21-241 MATRICES AND LINEAR TRANSFORMATIONS
SUMMER 1 2012
COURSE NOTES
MAY 31

PAUL MCKENNEY

The following theorem is the usual reason why we care about a basis; it represents a nice way of coding a subspace.

Theorem 1. *Let $\mathscr{A} = \{a_1, \dots, a_k\}$ be a basis for some subspace S of $\mathbb{R}^n$; then for any $b \in S$, there is a* unique *sequence of coefficients $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ such that*

$$b = \lambda_1 a_1 + \cdots + \lambda_k a_k$$

Proof. Since $\mathscr{A}$ is a basis for S, $\operatorname{span} \mathscr{A} = S$, and so there is some sequence of coefficients $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ such that

$$b = \lambda_1 a_1 + \cdots + \lambda_k a_k$$

Now if $\mu_1, \dots, \mu_k \in \mathbb{R}$ is another sequence of coefficients such that

$$b = \mu_1 a_1 + \cdots + \mu_k a_k$$

then we have

$$(\lambda_1 - \mu_1)a_1 + \cdots + (\lambda_k - \mu_k)a_k = 0$$

Thus by linear independence of $\mathscr{A}$, $\lambda_i - \mu_i = 0$ for all i, and so $\lambda_i = \mu_i$ for all i. □

We've already (essentially) seen the proofs of the following lemmas, through various other results throughout the course, but they deserve another look. They'll also play an important role in the theorems we prove today.

Lemma 1. *Let R be an $m \times n$ matrix in reduced row-echelon form. If $m < n$, then there is a nonzero vector $s \in \mathbb{R}^n$ such that $Rs = 0$. In other words,*

$$\operatorname{null}(R) \neq \{0\}$$

Proof. The number of variables in the system $Rx = 0$ is exactly n. There can be at most m-many of them that are leading variables (since there can only be one leading variable per row); hence if $m < n$, then there are some variables in this system which are free. Then by choosing any nonzero value for this free variable, and solving for the others, we get a nonzero solution to $Rx = 0$. □

Lemma 2. *Let A and B be $m \times n$ matrices which are row-equivalent. Then* $\operatorname{null}(A) = \operatorname{null}(B)$.

Proof. Suppose A and B are row-equivalent. Then there are elementary matrices $E_1, \ldots, E_k$ such that $B = E_k \cdots E_1 A$. So if $s \in \text{null}(A)$, then

$$Bs = (E_k \cdots E_1 A)s = E_k \cdots E_1(As) = E_k \cdots E_1 0 = 0$$

and so $s \in \text{null}(B)$. This shows $\text{null}(A) \subseteq \text{null}(B)$. Similarly, there are elementary matrices $F_1, \ldots, F_\ell$ such that $A = F_\ell \cdots F_1 B$, and the same argument proves that $\text{null}(B) \subseteq \text{null}(A)$. □

Corollary 1. *If A is an $m \times n$ matrix and $m < n$, then* $\text{null}(A) \neq \{0\}$.

Proof. Let R be the reduced row echelon form of A. Then by Lemma 1, $\text{null}(R) \neq \{0\}$, since R has more columns than rows. Since A and R are row-equivalent, by Lemma 2, $\text{null}(A) = \text{null}(R)$. So we're done. □

Theorem 2. *Let $a_1, \ldots, a_n \in \mathbb{R}^m$ be distinct vectors, and let A be the $m \times n$ matrix whose columns are $a_1, \ldots, a_n$. Then the following are equivalent;*

(i) $\{a_1, \ldots, a_n\}$ *is linearly independent,*
(ii) A *is left-invertible.*

The following are also equivalent (though not equivalent to the above two statements)

(1) $\text{span}\{a_1, \ldots, a_n\} = \mathbb{R}^m$,
(2) A *is right-invertible.*

Proof. I'll just prove (i) is equivalent to (ii). First, suppose $\{a_1, \ldots, a_n\}$ is linearly independent. Note that for all $s \in \mathbb{R}^n$,

$$As = s_1 a_1 + \cdots + s_n a_n$$

and therefore if $As = 0$, by linear independence it must be that $s = 0$; in other words, $\text{null}(A) = \{0\}$. Now let R be the reduced row echelon form of A; then $\text{null}(R) = \text{null}(A) = \{0\}$ by Lemma 2. It follows that R has the following form;

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ & & \vdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Let $L = R^\top$, ie the $n \times m$ matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots & \\ 0 & 0 & \cdots & 1 & \cdots & 0 \end{pmatrix}$$

Then $LR = I_n$. Since $R = EA$ for some matrix E, we get $(LE)A = I_n$, and so A is left-invertible.

Now suppose A is left-invertible, say with left inverse B. If $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ are such that

$$\lambda_1 a_1 + \cdots + \lambda_n a_n = 0$$

then

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = I \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = BA \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = B(\lambda_1 a_1 + \cdots + \lambda_n a_n) = B0 = 0$$

and hence $\lambda_1 = \cdots = \lambda_n = 0$. □

Corollary 2. *Let A be an $m \times n$ matrix. Then A is invertible if and only if its columns make up a basis for $\mathbb{R}^m$.*

Example. Is the following set a basis for $\mathbb{R}^4$?

$$\left\{ \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 6 \end{pmatrix} \right\}$$

Theorem 3. *Let $k \geq 1$ and let S be any subspace of $\mathbb{R}^k$. Then any two bases for S have the same size.*

Proof. Let $\mathscr{A} = \{a_1, \dots, a_n\}$ and $\mathscr{B} = \{b_1, \dots, b_m\}$ be two bases for S. Let A and B be the $k \times n$ and $k \times m$ matrices whose columns are $a_1, \dots, a_n$ and $b_1, \dots, b_m$ respectively. By Theorem 1, we can write b_i uniquely as a linear combination of $a_1, \dots, a_n$;

$$b_i = \lambda_{i1} a_1 + \cdots + \lambda_{in} a_n$$

Let L be the $m \times n$ matrix with entries λ_{ij}. Then the above proves that $B = AL$. Since B is left-invertible, so is L; for if C is a left inverse for B, then $(CA)L = C(AL) = CB = I$. So $\operatorname{null}(L) = \{0\}$. Then by Corollary 1, L can't have more columns than rows, ie, $n \leq m$.

By symmetry (swapping A with B and performing the same argument) we see that $m \leq n$. Then $m = n$. □

Now we can make the following definition.

Definition. If S is a subspace of $\mathbb{R}^n$, then $\dim(S)$, the dimension of S, is the unique size of any basis for S.

And now we can finally prove that all invertible matrices are square!

Corollary 3. *If A is an invertible matrix then A must be square.*

Proof. Suppose A is $m \times n$ and invertible. Then its columns form a basis for $\mathbb{R}^m$, by Theorem 2. There are n of them; there are also m many standard basis vectors for $\mathbb{R}^m$. Therefore $m = n$ by Theorem 3. $\square$