MATH 593 - Module

AResseges Stery

October 2, 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 $a_1, a_2 \in R$, $(a_1 + a_2)x = a_1x + a_2x$.*
  - *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/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 ideal. 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 R-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 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

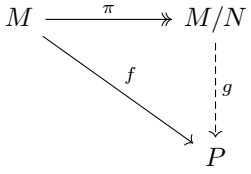
$\Rightarrow$: Consider the contraposition. Suppose that $0 \neq a \in \ker f$. Then $f(1) = f(1 + a)$ with $1 \neq 1 + a$ which is a contradiction.

$\Leftarrow$: 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 $0 \neq (a - b) \in \ker$.

□

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:*

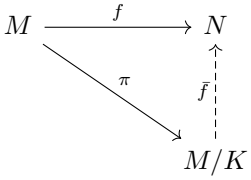


Proof. It suffices to verify that such map exists and is unique.

- *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.

□

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:*



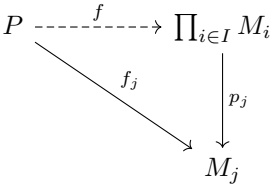
Then $\bar{f}$ is an isomorphism.

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 $(x - y) \in K$. □

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:*

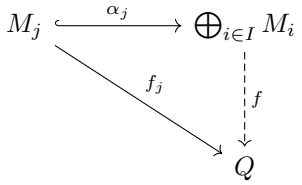


Proof. Uniqueness follows from the fact that $p_j \circ f$ should commute with f_j for all j. Existence holds as f_j is itself a morphism of R-modules. □

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.*

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

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:



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. □

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:*

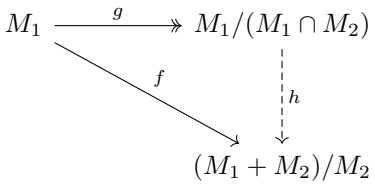
   $$\langle A\rangle = \left\{ \sum_{i\in I} a_i x_i \;\middle|\; a_i \in R,\ x_i \in A,\ \textit{finitely many nonzero } a_i \right\}$$

   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.

   □



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:

   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.

   □

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 are for some fixed family of elements $(r_i)_{i\in I}$ in R $\sum_{i\in I} x_i r_i$.*

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 a 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 $R^{(I)} := \bigoplus_{i\in I} M_i = \left\{(x_i)_{i\in I} \;\middle|\; \text{finitely nonzero } x_i\right\}$, 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 both sides are bases ensures that this is a morphism of R-modules. □

Remark 4.2. The general thought is the same as where 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

6 Modules of Finite Length