# Homework1

Andrew Tindall
Algebra II

September 16, 2019

## 1 Problems

**Problem 1.** Let $R$ be a commutative ring, and let $V$ and $W$ be $R$-modules. Consider the abelian group $\mathrm{Hom}_R(V, W)$.
(a) Show that the $R$-action on $V$ endows $\mathrm{Hom}_R(V, W)$ with the structure of an $R$-module.
(b) Show that the $R$-action on $W$ endows $\mathrm{Hom}_R(V, W)$ with the structure of an $R$-module.
(c) Show that these two $R$-module structures are identical.

*Proof.* $(a)$ and $(b)$ are very similar. First, let $\rho(r, v)$ be the left action of $R$ on $V$, and denote this by $r \cdot b$, and let the action $\sigma(r, w)$ on $W$ also (by abuse of notation) be denoted by $r \cdot w$.

We first form the action $\theta(r, f) = r \diamond f$ of $R$ on $\mathrm{Hom}_R(V, W)$. Let $f$ be a member of the hom set, and define $r \diamond f$ as the function taking $v \in V$ to the value $f(r \cdot v)$. We first verify that this is a legitimate homomorphism:

- $(r \diamond f)(v + u) = (r \diamond f)(v) + (r \diamond f)(u)$:

$$\begin{aligned}(r \diamond f)(v + u) &= f(r \cdot (v + u)) \\ &= f(r \cdot v + r \cdot u) \\ &= f(r \cdot v) + f(r \cdot u) \\ &= (r \diamond f)(v) + (r \diamond f)(u)\end{aligned}$$

- $(r \diamond f)(s \cdot v) = s \cdot (r \diamond f)(v)$:

$$\begin{aligned}(r \diamond f)(s \cdot v) &= f(r \cdot (s \cdot v)) \\ &= f((rs) \cdot v) \\ &= f((sr) \cdot v) \\ &= f(s \cdot (r \cdot v)) \\ &= s \cdot (f(r \cdot v)) \\ &= s \cdot (r \diamond f)(v)\end{aligned}$$

Thus $\diamond$ is a legitimate function from $R \times \mathrm{Hom}(V, W)$ to $\mathrm{Hom}(V, W)$. Now we verify that $\diamond$ satisfies the axioms of a left $R$-action. Let $v$ be an arbitrary element of $V$. Here and in the rest of the solutions, we are implicitly using extensionality to show that two functions are equal; if they take an arbitrary element $v$ to equal elements, then they are equal as functions.

- $r \diamond (f+g) = r \diamond f + r \diamond g$ :

$$\begin{aligned}(r \diamond (f+g))(v) &= (f+g)(r \cdot v) \\ &= f(r \cdot v) + g(r \cdot v) \\ &= (r \diamond f)(v) + (r \diamond g)(v) \\ &= (r \diamond f + r \diamond g)(v)\end{aligned}$$

- $(r+s) \diamond f = r \diamond f + s \diamond f$

$$\begin{aligned}((r+s) \diamond f)(v) &= f((r+s) \cdot v) \\ &= f(r \cdot v + s \cdot v) \\ &= f(r \cdot v) + f(s \cdot v) \\ &= (r \diamond f)(v) + (s \diamond f)(v) \\ &= (r \diamond f + s \diamond f)(v)\end{aligned}$$

- $(rs) \diamond f = r \diamond (s \diamond f)$

$$\begin{aligned}((rs) \diamond f)(v) &= f((rs) \cdot v) \\ &= f((sr) \cdot v) \\ &= f(s \cdot (r \cdot v)) \\ &= (s \diamond f)(r \cdot v) \\ &= (r \diamond (s \diamond f))(v)\end{aligned}$$

- $1 \diamond f = f$:

$$\begin{aligned}(1 \diamond f)(v) &= f(1 \cdot v) \\ &= f(v)\end{aligned}$$

Thus $\mathrm{Hom}_R(V, W)$ is a left $R$-module.

Now, let the left action $\phi(r, g) = r \star g$ be defined as $(r \star g)(v) = r \cdot (g(v))$. We verify the same axioms for this function to be a homomorphism:

- $(r \star f)(v+u) = (r \star f)(v) + (r \star f)(u)$:

$$\begin{aligned}(r \star f)(v+u) &= r \cdot (f(v+u)) \\ &= r \cdot (f(v) + (f(u))) \\ &= r \cdot f(v) + r \cdot f(u) \\ &= (r \star f)(v) + (r \star f)(u)\end{aligned}$$

- $(r \star f)(s \cdot v) = s \cdot (r \star f)(v)$:

$$\begin{aligned}(r \star f)(s \cdot v) &= f(r \cdot (s \cdot v)) \\ &= f((rs) \cdot v) \\ &= f((sr) \cdot v) \\ &= f(s \cdot (r \cdot v)) \\ &= s \cdot f(r \cdot v) \\ &= s \cdot (r \cdot f(v))\end{aligned}$$

We also verify the $R$-action axioms. Let $v$ be an arbitrary element of $V$:

- $r \star (f + g) = r \star f + r \star g$:

$$\begin{aligned}(r \star (f+g))(v) &= r \cdot ((f+g)(v)) \\ &= r \cdot (f(v) + g(v)) \\ &= r \cdot f(v) + r \cdot g(v) \\ &= (r \star f)(v) + (r \star g)(v) \\ &= (r \star f + r \star g)(v)\end{aligned}$$

- $(r + s) \star f = r \star f + s \star f$:

$$\begin{aligned}((r+s) \star f)(v) &= (r+s) \cdot (f(v)) \\ &= r \cdot f(v) + s \cdot f(v) \\ &= (r \star f)(v) + (s \star f)(v) \\ &= (r \star f + s \star f)(v)\end{aligned}$$

- $(rs) \star f = r \star (s \star f)$:

$$\begin{aligned}((rs) \star f)(v) &= (rs) \cdot (f(v)) \\ &= r \cdot (s \cdot (f(v))) \\ &= r \cdot ((s \star f)(v)) \\ &= (r \star (s \star f))(v)\end{aligned}$$

- $1 \star f = f$:

$$\begin{aligned}(1 \star f)(v) &= 1 \cdot (f(v)) \\ &= f(v)\end{aligned}$$

Thus this action makes $\mathrm{Hom}_R(V, W)$ into a left $R$-module.

Now we show that $r \star f = f \diamond r$.

$$\begin{aligned}(r \star f)(v) &= r \cdot (f(v)) \\ &= f(r \cdot v) \\ &= (r \diamond f)(v)\end{aligned}$$

So, for a commutative ring $R$, there is a natural $R$-module structure on the hom-sets $\mathrm{Hom}(V, W)$ of the category $R$-mod, where the $R$-module structure may come from either $V$ or $W$. This gives us an internal exponential object $W^V$ in $R$-mod. In fact, $R$-mod is Cartesian closed, since we also have a terminal object (the 0 object) and all finite products. □

**Problem 2.** Let $R$ be a commutative ring, and let $V$ be an $R$-module. Prove that $\mathrm{End}_R(V)$ is an $R$-algebra, where the multiplication operation is composition.

*Proof.* We show first that $\mathrm{End}_R(V)$ is a ring. It is immediate that it is an abelian group, as it is the hom-object $\mathrm{Hom}_R(V, V)$ in an abelian category. Taking composition as the multiplication operation, associativity and identity are also immediate, as they are implied by the fact that $R$-mod is a category. So we need only check the two distributivity properties. Let $f$, $g$, and $h$ be arbitrary endomoprhisms of $V$, and let $v$ be an arbitrary element of $v$.

- $f \circ (g + h) = f \circ g + f \circ h$:

$$\begin{aligned}(f \circ (g + h))(v) &= f((g + h)(v)) \\ &= f(g(v) + h(v)) \\ &= (f \circ g)(v) + (f \circ h)(v) \\ &= (f \circ g + f \circ h)(v)\end{aligned}$$

- $(f + g) \circ h = f \circ h + g \circ h$:

$$\begin{aligned}((f + g) \circ h)(v) &= (f + g)(h(v)) \\ &= f(h(v)) + g(h(v)) \\ &= (f \circ h)(v) + (g \circ h)(v)\end{aligned}$$

So $\mathrm{End}_R(V)$ is a valid ring. For it to be an $R$-algebra, we also need to exhibit a ring homomorphism $R \to \mathrm{End}_R(V)$, and show that this homomorphism maps $R$ into the center of $\mathrm{End}_R(V)$.

Let the function $\phi$ map $r \in R$ to the function $\phi(r)$ taking $v \in V$ to $r \cdot V$. We need to show that this function $\phi(r)$ is a homomorphism, so that the image of $\phi$ is in $\mathrm{End}_R(V)$:

- $\phi(r)(v + u) = \phi(r)(v) + \phi(r)(u)$:

$$\begin{aligned}\phi(r)(v + u) &= r \cdot (v + u) \\ &= r \cdot v + r \cdot u \\ &= \phi(r)(v) + \phi(r)(u)\end{aligned}$$

- $\phi(r)(s \cdot v) = s \cdot \phi(r)(v)$:

$$\begin{aligned}\phi(r)(s \cdot v) &= r \cdot (s \cdot v) \\ &= (rs) \cdot v \\ &= (sr) \cdot v \\ &= s \cdot (r \cdot v) \\ &= s \cdot \phi(r)(v)\end{aligned}$$

Therefore our map $\phi$ is a valid set-map from $R$ to $\mathrm{End}_R(V)$. We now need to show that it is a homomorphism of rings:

- $\phi(r + s) = \phi(r) + \phi(s)$:

$$\begin{aligned}\phi(r+s)(v) &= (r+s) \cdot v \\ &= r \cdot v + s \cdot v \\ &= \phi(r)(v) + \phi(s)(v) \\ &= (\phi(r) + \phi(s))(v)\end{aligned}$$

- $\phi(rs) = \phi(r) \circ \phi(s)$:

$$\begin{aligned}\phi(rs)(v) &= (rs) \cdot v \\ &= r \cdot (s \cdot v) \\ &= \phi(r)(s \cdot v) \\ &= \phi(r)(\phi(s)(v)) \\ &= (\phi(r) \circ \phi(s))(v)\end{aligned}$$

- $\phi(1) = \mathrm{Id}$:

$$\begin{aligned}\phi(1)(v) &= 1 \cdot v \\ &= v \\ &= \mathrm{Id}(v)\end{aligned}$$

Finally, we need to prove that the image of the map $\phi$ is contained within the center of $R$, i.e. that given any element $r \in R$ and any endomorphism $f \in \mathrm{End}_R(V)$, $\phi(r)$ commutes with $f$.

- $\phi(r) \circ f = f \circ \phi(r)$:

$$\begin{aligned}(\phi(r) \circ f)(v) &= \phi(r)(f(v)) \\ &= r \cdot f(v) \\ &= f(r \cdot v) \\ &= f(\phi(r)(v)) \\ &= (f \circ \phi(r))(v)\end{aligned}$$

So, indeed, $\mathrm{End}_R(V)$ is an $R$-algebra. It has some interesting sub-algebras; for instance (I know this holds for a vector space, but I think that the scalars can come from any commutative ring), the sub-algebra $R[A]$ generated by a single endomorphism $A$ is ismorphic to the quotient $R[x]/(p(x))$ of the free $R$-algebra over one variable by the ideal generated by the minimal polynomial of $A$. □

# 2 Optional/Practice Problems

**Problem 1.** Prove that $\mathbb{Z}$ is the initial object in the category of rings, based on the definition of $\mathbb{Z}$ as the unique ordered ring where the positive elements are well-ordered.

*Proof.* I won't write a complete proof of this, but I've thought a bit about how to prove it. I would start by "reinventing" the integers within an arbitrary ring, as the subring generated by the identity ($1$, $1+1$, $1+1+1$, etc.) and show that given the defining properties of $\mathbb{Z}$,

- Every element of $\mathbb{Z}$ is contained within this subring, and
- Within $\mathbb{Z}$, any two elements in this ring are equal only if they must be ($1 = 1, 1+1 = 1+1$, etc.)

This is easier to do with some abuse of notation, where we might write $1+1+1$ as $3 \cdot 1$, even though we don't "know" what 3 is. The proof depends on the fact that $0 < 1$, and that no other element of $\mathbb{Z}$ may lie between 0 and 1, as if some element $a$ did, the set $\{a, a^2, a^3, \dots\}$ would be infinite and decreasing, without containing its own lower bound, contradicting well-orderedness.

This totally determines the elements of $\mathbb{Z}$, and we can quickly recover the status of $\mathbb{Z}$ as an initial object, since every ring contains the subring generated by the identity, and any map out of $\mathbb{Z}$ is totally determined by its value on the identity, which is set in stone. □

**Problem 2a.** Prove that $n$ divides the characteristic of a ring $R$ if there exists a ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to R$, and that the converse is true if $n \in \mathbb{Z}_{\geq 1}$.

*Proof.* Let $\phi$ be some ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to R$. Then

$$0 = \phi(0) = \phi(\underbrace{1 + 1 + \cdots + 1}_{\text{n times}}) = \underbrace{\phi(1) + \phi(1) + \cdots + \phi(1)}_{\text{n times}}.$$

. This shows that $n \cdot 1 = 0$; to finish the first half of the proof we need to show that if $n \cdot 1 = 0$ in any ring, than $n$ is a multiple of the characteristic, which is a short proof - the characteristic $k$ must be less than or equal to $n$, so we see that

$$0 = \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} + \underbrace{1 + 1 + \cdots + 1}_{n-k \text{ times}} = 0 + \underbrace{1 + 1 + \cdots + 1}_{n-k\text{times}}.$$

Inductively, we get a series of decreasing natural numbers $n, n-k, n-2k$, which must terminate somewhere between 0 and $k$. It cannot go lower than $k$ and higher than 0 without

contradicting minimality of $k$, so we must have that $n - j \cdot k = 0$ for some for some $j$, and thus that $n$ is a multiple of the characteristic of $R$.

The reason that the opposite is true is that we may lower the unique map $\phi$ from $\mathbb{Z}$ into $R$ to a map from $\mathbb{Z}/n\mathbb{Z}$ to $R$, by the universal property of the quotient construction - the only necessary lemma is that $\phi$ is zero on the subring $n\mathbb{Z}$, which is relatively simple. □

**Problem 2b.** Show that the characteristic of a field $k$ is either 0 or a prime number.

*Proof.* It is immediate from the field axiom $1 \neq 0$ that the characteristic is not 1, so assume for contradiction that the characteristic of the field is a composite number, $m \cdot n$ for $m, n \geq 2$. Then by minimality of the characteristic, $m \cdot 1 \neq 0$ and $n \cdot 1 \neq 0$, but $(m \cdot 1) \cdot (n \cdot 1) = 0$, which is impossible in a field. □

**Problem 3.** Show that any homomorphism of a field into a ring is injective.

*Proof.* A homomorphism of rings may be decomposed into a quotient by a kernel and an injection into the target. A kernel is an ideal, and fields have very few ideals, so the quotient must be by the trivial ideal 0, making the map injective. (It cannot be the quotient by the field itself, because $1 \neq 0$ in the rings we are working with? Otherwise the zero homomorphism would be valid.) □

**Problem 4.** Show that if $V$ is an $(R, S)$-bimodule and $W$ is an $(R, T)$-bimodule, then $\mathrm{Hom}_R(V, W)$ is an $(S, T)$-bimodule.

*Proof.* This proof involves checking a few axioms, much like problem 1, so I won't run through the verification. We note that $V$ is a right $S$-module, but $\mathrm{Hom}_R(V, W)$ is a left $S$-module. This is an interesting result in noncommutative algebra, but it is also useful in the commutative case. One of the important uses for this bimodule-Hom structure is that it allows us to define a tensor-hom adjunction between arbitrary rings: let $S$ and $R$ be commutative rings, and let $M$ an $R$-module, $N$ be an $(R, S)$-bimodule, and $P$ an $S$-module. (In the commutative case, an $(R, S)$-bimodule is the same as an $(S, R)$-bimodule.) Then $\mathrm{Hom}_S(N, P)$ is both an $S$- and $R$-module, and we have a canonical isomorphism

$$\mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P)) \cong \mathrm{Hom}_S(M \otimes_R N, P).$$

This is an adjunction $F \vdash G$, where $F : R\text{-Mod} \Rightarrow S\text{-Mod}$ is the functor $- \otimes_R N$, and $G : S\text{-Mod} \Rightarrow R\text{-Mod}$ is the functor $\mathrm{Hom}_S(N, -)$ This of course reduces to the tensor-hom adjunction $- \otimes_R N \vdash \mathrm{Hom}_R(N, -)$ between endofunctors of $R$-mod in the case that $R = S$. □