Mathematics 189-133B, Winter 2003
Vectors, Matrices and Geometry
Written Assignment 5, due in class, March 14, 2003

1. Suppose that A and B are $n \times n$ matrices.

   (a) Show that if $AB = BA$, then $(AB)^2 = A^2B^2$.

   (b) Show that if A and B are invertible and $(AB)^2 = A^2B^2$, then $AB = BA$.

   (c) Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. Show that $(AB)^2 = A^2B^2$, but $AB \neq BA$.

   (d) Find an example where $(AB)^2 = A^2B^2$, $AB \neq BA$ and A is invertible.

   (a) Assume $AB = BA$. $(AB)^2 = (AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = A^2B^2$. We use associativity on both sides, and the commutativity assumption in the middle.

   (b) Suppose that $(AB)^2 = A^2B^2$, that is $ABAB = AABB$. Now suppose also that A^{-1} and B^{-1} exist. Then $A^{-1}(ABAB)B^{-1} = A^{-1}(AABB)B^{-1}$. Associativity (useful, that) gives us $(A^{-1}A)BA(BB^{-1}) = (A^{-1}A)AB(BB^{-1})$, so $IBAI = IABI$ and then $AB = BA$.

   (c) $AB = B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq BA = A$. Note also (by direct calculation) that $A^2 = A$, $B^2 = B$, so $A^2B^2 = B = AB = (AB)^2$.

   (d) How about $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$?

2. (a) Let $V = span\{\vec{v}_1, \ldots, \vec{v}_k\}$ be a subspace of $\mathcal{R}^n$, and suppose that $\{\vec{w}_1, \ldots, \vec{w}_\ell\}$ is an independent subset of V. Show that $\ell \leq k$.

   (b) Use this to show that any two bases for V have the same number of elements.

   (a) The idea of this proof (there are others) is to replace elements of $\{\vec{v}_1, \ldots, \vec{v}_k\}$ by $\vec{w}$'s one by one, until we run out of $\vec{w}$'s, and to show that until this happens we must still have at least one $\vec{v}$ left.

   Write $\vec{w}_1 = a_1\vec{v}_1 + \cdots + a_k\vec{v}_k$; since $\vec{w}_1 \neq \vec{0}$, at least one of the a_j's is not zero; without loss of generality (my favourite mathematical phrase) $a_1 \neq 0$. Then $\vec{v}_1 = \frac{1}{a_1}\vec{w}_1 - \frac{a_2}{a_1}\vec{v}_2 - \cdots - \frac{a_k}{a_1}\vec{v}_k$ and $\vec{v}_1 \in span\{\vec{w}_1, \vec{v}_2, \ldots, \vec{v}_k\}$. If $\ell = 1$, we're finished, since then all we would need to know is that $k \geq 1$. But most likely $\ell > 1$ so we keep going. Anyway, we know that $V = span\{\vec{w}_1, \vec{v}_2, \ldots, \vec{v}_k\}$, so $\vec{w}_2 = b_1\vec{w}_1 + b_2\vec{v}_2 + \cdots + b_k\vec{v}_k$ for some scalars $b_1, \ldots,$ b_k. We must have $b_j \neq 0$ for some $j \geq 2$ since otherwise $\vec{w}_2$ would be a multiple of $\vec{w}_1$, contradicting our assumption that the set of $\vec{w}$'s is independent. (You knew that had to come in somewhere.) WLOG, $b_2 \neq 0$ and then $\vec{v}_2 \in span\{\vec{w}_1, \vec{w}_2, \vec{v}_3, \ldots, \vec{v}_k\}$ which implies that $V = span\{\vec{w}_1, \vec{w}_2, \vec{v}_3, \ldots, \vec{v}_k\}$.

The rest of the proof is properly an induction, although the whole idea is in the last two paragraphs. Here goes: Suppose that we have $m < \ell$ and $V = span\{\vec{w}_1, \ldots, \vec{w}_m, \vec{v}_{m+1}, \ldots, \vec{v}_k\}$. We can find scalars $c_1, \ldots, c_k$ such that $\vec{w}_{m+1} = c_1\vec{w}_1 + \cdots + c_m\vec{w}_m + c_{m+1}\vec{v}_{m+1} + \cdots + c_k\vec{v}_k$. If it were the case that $c_j = 0$ for all $j > m$, we would have to have that $\vec{w}_{m+1} \in span\{\vec{w}_1, \ldots, \vec{w}_m\}$ contrary to our assumption that the set of $\vec{w}$'s is independent. WLOG, $c_{m+1} \neq 0$, so we can solve for $\vec{v}_{m+1}$ in terms of $\vec{w}_1, \ldots, \vec{w}_{m+1}$, $\vec{v}_{m+2}, \ldots, \vec{v}_k$. So if we replace $\vec{v}_{m+1}$ by $\vec{w}_{m+1}$ we still have a spanning set for V.

We keep doing this until we run out of $\vec{w}$'s; we cannot run out of $\vec{v}$'s first. So there are no more $\vec{w}$'s than $\vec{v}$'s; id est, $\ell \leq k$.

(b) Now this is easy. If $\mathcal{B} = \{\vec{v}_1, \ldots, \vec{v}_k\}$ and $\mathcal{C} = \{\vec{w}_1, \ldots, \vec{w}_\ell\}$ are both bases for V, then by the last part, $\ell \leq k$ (using that $\mathcal{B}$ spans V and $\mathcal{C}$ is independent). But since also $\mathcal{C}$ spans V and $\mathcal{B}$ is independent, $k \leq \ell$.