Linear mappings and matrices. We consider linear mappings

$$L : \mathbb{R}^2 \to \mathbb{R}^2,$$

which we can picture as motions of the plane, moving each vector v to $L(v) = w$, for example rotating around the origin by some angle. *Linear* means that L respects vector addition and scalar multiplication:

$$L(v_1{+}v_2) = L(v_1) + L(v_2) \qquad \text{and} \qquad L(rv) = rL(v) \ \text{ for } \ r \in \mathbb{R}.$$

Thus, once we know the outputs of the basis vectors $L(1,0) = (a,b)$ and $L(0,1) = (c,d)$, we can compute $L(x,y)$ for any $v = (x,y)$:

$$\begin{aligned} L(x,y) &= L(x(1,0) + (y(0,1)) \ = \ xL(1,0) + yL(0,1) \\ &= x(a,b) + y(c,d) \ = \ (ax{+}cy, bx{+}dy). \end{aligned}$$

The *matrix* of L, denoted $[L]$, records the outputs of the basis in its columns:

$$[L] \ = \ \left[\begin{array}{c|c} | & | \\ L(1,0) & L(0,1) \\ | & | \end{array}\right] \ = \ \left[\begin{array}{c|c} a & c \\ b & d \end{array}\right].$$

We define matrix multiplication of $[L]$ by a vector v to give the output $L(v)$:

$$L(x,y) \ = \ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \ = \ \begin{bmatrix} ax{+}cy \\ bx{+}dy \end{bmatrix}.$$

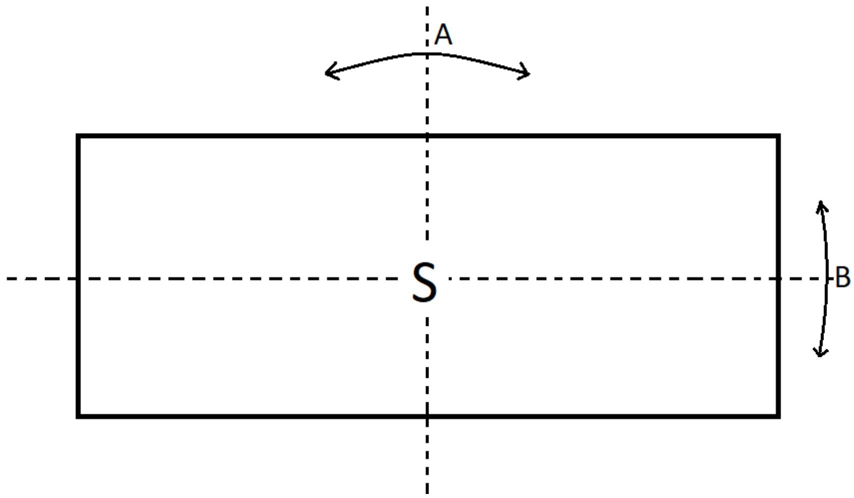
Given two linear mappings L, M, we can do one after the other to get the composition mapping $L \circ M$ defined by: $(L \circ M)(v) = L(M(v))$. We define matrix multiplication so that it gives the matrix of the composition:

$$[L \circ M] \ = \ [L] \cdot [M].$$

This is the main meaning of matrix multiplication.

To avoid fussy notation we drop the brackets, so that L can denote both the linear mapping and its matrix, and $\cdot$ denotes composition of mappings as well as matrix multiplication.

Symmetries. A *symmetry* of an object S is an invertible mapping from S to itself which preserves the structure of S. We consider the example where S is a rectangle in the plane, with the geometric structure of distance between points. The symmetries are the rigid (distance-preserving) mappings from S to itself, which are therefore linear mappings. Here are two examples:



The horizontal reflection A and the vertical reflection B both take S to itself; by contrast, a 90° rotation takes S to a different rectangle, and is *not* a symmetry. Taking the center of S as the origin, we can determine the matrix of A by recording the outputs $A(1,0) = (-1,0)$ and $A(0,1) = (0,1)$, so $A = \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$; and similarly $B = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$.

Are these all the symmetries? We also have inverse symmetries, but $A = A^{-1}$ and $A \cdot A = I$: a reflection undoes itself, and doing it twice is the same as doing nothing. (Here I is the identity mapping with $I(v) = v$, having matrix $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.) However, we can find a new symmetry by composing the two known ones, doing the horizontal reflection after the vertical one:

$$C \;=\; A \cdot B \;=\; \left[\begin{array}{r|r} -1 & 0 \\ 0 & -1 \end{array}\right].$$

What is the composite motion? Its matrix tells us that $C(1,0) = (-1,0)$ and $C(0,1) = (0,-1)$, so in fact $C(v) = -v$, and C takes each vector to its opposite. Another way to describe this is as a 180° rotation. Now we have all the symmetries.

Symmetry group. This means the set $G = \mathrm{Sym}(S)$ of all symmetries of S, endowed with the operation of composition, doing one symmetry after another to obtain a new symmetry. This allows us to think of G as a kind of number system, but only with multiplication, no addition. The rectangle symmetry group above is $G = \{I, A, B, C\}$ with multiplication table:

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	I	C	A
C	C	B	A	I

Definition: A *group* is a set G with an opertion $\cdot$ which satisfies the same axioms of multiplication as units in a ring:

- *Closed:* For $A, B \in G$ we have $A \cdot B \in G$.
- *Associative:* $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.
- *Identity:* For $A \in G$ we have $A \cdot I = I \cdot A = A$.
- *Inverses:* For $A \in G$ there is $A^{-1} = B \in G$ with $A \cdot B = B \cdot A = I$.

Note that G does not have a zero element or any addition operation. Although the above example satisfies the commutative law $A \cdot B = B \cdot A$, not all groups do; a commutative group is called *abelian* (after Niels Abel).

Groups can arise from geometric symmetries as above, or from other types of symmetries. In our example, we have $G \subset M_2(\mathbb{R})$, the ring of 2×2 matrices with real number entries, which guarantees it satisfies the group axioms. However, G is not a subring since it is not closed under addition; rather, G is a subgroup of all the invertible matrices, which form the *general linear group*:

$$\mathrm{GL}_2(\mathbb{R}) \;=\; \{A \in M_2(\mathbb{R}) \text{ such that } A \text{ is invertible}\}.$$

Like every group, $\mathrm{GL}_2(\mathbb{R})$ must be the symmetries of something. In fact, it is the symmetries of the plane $\mathbb{R}^2$, all invertible mappings which preserve (respect) the vector space structure of addition and scalar multiplication (not the geometric structure of distance).

Permutations. The most basic type of symmetry is that of an unstructured set $S = \{1, 2, \ldots, n\}$. Then $G = \mathrm{Sym}(S)$ consists of *all* invertible mappings $A : S \to S$, without any structure restrictions. A convenient notation for such a mapping is the two-line notation with the inputs i on the first line and the outputs $A(i)$ just below them: $A = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ A(1) & A(2) & \cdots & A(n) \end{smallmatrix}\right)$. For example:

$$I \;=\; \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix}, \qquad A \;=\; \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix}, \qquad B \;=\; \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}$$

means I is the idenity with $I(i) = i$ for all i; and $A(1) = 2$, $A(2) = 1$, $A(3) = 4$, $A(4) = 3$. We can compose these to get a new permutation $C = A \circ B$ with $C(i) = A(B(i))$.

$$C \;=\; A \circ B \;=\; \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix} \circ \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix} \;=\; \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix},$$

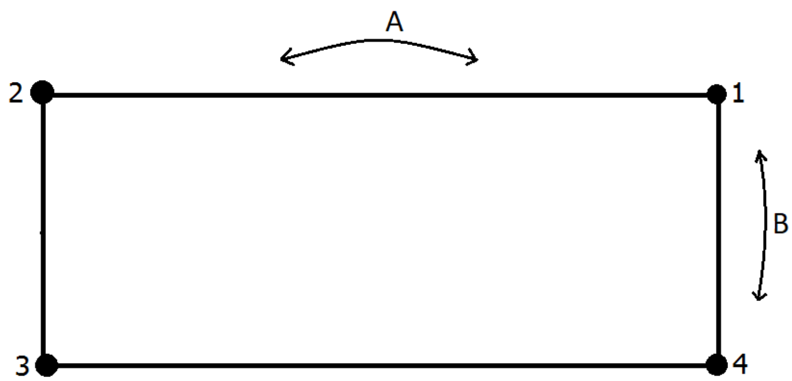
since $C(1) = A(B(1)) = A(4) = 3$ and $C(2) = A(B(2)) = A(3) = 4$, etc.

The group of all permutations of n objects, together with the composition operation, is called the *symmetric group* $G = S_n$. To construct a random permutation A, we have n choices for $A(1)$, then $n-1$ choices remaining for $A(2) \neq A(1)$, then $n-2$ choices for $A(3)$, etc., so the total number of permutations is:

$$\#S_n \;=\; n(n-1)(n-2)\cdots 1 \;=\; n!$$

This is the main significance of the factorial function.

We can realize the symmetry group of our rectangle by labeling vertices:



Then any symmetry moves the 4 vertices to each other, and the motion of the whole rectangle is determined by this permutation of $\{1, 2, 3, 4\}$. Thus, the symmetries of the rectangle described previously in geometric terms can also be written as the permutations I, A, B, C above. Thus our symmetry group becomes a subgroup $G \subset S_4$ and we can work out its multiplication table in terms of permutations more easily than in terms of matrices.