1.3 Matrix-Matrix Multiplication

We recall, from our previous notebook, the basic transformations

$$\textbf{dilations}: \ A(\alpha) = \begin{bmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{bmatrix} \qquad \textbf{shears}: \ N(\sigma) = \begin{bmatrix} 1 & \sigma \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad \textbf{rotations}: \ K(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \tag{1}$$

and ask what happens if we follow a dilation with a shear or rotation, or *vice versa.* For example, now that we understand matrix-vector multiplication we can simply multiply the vector $N(\sigma)x$ by $A(\alpha)$;

$$A(\alpha)N(\sigma)x = \begin{bmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{bmatrix} \begin{bmatrix} 1 & \sigma \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{bmatrix} \begin{bmatrix} x[0] + \sigma x[1] \\ x[1] \end{bmatrix} = \begin{bmatrix} \alpha(x[0] + \sigma x[1]) \\ x[1]/\alpha \end{bmatrix} = \begin{bmatrix} \alpha & \alpha\sigma \\ 0 & 1/\alpha \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \end{bmatrix}$$

from which we deduce that

$$A(\alpha)N(\sigma) = \begin{bmatrix} \alpha & \alpha\sigma \\ 0 & 1/\alpha \end{bmatrix} \tag{3}$$

Similarily, if we reverse the order of our composition

$$N(\sigma)A(\alpha)x = \begin{bmatrix} 1 & \sigma \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \end{bmatrix} = \begin{bmatrix} 1 & \sigma \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha x[0] \\ x[1]/\alpha \end{bmatrix} = \begin{bmatrix} \alpha x[0] + \sigma x[1]/\alpha \\ x[1]/\alpha \end{bmatrix} = \begin{bmatrix} \alpha & \sigma/\alpha \\ 0 & 1/\alpha \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \end{bmatrix} \tag{4}$$

from which we deduce that

$$N(\sigma)A(\alpha) = \begin{bmatrix} \alpha & \sigma/\alpha \\ 0 & 1/\alpha \end{bmatrix} \tag{5}$$

and note that multiplication is **not commutative**, i.e., $A(\alpha)N(\sigma) \neq N(\sigma)A(\alpha)$. These two calculations illustrate the basic rule of **matrix-multiplication**, if A and B are 2-by-2 then their product, C, is the 2-by-2 collection of inner products of the rows of A and columns of B;

$$C[i,j] = A[i,0]B[0,j] + A[i,1]B[1,j] \tag{6}$$

where i and j are each either 0 or 1. For example,

$$\begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ 8 & 7 \end{bmatrix} = \begin{bmatrix} 3 \cdot 5 + 1 \cdot 8 & 3 \cdot 6 + 1 \cdot 7 \\ 4 \cdot 5 + 2 \cdot 8 & 4 \cdot 6 + 2 \cdot 7 \end{bmatrix} = \begin{bmatrix} 23 & 25 \\ 36 & 38 \end{bmatrix} \tag{7}$$

Exercise 1 Show that for each postive integer n,

$$A(\alpha)^n = A(\alpha^n), \qquad N(\sigma)^n = N(n\sigma), \qquad K(\theta)^n = K(n\theta). \tag{8}$$

These are clearly true when $n = 1$. Try the $n = 2$ case as a warm-up to the demonstration, required by the Principle of Mathematical Induction, that their truth at power n implies their truth at power $n + 1$.

Exercise 2 As rotation by θ followed by rotation by $-\theta$ should get you back to where you started it follows that $K(-\theta)K(\theta)$ should be an especially simple matrix. Please confirm that

$$K(-\theta)K(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{9}$$

We call this end result the **identity matrix** and denote it I.

Exercise 3 Please confirm that

$$N(\sigma)N(-\sigma) = I \qquad \text{and} \qquad A(\alpha)A(1/\alpha) = I \tag{10}$$

and **explain** these results in geometric terms. We naturally call $N(-\sigma)$ the **inverse** of $N(\sigma)$ and $A(1/\alpha)$ the **inverse** of $A(\alpha)$.

Exercise 4 Please also show that

$$A(\alpha)A(\beta) = A(\alpha\beta), \qquad N(\sigma)N(\tau) = N(\sigma + \tau) \qquad \text{and} \qquad K(\theta)K(\phi) = K(\theta + \phi) \tag{11}$$

and **explain** these results in geometric terms.

Exercise 5 Let us now show that **every** matrix that preserves area and orientation can be expressed as a **unique** product of a dilation, shear and rotation. Beginning with

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad ad - bc = 1.$$

Let's first dispense with two special cases. Show that if $c = 0$ then $ad = 1$ so $a \neq 0$ and $M = N(ab)A(a)$.

Next, show that if $d = 0$ then $bc = -1$ so $b \neq 0$ and $M = N(-ab)A(b)K(\pi/2)$.

We may now assume that $cd \neq 0$. Find the $\alpha > 0$ and θ that allow you to achieve the bottom row of M via

$$\begin{bmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{bmatrix} \begin{bmatrix} * & * \\ \sin(\theta) & \cos(\theta) \end{bmatrix} = \begin{bmatrix} * & * \\ c & d \end{bmatrix}$$

Next find the σ that allows you to achieve the top row of M without disturbing its bottom row,

$$\begin{bmatrix} 1 & \sigma \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{bmatrix} \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

This last step appears to expect one parameter, σ, to generate both a and b. You will reconcile this with $ad - bc = 1$.

The matrices that preserve area but reverse orientation are commonly refered to as reflections.

Exercise 6 Consider the matrix

$$H = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}. \tag{12}$$

Experiment with this H in your widget above and explain why it is called a **reflection.** Across which line does it reflect? Argue, on strictly geometric grounds, why $H^2 = I$. To "see" this reflection please apply it to the lizard of our previous notebook.

We set the stage for reflections about arbitrary lines in Figure 1 below.

In [1]:

```
# set the context for reflection↔
```

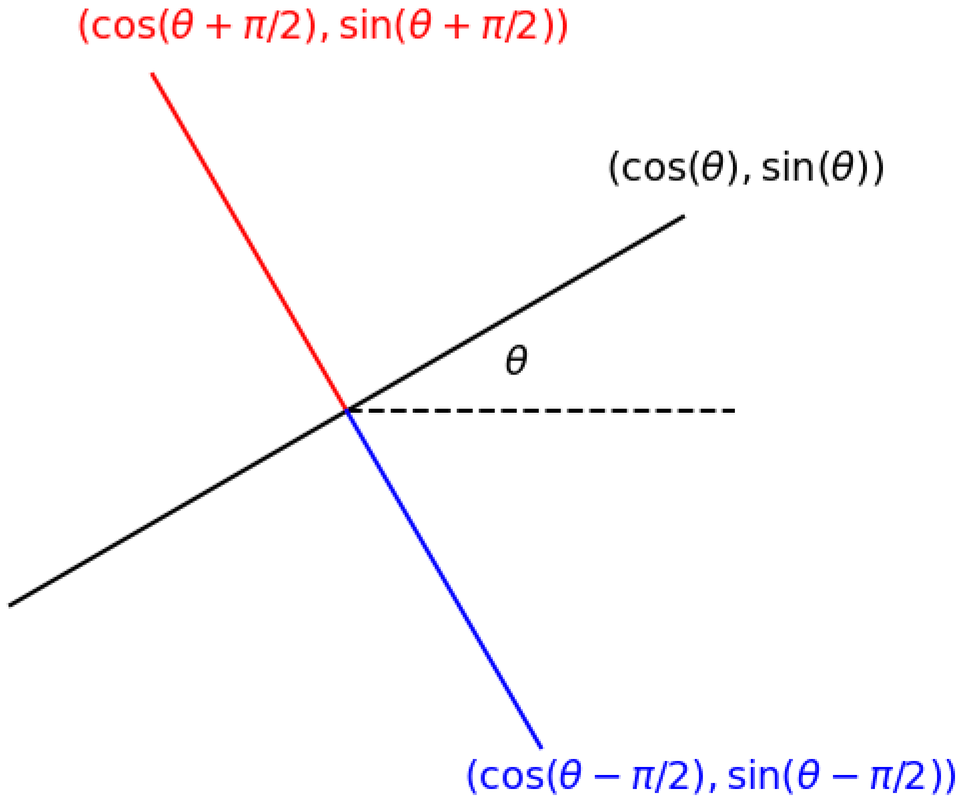
$(\cos(\theta + \pi/2), \sin(\theta + \pi/2))$
$(\cos(\theta), \sin(\theta))$
θ
$(\cos(\theta - \pi/2), \sin(\theta - \pi/2))$

Figure 1 *The (black) line through the origin makes the angle θ with the positive x-axis. The matrix, $H(\theta)$, that reflects across this black line should take the black vector to itself and exchange the red and blue vectors.*

Exercise 7 To build a reflection,

$$H(\theta) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

across the line through the origin of angle θ we note, following Figure 1, that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \cos(\theta) \\ \sin(\theta) \end{bmatrix} = \begin{bmatrix} \cos(\theta) \\ \sin(\theta) \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \cos(\theta + \pi/2) \\ \sin(\theta + \pi/2) \end{bmatrix} = \begin{bmatrix} \cos(\theta - \pi/2) \\ \sin(\theta - \pi/2) \end{bmatrix}$$

Show that these two conditions require that

$$H(\theta) = \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{bmatrix} \tag{13}$$

Please confirm that $H^2(\theta) = I$ and so every reflection is its own inverse.

Exercise 8 There is an intimate connection between reflections and rotations. Please show that every rotation is the product of two reflections, i.e.,

$$K(\theta) = H(\theta/2)H(0) \tag{14}$$

More generally, please show that

$$\begin{aligned} H(\theta)H(\phi) &= K(2\theta - 2\phi) \\ K(\theta)H(\phi) &= H(\phi + \theta/2) \\ H(\phi)K(\theta) &= H(\phi - \theta/2) \end{aligned} \tag{15}$$

These identities are specially helpful in cataloging and connecting the symmetries of planar objects. In Figure 2 below we mark the reflections enjoyed by the equilateral triangle.

In [182]:

```
# equilateral triangle and its Cayley graph↔
```

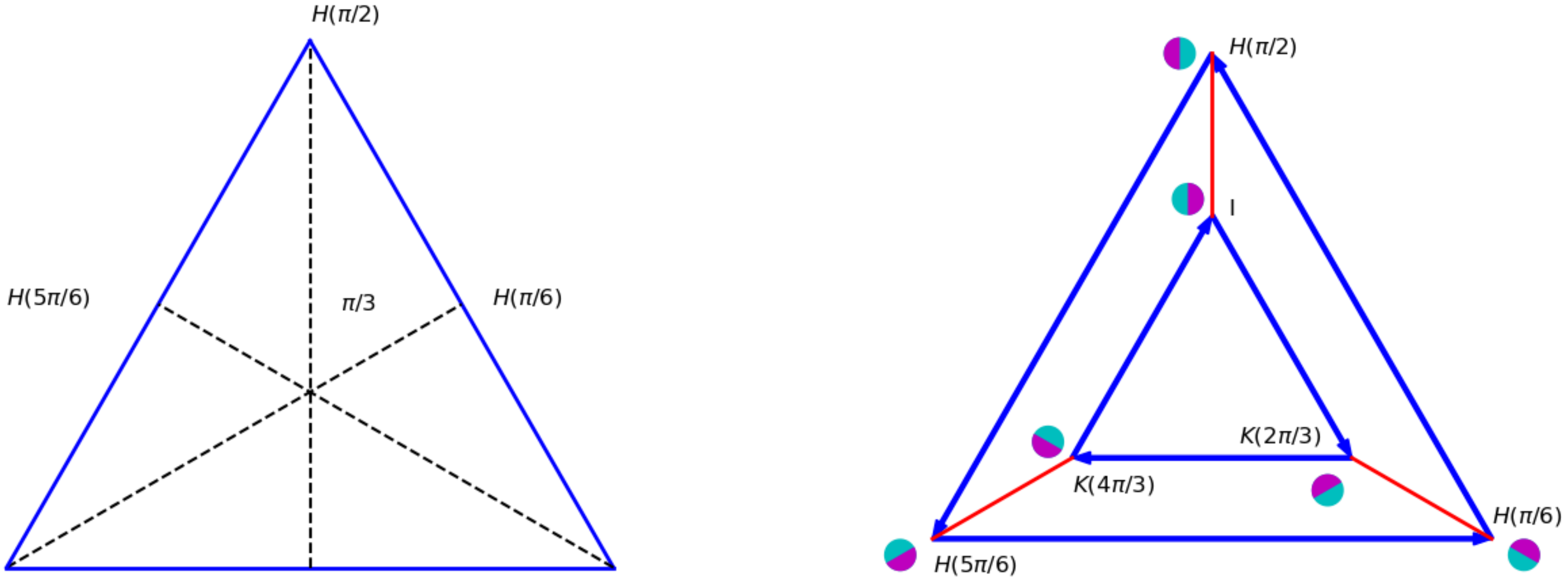

Figure 2 *(Left) An equilateral triangle with 3 (dashed) lines of symmetry labeled by their associated reflections. The triangle is also preserved by the the rotations* $K(2\pi/3)$ *and* $K(4\pi/3)$*. (Right) The Cayley Graph of* Dih_3 *with respect to* $K(2\pi/3)$ *and* $H(\pi/2)$*. The vertices of the graph are elements of* Dih_3 *and edges are colored blue for left multiplication by* $K(2\pi/3)$ *and red for left multiplication by* $H(\pi/2)$*. The blue edges are directed. To travel against a blue arrow requires multiplication by* $K(2\pi/3)^{-1}$*, i.e., by* $K(4\pi/3)$*. The red edges go both ways as* $H(\pi/2)$ *is its own inverse. As a further aid to navigation we have exhibited the transformation of the less symmetric cyan/magenta tablet at each vertex.*

Exercise 9 The symmetries of the equilateral triangle, per Figure 2, are the six matrices

$$I,\ K(2\pi/3),\ K(4\pi/3),\ H(\pi/6),\ H(\pi/2),\ H(5\pi/6) \tag{16}$$

Use the previous exercise to complete this remarkable multiplication table

Δ	I	$K(2\pi/3)$	$K(4\pi/3)$	$H(\pi/6)$	$H(\pi/2)$	$H(5\pi/6)$
I	I	$K(2\pi/3)$	$K(4\pi/3)$	$H(\pi/6)$	$H(\pi/2)$	$H(5\pi/6)$
$K(2\pi/3)$	$K(2\pi/3)$	$K(4\pi/3)$	I	$H(\pi/2)$	$H(5\pi/6)$	$H(\pi/6)$
$K(4\pi/3)$	$K(4\pi/3)$	I				
$H(\pi/6)$	$H(\pi/6)$	$H(5\pi/6)$				
$H(\pi/2)$	$H(\pi/2)$	$H(\pi/6)$				
$H(5\pi/6)$	$H(5\pi/6)$	$H(\pi/2)$				

(17)

The entries correspond to the product of a matrix in the first column with a matrix in the first row, in that order. For example, $K(2\pi/3)H(\pi/6) = H(\pi/2)$ while $H(\pi/6)K(2\pi/3) = H(5\pi/6)$.

Although his table is clean and, unlike your grade school multiplication, self-contained its patterns are not easy to see. We adress its visualization in the **Cayley Graph** at right in Figure 2. The six vertices of the graph correspond to the matrices in (16) while the edges code the relationship between vertices via either left multiplication by $K(2\pi/3)$ on blue edges or right multiplication by $H(\pi/2)$ on red edges.

This exercise gives us our first example of a matrix group.

Definition 1 *A collection G of 2-by-2 matrices is called a **matrix group** when*

(1) If $M \in G$ then $M^{-1} \in G$, and

(2) If $M \in G$ and $N \in G$ then $MN \in G$.

Exercise 10 Please confirm that the collection of matrices in (16) is a matrix group. Show that $\{I, H(\pi/6)\}$ is also a group. Show that $\{I, K(2\pi/3), K(4\pi/3)\}$ is a group. Is $\{I, H(\pi/6), H(\pi/2)\}$ a group?

In general we call the rotations and reflections enjoyed by a regular n-gon **Dihedral** symmetries. From this last exercise its natural to call the six matrices in (16) the dihedral group of the equilateral triangle, or Dih_3 for short. Do you see that the regular n-gon has $2n$ dihedral symmetries? Can you see its Cayley graph?

Exercise 11 Use Exercises 2 - 4 to show that

(i) the collection of dilations, $\{A(\alpha) : 0 < \alpha < \infty\}$ is a group,

(ii) the collection of shears, $\{N(\sigma) : \sigma \in \mathbb{R}\}$ is a group, and

(iii) the collection of rotations, $\{K(\theta) : 0 \leq \theta < 2\pi\}$ is a group.

We know how to invert dilations, shears, and rotations. The general case requires

Exercise 13 Please show that if $\det(M) \neq 0$ then

$$M^{-1} = \frac{1}{\det(M)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \tag{18}$$

is the **inverse** of M in the sense that $MM^{-1} = M^{-1}M = I$.

From here it not hard to see that each 2-by-2 matrix obeys a quadratic equation.

Exercise 14 Use (18), assuming $\det(M) \neq 0$, to achieve

$$M + \det(M)M^{-1} = (a + d)I \tag{19}$$

This sum, $a + d$, of the diagonal elements occurs so frequently that we give it a name. We call it the **trace** and abbreviate it by tr. To wit, $\mathrm{tr}(M) = a + d$. Use this notion as you multiply (19) by M to achieve the quadratic equation

$$M^2 - \mathrm{tr}(M)M + \det(M)I = 0 \tag{20}$$

Please explore the implications of this identity when M is $A(\alpha)$, $N(\sigma)$, $K(\theta)$, or $H(\theta)$.

From here we learn that that the eigenvalues of each 2-by-2 matrix obey the same quadratic equation.

Exercise 15 That polynomial in (20) deserves a second look. We will see that the most powerful descriptors of a linear transformation are its eigenvalues and eigenvectors. We have seen that 2-by-2 matrices rotate and scale planar nonzero vectors. We call a nonzero $q \in \mathbb{R}^2$ an **eigenvector** of $M \in \mathbb{R}^{2\times 2}$ when M scales, *but does not rotate*, q. The scale factor we call the **eigenvalue** of M associated with q. To see these objects please enter

$$\begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}$$

into our widget in our previous notebook (1.2.MatrixVectorMultiplication.ipynb) and confirm that vectors in the $[1, 1]$ direction are merely scaled by 1, while vectors in the $[1, -1]$ directions are scaled by 3.

(a) Use the widget to find the eigenvectors and eigenvalues of

$$\begin{bmatrix} 4 & 1 \\ 1 & 4 \end{bmatrix} \tag{21}$$

(b) With the right picture in mind let us develop an algebraic understanding of eigen-objects. To say that q is an eigenvector of M with eigenvalue λ is to say that Mq is simply λq, i.e.,

$$Mq = \lambda q \tag{22}$$

This says that M acts like a scalar, λ, for vectors on the line through q. As there is a common q on each side of (22) it makes sense to collect terms and land at

$$(M - \lambda I)q = 0 \tag{23}$$

This in turn states that $M - \lambda I$ sends a nonzero vector to 0. As $M - \lambda I$ also sends the zero vector to zero we see that $M - \lambda I$ cannot be invertible. It then follows from (18) that $\det(M - \lambda I) = 0$. Unpack this equation and conclude that λ must be a solution of

$$\lambda^2 - \mathrm{tr}(M)\lambda + \det(M) = 0 \tag{24}$$

the **exact same polynomial** that we discovered in the previous exercise.

(c) Confirm that the eigenvalues you computed by sight in part (a) indeed obey (24).

(d) Confirm that the sum of these eigenvalues equals the trace of M and that their product is the determinant of M.

As the determinant and trace are such "natural" descriptors we explore how they behave when we compose, i.e., multiply, matrices. First, as the determinant of a matrix measures the degree to which it scales areas we may guess that the change in area following a composition is the product of their individual area changes. To check this guess we set

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \tag{25}$$

and compute their product

$$MN = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} s & t \\ u & v \end{bmatrix} = \begin{bmatrix} as + bu & at + bv \\ cs + du & ct + dv \end{bmatrix} \tag{26}$$

and note that it's determinant

$$\det(MN) = (as + bu)(ct + dv) - (at + bv)(cs + du) = (ad - bc)(sv - tu) = \det(M)\det(N), \tag{27}$$

as we had guessed. This deserves a box,

$$\boxed{\det(MN) = \det(M)\det(N)} \tag{28}$$

Do you see how this produces $\det(M^{-1}) = 1/\det(M)$? Regarding the behavior of the trace under composition we note although $A(\alpha)N(\sigma) \neq N(\sigma)A(\alpha)$ we do observe that $\mathrm{tr}(A(\alpha)N(\sigma)) = \mathrm{tr}(N(\sigma)A(\alpha))$. To see that this is no accident, we compute the *other* product

$$NM = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} as + ct & sb + td \\ ua + vc & bu + dv \end{bmatrix} \tag{29}$$

and note that summing the diagonal terms in MN and NM reveals

$$\boxed{\mathrm{tr}(MN) = \mathrm{tr}(NM)} \tag{30}$$

Exercise 16 Use (28) and (30) to conclude that wrapping a matrix by a second matrix and its inverse does not disturb its determinant nor its trace. That is, show that

$$\det(NMN^{-1}) = \det(M) \quad \text{and} \quad \mathrm{tr}(NMN^{-1}) = \mathrm{tr}(M) \tag{31}$$

Exercise 17 Let $\mathrm{SL}_2(\mathbb{R})$ denote the collection of real 2-by-2 matrices with determinant 1. Use (28) to confirm that $\mathrm{SL}_2(\mathbb{R})$ is a matrix group. (Here SL stands for *special linear*).

This last exercise, together with Exercises 5 and 11, implies that $\mathrm{SL}_2(\mathbb{R})$ is a product of the subgroups of dilations, shears, and rotations. We will have cause to study quite a few other subgroups of $\mathrm{SL}_2(\mathbb{R})$. For example, if we restrict ourselves to matrices with integer entries and determinant 1, then it follows from (18) that these matrices have integer inverses with determinant 1. Denoting the integers by $\mathbb{Z}$ we see that $\mathrm{SL}_2(\mathbb{Z})$ forms a subgroup of $\mathrm{SL}_2(\mathbb{R})$. We note that I is the only dilation in $\mathrm{SL}_2(\mathbb{Z})$ while it contains the group of four rotations $\{K(n\pi/2) : n = 1, 2, 3, 4\}$ and the infinite group of shears

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}, \qquad n \in \mathbb{Z}. \tag{32}$$

We next show that this **particular** rotation and **particular** shear

$$A = K(\pi/2) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = N(1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{33}$$

together with their inverses,

$$A^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = -A \qquad \text{and} \qquad B^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \tag{34}$$

generate all of $\mathrm{SL}_2(\mathbb{Z})$. This kind of statement will become a theme throughout the coming notebooks, where, e.g., we will explore the tiling or *tesselation* of the plane by particular transformations and we will also show that all qubit *gates* can be effectively generated by a particular pair of transformations.

Proposition 1 *Each $M \in \mathrm{SL}_2(\mathbb{Z})$ can be written as a finite product of A, B, A^{-1} and B^{-1}.*

Proof: We write $M \in \mathrm{SL}_2(\mathbb{Z})$

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{35}$$

and note that if $c = 0$ then, as $ad - bc = 1$, M must be either

$$M_+ = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \qquad \text{or} \qquad M_- = \begin{bmatrix} -1 & b \\ 0 & -1 \end{bmatrix} \tag{36}$$

but $M_+ = B^b$ while $M_- = -B^{-b} = A^2 B^{-b}$ are both products of powers of A and B. Hence, to complete the proof we must show that $\{A, B, A^{-1}, B^{-1}\}$ can used to zero out the lower left element in M. To begin, we note that

$$AM = \begin{bmatrix} -c & -d \\ a & b \end{bmatrix} \qquad \text{and} \qquad B^n M = \begin{bmatrix} a + nc & b + nd \\ c & d \end{bmatrix} \tag{37}$$

and so will use B^n to modify the upper left element and then use A to exchange the upper left and the lower left elements. In particular, if $|a| \geq |c|$, divide a by c, i.e., express $a = cq + r$ with integer quotient q and remainder r and $0 \leq r < |c|$. Now, by (37),

$$B^{-q} M = \begin{bmatrix} a - qc & b - qd \\ c & d \end{bmatrix} = \begin{bmatrix} r & b - qd \\ c & d \end{bmatrix} \qquad \text{and} \qquad AB^{-q} M = \begin{bmatrix} -c & -d \\ r & b - qd \end{bmatrix} \tag{38}$$

and indeed $0 \leq r < |c|$. Now, if $r \neq 0$ we simply repeat this process. As it is guaranteed to diminish the magnitude of the lower left entry by at least one at each iteration then after a finite number of steps we must reach a zero remainder. **ALMOST End of Proof.**

We have coded this *triangulator* in the cell below on the matrix

$$M = \begin{bmatrix} 17 & 29 \\ 7 & 12 \end{bmatrix} \tag{39}$$

In [51]:

```
# SL2(Z) triangulator,↔
```

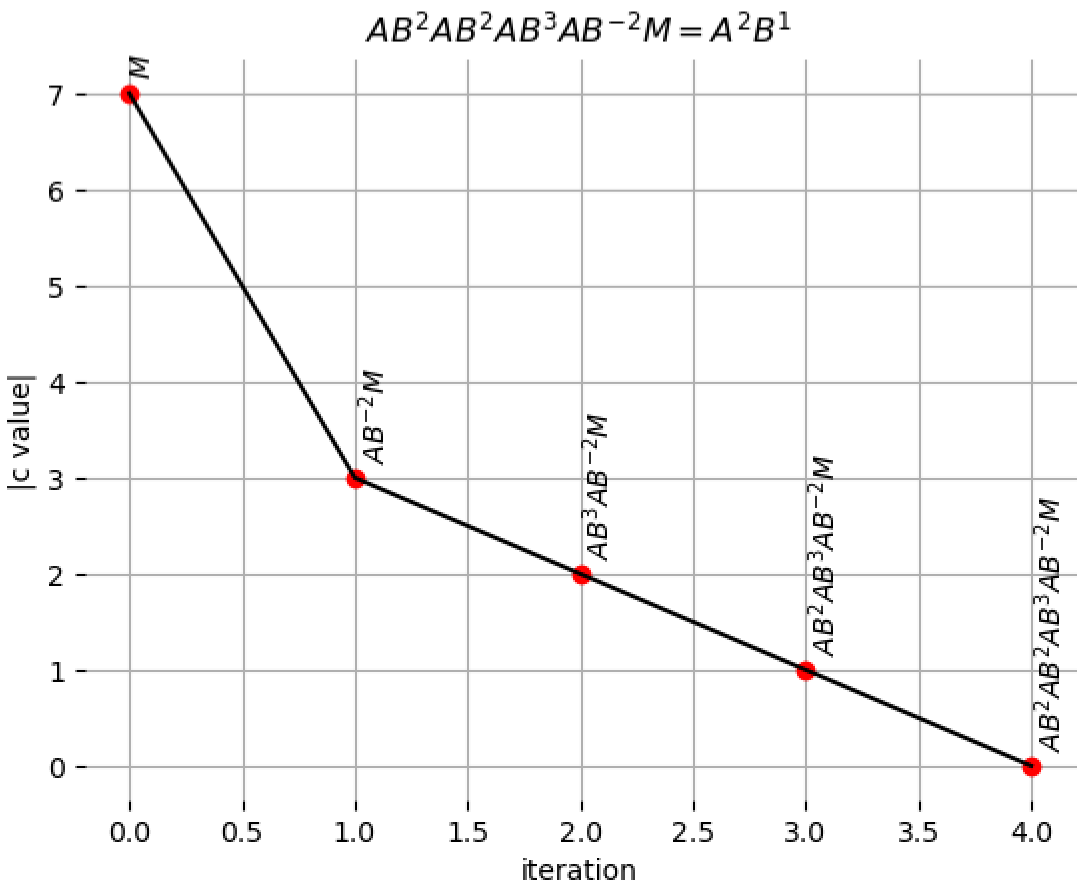

Figure 3 *Performance of the triangulator algorithm applied to the M of (39).*

We obtain finite subgroups of $\mathrm{SL}_2(\mathbb{Z})$ by replacing "regular" arithmetic with **modular** arithmetic. Recall that two integers, m and n, are said to be **congruent** modulo p, written $m \equiv n \bmod p$, when their difference is a multiple of p. In the simplest case, $p = 2$, we note that $1 + 1 = 2 \equiv 0 \bmod 2$ and $-1 \equiv 1 \bmod 2$. Then $\mathrm{SL}_2(2)$, the 2-by-2 matrices with elements from $\{0, 1\}$ and determinant 1 under mod 2 arithmetic are simply

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \tag{40}$$

Exercise 18 Show that the determinant of each matrix in (40) is 1 mod 2. Show that $\mathrm{SL}_2(2)$ is a group and, moreover, that it has the same multiplication table and Cayley graph as Dih_3.

On moving up to mod 3 arithmetic we may use the fact that $2 \cdot 2 \equiv 1 \bmod 3$ to see that each nonzero in $\{0, 1, 2\}$ has a mod 3 multiplicative inverse. As a result, in building a matrix in $\mathrm{SL}_2(3)$ we note that there are $3^2 - 1$ ways of choosing the first (nonzero) column, say (a, b). As the second column, (c, d), must be chosen so that $ad - bc = 1 \bmod 3$ we note that if $a \neq 0$ then $d = (1 - bc)a^{-1}$ where c is arbitrary, while if $a = 0$ then $c = -1b^{-1}$ and d is arbitrary. Hence, regardless of a, there are 3 choices for the second column. As a result, there are 24 matrices in $\mathrm{SL}_2(3)$. To move beyond mod 3 we need multiplicative inverses to accomodate the determinant equation. Do you see why this requires prime congruences? Please generalize the argument above to confirm that.

Exercise 19 For prime p, $\mathrm{SL}_2(p)$, the 2-by-2 matrices with elements from $\{0, 1, \ldots, p-1\}$ and determinant 1 under mod p arithmetic, is a group with $p(p^2 - 1)$ matrices.

Proposition 2 *The group* $\mathrm{SL}_2(p)$ *is generated by*

$$U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad L = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{41}$$

Proof: Writing $M \in \mathrm{SL}_2(p)$ as

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{42}$$

we note first that if $c \neq 0$ then

$$\begin{bmatrix} 1 & (a-1)/c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \begin{bmatrix} 1 & (d-1)/c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & (d-1)/c + d(a-1)/c \\ c & d \end{bmatrix} = M \tag{43}$$

because $(d-1)/c + d(a-1)/c = (ad-1)/c = (ad - (ad - bc))/c = b$. Note that, in terms of U and L this reads

$$M = U^{(a-1)/c} L^c U^{(d-1)/c} \tag{44}$$

Now if $c = 0$ then $ad = 1$ and so

$$\begin{bmatrix} a + b & b \\ d & d \end{bmatrix} \in \mathrm{SL}_2(p) \tag{45}$$

with a nonzero lower left entry and so can be written with U and L as above. It remains to note that this latter matrix is easily transformed to M;

$$\begin{bmatrix} a+b & b \\ d & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ p-1 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = M \tag{46}$$

That is, $M = U^{(a+b-1)/d} L^d U^{(d-1)/d} L^{p-1}$ when $c = 0$. **End of proof.**

Exercise 20 Write out and check the factorization (44) when $p = 5$ and

$$M = \begin{bmatrix} 4 & 1 \\ 2 & 2 \end{bmatrix} \tag{47}$$

Next Section: 1.4 Kinematics (1.4.Kinematics.ipynb)