

The 15-Puzzle Puzzled Out

with Zvezdelina Stankova
Teaching Professor of Mathematics
University of California at Berkeley
Founder and Director of the Berkeley Math Circle at UCB
Founding Director of the Math Taught the Right Way at UCB

You see below a 3x3 image of Cindy Lawrence, our host, made of 9 squares. But something's wrong! Two squares in the rightmost column are flip-flopped! Can we correct this and see the full picture of Cindy?

To the rescue comes the bottom left corner, which is empty and you can slide adjacent squares into the empty slot in trying to arrange the puzzle. If you are successful, the puzzle will fill in the empty square, giving the full picture:



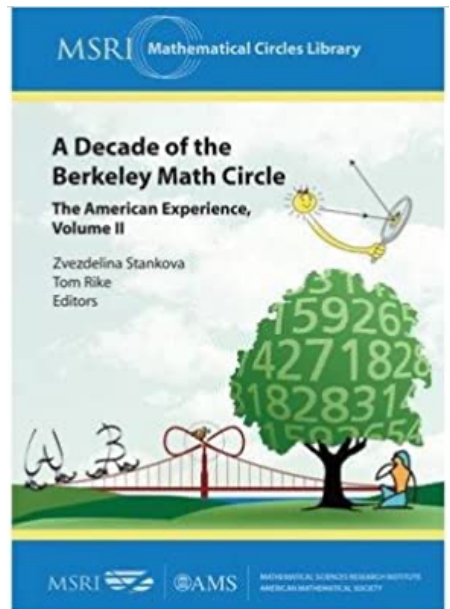
<https://www.geogebra.org/m/yqczqvxy>

The original and most popular version of this puzzle is the so-called 15-puzzle, made of 16 squares arranged in a 4x4 table and labeled 1-15. One square is empty and you can use it to try to arrange the puzzle in order. However, which mixed arrangements are possible to solve and which are not? In other words, if you take the puzzle apart and randomly put it back together, what is the chance that it will be solvable?

While the chances here will be fairly high: 50-50, you will not be so lucky with the Rubic's cube: only 1 in 12 randomly assembled versions will be solvable. Yet the explanation for the 15-puzzle and the Rubic's cube are of the same flavor and use deep ideas from Group Theory: a must to explore by any game fan and math aficionado.

In this talk, we will concentrate on demystifying the 15-puzzle, both in practice and in theory, and learn to immediately catch if anyone has cheated (by taking it apart and putting it back together) and has given us a "defective" puzzle! If you would like to get a head-start, try various puzzle sizes at

<https://www.jaapsch.net/puzzles/javascript/fifteenj.htm>
by Jaap Scherphuis



Session 5

Introduction to Group Theory

BASED ON TATIANA SHUBIN'S SESSION

SNEAK PREVIEW. Having played with Rubik's cube and taken it apart to see what is inside, it is now time to look under the hood and penetrate more deeply into what its true structure is. The building blocks are *groups*. Stubborn polynomials, symmetric elephants, and socks that beg to be put on, taken off, and permuted between your feet are all part of the story, directed by Galois. You will escape never-ending cycles in a complex world, only to stroll along in Permuterland and, ultimately, seek bi-polar paths in 15-Puzzleland.

1. Puzzling It Out

The well-known 15-puzzle consists of a shallow box filled with 16 squares in a 4×4 array. The bottom right corner square is removed, and the other squares are labeled 1 through 15 as in Figure 1a. Using the empty spot, we can slide the squares around without lifting them up.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

4	3	2	1
5	6	7	8
12	11	10	9
13	14	15	

10	9	8	7
11	2	1	6
12	3	4	5
13	14	15	

8	14	11	3
12	2	15	9
6	4	13	1
7	10	5	

FIGURE 1. Achievable or not?



Problem 1 (McCoy [53]). Starting from the initial position in Figure 1a, which 15-puzzle positions in Figures 1b–d can be achieved and why?

Understandably, a novice may ask: “What does this puzzle have to do with *serious* mathematics?” “Ah, . . . wrong question!” an advanced math circle will say. “Just about any interesting (or uninteresting) puzzle is somehow related to mathematics.” The puzzle is frequently a disguise for an actual problem from *group theory*. In fact, by the end of this session you will have seen such a variety of examples of groups, that (whether you wanted to or not) you will start seeing groups *everywhere* around you!

① Super-Challenge:

Prove: *isomorphic*

Any gp G w/ 4 elts \cong

(can relabel elt's to get identical tables)

T (soldier)

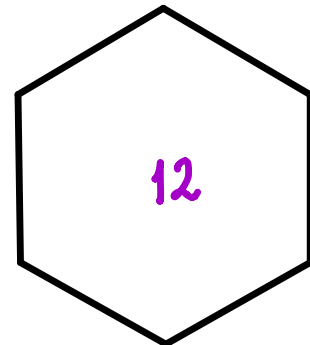
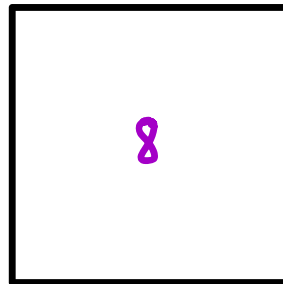
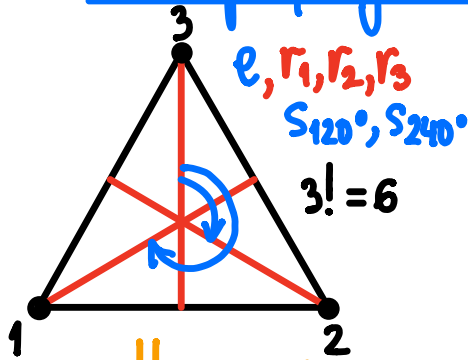
•	s	r	b	l
s	s	r	b	l
r	r	b	l	s
b	b	l	s	r
l	l	s	r	b

S (sock)

•	n	c	i	t
n	n	c	i	t
c	c	n	t	i
i	i	t	n	c
t	t	i	c	n

or

②.5 Group of Symmetries of:



How many elements?

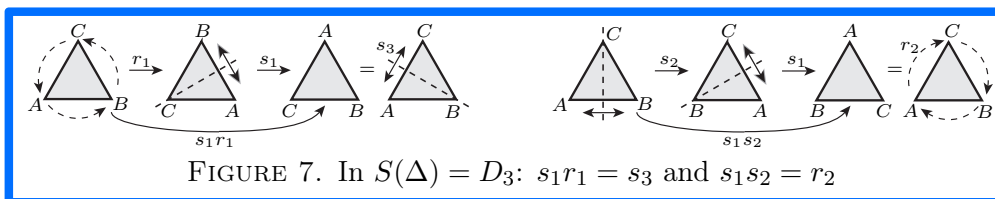
Q: Multiplication table?

What kind of a group?

P_{2-3}

HW (Informal)

- Construct the mult. tables for the 3 figures above.
- Think of groups around you. Describe them.
- Think of ∞ -groups consisting of numbers under some operation.
- * Prove that any group w/ 4 elements is the same as Soldier or Sock group.



a more general argument is usually much faster and more elegant. In our situation with $S(\Delta)$: think about why the composition of two symmetries of Δ is again a symmetry of Δ , and why a symmetry always has a counteraction, i.e., a “reverse” symmetry that undoes it. For example, the counteraction of r_1 is r_2 , and of s_1 is s_1 itself. \diamond

·	i
i	i

·	i	s
i	i	s
s	s	i

·	i	r ₁	r ₂	s ₁	s ₂	s ₃
i	i	r ₁	r ₂	s ₁	s ₂	s ₃
r ₁	r ₁	r ₂	i	s ₂	s ₃	s ₁
r ₂	r ₂	i	r ₁	s ₃	s ₁	s ₂
s ₁	s ₁	s ₃	s ₂	i	r ₂	r ₁
s ₂	s ₂	s ₁	s ₃	r ₁	i	r ₂
s ₃	s ₃	s ₂	s ₁	r ₂	r ₁	i

FIGURE 8. Tables for symmetry groups $S(\mathcal{E}_1)$, $S(\mathcal{E}_2)$, and $S(\Delta)$

If you are still unsure which “symmetries” of our figures we are allowed to consider in this session, check out the footnote on page 107: the allowable symmetries are called *Euclidean motions*. These are motions (bijections) of the plane that preserve distances, also known as *rigid motions* or *isometries*: imagine your figure made of cardboard and you want to transform the figure onto itself without bending, twisting, pinching, or doing other horrible stuff to the cardboard. Thus, a symmetry of a plane figure is not just any bijection of the figure onto itself: it is a rigid motion. For example, switching the vertices A and B of a square $ABCD$ while leaving the other two vertices C and D fixed is *not* part of a symmetry of the square (why?). Be aware that in some sources “rigid” motions exclude *orientation-changing* motions like reflections (a reflection changes a clockwise orientation $ABCD$ of the square to a counterclockwise orientation of the vertices, i.e., $ADCB$). However, we will consider reflections as part of our symmetry groups in this session.

Finally, a reflection across a line combined with a translation along this line is what is called a *glide reflection*. For any plane figure, its symmetry group will be generated by and will consist of the four types of plane transformations mentioned in the text: rotations, reflections, translations, and glide reflections. This is a fact that needs a proof, and we leave it to the more experienced reader to provide such a proof.

Exercise 4. For $n \geq 3$, D_n has $2n$ elements: n rotations and n reflections. The pattern breaks for $n = 1$ and $n = 2$. Of course, we may never think

Problem 4. If we add a reflectional symmetry s to R_4 (i.e., s is a reflection across one of the two diagonals or across one of the two midsegments of the square), then the products r_0s, r_1s, r_2s, r_3s must also be in our subgroup of D_4 . These products are obviously 4 *different* symmetries: all first apply s to the square, but then each continues with a *different* rotation r_j of the square. In addition, each reflection of the square *switches* the labeling of the vertices of the square from clockwise to counterclockwise orientation (check it!); yet any rotation of the square *preserves* the orientation of this labeling (check it!). Hence, each product $r_j s$ first *changes* the orientation of the labeling (via s) and then *preserves* this new orientation (via r_j); so overall, $r_j s$ *changes* the orientation of the vertices' labeling and, thus, must be one of the reflections of the square (cf. Fig. 10a).

·	r ₀	r ₁	r ₂	r ₃	s ₁	s ₂	s ₃	s ₄
·	r ₀	r ₁	r ₂	r ₃	s ₁	s ₂	s ₃	s ₄
r ₀	R ₄ : rotations				reflections			
r ₁								
r ₂								
r ₃								
s ₁	reflections				rotations			
s ₂								
s ₃								
s ₄								

·	r ₀	r ₁	r ₂	r ₃	s ₁	s ₂	s ₃	s ₄
r ₀	r ₀	r ₁	r ₂	r ₃	s ₁	s ₂	s ₃	s ₄
r ₁	r ₁	r ₂	r ₃	r ₀				
r ₂	r ₂	r ₃	r ₀	r ₁	s ₂	s ₁	s ₄	s ₃
r ₃	r ₃	r ₀	r ₁	r ₂				
s ₁	s ₁		s ₂		r ₀	r ₂		
s ₂	s ₂		s ₁		r ₂	r ₀		
s ₃	s ₃		s ₄				r ₀	r ₂
s ₄	s ₄		s ₃				r ₂	r ₀

FIGURE 10. Rotations vs. reflections in D_4

Therefore, $r_0s, r_1s, r_2s,$ and r_3s are the *four distinct reflections* of the square, and our subgroup $R_4 \cup \{r_0s, r_1s, r_2s, r_3s\}$ of D_4 has expanded to include *all* 8 elements of D_4 . To paraphrase, there is no subgroup of D_4 strictly between the rotational subgroup R_4 and D_4 itself. \square

It is clear that $\{r_0\}$ (called the *trivial* or the *identity* subgroup) is the only subgroup of D_4 of size 1; and that the subgroups of size 2 consist of the identity r_0 plus a self-counteracting symmetry, i.e., these are $\{r_0, r_2\}$ and $\{r_0, s_j\}$ for any reflection s_j . The previous argument shows that once a subgroup K contains r_1 and some reflection s_j , then K contains everything, i.e., $K = D_4$. A similar argument can be applied to r_3 and any reflection s_j , since r_3 generates the rotational subgroup R_4 , just as r_1 does. Thus, the rotations in any *other* subgroup of D_4 are at most r_2 and r_0 (of course).



Now, if you complete the full multiplication table for D_4 , you will notice that r_2 is a very special element: it *commutes* with everything in D_4 , i.e., $r_2x = xr_2$ for all $x \in D_4$ (cf. Fig. 10b). In particular, if a subgroup K contains r_2 and some reflection s_j , then $r_2s_j = s_jr_2 = s_k$ for some other reflection s_k . Since $r_2^2 = s_k^2 = s_j^2 = r_0$, the identity, with some more work, one can manipulate the above equalities to also obtain that $r_2s_k = s_kr_2 = s_j$ and $s_js_k = s_k s_j = r_2$. In other words, $\{r_0, r_2, s_j, s_k\}$ already forms a subgroup of D_4 of order 4. There are two such subgroups of D_4 ; the pairs $\{s_j, s_k\}$



The Plan

←	→	↑	↓
MIX	RESET	EDIT	HELP
SOLVE	▶		

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

solving & beyond!

possible vs. impossible states

closed paths

as action group

15-puzzle

Part III

fund'l theorems:
even vs. odd permutations

Permutation

Groups

products of transpositions

2-row notation

1-row (cyclic) notation

Part II

Groups

examples:
action groups

intro definition

bits of theory & group "jargon"

Part I

✓



Action Groups (Lecture)

Worksheet 3: Cycles, Transpositions, Even and Odd Permutations¹

Date: 11/18/2020

MATH 74: Transition to Upper-Division Mathematics

with Professor Zvezdelina Stankova, UC Berkeley

Read: *Session 5: Introduction to Group Theory*. (vol. II)

- §4. General Groups. (pp. 110-111)
- §5. Some More Examples of Groups. (pp. 112-115)
- §6. Permutation (or Symmetric) Groups. (pp. 116-121)

Write: clearly. Supply your reasoning in words and/or symbols. Show calculations and relevant pictures.

- (Famous Groups)** Show that the sets below are groups under the given operation. ($S^* = S - \{0\}$)
 - $(\mathbb{Z}, +)$; (b) $(\mathbb{R}, +)$; (c) (\mathbb{R}^*, \cdot) ; (d) (\mathbb{C}^*, \cdot) ;
 - $(\mathbb{Z}_n, +) = \{0, 1, 2, \dots, n-1\}, +(\text{mod } n)$;
 Which are *cyclic*? With how many generators?*
- (Roots of Unity)** Let \mathcal{C}_n be the set of solutions to the equation $z^n = 1$ in complex numbers.
 - Prove that \mathcal{C}_n is a group under complex multiplication, and hence a subgroup of (\mathbb{C}^*, \cdot) .
 - What is the order of \mathcal{C}_n ? (*Hint:* Why doesn't $z^n - 1 = 0$ have repetitive roots? Write all roots.)
 - Show that \mathcal{C}_n is cyclic, generated by the primitive n th root of unity $\zeta_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$.
- (2-Row Notation)** Perform the given operations:
 - $\pi\rho$ and $\rho\pi$ where $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$;
 - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 1 & 2 & 6 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 4 & 1 & 3 & 5 \end{pmatrix}$;
 - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 1 & 5 \end{pmatrix}^{-1}$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 8 & 5 & 7 & 6 & 2 & 3 \end{pmatrix}^3$;
 - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 2 & 9 & 8 & 12 & 3 & 4 & 1 & 11 & 5 & 7 & 6 \end{pmatrix}^{-2}$.
- (1-Row Cycle Notation)** Calculate $(1342)(123)$ and $(1534269)^{-1}$. (*Hint:* Apply from right to left!)
- (Cyclic Properties)** Prove that every permutation can be written as a product of:
 - disjoint* cycles (i.e., w/ no common elements);
 - The order of the product of disjoint cycles is the lcm of the lengths of these cycles.
 - transpositions*; i.e., $(a_1b_1)(a_2b_2)\cdots(a_kb_n)$.
- (Even-Odd Balance)** For $n \geq 2$, prove that the function ξ sending any even permutation α to the product $\alpha \circ (12)$ is a 1-1 correspondence between the set E_n of even and the set O_n of odd permutations in S_n . How many *odd* permutations are there in S_5 ? Why? (*Hint:* Prove that $\xi(\alpha)$ is indeed odd and that $\xi : E_n \rightarrow O_n$ is 1-1 and onto.)
- (Roots Shake-&-Bake)** For which parameters a does $ax^2 + 2(a-1)x + 1 = 0$ have *only one* root? (*Hint:* $ax^2 + 2b_1x + c = 0$ likes the shortcut quadratic formula $r = \frac{-b_1 \pm \sqrt{b_1^2 - ac}}{a}$. But there is another catch!)

HW

Key Group Takeaways:

- **(Groups)** To show that a set $S \neq \emptyset$ is a *group* under an *operation* $*$ that sends $(s_1, s_2) \mapsto s_1 * s_2 \in S$ for any $s_1, s_2 \in S$, verify the *definition* of a group; i.e., for all $s, s_1, s_2, s_3 \in S$:
 - $*$ is *associative*: $s_1 * (s_2 * s_3) = (s_1 * s_2) * s_3$;
 - an *identity* element $e \in S$: $e * s = s * e = s$;
 - an *inverse* $s^{-1} \in S$: $s * s^{-1} = s^{-1} * s = e$;
 Or find a known group G under the same $*$ that contains S , and show that S is a *subgroup*:
 - S is *closed* under $*$: $s_1 * s_2 \in S \forall s_1, s_2 \in S$;
 - S contains the *inverses*: $s^{-1} \in S \forall s \in S$.
- **Permutations** can be written in 2-row and in cycle (1-row) notation, as product of disjoint cycles, and as a product of transpositions.
- An **even** permutation is one that can be written as the product of an even number of transpositions, and analogously for **odd** permutations. No permutation is both even and odd.
- The **order** of an element $g \in G$ is the min $n \in \mathbb{N}$ such that $g^n = e_G$, the identity in G .
- **Cycles** are permutations $(a_1a_2 \dots a_k)$. The order of the cycle is its length k .

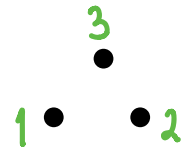
¹These worksheets are copyrighted and provided for the personal use of Fall 2020 MATH 74 students only. They may not be reproduced or posted anywhere without explicit written permission from Prof. Zvezdelina Stankova.

Part II Action Groups: Cycles, Transpositions

0.9 Permutations as Actions

P₁

(a) Set-up: $A = \{1, 2, 3\}$ = set of 3 elements



S_3 = the set of all $6 = 3!$ permutations of A → Think as: actions on $\{1, 2, 3\}$

① 2-Row notation: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ ← initial
 $= e$ = "do nothing" action ← result

P

transpositions:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_{12} = 1 \leftrightarrow 2$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau_{23} = 2 \leftrightarrow 3$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_{13} = 1 \leftrightarrow 3$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \rho = \begin{matrix} 1 \rightarrow 3 \\ 2 \rightarrow 1 \\ 3 \rightarrow 2 \end{matrix}$$

3-cycles

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \pi = \begin{matrix} 1 \rightarrow 2 \\ 2 \rightarrow 3 \\ 3 \rightarrow 1 \end{matrix}$$

transpositions:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

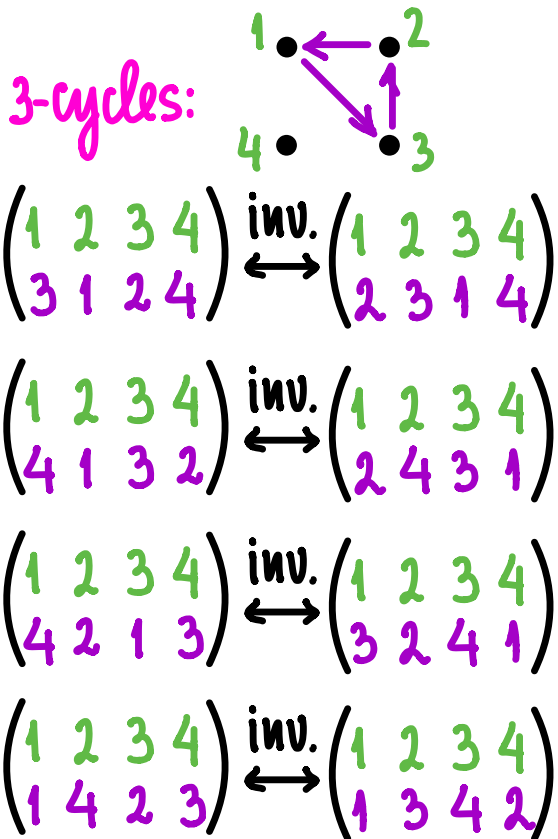
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Conclusion:

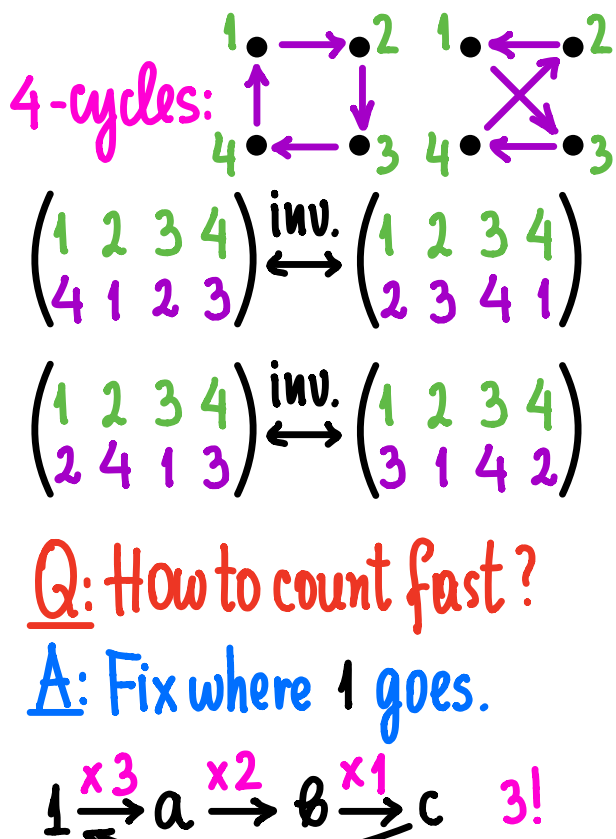
6 transpositions of 4 elements

P



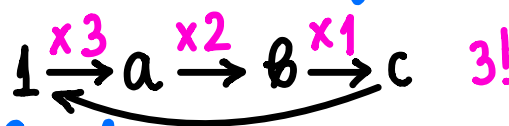
Conclusion:

8 3-cycles of 4 elements



Q: How to count fast?

A: Fix where 1 goes.



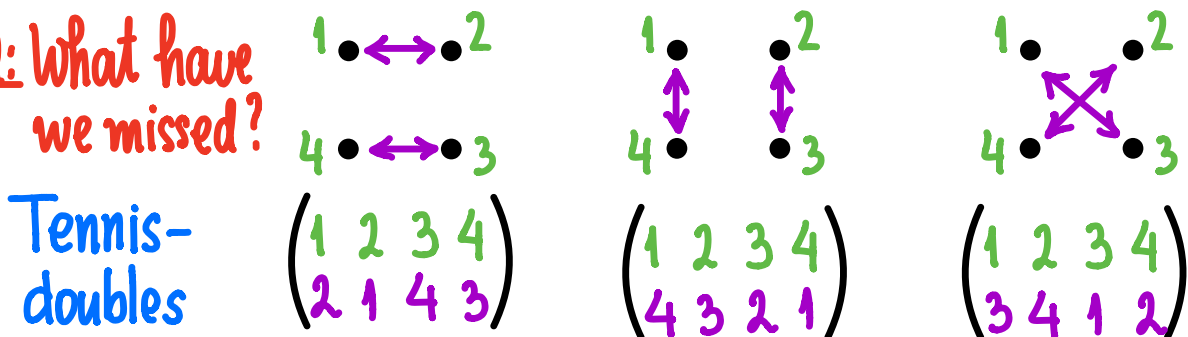
Conclusion:

6 4-cycles of 4 elements


⚠ Count so far for 4 elm's:

$6 + 8 + 6 + 1 + 3 = 4! = 24$
 transp. 3-cycles 4-cycles identity ? total

Q: What have we missed?

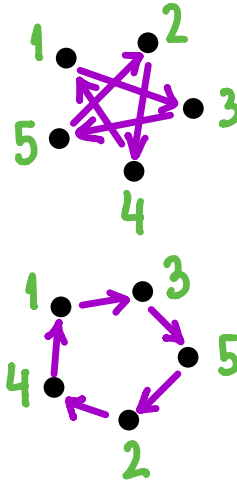


Summary: $S_4 =$ permutations of 4-elements

$a \leftrightarrow b$	transpositions (2-cycles)	$\binom{4}{2} = 6$	e	identity	1
$a \rightarrow b$ $d \leftarrow c$	4-cycles	$3! = 6$	$a \rightarrow b$ $c \rightarrow a$	3-cycles	$\binom{4}{3} \cdot 2 = 4 \cdot 2 = 8$
			$a \leftrightarrow b$ $c \leftrightarrow d$	pairings tennis doubles	 = 3

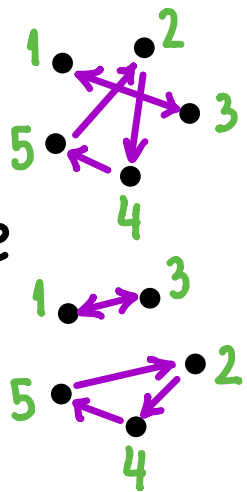
Ex. Describe in S_5 :

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$
 $a \xrightarrow{4} b \xrightarrow{3} c \xrightarrow{2} d \xrightarrow{1} e$
 5-cycles $4!$
24



$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$
 $a \xrightarrow{2} b \mid c \xrightarrow{4} d \xrightarrow{5} e$

2-cycle 10×2
20
 3-cycle
 disjoint cycles



Super-HW: Break S_5 ($5! = 120$ perm's) into subsets according to their cyclic structure:

Ex.

Describe

Classify

Count

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 4 & 1 & 3 & 5 & 2 \end{pmatrix}$
 $1 \rightarrow 7 \rightarrow 2 \rightarrow 6$
 $4 \leftarrow 3 \leftarrow 5$
 7-cycle!

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 2 \end{pmatrix}$
 $1 \circlearrowleft$ $2 \rightarrow 4$ $5 \circlearrowleft$
 $8 \leftarrow 6$ $7 \circlearrowleft$
 4-cycle

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 1 & 7 & 8 & 5 & 2 \end{pmatrix}$
 $1 \rightarrow 3 \rightarrow 6$
 $4 \leftarrow 2 \leftarrow 8$
 $5 \leftrightarrow 7$
 6-cycle
 transp.

③ 1-Row Cycle Notation

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_{12} = (12) \quad \text{(fix } \forall \text{ else)}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = (13524) \quad \text{5-cycle!}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) = (231)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (13)(245) \quad \heartsuit \text{ Disjoint cycles!}$$

Ex: Write as disjoint cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 1 & 2 & 6 & 7 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 4 & 1 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$


$$(13524)(6)(7) \cdot (175)(263)(4) = (1726534)$$

Conversely,

$$(2468)(341) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 5 & 6 & 7 & 8 \end{pmatrix}$$

\heartsuit Non-disjoint cycles! directly disjoint cycles

③.5 Back to: $S_4 =$ permutations of 4-elements

(ab)	transpositions (2-cycles)	$\binom{4}{2} = 6$	e	identity	1
			(abc)	3-cycles	$\binom{4}{3} \cdot 2 = 4 \cdot 2 = 8$
(abcd)	4-cycles	$3! = 6$	(ab)(cd)	pairings tennis doubles	 = 3