INVERTIBILITY OF AN OPERATOR; KERNEL

1. Recap

Last class period we covered a lot of ground. We began by talking a bit about the geometry of vectors. In particular we saw how one can draw the sum of two vectors or a scaled vector. We also discussed orthogonality and the dot product, in particular saying that two nonzero vectors are orthogonal (i.e., perpendicular) if and only if their dot product is zero. We then discussed the span of a collection of vectors, which also introduced us to linear combinations and the standard basis.

After discussing some algebraic properties of the dot product and matrix/vector multiplication (in particular, we saw that these operations are 'linear' in an appropriate sense) and recalling some definitions from the theory of functions (domain, codomain, range, etc.) we discussed linear operators: those functions $T : \mathbb{R}^m \to \mathbb{R}^n$ which are given by multiplication on the left by a matrix A. Today we'll talk about invertibility.

2. Invertibility

2.1. What is invertibility?

Definition 2.1. A function $f : D \to C$ is invertible if for every c in C there exists a unique d in D so that $f(d) = c$.

This definition can be restated as follows: a function is invertible if and only if every element of the codomain is hit by exactly one element in the domain. A function whose image is the entire codomain is called an *onto* function, and functions which map distinct inputs to distinct outputs are called *one-to-one*. Our definition just says that a function is invertible iff it is one-to-one (every element in the codomain gets hit by at most one element in the domain) and onto (every element in the codomain gets hit by at least one element).

Example. The first function depicted in Figure 1 is invertible because every element in C is hit by exactly one element in D. The second function in Figure 1 fails to be invertible because there is an element in the codomain that gets hit by more than one input (f_2 fails to be one-to-one in this case). The third function in Figure 1 fails to be invertible because there is an element in the codomain that does not get hit by any input (f_3 fails to be onto in this case).

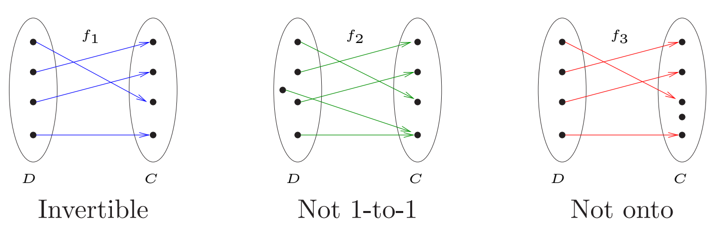

Figure 1.

Example. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ fails to be invertible for two reasons. First, there are elements in the codomain that are not hit by the function; in particular, no negative number is the square of a real number, and so (for example) there does not exist a solution to the equation $x^2 = -1$. This means f fails to be onto. Second, there are elements in the codomain that are hit by more than one element, e.g. $f(1) = f(-1) = 1$. This means f fails to be one-to-one.

Definition 2.2. If a function $f : D \to C$ is invertible, then the function $f^{-1} : C \to D$ defined by $f^{-1}(y) = x$, where x is the unique solution to $f(x) = y$, is called the inverse of f.

2.2. **When is a linear operator invertible?** Since we're not in a calculus class we won't be dealing with functions like $f(x) = x^2$ too much, instead favoring linear operators. So we ask: what linear operators are invertible? Further, if an operator is invertible, how do I calculate its inverse?

Since we know linear operators are represented by matrices, we will answer this question by examining characteristics of matrices.

Theorem 2.1. *A linear operator T associated to an $n \times m$ matrix A is not invertible if $n \neq m$. When $n = m$, then T is invertible if and only if rank$(A) = n$.*

Proof. We'll split this proof up into cases. In the first case, suppose $n < m$. Then we have $\text{rank}(A) \leq n < m$, so that $\text{rank}(A) < m$. One of our old theorems on rank tells us that any system whose coefficient matrix is A, say $\left(A|\overrightarrow{b}\right)$, will have either 0 solutions or infinitely many solutions. Hence the equation $T\overrightarrow{x} = \overrightarrow{b}$ will have either 0 or infinitely many solutions. For T to be invertible, though, an equation of this sort must have a unique solution. We conclude that T cannot be invertible if $n < m$. (Not convinced? Here's a specific example. We know that $T\overrightarrow{x} = \overrightarrow{0}$ has at least one solution—the zero vector—and hence our reasonsing says it has infinitely many solutions. This contradicts the definition of invertibility—T isn't one-to-one—so T can't be invertible.)

The case $m < n$ will be put off as an IOU, but here's the idea: when m, n we are mapping a 'small' space into a 'big' space, and so we shouldn't expect that the image covers the entire codomain. In fact, we could find a vector which is not hit by a map $T : \mathbb{R}^m \to \mathbb{R}^n$ with a little elbow grease, but I prefer to put this off for now and come back to it when we talk about dimension. In any event, a linear operator $T : \mathbb{R}^m \to \mathbb{R}^n$ will fail to be onto when $m < n$, and so T cannot be invertible.

The previous two cases show that if T is associated to a non-square matrix, then T cannot be invertible. Now we move on to the square case, $n = m$. In this case, recall we have shown before that a system S has a unique solution if and only if $\text{rank}(S) = n$. When $\text{rank}(A) = n$, any choice of a vector $\overrightarrow{b} \in \mathbb{R}^n$ gives rise to a system S, a system represented by the augmented matrix $\left(A|\overrightarrow{b}\right)$. Such a system has a unique solution (since $\text{rank}(S) = \text{rank}(A) = n$), and so we know that for any element $\overrightarrow{b}$ in the codomain there exists a unique solution to

$$A\overrightarrow{x} = \overrightarrow{b}.$$

But this means there is a unique solution to $T\overrightarrow{x} = \overrightarrow{b}$, and so T is invertible. If $\text{rank}(A) \neq n$ then there is choice of $\overrightarrow{b}$ in the codomain so that the system S represented by $\left(A|\overrightarrow{b}\right)$ does not have a unique solution (since $\text{rank}(S) = \text{rank}(A) \neq n$). Hence the equation $T\overrightarrow{x} = \overrightarrow{b}$ does not have a unique solution, and T isn't invertible. □

This result has an immediate consequence.

Corollary 2.2. *Let A be an $n \times n$ matrix. Then if the operator T associated to A is invertible, for any choice $\overrightarrow{b} \in \mathbb{R}^n$ there is a unique solution to $A\overrightarrow{x} = \overrightarrow{b}$. If the operator T is not invertible, then for any choice of vector $\overrightarrow{b} \in \mathbb{R}^n$, either there are no solutions to $A\overrightarrow{x} = \overrightarrow{b}$ or there are infinitely many.*

Before I write the proof, notice that the content of this statement is that in the square case one can check whether an operator is invertible by checking how many solutions $A\overrightarrow{x} = \overrightarrow{b}$ has *for any vector* $\overrightarrow{b} \in \mathbb{R}^n$ *you like.* In the non-square case this isn't so: there can be vectors for which $A\overrightarrow{x} = \overrightarrow{b}$ has a unique solution, but of course the operator T corresponding to A isn't invertible (since A isn't square).

Proof. We already know that if T is invertible, any choice of $\overrightarrow{b} \in \mathbb{R}^n$ gives rise to a unique solution $A\overrightarrow{x} = \overrightarrow{b}$; this is just the definition of invertibility.

So we need to prove the second statement. For this, since T is not invertible we have $\text{rank}(A) < n$. But since $n = m$ (where m is the number of columns, as per usual) we have $\text{rank}(A) < m$, and so an old result on rank tells us that $A\overrightarrow{x} = \overrightarrow{b}$ has either infinitely many solutions or no solutions at all.

For the final statement, notice that $T\overrightarrow{x} = \overrightarrow{0}$ already has one solution, the choice $\overrightarrow{x} = \overrightarrow{0}$. Since it cannot have a unique solution (since T isn't invertible), it must have infinitely many solutions. □

Let's look at the particular equation $T\overrightarrow{x} = \overrightarrow{0}$ and apply the previous corollary.

Corollary 2.3. *For a linear operator $T : \mathbb{R}^n \to \mathbb{R}^n$, the set $\{x \in \mathbb{R}^n : T\overrightarrow{x} = \overrightarrow{0}\}$*

- *has one element if T is invertible, and*
- *has infinitely many element if T is not invertible.*

Proof. The first statement is clear. For the second, notice that $T\overrightarrow{x} = \overrightarrow{0}$ has at least one solution ($\overrightarrow{x} = \overrightarrow{0}$), and hence the previous corollary tells us it has infinitely many solutions. □

2.3. **How do I compute the inverse of a linear operator?** Now that we know when an linear operator T is invertible, we ask how we can compute the inverse function T^{-1}. Happily, computing the inverse of a linear operator only involves row reduction of a particular matrix.

Theorem 2.4. *Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be a linear operator, and let A be the associated matrix. Then*

- *if* `rref`$((A|I_n)) = (I_n|B)$ *for some $n \times n$ matrix B, then T^{-1} is the operator defined by B; and*
- *if* `rref`$((A|I_n))$ *does not take the form $(I_n|B)$, then T is not invertible.*

Remark. We usually write the matrix B from the above theorem as A^{-1}. Once we talk about matrix multiplication we'll see that A^{-1} is the multiplicative inverse of A.

To see some examples of computing inverses, check out the Mathematica computations we did in class.

3. The kernel of a matrix

We have already seen the set $\{\overrightarrow{x} \in \mathbb{R}^m | A\overrightarrow{x} = \overrightarrow{0}\}$ come up in some of our theorems. This set is particular important for understanding the linear operator associated to T, and so it has a special name.

Definition 3.1. Let A be any matrix (i.e., not necessarily square). Then the kernel of A, written $\ker(A)$ is defined as

$$\ker(A) := \{\overrightarrow{x} \in \mathbb{R}^m | A\overrightarrow{x} = \overrightarrow{0}\}.$$

Theorem 3.1. *A corresponds to an invertible linear operator if and only if* $\ker(A) = \{\overrightarrow{0}\}$.

Proof. Notice that $\overrightarrow{0} \in \ker(A)$ automatically. Now we said that when A is invertible, $\ker(A)$ has one element. Hence when A is invertible, $\ker(A) = \{\overrightarrow{0}\}$. When A isn't invertible we said that $\ker(A)$ has infinitely many elements, and so $\ker(A) \neq \{\overrightarrow{0}\}$. ☐

Before ending class I made one last observation.

Theorem 3.2. *Let A be an $n \times m$ matrix, let $\overrightarrow{v}$ and $\overrightarrow{w}$ be elements of* $\ker(A)$*, and let k be a scalar. Then*

- $\overrightarrow{v} + \overrightarrow{w}$ *is an element of* $\ker(A)$*;*
- $k\overrightarrow{v}$ *is an element of* $\ker(A)$*; and*
- $\overrightarrow{0}$ *is an element of* $\ker(A)$*.*

Proof. The last statement has already been observed. For the first statement, notice that $A(\overrightarrow{v} + \overrightarrow{w}) = A\overrightarrow{v} + A\overrightarrow{w} = \overrightarrow{0} + \overrightarrow{0} = \overrightarrow{0}$, and so $\overrightarrow{v} + \overrightarrow{w}$ is in the kernel of A. The second statement is proved similarly. ☐