

# 1 Groups as Tools

10/3:

1. There are two **riffle shuffles** of a deck of 52 cards obtained as follows: Divide the deck into the top 26 and bottom 26 cards. Then interweave the two decks card by card; there are two different shuffles depending on whether the top card from the top deck ends up on top, or the top card from the bottom deck ends up on top. If we denote the shuffles by  $A$  and  $B$ , respectively, then we saw in class that  $A^8 = 1$  and  $B^{52} = 1$ . Determine whether every permutation of 52 cards can be obtained by some combination of riffle shuffles.
2. **The Orthogonal Group.** For two vectors  $\mathbf{v}$  and  $\mathbf{w}$  in  $\mathbb{R}^n$ , let  $\langle \mathbf{v}, \mathbf{w} \rangle$  denote the usual dot product of  $\mathbf{v}$  and  $\mathbf{w}$ , so, if  $\mathbf{v} = (v_i)$  and  $\mathbf{w} = (w_i)$ , then  $\langle \mathbf{v}, \mathbf{w} \rangle = \sum v_i w_i$ . If  $M = [a_{ij}]$  is a matrix with coefficients in  $\mathbb{R}$ , let  $M^T$  denote the transpose of  $M$ , which is the matrix  $[a_{ji}]$ .

- (a) Let  $O(n) \subset M_n(\mathbb{R})$  denote the set of matrices  $M$  such that  $MM^T = I$ . Prove that  $O(n)$  is a group. (Hint: Show that  $(AB)^T = B^T A^T$ .)
- (b) Prove that every element in  $O(n)$  has determinant 1 or  $-1$ . Let  $SO(n) \subset O(n)$  denote the matrices  $M \in O(n)$  such that  $\det(M) = 1$ . Prove that  $SO(n)$  is a group.
- (c) Show that any element  $M \in SO(2)$  is of the form

$$M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

where  $a, b \in \mathbb{R}$  satisfy  $a^2 + b^2 = 1$ . Prove that for such  $a$  and  $b$ , one can find a unique  $\theta \in [0, 2\pi)$  such that  $a = \cos(\theta)$  and  $b = \sin(\theta)$ , and that  $M$  is a rotation by  $\theta$  about the origin.

- (d) Show that any  $M \in O(2) \setminus SO(2)$  has the form

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -b & a \\ a & b \end{pmatrix}$$

Prove that these elements also have the following properties.

- i.  $M^2$  is the identity.
- ii.  $M$  is a reflection through some line that passes through the origin  $(0, 0)$ .
- iii. If  $M, N \in O(2) \setminus SO(2)$ , then  $MN \in SO(2)$  is a rotation.
- (e) Let  $\mathbf{u}$  be any non-zero vector in  $\mathbb{R}^3$  of length one, so  $\|\mathbf{u}\|^2 = \langle \mathbf{u}, \mathbf{u} \rangle = 1$ . The vectors  $\mathbf{v}$  with  $\langle \mathbf{u}, \mathbf{v} \rangle = 0$  live inside the plane orthogonal to  $\mathbf{u}$ . Show that if  $\mathbf{u}_1 = \mathbf{u}$ , then there exist vectors  $\mathbf{u}_i \in \mathbb{R}^3$  ( $i = 1, 2, 3$ ) which are orthonormal and mutually orthogonal, that is,  $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$  for  $i \neq j$  and  $\|\mathbf{u}_i\|^2 = \langle \mathbf{u}_i, \mathbf{u}_i \rangle = 1$ . Suppose that  $M \in SO(3)$  is a matrix such that  $M\mathbf{u} = \mathbf{u}$ . Prove that  $M\mathbf{u}_1 = \mathbf{u}_1$ ,  $M\mathbf{u}_2 = a\mathbf{u}_2 + b\mathbf{u}_3$ , and  $M\mathbf{u}_3 = -b\mathbf{u}_2 + a\mathbf{u}_3$  for some  $a, b$  with  $a^2 + b^2 = 1$ , that  $a = \cos(\theta)$  and  $b = \sin(\theta)$  for a unique  $\theta \in [0, 2\pi)$ , and deduce that  $M$  is a rotation about the line  $\mathbf{u}$  by angle  $\theta$ .
- (f) **Triviality:** Let  $\mathbf{v}_1, \mathbf{v}_2$  be any two linearly independent vectors in  $\mathbb{R}^3$ . Prove that if  $g \in SO(3)$  fixes  $\mathbf{v}_1, \mathbf{v}_2$ , then it is the identity. (Hint: Let  $\mathbf{u} = \mathbf{v}_1/|\mathbf{v}_1|$  and use part (e).)
- (g) **Equality:** Let  $\mathbf{v}_1, \mathbf{v}_2$  be any two linearly independent vectors in  $\mathbb{R}^3$ . Prove that if  $g \in SO(3)$  and  $h \in SO(3)$  satisfy  $g(\mathbf{v}_1) = h(\mathbf{v}_1)$  and  $g(\mathbf{v}_2) = h(\mathbf{v}_2)$ , then  $g = h$ .
- (h) Prove that any matrix  $M$  has the same eigenvalues as the transpose matrix  $M^T$ . (Hint: Show that  $M$  and  $M^T$  have the same characteristic polynomial.) Prove that if  $M$  is invertible, then the matrix  $M^{-1}$  has eigenvalues which are the inverses of the eigenvalues of  $M$ .
- (i) Deduce that if  $M \in SO(3)$ , then  $M^{-1} = M^T$ , and then use part (h) to deduce that 1 is an eigenvalue of  $M$ .
- (j) Deduce that every  $M \in SO(3)$  is a rotation about some line  $\mathbf{u}$  passing through the origin. Deduce that the composition of a rotation in  $\mathbb{R}^3$  about some line  $\mathbf{u}$  passing through the origin with a rotation about any second line  $\mathbf{v}$  also passing through the origin is also a rotation about some third line  $\mathbf{w}$  passing through the origin. Note that  $\mathbf{u}, \mathbf{v}, \mathbf{w}$  need not be distinct.