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 $\mathrm{Hom}_A(M, N)$. 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.

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 $a \in K$, $v \in V$).

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 $F : V \to W$.

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

$$T(a_1, \ldots, a_n) = a_1v_1 + \cdots + a_nv_n$$

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

Now let $c = (c_1, \ldots, c_n) \in A^n$. 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 $A^n \to A^n/Ac \xrightarrow{S} M$.

6.7. Let $c = (c_1, \ldots, c_n) \in A^n$. 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 $g(c) = 1$.

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

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 $A \to M$.

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.

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.

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 $n = 0, 1, 2, \ldots$.

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

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

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.