MATH 593 - Module

ARessegetes Stery

October 17, 2023

Contents

1 Module

Definition 1.1 (*R*-Module)**.** *An (left)* ***R-Module*** *M is a set with two operations, often denoted as $(M, +, \times)$:*

- *Addition $(+) : M \times M \to M$, s.t. $(M, +)$ is an abelian group.*

- *Multiplication $(\times) : R \times M \to M$, s.t. it has the following properties:*

    - *Identity. For all $x \in M$, there exists $1 \in R$ s.t. $1 \cdot x = x$.*

    - *Associativity. For all $a, b \in R, x \in M, a(bx) = (ab)x$.*

    - *Distributivity in R. For all $a_1, a_2 \in R, (a_1 + a_2)x = a_1 x + a_2 x$.*

    - *Distributivity in M. For all $a \in R, x_1, x_2 \in M, a(x_1 + x_2) = ax_1 + ax_2$.*

Right modules are defined with the same structure, but with $a \times b = b \cdot a$ for $a \in R, b \in M$, where $\times$ is the multiplication in M, and $\cdot$ the multiplication in R.

Definition 1.2 (Submodule)**.** *Let $(M, +, \times)$ be an R-module. $N \subseteq M$ is a **R-submodule** of M if $(N, +)$ is a subgroup of M; and for all $n \in N, r \in R, n \times r \in N$.*

Remark 1.1. Notice that R itself gives an R-module, just as $\mathbb{K}$ gives a $\mathbb{K}$-vector space. Therefore $\langle S, \varphi \rangle$ an R-algebra induces a two-sided R-module structure. Check that this is indeed the case:

- *Addition.* Adopt the addition in S as a ring.

- *Identity*: Since ring homomorphisms map identity to identity, $\varphi(1_R) = 1_S$, implying that 1_R is the identity for scalar multiplication.

- *Associativity.* Results from the fact that multiplication in S is associative.

- *Distributivity in R and M.* Follows from the fact that φ is a ring homomorphism.

In this sense, module generalizes the algebra structure. Generally one cannot "revert" the structure of a module back to an algebra. Specifically, suppose that R is not commutative, then R is not an R-algebra.

Remark 1.2. (Left) ideals of R are submodules of R taken as an R-submodule.

Remark 1.3. Let M be an abelian group. Making M into a (left) R-module is equivalent to specifying a ring homomorphism $\varphi : R \to \mathrm{End}(M)$, where $\mathrm{End}(\cdot)$ denotes the ring of endomorphisms on the specific structure.

It is worth noticing how the ring of endomorphism structure is defined. Specifically, the multiplication is the composition of endomorphisms on M. This can be viewed in two aspects:

- The associativity for R-modules is essentially stating that multiplication, i.e. elements of R "acting" on those in M is associative. Applying one action after another is the same as applying the composition of action.

- Consider the definition of function as a set of pairs. Then

$$R \times M \to M \cong (R \to M) \to M \cong R \to (M \to M)$$

as the application of functions is associative.

In particular, in the consideration of $\mathbb{Z}$-modules, the map $\varphi_{\mathbb{Z}} : \mathbb{Z} \to \mathrm{End}(M)$ is determined uniquely by the requirement that $1 \mapsto 1_M = \mathrm{Id}_M$. Since addition and multiplication should be preserved, $n \mapsto n \cdot \mathrm{Id}_M$ for all $n \in \mathbb{Z}$. With the specification above one could observe the correspondence:

- $\{\mathbb{Z} \text{ modules}\} \iff \{\text{Abelian groups}\}$

- $\{\mathbb{Z}/n\mathbb{Z} \text{ modules}\} \iff \{\text{Abelian groups } M \text{ s.t. } nx = 0 \ \forall x \in M\}$

2   Morphism of R-Modules

Definition 2.1 (Morphism of R-Modules)**.** *A **morphism of (left) R-modules** $f : M \to N$ is an $\underline{R\text{-linear map}}$, which satisfies:*

- *$f(u_1 + u_2) = f(u_1) + f(u_2)$ for all $u_1, u_2 \in M$.*

- *$f(au) = af(u)$, for all $u \in M, a \in R$.*

An $\underline{\text{isomorphism}}$ of R-modules $f : M \to N$ is equivalently stating that

- *There exists $g : N \to M$ s.t. $f \circ g = \mathrm{Id}_M$, $g \circ f = \mathrm{Id}_N$.*
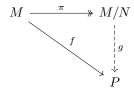
- *f is a bijection.*

Proposition 2.1. *Let $f : M \to N$ be a morphism of R-modules. Then $\mathrm{im}\, f \subseteq M$ and $\ker f \subseteq M$ are submodules; and f is injective if and only if $\ker f = \{0\}$.*

Proof. By the fact that f is R-linear, both the image and kernel should be closed w.r.t. addition and scalar multiplication, i.e. are submodules. For the condition of injectivity, check

$\Rightarrow$: Consider the contraposition. Suppose that $0 \neq a \in \ker f$. Then $f(1) = f(1 + a)$ with $1 \neq 1 + a$ which is a contradiction.

$\Leftarrow$: Consider the contraposition. Suppose that there exists $a \neq b \in R$ s.t. $f(a) = f(b)$, i.e. f is not injective; then $f(a - b) = 0$ which indicates that $0 \neq (a - b) \in \ker$.

$\square$

Definition 2.2 (Quotient Module)**.** *Let $N \subseteq M$ be a R-submodule. Define the equivalence relation $\sim$: $a \sim b$ if and only if $a - b \in N$. Then $M/N := M/\sim$ is a **quotient module**, with $\pi : m \to M/N$ the induced morphism of R-modules.*
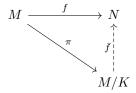
Theorem 2.1 (Universal Property of Quotient Modules)**.** *Let $f : M \to P$ be a morphism of R-modules. Let N be a submodule of M, with π the induced morphism of R-modules. Further suppose that $N \subseteq \ker f$. Then there exists a unique $g : M/N \to P$ s.t. $f = g \circ \pi$, i.e. the following diagram commutes:*

$$
\begin{array}{ccc}
M & \xrightarrow{\ \pi\ } & M/N \\
& \searrow{\scriptstyle f} & \ \ \downarrow{\scriptstyle g} \\
& & P
\end{array}
$$

Proof. It suffices to verify that such map exists and is unique.

- *Uniqueness.* Since the diagram is required to commute, if such function exists, it is fixed by $f(x) = g(\pi(x)) = g(\bar{x})$.

- *Existence.* Then it suffices to check that g such defined is indeed a morphism of R-modules. This is indeed the case as f is a morphism of R-modules.

$\square$

Theorem 2.2 (First Isomorphism Theorem). *Let $f : M \to N$ be a surjective morphism of R-modules. Define $K := \ker f$. If there exists a morphism of R-modules $\bar{f} : M/K \to N$ s.t. it is R-linear and $\bar{f} \circ \pi = f$, i.e. the following diagram commutes:*
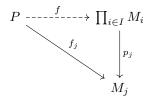
$$
\begin{array}{ccc}
M & \xrightarrow{\ f\ } & N \\
& \searrow{\scriptstyle \pi} & \uparrow{\scriptstyle \bar{f}} \\
& & M/K
\end{array}
$$

Then $\bar{f}$ is an isomorphism.

Proof. By the universal property of morphism of R-modules (Theorem 2.1), a morphism $f : M/K \to N$ s.t. the diagram above commutes exists. It suffices to verify that $\bar{f}$ is bijective. It is surjective as f is surjective; and is injective as $f(x) - f(y) = 0$ if and only if $(x - y) \in K$. $\square$

Definition 2.3 (Direct Product; Direct Sum). *Let $(R_i)_{i \in I}$ be a family (potentially infinite) of modules. Then*

- *The **direct product** of them is the cartesian product $\prod_{i \in I} R_i$, where addition and multiplication is defined element-wise.*

- *The **direct sum** is a sub-ring of the direct sum $\bigoplus_{i \in I} R_i$ where only finitely many elements can be non-zero.*

- *M is the **(internal) direct sum** if M_1 and M_2 if there exists an isomorphism $f : M_1 \oplus M_2 \to M$.*

Theorem 2.3 (Universal Property of Direct Product). *Let P be an R-module, $(M_i)_{i \in I}$ be a family of R-modules, with $f_j : P \to M_j$ a morphism of R-modules. Further let $p_j : \prod_{i \in I} M_i \to M_j$ the projection map s.t. $p_j(x) = x_j$ which is the j-th entry of the input. Then there exists a unique morphism of R-modules $f : P \to \prod_{i \in I} M_i$ s.t. $f(x) = (f_1(x), \cdots, f_n(x), \cdots)$; i.e. the following diagram commutes:*

$$
\begin{array}{ccc}
P & \dashrightarrow^{\ f\ } & \prod_{i \in I} M_i \\
& \searrow{\scriptstyle f_j} & \downarrow{\scriptstyle p_j} \\
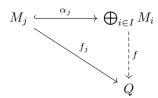& & M_j
\end{array}
$$

Proof. Uniqueness follows from the fact that $p_j \circ f$ should commute with f_j for all j. Existence holds as f_j is itself a morphism of R-modules. $\square$

Theorem 2.4 (Universal Property of Direct Sum). *Let $(M_i)_{i \in I}$ be a family of modules, with $f_j : M_j \to Q$ a family of morphism of R-algebras. Denote α_j to be the natrual embedding s.t.*

$$\alpha_j : M_j \to \bigoplus_{i \in I} M_i, \qquad \alpha_j(x) = (x_i)i, \quad \text{where } x_i = \begin{cases} x, & i = j \\ 0, & \text{otherwise} \end{cases}$$

Then there exists a unique R-linear map $f : \bigoplus_{i \in I} M_i \to Q$ s.t. $f \circ \alpha_j = f_j$ for all j, i.e. the following diagram commutes:

$$
\begin{array}{ccc}
M_j & \xhookrightarrow{\quad \alpha_j \quad} & \bigoplus_{i \in I} M_i \\
& \searrow{\scriptstyle f_j} & \downarrow{\scriptstyle f} \\
& & Q
\end{array}
$$

Proof. Since f is required to be a morphism of R-modules, for all $x = (x_i)_{i \in I} \in \bigoplus_{i \in I} M_i$ it should satisfy the following conditions:

$$f(x) = f \left(\sum_{k \in I} \alpha_k(p_k(x)) \right) = \sum_{k \in I} f(\alpha_k(p_k(x))) = \sum_{k \in I} f_k(p_k(x))$$

which is unique as f_ks and p_ks are uniquely defined. Since both f_k and p_k are homomorphisms, the composition is also a homomorphism. $\qquad\square$

3   Construction of Submodules

This interlude provides some general constructions on how to obtain submodules of a given module. For the setup, let R be a ring, with M a left R-module.

1. Let $(M_i)_{i \in I}$ be a family of submodules of M. Then $\bigcap_{i \in I} M_i$ is a submodule of M.

2. Consider the submodule generated by a subset $A \subseteq M$. By definition, $\langle A \rangle := \bigcup \{N \mid N \subseteq M, a \subseteq N, N \text{ submodules}\}$. The following proposition provides an explicit expression:

   Proposition 3.1. *The submodule generated by $A \subseteq M$ has the following explicit expression:*

   $$\langle A \rangle = \left\{ \sum_{i \in I} a_i x_i \; \middle| \; a_i \in R, \; x_i \in A, \text{ finitely many nonzero } a_i \right\}$$

   Proof. This is simply a re-formalization of the definition. Proceed by showing the double inclusion:

   $\subseteq$: Notice that RHS is indeed a module; and all elements in A are contained in it by setting $a_i = 1$ and x_i to be the desired element.

   $\supseteq$: By the fact that module should be closed w.r.t scalar multiplication and addition.

   $\qquad\square$
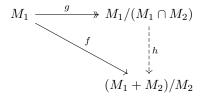
3. Let $(M_i)i \in I$ a family of modules. Then

$$\sum_{i \in I} M_i := \left\langle \bigcup_{i \in I} M_i \right\rangle := \left\{ \sum_{i \in I} x_i \mid x_i \in M_i \ \forall i, \text{ finitely many nonzero } x_i \right\}$$

4. It would be interesting to consider the following isomorphism of quotient of R-modules:

Theorem 3.1 (Third Isomorphism Theorem). *Let M_1 and M_2 be R-submodules of M. Then*

$$(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2)$$

Proof. Consider two functions $f : M_1 \to (M_1 + M_2)/M_2$ and $g : M_1 \to M_1 \cap M_2$. Attempt to show this via applying the first isomorphism theorem. Consider the following diagram:

$$
\begin{array}{ccc}
M_1 & \xrightarrow{\ \ g\ \ } & M_1/(M_1 \cap M_2) \\
& f \searrow & \big\downarrow h \\
& & (M_1 + M_2)/M_2
\end{array}
$$

In order to apply the first isomorphism theorem, it suffices to show that $M_1 \cap M_2 = \ker f$: as then the universal property grants the existence of such h, which allows the application of the First Isomorphism Theorem. This is indeed the case, as

- $M_1 \cap M_2 \subseteq \ker f$, as $M_1 \cap M_2 \subseteq M_2$ which is mapped to 0 by f.

- $M_1 \cap M_2 \supseteq \ker f$. For all $x \in \ker f$, by hypothesis $x \in M_1$; and the only elements that are annihilated by the quotient are those in M_2.

$\qquad \square$

5. Let $N \subseteq M$ a left submodule. Let $I \subseteq R$ an ideal. Then consider the submodule

$$IN := \left\{ IN := \sum_{i \in \mathcal{I}} a_i x_i \ \middle|\ a_i \in I, \ x_i \in N, \text{ finitely many nonzero } a_i \right\}$$

4   Free Modules

Definition 4.1 (Linear Combination (Module)). *Let M be an R-module, with $(x_i)_{i \in I}$ a finite family of elements in M. Then a* ***linear combination*** *of x_is for some fixed family of elements $(r_i)_{i \in I}$ in R is the sum $\sum_{i \in I} x_i r_i$.*

For the following definitions, fix M to be an R-module.

Definition 4.2 (System of Generators). *$(x_i)_{i \in I} \subseteq M$ is a* ***system of generators*** *if $\langle \{x_i \mid i \in I\} \rangle = M$; i.e. every element in M is a finite linear combination of generators.*

Definition 4.3 (Finite Generation). *M is* ***finitely generated*** *if it admits a finite system of generators.*

Definition 4.4 (Linear Independence). *$A \subseteq M$ a subset of M is* ***linearly independent*** *if the finite sum $\sum_{a_i \in A, u_i \in U} a_i u_i = 0$ implies that for all i, $u_i = 0$.*

Definition 4.5 (Basis). *A basis of M is an independent system of generators.*

Definition 4.6 (Free Module). *M is a **Free R-module** if it admits a basis.*

Remark 4.1. R not admitting a multiplicative inverse makes modules slightly different from vector spaces. Consider the following examples:

1. A nonzero module may not admit an independent subset. For example $R = \mathbb{Z}$ with $M = \mathbb{Z}/n\mathbb{Z}$. Then n annihilates the whole ring.

2. For $N \subseteq M$ a submodule, generally $M \cong N \oplus M/N$ does not hold. Take the example where $M = \mathbb{Z}$ and $N = n\mathbb{Z}$. $N \oplus (M/N)$ is not an integral domain as $n \cdot (0,1) = (0,0)$; but M is effectively an integral domain.

3. Similar to the case of vector spaces, it is useful to think in terms of modules in the canonical form. A useful result in vector space is that all K-vector spaces with dimension n is isomorphic to K^n. We make the analogy in terms of modules.

   Let I be a set. Denote $R^{(I)} := \bigoplus_{i \in I} M_i = \left\{ (x_i)_{i \in I} \;\middle|\; \text{finitely nonzero } x_i\text{s} \right\}$, where $M_i = R$. This has a basis $(e_j)_{j \in I}$ which has 1 in the j-th entry. Every free (left) R-module is isomorphism to some $R^{(I)}$ which sends the bases to bases.

4. If R is commutative, then any two bases of a free R-module has the same cardinality (which is given by considering the quotient of maximal ideals and observe that every basis is a basis in the field; which has the same cardinality as this is in a vector space). But this can fail if R is not commutative.

Theorem 4.1 (Universal Property of Free Modules). *Let F be a free R-module with basis $(e_i)_{i \in I}$, and N an arbitrary R-module. For all $(u_i)_{i \in I} \subseteq N$, there exists a unique morphism of R-modules $f : F \to N$ s.t. $f(e_i) = u_i$ for all i.*

Proof. f gives the definition and therefore restricts the map to be unique. The fact that e_is construct a basis in F ensures that this is a morphism of R-modules. $\qquad\square$

Remark 4.2. The general thought is the same as that of the universal property of ring homomorphisms of polynomial rings, where it is possible to decomposition the whole structure into several discrete structures; and designate maps on them correspondingly.

5   Finiteness Conditions on Modules

Definition 5.1 (Noetherian Module). *Let R be a ring and M a left R-module. Then M is **Noetherian** if it satisfies the ACC (Ascending Chain) condition on submodules, i.e. there does not exist a family of submodules of M $(M_i)_{i \in I}$ s.t.*

$$(0) \subseteq M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n \subsetneq \cdots$$

Definition 5.2 (Artinian Module). *Let R be a ring and M a left R-module. Then M is **Artinian** if it satisfies the DCC (Descending Chain) condition on submodules, i.e. there does not exist a family of submodules of M $(M_i)_{i \in I}$ s.t.*

$$\cdots \subsetneq M_n \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 \subseteq M$$

Remark 5.1. R is Noetherian (or Artinian) if it is a Noetherian (or Artinian) R-module.

Proof. This simply results from the fact that when R is taken as an R-module, then its submodules are the ideals of R. $\qquad\square$

Remark 5.2. M is a Noetherian R-module if and only if all of its submodules are finitely generated. The proof is generally the same as that for rings.

Remark 5.3. Modules generally are not Artinian. The ring of integers $\mathbb{Z}$ is a clear counterexample, with the infinite descending chain (2^n). The following are some examples:

- All K fields. This is trivial as the only ideals in K are (1) and (0); and submodules of a ring corresponds to its ideals.

- $\mathbb{Z}/n\mathbb{Z}$ for all $n \in \mathbb{Z}_{\geq 0}$. Rings of such form are finite, which can only admit finitely many ideals as they are by definition subsets of R.

- $K[x]/(x^n)$ for all $n \in \mathbb{Z}_{\geq 0}$ and K fields. Since $K[x]/(x^n)$ contains only elements of degree less than or equal to $(n-1)$ and K is a field, any element with degree $n_0 < n$ linearly spans all elements of the same degree.

  Claim that if $I_1 \subsetneq I_2$ in $k[x]/x^n$, then there exists some k s.t. $n^k \notin I_1$ and $n^k \in I_2$. Suppose not, i.e. for all k there exists some $a_1^{(k)}, a_2^{(k)} \in K$ s.t. $a_1^{(k)} n^k \in I_1$ and $a_2^{(k)} n^k \in I_2$. Since $(a_1^{(k)})^{-1} a_2^{(k)} \in K$, this implies that $I_2 \subseteq I_1$, which is a contradiction.

  Therefore, for each proper submodule the number of monomials with different degrees in the submodule must decrease; and since there are only finitely many (n) of them, the descending chain must terminate at some point.

Proposition 5.1. *Let N be a submodule of M. Then M is Noetherian (or Artinian) if and only if both N and M/N are Noetherian (or Artinian)*

Proof. Consider implication in both directions:

$\Rightarrow$: Since M is Noetherian, all of its submodules are finitely generated. Since N is a submodule of M, all of its submodules are also submodules of M, which are finitely generated, i.e. N is Noetherian.

To verify that the quotient module M/N is Noetherian, consider the following parenthesis:

Parenthesis 5.1 (Correspondence). There is a bijection between submodules of M/N and submodules of M containing N.

Proof. It suffices to specify the map and check that it is indeed bijective. Define $\pi : M \to M/N$ which is the induced morphism of R-modules. Check that it is bijective:

- For any submodule $U \subseteq M/N$, $\pi^{-1}(U) = \{u + n \mid u \in U, n \in N_s\}$ where $N_s \subseteq N$ is an arbitrary submodule of N. Codomain being submodules in M containing N restricts $N_s = N$. This gives $\pi(\pi^{-1}(U)) = U$ by definition of the quotient.

- For any submodule $S \subseteq M$, $\pi(S) = \{\pi(s) \mid s \in S\}$; with $\pi^{-1}(\pi(S)) = \{s + n \mid s \in S, n \in N_s\}$ where N_s is some submodule of N. Similarly since it is required that the module in M should contain N, it fixes $N_s = N$.

$\square$

$\Leftarrow$: The general idea is to split M into those contained in N and those which maps non-trivially to M/N, and use the fact that both N and M/N are Noetherian to conclude that any ascending chain in M must also stabilize.

Consider $\{M_1, \cdots, M_n, \cdots\}$ to be an infinite ascending chain s.t. $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$. We seek to verify that this ascending chain stabilizes at some time, i.e. there exists some n_0 s.t. for all $n \geq n_0$, $M_n = M_{n+1}$. Consider the following two ascending chains:

(1) $M_1 \cap N \subseteq \cdots \subseteq M_k \cap N \subseteq \cdots$

(2) $\pi(M_1) \subseteq \cdots \subseteq \pi(M_k) \subseteq \cdots$

Since both N and M/N are Noetherian, the two chains must stabilize, i.e. there exists some i_0 s.t. beyond which both chains stabilize. Claim that $n_0 = i_0$. It suffices to verify that $\forall i \geq i_0$, $M_{i+1} = M_i$. By definition $M_i \subseteq M_{i+1}$. For inclusion in the other direction consider $x \in M_i$ and $y \in M_{i+1}$. Notice $\pi(x) = \pi(y)$ since $M_i/N = M_{i+1}/N$ by hypothesis, i.e. $x - y \in \ker \pi = N$. Further notice that $x - y \in M_{i+1}$ by inclusion $M_i \subseteq M_{i+1}$. Therefore $x - y \in M_{i+1} \cap N$. Since the first chain stabilizes, $x - y \in M_i \cap N$, i.e. $x \in M_i \cap N$, which implies $x \in M_i$. This gives $M_{i+1} \subseteq M$, i.e. $M_i = M_{i+1}$.

$\square$

Corollary 5.1. Let M_1, M_2 be left R-modules. Then $M_1 \oplus M_2$ is Noetherian (Artinian) if and only if both M_1 and M_2 are Noetherian (Artinian). If R is Noetherian, then R^n is Noetherian for all $n \in \mathbb{Z}_{\geq 0}$.

Remark 5.4. In Remark 4.1 it is mentioned that generally $M \not\simeq M/N \times N$. However this is true if the product is an internal direct sum. Generally, if there exists some submodule $K \subseteq M_1 \oplus M_2$ s.t. $K \simeq M_1$, then $(M_1 \oplus M_2)/K \simeq M_2$.

Proposition 5.2. *Let R be a left Noetherian ring. Then a left R-module M is Noetherian if and only if M is finitely generated.*

Proof. Proceed via showing implication in two directions:

$\Rightarrow$: M being Noetherian implies that every submodule of it is finitely generated. Specifically, M is finitely generated.

$\Leftarrow$: Proceed via finding a surjective map from a Noetherian R-module to M. Since M is finitely generated, it attains a system of generators in the form of $\{u_1, \cdots, u_n\}$. Consider the morphism of R-modules $\varphi : R^n \to M$ s.t. $\varphi(e_i) = u_i$, where e_i is the i-th element of the canonical basis of R^n. Since u_is give a system of generators, φ is surjective. M having an infinite ascending chain implies there exists an infinite ascending chain in R^n, which contradicts the hypothesis that R is Noetherian. Therefore M is Noetherian.

$\square$

6 Modules of Finite Length

7 Digression on Commutative Algebra

8 Artinian/Noetherian Commutative Ring

9 Finitely Generated Modules Over PIDs