6 Getting Comfortable With Modules

All modules considered are left modules. Given A-modules M, N, the set of all A-module homomorphisms from $M \to N$ is denoted by $\operatorname{Hom}_A(M, N)$. It is an additive abelian group.

2/17: **6.1.** Let M be an A-module and let $e : M \to M$ be an A-module homomorphism satisfying $e \circ e = e$. We have shown that both $e(M)$ and $\ker(e)$ are submodules of M.

(i) Prove that $\phi : e(M) \oplus \ker(e) \to M$ given by $\phi(v, w) = v + w$ for all $v \in e(M)$, $w \in \ker(e)$ is an isomorphism of A-modules.

(ii) Define $P : e(M) \oplus \ker(e) \to e(M) \oplus \ker(e)$ by $P(v, w) = (v, 0)$ for all $(v, w) \in e(M) \oplus \ker(e)$. Prove that $P = \phi^{-1} \circ e \circ \phi$.

6.2. Let $f : M \to N$ and $g : N \to M$ be A-module homomorphisms such that $g(f(m)) = m$ for all $m \in M$. Prove that $H : M \oplus \ker(g) \to N$ given by $H(m, n) = f(m) + n$ for all $m \in M$, $n \in \ker(g)$ is an isomorphism of A-modules.

Proof. To prove the claim, we will apply Problem 6.1(i). In particular, we will first define a relevant helper function e and show that it satisfies the same properties as the e from Problem 6.1. We will use this e to define an isomorphism $\phi : e(N) \oplus \ker(e) \to N$, in line with Problem 6.1. Lastly, we will show that there is an isomorphism $\psi : M \oplus \ker(g) \to e(N) \oplus \ker(e)$ and define H to be the composition isomorphism $\phi \circ \psi$. Let's begin.

Define $e : N \to N$ by $e = f \circ g$. By Proposition 10.2, e is an A-module homomorphism. Additionally, we can demonstrate that $e \circ e = e$: If we let $n \in N$ be arbitrary, then we have

$$\begin{aligned}
(e \circ e)(n) &= (f \circ g \circ f \circ g)(n) \\
&= f((g \circ f)(g(n))) \\
&= f(g(n)) \\
&= (f \circ g)(n) \\
&= e(n)
\end{aligned}$$

as desired. Therefore, by Problem 6.1(i), there exists an A-module isomorphism $\phi : e(N) \oplus \ker(e) \to N$ defined by $\phi(v, w) = v + w$ for all $v \in e(N)$, $w \in \ker(e)$.

Moving on, we can show that $M \cong e(N)$. In particular, since $g(f(m)) = m$ for all $m \in M$ by hypothesis, we know that f is injective and g is surjective. It follows from the latter statement that $g(N) = M$. Thus, combining results, we have that

$$M \cong f(M) = f(g(N)) = (f \circ g)(N) = e(N)$$

where the isomorphism is given by $\tilde{f} : M \to e(N)$ defined by $\tilde{f}(m) = f(m)$ for all $m \in M$.

Next, we can show that $\ker(e) = \ker(g)$. Suppose first that $n \in \ker(e)$. Then $e(n) = 0$. It follows by the definition of e that $f(g(n)) = 0$. Additionally, we know that $f(0) = 0$ since f is a group homomorphism (as an A-module homomorphism). Thus, by transitivity, $f(g(n)) = f(0)$. It follows since f is injective (as stated above) that $g(n) = 0$. Therefore, $n \in \ker(g)$ by definition, as desired. Now suppose that $n \in \ker(g)$. Then $g(n) = 0$. It follows for analogous reasons to the other direction (e.g., f is a group homomorphism; definition of e) that $e(n) = f(g(n)) = f(0) = 0$. Therefore, $n \in \ker(e)$ by definition, as desired.

At this point, we may define $\psi : M \oplus \ker(g) \to e(N) \oplus \ker(e)$ by $\psi(m, n) = (\tilde{f}(m), \operatorname{id}(n))$ for all $(m, n) \in M \oplus \ker(g)$. As a componentwise A-module isomorphism, ψ is also an A-module isomorphism, itself (see the analogous justification in Problem 3.2). Thus, we may define the A-module isomorphism $H = \phi \circ \psi$, where the fact that H is an A-module homomorphism is justified by Proposition 10.2 and the fact that it is bijective follows from the bijectivity of both ϕ, ψ. H, as defined, maps the correct sets (i.e., $M \oplus \ker(g) \to N$) and has the correct rule:

$$H(m, n) = (\phi \circ \psi)(m, n) = \phi(\psi(m, n)) = \phi(\tilde{f}(m), n) = \phi(f(m), n) = f(m) + n$$

$\square$

6.3. Let $\phi : A \to B$ be a ring homomorphism, and let M be a B-module. Show that $\cdot : A \times M \to M$ defined by

$$(a, m) \mapsto \phi(a)m$$

for all $a \in A$, $m \in M$ gives M the structure of an A-module.

In particular, every B-module M has the structure of an A module for every subring A of B.

A very important application of this observation ($F[X]$-modules) is discussed on Dummit and Foote (2004, p. 340); it will be all-important later on in this course.

6.4. Let K be the fraction field of an integral domain R. Let V and W be K-modules (i.e., vector spaces over the field K). The preceding problem shows that V and W are also R-modules in a natural manner.

Prove that every R-module homomorphism $f : V \to W$ is also a K-module homomorphism (it has to be shown that $f(av) = af(v)$ for all $a \in K$, $v \in V$).

Proof. Let $a \in K$ and $v \in V$ be arbitrary. Suppose $a = b/c$, where $b, c \in R$. Then

$$af(v) = \frac{b}{c}f(v) = \frac{1}{c}f(bv) = \frac{1}{c}f(acv) = \frac{c}{c}f(av) = 1f(av) = f(av)$$

as desired. $\square$

6.5. With K, R, V, W as in the preceding problem, let M be an R-submodule of V. Assume that for every $v \in V$, there is a nonzero $a \in R$ such that $av \in M$. Let $f : M \to W$ be an R-module homomorphism. Prove that f extends in a unique manner to a K-module homomorphism $F : V \to W$.

Proof. Define $F : V \to W$ by

$$F(v) = \frac{1}{a}f(av)$$

for all $v \in V$, where $a \in R$ satisfies $av \in M$.

To prove that F is well-defined, it will suffice to show that for all $a, b \in R$ satisfying $av, bv \in M$, we have that $f(av)/a = f(bv)/b$. Let a, b be arbitrary elements of R satisfying the desired property. Then

$$\frac{1}{a}f(av) = \frac{ab}{a^2b}f(av) = \frac{1}{a^2b}f(a^2bv) = \frac{a^2}{a^2b}f(bv) = \frac{1}{b}f(bv)$$

as desired.

To prove that F is a homomorphism of abelian groups, it will suffice to show that $F(v_1 + v_2) = F(v_1) + F(v_2)$ for all $v_1, v_2 \in V$. Let $v_1, v_2 \in V$ be arbitrary. Suppose

$$F(v_1 + v_2) = \frac{1}{a}f(a(v_1 + v_2)) \qquad F(v_1) = \frac{1}{b}f(bv_1) \qquad F(v_2) = \frac{1}{c}f(cv_2)$$

for some $a, b, c \in R$. Then

$$\begin{aligned} F(v_1) + F(v_2) &= \frac{1}{b}f(bv_1) + \frac{1}{c}f(cv_2) \\ &= \frac{cf(bv_1) + bf(cv_2)}{bc} \\ &= \frac{1}{bc}f(bc(v_1 + v_2)) \\ &= \frac{1}{a}f(a(v_1 + v_2)) \\ &= F(v_1 + v_2) \end{aligned}$$

as desired, where the fourth equality holds by the above argument used to show that F is well-defined.

To prove that F is a K-module homomorphism, it will suffice to additionally show that $F(kv) = kF(v)$ for all $k \in K$ and $v \in V$. Let $k = l/n \in K$ and $v \in V$ be arbitrary. Then

$$kF(v) = \frac{l}{n} \cdot \frac{1}{a} f(av) = \frac{1}{a} f(a(kv)) = F(kv)$$

as desired.

To prove that F is an extension of f, it will suffice to show that for all $m \in M$, $F(m) = f(m)$. Let $m \in M$ be arbitrary. Then

$$F(m) = \frac{1}{a} f(am) = \frac{a}{a} f(m) = f(m)$$

as desired.

To prove that F is unique, it will suffice to show that if $\tilde{F} : V \to W$ is an extension of f to V, then $F = \tilde{F}$. Let $v \in V$ be arbitrary. Then

$$F(v) = \frac{1}{a} f(av) = \frac{1}{a} \tilde{F}(av) = \frac{a}{a} \tilde{F}(v) = \tilde{F}(v)$$

where the second equality holds because $\tilde{F} = f$ on M by definition and $av \in M$. □

6.6. We have shown in class that every A-module homomorphism $T : A^n \to M$ (where M is an A-module) is given by

$$T(a_1, \dots, a_n) = a_1 v_1 + \cdots + a_n v_n$$

for all $(a_1, \dots, a_n) \in A^n$ and some $v_1, \dots, v_n \in M$. This gives a bijection between $\mathrm{Hom}_A(A^n, M)$ and M^n.

Now let $c = (c_1, \dots, c_n) \in A^n$. We have the A-submodule $Ac = \{ac : a \in A\}$ of A^n and the quotient module A^n/Ac. Show that there is a bijection from the set of A-module homomorphisms $S : A^n/Ac \to M$ and a certain additive subgroup G of M^n. Describe G explicitly.

Hint: Given S, consider the composite $A^n \to A^n/Ac \xrightarrow{S} M$.

Proof. Let

$$\boxed{G = \{(v_1, \dots, v_n) \in M^n : c_1 v_1 + \cdots + c_n v_n = 0\}}$$

To confirm that G is an additive subgroup of M^n, Proposition 2.1 tells us that it will suffice to show that $G \neq \emptyset$ and $x, y \in G$ implies $x - y \in G$. Since $c_1 \cdot 0 + \cdots + c_n \cdot 0 = 0$, $(0, \dots, 0) \in G$ and hence $G \neq \emptyset$, as desired. Now suppose $(v_1, \dots, v_n), (w_1, \dots, w_n) \in G$. Then $c_1 v_1 + \cdots + c_n v_n = 0$ and $c_1 w_1 + \cdots + c_n w_n = 0$. It follows that

$$\begin{aligned} 0 &= (c_1 v_1 + \cdots + c_n v_n) - (c_1 w_1 + \cdots + c_n w_n) \\ &= c_1(v_1 - w_1) + \cdots + c_n(v_n - w_n) \end{aligned}$$

and hence $(v_1, \dots, v_n) - (w_1, \dots, w_n) = (v_1 - w_1, \dots, v_n - w_n) \in G$, as desired.

We define $\phi : G \to \mathrm{Hom}_A(A^n/Ac, M)$ by

$$\phi(v_1, \dots, v_n) = \Big[S : (a_1, \dots, a_n) + Ac \mapsto a_1 v_1 + \cdots + a_n v_n \Big]$$

We first show that ϕ is injective. Suppose $\phi(v_1, \dots, v_n) = \phi(w_1, \dots, w_n)$. Then $S_v = S_w$. In particular,

$$v_i = S_v(e_i + Ac) = S_w(e_i + Ac) = w_i$$

for all $1 \leq i \leq n$. Therefore, since each component is equal, we must have $(v_1, \dots, v_n) = (w_1, \dots, w_n)$, as desired.

We now show that ϕ is surjective. Let $S \in \mathrm{Hom}_A(A^n/Ac, M)$ be arbitrary. Consider $\pi : A^n \to A^n/Ac$ and $T = S \circ \pi$. Since $T : A^n \to M$ is an A-module homomorphism, there exist $v_1, \dots, v_n \in M$ such that for all $(a_1, \dots, a_n) \in A^n$, $T(a_1, \dots, a_n) = a_1v_1 + \cdots + a_nv_n$. It follows that

$$\begin{aligned} a_1v_1 + \cdots + a_nv_n &= (S \circ \pi)(a_1, \dots, a_n) \\ &= S[(a_1, \dots, a_n) + Ac] \end{aligned}$$

so $S = \phi(v_1, \dots, v_n)$, as desired.

It follows that $\phi^{-1} : \mathrm{Hom}(A^n/Ac, M) \to G$ is the desired isomorphism. $\square$

6.7. Let $c = (c_1, \dots, c_n) \in A^n$. Assume that the *right* ideal $c_1A + \cdots + c_nA$ equals A itself.

(i) Prove that there is a left A-module homomorphism $g : A^n \to A$ such that $g(c) = 1$.

Proof. Since $A = c_1A + \cdots + c_nA$ by hypothesis, there exist $v_1, \dots, v_n \in A$ such that $1 = c_1v_1 + \cdots + c_nv_n$. Define $g : A^n \to A$ by

$$g(a_1, \dots, a_n) = a_1v_1 + \cdots + a_nv_n$$

Since A is an A-module and g is of the form specified in class (and in the statement of Problem 6.6), we know that g is a left A-module homomorphism. Moreover, we have that

$$g(c) = g(c_1, \dots, c_n) = c_1v_1 + \cdots + c_nv_n = 1$$

as desired. $\square$

(ii) Deduce that there is an isomorphism $A \oplus \ker(g) \to A^n$ of left A-modules. *Hint*: Problem 6.2.

Proof. Taking the hint, we build up to the point where we can apply Problem 6.2.

Define $f : A \to A^n$ by $f(a) = ac$. Per Lecture 6.1, this instance of left multiplication (like all others) constitutes an A-module homomorphism. Additionally, define $g : A^n \to A$ as in part (i). It follows from part (i) that g is an A-module homomorphism as well. Furthermore, we have for all $a \in A$ that

$$(g \circ f)(a) = g(f(a)) = g(ac) = ag(c) = a \cdot 1 = a$$

Therefore, by Problem 6.2, $A \oplus \ker(g) \cong A^n$, as desired. $\square$

6.8. Assume that A is a commutative ring. Prove that if M is an A-module such that $M \oplus A \cong A^2$, then there is an A-module isomorphism $A \to M$.

Proof.

- Let $\phi : M \oplus A \to A^2$ denote the given isomorphism.
- By definition ($\phi^{-1} = \phi^{-1}$ and $i^{-1} = \pi_2$), the diagram

$$A \xhookrightarrow{i} M \oplus A \xrightarrow{\phi} A^2 \xrightarrow{\phi^{-1}} M \oplus A \xrightarrow{\pi_2} A$$

  commutes. *draw nicely.*
  - Lecture 6.1: i, π_2 are A-module homomorphisms, too.
- To define $\psi : A \to M$, it will suffice to define $\psi(1)$.
- $i(1) = (0, 1)$.
- Let $(a, b) := \phi(0, 1)$.
- Let $(m_1, c) := \phi^{-1}(0, 1)$.
- Let $(m_2, d) := \phi^{-1}(1, 0)$.
- Relating the values a, b, c, d.
  - Since the above diagram commutes, we have that

$$\begin{aligned}
1 &= (\pi_2 \circ \phi^{-1} \circ \phi \circ i)(1) \\
&= \pi_2(\phi^{-1}(\phi(i(1)))) \\
&= \pi_2(\phi^{-1}(\phi(0, 1))) \\
&= \pi_2(\phi^{-1}(a, b)) \\
&= \pi_2(\phi^{-1}[a(1, 0) + b(0, 1)]) \\
&= a\pi_2(\phi^{-1}(1, 0)) + b\pi_2(\phi^{-1}(0, 1)) \\
&= a\pi_2(m_2, d) + b\pi_2(m_1, c) \\
&= ad + bc
\end{aligned}$$

- Prove that $T : A \to A^2$ defined by $a \mapsto a(-d, c)$ is an injective A-module homomorphism.
  - A-module homomorphism: It's just right multiplication.
  - Injectivity: Apply the cancellation lemma for nonzero $(-d, c)$.
  - Surjectivity:
    - ■ We start with

$$\{(u, v) \in A^2 : \phi^{-1}(u, v) \in M \oplus 0\} = \{(u, v) \in A^2 : uc + vd = 0\}$$

    - ■ We have

$$ub = -kdb = k(ac - 1) = kac - k = av - k$$

      so $k = av - ub$. Indeed,

$$kc = avc - ubc = v(1 - bd) - ubc = v - bd - bcu = v - bd + vd$$

    - ■ We want to find (u, v) such that $(u, v) = k(-d, c)$. $\phi(m, 0)$.
    - ■ Swap $(-d, c)$ for $(-c, d)$??
- Use the "injectivity" and "surjectivity" of ϕ^{-1}, π_2 to complete the proof.

□

6.9. Let R be a commutative ring. Assume that there are $x, y, z \in R$ such that $x^2 + y^2 + z^2 = 1$. Define $f : R^3 \to R$ by $f(a, b, c) = ax + by + cz$. Let $M = \ker(f)$.

Prove that there is an R-module isomorphism $M \oplus R \to R^3$.

Note: However, M need not be isomorphic to R^2. For example, if $R = \mathbb{R}[X, Y, Z]/(X^2+Y^2+Z^2-1)$ and x, y, z are $\bar{X}, \bar{Y}, \bar{Z}$, respectively, here M is not isomorphic to R^2. This is saying that the tangent bundle of the two-sphere is nontrivial. It is proved using Algebraic Topology, but purely algebraic proofs exist.

Proof. Since $M = \ker(f)$ and $\oplus$ is commutative, $M \oplus R \cong R \oplus \ker(f)$. Thus, we need only prove that there is an isomorphism $R \oplus \ker(f) \to R^3$. To do so, Problem 6.7 tells us that it will suffice to show that $c = (x, y, z) \in R^3$, $xR + yR + zR = R$, and $f : R^3 \to R$ satisfies $f(c) = 1$. Let's begin.

For the first claim, we have by definition that $c \in R^3$.

For the second claim, we have by definition that $xR + yR + zR \subset R$. Now let $r \in R$ be arbitrary. Then

$$r = r \cdot 1 = r \cdot (x^2 + y^2 + z^2) = x \cdot (rx) + y \cdot (ry) + z \cdot (rz) \in xR + yR + zR$$

as desired.

For the third claim, we have that

$$f(c) = f(x, y, z) = xx + yy + zz = x^2 + y^2 + z^2 = 1$$

as desired. □

6.10. Prove that every (left) A-module homomorphism from A to itself is right multiplication by a, denoted by $r_a : A \to A$, for a unique $a \in A$.

6.11. Let R be a commutative ring. Show that if $T : M \to N$ is a homomorphism of R-modules and if $a \in R$, then $S : M \to N$ given by $S(m) = aT(m)$ for all $m \in M$ is also an R-module homomorphism. Deduce that $\mathrm{Hom}_R(M, N)$ has the structure of an R-module.

Proof. For all $m \in M$,

$$S(m) = aT(m) = T(am) = T(ma) = T(r_a(m)) = (T \circ r_a)(m)$$

Note that the second equality holds because T is an R-module homomorphism and the third equality holds because R is commutative (and hence the left and right R-module structures are equivalent). It follows from the above $S = T \circ r_a$. Additionally, by Problem 6.10, $r_a \in \mathrm{Hom}_R(R, R)$. It follows by Proposition 10.2 that S is an R-module homomorphism.

By a similar argument to that used in Problem 1.14, $(\mathrm{Hom}_R(M, N), +)$ is an abelian group, where addition is taken pointwise. By the above $\cdot : A \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$ defined by $(a, T) \mapsto a \cdot T$ is closed. Additionally, if $a, b \in R$ and $S, T \in \mathrm{Hom}_R(M, N)$, we can use the fact that M, N are R-modules to confirm that

$$\begin{gathered} a(S + T)(m) = a[S(m) + T(m)] = aS(m) + aT(m) = (aS + aT)(m) \\ a(S + T) = aS + aT \end{gathered} \tag{1}$$

$$\begin{gathered} (a + b)T(m) = aT(m) + bT(m) \\ (a + b)T = aT + bT \end{gathered} \tag{2}$$

$$\begin{gathered} a(bT(m)) = (ab)T(m) \\ a(bT) = (ab)T \end{gathered} \tag{3}$$

$$\begin{gathered} 1_R T(m) = T(m) \\ 1_R T = T \end{gathered} \tag{4}$$

Therefore, $\mathrm{Hom}_R(M, N)$ is an R-module, as desired. □

6.12. Give an example of a PID A and an A-submodule M' of an A-module M such that M and $M' \oplus (M/M')$ are not isomorphic to each other (as A-modules).

Note: If A is a field, then there is an isomorphism $M \to M' \oplus (M/M')$. In class, it was shown that there is such an isomorphism if M/M' is isomorphic to A^n for some $n = 0, 1, 2, \dots$.

Proof. Pick

$$\boxed{A = \mathbb{Z} \qquad\qquad M = \mathbb{Z}/4\mathbb{Z} \qquad\qquad M' = (2) \subset M}$$

By Section 8.2 of Dummit and Foote (2004), we know that $A = \mathbb{Z}$ is a PID. Additionally, we know from last quarter that M is an abelian group and M' is a subgroup of M. It follows by Dummit and Foote (2004, p. 339) that these are valid examples of a $\mathbb{Z}$-module and a $\mathbb{Z}$-submodule. Moreover, we know from group theory that $(\mathbb{Z}/4\mathbb{Z})/(2)$ is isomorphic (as a group [or A-module]) to $\mathbb{Z}/2\mathbb{Z}$ and, similarly, $(2) \cong \mathbb{Z}/2\mathbb{Z}$ as a group (or A-module). Therefore,

$$M \oplus (M/M') \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = K \ncong \mathbb{Z}/4\mathbb{Z} = M$$

as desired, where K denotes the Klein 4-group. $\square$

6.13. Let $f, g \in F[X]$ be polynomials of degrees d and e, respectively, where F is a field. Assume that $\gcd(f, g) = 1$. Prove that there is a unique pair $a, b \in F[X]$ such that

$$af + bg = 1 \qquad\qquad \deg(a) < e \qquad\qquad \deg(b) < d$$

Hint: One already knows that there exist a, b satisfying $af + bg = 1$, but the a, b satisfying this equation are far from being unique. Given a, b, first find *all* a', b' satisfying $a'f + b'g = 1$. After this, you will see that the problem is easily solved.

Note: There is also a different constructive method of finding the desired a, b that relies on determinants and resultants.

Proof. By hypothesis, there exist polynomials $a_0, b_0 \in F[X]$ such that $a_0 f + b_0 g = 1$. We can easily show that the set of all (a, b) satisfying $af + bg = 1$ is

$$\{(a_0 + gh, b_0 - fh) : h \in F[X]\}$$

In particular, for any element of this set, we have

$$(a_0 + gh)f + (b_0 - fh)g = (a_0 f + b_0 g) + (gfh - fgh) = 1 + 0 = 1$$

and for any (a, b) satisfying the equation, we have

$$\begin{aligned}
(af + bg) - (a_0 f + b_0 g) &= 1 - 1 \\
(a - a_0)f + (b - b_0)g &= 0 \\
a &= a_0 + \frac{b - b_0}{f} g
\end{aligned}$$

so that $a \in a_0 + (g)$, as desired.

Elaborating on the observation that any a is an element of $a_0 + (g)$: Since $F[X]/(g) \cong \{h \in F[X] : \deg(h) < e\}$ by the corollary from Lecture 3.1, there exists a unique a with $\deg(a) < e$ such that $a \mapsto a_0 + (g)$. It follows by the construction of the isomorphism that $a \in a_0 + (g)$, and hence $a + (g) = a_0 + (g)$. A similar argument holds for b. This yields the desired result. $\square$