Algebra II Homework 1 Commentary

Zachary Gardner

This document is intended to be a resource for you, the student. I highly encourage you to read it carefully, though of course you should first skip to the parts you feel are most relevant to you. When in doubt, V and W denote vector spaces over a fixed field k and $T : V \to W$ a k-linear map.

General Commentary

Let's start with some general comments that apply to the entire problem set.

- The main point of this homework is to help you understand how and why linear algebra works. Simply saying "by linear algebra" won't cut it for most problems. Using rank-nullity and the notion of dimension prior to Problems 4 and 5, respectively, is also a no-go.
- Problems 2 and 8 have ties to older homework problems. Many students lost points by referencing results from those problems without giving requisite proofs.

Bases

- Never talk about 'the' basis of a vector space, only 'a' basis. Every nonzero vector space has many bases (infinitely many if k is infinite), related to each other by, well, change of basis.
- The only case where the above point **might** be arguable is for k^n, which has a standard basis given by $e_1 := (1, 0, \ldots, 0), \ldots, e_n := (0, \ldots, 0, 1)$.
- A basis is the same thing as a linearly independent spanning set. A spanning set may **not** be linearly independent. A linearly independent set may **not** span. This is why we have three separate notions.
- When talking about vector spaces, use words like 'dimension' or 'rank' instead of words like 'size' or phrases like 'the number of elements.' Remember that many vector spaces you encounter in daily life (such as $\mathbb{R}^n$) have finite dimension but are infinite as sets.

Kernels, Images, and Quotients

Fix $T : V \to W$ a k-linear map.

- Recall that the kernel of T is $\ker(T) := \{v \in V : Tv = 0\}$. It is a linear subspace of V. T is injective if and only if $\ker(T) = 0$.
- Recall that the image of T is $\mathrm{im}(T) := \{Tv : v \in V\}$. It is a linear subspace of W (not V!). T is surjective if and only if $\mathrm{im}(T) = W$. Equivalently, if and only if the **cokernel** $\mathrm{coker}(T) := W/\mathrm{im}(T)$ vanishes.

- The quotient $V/\ker(T)$ is neither a subspace of V nor of W. Its elements are cosets $v+\ker(T)$, with operations defined on coset representatives.
- There is a map $\overline{T} : V\ker(T) \to W$ given by $v+\ker(T) \mapsto Tv$. You can check by hand that this a well-defined injective linear map. It fits into a so-called *commutative diagram* (commutative in the sense that you get the same answer no matter how you follow the arrows)

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{T}} & \\ V/\ker(T) & & \end{array}$$

  where π is the so-called *canonical projection* sending an element of V to its coset.
- You should always give a clear definition of the map $\overline{T}$ above, even if it seems obvious to you in context. If you don't feel like writing a formula for $\overline{T}$ then you can simply say it is the "induced map from the quotient."
- The map $\overline{T}$ defines an isomorphism $V/\ker(T) \xrightarrow{\sim} \text{im}(T)$. This is the content of the so-called *first isomorphism theorem* and is related to factoring triangles.
- Let's say $V = k^m$, $W = k^n$, and $\ker(T) \cong k^r$. Then, it's not generally true that $k^m/\ker(T) = k^m/k^r$. First of all, k^r is not literally a subspace of k^m and so k^m/k^r does not make sense strictly speaking. We can, however, get around this difficulty by thinking of k^r as a subspace of k^m by putting in some extra 0's. Even still, it may not be true that $k^m/\ker(T) = k^m/k^r$. What is true is that $k^m/\ker(T) \cong k^m/k^r$ with this setup.
- Let's say $V \cong k^m$ and $W \cong k^n$. Then, you can't just write $T : k^m \to k^n$. There are, fortunately, several ways around this. The first is to use the phrase "by abuse of notation." This signals to the reader "I know this is not literally the same thing, but let's make our lives easier and use the same notation." The second is to use the phrase "assume without loss of generality (WLOG) that $V = k^m$ and $W = k^n$." This way you don't have to keep track of the isomorphisms.

Problem 1

Part (a) and Part (b)

Let's say the matrix of T is A. We do some row and column operations to put A in RREF or Smith normal form A' (they're basically the same in this setting). These operations are all invertible (they can be "reversed"), and their net effect is captured by an invertible linear transformation $S : k^m \to k^m$ such that A' is the matrix of $T \circ S$ (S changes things in the domain of T so that T has a nice formula). More concretely, we can say A' has block form

$$\begin{pmatrix} I_{m-r} & 0 \\ 0 & 0 \end{pmatrix}$$

with I_{m-r} the $(m-r)\times(m-r)$ identity matrix. The key (which most people picked up on) is that r (or the number of 0's on the diagonal) counts the dimension of $\ker(T)$ and $m-r$ (or the number of $1's$ on the diagonal) counts the dimension of $\text{im}(T)$. Most arguments mentioning pivot points or free/bound variables implicitly assume that $\ker(T)$ and $\text{im}(T)$ have complementary dimension, which is the content of the rank-nullity theorem (unproven at this point!). We can't, of course,

talk about dimension at this point and so we need to give explicit isomorphisms $\ker(T) \cong k^r$ and $\mathrm{im}(T) \cong k^{m-r}$. This is where $S \in \mathrm{GL}_n(k)$ as above comes in. Let $e_1, \ldots, e_m$ be the standard basis of k^m. It follows that $Se_1, \ldots, Se_m$ is also a basis for k^m since S is invertible. One then checks that $Se_{m-r+1}, \ldots, Se_m$ is a basis for $\ker(T)$ and $T(Se_1), \ldots, T(Se_{m-r})$ is a basis for $\mathrm{im}(T)$.

Remark. *Some students said that* 0 *is not in* $\mathrm{im}(T)$*, which is false. What is true is that the first* $m - r$ *columns of* A' *correspond to things with* ***nonzero*** *image under* T*.*

Part (c)

- Many students who used proof by contradiction here straight up proved the contrapositive. In such situations it is cleaner to just prove the contrapositive.
- You can use work from (a) and (b) to do things explicitly. Unless you use the factoring triangle, this is the only way to get full points for (ci) and (cii).
- k^m and k^n may both be infinite sets (if k is infinite) so comparing the size of both is not enough to relate m and n to statements about the injectivity and surjectivity of T.

Problem 2

Base Step

- Many people said that k has no nontrivial subspaces and left it at that. But proof is needed!
- The terms 'subgroup' and 'subspace' are not interchangeable, despite the fact that vector spaces form groups under addition. As an example, $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ under addition but is not a subspace.
- There is no such thing as a "trivial field." Every field k has elements $0, 1$ that obey certain properties and are **required** to be distinct.
- Every field does have a so-called *prime field* – i.e., a subfield which itself has no proper subfields. It turns out that such a prime field is (isomorphic to) either $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime $p > 0$. This is related to characteristic, which is discussed more in Problem 8.
- There is such a thing as a "trivial vector space" – namely, the zero vector space often denoted simply 0. If you like, this is k^0.

Inductive Step

- Many students failed to state their inductive hypothesis, either explicitly or implicitly.
- The inductive hypothesis should be handled with some care here. In particular, there should be no mention of dimension.
- Most students correctly invoked a (last coordinate) projection map $\pi : k^{n+1} \to k$ and identified that $\ker(\pi) \cong k^n$. However, a good number gave no information about π. Functions need formulas or some other kind of identifying information.
- Let's say H is a subspace of k^{n+1}. Many students correctly obtained an isomorphism $H \cap \ker(\pi) \cong k^m$ and even correctly reasoned that $H/H \cap \ker(\pi)$ is isomorphic to k or 0. However,

many students had trouble completing the induction from here. One method is to identify $H/H \cap \ker(\pi)$ as a subspace of H using the factoring triangle and work from there (this can be used to make precise the "intersection" of V/W and W). Here is another more explicit method. By assumption we have an isomorphism $\varphi : k^m \xrightarrow{\sim} H \cap \ker(\pi)$. Either H is equal to $H \cap \ker(\pi)$ and we are done or the two are not equal. Assume the latter. Choose some $v \in H \setminus H \cap \ker(\pi)$ and consider the k-linear map $\psi : k^{m+1} \to H$ defined by

$$\begin{aligned} e_1 &\mapsto \varphi(e_1) \\ &\vdots \\ e_m &\mapsto \varphi(e_m) \\ e_{m+1} &\mapsto v \end{aligned}$$

One then argues that ψ is an isomorphism.

Problem 3

- For (b) $\implies$ (c), all you need is the factoring triangle.
- Clearly write which implications you are proving. Use $\implies$ and not some other kind of arrow.
- To prove the full equivalence you only need to prove three implications. Four if you're torturing yourself, and by the time you have five you must be done. Which ones you should prove is usually determined by lecture theory – i.e., the order in which things are listed on the sheet.

Problem 4

Part (a)

- Uniqueness is an important part of the problem that many people forgot to prove. To do so, use Problem 1(ciii).
- The statement of 4(a) is equivalent to the statement that every finitely generated vector space V has a basis (with uniquely defined size). Thus, starting with the assumption that V has a basis to, say, construct an isomorphism from V to k^n, is a non-starter.

Part (b)

- A lot of people simply restated the problem without proving anything.
- It's not true that W is spanned by any spanning set of V. A spanning set of V spans, well, V – it is probably "too big" in relation to W.
- Assuming W has a basis, you need to do some work to show that the size of this basis is no larger than the size of a basis for V – it's not automatic!.
- Perhaps more specifically, it is not immediate that a basis for W extends to a basis for V. This is the content of Homework 2 Problem 4.

Problem 5

- The most direct way to do this problem is probably to use the results of Problem 4 and the factoring triangle.
- There is an alternative method that extends a basis of $\ker(T)$, but you need to explain how to do this using the factoring triangle for the quotient.
- Yet another method is to appeal directly to Problem 1, though beware that many people basically used this result to do Problem 1.
- Yet another method is to appeal to the finite dimensionality of $\mathrm{im}(T)$ (as a subspace of W, which is assumed to have finite dimension) and then look at some preimages of a basis for $\mathrm{im}(T)$. Morally, though, this argument frames $\mathrm{im}(T)$ in the wrong way. Rank-nullity still holds even if W has infinite dimension – the fact that $\mathrm{im}(T)$ has finite dimension is a reflection of the fact that V and not W has finite dimension.

Problem 6

- The map $T : P_6(k) \to k^3$ needs to have a special property – it can't just be any old k-linear map! The map T needs to capture the information of polynomials $q(x) \in P_6(k)$ such that $q(0), q(1), q(2)$ all vanish. You can define T by $q \mapsto (q(0), q(1), q(2))$ or, if you don't feel like writing elements, as $(\mathrm{ev}_0, \mathrm{ev}_1, \mathrm{ev}_2)$ for $\mathrm{ev}_a : P_6(k) \to k$ the "evaluate at $a \in k$" map.
- We are trying to find the polynomials of degree **exactly** 6 with the desired property. Looking at all of $\ker T$ gives polynomials of degree **at most** 6. Thus, when you take a linear combination of basis elements for $\ker T$, make sure the coefficient in front of the degree 6 term is nonzero.
- An alternative method for this problem that does not use linear algebra makes use of polynomial arithmetic and rests on the idea that if $f(x) \in k[x]$ vanishes at some $a \in k$ then $(x-a) \mid f(x)$ (this requires proof!). Several students who took this approach neglected to explain why we can work with more than one value at once – i.e., why if $f(0) = f(1) = f(2) = 0$ then $x(x-1)(x-2) \mid f(x)$. The key is that $x, x-1, x-2$ are pairwise relatively prime in $k[x]$ if $2 \neq 0$ in k and so we can use a polynomial form of Bézout's lemma (since $k[x]$ is a Euclidean domain).

Problem 7

- If you went the route of explicitly writing things in terms of basis vectors then remember that you need to check spanning **and** linear independence.
- A lot of people said $V \cong L^m$ and $L \cong k^n$, so $V \cong (k^n)^m \cong k^{nm}$. The issue with this argument is that V does not even a priori have a k-vector space structure. The first isomorphism above is only L-linear, while the second is only k-linear. You need to put a k-vector space structure on V so that the first L-linear isomorphism is a k-linear isomorphism.
- When you have a field extension L/k, the degree of the extension should be written as $[L : k]$ (and not the other way around; the notation is similar to that for subgroup index).

- That said, degrees of field extensions don't behave exactly like indices of subgroups. Namely, it is **not** the case that $[L : k] = |L|/|k|$ when L, k are finite fields. If $[L : k] = n > 1$ and $|k| = p^r$ then $|L|/|k| = p^{rn}/p^r = p^{r(n-1)} \neq n$ in general.

Problem 8

Part (a)

- Several students essentially tried to argue that the characteristic of a finite field is prime by using that the characteristic of a finite field is prime. This is circular reasoning.
- Don't use a "subfield criterion" without at least explaining what the criterion says (I wasn't around last semester, so have mercy on me!).
- Since the notion of characteristic is super important here, let's talk about it. We want to see that k must have the structure of a vector space over $\mathbb{F}_p$ for some prime $p > 0$. Intuitively, this means that we can scale elements of k by elements of $\mathbb{F}_p$ in a way compatible with the additive structure of k and the field structure of $\mathbb{F}_p$. One way we can obtain $\mathbb{F}_p$ is as the quotient ring $\mathbb{Z}/p\mathbb{Z}$. Scaling by $\mathbb{F}_p$ is then the same thing as scaling by $\mathbb{Z}$ except that multiplying by p kills everything. So, we're golden if we can get a map like the latter. Fortunately, there is an "obvious" ring homomorphism from $\varphi : \mathbb{Z} \to k$ that, well, scales things (this must be interpreted with some care for negative integers). Since k is a field, $\ker \varphi$ must be a prime ideal of $\mathbb{Z}$. And we know what such ideals look like – they have the form $p\mathbb{Z}$! This p is the characteristic of k.

Part (b)

- To prove that $r \mid s$, it is best to cite Problem 7.
- The statement that $p = q$ is equivalent to the statement that k (or any finite field) has a unique characteristic. Here's one way to see this that makes precise what a lot of students tried to argue. Suppose that k has distinct characteristics p and q. By definition, $p \cdot 1_k = 0_k = q \cdot 1_k$ for 0_k the additive identity of k and 1_k the multiplicative identity. Since $\gcd(p, q) = 1$, there exist (by Bézout's lemma) integers $a, b \in \mathbb{Z}$ such that $ap + bq = 1$. But then $1 \cdot 1_k = 0_k$ and so everything in k vanishes. In particular, $1_k = 0_k$, which contradicts the fact that these two elements are distinct.