Midterm Exam: Solutions

Math 700: Spring 2014

INSTRUCTIONS:

- Solve the problems below. Write up your solutions (neatly!), giving complete justifications for all arguments, and turn in a hard copy of your solutions in class on the

  Due Date: **Wednesday, March 19**

- The questions are meant to test your understanding of elementary concepts, and you should write down definitions of any technical terms you use, even if these terms are mentioned in the statement of the problem. Of course, you must use your best judgment about which definitions to state. (You probably don't want to define the integers or real numbers, for example.)

- It will help me (and probably your grade) if you do the following:
  1. State what you are trying to prove.
  2. Mention informally how you plan to prove it before giving the details.
  3. If you believe your proof is complete, use an end-of-proof symbol (like QED or $\square$); on the other hand, if you believe your proof is incomplete, say so.

HONOR CODE: You are expected to solve the exam problems on your own with no outside help. You may consult the lecture notes and textbook for this course only. No other books or internet usage is allowed. If you get stuck, please ask *me* for help, and I may post hints on our wiki page.

When you finish the exam, please sign the following pledge:

"On my honor as a student I, ________________________, have neither given nor received unauthorized aid on this exam." (Print Name)

Signature: ______________________________ Date: _______________

NOTATION: For the most part, we follow the notation used in the textbook. Recall that if V is a vector space over the field F and if $c \in F$, then $\sigma_c v = cv$ for all $v \in V$. In particular, σ_0 and σ_1 denote the zero and identity maps, respectively. However, when V and W are vector spaces over the same field, it is clearer to denote their identity maps by id_V and id_W, resp. We use $W \leqslant V$ to denote that W is a subspace of V, whereas $W \subseteq V$, means that W is a subset of V (which may or may not be a subspace). By an "F-vector space" we mean a vector space over the field F. If $\varphi : V \to W$, then $\mathrm{im}(\varphi) := \varphi(V)$, $\ker(\varphi) := \{v \in V : \varphi(v) = 0_W\}$, $\mathrm{rank}(\alpha) := \dim(\mathrm{im}(\alpha))$, and $\mathrm{null}(\alpha) := \dim(\ker(\alpha))$.

Problem 1. Let V and W be finite dimensional vector spaces over the field F, and suppose $\alpha \in \operatorname{Hom}(V, W)$. Circle true or false, where true means "always true" (no proof required):

(a) If $\alpha(v) = 0_W$ only when $v = 0_V$, then $\dim(V) = \dim(W)$. true $\boxed{\text{false}}$

(b) If $\operatorname{im}(\alpha) = \{0_W\}$, then $\alpha = \sigma_0$. $\boxed{\text{true}}$ false

(c) If $\dim(V) = \operatorname{rank}(\alpha)$, then $\ker(\alpha) = \{0_V\}$. $\boxed{\text{true}}$ false

(d) $\ker(\alpha) \leqslant \ker(\alpha^2)$ (assuming $W = V$) $\boxed{\text{true}}$ false

(e) $\operatorname{im}(\alpha) \geqslant \operatorname{im}(\alpha^2)$ (assuming $W = V$) $\boxed{\text{true}}$ false

(f) $\operatorname{null}(\alpha) \leqslant \operatorname{rank}(\alpha)$ true $\boxed{\text{false}}$

(g) $\operatorname{null}(\alpha) \leqslant \dim(V)$ $\boxed{\text{true}}$ false

(h) α is a one-to-one if and only if $\ker(\alpha) = \{0_V\}$. $\boxed{\text{true}}$ false

(i) α is a one-to-one if and only if $\dim(V) \leqslant \dim(W)$. true $\boxed{\text{false}}$

(j) α is a one-to-one if and only if $\operatorname{null}(\alpha) = 0$. $\boxed{\text{true}}$ false

(k) α is a onto if and only if $\dim(V) \geqslant \dim(W)$. true $\boxed{\text{false}}$

(l) α is a onto if and only if $\operatorname{rank}(\alpha) = \dim(W)$. $\boxed{\text{true}}$ false

Problem 2. Prove that the lattice of subspaces of a vector space is modular but not necessarily distributive, as follows: Let U, Y, and W be subspaces of a vector space V.

(a) Show that $U \cap (Y + (U \cap W)) = (U \cap Y) + (U \cap W)$.

(b) Show that $U \cap (Y + W) = (U \cap Y) + (U \cap W)$ is not always valid.

Solution. To prove (a), we show the right hand side is contained in the left and vice-versa. First note that $U \cap Y \subseteq U \cap (Y + (U \cap W))$ and $U \cap W \subseteq U \cap (Y + (U \cap W))$. Therefore, since $(U \cap Y) + (U \cap W)$ is the smallest subspace containing both $U \cap Y$ and $U \cap W$, we see that the right hand side is contained in the left. On the other hand, suppose $x \in U \cap (Y + (U \cap W))$. Then $x = u = y + z$ with $u \in U$, $y \in Y$, and $z \in U \cap W$. Whence, $y = u - z \in U \cap Y$, so $x = y + z$ belongs to the right hand side. The equation in part (a) is called the *modular law*, and we have just shown that, for any vector space V, the lattice $\langle \operatorname{Sub}(V), \cap, + \rangle$ of subspaces of V is a *modular lattice*.

To prove (b), consider the following subspaces of $\mathbb{R}^2$:

$$U = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} : a \in \mathbb{R} \right\}, \quad Y = \left\{ \begin{pmatrix} b \\ b \end{pmatrix} : b \in \mathbb{R} \right\}, \quad W = \left\{ \begin{pmatrix} 0 \\ c \end{pmatrix} : c \in \mathbb{R} \right\}.$$

Let us denote the zero vector of $\mathbb{R}^2$ by $\mathbf{0} = (0, 0)$. Note that any pair of (distinct) subspaces chosen from the set $\{U, Y, W\}$ intersects at $\{\mathbf{0}\}$ and sums to $\mathbb{R}^2$. Therefore, the left hand side of the equation in (b) is $U \cap (Y + W) = U \cap \mathbb{R}^2 = U$, while the right hand side is

$$(U \cap Y) + (U \cap W) = \{\mathbf{0}\} + \{\mathbf{0}\} = \{\mathbf{0}\}.$$

The equation in part (b) is called the *distributive law* and we have just shown that the lattice $\langle \mathrm{Sub}(V), \cap, + \rangle$ of subspaces of a vector space is not always a *distributive lattice*.

Problem 3. Prove that every nontrivial vector space V has a basis.

[*Hint:* First prove that every linearly independent subset of V is contained in a basis. As we did in class, let S be a linearly independent subset and let $\mathcal{S}$ be the set of all linearly independent subsets that contain S. Partially order $\mathcal{S}$ by inclusion $\subseteq$ and apply Zorn's Lemma.[1] Finally, say why if follows from this that every vector space has a basis.]

Solution. Let S be a linearly independent subset of V and let $\mathcal{S}$ be the set of all linearly independent subsets that contain S. Partially order $\mathcal{S}$ by set inclusion to obtain a poset $(\mathcal{S}, \subseteq)$. To apply Zorn's Lemma, we must check that every chain in $\mathcal{S}$ has an upper bound in $\mathcal{S}$. Fix a chain $\mathcal{C} = \{S_\alpha : \alpha \in \mathcal{A}\}$ in $\mathcal{S}$. Let $B = \bigcup \mathcal{C}$. Since every $S_\alpha \in \mathcal{C}$ is contained in B, it's clear that B is an upper bound for $\mathcal{C}$, with respect to $\subseteq$. We must show that B belongs to $\mathcal{S}$. Since $S \subseteq B$ is obvious, we just need to check that B is linearly independent. Let $b_1, \ldots, b_n$ be elements of B. Then there exist $\alpha(1), \ldots, \alpha(n)$ such that $b_i \in S_{\alpha(i)}$. Let $N = \max\{\alpha(i) : 1 \leqslant i \leqslant n\}$. Since $\mathcal{C}$ is a chain, all the elements $b_1, \ldots, b_n$ belong to S_N. Since S_N is linearly independent, the $b_1, \ldots, b_n$ are linearly independent. Now $b_1, \ldots, b_n$ was an arbitrary finite collection of vectors from B, so B is linearly independent. Thus, the hypotheses of Zorn's Lemma are satisfied, and we see that $\mathcal{S}$ has a maximal element; that is, a maximal linearly independent set that contains S. Finally, note that $\varnothing$ is a linearly idependent subset of every vector space. So, by the foregoing argument with S replaced by $\varnothing$, we see that every vector space contains a maximal linearly independent set (i.e., a basis).

Problem 4. Let V be a vector space over the field F, and suppose the subset $S \subseteq V$ satisfies $FS = V$. Prove that S contains a basis.

Problem 5. Let V be a vector space over the field F and let Ω be a (possibly uncountable) set. Describe V^Ω. Can you make V^Ω into an F-vector space? An F-algebra? Explain.

Solution. The set V^Ω is the set of all functions from Ω into V. That is, $V^\Omega = \{f : \Omega \to V\}$. We can make V^Ω into a vector space by defining

- *addition:* $\forall\, f, g \in V^\Omega$, define $f + g \in V^\Omega$ to be the map $(f+g) : \omega \mapsto f(\omega) +^V g(\omega)$. (Here $f(\omega) +^V g(\omega)$ means addition in V, which is available by the initial assumption that V is a vector space.)
- *additive identity:* $\sigma_0 \in V^\Omega$ is the map $\sigma_0 : \omega \mapsto 0_V$.
- *additive inverse:* $\forall\, f \in V^\Omega$, define $-f \in V^\Omega$ by $(-f)(\omega) = -f(\omega)$. (Again, interpret $-f(\omega)$ as additive inverse in the vector space V.)
- *scalar multiplication:* $\forall\, r \in F$, $\forall\, f \in V^\Omega$ define $rf \in V^\Omega$ to be the map $(rf) : \omega \mapsto rf(\omega)$ (where $rf(\omega)$ is scalar multiplication in V).

[1] **Zorn's Lemma:** If a partially ordered set $(\mathcal{S}, \subseteq)$ has the property that every chain $S_1 \subseteq S_2 \subseteq \cdots$ has an upper bound in $\mathcal{S}$, then $\mathcal{S}$ contains a maximal element.

It is easy to see that $\langle V^\Omega, +, -, \sigma_0\rangle$ is an abelian group, since $+$ is a commutative and associative by virtue $+^V$ having these properties, and since every $f \in V^\Omega$ has an inverse, namely $-f$, since $f + (-f) = \sigma_0$. Therefore, V^Ω is given the following vector space structure: $\langle V^\Omega, +, -, \sigma_0, \{r : r \in F\}\rangle$. (Technically, we should also check that scalar multiplication distributes over addition, and the other vector space properties, but this is also straight forward.)

There's no obvious or "natural" way to make V^Ω into an F-algebra, unless we have more assumptions about V. For example, we might want to define a binary multiplication as the "pointwise" product, $(f \circ g)(\omega) = f(\omega) \cdot g(\omega)$. However, it's unclear what we mean by $f(\omega) \cdot g(\omega)$? We need some notion of product $\cdot$ in the underlying vector space, V. This would be available if, for instance, we assumed V itself were an F-algebra. Alternatively, we might consider defining multiply by function composition: $(f \circ g)(\omega) = f(g(\omega))$. But for this to make sense, we need the domain of f to contain the range of g. If we assume $\Omega = V$ (e.g., $\Omega = V = F$), then we can make V^V into an F-algebra by defining product to be funciton composition.

Problem 6. Let V and W be vector spaces over the field F, and let $\varphi : V \to W$ be a linear transformation. Give details and proof of the following: φ is injective (respectively, surjective) if and only if there is a linear transformation $\psi : W \to V$ such that the composition of φ with ψ is the identity map.

[*Hint:* There are two claims to prove, (a) "φ is injective iff...", and (b) "φ is surjective iff..." There are two ways to form the composition, $\varphi\psi = \mathrm{id}_W$ and $\psi\varphi = \mathrm{id}_V$. Figure out which composition you need to prove each claim.]

Solution. We prove the following claims

(a) $\varphi \in \mathrm{Hom}(V, W)$ is injective iff there exists $\psi \in \mathrm{Hom}(W, V)$ such that $\psi\varphi = \mathrm{id}_V$.

(b) $\varphi \in \mathrm{Hom}(V, W)$ is surjective iff there exists $\psi \in \mathrm{Hom}(W, V)$ such that $\varphi\psi = \mathrm{id}_W$.

(a) ($\Leftarrow$) Assume there exists $\psi : W \to V$ such that $\psi\varphi = \mathrm{id}_V$, and fix $v_1, v_2 \in V$. If $\varphi(v_1) = \varphi(v_2)$, then $v_1 = \mathrm{id}_V(v_1) = \psi\varphi(v_1) = \psi\varphi(v_2) = \mathrm{id}_V(v_2) = v_2$. This proves that φ is one-to-one.

($\Rightarrow$) Assume φ is one-to-one. Let A be a basis for V. Then, since V is a homomorphism, $\varphi(A) = B$ is a basis for the subspace $\mathrm{im}(\varphi) \leqslant W$. Extend B to a basis $B \cup C$ for W. Define $\tilde{\psi} : B \cup C \to V$ as follows: for $w \in B \cup C$,

$$\tilde{\psi}(w) = \begin{cases} \varphi^{-1}(w), & \text{if } w \in B, \\ 0_V, & \text{if } w \in C. \end{cases}$$

Define $\psi : W \to V$ by linear extension of $\tilde{\psi}$. That is, given an arbitrary $w \in W$, which has a basis decomposition $w = \sum_B w(b)b + \sum_C w(c)c$, define $\psi \in V^W$ by

$$\psi(w) = \sum_{b\in B} w(b)\tilde{\psi}(b) + \sum_{c\in C} w(c)\tilde{\psi}(c) = \sum_{b\in B} w(b)\varphi^{-1}(b) + 0_V.$$

We claim $\psi\varphi = \mathrm{id}_V$. Indeed, fix an arbitrary $v \in V$, which has a unique basis decomposition as $v = \sum_A v(a)a$. Then, $\varphi(v) = \sum_A v(a)\varphi(a)$, so

$$\psi\varphi(v) = \sum_{a\in A} v(a)\psi\varphi(a) = \sum_{a\in A} v(a)\tilde{\psi}\varphi(a) = \sum_{a\in A} v(a)\varphi^{-1}\varphi(a) = \sum_{a\in A} v(a)a = v.$$

Therefore, $\psi\varphi = \mathrm{id}_V$.

(b) ($\Leftarrow$) Assume there exists $\psi : W \to V$ such that $\varphi\psi = \mathrm{id}_W$. Fix $w \in W$. We want to show there is a $v \in V$ such that $\varphi(v) = w$. Indeed, take $v = \psi(w)$. Then, $\varphi(v) = \varphi(\psi(w)) = \mathrm{id}_W(w) = w$.

($\Rightarrow$) Assume φ is surjective. Let D be a basis for W. Define $\tilde{\psi} : D \to V$ by $\tilde{\psi}(d) = v \in \varphi^{-1}(d)$. That is, for each $d \in D$, we simply pick our favorite element $v \in \varphi^{-1}(d)$.[2] Note that $\varphi\tilde{\psi}(d) = d$. Extend $\tilde{\psi}$ to all of W in the usual way: each $w \in W$ has a basis decomposition $w = \sum_D w(d)d$ and we define $\psi(w) = \sum_D w(d)\tilde{\psi}(d)$. Then,

$$\varphi\psi(w) = \varphi\sum_{d\in D} w(d)\tilde{\psi}(d) = \sum_{d\in D} w(d)\varphi\tilde{\psi}(d) = \sum_{d\in D} w(d)d = w.$$

Therefore, $\varphi\psi = \mathrm{id}_W(w)$.

Problem 7. Let V and W be vector spaces over the field F. Recall that W^V denotes the set of maps $\{f : V \to W\}$. For fixed $\alpha \in \mathrm{Hom}(V, W)$ and $w \in W$, define the *affine transformation* $\zeta_{\alpha,w} : V \to W$ to be the map $v \mapsto \alpha(v) + w$. Denote by $\mathrm{Aff}(V, W)$ the set of all such affine transformations. That is, $\mathrm{Aff}(V, W) := \{\zeta_{\alpha,w} : \alpha \in \mathrm{Hom}(V, W) \text{ and } w \in W\}$.

(a) Can you make W^V into an F-vector space? An F-algebra? Explain.

(b) Prove or disprove: $\mathrm{Hom}(V, W) \leqslant \mathrm{Aff}(V, W) \leqslant W^V$. (Interpret $\leqslant$ here as you see fit.)

(c) Note that ζ (without subscripts) may be viewed as a map from $\mathrm{Hom}(V, W)$ to $\mathrm{Aff}(V, W)^W$. Is ζ a vector space homomorphism? An F-algebra homomorphism? Prove.

Problem 8.

Let V be a finite dimensional vector space over the field F and suppose $T \in \mathrm{End}(V)$.
Prove the following:

(a) $\{0_V\} \leqslant \ker(T) \leqslant \ker(T^2) \leqslant \cdots$

(b) $V \geqslant \mathrm{im}(T) \geqslant \mathrm{im}(T^2) \geqslant \cdots$

(c) $\dim(V) = \mathrm{rank}(T^k) + \mathrm{null}(T^k)$, for each $k = 0, 1, \ldots$

(d) The sets $V_1 := \bigcap_{k=1}^{\infty} \mathrm{im}(T^k)$ and $V_2 := \bigcup_{k=1}^{\infty} \ker(T^k)$ are T-invariant subspaces.

[2] We must appeal to the Axiom of Choice here, since $\{\varphi^{-1}(d) : d \in D\}$ may be an infinite collection of inifinite sets.

(e) $V = V_1 \oplus V_2$.

(f) If T_i is the restriction of T to V_i, then T_1 is an isomorphism and T_2 is *nilpotent*.[3]

Solution. (a) If $T \in \mathrm{End}(V)$, then $T(0_V) = 0_V$, so $0_v \in \ker(T)$, so $\{0_v\} \leqslant \ker(T)$. Fix $n \in \mathbb{N}$. We want to show $\ker(T^n) \leqslant \ker(T^{n+1})$. If $v \in \ker(T^n)$, then $T^n v = 0_V$, so $T^{n+1}v = T(T^n v) = T(0_V) = 0_V$, so $v \in \ker(T^{n+1})$.

(b) Fix $n \in \mathbb{N}$. We must show $\mathrm{im}(T^n) \geqslant \mathrm{im}(T^{n+1})$. If $w \in \mathrm{im}(T^{n+1})$, then $w = T^{n+1}v$ for some $v \in V$. Let $v' = Tv$. Then $w = T^n(Tv) = T^n v'$, so $w \in \mathrm{im}(T^n)$.

(c) There are two ways we could proceed. First, note that for each $k = 0, 1, \dots$ we have $T^k \in \mathrm{End}(V)$, so $\dim(V) = \mathrm{rank}(T^k) + \mathrm{null}(T^k)$ follows from Proposition 6.10.

Alternatively, we can verify it directly (essentially reproving Proposition 6.10), as follows: Fix an arbitrary $k \in \{0, 1, \dots\}$, and let $N = \ker(T^k)$ Let W be a complement of N in V. Then, by Grassman's Theorem,

$$\dim(V) = \dim(N) + \dim(W) - \dim(K \cap W) = \mathrm{null}(T^k) + \dim(W) - 0.$$

It remains to show $\dim(W) = \mathrm{rank}(T^k)$, which would follow from $W \cong \mathrm{im}(T^k)$, so we prove the latter. Consider $T^k|_W$, the restriction of T^k to W. This is a homomorphism from W into $\mathrm{im}(T^k)$. We will show it is an isomorphism by proving that it is one-to-one and onto. It's one-to-one because $T^k|_W(v) = 0_V$ implies $v \in W \cap \ker(T^k) = W \cap N = \{0_V\}$; that is, $T^k|_W(v) = 0_V$ implies $v = 0_V$. To see that $T^k|_W$ is onto, fix $u \in \mathrm{im}(T^k)$. Then there exists $v \in V$ with $T^k(v) = u$. Let $v = z + y$, where $z \in N$ and $y \in W$. (Recall, N and W are complementary subspaces). Then $u = T^k(v) = T^k(z+y) = T^k(z) + T^k(y) = T^k(y)$, since $z \in N = \ker(T^k)$. Finally, since $y \in W$, we have $u = T^k(y) = T^k|_W(y)$. This proves that $T^k|_W$ is a bijective homomorphism from W onto $\mathrm{im}(T^k)$, as desired.

(d) (it's easy)

(e) In light of parts (a) and (b), and the finite dimensionality of V, there exists $n \in \mathbb{N}$ such that $\ker(T^{n+k}) = \ker(T^n)$ for all $k = 0, 1, \dots$. Similarly, there exists $m \in \mathbb{N}$ such that $\mathrm{im}(T^{m+k}) = \mathrm{im}(T^m)$ for all $k = 0, 1, \dots$. Let $N = \max\{n, m\}$. Then,

$$V_1 := \bigcap_{k=1}^{\infty} \mathrm{im}(T^k) = \mathrm{im}(T^N) \quad \text{and} \quad V_2 := \bigcup_{k=1}^{\infty} \ker(T^k) = \ker(T^N).$$

So, the goal is to prove $V = \mathrm{im}(T^N) \oplus \ker(T^N)$. First we show that $\mathrm{im}(T^N) \cap \ker(T^N) = \{0_V\}$. Suppose $w \in \mathrm{im}(T^N) \cap \ker(T^N)$. Then $w = T^N v$ for some $v \in V$, and

$$0_V = T^N w = T^N(T^N v) = T^{2N} v,$$

so $v \in \ker(T^{2N}) = \ker(T^N)$. Therefore, $w = T^N(v) = 0_V$.

It remains to show $V = \mathrm{im}(T^N) + \ker(T^N)$. This can be seen in at least two ways. One way is to notice that, by (c), we have

$$\dim(V) = \dim(\mathrm{im}(T^N)) + \dim(\ker(T^N)) = \dim(\mathrm{im}(T^N) + \ker(T^N)). \tag{1}$$

[3] $\alpha \in \mathrm{End}(V)$ is called *nilpotent* if there is a positive integer k such that $\alpha^k = \sigma_0$.

If A is a basis for $\mathrm{im}(T^N)$ and B is a basis for $\ker(T^N)$, then since these subspaces intersect at 0_V, the set $A \cup B$ is a basis for V. Otherwise there would be a vector $u \notin F(A \cup B)$ so that $A \cup B \cup \{u\}$ is linearly independent; but then

$$\dim(V) \geqslant \dim(F(A \cup B \cup \{u\})) > \dim(F(A \cup B)) = \dim(\mathrm{im}(T^N)) + \dim(\ker(T^N)),$$

which would violate (1).

As an alternative way to prove $V = \mathrm{im}(T^N) + \ker(T^N)$, we fix an arbitrary $v \in V$ and show that $v = x + y$ for some $x \in \ker(T^N)$ and $y \in \mathrm{im}(T^N)$. Indeed, since $\mathrm{im}(T^N) = \mathrm{im}(T^{2N})$, we have $T^N(v) = T^{2N}(w)$, for some $w \in V$. Therefore, $T^N(v - T^N(w)) = 0$, that is, $v - T^N(w) \in \ker(T^N)$. Thus,

$$v = (v - T^N(w)) + T^N(w) = x + y,$$

where $x \in \ker(T^N)$ and $y \in \mathrm{im}(T^N)$.