# Algebra II Homework 4 Commentary

Zachary Gardner

Unless otherwise stated, $R$ denotes a commutative ring with 1 and $I$ denotes an ideal of $R$. Similarly, $A \in M_n(k)$ denotes a matrix and $f_1(x), \dots, f_r(x) \in k[x]$ its (monic) invariant factors (so $f_1 \mid \cdots \mid f_r$). We use parentheses for principal ideals.

## General Commentary

- How should we write elements of the quotient $R/I$? Certainly the elements are cosets $r + I$ for $r \in R$. While this notation is correct it can often get quite cumbersome and confusing (since the "+" in $r+I$ is **not** addition in the ring $R$). When there is little chance of confusion it is often better to write $\overline{r}$. Then, the equations for addition and multiplication of cosets look like $\overline{r} + \overline{s} = \overline{r+s}$ and $\overline{r} \cdot \overline{s} = \overline{rs}$ in contrast with $(r+I) + (s+I) = (r+s) + I$ and $(r+I)(s+I) = rs + I$. This notation also makes it easier to see the $R$-module structure of $R/I$ since we can write $r \cdot \overline{s} = \overline{rs}$.
- It's important to be clear about what we mean by the phrase *relatively prime*. By definition, two ideals $I, J$ are relatively prime if $I + J = R$ or, equivalently, we can find elements $\alpha \in I$ and $\beta \in J$ such that $\alpha + \beta = 1$. It then makes sense to say that two elements $a, b \in R$ are relatively prime if the ideals they generate are relatively prime – i.e., $(a) + (b) = R$. For $R$ a general ring this is the most we can say. For $R$ a PID we can say a little more. Namely, $(a) + (b) = (\gcd(a, b))$ and so $a, b$ are relatively prime if and only if $\gcd(a, b) = 1$ (it's worth thinking carefully about what exactly we mean by gcd).
- Vector spaces don't have ideals since they aren't rings. What is true that a vector space over a field $k$ is the same thing as a $k$-module, and a subspace is the same thing as a $k$-submodule. You should view the notion of module as a generalization of the notion of vector space that works over any ring.
- Modules don't have a multiplication and so it doesn't make sense to talk about 1 and multiplicative inverses as elements of a module. What's confusing about this is that many things we work with in practice such as $R/I$ have *simultaneous* ring and module structures.
- Saying that a linear map between vector spaces is not an isomorphism means that it is not injective **or** not surjective. In the special case that we have a linear map $T : k^n \to k^n$ (so the source and target are the same and have finite dimension), the Rank-Nullity Theorem tells us that $T$ is injective if and only if it is surjective. This is a rather rare property for maps to have in general.

## Problem 2

Let $\varphi : R/(a) \to R/(a)$ be the map given by multiplication by $b \in R$. Then, we can think of this map in two different ways. The first is that it is multiplication by $b + (a) = \bar{b}$. The second is that it is the scalar multiplication map associated to $b$, using the $R$-module structure of $R/(a)$ with $b \cdot \bar{c} = \overline{bc}$.

- If $b + (a)$ is a unit in $R/(a)$ then it is not necessarily true that $b$ is a unit in $R$. For this reason the inverse of $b + (a)$ should **not** be written as $b^{-1} + (a)$. A better choice of notation is $(b + (a))^{-1}$.
- Even though $R/(a)$ is a ring, the map $\varphi$ is only an $R$-module homomorphism and not a ring homomorphism for $b \neq 1$. This is because $\varphi$ is not compatible with multiplication.
- It's not a valid tactic to use Problem 3 for proving (c) $\implies$ (a) unless your proof for Problem 3 does not use Problem 2 (which I would say is unlikely).

## Problem 3

Let $\varphi$ denote multiplication by $f(x)$ on the quotient $k[x]/(q(x))$.

- There was some confusion about what part (a) means. Part (a) is saying that $f(x) \mid q(x)$ if and only if $f(x)$ and $q(x)$ are not relatively prime. This is because $f(x)$ is irreducible. Its not clear from the problem statement if Keerthi wanted people to comment on the equivalence of these two statements.
- Problem 2 does have a part to play here but is a statement about ideals. Since this problem needs a statement about elements you need to show the process of translating between the two statements to get full points.
- A multiplication map like $\varphi$ need not be surjective. For an example using $\mathbb{Z}$ consider multiplication by 2 on $\mathbb{Z}/4\mathbb{Z}$.
- In the case that $f(x) \mid q(x)$ and so $q(x) = f(x)g(x)$ for some $g(x) \in k[x]$, many people failed to explain why $\overline{g(x)}$ is a nontrivial element of $\ker \varphi$. It's not enough to say that $g(x) \neq 0$ as a polynomial. On a related note, saying that two coset representatives are different is not enough to say that the cosets they represent are different.

## Problem 4

- Keep in mind that $A$ may not be diagonalizable. Just because we can find one eigenvalue does not mean we can find an eigenbasis.
- Remember that we *define* the minimal and characteristic polynomials of $A$ to be $\min_A(x) := f_r(x)$ and $\mathrm{ch}_A(x) := f_1(x) \cdots f_r(x)$. Arguments using other conventions did not receive full points for this problem set.
- Take heed that $k[x]/(\mathrm{ch}_A(x))$ is **not** isomorphic to $k[x]/(f_1(x)) \times \cdots \times k[x]/(f_r(x))$. Indeed, the polynomials $f_1(x), \ldots, f_r(x)$ are by definition not pairwise relatively prime!
- One detail many people missed is exactly what is happening with $k$-pairs in this problem. The action of $x - \lambda$ on $V_{f_1} \times \cdots \times V_{f_r}$ corresponds to the action of $T_A - \lambda\,\mathrm{id}$ on $V_A$ by virtue

of the isomorphism of $k$-pairs $V_{f_1} \times \cdots \times V_{f_r} \cong V_A$ with the action of $x$ (by multiplication) corresponding to the action of $T_A$. If $x - \lambda$ acts non-injectively on some $V_{f_i}$ then it acts non-injectively on $V_{f_1} \times \cdots \times V_{f_r}$ since we can stick the nontrivial element of the kernel in the $i$th slot (and put 0's everywhere else). Conversely, if $x - \lambda$ acts non-injectively on $V_{f_1} \times \cdots \times V_{f_r}$ then it acts non-injectively on some $V_{f_i}$ since something "nontrivial" must be happening in at least one of the slots (this is a somewhat heuristic argument that you should try fleshing out for yourself).

- Your argument for (d) $\implies$ (a) should pretty much be the reverse of the one for (b) $\implies$ (c). Note that $\min_A(\lambda) = 0$ and $\min_A(\lambda \, \mathrm{id}) = 0$ are very much **not** the same statement! The former is a statement about elements of $k$ and the latter is a statement about either elements of $M_n(k)$ or linear maps from $k^n$ to itself.

## Problem 5

- While Problem 4 is closely related to Problem 5, we can't directly use Problem 4 in general here since $\min_A(x)$ may not factor completely into linear factors (or factor at all, for that matter...).
- Many people forgot to say something about the characteristic polynomial $\mathrm{ch}_A(x)$. This is understandable because of how the problem was formatted on the problem set.
- This problem has three different but closely related objects floating around: $p(x)$, $p(A)$, and $p(T_A)$. These are, respectively, a polynomial, a matrix, and a $k$-linear endomorphism ($k$-linear map with the same domain and codomain). The endomorphism $p(T_A)$ is the endomorphism of $V_A$ induced by $p(A)$ and, conversely, $p(A)$ is the matrix representation of $p(T_A)$ with respect to the standard basis on $V_A$. Analogous to Problem 4 the action of $p(T_A)$ on $V_A$ corresponds to the action of $p(x)$ on $V_{f_1} \times \cdots \times V_{f_r}$ by way of the isomorphism of $k$-pairs $V_{f_1} \times \cdots \times V_{f_r} \cong V_A$.
- It's true that (b) $\implies$ (a) can be reduced to showing that $\min_A(A) = 0$ in $M_n(k)$ but this a nontrivial statement that still requires proof.
- It's not immediate that matrix factorizations give rise to polynomial factorizations, since the evaluation map from polynomials to matrices forgets some information. More specifically, we have an evaluation map $\mathrm{ev} : k[x] \to M_n(k)$ given by $p(x) \mapsto p(A)$. What is the kernel of this map? Precisely the principal ideal $(m_A(x))$ by virtue of this problem.

## Problem 6

- If you did not use the definition of determinant given on this problem set then you did not receive full points for this problem. Many facts about determinants require careful proof depending on the definition you choose. For example, why is the determinant multiplicative and why do cofactor expansions work?
- It's a general fact that a polynomial in $k[x]$ has a root at 0 if and only if its constant term vanishes.
- For this problem it's not so helpful to try to reason in terms of nonzero eigenvalues.
- If $\det(A) \neq 0$ then we can use $\mathrm{ch}_A(A) = 0$ to explicitly find an inverse for $A$.

- If $\det(A) = 0$ then we can use $\mathrm{ch}_A(A) = 0$ to get $Af(A) = 0$ for some $f(x) \in k[x]$. Is this enough to conclude that $A$ is not invertible in $M_n(k)$?

# Problem 7

- The computations for this problem are much easier if you reduce mod 5 along the way.
- Note that $(x-2)^2$ and $(x-3)^2$ are **not** allowed as invariant factors since they don't divide the minimal polynomial.
- The linear factors $x-2$ and $x-3$ are **not** both allowed to be invariant factors since neither divides the other.
- The trace of the polynomial $(x^2+1)^2$ is 0 since you are looking at the coefficient of the $x^3$ term.
- Remember that the sum of the degrees of the invariant factors must be 4 for this problem.
- For diagonalizability it is not enough for the minimal polynomial to split into linear factors since these factors must also be pairwise distinct.

# Problem 8

It is an important yet subtle point here that $R$ is commutative since this allows us to exchange the order of scalar multiplication. For ease let $\varphi$ be the isomorphism from $M$ to $N$.

## Part (a)

- Part of proving that $M^{\text{tors}}$ is a submodule is showing that it is a group under addition.
- For showing that $M^{\text{tf}}$ is torsion-free, there is no need to use contradiction since we can just show directly that the only torsion element of $M^{\text{tf}}$ is 0.

## Part (b)

- We have $M^{\text{tf}} = M/M^{\text{tors}}$ by definition. An equation like $M^{\text{tors}} = M/M^{\text{tf}}$ makes no sense since $M^{\text{tf}}$ is not a submodule of $M$. I should note, however, that there is a way to make some sense of this in general using the notion of "splitting."
- If you are trying to show that $\varphi(M^{\text{tors}}) = N^{\text{tors}}$ remember that you need to check containment both ways.
- One way of going about this is to show that $\varphi^{-1}$ carries $N^{\text{tors}}$ into $M^{\text{tors}}$ and so the restriction of $\varphi$ to $M^{\text{tors}}$ is an isomorphism onto $N^{\text{tors}}$. Note that it's really a miracle that $\varphi^{-1}$ is itself a homomorphism (if you're familiar with topology then this is not something you can expect from bijective continuous maps).
- Checking the second half of the problem about the torsion-free parts of $M$ and $N$ is something that needs to be done explicitly and is not just "clear." One way to handle this is to define an explicit isomorphism $\overline{\varphi} : M^{\text{tf}} \to N^{\text{tf}}$ using $\varphi : M \to N$. The "obvious" thing to try is $\overline{\varphi}(m + M^{\text{tors}}) := \varphi(m) + N^{\text{tors}}$. One must then check that this is well-defined, injective, and surjective. The homomorphism $\overline{\varphi}$ fits into a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \downarrow & & \downarrow \\ M^{\mathrm{tf}} & \xrightarrow[\overline{\varphi}]{} & N^{\mathrm{tf}} \end{array}$$

with vertical arrows given by quotient projection maps.

### Part (c)

- This problem is one of the ingredients that goes into proving the fundamental theorem for finitely generated modules over PIDs, so you certainly can't use it to prove this problem.
- Infinite products of torsion rings need not be torsion. So you need to briefly explain why *finite* products of torsion rings are torsion.