Reading: Dummit–Foote Ch 10.2–10.3.

Recall: We assume that all rings have a multiplicative identity 1, that a subring of R must contain 1_R, and that a ring homomorphism $R \to S$ must map 1_R to 1_S.

Summary of definitions and main results

Definitions we've covered: Homomorphism of R–modules, isomorphism of R–modules, kernel, image, $\mathrm{Hom}_R(M,N)$, $\mathrm{End}_R(M)$, quotient of R–modules, sum of R–submodules.

Main results: R–linearity criterion for maps, kernels and images are R–submodules, for R commutative $\mathrm{Hom}_R(M,N)$ is an R–module, $\mathrm{End}_R(M)$ is a ring, factor theorem, four isomorphism theorems.

Warm-Up Questions

The "warm-up" questions do not need to be submitted (and won't be graded), however, you should understand how to solve them!

1. Find an example of an R-module M that is isomorphic as R–modules to one of its proper submodules.
2. We saw that a R–module structure on M can also be defined by a homomorphism of rings $R \to \mathrm{End}_{\mathbb{Z}}(M)$. From this perspective, give an equivalent definition of the R–linear endomorphisms $\mathrm{End}_R(M) \subseteq \mathrm{End}_{\mathbb{Z}}(M)$.
3. (a) Prove the R–linearity criterion: $\phi : M \to N$ is an R–module map if and only if
$$\phi(rm+n) = r\phi(m) + \phi(n) \qquad \text{for all } m, n \in M \text{ and } r \in R.$$
   (b) Prove that the composition of R–module homomorphisms is again an R–module homomorphism.
   (c) Let $\phi : M \to N$ be an R–module homomorphism. Show that $\ker(\phi)$ is an R–submodule of M, and that $\mathrm{im}(\phi)$ is an R–submodule of N.
   (d) Show that if a map of R–modules $\phi : M \to N$ is invertible as a map of sets, then its inverse ϕ^{-1} is also R–linear, and an isomorphism of R–modules $N \to M$.
   (e) Show that a homomorphism of R–modules ϕ is injective if and only if $\ker(\phi) = \{0\}$.
4. (a) Let M and N be R–modules. Show that every R–module map $M \to N$ is also a group homomorphism of the underlying abelian groups M and N.
   (b) Show that if R is a field, then R–module maps are precisely linear transformations of vector spaces.
   (c) Show that if $R = \mathbb{Z}$, then R–module maps are precisely group homomorphisms.
   (d) Show by example that a homomorphism of the underlying abelian groups M and N need not be a homomorphism of R–modules.
   (e) Now let $M = N$. Show that the set $\mathrm{End}(M) = \mathrm{End}_{\mathbb{Z}}(M)$ (the group endormophisms of the underlying abelian group M) and the set $\mathrm{End}_R(M)$ (the R–linear endomorphisms of the R–module M) may not be equal.
5. Let R be a ring. Its *opposite ring* R^{op} is a ring with the same elements and addition rule, but multiplication is performed in the opposite order. Specifically, the opposite ring of $(R,+,\cdot)$ is a ring $(R^{\mathrm{op}},+,*)$ where $a * b := b \cdot a$.
   (a) Show that if R is commutative, $R = R^{\mathrm{op}}$.
   (b) Show that a left R–module structure on an abelian group M is equivalent to a right R^{op}–module structure on M.
6. Consider R as a module over itself.

(a) Show by example that not every map of R–modules $R \to R$ is a ring homomorphism.

(b) Show by example that not every ring homomorphism is an R–module homomorphism.

(c) Suppose that ϕ is both a ring map and a map of R–modules. What must ϕ be?

7. (a) For R–modules M and N, prove that $\mathrm{Hom}_R(M, N)$ is an abelian group, and $\mathrm{End}_R(M)$ is a ring.

   (b) For a commutative ring R, what is the ring $\mathrm{End}_R(R)$?

   (c) When R is commutative, show that $\mathrm{Hom}_R(M, N)$ is an R–module. What if R is not commutative?

   (d) Let M be a right R–module. Prove that $\mathrm{Hom}_{\mathbb{Z}}(M, R)$ is a left R–module. What if M is a left R–module?

8. (a) Let M be an R–module. For which ring elements $r \in R$ will the map $m \mapsto rm$ define an R–module homomorphism on M?

   (b) Show that if R is commutative then there is a natural map of rings $R \to \mathrm{End}_R(M)$.

   (c) Show by example that the map $R \to \mathrm{End}_R(M)$ may or may not be injective.

9. Let A and B be R–submodules of an R–module M.

   (a) Prove that the sum $A + B$ is an R–submodule of M.

   (b) Prove that $A + B$ is the smallest submodule of M containing A and B in the following sense: if any submodule N of M contains both A and B, then N contains $A + B$.

10. State and prove the four isomorphism theorems for modules (Section 10.2 Theorem 4.)

11. Use the first isomorphism theorem to prove that if $x \in R$ then the cyclic module Rx is isomorphic to the R–module $R/\mathrm{ann}(x)$. Deduce that if R is an integral domain, then $Rx \cong R$ as R–modules.

12. Show that the rank-nullity theorem for linear transformations of vector spaces is a consequence of the first isomorphism theorem for modules.

13. Let R be a ring. A left ideal I in R is *maximal* if the only left ideals in R containing I are I and R. Use the fourth isomorphism theorem to show that R/I is *simple* (it has no proper nontrivial submodules).

14. **(Group theory review)** Compute the following $\mathbb{Z}$–modules in the sense of the structure theorem for finitely generated abelian groups.

    (a) Compute $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/15\mathbb{Z})$ as a $\mathbb{Z}$–module.

    (b) For integers m, n, compute $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ as a $\mathbb{Z}$–module.

15. **(Group theory review)** Consider the abelian group $\mathbb{Q}/\mathbb{Z}$.

    (a) Show that every element of $\mathbb{Q}/\mathbb{Z}$ is torsion.

    (b) Show that $\mathbb{Q}/\mathbb{Z}$ is *divisible*: for every $a \in \mathbb{Q}/\mathbb{Z}$ and $n \in \mathbb{Z}$, there is an element $b \in \mathbb{Q}/\mathbb{Z}$ with $nb = a$ (so 'division by integers' $\frac{a}{n} = b$ is well-defined in $\mathbb{Q}/\mathbb{Z}$).

    (c) Show that $\mathbb{Q}/\mathbb{Z}$ is not finitely generated.

16. **(Ring theory review)** Classify all ideals of the ring $\mathbb{Z}$.

17. **(Linear algebra review)** Let V, W be vector spaces over a field $\mathbb{F}$ of dimension n and m, respectively. Show that $T : V \to W$ is a linear transformation if and only if it can be represented by an $m \times n$ matrix. Show that matrix multiplication corresponds to composition of functions.

18. **(Linear algebra review)** Let V, W be vector spaces over a field $\mathbb{F}$ and suppose that V has basis $B = \{b_1, b_2, \ldots, b_n\}$. Show that any maps of sets $\varphi : B \to W$ can be extended to a linear map $T : V \to W$, and that the map T is uniquely determined by the map φ.

Assignment Questions

The following questions should be handed in.

1. Let R be a commutative ring and N an R–module.
   (a) Prove that there is an isomorphism of left R–modules $N \cong \mathrm{Hom}_R(R, N)$.
   (b) Let n be a positive integer. Compute $\mathrm{Hom}_R(R^n, N)$.
   (c) Do these same arguments work for $\mathrm{Hom}_R(N, R)$?

2. If R is a commutative ring, then for any positive integer n, $\mathrm{End}_R(R^n)$ is isomorphic (as a ring) to the ring $M_{n\times n}(R)$ of $n \times n$ matrices with entries in R. Find and prove the appropriate generalized statement if R is any (not necessarily commutative) ring. (Your proof should specialize to proving an isomorphism of rings $\mathrm{End}_R(R^n) \cong M_{n\times n}(R)$ in the case that R is commutative.) *Hint:* Warm-Up Problem #5

3. Suppose that M, N are modules over a ring R, and that $S \subset R$ is a subring. Recall that M and N inherit S–module structures.
   (a) Show that $\mathrm{Hom}_R(M, N) \subseteq \mathrm{Hom}_S(M, N)$.
   (b) Find an example of a ring R, a proper subring $S \subset R$, and nonzero R–modules M and N so that $\mathrm{Hom}_R(M, N) = \mathrm{Hom}_S(M, N)$.
   (c) Find an example of a rings $S \subseteq R$, and R–modules M and N so that $\mathrm{Hom}_R(M, N) \neq \mathrm{Hom}_S(M, N)$. (Choose an example different from our example of Gaussian integers $\mathbb{Z} \subseteq \mathbb{Z}[i]$ in class.)

4. For R–modules M, N, P, there is a composition map $\mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(N, P) \longrightarrow \mathrm{Hom}_R(M, P)$ given by $(f, g) \longmapsto g \circ f$.
   (a) When R is commutative, is this map a homomorphism of R–modules?
   (b) Give an example of a ring R and distinct R–modules M, N, P such that this map is surjective, and an example where this map is not surjective.

5. Let $R[x, y]$ denote polynomials in (commuting) indeterminates x and y over a commutative ring R. Use the isomorphism theorems to prove the following isomorphisms of R–modules.
   (a) $R[x, y]/(x) \cong R[y]$.
   (b) Let $p(x, y)$ be a polynomial in x and y. Then $R[x, y]/\Big(x, p(x, y)\Big) \cong R[y]/\Big(p(0, y)\Big)$.
   (c) Let $q(x)$ be a polynomial in x. Then $R[x, y]/\Big(y - q(x)\Big) \cong R[x]$.

6. Let U, V, W be vector spaces over a field $\mathbb{F}$. Let $\phi : U \to V$ be an injective linear map, and let $\psi : V \to W$ be a surjective linear map. Prove that both ϕ and ψ have one-sided inverses. Show by example that when R is not a field, not all surjective maps of R–modules have (one-sided) inverses, and show that not all injective maps of R–modules have (one-sided) inverses. (Later in the course, we will describe this phenomenon by the phrase "Every short exact sequence of vector spaces splits")