L16: R-module homomorphisms

Definition 16.1: $\mathrm{Hom}_R(M,N)$, Kernel, Image, Isomorphism

The **set of R-module homomorphisms from M to N** is denoted $\mathrm{Hom}_R(M,N)$.
The **kernel** of an R-module homomorphism $f \in \mathrm{Hom}_R(M,N)$ is

$$\mathrm{Ker}\, f \coloneqq \{m \in M \mid f(m) = 0\}$$

The **image** of $f \in \mathrm{Hom}_R(M,N)$ is

$$\mathrm{Im}\, f \coloneqq \{n \in N \mid \exists m \in M,\ f(m) = n\}$$

If $f \in \mathrm{Hom}_R(M,N)$ is bijective then we say f is an **isomorphism of R-modules**. We say M, N are **isomorphic** if there is an isomorphism $f\colon M \to N$ and we write $M \cong N$.

Example 16.1. $R = \mathbb{Z}, M = \mathbb{Z}$ is a $\mathbb{Z}$-module.
Note: A subtle distinction between this and the ring of integers $\mathbb{Z}$ is that you don't have multiplication between the elements of the module but rather it has an action of the integers by multiplication.
What do the $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ look like? Consider

$$\begin{aligned} f\colon \mathbb{Z} &\to \mathbb{Z} \\ 1 &\mapsto a \\ n &\mapsto \underbrace{a + a + a + \cdots + a}_{n\text{-times}} \end{aligned}$$

Then we see that, in this case, f is specified by where it sends one, i.e $f(1) = a$.

Note: There are functions f which are R-module homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ which are not ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$. Consider the doubling function

$$\begin{aligned} f_2\colon \mathbb{Z} &\to \mathbb{Z} \\ 1 &\mapsto 2 \end{aligned}$$

is a $\mathbb{Z}$-module homomorphism as

$$\begin{aligned} f_2(m+n) &= 2 \cdot (m+n) = 2 \cdot m + 2 \cdot n = f_2(m) + f_2(n) \\ f_2(a \cdot m) &= 2 \cdot (a \cdot m) = a \cdot 2 \cdot m = a \cdot f_2(m) \end{aligned}$$

However it is **not** a ring homomorphism as

$$f_2(2 \cdot 3) = 2 \cdot 2 \cdot 3 = 12 \neq 24 = 4 \cdot 6 = (2 \cdot 2) \cdot (3 \cdot 2) = f_2(2) \cdot f_2(3)$$

Proposition 16.2: Kernel and Image are submodules

Suppose $f \in \mathrm{Hom}_R(M,N)$. Then the kernel, $\mathrm{Ker}\, f \subset M$, and the image, $\mathrm{Im}\, f \subset N$, are R-submodules.

Proof. First we prove the claim for the kernel. If $a, b \in \operatorname{Ker} f$ and $r \in R$ then

- $f(0) = 0 \implies 0 \in \operatorname{Ker} f$
- $f(a+b) = f(a) + f(b) = 0 + 0 = 0 \implies a + b \in \operatorname{Ker} f$
- $f(r \cdot a) = r \cdot f(a) = r \cdot 0 = 0 \implies r \cdot a \in \operatorname{Ker} f$
- $0 = f(0) = f(a + (-a)) = f(a) + f(-a) = 0 + f(-a) = f(-a) \implies -a \in \operatorname{Ker} f$

hence, $\operatorname{Ker} f \subset M$ is a submodule.
If $a, b \in \operatorname{Im} f, r \in R$ such that $a = f(a'), b = f(b')$ for $a', b' \in M$, then

- $f(0) = 0 \implies 0 \in \operatorname{Im} f$
- $a + b = f(a') + f(b') = f(a' + b') \implies a + b \in \operatorname{Im} f$
- $r \cdot a = r \cdot f(a') = f(r \cdot a') \implies r \cdot a \in \operatorname{Im} f$
- $-a = -f(a') = f(-a') \implies -a \in \operatorname{Im} f$

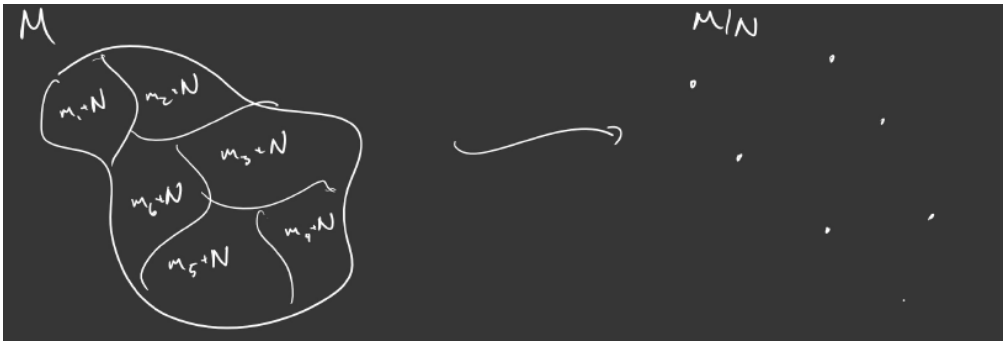
Hence, $\operatorname{Im} f$ is a submodule. ■

Definition 16.3: Coset

If $N \subset M$ is an R-submodule and $m \in M$, then the N **coset** of m is

$$m + N \coloneqq \{m + n \mid n \in N\}$$

Exercise: We can define an equivalence relation on M by $m \sim m'$ if and only if $m + N = m' + N$ as sets.



Definition 16.4: Quotient Module

The **quotient module** of M by N is

$$M/N \coloneqq \{m + N \mid m \in M\}$$

Proposition 16.5: Quotient Module is R-module

Quotient modules are R-modules.

Proof. Define addition of cosets as

$$(m + N) + (m' + N) \coloneqq (m + m') + N$$

Just as for rings, we will write $\overline{m}$ for $m \in M$ if N is understood.
It is simple enough to check that the addition is well defined:

$$m + N = m_1 + N \implies m - m_1 = n \in N$$
$$m' + N = m_1' + N \implies m' - m_1' = n' \in N$$

Then by direct calculation

$$\begin{aligned}(m_1 + N) + (m_1' + N) = (m + m_1') + N &= (m + n + m' + n') + N \\ &= (m + m') + \underbrace{(n + n')}_{\in N} + N = (m + m') + N\end{aligned}$$

If $r \in R$ and $m + N \in M/N$. The R-action is then defined

$$r \cdot (m + N) \coloneqq (r \cdot m) + N$$

Exercise: Check that the R-action is well defined. ■

Proposition 16.6: Canonical quotient map is surjective

The natural quotient map

$$\begin{aligned}p \colon M &\to M/N \\ m &\mapsto M + N\end{aligned}$$

is a surjective R-module homomorphism such that $\operatorname{Ker} p = N$.

Proof. Properties of an R-module homomorphism:

$$p(a + b) = (a + b) + N = (a + N) + (b + N) = p(a) + p(b)$$
$$p(r \cdot a) = (r \cdot a) + N = r \cdot (a + N) = r \cdot p(a)$$

Surjectivity is clear as before (think of the representative of the coset).
Suppose $a \in \operatorname{Ker} p$, then $f(a) = a + N = 0 + N$ i.e. there exists $n \in N$ such that $a - 0 = n \in N$ and hence $a = n \in N$ so that $a \in N$. Hence, $\operatorname{Ker} p \subset N$. Suppose $n \in N$. Then

$$f(n) = n + N \implies n - 0 \in N \implies n + N = 0 + N \implies f(n) = 0 + N \implies n \in \operatorname{Ker} p$$

and therefore $N \subset \operatorname{Ker} p$. ■

Theorem 16.7: The First Isomorphism Theorem

Let M, N be R-modules and $f \in \operatorname{Hom}_R(M, N)$. Then $\operatorname{Ker} f \subset M$ is a submodule and

$$M/\operatorname{Ker} f \cong \operatorname{Im} f$$

Theorem 16.8: The Second Isomorphism Theorem

Let $A, B \subset M$ be submodules, then

$$(A + B)/B \cong A/A \cap B$$

Theorem 16.9: The Third Isomorphism Theorem

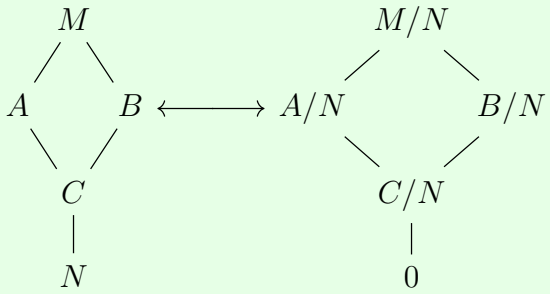
Let $A \subset B \subset M$ be submodules, then

$$(M/A)/(B/A) \cong M/B$$

Theorem 16.10: The Fourth Isomorphism Theorem

There is a bijection of sets

$$\{\text{submodules of } M \text{ containing } N\} \longleftrightarrow \{\text{submodules of } M/N\}$$



Proposition 16.11: $\mathrm{Hom}_R(M,N)$ is an R-module

Suppose M, N are R-modules, then $\mathrm{Hom}_R(M,N)$ is itself an R-module

Proof. Define addition for $f, g \in \mathrm{Hom}_R(M,N)$ as

$$(f+g)(m) \coloneqq f(m) + g(m)$$

Exercise: Check that

$$\begin{aligned} 0 \colon M &\to N \\ m &\mapsto 0 \end{aligned}$$

is the additive identity and

$$\begin{aligned} -f \colon M &\to N \\ m &\mapsto -f(m) \end{aligned}$$

is the additive inverse. Thus it is shown that $\mathrm{Hom}_R(M,N)$ is an abelian group with the binary operation $+$.

Then the R-action for $r \in R$ and $f \in \mathrm{Hom}_R(M,N)$ is

$$\begin{aligned} (r \cdot f) \colon M &\to N \\ m &\mapsto r \cdot f(m) \end{aligned}$$

Exercise: Check that $\mathrm{Hom}_R(M,N)$ satisfies all the R-module action properties. ■

Note: These operations are the same operations one learns for functions in middle school (even linear transformations in Linear Algebra):

$$f\colon \mathbb{R}^n \to \mathbb{R}^m$$

This can be seen by the following

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$
$$\alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix}$$

But there is one additional operation that you can preform with homomorphisms which can not be performed by elements of the module, and that is function composition.

Proposition 16.12

If $f \in \mathrm{Hom}_R(M,N), g \in \mathrm{Hom}_R(N,L)$ then $g \circ f\colon M \to L$ and $g \circ f \in \mathrm{Hom}_R(M,L)$

Proof. Shown by direct check of homomorphism properties
$g \circ f(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x)) + g(f(y)) = g \circ f(x) + g \circ f(y)$
$g \circ f(a \cdot x) = g(f(a \cdot x)) = g(a \cdot f(x)) = a \cdot g(f(x)) = a \cdot g \circ f(x)$ ■

In particular, if $M = N = L$, then $f, g \in \mathrm{Hom}_R(M,M)$ and $g \circ f \in \mathrm{Hom}_R(M,M)$, i.e. you stay in the same set by composition if the domain and range are the same set. This leads naturally to the following observation

Corollary 16.13: $\mathrm{Hom}_R(M,M)$ is a ring

$\mathrm{Hom}_R(M,M)$ is a ring with 1. In this ring, addition are $f+g$ and multiplication as composition $f \circ g$.

Proof. We know $(\mathrm{Hom}_R(M,M), +)$ is an abelian group.
It remains to check that composition is/has
(**Associativity**)

$$[(f \circ g) \circ h](x) = (f \circ g)[h(x)] = f[g(h(x))] = f[(g \circ h)(x)] = [f \circ (g \circ h)](x)$$

(**Distributivity over** $+$)
$[f \circ (g+h)](x) = f[(g+h)(x)] = f[g(x)+h(x)] = f(g(x)) + f(h(x)) = (f \circ g)(x) + (f \circ h)(x)$
(**Identity**) The identity map is simply given by

$$\mathrm{Id}\colon M \to M$$
$$m \mapsto m$$

Exercise: Check that this is truly the identity for composition. ■

Definition 16.14: Endomorphisms and Endomorphism Ring

The ring $\mathrm{Hom}_R(M, M)$ is called the **endomorphism ring** of M. We sometimes denote it by $\mathrm{End}_R(M)$.
The elements of $\mathrm{End}_R(M)$ are **endomorphisms**.

Example 16.2. If M is any R-module and $a \in R$ where R is commutative, then we can define

$$\begin{aligned} a \cdot \mathrm{Id} \colon M &\to M \\ m &\mapsto a \cdot m \end{aligned}$$

is an endomorphism.

Proof. Simply check homomorphism properties

$$(a \cdot \mathrm{Id})(m+n) \coloneqq a \cdot (m+n) = a \cdot m + a \cdot n = (a \cdot \mathrm{Id})(m) + (a \cdot \mathrm{Id})(n)$$
$$(a \cdot \mathrm{Id})(r \cdot m) \coloneqq a \cdot (r \cdot m) = (ar) \cdot m = (ra) \cdot m = r \cdot (a \cdot m) = r \cdot (a \cdot \mathrm{Id})(m) \qquad \blacksquare$$

This leads naturally the the following map from the ring R to the endomorphisms:

$$\begin{aligned} f \colon R &\to \mathrm{End}_R(M) \\ r &\mapsto r \cdot \mathrm{Id} \end{aligned}$$

Claim: This map is a ring homomorphism.

Proof. We check ring homomorphism properties for $r, s \in R$

$$f(r+s) \coloneqq (r+s) \cdot \mathrm{Id} = r \cdot \mathrm{Id} + s \cdot \mathrm{Id} = f(r) + f(s)$$
$$f(rs) = (rs) \cdot \mathrm{Id} = (r \cdot \mathrm{Id}) \circ (s \cdot \mathrm{Id}) = f(r) \cdot f(s) \qquad \blacksquare$$

The equality in blue can be seen by evaluating at $m \in M$,

$$[(rs) \cdot \mathrm{Id}](m) = (rs) \cdot m = r \cdot (s \cdot m) = r \cdot (s \cdot \mathrm{Id})(m) = (r \cdot \mathrm{Id}) \circ (s \cdot \mathrm{Id})(m)$$

Warning: This map is not always injective as seen by the following example:

Example 16.3. $\mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module and so consider the map

$$\begin{aligned} f \colon \mathbb{Z} &\to \mathrm{End}(\mathbb{Z}/4\mathbb{Z}) \\ 4 &\mapsto 4 \cdot \mathrm{Id} \end{aligned}$$

However we can see that $\mathrm{Ker}\, f$ does not contain only 0,

$$4 \cdot \mathrm{Id}(\overline{a}) = 4 \cdot \overline{a} = \overline{4a} = \overline{0} \implies 4 \in \mathrm{Ker}\, f$$

Hence f is not injective.