Reading: Dummit–Foote Ch 10.2, 11.3.

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).

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. Let M be an R–module, and suppose that $I \subset R$ is a two-sided ideal that annihilates M. Prove that the action of R on M factors through an action of R/I on M by $(r \bmod I)m := rm$ for $r \in R$ and $m \in M$. This means checking
   (i) the action is well-defined: if r and s represent the same coset modulo I, then $rm = sm$ for all $m \in M$,
   (ii) the action satisfies the axioms of an R–module structure.
4. (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 $\ker(\phi) = \{0\}$.
5. (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 $\mathrm{End}_{\mathbb{Z}}(M)$ and the set $\mathrm{End}_R(M)$ may not be equal.
6. 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.

7. Let $\phi : M \to N$ be a map of R–modules. Show that $\phi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$.
8. 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?
9. (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?
10. (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.
11. State and sketch proofs of the four isomorphism theorems for modules (Section 10.2 Theorem 4.)
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 $\mathbb{Q}[x, y]$ denote polynomials in (commuting) indeterminates x and y over $\mathbb{Q}$. Use the isomorphism theorems to prove the following isomorphisms of $\mathbb{Q}[y]$–modules.
    (a) $\mathbb{Q}[x, y]/(x) \cong \mathbb{Q}[y]$.
    (b) Let $p(x, y)$ be a polynomial in x and y. Then $\mathbb{Q}[x, y]/\Big(x, p(x, y)\Big) \cong \mathbb{Q}[y]/\Big(p(0, y)\Big)$.
    (c) Let $q(y)$ be a polynomial in y. Then $\mathbb{Q}[x, y]/\Big(x - q(y)\Big) \cong \mathbb{Q}[y]$.
14. 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).
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 $nb = a$.
    (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.
    (a) Show that $T : V \to W$ is a linear transformation if and only if it can be represented by an $m \times n$ matrix with respect to a choice of basis. Show that matrix multiplication corresponds to composition of functions.
    (b) Explain the principle of *change of basis*. Show that re-expressing a linear map as a matrix in a different basis corresponds to conjugation of matrices. Show that *similar* matrices represent the same linear map in different bases.
18. **(Linear algebra review)**
    (a) 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.
    (b) 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.

Assignment Questions

The following questions should be handed in.

1. **(Group theory review)** Suppose $m, n \geq 2$ are integers.
   (a) Prove that there is an injective map of abelian groups $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ if and only if $m|n$.
   (b) Prove that if this map exists, it is unique up to pre-composing with an automorphism of $\mathbb{Z}/m\mathbb{Z}$. This means if $g, g' : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ are injective maps, then $g' = g \circ f$ for some $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Conclude in particular that the image of an injective map is a uniquely determined subset of $\mathbb{Z}/n\mathbb{Z}$.
   (c) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is an abelian group under pointwise addition of maps. Compute this group (as a product of cyclic groups, in terms of the classification of finitely generated abelian groups).

2. 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) In a sentence, explain whether these same arguments work for $\mathrm{Hom}_R(N, R)$.

3. 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 #6.

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 k be a field, and let V be a finite dimensional k-vector space. Define the *dual space of* V by

$$V^* := \mathrm{Hom}_k(V, k).$$

   Recall that V^* has the structure of a k-vector space under pointwise addition and scalar multiplication. Use the notation A^T or v^T to denote the *transpose* of a matrix A or column vector v. You may use the identity $(AB)^T = B^T A^T$ without proof.
   (a) Given a choice of basis $B = \{b_1, \ldots, b_n\}$ for V, define a symmetric bilinear form

$$(-,-) : V \times V \longrightarrow k$$

   on V by the condition

$$(b_i, b_j) = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

   Let $v, u \in V$. Show that this definition completely determines the value of (v, u), and moreover that (v, u) is equal to the *dot product* $v^T u$ of v and u when they are expressed as column vectors with respect to the basis B.
   (b) For each $i = 1, \ldots, n$, define the map $b^i : V \to k$ by

$$b^i(v) := (b_i, v).$$

   Check that b^i is a *functional*, ie, a k–linear map $V \to k$, and show moreover that the map $b_i \mapsto b^i$ extends to a k-linear map

$$\begin{aligned} V &\longrightarrow V^* \\ w &\longmapsto \big[v \mapsto (w, v)\big] \end{aligned}$$

(c) Show that the functionals $b^1, \ldots, b^n$ are linearly independent and span V^*, and therefore form a basis B^* (called the *dual basis* to B). Conclude that a choice of basis for V defines an isomorphism of vector spaces $V \cong V^*$.

(d) Show that if $A : V \to W$ is a linear map given by a matrix with respect to orthonormal bases B_V and B_W. Show that

$$(w, Av)_W = (A^T w, v)_V.$$

Hint: Use the formula $(u, u') = u^T u'$. This should be a one-line solution.

(e) A linear map $\phi : V \to W$ induces a map $\phi^* : W^* \to V^*$ by precomposition:

$$W^* \longrightarrow V^*$$
$$[f : W \to k] \longmapsto [f \circ \phi : V \to k]$$

Show that if a linear map $V \to W$ given by a matrix A with respect to bases B_V and B_W, then the induced map $W^* \to V^*$ is given by the matrix A^T with respect to the dual bases B_V^* and B_W^*.

(f) Although V and V^* are isomorphic as abstract vector spaces, they are not *naturally isomorphic* in the sense that any isomorphism involves a choice of basis or choice of nondegenerate symmetric bilinear form on V. Show, in contrast, that V and $(V^*)^*$ are naturally isomorphic, by constructing an isomorphism that does not require a choice of basis or a choice of form.

6. **Bonus (Optional).**

(a) Let V be a vector space over a field k, and let $U \subseteq V$ be a subspace. Show that there exists a subspace $W \subseteq V$ so that $V = U \oplus W$. The subspace W is called a *direct complement* of U in V.

(b) Show that, if U is strictly smaller dimension than V, then its direct complement is not uniquely defined. In other words, $U \oplus W = U \oplus W'$ does not imply that $W = W'$ as subspaces of V.

(c) Show direct complements need not always exist in free abelian groups[1]: Let $M = \mathbb{Z}^n$ for some n and let $N \subset M$ be a $\mathbb{Z}$–submodule. Show by example that there may not exist a $\mathbb{Z}$–submodule P such that $M = N \oplus P$. If (at least one) direct complement P of N exists, let's call N a *splittable* submodule of M.

(d) Let V be a vector space, and let $U, W \subset V$ be subspaces such that $U \cap W = 0$. Show that we can find a direct complement of U in V that contains W.

(e) Determine whether or not the same property holds for splittable submodules of free abelian groups. In other words, suppose that N, P are splittable $\mathbb{Z}$–submodules of $M = \mathbb{Z}^n$ and that $N \cap P = 0$. Either prove that N must have a direct complement in $\mathbb{Z}^n$ containing P, or give a counterexample.

[1] The direct sum of two abelian groups $N \oplus P$ turns out to be the same as the direct product $N \times P$, and is analogous to the direct sum of vector spaces. You can review the notes from Fall 2017 Math 120, `http://web.stanford.edu/~mkemeny/120lectures/L6.pdf`.