is an R-module.
4. Let $R = F[x]$, V an F-vector space, $T : V \to V$ a linear map. The pair (V, T) is a vector space with endomorphism. Then, V is an $F[x]$-module, where $f(x) \cdot v = f(T)(v)$, i.e., $(a_0 + a_1 x + \dots + a_n x^n) v = a_0 v + a_1 T(v) + \dots + a_n T^n(v)$, where $a_i \in F$, $v \in V$. We denote this module by V_T.

If $1 \in R$, and M is an R-module, and $1 \cdot x = x$ for all $x \in M$, then M is a unitary R-module.

Remark: Sometimes, this assumption is built into the definition.

Examples 1, 2, 3, 4 are all unitary

Non-example: Let $S = M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \right\}$; $\quad 1_S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$R = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}; \quad 1_R = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

Then $R \subseteq S$ is a subring, and S is a left R-module.

But $1_S \neq 1_R$; so $1_R \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, i.e, $1_R x \neq x \in S$, so S is not a unitary R-module.

<u>Def</u>: A subgroup N of an R-module M is a <u>submodule</u> if $rx \in N$ $\forall r \in R$, $x \in N$.

<u>Examples</u>:

1. If R is an F-vector space (i.e, an F-module), then a submodule is a subspace.
2. If G is an abelian group (i.e, a $\mathbb{Z}$-module), then a submodule is a subgroup.
3. If R is a commutative ring (i.e, an R-module), then a submodule is an ideal.
4. If V is an F-vector space with endomorphism T (i.e, an $F[x]$-module), then a submodule is an <u>invariant subspace</u>, i.e, a subspace $W \subseteq V$ such that $T(W) \subseteq W$.

<u>Prop 1.1</u>: If M is an R-module, and $\{M_\alpha\}$ any nonempty collection of submodules, then $\bigcap_\alpha M_\alpha$ is a submodule. $\square$

<u>Def</u>. If M is an R-module, and $S \subseteq M$, then define $R\langle S \rangle = \bigcap \{N : S \subseteq N,\ N \text{ is a submodule of } M\}$, the submodule of M <u>generated</u> by S.

<u>Def</u>: If $M = R\langle S \rangle$ for some $|S| < \infty$, then M is <u>finitely generated</u> over R, and if $|S| = 1$, then M is <u>cyclic</u> over R.

Example: Let $F = \mathbb{Q}$, V a 2-dimensional $\mathbb{Q}$-vector space, and $T: V \longrightarrow V$ the linear map given by $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then V_T is a $\mathbb{Q}[x]$-module.

We can write an element in V by $\begin{pmatrix} a \\ b \end{pmatrix}$, $a, b \in \mathbb{Q}$.

- If $f_1(x) = x^2 - x$, then $f_1(x) \cdot \begin{pmatrix} a \\ b \end{pmatrix} = A^2 \begin{pmatrix} a \\ b \end{pmatrix} - A \begin{pmatrix} a \\ b \end{pmatrix}$
$$= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} - \begin{pmatrix} a+b \\ b \end{pmatrix} = \begin{pmatrix} b \\ 0 \end{pmatrix}$$
Thus, if $v = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$, then $f_1(x) \cdot v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
- If $f_2(x) = x^2 - x + 1$, then $f_2(x) \cdot \begin{pmatrix} a \\ b \end{pmatrix} = A^2 \begin{pmatrix} a \\ b \end{pmatrix} - A \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a+b \\ b \end{pmatrix}$.
Thus, if $v = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$, then $f_2(x) \cdot v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Since $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ spans V, $M = \mathbb{Q}[x] \left\langle \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\rangle$, i.e, V_T is a cyclic $\mathbb{Q}[x]$-module.

Now, consider the submodule $N = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} : a \in \mathbb{Q} \right\}$

Since $x \cdot \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}$, $N = \mathbb{Q}[x] \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$, i.e, N is a cyclic submodule of V_T.

Note: Neither M nor N are cyclic, as additive subgroups.

Def: If M & N are R-modules, then a module homomorphism (or R-homomorphism) is a group homomorphism $f: M \to N$ such that $f(rx) = r f(x)$ $\forall r \in R$, $x \in M$. (We define an R-isomorphism, R-automorphism, etc, in the obvious fashion)

Examples:

1. If V, W are F-vector spaces, then an F-homomorphism $V \to W$ is a linear map.
2. If G, H are abelian groups, then a $\mathbb{Z}$-homomorphism $G \to H$ is an ordinary (group) homomorphism.

The <u>kernel</u> and <u>image</u> are defined as usual, and are clearly submodules of M and N, respectively.

Denote the set of R-homomorphisms from M to N by $\mathrm{Hom}_R(M,N)$.

<u>Prop 1.2</u>: $\mathrm{Hom}_R(M,N)$ is an abelian group if we define $(f+g)(x) = f(x) + g(x)$. If R is a commutative ring, then $\mathrm{Hom}_R(M,N)$ is an R-module if we define $(rf)(x) = r \cdot f(x)$. Moreover, if R is a commutative ring with 1, and N is a unitary R-module, then $\mathrm{Hom}_R(M,N)$ is a unitary R-module.

<u>Pf</u>: Exercise.

<u>Def</u>: If M is an R-module and N a submodule, then the quotient abelian group M/N can be made into an R-module by defining $r(m+N) = rm + N$. Then, M/N is a <u>quotient module</u>, and $M \to M/N$, $m \mapsto m+N$ the quotient homomorphism.

Examples:

1. If V is an F-vector space, then a quotient module is a quotient vector space.

2. For abelian groups (i.e, $\mathbb{Z}$-modules), a quotient module is just a quotient group.
3. If V is an F-vector space with endomorphism T, then a quotient module is a quotient vector space V/W (W an invariant subspace), with the $F[x]$-action given by $\bar{T}: V/W \to V/W$ induced by T.

It is elementary to extend the homomorphism and isomorphism theorems from abelian groups to arbitrary R-modules.

We will state them here without proof.

<u>Thm 1.3</u>: (Fundamental Homomorphism Theorem for Modules):

Suppose M and N are R-modules and $f \in Hom_R(M, N)$ has kernel K. If $\eta: M \to M/K$ is the canonical quotient, then $\exists!$ R-isomorphism $g: M/K \to Im\, f \subseteq N$ such that $f = g\eta$.

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\eta"'] & & Im\, f \subseteq N \\ & M/K \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

<u>Prop 1.4</u>: (Correspondence Theorem). Let M, N be R-modules, $f: M \to N$ an epimorphism with kernel K. Then there is a 1-1 correspondence between the set of submodules $L \subseteq N$ and the set of submodules P such that $K \subseteq P \subseteq M$, given by $L \longleftrightarrow f^{-1}(L) = P$. In particular, each submodule of a quotient submodule has the form P/K for some submodule P, $K \subseteq P \subseteq M$.

Prop 1.5: (Freshman Theorem for Modules): Suppose K and N are submodules of an R-module M, with $K \subseteq N$. Then N/K is a submodule of M/K and $(M/K)/(N/K) \cong M/N$.

Thm 1.6: (Isomorphism Theorem for Modules). If K and N are submodules of an R-module M, then $K+N$ and $K \cap N$ are submodules of M and $(K+N)/K \cong N/(K\cap N)$.

$$\begin{tikzcd}[column sep=small]
& M \arrow[d, dash] & \\
& K+N \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & N \arrow[dl, dash] \\
& K\cap N &
\end{tikzcd}$$

Def: An R-module $M \neq 0$ is called simple if its only submodules are M and 0.

Def: A sequence $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots \supseteq M_k = 0$ of submodules of an R-module is a composition series if each M_{i+1} is a maximal (proper) submodule of M_i, or equivalently (by Correspondence Thm) if every factor M_i/M_{i+1} is simple.

Thm 1.7: (Jordan-Hölder). Suppose an R-module M has a composition series $M = M_0 \supseteq M_1 \supseteq \dots \supseteq M_k = 0$ and

$N = N_0 \supseteq N_1 \supseteq \dots \supseteq N_m = 0$

Then $k = m$ and there is a 1-1 correspondence between the sets of factors so corresponding factors are R-isomorphic.

Pf: Almost the same as Thm 5.5 (Groups).

Def: An R-module M is Noetherian if it satisfies the ascending chain condition (ACC) for submodules, i.e, given $M_1 \subseteq M_2 \subseteq \dots$, either the chain is finite or $M_n = M_k$, i.e., the chain terminates.

Prop 1.8: If M is an R-module, then the following are equivalent:

(i) M is Noetherian

(ii) Every submodule of M is finitely generated

(iii) Every non-empty set $\{M_\alpha\}$ of submodules has a maximal element w.r.t. set inclusion.

Pf:

(i)$\Rightarrow$(ii): If a submodule N is not finitely generated, choose $x_1 \in N$ and set $M_1 = R\langle x_1 \rangle$. Then choose $x_2 \in N \setminus M$, and set $M_2 = R\langle x_1, x_2 \rangle$, etc. Clearly, $M_1 \subsetneq M_2 \subsetneq \dots$ ✓

(ii)$\Rightarrow$(iii) If there is a set of submodules without a maximal element, then choose $M_1 \subsetneq M_2 \subsetneq \dots$ from the set. Put $N = \bigcup_{i=1}^{\infty} M_i$, a submodule of M. Then $N = R\langle x_1, \dots, x_k \rangle$ for some $x_1, \dots, x_k \in N$, hence for each i, x_i is in some M_{j_i}.

If j_m is the largest index, then all $x_i \in M_{j_m} \Rightarrow N = M_{j_m}$, contradicting the fact that $M_i \subsetneq M_{i+1}$ for all i. ✓

(iii)$\Rightarrow$(i) Obvious ✓

$\square$

Prop 1.9: Let K be a submodule of the R-module M, and set $N = M/K$. Then M is Noetherian iff both K and N are Noetherian.

Pf: ($\Rightarrow$) All submodules of K are submodules of M, so they are all finitely generated, thus Noetherian (Prop 1.8). ✓

Any ascending chain $N_1 \subseteq N_2 \subseteq \cdots$ of submodules of $N = M/K$ has the form $M_1/K \subseteq M_2/K \subseteq \cdots$ with $M_i \subseteq M$ (Corresp. Thm)

Since $M_1 \subseteq M_2 \subseteq \cdots$ terminates, so does $M_1/K \subseteq M_2/K \subseteq \cdots$

Therefore, N is Noetherian. ✓

($\Leftarrow$) Let $M_1 \subseteq M_2 \subseteq \cdots$ be an ascending chain of submodules of M. Then $M_1 \cap K \subseteq M_2 \cap K \subseteq \cdots$ terminates, say at $M_j \cap K$. Likewise, $(M_1+K)/K \subseteq (M_2+K)/K \subseteq \cdots$ terminates, say at $(M_m+K)/K$.

Set $n = \max\{j, m\}$.

If $k \geq n$ and $x \in M_k$, then $(M_k+K)/K = (M_m+K)/K$,

so $x+K = y+K$ for some $y \in M_n$.

But then $x-y \in M_k \cap K = M_n \cap K \Rightarrow x \in M_n$.

Thus, $M_1 \subseteq M_2 \subseteq \cdots$ terminates at $M_n \Rightarrow M$ is Noetherian. ✓

$\square$