Previously in Math 103a:

Every permutation $\alpha \in S_n$ may be written as a product of 2-cycles

α is even if it is the product of an even # of 2-cycles

α is odd if it is the product of an odd # of 2-cycles

Every α is either even or odd, but not both

Products: Multiplication in S_n is composition

α even, β odd $\Rightarrow$ $\alpha\beta$ odd

α even, β even $\Rightarrow$ $\alpha\beta$ even

α odd, β odd $\Rightarrow$ $\alpha\beta$ even

Cycles: σ cycle

$|\sigma|$ odd $\Leftrightarrow$ σ even
$|\sigma|$ even $\Leftrightarrow$ σ odd

check it!

e.g. $(312) = (13)(12)$

$|(312)| = 3$ $\quad$ (312) even permutation

$A_n = \{\alpha \in S_n : \alpha \text{ even}\}$

Thm. $\boxed{|A_n| = \frac{n!}{2}}$, $n \geq 2$

Note that $\frac{n!}{2}$, $n \geq 2$ is an integer since $n!$ has a factor of 2

Pf of Thm: If X and Y are 2 finite sets for which $\exists$ i_1 & i_2

$$i_1 : X \longrightarrow Y \quad 1\text{-}1$$
$$i_2 : Y \longrightarrow X \quad 1\text{-}1$$

Then $\#(X) = \#(Y)$, where $\#(S)$ is the number of elements in a set S.

Let Odd_n be the odd permutations in S_n, so that $A_n \cup Odd_n = S_n$

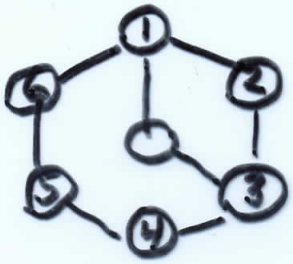
Since $|S_n| = n!$, to prove the Thm, need only show $\boxed{\#(A_n) = \#(Odd_n)}$

Let $i_1 : A_n \longrightarrow Odd_n$ given by $\alpha \longmapsto \alpha \circ (12)$ (even → odd)

$i_2 : Odd_n \longrightarrow A_n$ by $\beta \longmapsto \beta \circ (12)$ (odd → even)

Since $\gamma \circ (12) = \gamma' \circ (12) \Rightarrow \gamma = \gamma'$ (cancellation), i_1 & i_2 are 1-1 //

Now for some fun: Using knowledge of permutation groups to think about a puzzle.



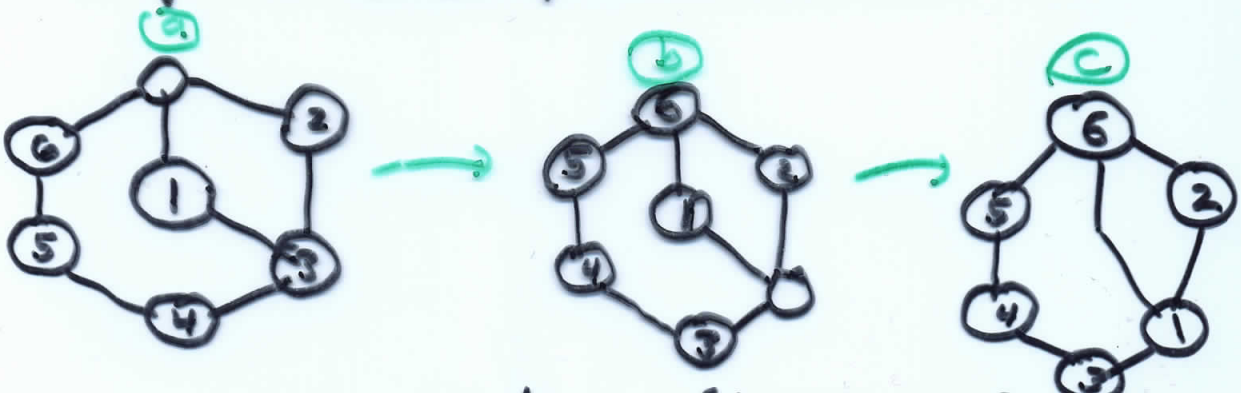
Moves are allowed along lines only into an empty space.

Can this figure be transformed into

?

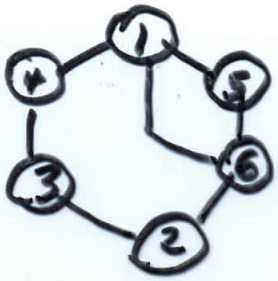
Idea: think of this as a 2-cycle interchanging 1 & 4. Thats an odd permutation.

Answer will be "No" if allowable moves lead only to even permutations.



permutation: $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{bmatrix} = (13456)$ even!

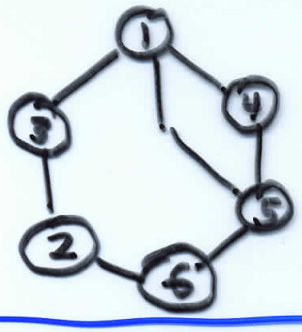
Another possibility from position (b) is to rotate clockwise into empty space & then put 1 back in its space.

e.g. 

corresponding to the permutation:

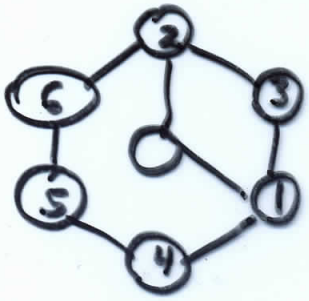
(2 4 6 3 5) also even!

other possibilities, rotate more before putting back 1 e.g.



(2 5 3 6 4) even!

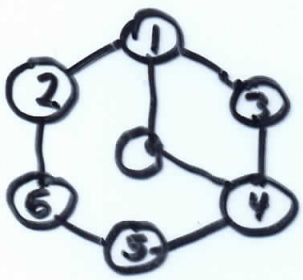
Another possibility: start with (a) and rotate counter-clockwise. Simplest is



(2 1 3) even!

from (a)

or: rotate counterclockwise ↑ and put 1 back

e.g. 

(2 6 5 4 3) even!

with much work, can check that no odd permutation is possible, but all even permutations are possible.

Application of permutation:

check digit scheme that detects all single digit errors & all transposition errors of adjacent digits, using no new symbols. (Verhoeff's scheme.)

Also: was once a secret formula!

used for a string of 10 digits

$a_1 a_2 a_3 \cdots a_{10}$

How to do it

Identify $\{0,1,2,\ldots,9\}$ with the 10 elements of D_5

$0,1,2,3,4 \longrightarrow$ rotations with $0 \longrightarrow$ identity

$5,6,7,8,9 \longrightarrow$ reflections

Want a permutation $\sigma \in S_{10}$ with property

$$\sigma^i(a) * \sigma^{i+1}(b) \neq \sigma^i(b) * \sigma^{i+1}(a) \quad (*)$$

if $a,b \in \{0,1,\ldots,9\}$, $a \neq b$,

where $*$ denotes group operation in D_5. Can take $\sigma = (0\,1\,5\,8\,9\,4\,2\,7)(3\,6)$

Now $\sigma(a_1) * \sigma^2(a_2) * \cdots * \sigma^9(a_9) * \sigma^{10}(a_{10})$ has an inverse in D_5. Call it a_{11}. This is check digit

Why it works: Condition (*) guarantees that if 2 adjacent digits are interchanged check digit will change. Since

$$\sigma^i(a) = \sigma^i(b) \Longrightarrow a = b$$

it follows that check digit will change also if exactly 1 digit is copied wrong.

Back to automorphisms.

Recall G group, $\varphi: G \to G$ isomorphism is called an automorphism.

Notation: $\mathrm{Aut}(G)$ = all automorphisms of G.

Let $a \in G$. Then $\varphi_a: G \to G$ $\varphi_a(x) = axa^{-1}$ is an automorphism (check it), called an inner automorphism. $\mathrm{Inn}(G)$ = all inner automorphisms.

Note: If G is abelian, the identity is the only inner automorphism.

Ex: $G = \left\{ \begin{pmatrix} c & b \\ 0 & c^{-1} \end{pmatrix} : b, c \in \mathbb{Q},\ c \neq 0 \right\} \subset SL(2, \mathbb{Q})$

Take $a = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}$, $x = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$

$$\varphi_a(x) = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c^{-1} & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} c & cy \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} c^{-1} & 0 \\ 0 & c \end{pmatrix}$$

$$= \begin{pmatrix} 1 & c^2 y \\ 0 & 1 \end{pmatrix}$$

Caution $\varphi_a = \varphi_b \not\Rightarrow a = b$

Thm: $Aut(G)$ & $Inn(G)$ are groups under composition.

Partial proof: $\varphi_1, \varphi_2 \in Aut(G)$

$\Rightarrow \varphi_1 \circ \varphi_2 : G \to G$ is 1-1 & onto

Check that $\varphi_1 \circ \varphi_2$ preserves group operation.

Let $a, b \in G$

$$(\varphi_1 \circ \varphi_2)(a \cdot b) = \varphi_1(\varphi_2(a \cdot b))$$

$$= \varphi_1(\varphi_2(a) \cdot \varphi_2(b)) \quad \varphi_2 \text{ is isom.}$$

$$= \varphi_1(\varphi_2(a)) \cdot \varphi_1(\varphi_2(b)) \quad \varphi_1 \text{ is isom}$$

$$= (\varphi_1 \circ \varphi_2)(a) \cdot (\varphi_1 \circ \varphi_2)(b)$$

An intriguing isomorphism!

Thm: $Aut(\mathbb{Z}_n) \approx U(n)$.

Recall that $U(n) = \{ k : 0 \le k \le n-1, \gcd(k, n) = 1 \}$