Math 110, Fall 2013. Proof Tips

The following are some tips that may (or may not) beuseful when attempting to prove statements. Of course, approaching a proof is like fixing a drink - there are many ways to make a good margarita :)

Subspaces, Sums, Direct Sums.

- to show that $U \subset V$, for V some F-vector space, is a subspace of V it suffices to show: for every $\lambda, \mu \in F$ and every $u, v \in U$ we have $\lambda u + \mu v \in F$.
- to show that $U \subset V$, for V some F-vector space, is NOT a subspace of V, you need to show that U does not satisfy the three axioms defining a subspace: either show
  - $0_V \notin U$ eg. $\{\underline{x} \in F^3 \mid x_1 + x_2 + x_3 = 1\}$
  - there are some $u, v \in U$ such that $u + v \notin U$ eg. $\{\underline{x} \in F^2 \mid x_1^2 = x_2\}$, take $u = v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.
  - there is a scalar $c \in F$ and some $u \in U$ such that $cu \notin U$ eg. U as in previous example and $c = 2$ and $u = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.
- to show that two subspaces $U, W \subset V$ are EQUAL you need to show that $U \subset W$ and $W \subset U$.
- to show that a subspace $U \subset V$ is equal to V it suffices to show that $\dim U = \dim V$.
- to show that a vector space $V = U + W$, for subspaces $U, W \subset V$, you need to show: for every $v \in V$, you can find some $u \in U$ and $w \in W$ (these choices will usually depends on v somehow) such that $v = u + w$.
- to show that $V = U \oplus W$ you need to show two things:
  1. $V = U + W$
  2. $U \cap W = \{0_V\}$
- you can also show that $V = U \oplus W$ if you know that $\dim V + \dim W = \dim V$ and $U \cap W = \{0\}$. OR, you can show that $V = U \oplus W$ if you know that $V = U + W$ and $\dim V + \dim W$. (this follows from the dimension formula)
- if you have a basis $(u_1, \dots, u_k)$ of U and a basis $(w_1, \dots, w_l)$ of W and $U \oplus W = V$, then $(u_1, \dots, u_k, w_1, \dots, w_l)$ is a basis of V. (you should be able to prove this, but it's also useful to know)
- if you're asked a questions like "... show there exists a subspace W such that..."you will usually have to consider some vectors $(v_1, \dots, v_m)$ (say vectors obtained by extending a basis of some given subspace U) and consider $W = \text{span}(v_1, \dots, v_m)$. Basically, the only way you can cook up a subspace out of thin air is to consider the span of some list of vectors (or perhaps the null space or range of a linear map).

Linear (in)dependence, span, bases, dimension.

- to prove that a given list $(v_1, \dots, v_k) \subset V$ is linearly dependent you have to find some $a_1, \dots, a_k \in F$ such that $a_1 v_1 + \dots + a_k v_k = 0_V$.

- linear independence proofs ALWAYS start with the sentence

  "Suppose that $a_1v_1 + ... + a_kv_k = 0_V$."

  You must then (somehow, using the information given in the statemen of the problem) show that the ONLY way that this linear equation can hold true is if $a_1 = ... = a_k = 0$.

- REMEMBER: a list is either linearly dependent OR linearly independent. You can use this fact to prove linear (in)dependence statements by contradiction (ie, assume the opposite holds and obtain some absurdity).

- to show that $\text{span}(v_1, \dots, v_n) \subset U$, for some subspace $U \subset V$, and $(v_1, \dots, v_n) \subset V$, it suffices to show that $v_i \in U$, for each $i = 1, \dots, n$. (Why?)

- if $\dim V = n$, then to find a basis of V you need only find a list $(v_1, \dots, v_n)$ (of length n) that is linearly independent OR spanning (ie, you only have to show one of the conditions for a list to be a basis).

- whenever you are given a linearly independent list $(v_1, \dots, v_k) \subset V$ ALWAYS think about extending it to a basis. Examples of such linearly independent lists are bases of subspaces $U \subset V$.

- if $(v_1, \dots, v_k)$ is linearly independent then so is any sublist.

- for ANY finite dimensional vector space V you know that a basis EXISTS; always choose a basis of V at the beginning of your problem. However, it is not always the case that you need to use the basis.

- determining the dimension of a subspace usually requires a **dimension formula** (you know two dimension formulae - one for sums of subspaces, one for null spaces/ranges of linear maps).

- if $u, v \in V$ are both nonzero and $u \notin \text{span}(v)$, then (u, v) is linearly independent.

Linear maps

- to show that a function $T : V \to W$ is linear it suffices to show: for every $\lambda, \mu \in F$ and $u, v \in V$, we have
  $$T(\lambda u + \mu v) = \lambda T(u) + \mu T(v).$$

- to define a linear map $T : V \to W$ it suffices to say what happens to a basis $(v_1, \dots, v_n)$ of V, ie, if $(v_1, \dots, v_n)$ is a basis of V and $w_1, \dots, w_n \in W$ are ARBITRARY, then there is a unique linear map $T : V \to W$ such that $T(v_i) = w_i$, for each $i = 1, \dots, n$. This is useful when you have problems of the form "Show that there exists a linear map T such that..."

- two linear maps $S, T \in L(V, W)$ are equal if they agree on a basis of V - ie, $S = T$ if and only if $S(v_i) = T(v_i)$, for $(v_1, \dots, v_n)$ a basis of V.

- the set $L(V, W)$ of all linear maps from V to W is a vector space (make sure you know the vector space structure). Moreover, if $\dim V = n, \dim W = m$ then $L(V, W)$ is isomorphic to $Mat_{m\times n}(F)$. Inj particular, $\dim L(V, W) = \dim V \dim W = mn$.

- for bases $B \subset V$ and $C \subset W$ there is an isomorphism

$$[-]_B^C : L(V, W) \to Mat_{m \times n}(F) \; ; \; T \mapsto [T]_B^C,$$

where $[T]_B^C$ is the matrix of T with respect to B and C.

- to show that $T \in L(V, W)$ is injective it suffices to show that $\text{null}(T) = \{0_V\}$. This means that you start with a sentence "Let $v \in \text{null}(T)$..." You then want to show that $v = 0_V$.

- $T \in L(V, W)$ is surjective if and only if $\text{range}(T) = W$.

- for $T \in L(V, W)$ we have the dimension formula $\dim V = \dim \text{null}(T) + \dim \text{range}(T)$. This formula tells you, for example, that there are no surjective maps from F^5 to F^7.

- for $T \in L(V)$, we have T is injective if and only if T is surjective. In this case, T is invertible (and there exists $S \in L(V)$ such that $TS = \text{id}_V = ST$). So, to show that an operator on V is invertible it suffices to show that it is either injective or surjective (I usually try and show injective...)

Polynomials

Make sure that you know the Fundamental Theorem of Algebra!

Eigenstuff, invariant subspaces

- to determine the eigenvalues/eigenvectors of a linear map $T \in L(V)$ you need to consider the equation $T(v) = \lambda v$ - you must find **NONZERO** $v \in V$ and λ for which this equation holds. It can often be useful to consider the cases $\lambda = 0$ and $\lambda \neq 0$ separately.

- remember the basic fact that $v \in V$ is an eigenvector if $v \neq 0$ and $T(v) \in \text{span}(v)$.

- any operator $T \in L(V)$ for a complex vector space V admits an eigenvalue. This does not hold for real vector spaces however - eg

$$T : \mathbb{R}^2 \to R^2 \; ; \; \underline{x} \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \underline{x}$$

has no (real) eigenvalues.

- if the matrix of a linear operator is in upper-triangular form then its eigenvalues are precisely the scalars appearing on the diagonal.

- in order to show that $U \subset V$ is T-invariant, it suffices to show that $T(u_i) \in U$, for each vector in a basis $(u_1, \dots, u_k)$ of U.

- an operator is diagonalisable if and only if there exists a basis of V consisting of eigenvectors of T.

- 0 is an eigenvalue of T is and only if $\text{null}(T) \neq \{0\}$.

- there is no relationship between diagonalisability and invertibility.

- the following are useful counterexamples to keep in mind: consider $T : \mathbb{R}^2 \to \mathbb{R}^2 \; ; \; \underline{x} \mapsto A\underline{x}$, where

- $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ - not invertible, not diagonalisable
- $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ - invertible, not diagonalisable
- $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ - not invertible, diagonalisable
- $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ - invertible, diagonalisable

- remember the zero linear map! This can often be a good counterexample to have.
- there are nonzero linear maps T such that $T^2 = 0$ - eg, the first linear map defined by the matrix A above.

General Proof Tips

- if you are given a statement like "Suppose ..... for every ..... Then, ..." (eg suppose that every subspace $U \subset V$ with $\dim U = \dim V - 1$ is T-invariant. Then, T is a scalar multiple of the identity.) - it can often be useful to proceed by contradiction - ultimately, you will want to construct an object (eg, subspace, linear map, whatever) which fails to satisfy the assumption given in the problem (ie, the statement coming after "Suppose...") So, in the example above we assume that T is not a scalar multiple of the identity and then try to construct a subspace U with $\dim U = \dim V - 1$ which is not T-invariant.
- always write down what you KNOW (the assumptions) and the immediate consequences of these assumptions (eg, if T is injective, then $\text{null}(T) = \{0\}$). This will allow the grader to see that you understand what you are supposed to use in order to solve the problem.
- always write down what it is that you WANT TO SHOW - again, noting any theorems that are related to the ideas in the conclusion of the statement.
- if you are given a statement "Show that there exists....", you need to give an actual example. For example, "Show that there exists a subspace such that...." means that you have to give a subspace satisfying the conclusion of this statement. As noted above, the only way you know to provide examples of subspaces is by using the span construction. Similarly, if the statement is "Show that there exists a linear map such that..." it is often the case that you define the required linear map by defining it on a basis of V (usually a particular basis), ie, state what the outputs are for these inputs.
- WRITE CLEARLY!!!
- if you want to quote a theorem from class write "..., by a theorem from class."