MATH 574 Homework 1

Qilin Ye

September 20, 2022

Problem 1

Let V, W be finite dimensional vector spaces over F and let $T : V \to W$ a linear transformation.

(1) Show that $\ker(T) = 0$ iff T maps any linearly independent subset of V to a linearly independent subset of W.

(2) Show that $T(V) = W$ iff T takes any spanning subset of V to a spanning subset of W.

(3) Show that T is an isomorphism of V and W iff T maps every basis of V to a basis of W.

Proof. (1) Let $v_1, \dots, v_n$ be a basis of V. If a linear combination $\sum c_i T(v_i) = T(\sum c_i v_i) = 0$, by the assumption that $\ker(T) = 0$ we see $\sum c_i v_i = 0$. In addition, from linear independence of v_i's, we see $c_i = 0$ for all i. This proves the linear independence of $T(v_i)$ for $1 \leqslant i \leqslant n$.

Conversely, suppose T maps linear independent subsets of V to that of W but $\ker(T) \neq \{0\}$. Assume $0 \neq v \in \ker(T)$. Then $\{v\}$ is linearly independent in V but $T(V) = \{0\}$ is not in W. This proves the claim.

(2) Suppose $T(V) = W$ and let $S \subset T$ be a spanning subset. For any $w \in W$, there then exists $v \in V$ with $T(v) = w$. By assumption, there exist $s_1, \dots, s_k \in S$ and $c_1, \dots, c_k \in F$ such that $v = \sum c_i s_i$. By linearity we must have $\sum c_i T(s_i) = T(v) = w$, so any $w \in W$ is indeed a linear combination of elements in $\{T(v_i)\}_{i=1}^{k}$, i.e., $T(S)$ spans W.

Conversely, suppose $T(V) \neq W$. Pick $w \in W \backslash T(V)$. Since V trivially spans V, by assumption $T(V)$ spans W. Therefore, there exist $T(v_1), \dots, T(v_k)$ and coefficients $c_1, \dots, c_k \in F$ such that $w = \sum c_i T(v_i)$. But then by linearity $w = T(\sum c_i v_i)$ so $w \in T(V)$, contradiction.

(3) Let T be isomorphic and let $v_1, \dots, v_n$ be a basis of V. By (a) T maps such basis to a linearly independent subset of W and by (b) such set spans W. Hence T maps bases to bases.

Conversely, if T maps bases to bases, in particular let $v_1, \dots, v_n$ and $w_1, \dots, w_n$ be a corresponding pair of bases. (1) implies T is injective, and for any $w \in W$, writing it as a linear combination $\sum c_i w_i$ and using the linearity of T, we see $w = \sum c_i w_i = \sum c_i T(v_i) = T(\sum c_i v_i) \in T(W)$ so T is surjective. Hence T is bijective and linear. Since V, W are finite dimensional we conclude T is an isomorphism.

□

Problem 2

Let $T : M_n(F) \to M_n(F)$ be the map $T(A) := A - A^T$.

(1) Describe $\ker(T)$ and compute $\dim\ker(T)$.

(2) Describe the image of T and compute its dimension.

(3) Show that if the characteristic of F is not 2, then $\ker(T) \cap \operatorname{im}(T) = 0$.

Proof. (1) $T(A) = 0$ iff $A = A^T$, i.e., iff A is symmetric. A $n \times n$ symmetric matrix is uniquely determined by the $n(n+1)/2$ entries above and on its diagonal so $\dim\ker(T) = n(n+1)/2$.

(2) Note $(A - A^T)^T = A^T - (A^T)^T = A^T = -(A - A^T)$, so (unless in a characteristic 2 field) the diagonal entries must equal to 0, and the (j, i) entry is determined once (i, j) is. That is, it suffices to decide all the entries above the diagonal, making $\dim\operatorname{im}(T) = n(n-1)/2$. If $\operatorname{char}(F) = 2$, however, the diagonal entries need not to be 0, so in this case $\dim\operatorname{im}(T) = n(n+1)/2$.

(3) If $\operatorname{char}(F) \neq 2$ then if $A \in \ker(T) \cap \operatorname{im}(T)$, symmetry and skew symmetry together force $A = 0$. □

Problem 3

Let F be a finite field with q elements.

(1) Show that if V is a d-dimensional vector space over F then $|V| = q^d$.

(2) Prove that

$$|\mathrm{GL}_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1}).$$

(3) Let $\mathrm{SL}_n(F)$ denote the subgroup of $\mathrm{GL}_n(F)$ consisting of all matrices of determinant 1. Determine $|\mathrm{GL}_n(F)|/|\mathrm{SL}_n(F)|$.

Proof. (1) Let $v_1, \ldots, v_d$ be a basis of V. Therefore, any $v \in V$ can be written of form $\sum c_i v_i$ where $c_i \in F$. That is, $|V| \leqslant q^d$. Now suppose that some different linear combinations of v_i result in the same element, namely, for some $c_i, e_i \in F$, $\sum c_i v_i = \sum e_i v_i$. Subtracting gives $\sum (c_i - e_i) v_i = 0$, and by linear independence this forces $c_i = e_i$. Therefore $|V| = q^d$.

(2) In an invertible $n \times n$ matrix, the rows form a linearly independent subset of $\mathbb{R}^n$. For a matrix to be invertible, its first row cannot be identically 0. Therefore there are $q^n - 1$ ways to choose. The second row must be picked such that it is not a multiple of the first row. Among all q^n options, exactly q are multiples of the first row (including $0\cdot$ the first row = the zero row), hence $q^n - q$ options. Repeating this reasoning, we obtain the claim.

(3) Let $A \in \mathrm{SL}_n(F)$. For $0 \neq k \in F$, we define $\varphi_k : \mathrm{SL}_n(F) \to \mathrm{GL}_n(F)$ by $\varphi_k(A) :=$ the matrix such that its first row is k times A's first row, and that its all other rows agree with A's. Note that for a fixed k, φ_k is bijective. Letting exhausting all nonzero$k \in F$, we obtain a partition of $\mathrm{GL}_n(F)$ based on determinants,

with each set having the same cardinality, in particular, $|\mathrm{SL}_n(F)|$. Hence $|\mathrm{GL}_n(F)|/|\mathrm{SL}_n(F)| = q-1$. □

Problem 4

Let A, B be $m \times m$ matrices over a field F.

(1) Show that if A is invertible then AB and BA are similar.

(2) Show by example that this need not be the case if A and B are not invertible.

(3) Prove that $\det(AB) = \det(BA)$.

(4) Prove that AB and BA have the same trace.

(5) Prove that if x is a variable then $\det(xI - AB) = \det(xI - BA)$.

Proof. (1) If A is invertible, then $(A^{-1})^{-1}BAA^{-1} = AB$ so AB and BA are similar.

(2) $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$

(3) Fix A and consider the mapping $B \mapsto \det(AB)$. If we multiply one column of B by $c \in F$, exactly one term in

$$\det(AB) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)(AB)_{1,\sigma(1)}(AB)_{2,\sigma(2)} \cdots (AB)_{n,\sigma(n)}$$

will be multiplied by c. Similarly, an addition done within one column of B will affect precisely one term above. Therefore $B \mapsto \det(AB)$ is multilinear. The mapping is also alternating because swapping row columns results in change of parity of σ. These imply that $B \mapsto \det(AB)$ is an alternating n-linear form on the row space, so $\det(AB) = \lambda \det(B)$ for some b. Letting $B = I$ we see $\lambda = \det(A)$, so $\det(AB) = \det(A)\det(B)$, and the claim follows from the fact that

$$\det(AB) = \det(A)\det(B) = \det(B)\det(A) = \det(BA).$$

(4) By brute force computation,

$$\operatorname{tr}(AB) = \sum_{k=1}^{n}(AB)_{k,k} = \sum_{k=1}^{n}\sum_{j=1}^{n} A_{k,j}B_{j,k} = \sum_{j=1}^{n}\sum_{k=1}^{n} A_{k,j}B_{j,k} = \sum_{j=1}^{n}\sum_{k=1}^{n} B_{k,j}A_{j,k} = \operatorname{tr}(BA).$$

(5) We view matrix determinants as polynomials over F. In particular,

$$\det(B)\det(xI - AB) = \det(xB - BAB) = \det(xI - BA)\det(B).$$

If B is the zero matrix the claim is trivial; otherwise, viewing it as a polynomial of its entries $B_{i,j}$ and x, we may divide it and obtain $\det(xI - AB) = \det(xI - BA)$ as desired.

□

Problem 5

Let $T : V \to V$ be such that $T^2 = T$. Prove every $v \in V$ can be written uniquely as $v_1 + v_2$ where $v_1 \in \operatorname{im}(T)$ and $v_2 \in \ker(T)$.

Proof. Let $v \in V$. From idempotency we have

$$T(v - T(v)) = T(v) - T^2(v) = 0,$$

so $v - T(v) \in \ker(T)$ for all v. This proves the claim, as $v = (v - T(v)) + T(v)$ where $v - T(v) \in \ker T(T)$ and $T(v) \in \operatorname{im}(T)$. □