R-module homomorphisms

<u>Recall</u>: An R-module homomorphism is a map

$$f : M \longrightarrow N$$

s.t.
- $f(m+m') = f(m) + f(m')$ $\quad \forall m, m' \in M$
- $f(a \cdot m) = a \cdot f(m)$ $\quad \forall a \in R,\ m \in M$

<u>Defn</u>: (0) The set of R-module homomorphisms from M to N is denoted $\mathrm{Hom}_R(M,N)$

(1) The <u>kernel</u> of an R-module homomorphism $f \in \mathrm{Hom}_R(M,N)$ is $\mathrm{Ker} f := \{ m \in M \mid f(m) = 0 \}$

(2) The <u>image</u> of $f \in \mathrm{Hom}_R(M,N)$ is $\mathrm{Im} f := \{ n \in N \mid \exists\, m \in M \text{ s.t. } f(m) = n \}$

(3) If $f \in \mathrm{Hom}_R(M,N)$ is bijective then we say f is an <u>isomorphism</u> of R-modules

We say M, N are <u>isomorphic</u> if there is an iso $f : M \to N$.
and we write $M \cong N$

<u>Ex</u>: $R = \mathbb{Z}$, $M = \mathbb{Z}$ as a $\mathbb{Z}$-module

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

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ 1 &\longmapsto a \\ n &\longmapsto \underbrace{a + a + a + \cdots + a}_{n\text{-times}} \end{aligned}$$

f is specified by $f(1) = a$

Note: $f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ is a $\mathbb{Z}$-module homomorphism.
$\qquad 1 \longmapsto 2$

$\mathbb{Z}$-mod homom.
$$\left[\begin{array}{l} f_2(m+n) = 2\cdot(m+n) = 2m + 2n = 2f_2(m) + 2\cdot f_2(n) \\ f_2(a\cdot m) = 2\cdot(a\cdot m) = a\cdot 2m = a\cdot f_2(m) \end{array}\right.$$

BUT: f_2 is not a ring homomorphism.

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

Don't agree.

Prop: Suppose $f \in \mathrm{Hom}_R(M, N)$

The kernel $\mathrm{Ker} f \subset M$ is an R-submodule

The image $\mathrm{Im} f \subset N$ is an R-submodule.

Pf: • $f(0) = 0 \implies 0 \in \mathrm{Ker} f$

• If $a, b \in \mathrm{Ker} f$, $r \in R$.

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

$$0 = f(0) = f(a + (-a)) = f(a) + f(-a) = 0 + f(-a)$$
$$= f(-a) \implies -a \in \mathrm{Ker} f.$$

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

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

• $f(0) = 0 \implies 0 \in \mathrm{Im} f$

• $a+b = f(a') + f(b') = f(a'+b') \implies a+b \in \mathrm{Im} f$

• $ra = r\cdot f(a') = f(r\cdot a') \implies ra \in \mathrm{Im} f$

• $-a = -f(a') = f(-a') \implies -a \in \mathrm{Im} f$. $\square$

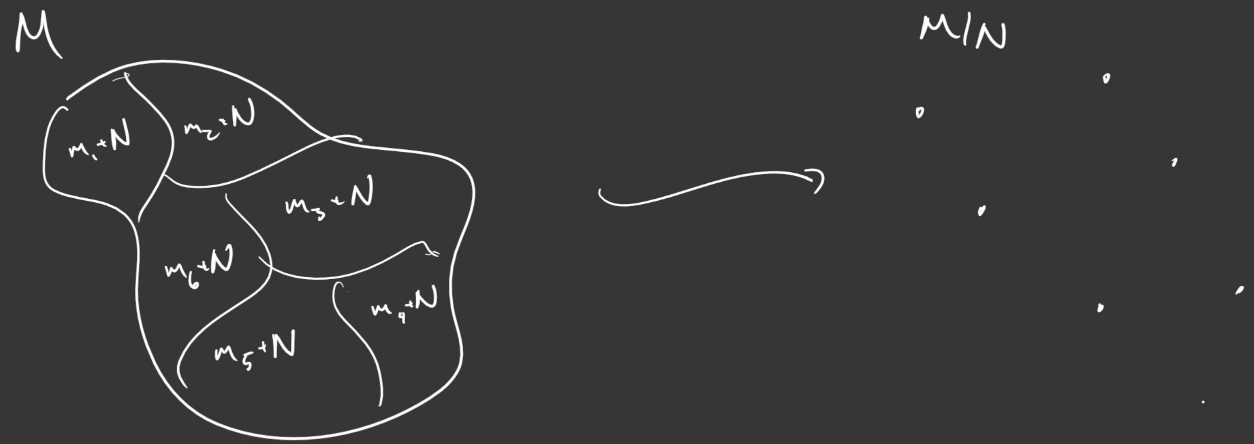
Defn: If $N \subset M$ is an R-submodule and $m \in M$

Then the <u>N coset</u> of m is

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

Easy check: we can define an equivalence relation on M by

$$m \sim m' \text{ iff } m + N = m' + N \text{ as sets}$$



Defn: The <u>quotient module</u> of M by N is

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

Prop: Quotient modules are R-modules

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

Notation: we'll write $\bar{m}$ for $m + N$ if N is understood.

Check for well-definedness

$$\text{Say } \begin{array}{l} m + N = m_1 + N \\ m' + N = m_1' + N \end{array} \implies \begin{array}{l} \overset{n}{\overset{\shortparallel}{m - m_1}} \in N \\ \underset{n'}{\underset{\shortparallel}{m' - m_1'}} \in N \end{array}$$

$$\implies (m_1 + N) + (m_1' + N) = (m_1 + m_1') + N = (m + n + m' + n') + N$$
$$= (m + m') + \underbrace{(n + n')}_{\in N} + N = (m + m') + N$$

If $r \in R$, $m+N \in M/N$.

R-action: $r.(m+N) := (rm)+N$

Easy check: This is well-defined $\square$

<u>Prop</u>: The natural quotient map

$$p: M \longrightarrow M/N$$
$$m \longmapsto m+N$$

is a surjective R-module homomorphism.

s.t. $\operatorname{Ker} p = N$

<u>Pf</u>: $p(a+b) = (a+b)+N = (a+N)+(b+N) = p(a)+p(b)$

$p(ra) = (ra)+N = r(a+N) = r.p(a)$

Surjectivity is clear.

$\operatorname{Ker} p \subset N$: Suppose $a \in \operatorname{Ker} p$.

So $f(a) = a+N = 0+N$

i.e. $\exists n \in N$ s.t. $a-0 = n \in N$

i.e. $a = n \in N \Longrightarrow a \in N$.

$N \subset \operatorname{Ker} p$: Suppose $n \in N$.

$f(n) = n+N$

$n-0 \in N \Longrightarrow n+N = 0+N \Longrightarrow f(n) = 0+N$

$\Longrightarrow n \in \operatorname{Ker} p$ $\square$

The Isomorphism Thms

Thm:

1. Let M, N be R-modules, $f \in \mathrm{Hom}_R(M,N)$

   Then $\mathrm{Ker} f \subset M$ is a submodule and

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

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

4. There is a bijection of sets

   $$\left\{ \begin{array}{c} \text{Submodules of } M \\ \text{containing } N \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Submodules} \\ \text{of } M/N \end{array} \right\}$$

$$\begin{tikzcd}[column sep=small]
 & M \arrow[dl, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & B \arrow[dl, dash] \\
 & N &
\end{tikzcd}
\quad \longleftrightarrow \quad
\begin{tikzcd}[column sep=small]
 & M/N \arrow[dl, dash] \arrow[dr, dash] & \\
A/N \arrow[dr, dash] & & B/N \arrow[dl, dash] \\
 & 0 &
\end{tikzcd}$$

Prop: Suppose M, N be R-modules. Then $\mathrm{Hom}_R(M,N)$ is itself an R-module.

Pf: Addition: $f, g \in \mathrm{Hom}_R(M,N)$

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

Easy check: $0 : M \longrightarrow N$, $m \longmapsto 0$ is the additive identity in $\mathrm{Hom}_R(M,N)$

$$-f : M \longrightarrow N$$
$$m \longmapsto -f(m)$$

$\Longrightarrow$ $\mathrm{Hom}_R(M,N)$ is an abelian group with $+$.

R-action: $r \in R$, $f \in \mathrm{Hom}_R(M,N)$

$$(r \cdot f) : M \longrightarrow N$$
$$m \longmapsto r \cdot f(m)$$

Easy check: $\mathrm{Hom}_R(M,N)$ satisfies all the R-module action properties with this action $\square$

Note: These are operations are the same operations we learned for functions (even linear transformations)

$$f : \mathbb{R}^n \longrightarrow \mathbb{R}^m$$

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

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

Prop: If $f \in \mathrm{Hom}_R(M,N)$, $g \in \mathrm{Hom}_R(N,L)$

then $g \circ f : M \longrightarrow L$ and $g \circ f \in \mathrm{Hom}_R(M,L)$

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

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

$g \circ f(ax) = g(f(ax)) = g(af(x)) = a\, g(f(x))$

$= a \cdot g\circ f(x)$

$\square$

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

$g\circ f \in \mathrm{Hom}_R(M,M)$

Cor: $\mathrm{Hom}_R(M,M)$ is a <u>ring</u> with 1

addition $f+g$ as above

multiplication $f \circ g$

Pf: $(\mathrm{Hom}_R(M,M), +)$ is an abelian group

we must check that composition is

- associative
- distributes over addition
- has an identity

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

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

- Identity is the identity map $\mathrm{Id} : M \longrightarrow M$, $m \longmapsto m$

$\square$

<u>Defn:</u> The ring $\mathrm{Hom}_R(M,M)$ is called the <u>endomorphism ring</u> of M

we sometimes denote it by $\mathrm{End}_R(M)$

The elements of $\mathrm{End}_R(M)$ are <u>endomorphisms</u>

<u>Example:</u> If M is any R-module, $a \in R$, R commutative

Then $a \cdot \mathrm{Id} : M \longrightarrow M$ is an endomorphism.

$$m \longmapsto a \cdot m$$

<u>Check:</u> $\left(a \cdot \mathrm{Id}\right)(m+n) := a \cdot (m+n) = a \cdot m + a \cdot n = (a \cdot \mathrm{Id})(m) + (a \cdot \mathrm{Id})(n)$

$$(a \cdot \mathrm{Id})(r \cdot m) := a(r \cdot m) = (a \cdot r) \cdot m = (r \cdot a) \cdot m$$
$$= r \cdot (a \cdot m) = r \cdot (a \cdot \mathrm{Id})(m)$$

We get a map

$$f : R \longrightarrow \mathrm{End}_R(M)$$
$$r \longmapsto r \cdot \mathrm{Id}.$$

<u>Claim:</u> This map is a ring homomorphism

<u>Pf:</u>

$$f(r+s) := (r+s) \cdot \mathrm{Id} = r \cdot \mathrm{Id} + s \cdot \mathrm{Id} = f(r) + f(s)$$

$$f(r \cdot s) = (r \cdot s) \cdot \mathrm{Id} = (r \cdot \mathrm{Id}) \circ (s \cdot \mathrm{Id}) = f(r) \cdot f(s)$$

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

Warning: This map is not always injective:

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

$$f: \mathbb{Z} \longrightarrow \mathrm{End}(\mathbb{Z}/4\mathbb{Z})$$

$$4 \longmapsto 4\cdot \mathrm{Id}.$$

$$4\cdot \mathrm{Id}(\bar{a}) = 4\cdot\bar{a} = \overline{4a} = \bar{0}$$

$$\Longrightarrow 4 \in \mathrm{Ker}\, f \Longrightarrow f \text{ is not injective.}$$