Notes on Modules and Linear Algebra

Mike Pierce

Everyone's Favorite Category, R-MOD

For a fixed ring R we'll let R-MOD denote the category of all left R-modules. Analogously, MOD-R is the category of all right modules over R. The categories are equivalent though, so it's safe to assume a module is a left R-module if it's not specified. We only run into trouble if we're thinking of our module as having both a left and right R-module structure that aren't necessarily compatible.

If rings R and S have identity 1_R and 1_S and if we live in a world where we insist that a homomorphism of rings $R \to S$ sends $1_R \mapsto 1_R$, then we'll say that R and S are unital rings. Then an R-module M is unitary if R is unital and if the action of 1_R on M does exactly what we'd expect: $1_R.m = m$ for all $m \in M$.

A category R-MOD is an example of an abelian category, which, glossing over some details, means that (1) the Hom-sets have an abelian group structure, (2) finite direct sums and products exist, (3) it has a zero object, (4) every map has a kernel and cokernel, and (5) all monomorphisms and epimorphisms are normal, which just means they behave exactly as you'd want them to behave relative to their kernels and cokernels. Now the reason we *really* love module categories is that *every* small abelian category is equivalent to some full subcategory of a module category. Albeit cool and motivating, that fact is beyond the scope of what we're talking about.

EXERCISE 1 — Prove that the category RING of unital rings is *not* an abelian category. Prove that RNG, the category of not-necessarily-unital rings is also not an abelian category. Does this change if we consider only *commutative* rings?

> The category RING doesn't have a zero object since the initial object is $\mathbf{Z}$ and the terminal object is $\{0\}$. In the category RNG, the Hom-sets don't carry a group structure: try writing out $(f+g)(ab)$ in two different ways. Considering only commutative rings doesn't fix these issues.

An example of modules to keep in mind: each ideal I of R is an R-module, where the action of R on I is just given by multiplication in the ring. You can prove certain things about the category R-MOD just by proving them for the ideals of R.

EXERCISE 2 — For a commutative ring R, to have the property in R-MOD that every submodule of a finitely generated R-module is itself finitely generated, it is sufficient to have the property hold for the submodules (ideals) of R. I.e. if R is Noetherian, then every finitely generated R-module is Noetherian.

> A proof of this can be extracted from the proofs of Theorems 1.8 and 1.9 in Hungerford Chapter VIII. ◂

Another example to keep in mind is that the category of abelian groups is just the category of $\mathbf{Z}$-modules, where the action of $\mathbf{Z}$ on a group G is given by

$$n.g = \underbrace{g + \cdots + g}_{n \text{ times}}.$$

So your extensive knowledge of abelian groups carries over a bit into module theory. Like, a bunch of the counterexamples you should know are just $\mathbf{Z}$-modules.

Exercise 3 — For unital ring R, recall that unitary R-module is simple if it admits no quotients. This is the same as saying a module has no submodules. Prove that a simple R-module M must be cyclic, and that the ring $\mathrm{End}_R(M)$ is a division ring. What about the converse? Is it true that if $\mathrm{End}_R(M)$ is a division ring then M must be simple?

> The first part is chill since for any $\varphi \in \mathrm{End}_R(M)$ we'll find that $\mathrm{Ker}\,\varphi$ and $\mathrm{Im}\,\varphi$ are submodules of M. The converse is not true though. Take $R = \mathbf{Z}$ and $M = \mathbf{Q}$.

Short Exact Sequences, and Other Drawings

A sequence of R-modules

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \longrightarrow \cdots$$

is exact provided that $\mathrm{Ker}\,\varphi_j = \mathrm{Im}\,\varphi_{j-1}$. Then a short exact sequence is an exact sequence that is short: In a short exact sequence like the following, the map i must be injective (monic) and so $B \cong \mathrm{Ker}\,\pi$, and π must be surjective (epic), so $A \cong \mathrm{CoKer}\,i \cong X/B$.

$$0 \longrightarrow B \xrightarrow{i} X \xrightarrow{\pi} A \longrightarrow 0$$

Exercise 4 — Consider a commutative diagram in R-Mod of the form

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \overset{i_1}{\rightarrowtail} & C & \overset{\pi_1}{\twoheadrightarrow} & A & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle h} & & & & \\ 0 & \longrightarrow & Y & \underset{i_2}{\rightarrowtail} & Z & \underset{\pi_2}{\twoheadrightarrow} & X & \longrightarrow & 0 \end{array}$$

such that the top and bottom rows are exact

(a) Suppose there exists a morphism $f\colon A \to X$ such that $\pi_2 h = f\pi_1$, so the right-most square commutes. Prove that there exists some $g\colon B \to Y$ that makes the whole diagram commutes. What condition(s) must f and h satisfy to ensure that g is injective?

(b) Suppose there exists a morphism $g\colon B \to Y$ such that $i_2 g = h i_1$, so the left-most square commutes. Prove that there exists some $f\colon A \to X$ that makes the whole diagram commutes. What condition(s) must g and h satisfy to ensure that f is surjective?

(a) Take $b \in B$, and consider $i_1(b) \in C$. Since the top row is exact and $f\pi_1 = \pi_2 h$, we have $0 = \pi_2 i_1(b)$, and so $\pi_2 h i_1(b) = 0$. So since $h i_1(b)$ is in the kernel of π_2 and since the bottom row is exact, there exists $y \in Y$ such that $i_2(y) = h i_1(b)$, and this y is unique since i_2 is injective. Then we can define $g\colon B \to Y$ where $g(b) = y$. This map is well-defined, and $h i_1 = i_2 g$ by construction.

If $g(b) = 0$, then we need $h i_i(b) = 0$, so we get g is injective if $h|_{\operatorname{Im} i_1}$ is injective.

(b) Take some $a \in A$. Since π_1 is surjective, there exists some $c \in C$ such that $\pi_1(c) = a$. Let's tentatively define the map $f\colon A \to X$ such that $f(a) = \pi_2 h(c)$. Now we've made a *choice* of c here. To prove our function f is well-defined, we must prove that the value of $f(a)$ doesn't depend on our choice of c in the preimage of a. So suppose we have $c' \in C$ such that $\pi_1(c') = a$. Notice that since c and c' both map to a, $c - c'$ is in the kernel of π_1. Since the top row is exact, there is a unique $b \in B$ such that $i_1(b) = c - c'$. Following b down via g, since $h i_1 = i_2 g$ we get $i_2 g(b) = h(c - c')$. Then since the bottom row is exact, following π_2 we get $0 = \pi_2 i_2 g(b) = \pi_2 h(c - c') = \pi_2 h(c) - \pi_2 h(c')$, which means $\pi_2 h(c) = \pi_2 h(c')$, so our map f is well-defined.

For $x \in X$, there is some $z \in Z$ such that $\pi_2(z) = x$. We need there to be a $c \in C$ such that $h(c) = z$ to guarantee that we have a $\pi_1(c) \in A$ that maps to x. So for f to be surjective we need to require that h is surjective onto the preimage of π_2.

Exercise 5 (The Short-Five Lemma)— Given a commutative diagram in R-Mod of the form

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \overset{i_1}{\rightarrowtail} & C & \overset{\pi_1}{\twoheadrightarrow} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & Y & \underset{i_2}{\rightarrowtail} & Z & \underset{\pi_2}{\twoheadrightarrow} & X & \longrightarrow & 0 \end{array}$$

with top and bottom rows exact, if f and g are monomorphisms then so is h. Similarly if f and g are epimorphisms then so is h.

This is proven similarly to the previous exercise. ◂

A short exact sequence

$$0 \longrightarrow B \xrightarrow{\ i\ } X \xrightarrow{\ \pi\ } A \longrightarrow 0$$

is split if (1) there exists a section $s\colon A \to X$ of the map π such that $\pi s = \mathbf{1}_A$, or (2) if there exists a retract $r\colon B \to X$ of the map i such that $ir = \mathbf{1}_B$, or (3) if there exists an isomorphism $\varphi\colon X \to A \oplus B$ such that the following diagram commutes,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{\ i\ } & X & \xrightarrow{\ \pi\ } & A & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 0 & \longrightarrow & B & \rightarrowtail & B \oplus A & \twoheadrightarrow & A & \longrightarrow & 0 \end{array}$$

where $B \rightarrowtail B \oplus A$ and $B \oplus A \twoheadrightarrow A$ are the canonical inclusion and projection. These three

conditions are equivalent, and you can prove they are equivalent either manually, or using the Short-Five Lemma to do some of the heavy lifting. Note that for (3), it is not sufficient to just require that $X \cong B \oplus A$.

> Ralf Schiffler uses a different description of the terms section and retraction in his quiver representations book (page 16), and now I'm concerned where I heard these definitions. Like, he says a section is a map $B \to X$ and a retract is your map $X \to A$, and we only call them that if the sequence splits, which does make sense.

Exercise 6 — Find an example of a ring R and a short exact sequence of R-modules

$$0 \longrightarrow B \xrightarrow{\ i\ } X \xrightarrow{\ \pi\ } A \longrightarrow 0$$

such that $X \cong A \oplus B$ but the exact sequence does not split.

> The idea is that if $X \cong A \oplus B$, then there is a short exact sequence that splits, but not *every* short exact sequence splits. See
>
> math.stackexchange.com/q/135444
>
> Note that if R is Noetherian, $X \cong A \oplus B$, and X, A, and B are finitely generated over R, then every such short exact sequence splits. ◂

Exercise 7 — Let $\mathscr{C}$ be the full subcategory of R-Mod consisting of modules M with the property that every R-submodule of M which is also in $\mathscr{C}$ has a complement in $\mathscr{C}$. That is to say, if $N_1 \hookrightarrow M$ is an object in $\mathscr{C}$, there there is another object $N_2 \hookrightarrow M$ in $\mathscr{C}$ such that $N_1 \oplus N_2 \cong M$. Prove that every short exact sequence in $\mathscr{C}$ splits.

> Write down an arbitrary short exact sequence $0 \to A \to B \to C \to 0$. Since A is a submodule of B, there's a submodule A' of B such that $B \cong A \oplus A'$. Underneath the first short exact sequence draw the (split) sequence $0 \to A \to A \oplus A' \to A' \to 0$, draw the appropriate vertical arrows, and apply the Short-Five Lemma. ◂

Given R-modules A and B, an extension of A by B (also called an extension of B by A) is an object X such that there is a short exact sequence $0 \to B \to X \to A \to 0$. The set of (isomorphism classes of) extensions of B by A actually form a group denoted $\mathrm{Ext}^1(A, B)$.

Exercise 8 — For a commutative unital ring R, a full subcategory $\mathscr{C}$ of R-Mod is called a Serre (or thick) subcategory if for every short exact sequence

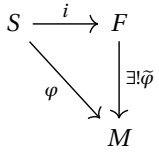
$$0 \longrightarrow B \xrightarrow{\ i\ } X \xrightarrow{\ \pi\ } A \longrightarrow 0,$$

in R-Mod, X is an object of $\mathscr{C}$ if and only if A and B are objects of $\mathscr{C}$. Another way to say this is that $\mathscr{C}$ is closed under taking extensions, subobjects, and quotients. If R is an integral domain prove that the full subcategory of torsion R-modules, modules M such that for each $m \in M$ there exists some $r \in R$ such that $r.m = 0$, form a Serre subcategory of R-Mod. Is the subcategory of torsion-free R-modules a Serre subcategory?

◂

Free and Projective Modules (and Maybe Injective Modules)

An object F in a (concrete) category is free on a set S if there exists a map (of sets) $i\colon S \to F$ with the following universal property: for any other object M in the category such that there exists a map φ into (the underlying set of) M, there exists a unique map $\widetilde{\varphi}$ such that this diagram commutes:



Equivalently, if we're in the category of all unitary R-modules for some unital ring R, then an R-module F is free if F has a basis, or equivalently if $F \cong \bigoplus R$.

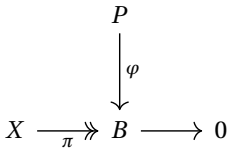
Exercise 9 — Suppose that we have an exact sequence of vector spaces (which are modules over a division ring $\boldsymbol{k}$ and are inherently free)

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow \cdots \longrightarrow V_n \longrightarrow 0$$

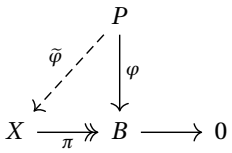
such that $\dim_{\boldsymbol{k}} V_i$ is finite for each i. Prove that $\sum_{i=1}^{n} (-1)^i \dim_{\boldsymbol{k}} V_i = 0$.

> For $n = 1$ or $n = 2$ this is chill. For $n = 3$ we have a sequence $0 \to V_1 \xrightarrow{i} V_2 \xrightarrow{\pi} V_3 \to 0$ where $V_2 \cong \operatorname{Ker}\pi \oplus \operatorname{Im}\pi \cong V_1 \oplus V_3$. I.e. every short exact sequence of vector spaces splits. You can write out the induction formally from here, or just expand everything as $\operatorname{Ker} \oplus \operatorname{Im}$ and note that everything cancels.

An R-module P is projective (or P is a projective object in the category R-Mod) if for any diagram in R-Mod that looks like



there exists some map $\widetilde{\varphi}\colon P \to X$ such that $\pi\widetilde{\varphi} = \varphi$ (the diagram commutes)



Exercise 10 — In a category of unital R-modules over a unitary ring R, a free object is projective.

> Draw the diagram for a free object, and use the universal property of a free object to get that map you need to show it's projective. ◂

Note that the converse of the previous exercise is true if your ring R is a PID: For a PID R, an R-module is projective if and only if it's free.

Exercise 11 — Prove that $\mathbf{Q}$ is *not* a projective $\mathbf{Z}$-module.

Since $\mathbf{Z}$ is a PID, it's sufficient to show that $\mathbf{Q}$ is not a free $\mathbf{Z}$-module. First prove that $\mathbf{Q}$ is not a 1-dimensional $\mathbf{Z}$-module, and then prove that any two elements of $\mathbf{Q}$ are linearly dependent over $\mathbf{Z}$.

Exercise 12 — Characterize all projective abelian groups.

Since abelian groups are $\mathbf{Z}$-modules and $\mathbf{Z}$ is a PID, the projective abelian groups are exactly the free ones.

Exercise 13 — For a field $\boldsymbol{k}$, is the field of rational functions $\boldsymbol{k}(x)$ a projective $\boldsymbol{k}[x]$-module? How do you describe the dual module of $\boldsymbol{k}(x)$ as a $\boldsymbol{k}[x]$-module? How do your answers to the previous questions change if you replace $\boldsymbol{k}$ with just some integral domain? How do your answers to the previous questions change if you replace $\boldsymbol{k}[x]$ with just some integral domain R and $\boldsymbol{k}(x)$ with it's field of fractions $\mathrm{Frac}(R)$?

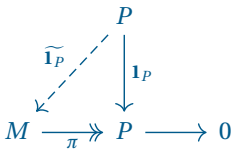
Similar to the last exercise, but meatier. So $\boldsymbol{k}(x)$ is not a projective $\boldsymbol{k}[x]$-module by an argument identical to that in the previous exercise. The module dual of $\boldsymbol{k}(x)$, $\boldsymbol{k}(x)^* := \mathrm{Hom}_{\boldsymbol{k}[x]}(\boldsymbol{k}(x), \boldsymbol{k}[x])$ turns out to be $\{0\}$. If $\varphi \in \boldsymbol{k}(x)^*$, say the degree of $\varphi(1)$ is n. But the degree can't be n because

$$x^{n+1}\varphi\left(\frac{1}{x^{n+1}}\right) = \varphi\left(\frac{x^{n+1}}{x^{n+1}}\right) = \varphi(1)\,.$$

Then it turns out this is true even if the ring you're working over is just some is just some integral domain. See math.stackexchange.com/q/3331287

Exercise 14 — Suppose that P is a projective R-module, and is the homomorphic image of some R-module M. Prove that P is isomorphic to a direct summand of M. What is the analogous fact to this one concerning injective R-modules?

Draw the diagram



and you've just shown the short exact sequence $0 \to \mathrm{Ker}\,\pi \to M \xrightarrow{\pi} P \to 0$ splits. Then if you rotate that diagram by 180° degrees and change the direction of all the arrows, you'll see that, analogously, if an injective module is isomorphic to a submodule of M, then it is a direct summand of M.

Exercise 15 — In R-Mod, a direct sum $\bigoplus P_i$ is projective if and only if each P_i is projective.

We'll prove it for $P_1 \oplus P_2$, and the general result will follow inductively.

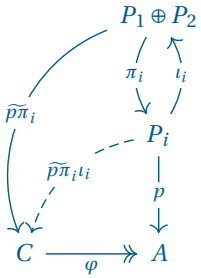
Recall we have an isomorphism

$$\mathrm{Hom}_R(P_1, X) \oplus \mathrm{Hom}_R(P_2, X) \cong \mathrm{Hom}_R(P_1 \oplus P_2, X).$$

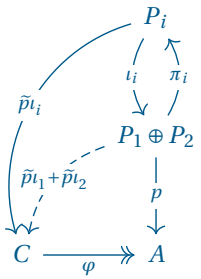
This isomorphism basically tells us that if we have a maps f and g from P_1 and P_2 respectively with a common codomain, we can glue them together to get a map $f+g$ from $P_1 \oplus P_2$. Another key fact is that $\oplus$ is both the product and coproduct in the category R-MOD, so for $i \in \{1,2\}$ we have the projection maps $\pi_i \colon P_i \oplus P_2 \twoheadrightarrow P_i$ and inclusion maps $\iota_i \colon P_i \hookrightarrow P_1 \oplus P_2$.

Start with a surjective map of R-modules $\varphi \colon C \twoheadrightarrow A$.

Suppose that $P_1 \oplus P_2$ is projective, and suppose we have a map $p \colon P_i \to A$. Then we have a map $p\pi_i \colon P_1 \oplus P_2 \to A$ which will lift to maps $\widetilde{p\pi}_i \colon P_1 \oplus P_2 \to C$. Then by construction the map $\widetilde{p\pi}_i \iota_i$ will be the lifting of p such that $\varphi \widetilde{p\pi}_i \iota_i = p$, which shows P_i is projective.



Conversely suppose that both P_1 and P_2 are projective and we have a map $p \colon P_1 \oplus P_2 \to A$. Since P_1 and P_2 are each projective, the maps $p\iota_i$ will each lift to a map $\widetilde{p\iota}_i \colon P_i \to C$. Then by construction the map $\widetilde{p\iota}_1 + \widetilde{p\iota}_2$ (which uses each π_i) will be the lifting of p such that $\varphi(\widetilde{p\iota}_1 + \widetilde{p\iota}_2) = p$, which shows $P_1 \oplus P_2$ is projective.



Good ol' Hom and $\otimes$

For two R-modules A and B the set $\mathrm{Hom}_R(A,B)$ of all R-linear maps $A \to B$ naturally has the structure of an abelian group, which it inherits from the abelian group structure on the underlying groups of A and B. This is is a requirement for R-MOD to be an abelian category.

EXERCISE 16 — For a commutative unital ring R and left R-modules M and N, does $\mathrm{Hom}_R(M,N)$ naturally inherit an R-module structure from M and N? Is it necessary to

assume that R is commutative? What if M is a right R-module instead?

> Yes, and yes because of the axiom where we require that $(rs)f = r(sf)$ for $r, s \in R$ and $f \in \mathrm{Hom}_R(M, N)$. And it's fine if M is a right R-module; you just have to define the action differently.

A functor $F\colon \mathscr{C} \to \mathscr{D}$ is covariant if it preserves the direction of morphisms (so it's just a normal functor). Specifically, given objects A and B of $\mathscr{C}$, for any morphism $A \to B$ we get a morphism $F(A) \to F(B)$. A functor is contravariant if it turns morphisms around, so a morphism $A \to B$ becomes a morphism $F(A) \leftarrow F(B)$. Or you could think of a contravariant functor $F\colon \mathscr{C} \to \mathscr{D}$ as a covariant (usual) functor $F\colon \mathscr{C} \to \mathscr{D}^{\mathrm{op}}$.

Exercise 17 — Each of $\mathrm{Hom}_R(D, -)$ and $\mathrm{Hom}_R(-, D)$, are functors R-Mod $\to R$-Mod. One is covariant and the other is contravariant. Which is which?

> Draw the diagrams. ◂

Each of the functors $\mathrm{Hom}_R(D, -)$ and $\mathrm{Hom}_R(-, D)$ are left-exact, which means that given a short exact sequence $0 \to B \to X \to A \to 0$, the induced sequence that is the image of the functor might not be exact on the right.

$$\begin{aligned} 0 \longrightarrow &\mathrm{Hom}_R(D, B) \longrightarrow \mathrm{Hom}_R(D, X) \longrightarrow \mathrm{Hom}_R(D, A) \\ &\mathrm{Hom}_R(A, D) \longleftarrow \mathrm{Hom}_R(X, D) \longleftarrow \mathrm{Hom}_R(B, D) \longleftarrow 0\,. \end{aligned}$$

This should be easy to remember if you know about the long exact sequence in (co)homology that comes up in algebraic topology. This long-exact sequence measures exactly how much a functor, like $\mathrm{Hom}_R(D, -)$ or $\mathrm{Hom}_R(-, D)$ in this case, fails to be right exact.

Exercise 18 — For a unital ring R and a unitary left R-module M, write out the details of the left R-module isomorphism $M \cong \mathrm{Hom}_R(R, M)$.

> A map $f \in \mathrm{Hom}_R(R, M)$ is an R-module homomorphism and so has the property that $f(r) = rf(1_R)$. That is to say f is completely determined by the image of 1_R. So the isomorphism in question is given by $m \mapsto (1 \mapsto m)$.

Exercise 19 — Prove that P is a projective R-module if and only if $\mathrm{Hom}_R(P, -)$ is an exact functor, so it sends short exact sequences to short exact sequences.

> Given a short exact sequence $0 \to B \to X \to A \to 0$ we only need to prove that $\mathrm{Hom}_R(P, X) \to \mathrm{Hom}_R(P, A)$ is surjective. To do this, draw the diagram. ◂

Exercise 20 — Consider a fixed short exact sequence $0 \to B \to X \to A \to 0$ of objects in R-Mod. Prove that the functor $\mathrm{Hom}_R(D, -)$ preserves the exactness of the sequence for any object D if and only if the sequence is split.

> For one direction, draw the diagram. For the other direction, pick the right D.

To formally define the tensor product $A \otimes_R B$ of two R-modules A and B, you start with the *free abelian group generated by* $A \times B$, so formal sums of elements (a_i, b_i). Then you quotient

by the normal subgroup generated by the relations

$$(ar, b) = (a, rb) \qquad (a+\alpha, b) = (a, b) + (\alpha, b) \qquad (a, b+\beta) = (a, b) + (a, \beta) \qquad (\star)$$

for $a, \alpha \in A$, $b, \beta \in B$, and $r \in R$. A good way to think about a tensor product $M \otimes_R N$ is as formally defining the "most free" multiplication you can between elements of M and elements of N that is still compatible with the R-module structure. In fact, you can use $\otimes$ to define multiplication in general. Recall that you can think of an abelian group G as a $\mathbf{Z}$-module. Then you can define a unital ring-structure on G by designating some element $1 \in G$ as your identity and defining a unital associative group homomorphism $G \otimes_{\mathbf{Z}} G \to G$. This is an alternative way of defining unital rings: you have to specify the associativity of the ring multiplication manually, but left- and right-distributivity is covered by the $\otimes$ relations.

Since algebras are just modules equipped with a multiplication, you define algebras similarly in terms of a map out of a tensor product. For a commutative unital ring R, an R-algebra is a unitary left R-module A and an associative module homomorphism $A \otimes_R A \to A$ such that $r(a \otimes \alpha) = ra \otimes \alpha = a \otimes r\alpha$.

Exercise 21 — For a torsion abelian group A (every element of A has finite order), and considering $\mathbf{Q}$ as an additive group, prove that

$$A \otimes_{\mathbf{Z}} \mathbf{Q} = 0 \qquad \text{and} \qquad \mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q} \cong \mathbf{Q} \qquad \text{and} \qquad \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}_3 = 0\,.$$

◂

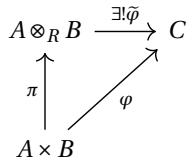
Exercise 22 — If α is the nontrivial $\mathbf{Z}$-module homomorphism $\mathbf{Z}_2 \to \mathbf{Z}_4$, prove that $\mathbf{1} \otimes \alpha \colon \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}_2 \to \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}_4$ is the zero map.

There aren't many possible maps. Exhaust them. ◂

Now often we have to define a homomorphism into or out of a tensor product, but it can be kinda tricky to make sure such a map is well-defined since the tensor product is defined as a quotient. Luckily there's a nice universal property we can utilize. We'll say a map φ out of a product $A \times B$ of R-modules is middle-linear if it satisfies the same sort of relations as in $(\star)$. Explicitly φ is middle-linear if

$$\varphi(ar, b) = \varphi(a, rb) \qquad \varphi(a+\alpha, b) = \varphi(a, b) + \varphi(\alpha, b) \qquad \varphi(a, b+\beta) = \varphi(a, b) + \varphi(a, \beta)\,.$$

Let π be the quotient map $A \times B \to A \otimes_R B$, and notice that π is a middle-linear map. For R-modules A and B and an abelian group C, for any other middle linear map $\varphi \colon A \times B \to C$ there exists a unique *group* homomorphism $\tilde{\varphi}$ such that $\tilde{\varphi}\pi = \varphi$.



Anytime you need to show that something is isomorphic (as an abelian group) to a tensor product $A \otimes_R B$, and you feel compelled to be really careful about things, define your map first as a middle-linear map out of the prodcut $A \times B$, then cite the universal property to get your map out of $A \otimes_R B$, then argue injectivity and surjectivity separately.

Now that universal property only guarantees you a homomorphism of *abelian groups*! If you want to exend that to a homomorphism of R-modules, you first have to define an R-module structure on $A \otimes_R B$, and then you have to make sure your homomorphism respects that structure manually. If R is a commutative ring, then any left R-module M is naturally a bimodule (left- and right-module such that the left and right actions are compatible) too, where you define the right R-module structure to be equivalent to the left R-module structure. I.e define $rm = mr$ for all $m \in M$ and $r \in R$. So over a commutative ring R a tensor product of R-modules $A \otimes_R B$ is also an R-module, where

$$r(a \otimes b) = ra \otimes b = ar \otimes b = a \otimes rb = a \otimes br = (a \otimes b)r\,.$$

If R is *not* commutative, if A is a right R-modules and B is a left R-module, then you can still define an R-module structure on $A \otimes_R B$ if either A or B has a bimodule structure. There are no surprises writing out the details of this. We don't even need the bimodule structure to be over the same ring! But then the real question is, why aren't we guaranteed the nice universal property of $\otimes$ in any module category, not just in the category of abelian groups? Anyways ...

Exercise 23 — For a unital ring R and a unitary left R-module M, prove that every element of $R \otimes_R M$ is equivalent to a simple tensor ($r \otimes m$ as opposed to a sum $\sum_i r_i \otimes m_i$), and write out the details of the left R-module isomorphism $R \otimes_R M \simeq M$.

> Since $R \otimes_R M$ is generated by simple tensors, so it's sufficient to define the isomorphism on those. Also $r \otimes m = 1_R \otimes rm$, which strongly suggests the natural isomorphism. But we've still got to define the map out of $R \times M$, prove the map is middle-linear, and show the the induced map $R \otimes_R M \to M$ is a bijection. ◂

Exercise 24 — Let S be a two-sided ideal of a ring R and let SM denote the abelian subgroup of an R-module M generated by elements of the form sm for $s \in S$ and $m \in M$. Show that SM is an honest submodule of M, describe the natural left R-module structure on $R/S \otimes_R M$, and show that $R/S \otimes_R M \simeq M/SM$ as left R-modules.

◂

For any right R-module D, we get a functor $D \otimes_R -$ from the category of right R-modules to the category of abelian groups. Similary you can look at the functor $- \otimes_R D$ and switch all the words left/right, and nothing else really changes because of the symmetry of $\otimes$. This functor is covariant (prove it!) and, contrasting with $\mathrm{Hom}_R(D, -)$, is *right*-exact: for an exact sequence $0 \to B \to X \to A \to 0$ we get an induced short exact sequence of abelian groups

$$D \otimes_R B \longrightarrow D \otimes_R X \longrightarrow D \otimes_R A \longrightarrow 0\,.$$

Exercise 25 — Given an example of a unital ring R and unitary R-module M such that (i)

the functor $- \otimes_R M$ is not exact, and an example such that (ii) the functor $\mathrm{Hom}_R(M, -)$ is not exact.

For (i) let $R = \mathbf{Z}$ and $M = \mathbf{Z}_2$, and consider the short exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Q} \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0\,.$$

For (ii) consider the same R and M and the short exact sequence

$$0 \longrightarrow 2\mathbf{Z} \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Z}_2 \longrightarrow 0\,.$$

◂

Exercise 26 — Give examples of a commutative ring R, of R-modules M, M', and N, and of a map $f \in \mathrm{Hom}(M, M')$ such that

(a) f is injective, but $1 \otimes f : N \otimes_R M \to N \otimes_R M'$ is not injective.

(b) f is surjective, but $f_* : \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M')$, where $f_*(h) = f \circ h$, is not surjective.

For part (a), look at the map $1 \otimes f : \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z} \to \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}$ where $f : 1 \mapsto 2$. For part (b), look at part (ii) above. ◂

Exercise 27 — Suppose that A and A' are left R-modules and B and B' are right R-modules. Take $f \in \mathrm{Hom}(A, A')$ and $g \in \mathrm{Hom}(B, B')$. Is it necessarily true that

$$\mathrm{Ker}(f \otimes g) \simeq (\mathrm{Ker}\, f \otimes B) + (A \otimes \mathrm{Ker}\, g)\,?$$

Look at the map, from part (a) above, the map $1 \otimes f : \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z} \to \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}$ where $f : 1 \mapsto 2$. ◂

And of course, since we're talking about them in the same section, there's going to be a cool relationship between Hom and $\otimes$. For rings R and S, right R-module A, (R, S)-bimodule B, and right S-module C, we have an isomorphism of abelian groups

$$\begin{gathered}\mathrm{Hom}_S\big(A \otimes_R B, C\big) \cong \mathrm{Hom}_R\big(A, \mathrm{Hom}_S(B, C)\big) \\ \big((a \otimes b) \mapsto c\big) \mapsto \big(a \mapsto (b \mapsto c)\big)\end{gathered}$$

We call this isomorphism the Hom-tensor adjunction, which is just cool high-brow algebraic term for what the computer scientists call it currying: where a function of two variables can be thought of as a collection of "partially applied" functions of a single variable. For example, if you have a function $f(a, b)$ defined to output $a + b$, for each a you naturally have a function f_a where $f_a(b) = a + b$. While this is a cool fact to keep in mind, it doesn't really help solve any exercises that I've seen.

Exercise 28 — For a ring R and left R-modules M and N, write down the details of the

homomorphism of abelian groups

$$M^* \otimes_R N \longrightarrow \mathrm{Hom}_R(M,N)\,.$$

Prove that this homomorphism is in fact an isomorphism if R is a field and M and N are finite-dimensional vector spaces over R.

Remember $M^* := \mathrm{Hom}_R(M,R)$. The natural isomorphism is $(f \otimes n) \mapsto (- \mapsto f(-).n)$. To help with second part, recall that if M and N are vector spaces, then, per a choice of basis for M and N, $\mathrm{Hom}_R(M,N)$ is the set of $\dim N \times \dim M$ matrices with entries in R. ◀

Exercise 29 — Write out the details of the isomorphisms

$$\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_m, \mathbf{Z}_n) \cong \mathbf{Z}_{(m,n)} \cong \mathbf{Z}_m \otimes_{\mathbf{Z}} \mathbf{Z}_n\,.$$

◀

Linear Algebra, as you Learned at your Grandfather's Knee

Exercise 30 — Suppose R is a ring with no zero divisors such that for all $r, s \in R$ there exist $a, b \in R$ not both zero such that $ar + bs = 0$.

(a) If $R = K \oplus L$ as modules, then either $K = 0$ or $L = 0$.

(b) If R has an identity, then R has the invariant dimension property.

This solution is from Derek Lowenberg.

(a) Suppose $R = K \oplus L$ and $K \neq 0$. Suppose towards a contradiction that there is some $s \in L$ that is nonzero. Pick a nonzero $r \in K$. Then there exist $a, b \in R$ not both zero such that $ar + bs = 0$. If $a = 0$ then by hypothesis b is nonzero but since $bs = 0$ and R has no zero divisors this implies that $s = 0$, a contradiction. Similarly if $b = 0$ then a is nonzero and $ra = 0$ implies $r = 0$, again a contradiction. Therefore $L = 0$.

(b) If R has identity, then any infinite bases for a free R module have the same cardinality. Suppose that F is a free module with bases $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ where $n < m$. That is, there is an isomorphism

$$\varphi\colon Rx_1 \oplus \cdots \oplus Rx_n \to Ry_1 \oplus \cdots \oplus Ry_m$$

With the given bases we can write φ as an $n \times m$ matrix A and an $m \times n$ matrix B such that $AB = I_n$ and $BA = I_m$.

Now the hypothesis on R allows us to preform the elementary row operation of adding a multiple of one row to a multiple of another to reduce matrices with entries in R to row echelon form. For example, if $n = 2$ and $m = 3$ and

$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$ with $a_{11} \neq 0$ and $a_{21} \neq 0$ then there exist $c, d \in R$, both nonzero, such that $ca_{11} + da_{21} = 0$. Then multiplication on the left by the matrix $\begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix}$ gives a matrix with 0 in the $1,2$ position.

In general, consider a $k \times k$ matrix M with a nonzero $c \in R$ in the j^{th} spot of the diagonal, 1's elsewhere on the diagonal, some nonzero $d \in R$ in the i^{th} column of the j^{th} row ($i \neq j$) and 0's elsewhere. Then $Mv = 0$ gives $v_t = 0$ for $t \neq j$ and $v_i = 0$ along with $cv_i + dv_j = 0$ implies $dv_j = 0$ so that $v_j = 0$ as $d \neq 0$ and R has no zero divisors. Hence $\ker(M) = 0$.

Using only matrices of the above description along with permutation matrices (which also have 0 kernel) one can reduce B to row echelon form. Since B has more rows than columns, its row echelon form has a row of 0's. Let X be the matrix which reduces B to row echelon form, so that XB has a row of zeros.

Now we have $(XB)A = X$. Then $(XB)A$ has a row of 0's (since XB does) and hence a nonzero kernel. However, X has a 0 kernel since it is the composition of maps with 0 kernel. This is a contradicton, so no such φ can exist. Hence R has the invariant dimension property.

Exercise 31 — For a field $\boldsymbol{k}$ and finite dimensional free $\boldsymbol{k}$-module V, prove that if $\varphi \in \mathrm{End}_{\boldsymbol{k}}(V)$ is monic, then it's invertible with an invertible inverse. Is this still true if $\boldsymbol{k}$ is an integral domain?

If $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \subset \boldsymbol{k}^n$ is a basis for V, note that the vectors $\{\varphi\boldsymbol{v}_1, \ldots, \varphi\boldsymbol{v}_n\}$ will be linearly independent: If they weren't you'd have some nontrivial linear combination

$$a_1\varphi\boldsymbol{v}_1 + \cdots + a_n\varphi\boldsymbol{v}_n \;=\; \varphi(a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n) \;=\; 0$$

but this cannot be since φ is monic and the $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ are linearly independent. Since the vectors $\{\varphi\boldsymbol{v}_1, \ldots, \varphi\boldsymbol{v}_n\}$ are n linearly independent vectors in $\boldsymbol{k}^n$, and since $\boldsymbol{k}$ has the invariant dimension property, they form a basis for V. Therefore we can define φ^{-1} on the basis as $\varphi^{-1}\colon \varphi\boldsymbol{v} \mapsto \boldsymbol{v}$. And naturally $\varphi = \left(\varphi^{-1}\right)^{-1}$.

This is not true if $\boldsymbol{k}$ is just an integral domain. Let $\boldsymbol{k} = V = \mathbf{Z}$ and consider $\varphi\colon x \mapsto 2x$.

Let R be a commutative unital integral domain. The ring $\mathrm{End}_R(R^n)$ of endomorphisms of a free R module, will also be unital with unit $\mathbf{1}$, and zero map denoted $\mathbf{0}$. Recall that a unital ring can be thought of as a monoid with its multiplicative structure. Considering this, there is a unique alternating, R-multilinear monoid homomorphism $\det\colon \mathrm{End}(R^n) \to R$ called the determinant map. The determinant lets us make lofty conclusions about elements of $\mathrm{End}_R(R^n)$ by just looking at their image in R. Since the determinant is a monoid homomorphism, it'll map invertible endomorphisms to units in R.

Now we're very used to thinking of the determinant of a *matrix* in terms of its Laplace expansion and not a linear transformation, and that's okay. If we fix a basis for R^n and

identify $\mathrm{End}(R^n)$ with $\mathrm{Mat}_n(R)$, the collection of $n \times n$ matrices over R, then the determinant maps similar matrices to associates in R: If A and B are similar, then for invertible P we have

$$\det(A) \;=\; \det\left(PBP^{-1}\right) \;=\; \det(P)\det(B)\det\left(P^{-1}\right) \;=\; \left(\det(P)\det(P)^{-1}\right)\det(B) \;=\; \det(B)\,.$$

This is to say that it doesn't matter what choice of basis we pick for R^n, the determinant will be the same.

Now it's often an important question to ask if a given linear transformation is invertible, and to compute it's inverse. Thinking in terms of matrices, we can (at least attempt to) get at the inverse of transformation computationally. For a matrix $A \in \mathrm{Mat}_n(R)$, define the (i,j)-minor M_{ij} of A to be the determinant of the matrix resulting from removing the i^{th} row and j^{th} column from A. The signed minor $(-1)^{i+j}M_{ij}$ is called the (i,j)-cofactor, and the adjugate matrix (classical adjoint) $\mathrm{adj}(A)$ of A, is the transpose of the matrix consisting of these cofactors. That is, $(\mathrm{adj}(A))_{ij} = (-1)^{j+i}M_{ji}$. The motivation for is that, by construction, you have

$$\mathrm{adj}(A)\,A = A\,\mathrm{adj}(A) = \det(A)\mathbf{1}\,.$$

So if A is invertible, then you'll be able to write A^{-1} explicitly as $\det(A)^{-1}\mathrm{adj}(A)$. But even if A is *not* invertible, you can compute $\mathrm{adj}(A)$ and do matrix arithmetic to draw conclusions.

Exercise 32 — Prove that for a field R and $A \in \mathrm{Mat}_n(R)$, $\det(A) = 0$ implies that $A\boldsymbol{v} = 0$ for some nonzero $\boldsymbol{v} \in R^n$.

> If $\det(A) = 0$, then $A\,\mathrm{adj}(A) = \det(A)\mathbf{1} = \mathbf{0}$. This means that if $\mathrm{adj}(A) \neq 0$, then any column of $\mathrm{adj}(A)$ will be a suitable choice of $\boldsymbol{v}$. If $\mathrm{adj}(A) = 0$, then we need to work harder. I wish there were a more elegant solution to this one. ◀

Exercise 33 — For a commutative unital integral domain R, let A be an $n \times n$ matrix over R. Prove that $\det(A) = 0$ if and only if the system of linear equations $A\boldsymbol{v} = 0$ has a nontrivial solution (that an endomorphism corresponding to A is not monic). Does either direction of this statement remain true if we drop the assumption that R is an integral domain?

> Suppose $A\boldsymbol{v} = 0$ for some non-zero $\boldsymbol{v}$. Then
>
> $$A\boldsymbol{v} = 0 \implies \mathrm{adj}(A)A\boldsymbol{v} = \mathrm{adj}(A)0 \implies \det(A)\mathbf{1}\boldsymbol{v} = 0 \implies \det(A)\boldsymbol{v} = 0\,.$$
>
> But since $\boldsymbol{v} \neq 0$ and R is an integral domain, we must have $\det(A) = 0$.
>
> To prove the converse, we need to consider A as a matrix over $\mathrm{Frac}(R)$ and use the fact from Exercise 32 that $\det(A) = 0$ gives us a nonzero solution to $A\boldsymbol{v} = 0$ for $\boldsymbol{v} \in \mathrm{Frac}(R)^n$. This $\boldsymbol{v}$ will look like $\left\langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \right\rangle$, where $a_i, b_i \in R$. Let b be the product $b_1 \cdot \cdots \cdot b_n$. If $\boldsymbol{v}$ is a solution to $A\boldsymbol{v} = 0$, then $b\boldsymbol{v}$ will be too, and $b\boldsymbol{v} \in R^n$.
>
> If R is not an integral domain, then the correct version of this statement becomes "$A\boldsymbol{v} = 0$ has a nonzero solution iff $\det(A)$ is not zero or a zero-divisor." Proving this is kinda tough, but we can see that we at least need to add the condition that $\det(A)$

be a zero divisor with the example of $R = \mathbf{Z}_6$ and

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \qquad \boldsymbol{v} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}.$$

Exercise 34 — Prove that if A and B are invertible $n \times n$ matrices with entries in an integral domain $\boldsymbol{k}$, then $A + rB$ is invertible in the quotient field K of $\boldsymbol{k}$ for all but finitely many r.

For $n \times n$ matrices A and B which are invertible over an integral domain, the matrix $A + rB$, for $r \in K$, is *not* invertible in K if and only if $\det(A + rB) = 0$. But $\det(A + rB)$ is just a polynomial in r. Furthermore it'll be a non-constant polynomial of degree n since the coefficient on r^n will be $\det(B)$, and so it'll have at most n roots in K. That is, there will be at most n distinct values of r such that $\det(A + rB) = 0$.

Exercise 35 — What is the companion matrix M of the polynomial $f = x^2 - x + 2$ over $\boldsymbol{C}$? Prove that f is the minimal polynomial of M.

Answering this first bit just comes down to recalling that the companion matrix of a *monic* polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a + 0$ is

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}.$$

Note that this is how Hungerford defines it, but most other authors consider the transpose matrix instead (and I suppose define their action of $\boldsymbol{k}[x]$ on a vector space over $\boldsymbol{k}$ to be a right action instead too). So the companion matrix of our polynomial f is

$$\begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}.$$

To show that f is the minimal polynomial of M, you just need to show that M satisfies $f(M) = 0$, and that $g(M) \neq 0$ for any linear polynomial g. The second bit should obviously be true. The first bit we just need to verify manually:

$$\begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}^2 - \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix} + 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0.$$

EXERCISE 36 — Find the minimal polynomial of this matrix:

$$\begin{pmatrix} 2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 2 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \end{pmatrix}$$

Any matrix is similar to its transpose, so we might as well flip that 1 over and write the Jordan blocks in a reasonable order that correspond to the invariant factors of the matrix:

$$\begin{pmatrix} 2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \end{pmatrix} = \begin{pmatrix} 2 & \cdot & \cdot & \cdot \\ \cdot & 1 & 1 & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & -1 \end{pmatrix} \oplus \begin{pmatrix} 2 & \cdot & \cdot \\ \cdot & 1 & \cdot \\ \cdot & \cdot & -1 \end{pmatrix} \oplus \begin{pmatrix} -1 \end{pmatrix}$$

Remember that the minimal polynomial is the characteristic polynomial of the largest invariant factor, so the minimal polynomial is $(x-2)(x-1)^2(x+1)$.

EXERCISE 37 — Prove that two 3×3 matrices over an algebraically closed field $\boldsymbol{k}$ are similar if they have the same minimal polynomial and the same characteristic polynomial. Find an example to show that the analogous statement is not true for 4×4 matrices.

If two matrices are similar, then they correspond to the same endomorphism, and so they must have the same characteristic polynomial and minimal polynomial.

Proving the other implication comes down to doing some case-analysis on the possible shapes of the Jordan canonical forms of 3×3 matrices and using the fact that the minimal polynomial is the largest invariant factor of the transformation given by a matrix. For a choice of $a, b, c \in \boldsymbol{k}$, all the possible patterns of a Jordan canonical form will be

$$\begin{pmatrix} a & \cdot & \cdot \\ \cdot & b & \cdot \\ \cdot & \cdot & c \end{pmatrix} \begin{pmatrix} a & \cdot & \cdot \\ \cdot & a & \cdot \\ \cdot & \cdot & b \end{pmatrix} \begin{pmatrix} a & 1 & \cdot \\ \cdot & a & \cdot \\ \cdot & \cdot & b \end{pmatrix} \begin{pmatrix} a & \cdot & \cdot \\ \cdot & a & \cdot \\ \cdot & \cdot & a \end{pmatrix} \begin{pmatrix} a & 1 & \cdot \\ \cdot & a & \cdot \\ \cdot & \cdot & a \end{pmatrix} \begin{pmatrix} a & 1 & \cdot \\ \cdot & a & 1 \\ \cdot & \cdot & a \end{pmatrix}.$$

Each of these correspond uniquely to the six different options we could have for a

characteristic polynomial and minimal polynomial

$$(x-a)(x-b)(x-c)|(x-a)(x-b)(x-c)$$
$$(x-a)(x-b)|(x-a)^2(x-b)$$
$$(x-a)^2(x-b)|(x-a)^2(x-b)$$
$$(x-a)|(x-a)^3$$
$$(x-a)^2|(x-a)^3$$
$$(x-a)^3|(x-a)^3$$

Then this statement isn't true for 4×4 matrices because we have these two matrices that each have characteristic polynomial $(x-a)^4$ and minimal polynomial $(x-a)^2$:

$$\begin{pmatrix} a & 1 & \cdot & \cdot \\ \cdot & a & \cdot & \cdot \\ \cdot & \cdot & a & 1 \\ \cdot & \cdot & \cdot & a \end{pmatrix} \quad \begin{pmatrix} a & 1 & \cdot & \cdot \\ \cdot & a & \cdot & \cdot \\ \cdot & \cdot & a & \cdot \\ \cdot & \cdot & \cdot & a \end{pmatrix}$$

Exercise 38 — Prove that the minimal polynomial of a linear transformation of an n-dimensional vector space has degree at most n.

For your vector space over field $\boldsymbol{k}$, fix a basis, so your linear transformation can be thought of as a matrix M. The characteristic polynomial of M is defined as $\det(M-x\mathbf{1})\in\boldsymbol{k}[x]$, and this will have degree n, the coefficient of the x^n term being $\det(\mathbf{1})=1$. Note that M is a root of it's characteristic polynomial since, letting $x=M$, we have $\det(M-M\mathbf{1})=\det(0)=0$. The minimal polynomial of M, being the smallest monic polynomial of which M is a root, must divide the characteristic polynomial, and so will have degree at most n.

Start with an n-dimensional vector space V over a field $\boldsymbol{k}$, and with an linear endomorphism $\varphi\in\mathrm{End}_{\boldsymbol{k}}(V)$. An eigenvector for φ is a vector $\boldsymbol{v}$ such that $\varphi\boldsymbol{v}=\lambda\boldsymbol{v}$ for some $\lambda\in\boldsymbol{k}$, and λ is said to be the corresponding eigenvalue. An single eigenvalue might have multiple eigenvectors, and any linear combination of those eigenvectors will also be an eigenvector for that eigenvalue. So for an eigenvalue λ, let the eigenspace of λ, denoted $V_{\varphi,\lambda}$ or sometimes just V_λ be the subspace of V spanned by the eigenvectors of λ.

Exercise 39 — Suppose that φ and ψ are endomorphisms of a finite dimensional vector space V over an algebraically closed field $\boldsymbol{k}$.

(a) Prove that φ has an eigenvector in V.

(b) Prove that if φ and ψ are commuting endomorphisms, then φ and ψ have a common eigenvector in V.

(c) Prove that if φ and ψ are commuting endomorphisms, and one of φ or ψ has distinct eigenvalues, then there exists a basis of V consisting of vectors that are eigenvectors for both φ and ψ.

(a) An eigenvector for φ is a vector $\boldsymbol{v} \in V$ such that $\varphi\boldsymbol{v} = \lambda\boldsymbol{v}$ for some $\lambda \in \boldsymbol{k}$. Rearranging this a bit and taking a determinant, such a λ must be a root of $\det(\varphi - x\mathbf{1}_V) \in \boldsymbol{k}[x]$. Since $\boldsymbol{k}$ is algebraically closed, $\det(\varphi - x\mathbf{1}_V)$ is guaranteed to have a root in $\boldsymbol{k}$, and that root corresponds to an eigenvalue λ, which corresponds to some eigenvector $\boldsymbol{v}$.

(b) Since $\boldsymbol{k}$ is algebraically closed, φ has at least one eigenvector $\boldsymbol{v}$. If φ and ψ commute, since

$$\varphi\boldsymbol{v} = \lambda\boldsymbol{v} \implies \psi\varphi\boldsymbol{v} = \psi(\lambda\boldsymbol{v}) \implies \varphi\big(\psi\boldsymbol{v}\big) = \lambda\big(\psi\boldsymbol{v}\big),$$

$\psi\boldsymbol{v}$ is an eigenvector for φ too. This means that the eigenspace $V_{\varphi,\lambda}$ is ψ-invariant. So we can restrict ψ and consider it as an endomorphism of $V_{\varphi,\lambda} \subset V$. Since $V_{\varphi,\lambda}$ is a vector space over $\boldsymbol{k}$, ψ will have an eigenvector in $V_{\varphi,\lambda}$, and this eigenvector will also be an eigenvector of φ.

(c) Suppose that φ is the endomorphism with distinct eigenvalues $\{\lambda_1, \ldots, \lambda_n\}$. This means you get n linearly independent eigenvectors $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ for φ that form a basis for V, each spanning a 1-dimensional eigenspace V_{φ,λ_i}. But each of these 1-dimensional eigenspaces is ψ-invariant, and must contain an eigenvector of ψ since $\boldsymbol{k}$ is algebraically closed. So each $\boldsymbol{v}_i$ is an eigenvector for ψ too, and $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is the basis we're looking for.

Part (c) of this exercise is actually true in greater generality, but is the proof of the more general statement is quite a bit meatier.

Exercise 40 — Suppose that φ and ψ are endomorphisms of a finite dimensional vector space V. Assume that V has a basis consisting of eigenvectors of φ and that V has a basis consisting of eigenvectors of ψ.

(a) Prove that any φ-invariant subspace of V has a basis consisting of eigenvectors of φ.

(b) Prove that if φ and ψ are commuting endomorphisms, then V has a basis consisting of vectors that are eigenvectors for both φ and ψ simultaneously.

This solution is based on a note by Keith Conrad:

kconrad.math.uconn.edu/blurbs/linmultialg/simulcomm.pdf

(a) Let $\{\lambda_1, \ldots, \lambda_k\}$ be the distinct eigenvalues of φ. Each of these eigenvalues λ_i corresponds to an eigenspace V_{φ,λ_i}, and since V has a basis of eigenvectors of φ, we can decompose V as $\bigoplus_j V_{\varphi,\lambda_j}$ (i.e. these eigenspaces cover all of V). Take $\boldsymbol{w} \in W$ and under this decomposition we can write $\boldsymbol{w} = \boldsymbol{v}_1 + \ldots + \boldsymbol{v}_n$ where each $\boldsymbol{v}_i$ is in V_{φ,λ_i}. Since W is φ-invariant, we have that $\{\boldsymbol{w}, \varphi\boldsymbol{w}, \varphi^2\boldsymbol{w}, \ldots\}$ are

all in W. Then since φ is linear, for any positive integer m we have

$$\varphi^m(\boldsymbol{w}) = \lambda_1^m \boldsymbol{v}_1 + \cdots + \lambda_n^m \boldsymbol{v}_n .$$

Over each $m \in \{0, \ldots, k-1\}$ this gives us a system of k linear equations

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \ldots & \lambda_k^{k-1} \end{pmatrix} \begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_k \end{pmatrix} = \begin{pmatrix} \boldsymbol{w} \\ \varphi\boldsymbol{w} \\ \vdots \\ \varphi^{k-1}\boldsymbol{w} \end{pmatrix}.$$

The matrix on the left is the Vandermonde matrix of the $\{\lambda_1, \ldots, \lambda_k\}$, and will be invertible since the $\{\lambda_1, \ldots, \lambda_k\}$ are distinct. This means that we can write each $\boldsymbol{v}_i$ as a linear combination of the $\{\boldsymbol{w}, \varphi\boldsymbol{w}, \ldots, \varphi^{k-1}\boldsymbol{w}\}$ as

$$\begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_k \end{pmatrix} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \ldots & \lambda_k^{k-1} \end{pmatrix}^{-1} \begin{pmatrix} \boldsymbol{w} \\ \varphi\boldsymbol{w} \\ \vdots \\ \varphi^{k-1}\boldsymbol{w} \end{pmatrix}.$$

The point being that each $\boldsymbol{v}_i$ must then be in W, and so the eigenspace decomposition $V = \bigoplus_j V_{\varphi,\lambda_j}$ restricts to a decomposition $W = \bigoplus_j \left(V_{\varphi,\lambda_j} \cap W\right)$, and W will inherit a basis of eigenvectors of φ from each V_{φ,λ_j}.

(b) Let $\{\lambda_1, \ldots, \lambda_k\}$ be the distinct eigenvalues of φ, and let $\{\kappa_1, \ldots, \kappa_r\}$ be the distinct eigenvalues of ψ. Since φ and ψ are each diagonalizable, we have two decompositions of V into eigenspaces for φ and ψ as

$$V = \bigoplus_j V_{\varphi,\lambda_j} \qquad\qquad V = \bigoplus_j V_{\psi,\kappa_j}$$

Each one of these V_{φ,λ_j} is a ψ-invariant subspace since φ and ψ commute. And since V_{φ,λ_j} is ψ-invariant, by part (a) we we can restrict the decomposition of eigenspaces of ψ to each V_{φ,λ_j}, giving us a basis of V_{φ,λ_j} of eigenvectors for both φ and ψ. Glueing all the V_{φ,λ_j} back together into V Then this gives us a basis of V of eigenvectors for both φ and ψ.

The previous two exercises could be rephrased with the different, but equivalent, hypotheses.

- The vector space V has a basis consisting of eigenvectors of φ.
- The endomorphism φ of V is diagonalizable.
- The elementary divisors of φ are all linear.