R.2. Modules

Let R be a $\mathbb{Z}$-algebra with identity $1 \in R$.

Definition R.2.1. —

- A **left R-module** is a set M with functions $+\colon M \times M \to M$ (**addition**) and (the **R-action** or **scalar multiplication**) $\times\colon R \times M \to M$ (we write $m_1 + m_2$ instead of $+(m_1, m_2)$ and rm instead of $\times(r, m)$) such that
  (a) If $m_1, m_2, m_3 \in M$ then $(m_1 + m_2) + m_3 = m_1 + (m_2 + m_3)$,
  (b) If $m_1, m_2 \in M$ then $m_1 + m_2 = m_2 + m_1$,
  (c) There exists a **zero**, or **additive identity**, $0 \in M$ such that if $m \in M$ then $0 + m = m$,
  (d) If $m \in M$ then there exists $-m \in M$, the **additive inverse of** m, such that $m + (-m) = 0$,
  (e) If $r_1, r_2 \in R$ and $m \in M$ then $r_1(r_2 m) = (r_1 r_2)m$,
  (f) If $m \in M$ then $1m = m$,
  (g) If $r \in R$ and $m_1, m_2 \in M$ then $r(m_1 + m_2) = rm_1 + rm_2$,
  (h) If $r_1, r_2 \in R$ and $m \in M$ then $(r_1 + r_2)m = r_1 m + r_2 m$.
- A **submodule** of a left R-module M is a subset $N \subseteq M$ such that
  (a) If $n_1, n_2 \in N$ then $n_1 + n_2 \in N$,
  (b) $0 \in N$,
  (c) If $n \in N$ then $-n \in N$,
  (d) If $r \in R$ and $n \in N$ then $rn \in N$.
- The **zero R-module** $\{0\}$ is the set containing only 0 with the operations $+$ and $\times$ given by $0 + 0 = 0$ and $r \cdot 0 = 0$ for $r \in R$.

R-modules are the analogues of group actions except for rings.

The conditions (a), (b), (c) and (d) in the definition of a left R-module imply that every left R-module is an abelian group under addition.

HW: Show that the element $0 \in M$ is unique.

HW: Show that if $m \in M$ then the element $-m \in M$ is unique.

HW: Show that if $m \in M$ then $0m = 0$. (The 0 on the left hand side of this equation is the zero in R and the 0 on the right hand side of this equation is the zero in M.)

HW: Show that if $r \in R$ then $r\,0 = 0$. (The 0 on both sides of this equation is the zero in M.)

Important examples of modules are:

(a) If R is a ring then R, with the operation of left multiplication, is a left R-module.
(b) The abelian groups are the $\mathbb{Z}$-modules.
(c) If $\mathbb{F}$ is a field then the $\mathbb{F}$-modules are the $\mathbb{F}$-vector spaces.

Notes of Arun Ram aram@unimelb.edu.au, Version: 7 April 2020

Module homomorphisms are used to compare R-modules. A module homomorphism must preserve the structures that distinguish an R-module: the addition and the R-action.

Definition R.2.2. —

- An R-**module homomorphism** is a function $f\colon M \to N$ between left R-modules M and N such that
  (a) If $m_1, m_2 \in M$ then $f(m_1 + m_2) = f(m_1) + f(m_2)$,
  (b) If $r \in R$ and $m \in M$ then $f(rm) = rf(m)$.
- An R-**module isomorphism** is an R-module homomorphism $f\colon M \to N$ such that the inverse function $f^{-1}\colon N \to M$ exists and f^{-1} is an R-module homomorphism.
- Two left R-modules M and N are **isomorphic**, $M \simeq N$, if there exists an R-module isomorphism between them.

Two R-modules are isomorphic if the elements of the modules spaces and the operations and the actions match up exactly. Think of two modules that are isomorphic as being "the same".

HW: Let $f\colon M \to N$ be an R-module homomorphism. Show that f is an isomorphism if and only if f is bijective.

Condition (a) in the definition of an R-module homomorphism implies that f is a group homomorphism.

Proposition R.2.1. — *Let $f\colon M \to N$ be an R-module homomorphism. Let 0_M and 0_N be the zeros for M and N respectively. Then*
(a) *$f(0_M) = 0_N$, and*
(b) *If $m \in M$ then $f(-m) = -f(m)$.*

R.2.1. Cosets. —

Definition R.2.3. —

- A **subgroup** of a left R-module M is a subset $N \subseteq M$ such that
  (a) If $n_1, n_2 \in N$ then $n_1 + n_2 \in N$,
  (b) $0 \in N$,
  (c) If $n \in N$ then $-n \in N$.

Let M be a left R-module and let N be a subgroup of M. We will use the subgroup N to divide up the module M.

Definition R.2.4. —

- A **coset** of N in M is a set $m + N = \{m + n \mid n \in N\}$, where $m \in M$.
- M/N (pronounced "M **mod** N") is the set of cosets of N in M.

Proposition R.2.2. — *Let M be a left R-module and let N be a subgroup of M. Then the cosets of N in M partition M.*

Notice the analogy between Proposition F.2.2 and Proposition R.1.2 and Proposition R.2.2 and Proposition G.1.2.

R.2.2. Quotient Modules ↔ Submodules. — Let M be a left R-module and let N be a subgroup of M. We can try to make the set M/N of cosets of N in M into an R-module by defining an addition operation and an action of R. This doesn't work with just any subgroup of N, the subgroup must be a submodule.

Theorem R.2.3. — *Let N be a subgroup of a left R-module M. Then N is a submodule of M if and only if M/N with the operations given by*

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N \qquad \textit{and} \qquad r(m_1 + N) = rm_1 + N,$$

is a left R-module.

Notice the analogy between Theorem F.2.3, Theorem R.2.3, Theorem R.1.3 and Theorem G.1.5.

Definition R.2.5. —

- The **quotient module** M/N is the left R-module of cosets of a submodule N of an R-module M with operations given by

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N \qquad \text{and} \qquad r(m_1 + N) = rm_1 + N.$$

So we have successfully made M/N into a left R-module when N is a submodule of M.

HW: Show that if $N = M$ then $M/N \simeq \{0\}$.

R.2.3. Kernel and image of a homomorphism. —

Definition R.2.6. — Let $f\colon M \to N$ be an R-module homomorphism.

- The **kernel** of f is the set

$$\ker f = \{m \in M \mid f(m) = 0_N\},$$

where 0_N is the zero in N.

- The **image** of f is the set

$$\mathrm{im} f = \{f(m) \mid m \in M\}.$$

Proposition R.2.4. — *Let $f\colon M \to N$ be an R-module homomorphism. Then*

(a) $\ker f$ *is a submodule of M.*

(b) $\mathrm{im}\, f$ *is a submodule of N.*

Proposition R.2.5. — *Let $f\colon M \to N$ be an R-module homomorphism. Let 0_M be the zero in M. Then*

(a) $\ker f = \{0_M\}$ *if and only if f is injective.*

(b) $\mathrm{im} f = N$ *if and only if f is surjective.*

Notice that the proof of Proposition R.2.5 (b) does not use the fact that $f\colon M \to N$ is a homomorphism, only the fact that $f\colon M \to N$ is a function.

Theorem R.2.6. —

(a) Let $f\colon M \to N$ be an R-module homomorphism and let $K = \ker f$. Define

$$\begin{array}{rccc} \hat{f}\colon & M/\ker f & \to & N \\ & m + K & \mapsto & f(m). \end{array}$$

Then $\hat{f}$ is a well defined injective R-module homomorphism.

(b) Let $f\colon M \to N$ be an R-module homomorphism and define

$$\begin{array}{rccc} f'\colon & M & \to & \mathrm{im} f \\ & m & \mapsto & f(m). \end{array}$$

Then f' is a well defined surjective R-module homomorphism.

(c) If $f\colon M \to N$ is an R-module homomorphism, then

$$M/\ker f \simeq \mathrm{im} f,$$

where the isomorphism is an R-module isomorphism.

R.2.4. Direct Sums. — Suppose M and N are R-modules. The idea is to make $M \times N$ into an R-module.

Definition R.2.7. —

- The **direct sum**, $M \oplus N$, of two left R-modules M and N is the set $M \times N$ with operations given by

  $$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2) \quad \text{and} \qquad r(m_1, n_1) = (rm_1, rn_1)$$

  for $m_1, m_2 \in M$, $n_1, n_2 \in N$, and $r \in R$.
- More generally, given left R-modules $M_1, \ldots, M_n$, the **direct sum** $M_1 \oplus \cdots \oplus M_n$ is the set given by $M_1 \times \cdots \times M_n$ with operations given by

  $$\begin{aligned} (m_1, \ldots, m_i, \ldots, m_n) + (n_1, \ldots, n_i, \ldots, n_n) &= (m_1 + n_1, \ldots, m_i + n_i, \ldots, m_n + n_n) \\ \text{and} \quad r(m_1, ..., m_i, ..., m_n) &= (rm_1, ..., rm_i, ..., rm_n), \end{aligned}$$

  where $m_i, n_i \in M$ and $m_i + n_i$ and rm_i are given by the operations for the module M_i.

The operations on the direct sum are just the operations from the original modules acting **componentwise**.

HW: Show that these are good definitions, i.e. that, as defined above, $M \oplus N$ and $M_1 \oplus \cdots \oplus M_n$ are left R-modules with zeros given by $(0_M, 0_N)$ and $(0_{M_1}, \ldots, 0_{M_N})$ respectively. (0_{M_i} denotes the zero in the left R-module M_i.)

R.2.5. Further Definitions. —

Definition R.2.8. —

- Let M be a left R-module and let S be a subset of M. The **submodule generated by** S is the submodule $\mathrm{span}_R(S)$ of M such that
  (a) $S \subseteq \mathrm{span}_R(S)$,
  (b) If T is a submodule of M and $S \subseteq T$ then $\mathrm{span}_R(S) \subseteq T$.

The left R-module $\mathrm{span}_R(S)$ is the smallest submodule of M containing S. Think of $\mathrm{span}_R(S)$ as gotten by adding to S exactly those elements of M that are needed to make a submodule.

Definition R.2.9. —

- A **proper submodule** of an R-module M is a submodule that is not $\{0\}$ or M.
- A **maximal proper submodule** of an R-module M is a proper submodule of M that is not contained in any other proper submodule of M.
- A **simple module** is an R-module with no proper submodules.

HW: Let $\mathbb{F}$ be a field and let $n \in \mathbb{Z}_{>0}$. Show that the $\mathbb{F}$-module $\mathbb{F}^n$ of column vectors of length n is a simple module for the ring $M_n(\mathbb{F})$ of $n \times n$ matrices with entries in $\mathbb{F}$.