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

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

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

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

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.
What do the $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ look like?

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

Note: 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

$$f_2(m+n) = 2 \cdot (m+n) = 2 \cdot m + 2 \cdot n = f_2(m) + f_2(n)$$
$$f_2(a \cdot m) = 2 \cdot (a \cdot m) = a \cdot 2 \cdot m = a f_2(m)$$

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 on the kernel. If $a, b \in \mathrm{Ker}\, f$ and $r \in R$ then

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

hence, $\mathrm{Ker}\, f \subset M$ is a submodule.

If $a, b \in \operatorname{Im} f, r \in R$ say $a = f(a'), b = f(b'), a', b' \in M$

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

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

$$m + N := \{m + n \mid n \in N\}$$

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

$$M/N := \{m + N \mid m \in M\}$$

Proposition 16.5: Quotient Module is R-module

Quotient modules are R-modules

Proof. Define addition of cosets as

$$(m + N) + (m' + N) := (m + m') + N$$

We will write $\overline{m}$ for $m \in M$ if N is understood.

Exercise: Check for well-definedness

$$m + N = m_1 + N \implies m - m_1 = n \in N$$
$$m' + N = m'_1 + N \implies m' - m'_1 = n' \in N$$

Then

$$\begin{aligned}(m_1 + N) + (m'_1 + N) = (m + m'_1) + N =& (m + n + m' + n') + N \\ =& (m + m') + \underbrace{(n + n')}_{\in N} + N = (m + m') + N\end{aligned}$$

If $r \in R$ and $m + N \in M/N$. The R-action is then defined $r \cdot (m + N) := (rm) + N$.

Exercise: Check it is well defined. ■

Proposition 16.6: Canonical quotient map

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:

$$\begin{aligned} p(a+b) &= (a+b)+N = (a+N)+(b+N) = p(a)+p(b) \\ p(ra) &= (ra)+N = r(a+N) = r \cdot p(a) \end{aligned}$$

Surjectivity is clear.
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 $a \in N$.
Suppose $n \in N$. Then

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

■

Theorem 16.7: Module Isopmorphism Theorems

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

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

(2) Let $A, B \subset M$ be submodules, then

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

(3) Let $A \subset B \subset M$ be submodules, then

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

(4) There is a bijection of sets

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

$$\begin{tikzcd}
& M \arrow[dl, dash] \arrow[dr, dash] & & & M/N \arrow[dl, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & B \arrow[dl, dash] \arrow[r, leftrightarrow] & A/N \arrow[dr, dash] & & B/N \arrow[dl, dash] \\
& C \arrow[d, dash] & & & C/N \arrow[d, dash] & \\
& N & & & 0 &
\end{tikzcd}$$

Proposition 16.8: $\mathrm{Hom}_R(M,N)$ **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

$$(f+g)(m) := f(m) + g(m)$$

Exercise:

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

is the additive identity and

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

is the additive inverse. Hence, $\mathrm{Hom}_R(M,N)$ is an abelian group with $+$.
Then the R-action for $r \in R$ and $f \in \mathrm{Hom}_R(M,N)$ is

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

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

Note: These operations are the same operations we learned for functions (even linear transformations). Let $f\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation, then

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

$$\alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix}$$

Proposition 16.9

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. Check homomorphism properties

$g \circ f(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x)) + g(f(y)) = g \circ f(x) + g \circ f(y)$

$g \circ f(ax) = g(f(ax)) = g(af(x)) = ag(f(x)) = a \bullet g \circ f(x)$ ∎

In particular, if $M = N = L$, then $f, g \in \mathrm{Hom}_R(M,M)$ and $g \circ f \in \mathrm{Hom}_R(M,M)$

Corollary 16.10

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

Proof. We know $(\mathrm{Hom}_R(M,M),+)$ is an abelian group.
We must check that composition is

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

(ii) distributes over addition
$$[f\circ(g+h)](x) = f[(g+h)(x)] = f[g(x)+h(x)] = f(g(x))+f(h(x)) = (f\circ g)(x)+(f\circ h)(x)$$

(iii) has an identity. The identity map is
$$\begin{aligned}\mathrm{Id}\colon M &\to M\\ m &\mapsto m\end{aligned}$$

■

Definition 16.11: 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, $a\in R$, R commutative, then
$$\begin{aligned}a\cdot\mathrm{Id}\colon M &\to M\\ m &\mapsto a\cdot m\end{aligned}$$
is an endomorphism.
Check
$$(a\cdot\mathrm{Id})(m+n) := a\cdot(m+n) = a\cdot m + a\cdot n = (a\cdot\mathrm{Id})(m) + (a\cdot\mathrm{Id})(n)$$
$$(a\cdot\mathrm{Id})(r\cdot m) := a(r\cdot m) = (a\cdot)\cdot m = (r\cdot a)\cdot m = r\cdot(a\cdot m) = r\cdot(a\cdot\mathrm{Id})(m)$$

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

Claim: This map is a ring homomorphism.

Proof. Homomorphism properties
$$f(r+s) := (r+s)\cdot\mathrm{Id} = r\cdot\mathrm{Id} + s\cdot\mathrm{Id} = f(r)+f(s)$$
$$f(r\cdot s) = (r\cdot s)\cdot\mathrm{Id} = (r\cdot\mathrm{Id})\cdot(s\cdot\mathrm{Id}) = f(r)\cdot f(s)$$
$$[(r\cdot s)\cdot\mathrm{Id}](m) = (r\cdot s)\cdot m = r\cdot(s\cdot m) = r\cdot(s\cdot\mathrm{Id})(m) = (r\cdot\mathrm{Id})\cdot(s\cdot\mathrm{Id})(m)$$

■

Warning: This map is not always injective

Example 16.3. $\mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module

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

Then

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

Hence f is not injective.