Permutations.

1. **Definition (Permutation).** A *permutation* of a set A is a bijective function $f : A \to A$. The set of all permutations of A is denoted by $\mathrm{Perm}(A)$.

2. If A has cardinality n, then $\mathrm{Perm}(A)$ has cardinality $n! = (n)(n-1)\dots(2)(1)$.

   This is because there are n choices for the output of the first element of A under f, and given one such choice there are now $(n-1)$ choices for the output of the second element of A under f, and so on.

3. The set $\mathrm{Perm}(A)$ together with the operation of composition of functions satisfies the following properties.

   - *Closure.* If $f, g \in \mathrm{Perm}(A)$, then $f \circ g \in \mathrm{Perm}(A)$.
   - *Identity.* The function $\mathbb{I}_A \in \mathrm{Perm}(A)$ satisfies
     $$f \circ \mathbb{I}_A \;=\; \mathbb{I}_A \circ f \;=\; f$$
     for all $f \in \mathrm{Perm}(A)$.
   - *Inverses.* Given $f \in \mathrm{Perm}(A)$ there is $f^{-1} \in \mathrm{Perm}(A)$ such that
     $$f \circ f^{-1} \;=\; f^{-1} \circ f \;=\; \mathbb{I}_A$$
   - *Associativity.* For all $f, g, h \in \mathrm{Perm}(A)$
     $$f \circ (g \circ h) \;=\; (f \circ g) \circ h$$

   We say that $\mathrm{Perm}(A)$ forms a *group* under composition of functions.

4. **Definition (Cyclic permutation).** Let U be a set of m elements. A permutation f of U is called an *m–cycle* (and is said to be a *cyclic permutation*) if there is some labeling $a_1, \dots, a_m$ of the elements of U such that
   $$f(a_1) = a_2,\; f(a_2) = a_3,\; \dots,\; f(a_{m-1}) = a_m,\; f(a_m) = a_1$$
   We denote the m–cycle f by $(a_1 a_2 \dots a_m)$. Note that $(a_2 a_3 \dots a_m a_1)$ denotes the same m–cycle f. A 2–cycle is called a *transposition*.

5. Prove that there are $(n-1)!$ many distinct n–cycles.

6. Prove that $(a_1 \dots a_m)$ has inverse $(a_m \dots a_1)$.

7. Prove that the m–fold composite of an m–cycle with itself yields the identity permutation.

8. Prove that a general permutation $f \in \mathrm{Perm}(A)$ is a composition of cycles on disjoint subsets of A.

9. **Definition (Cycle notation for permutations).** From the property above we know that a permutation on a finite set A is a composition (product) of cyclic permutations on disjoint subsets of A. We write each cyclic permutation out using cycle notation ignoring the cycles of size 1. This is the standard notation for permutations.

   If $A = \{1, 2\}$ then $\mathrm{Perm}(A)$ has $2! = 2$ elements: $\mathbb{I}_A$ and the 2–cycle (transposition) (12).

   If $A = \{1, 2, 3\}$ then $\mathrm{Perm}(A)$ has $3! = 6$ elements: $\mathbb{I}_A$, (12), (23), (13), (123), and (132).

   Write out the elements of $\mathrm{Perm}(A)$ when $A = \{1, 2, 3, 4\}$ and when $A = \{1, 2, 3, 4, 5\}$.

10. **Multiplication table for** $\mathrm{Perm}(\{1,2\})$**.**

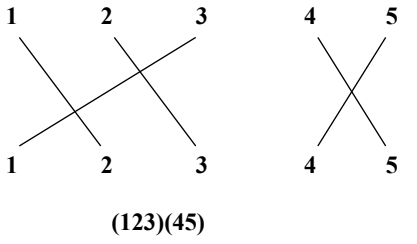
$\circ$	$\mathbb{I}$	(12)
$\mathbb{I}$	$\mathbb{I}$	(12)
(12)	(12)	$\mathbb{I}$

11. **Multiplication table for** $\mathrm{Perm}(\{1,2,3\})$**.** Note that the convention for these multiplication tables is that the entry in the box which is the intersection of the ith row (with function f_i on the leftmost column) and the jth column (with function f_j on the topmost row) is the composition $f_i \circ f_j$. The composition symbol is often dropped, and the composition is written simply by juxtaposition $f_i f_j$. In the table below we compute each of these compositions $f_i f_j$ and write the answers in cycle notation in the ij-slot.

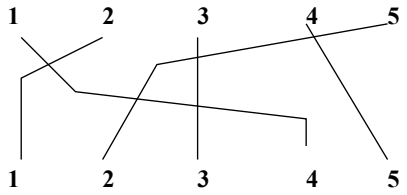
$\circ$	$\mathbb{I}$	(123)	(132)	(12)	(13)	(23)
$\mathbb{I}$	$\mathbb{I}$	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	$\mathbb{I}$	(13)	(23)	(12)
(132)	(132)	$\mathbb{I}$	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	$\mathbb{I}$	(132)	(123)
(13)	(13)	(12)	(23)	(123)	$\mathbb{I}$	(132)
(23)	(23)	(13)	(12)	(132)	(123)	$\mathbb{I}$

12. **Braid diagrams for permutations.** Given a permutation f of the set $\{1,\ldots,n\}$ we can represent it geometrically using a *braid diagram* as follows. Draw two rows of numbers $1,2,\ldots,n$; the top row will be the input row, and the bottom row will be the output row. Now draw a line from i in the top row to $f(i)$ in the bottom row. Draw lines so that they cross at most two at a time (wiggle/perturb your lines a bit so that there are no points where three or more lines cross).

    Here are some examples of braid diagrams for permutations on $\{1,2,3,4,5\}$.

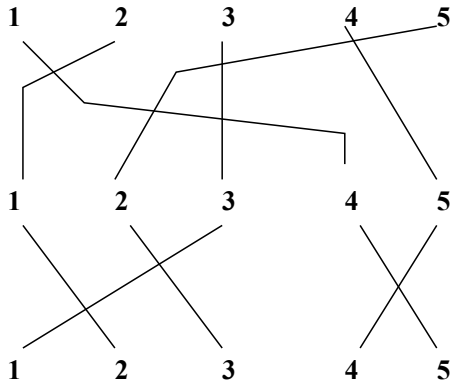


(123)(45)



(1452)

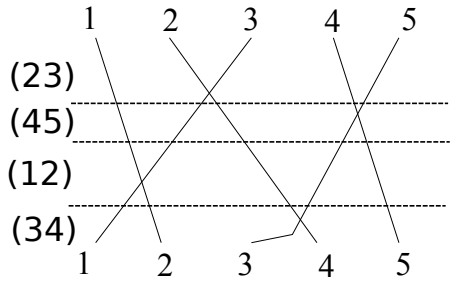
    Multiplication (composition) of permutations is easy to determine by concatenating the braid diagrams in the correct order. For example, the composition $(123)(45)(1452)$ is obtained by first writing down the (1452) diagram and placing the $(123)(45)$ diagram underneath as shown.



(153) = (123)(45)(1452)

13. **Braid diagrams and products of transpositions.** Here is an immediate consequence of braid diagrams. Given a permutation f, draw a braid diagram. Wiggle the strands so that no two crossings occur on the same level. Now draw horizontal lines between crossing levels. On a given level there is a single crossing of adjacent (as seen from that level) strands. This is a transposition of the form (ij) where $j = i+1$. Check that the permutation f is a composition of these transpositions in order as you read from top to bottom.

    Here is an example which shows how to write the 5–cycle (12453) as a product of 4 transpositions.



(12453)=(34)(12)(45)(23)

14. **Sign of a permutation.** The *sign* of a permutation f is defined by drawing a braid diagram for f and counting all the pairwise crossings of lines mod 2. Thus the sign of a permutation is either 0 or 1. We call permutations with sign 0 *even* and permutations with sign 1 *odd*.

    There may be many braid diagrams for the same permutation. For example, the concatenated diagram above for the permutation (153) is different from the diagram you might draw yourself. In particular, you would be unlikely to have the stands from 3 to 1 and from 5 to 3 overlap like they do in the concatenated diagram. So how do we know that these different diagrams all give the same number of crossings mod 2?

    Here is the reason. Look at two input numbers $i < j$. If $f(i) > f(j)$ then the strand from i to $f(i)$ must cross from the left side to the right side of the strand from j to $f(j)$. Thus it must cross this strand an odd number of times, this is equivalent to 1 mod 2.

    In the case that $i < j$ and $f(i) < f(j)$ then the strand from i to $f(i)$ starts and ends on the left hand side of the strand from j to $f(j)$ and so it must cross this strand an even number of times, and this is equivalent to 0 mod 2.

This reasoning tells us that the following is another definition of the sign of f, and is one which does not depend on the particular braid picture for f.
sign(f) is the number (mod 2) of pairs $i < j$ for which $f(i) > f(j)$.

15. **Properties of sign**. The following are two useful properties of sign(f).

    - The sign of a product of permutations is the sum of the signs.

      $$\text{sign}(f \circ g) \;=\; \text{sign}(f) + \text{sign}(g) \mod 2$$

      We see this by concatenating two braid diagrams (one for f and one for g). Clearly, the number of crossings adds, and so does the answer mod 2.

    - The sign of a transposition (ij) is 1.

      Draw a braid diagram. The strand from i to j crosses all $(j-i-1)$ intermediate strands, the strand from j to i crosses all $(j-i-1)$ intermediate strands, and these two strands cross over each other. The total number of crossings is $2(j-i-1)+1 \equiv 1 \mod 2$.

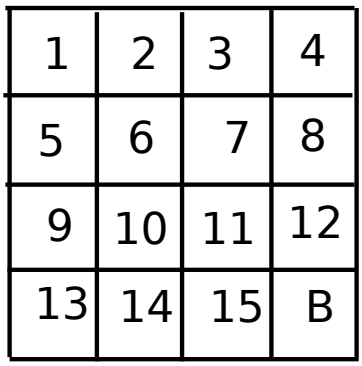
    - As a consequence of the two previous properties and the fact that every permutation is a product of transpositions, we can now say that every even permutation is a product of an even number of transpositions (there may be many distinct products for a given permutation but they will all involve an even number of transpositions) and every odd permutation is a product of an odd number of transpositions.

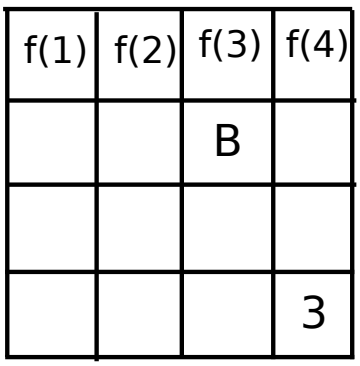
    - The collection of all permutations of the set $\{1, \ldots, n\}$ is called the *symmetric group* on n elements and is denoted by S_n.

      $$S_n \;=\; \text{Perm}(\{1, \ldots, n\})$$

      Note that the identity permutation is even, and that the product of two even permutations is even. Thus, the set of all even permutations on the set $\{1, \ldots, n\}$ is a group under composition. It is called the *alternating group* and is denoted by A_n.
      For example $A_3 = \{\mathbb{I}, (123), (132)\}$ has size 3. In general A_n has size $\frac{n!}{2}$.

16. **The 15-puzzle.** The 15-puzzle consists of a 4×4 frame of numbered square tiles in random order with one tile missing. The 15 tiles can slide horizontally or vertically in the frame to an adjacent empty slot. The game consists of making slide moves until the configuration is restored to some starting configuration. Here we show an example where the tiles are all numbered with the integers 1 through 15, and the starting configuration consists of all 15 numbered tiles in sequence as shown with the last (or 16th slot) empty. This is denoted by **B** (for blank) in the figure.





Unscrambled Scrambled

The slots are numbered 1 through 4 on the top row, 5 through 8 on the second row, 9 through 12 on the third row, and 13 through 16 on the last row, A scrambled puzzle is shown on the right in the figure. We encode a scrambled puzzle by a permutation $f \in \mathrm{Perm}(\{1, \ldots, 16\})$ as follows. "$f(i)$ is the value on the tile in the ith slot."

For example, in our scrambled puzzle $f(7) = 16$ because the blank tile (which we denote by 16 or by **B**) is in slot 7, and $f(16) = 3$ because the tile numbered 3 is in slot 16. Some tiles with numbers from $\{1, \ldots, 16\} - \{3, 16\}$ are the labels on the tiles in the first 4 slots. We haven't specified these explicitly and so they are labeled as $f(1), \ldots, f(4)$ in the diagram. We haven't labeled the remaining squares in this diagram.

The challenge of the 15-puzzle is to slide tiles around to get to the base configuration on the left side of the figure. See the wiki page for the history of the 15-puzzle. In the early 1900's one of America's great puzzle-writers, Sam Loyd, offered $1,000 to anyone who could get from the base configuration to a configuration with the 14 and 15 tiles switched. Do you see a way of doing this?

Permutations offer a great insight into the 15-puzzle. A given configuration comes with two pieces of data.

- A permutation f describing the configuration.
- A positive integer n which is the minimum number of slide moves necessary to "move" the blank square back to slot 16.

Claim: The following number

$$\mathrm{sign}(f) + n \mod 2$$

is an invariant of a slide move.

The idea is very elegant. A slide move post-composes f with a transposition. Some slot i with tile whose face value $f(i)$ is adjacent to the empty square (face value **B** or 16) after sliding the tile labeled $f(i)$ into the blank slot we have a new permutation g. Note that g agrees with f for exactly 14 out of the 16 inputs, but $g(i) = 16$, and g on the adjacent slot (which may correspond to input $i + 1$, $i - 1$, $i + 4$, $i - 4$ depending on where the adjacent blank square was) is now equal to the number $f(i)$. Thus g is equal to $t \circ f$ where t is the transposition which interchanges $f(i)$ and 16. In particular, $\mathrm{sign}(g) = \mathrm{sign}(f) + 1 \mod 2$.

But the blank square is now either one unit closer or 1 unit further from the slot 16, and so the integer n has changed by 1 mod 2.

Therefore the sum changes by $1+1 \equiv 0 \mod 2$ and so the quantity $\text{sign}(f)+n$ is an invariant mod 2.

Exercise. Is the Sam Loyd Challenge solvable? Give a proof of your answer.

Exercise. Is the following variation of the Sam Loyd puzzle solvable? Obtain a configuration whose first three rows agree with the standard configuration, and whose last row reads: 14, 15, 13, B.

17. **Determinants.** Here is another use of permutations and their signs, that you may be intuitively aware of but not explicitly aware of. The *determinant* of a 2×2 matrix is given by the formula

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

Looking at subscripts we notice that if the two subscripts repeat (identity permutation of $\{1, 2\}$) we have a product with a + sign, whereas if the subscripts interchange (undergo a transposition (12)) then the product has a - sign. A way to write this using permutations and signs is as follows

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \sum_{f \in \text{Perm}(\{1,2\})} (-1)^{\text{sign}(f)} a_{1f(1)}a_{2f(2)}$$

This generalizes to any size of square matrix to give a succinct formula for the determinant.

$$\det \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} = \sum_{f \in \text{Perm}(\{1,\dots,n\})} (-1)^{\text{sign}(f)} a_{1f(1)} \cdots a_{nf(n)}$$

Note that the determinant of an $n \times n$ matrix is a sum of $n!$ terms each of which is a product of n entries of the matrix. Half of the $n!$ terms are multiplied by (-1) before the sum is computed.

Exercise. Check that this permutation definition of determinant agrees with the other way you know how to compute determinants of 3×3 matrices, for example from the vectors section (cross products, triple products etc) of your calculus class.

18. **Orders.** Note that the square of a transposition gives the identity permutation. We say that a transposition has *order* 2.

In general the *order* of a permutation f is the least positive power of f which yields the identity permutation. We denote the order of f by $\text{ord}(f)$. Note that $\text{ord}(\mathbb{I}) = 1$, and that the identity is the only permutation with order 1.

Exercise. Prove that the order of an m–cycle is equal to m.

Exercise. Prove that if f is a product of an m–cycle and a k–cycle on a disjoint subset, then $\text{ord}(f) = \text{lcm}(m, k)$. For example, (123)(45) has order 6.

19. **Conjugation.** The *conjugate of a permutation f by the permutation g* is defined to be the product

$$gfg^{-1}$$

By inspecting the diagram of sets and functions (permutations) below we see that the conjugate gfg^{-1} can be thought of as *"what f would look like after we apply g to the universe."*

$$\begin{array}{ccc} \{1,\ldots,n\} & \xrightarrow{f} & \{1,\ldots,n\} \\ \downarrow g & & \downarrow g \\ \{1,\ldots,n\} & \xrightarrow{gfg^{-1}} & \{1,\ldots,n\} \end{array}$$

This is a great intuition to have about conjugation. In particular if f is a 5–cycle, then gfg^{-1} will also be a 5–cycle; the only change is that everything gets relabeled by g.

It is remarkably easy to compute conjugates with cycle notation. Simply take the cycle decomposition for f and apply g to all the entries.

$$(12)(13425)(12)^{-1} \;=\; (23415)$$

$$(15)(234)(12)[(15)(234)]^{-1} \;=\; (53)$$