Math 260
Group of Transformations

David L. Meretzky

November 11th, 2018

In these notes we will investigate certain collections of linear operators.

Definitions

Let V be a finite dimensional vectorspace. Let $\mathscr{L}(V)$ be the linear operators on V.

Definition 1. A non-empty subset G of $\mathscr{L}(V)$ is called a group of linear operators if the following two properties hold:

1. G is closed under inverses, that is, if $T \in G$, then $T^{-1} \in G$.
2. G is closed under composition, that is, if S, and T are in G then $S \circ T \in G$.

For short we call G a group.

Proposition 1. Every group of linear operators contains the identity transformation.

Proof. Since G is non-empty, there exists a $T \in G$ and since G is closed under inverses, $T^{-1} \in G$. Then because G is closed under composition $T \circ T^{-1} \in G$. Since $I = T \circ T^{-1}$, $I \in G$. □

Example 1. The entire collection of linear operators $\mathscr{L}(V)$ is not a group because it is not closed under inverses. The 0 transformation has no inverse. However, the collection of all *invertable* linear operators denoted $GL(V)$ is a group. It is called the general linear group of the vectorspace V.

Since $GL(V)$ is the collection of all invertable operators, if one can show that a specific operator is invertable then it must be in $GL(V)$.

Verification of closure under inverses: if $T \in GL(V)$, then T is invertable. So T^{-1} exists. Moreover, T^{-1} itself is invertable with inverse T and is therefore in $GL(V)$. Verification of closure under composition. Suppose S and T are invertable, and therefore in $GL(V)$. We must show that $S \circ T$ is invertable and therefore in $GL(V)$. Because S and T are invertable, S^{-1} and T^{-1} exist. Their composition $T^{-1} \circ S^{-1}$ is the inverse of $S \circ T$. Thus $S \circ T$ is invertable and is thus in $GL(V)$. Thus $GL(V)$ is a group.

Even if V is finite dimensional $GL(V)$ is an infinite collection of operators. We will now examine some groups of transformations which are finite.

Definition 2. Let $T \in \mathscr{L}(V)$ denote the n-fold composition of T with itself as T^n. For instance, the two fold composition, $T \circ T$ is denoted T^2. Let T^{-n} denotes the n-fold composition of T^{-1}.

Definition 3. Let $T \in \mathscr{L}(V)$. We call T idempotent if there exists a positive integer $n > 0$ such that $T^n = I$. We call T nilpotent if there exists a positive integer $n > 0$ such that $T^n = 0$. Recall I is the identity operator and 0 is the zero operator.

Proposition 2. A group cannot contain a nilpotent operator.

Proof. Suppose $G \subset \mathscr{L}(V)$ is a group of transformations with a nilpotent element $T \in G$. Since G is closed under composition, $T \circ T \in G$. Continuing in this manner $T^n \in G$ for all positive integers n. However, since T is nilpotent there exists some integer n such that $T^n = 0$. So therefore $0 \in G$. Since 0 is not invertable this is impossible. Therefore G cannot have a nilpotent element. □

Cyclic Groups

A group of transformations may however contain idempotent operators. In fact, the simplest classes of groups are just collections of idempotent operators.

Example 2. Let V be a vectorspace. Let $T \in \mathscr{L}(V)$ such that $T \neq I$ and $T^2 = I$. Let $C_2 = \{I, T\}$. We show that C_2 is a group. Note: C_2 could just as well be written $C_2 = \{T, T^2\}$.

First we must verify that both of the elements of C_2 have inverses. The inverse of I is itself. So there is nothing to check for I. The inverse of T is also itself since $T \circ T = I$. So C_2 is closed under inverses.

Next we must check that C_2 is closed under composition. Since there are so few elements of C_2 there are only a few ways we can compose elements. In particular we can form the following 4 composites.

1. $I \circ I = I$
2. $I \circ T = T$
3. $T \circ I = T$
4. $T \circ T = I$

So C_2 is closed under composition since I and T are the possible results of the compositions and are both in C_2.

Since C_2 is closed under composition and inverses, it is a group.

Exercise 1. Show $C_n = \{I,\ T,\ T^2,\ ...T^{n-1}\}$ is a group where $T^n = I$ and $T \neq I$. Groups of this form are called the cyclic groups.

Proposition 3. If $V = \mathbf{F}$ then there is only one $T : \mathbf{F} \to \mathbf{F}$ such that $T^2 = I$ and $T \neq I$.

In the case $V = \mathbf{F}$, the requirement $T \neq I$ means that there exists at least one vector $v \in \mathbf{F}$, such that $Tv \neq v$. However, the requirement $T^2 = I$ means that $T^2 v = v$ for all $v \in \mathbf{F}$. Since every linear operator on $\mathbf{F}$ is of the form multiplication by a scalar, these two requirements become $Tv = \lambda v \neq v$ and $T^2 v = \lambda^2 v = v$ for some $\lambda \in \mathbf{F}$. In either the real or complex case, the only lambda that fits this requirement is -1.

Exercise 2. Let $V = \mathbf{R}^2$. Let $B = v_1, v_2$ be a basis for V. Let $T \in \mathscr{L}(V)$ be defined to be the unique linear transformation which takes $Tv_1 = v_2$ and $Tv_2 = v_1$. Show that $T \neq I$ and $T^2 = I$. Therefore $C_2 = \{I, T\}$. Furthermore find the matrices $\{[I]_B^B, [T]_B^B\}$ with respect to this basis. Note: T is unique because of 3.5 of the text.

Definition 4. The matrix representation of a group $G = \{I, T_1, T_2, ...\}$ of linear transformations of a vector space V with respect to a pair of bases B_1 and B_2 is defined to be the collection of matricies $\{[I]_{B_2}^{B_1}, [T_1]_{B_2}^{B_1}, [T_2]_{B_2}^{B_1}, ...\}$. Denote the representation $[G]_{B_2}^{B_1}$. The dimension of V is said to be the dimension of the representation.

Exercise 3. The result of the prevous exercise generalizes to the group C_n. Let $V = \mathbf{R}^n$. Let $B = v_1, ..., v_n$ be a basis of V. Let $T \in \mathscr{L}(V)$ be the unique linear transformation such that $Tv_1 = v_2$, $Tv_2 = v_3$, and so on until $Tv_n = v_1$. Find $[C_n]_B^B$.

We have already described all representations of the group of linear operators C_2 of a vector space of dimension 1 (see exercise 2) with field $\mathbf{F}$. This follows from the fact that there is only one square root of 1 which is not equal to 1, that is, $-1^2 = 1$.

Theorem 1. Let V be a finite dimensional vectorspace. Let C_2 be the collection of linear operators $\{I, T\}$ on V such that $T \neq I$ and $T^2 = I$. Then there is always a way to express V as a direct sum of subspaces $V = U_1 \oplus U_2 \oplus ... \oplus U_m$ such that C_2 is invariant on each subspace. Moreover, if our vector space is over the field $\mathbf{F} = \mathbf{C}$ then each subspace is of dimension at most 1. If our vector space is over the field $\mathbf{F} = \mathbf{R}$ then each subspace is of dimension at most 2.

This theorem is stated without proof. Instead we look at some examples which will instruct us on how to prove it in the case where $\mathbf{F}$ is either $\mathbf{R}$ or $\mathbf{C}$.

In the case $V = \mathbf{F}$. As an operator, T must send V to itself, and moreover V is of dimension 1. So the decomposition in the theorem is trivial, $V = V$.

Proposition 4. Let $V = \mathbf{R}^2$. Then there are two possible decompositions of

V as a direct sum of invariant subspaces: $V = V$, the trivial decomposition, or $V = U_1 \oplus U_2$ where U_1 and U_2 are each of dimension 1. The trivial decomposition is allowable because V is of dimension 2.

Proof. The requirement $T \neq I$ means that there exists at least one vector $v \in \mathbf{R}^2$, such that $Tv \neq v$. There are now two possibilities, v is either an eigenvector of T or it is not. If it is not an eigenvector then we will obtain the trivial decomposition. If it is an eigenvector then we will have a decomposition $V = U_1 \oplus U_2$ where U_1 and U_2 are each of dimension 1.

Suppose that v is an eigenvector for T. In this case the eigenvalue must be equal to -1 by the same arguement as proposition 3, that is $Tv = \lambda v \neq v$, and $T^2 v = \lambda^2 v = v$. Thus let $U_1 = span(v)$. Since v is an eigenvector, U_1 is an invariant subspace of dimension 1. By the direct sum decomposition theorem (2.34), there exists a subspace U_2 such that $V = U_1 \oplus U_2$. By examining the dimensions of the spaces, U_2 must be dimension 1, thus a basis for it is a list of a single vector u. I leave it to you to show that T is invariant on U_2, equivalently that u is an eigenvalue of T with eigenvector 1 or -1.[1] T can either act as the identity operator on U_2 or also by multiplication by -1:

For instance $T_1(v, u) = (-v, u)$ and $T_2(v, u) = (-v, -u)$ are both options for our transformation T. With respect to the basis $B = v, u$ we have

$$[T_1]_B^B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad [T_2]_B^B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

The other option for a decomposition of V comes from the possiblity that v is not an eigenvector. Then $Tv \neq \lambda v$ for any choice of λ. This means that v and Tv are linearly independent. Let $u = Tv$. Thus v, u form a basis for the dimension 2 space. This gives us the trivial decomposition. T is not invariant on any subspaces of V other than $\{0\}$ and all of V.

In this case, $T(v, u) = (u, v)$ and representing T with respect to the basis $B' = v, u$ we have

$$[T]_{B'}^{B'} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2}$$

□

Next we will prove that in the case that V is a complex vector space, that is where $\mathbf{F} = \mathbf{C}$, then for any $T \in \mathscr{L}(V)$, T always has an eigenvalue. It will follow from this result that V can always be decomposed as a direct sum of 1-dimensional invariant subspaces of T. Only in the case $\mathbf{F} = \mathbf{R}$ can we have invariant subspaces of dimension 2 which cannot be further decomposed into subspaces of dimension 1 i.e. the case where T does not have an eigenvalue.

[1] Begin by supposing u is not an eigenvector of T but v is an eigenvector. Then use the arguement in the second half of the proof to show that v cannot be an eigenvector. Use a similar arguement to proposition 3 to show that the eigenvalues associated to u must be 1 or -1

Proposition 5. Let V be a finite dimensional vectorspace over the field $\mathbf{F} = \mathbf{C}$. Then for any linear operator $T \in \mathscr{L}(V)$, (note T does not have to be in C_2), T has an eigenvector.[2]

Proof. Let n be the dimension of V. Suppose we take any non-zero vector $v \in V$ and by applying T, obtain the list $v, Tv, T^2v, ...T^nv$. This list has $n+1$ vectors. It cannot be linearly independent because no list of length $n+1$ is linearly independent in V. Thus there exist scalars $a_0, ..., a_n \in \mathbf{C}$ not all zero such that

$$a_0v + a_1Tv + ... + a_nT^nv = 0$$

It is a fact that polynomials with coefficients in $\mathbf{C}$ factor completely in $\mathbf{C}$. That is, there exist n complex numbers $b_1, ..., b_n$ such that

$$a_0v + a_1Tv + ... + a_nT^nv = (T - b_1I)(T - b_2I)...(T - b_nI)v = 0$$

If $(T - b_nI)v = 0$ then $v \in ker(T - b_nI)$ and v is an eigenvector of T with eigenvalue b_n. Otherwise let $(T - b_nI)v = v_1 \neq 0$. Then check if $(T - b_{n-1}I)v_1 = 0$ if so, $v_1 \in ker(T - b_{n-1}I)$ and v_1 is an eigenvector of T with eigenvalue b_{n-1}, if not proceed with $(T - b_{n-1}I)v_1 = v_2 \neq 0$. Continuing in this manner we have eventually in the worst case $(T - b_1I)v_n = 0$. Thus v_n is an eigenvalue and b_1 is the associated eigenvector. □

We will now prove theorem 1 for the case $\mathbf{F} = \mathbf{C}$

Proof. Since $T \in C_2$ is an operator on a complex vector space. By the prevous theorem it has an eigenvalue and eigenvector. Let λ_1 be an eigenvalue associated to an eigenvector v_1. Then let $U_1 = span(v_1)$. Since v_1 is an eigenvector T is invariant on U_1. By the direct sum decomposition theorem, $V = U_1 \oplus W$. Again, T is invariant on W because if for any $w \in W$, $Tw \in U_1 \oplus W$, $Tw = u' + w'$. Then $T^2w = w$ implies that $Tw = w' \in W$. Because if $u' \neq 0$, then T is not invariant on U_1 as applying T to u' would leave it inside of U_1. Thus T is an operator on a complex vectorspace W. Thus it has an eigenvalue λ_2. Repeating the arguement we can draw out another 1-dimensional invariant subspace U_2 such that $V = U_1 \oplus U_2 \oplus W'$. Continuing in this fashion we obtain the required decomposition once the dimension of the completion $W^{(n)}$ dwindles to 1. □

Exercise 4. Combine the proof of the complex case of theorem 1 with the proof of proposition 4 to prove theorem 1 for the case $\mathbf{F} = \mathbf{R}$.

Exercise 5. Let $C_2 \subset \mathscr{L}(R)^5$. Define $T \in C_2$ to be $T(x, y, z, w, u) = (z, -y, x, -u, -w)$. Show that this indeed defines an instance of C_2. Furthermore, find the decomposition guaranteed by theorem 1 it will be of the form $R^5 = U_1 \oplus ... \oplus U_n$. Hint: $n < 5$. Then take a basis B_i for each U_i and adjoin these basis to get a basis $B = B_1, ..., B_n$ for R^5. Write out $[T]_B^B$.

[2]This theorem does not hold for $\mathbf{F} = \mathbf{R}$.