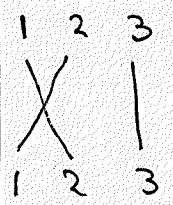
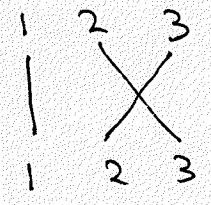
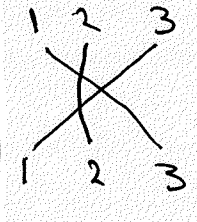
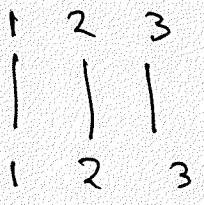
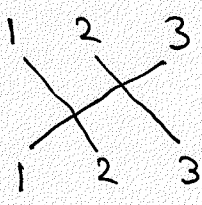
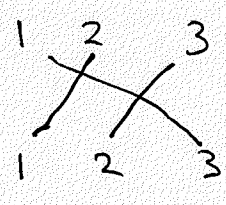
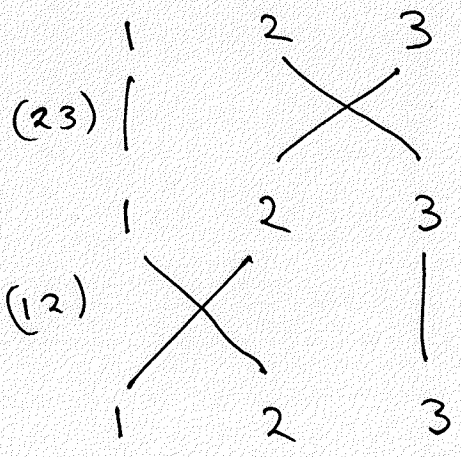
Elements of Perm($\{1,2,3\}$)

CYCLE NOTATION	(12)	(23)	(13)	$\mathbb{1}$	(123)	(132)
BRAID NOTATION						

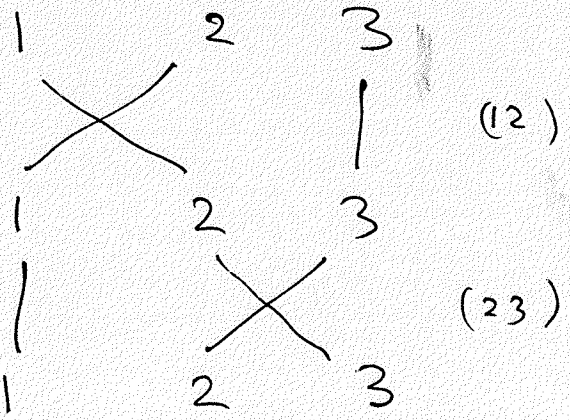
Some products... (remember these are "compositions of functions" so... Read right-to-left !!)

(12) (23)
↑ 2nd ↑ 1st

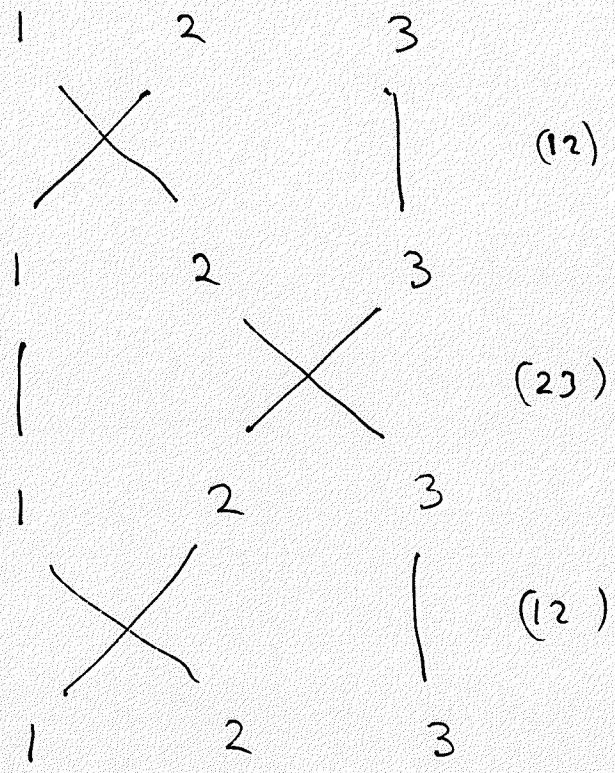


Ans (123)

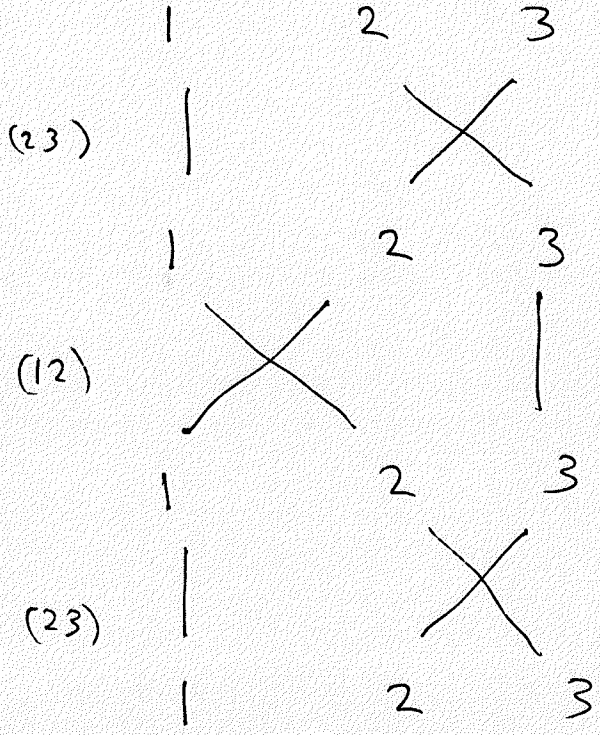
(23) (12)



Ans: (132)



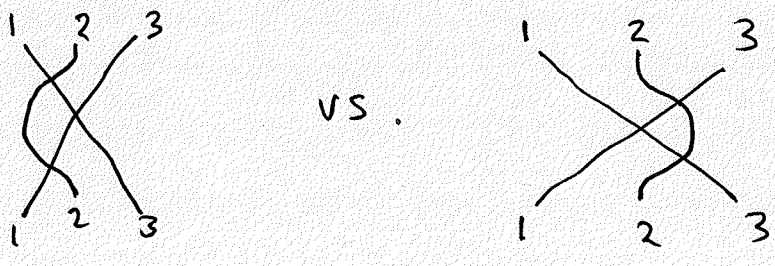
$(12)(23)(12) = (13)$



$(23)(12)(23) = (13)$

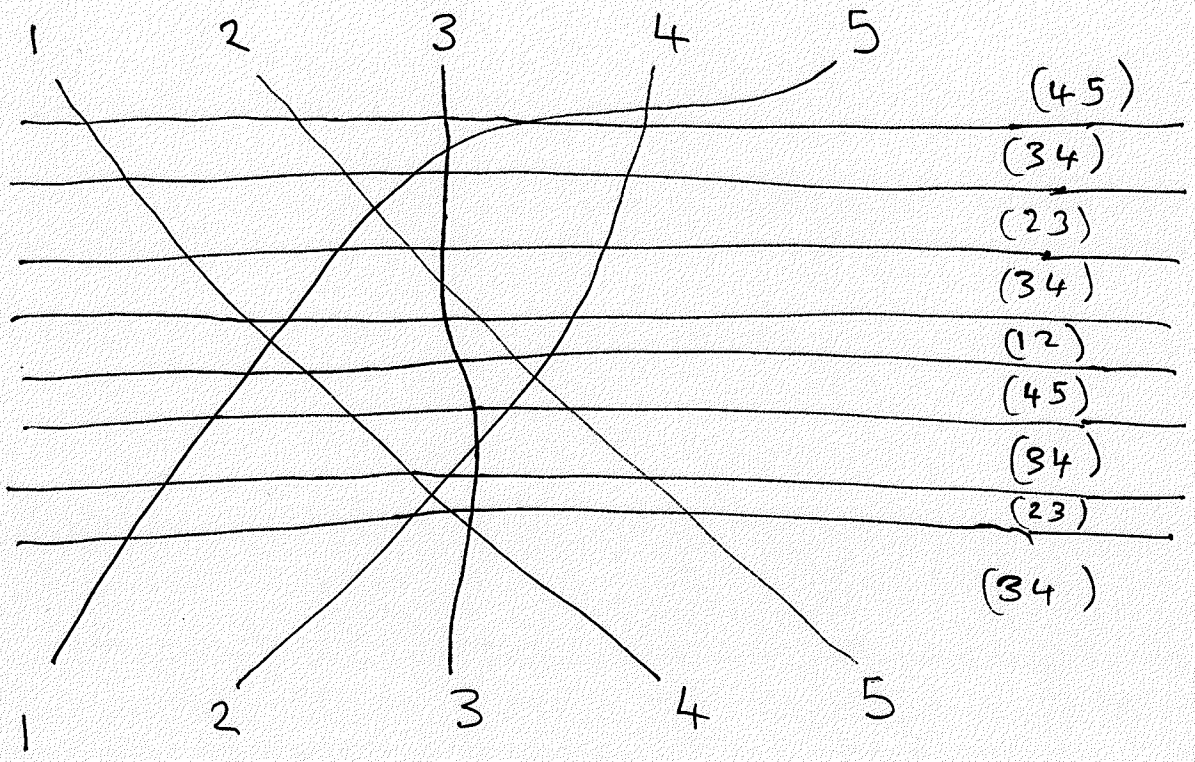
SAME result

Note diagrams look like the braid that switches 1 & 3 with the 2-to-2 strand on LHS of crossing or on RHS of crossing



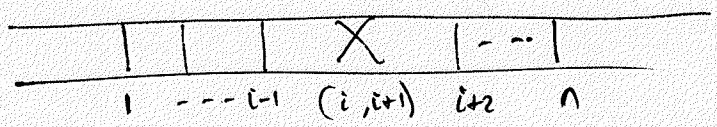
This suggests something really cool----

(1) Draw a "stretched out" braid diagram for some random permutation. eg. $(14\,25)$ in $\mathrm{Perm}(\{1,2,3,4,5\})$.



(2) Draw horizontal lines between crossings of braid strands; perturb crossing heights if necessary!

(3) Focus on narrow strip at a given level



It has one crossing of adjacent strands in positions $(i, i+1)$ at that level. Write this transposition down.

(4) Your original permutation is the product (composition) of these transpositions!

Read this way! ←

$$(14\,25) = (34)(23)(34)(45)(12)(34)(23)(34)(45)$$

Using this idea we can prove the following proposition about permutations.

Prop Every permutation in $\mathrm{Perm}(\{1, \dots, n\})$ can be expressed as the composition of transpositions of adjacent letters $(i, i+1)$. ▨

~~(Here is a def)~~

Note that the set $\mathrm{Perm}(\{1, \dots, n\})$ is closed under composition of functions. It also satisfies the following properties

(1) Composition is <u>associative</u>

$$f \circ (g \circ h) = (f \circ g) \circ h$$

for all $f, g, h \in \mathrm{Perm}(\{1, \dots, n\})$.

(2) there is an <u>identity</u> element $\mathbb{1} \in \mathrm{Perm}(\{1, \dots, n\})$

so that $\mathbb{1} \circ f = f \circ \mathbb{1} = f$ for all $f \in \mathrm{Perm}(\{1 \dots n\})$.

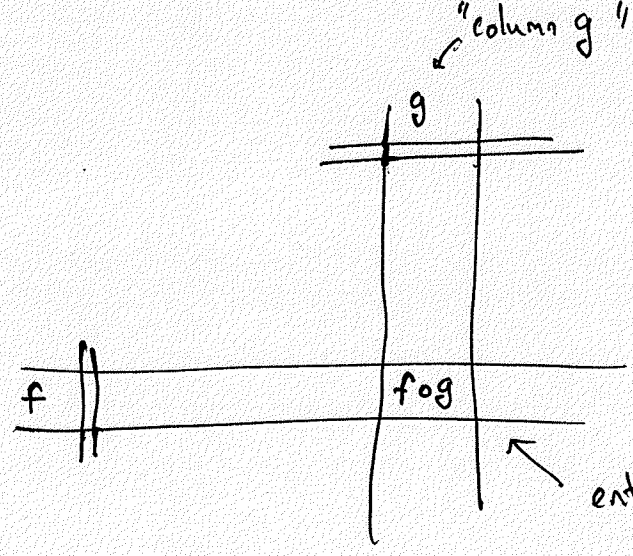
(3) there are <u>inverses</u>. For every $f \in \mathrm{Perm}(\{1, \dots, n\})$ there is an inverse $f^{-1} \in \mathrm{Perm}(\{1, \dots, n\})$ such that $f \circ f^{-1} = f^{-1} \circ f = \mathbb{1}$.

Here is the multiplication ("composition") table for $\mathrm{Perm}(\{1,2,3\})$

Multiplication table for $\mathrm{Perm}(\{1,2,3\})$

$\circ$	$\mathbb{1}$	(123)	(132)	(12)	(23)	(13)
$\mathbb{1}$	$\mathbb{1}$	(123)	(132)	(12)	(23)	(13)
(123)	(123)	(132)	$\mathbb{1}$	(13)	(12)	(23)
(132)	(132)	$\mathbb{1}$	(123)	(23)	(13)	(12)
(12)	(12)	(23)	(13)	$\mathbb{1}$	(123)	(132)
(23)	(23)	(13)	(12)	(132)	$\mathbb{1}$	(123)
(13)	(13)	(12)	(23)	(123)	(132)	$\mathbb{1}$

Notation →



In fact, this holds for any set A, (even infinite sets):

$\text{PERM}(A)$ satisfies the 3 properties above.

In math we say that $\text{Perm}(A)$ forms a group under composition. Here's the general definition.

Def: (GROUP) A group is a set G and a binary operation $\cdot : G \times G \longrightarrow G$ (which could be called "composition", "addition," "multiplication," etc depending on the situation) satisfying 3 properties:

(1) $\cdot$ is associative

$$(\forall g \in G)(\forall h \in G)(\forall k \in G)\ \left(g \cdot (h \cdot k) = (g \cdot h) \cdot k \right)$$

(2) there is an identity element for $\cdot$

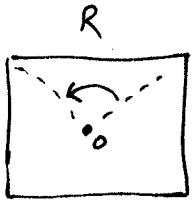
$$(\exists e \in G)(\forall g \in G)\ \left(e \cdot g = g \cdot e = g \right)$$

(3) every element of G has an inverse

$$(\forall g \in G)(\exists\ g^{-1} \in G)\ \left(g \cdot g^{-1} = g^{-1} \cdot g = e \right)$$

Occasionally you'll encounter two groups which are essentially the same (they are just disguised versions of each other).

For example the group of Rotational symmetries of the square  and the group $(\mathbb{Z}_4, +)$ are essentially the same!



R = Rotation about O through $\frac{2\pi}{4} = \frac{\pi}{2}$

$R^2 = R \circ R =$ π rotation

$R^3 = R \circ R^2 = \frac{3\pi}{2}$ rotation

$R^4 = R \circ R^3 = 2\pi$ rotation = identity $\mathbb{1}$.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$1+1 = 2$

$1+2 = 3$

$1+3 = 4 = 0$
= identity

$\circ$	$\mathbb{1}$	R	R^2	R^3
$\mathbb{1}$	$\mathbb{1}$	R	R^2	R^3
R	R	R^2	R^3	$\mathbb{1}$
R^2	R^2	R^3	$\mathbb{1}$	R
R^3	R^3	$\mathbb{1}$	R	R^2

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The multiplication tables look the same — we can "translate" (as in a dictionary between two languages) between those as follows

$$0 \longleftrightarrow +$$

$$\mathbb{R} \longleftrightarrow 1$$

$$\mathbb{R}^2 \longleftrightarrow 2$$

$$\mathbb{R}^3 \longleftrightarrow 3$$

$$\mathbb{1} \longleftrightarrow 0$$

Composition corresponds to +

R corresponds to 1

etc.

Formally, we say

<u>Def</u>: (Isomorphic Groups) Two groups $(G_1, \cdot)$ $(G_2, *)$ are <u>isomorphic</u> if there is a bijection between them:

$$f : G_1 \longrightarrow G_2,$$

which respects the G_1 and G_2 multiplications:

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2)$$

$\cdot$: mult^n on G_1

$*$: mult^n on G_2.

Here are some examples

eg (1) $\mathrm{Symm}(\triangle)$ and $\mathrm{Perm}(\{1,2,3\})$

eg (2) $(\{-1, 1\}, \times)$ and $(\mathbb{Z}_2, +)$

eg (3) $(\mathbb{Z}_5 - \{0\}, \times)$ and $(\mathbb{Z}_4, +)$

eg (4) $(\mathbb{R}^+, \times)$ and $(\mathbb{R}, +)$

$\exp : \mathbb{R} \longrightarrow \mathbb{R}^+$

$: x \longmapsto \exp(x) = e^x$

& inverse

$\log : \mathbb{R}^+ \longrightarrow \mathbb{R}$

$: x \longmapsto \ln(x)$

$e^{x+y} = e^x \cdot e^y$

add^n mult^n

$\ln(x \cdot y) = \ln(x) + \ln(y)$

mult^n add^n

"Rules of exponents" and "rules of logs" just say precisely that these bijections respect the operations of multiplication and addition.

A <u>subgroup</u> of a group $(G, \cdot)$ is a subset $H \subset G$ which is a group under the operation $\cdot$ inherited from G. We denote it by $H < G$

<u>eg(1)</u> $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$

<u>eg(2)</u> $(n\mathbb{Z}, +) < (\mathbb{Z}, +)$

<u>eg(3)</u> $\{1, (123), (132)\} < \text{Perm}(\{1,2,3\})$

<u>eg(4)</u> $\{1, (12)\} < \text{Perm}(\{1,2,3\})$

<u>eg(5)</u> $\{1\} < \text{Perm}(\{1,2,3\})$

<u>eg(6)</u> $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$

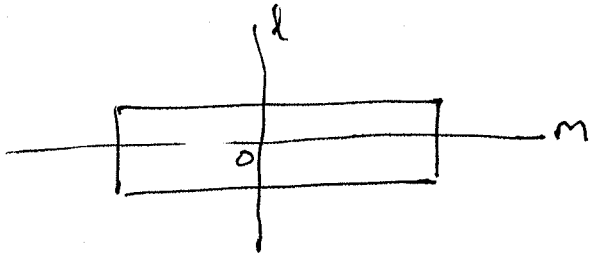
<u>eg(7)</u> $(\mathbb{R}^+, \times) < (\mathbb{R} - \{0\}, \times)$

<u>eg(8)</u> If G is any group, and $g \in G$ is any element the subset $\langle g \rangle \underset{\text{def}}{=} \{ g^n \mid n \in \mathbb{Z} \}$ is a subgroup of G.

Here are some cool results in group theory. The first says why people are interested in $\mathrm{Perm}(A)$.

Thm (Cayley) Every group is isomorphic to a subgroup of some $\mathrm{Perm}(A)$.

Proof Example first... $G = \mathrm{Symm}($ $)$



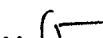
ℓ = reflection in ℓ $\quad$ M = reflection in m

R = rotation about o through π $\quad$ $\mathbb{1}$ = identity $= R^2$.

o	$\mathbb{1}$ (1)	R (2)	ℓ (3)	M (4)	
$\mathbb{1}$	$\mathbb{1}$	R	ℓ	M	← $\mathbb{1}$
R	R	$\mathbb{1}$	M	ℓ	← (12)(34)
ℓ	ℓ	M	$\mathbb{1}$	R	← (13)(24)
M	M	ℓ	R	$\mathbb{1}$	← (14)(23)

← Label the elements 1, ---, 4

Each row of the mult^n table gives a permutation of 1, —, 4

Cayley's claim: $\mathrm{Symm}($  $)$ is isomorphic to the 4-element subgroup $\{\mathbb{1}, (12)(34), (13)(24), (14)(23)\}$ of $\mathrm{Perm}(\{1,2,3,4\})$

Note that a given row of the mult^{n} table is obtained by multiplying all the elements of $\mathrm{Symm}(\square)$ on the left by a given element.

In general if G is a group, $g \in G$

then $L_g : G \longrightarrow G$

$: x \longmapsto L_g(x) \overset{\text{def}}{=} g \cdot x$

(1) is a bijection (with inverse $L_{g^{-1}}$)!

And the bijection

$$G \longrightarrow \{L_g \mid g \in G\} \subseteq \mathrm{Perm}(G)$$

(2) is an isomorphism between G and the subgroup

$$\{L_g \mid g \in G\} \text{ of } \mathrm{Perm}(G).$$

$\square$

Exercise verify (1) & (2)

↑

in class

Here's a very useful result about subgroups due to Lagrange.

Th^{m} (Lagrange) If G is a finite group and H a subgroup of G, then $|H| \mid |G|$.

eg $\{\mathbb{1}, (12)\} < \mathrm{Perm}(\{1,2,3\})$ $\quad 2 \mid 6$ ✓

$\{1, (123), (132)\} < \mathrm{Perm}(\{1,2,3\})$ $\quad 3 \mid 6$ ✓

$\{1, (12)(34), (13)(24), (14)(23)\} < \mathrm{Perm}(\{1,2,3,4\})$ $\quad 4 \mid 24$ ✓

Here's Lagrange's idea. Consider what happens when we multiply everything in H on the left by $g \in G$.

$$gH = \{gh \mid h \in H\}$$

$(23)\{\mathbb{1}, (12)\} = \{(23)\mathbb{1}, (23)(12)\} = \{(23), (132)\}$

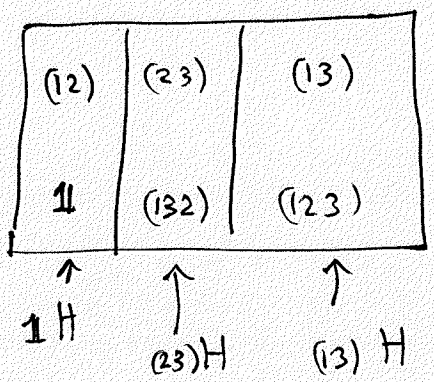
$(13)\{\mathbb{1}, (12)\} = \{(13)\mathbb{1}, (13)(12)\} = \{(13), (123)\}$

$\mathbb{1}\{\mathbb{1}, (12)\} = \longrightarrow = \{\mathbb{1}, (12)\}$

$\uparrow$

H

Note that these 3 sets divide all of Perm($\{1,2,3\}$) up evenly



and $b = 3(2)$
$= 3|H|.$

$\Rightarrow |H| \mid b$

This works in general ---- here's the key fact

$g_1 H$ and $g_2 H$ are either <u>disjoint</u> (empty intersection) or are <u>equal</u> (as sets).

↓

<u>Proof</u> Either $g_1 H \cap g_2 H = \emptyset \Rightarrow$ disjoint

<u>OR</u> $g_1 H \cap g_2 H \neq \emptyset$

↙

This means $\exists$ common element x (say)

$x = g_1 h_1$ for some $h_1 \in H$ --- since $x \in g_1 H$

and $x = g_2 h_2$ for some $H_2 \in H$ --- since $x \in g_2 H$.

But then $g_1 h_1 = g_2 h_2$

$\Rightarrow g_2^{-1}(g_1 h_1) = g_2^{-1}(g_2 h_2)$

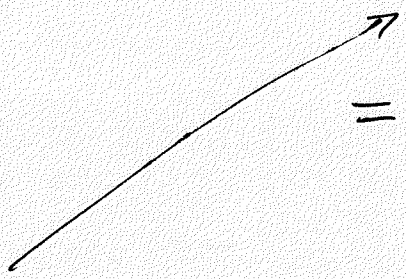
$$\Rightarrow (g_2^{-1} g_1 h_1) h_1^{-1} = (h_2) h_1^{-1}$$

$$\Rightarrow \quad g_2^{-1} g_1 = h_2 h_1^{-1}$$

This means $g_2^{-1} g_1 H = L_{g_2^{-1} g_1}(H)$

$$= L_{h_2 h_1^{-1}}(H)$$

$$= H$$



Note • H a subgroup & $h_1 \in H \Rightarrow h_1^{-1} \in H$

• H a subgroup & $h_1^{-1}, h_2 \in H \Rightarrow \underline{h_2 h_1^{-1} \in H}$

Therefore Left multiplication by $h_2 h_1^{-1}$ will just permute all the elements of H around (just Cayley's argument!) and so

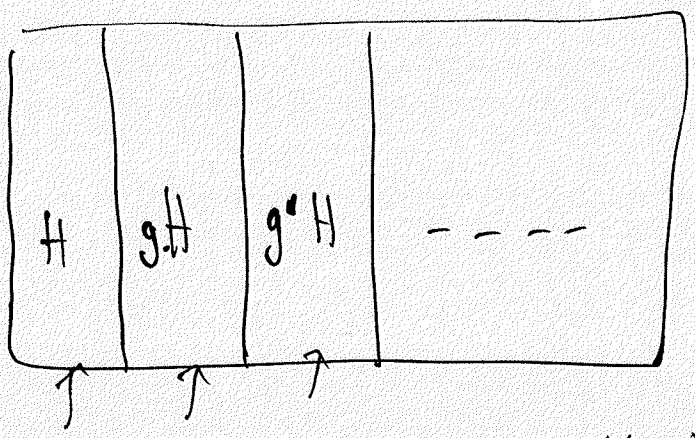
$$L_{h_2 h_1^{-1}}(H) = H$$

Thus $g_2^{-1} g_1 H = L_{h_2 h_1^{-1}}(H) = H$

$$\Rightarrow \quad g_2 (g_2^{-1} g_1 H) = g_2 (H)$$ ... This is equality of sets!

$\Rightarrow g_1 H = g_2 H$

i.e. if $g_1 H$ and $g_2 H$ have nonempty intersection, they must be equal!



disjoint translates cover all of G

$\Rightarrow$ since each gH has the same cardinality as H (because $L_g : H \longrightarrow gH$ is a bijection)

we have $|G| = |H| + |gH| + |g'H| + \cdots$

$= |H| + |H| + |H| + \cdots$

$=$ multiple of $|H|$.

∎

Orders of elements:

Suppose G is a finite group, and $g \in G$.

Then the elements $\{g, g^2, g^3, g^4, \ldots\}$ can't all be distinct, because G is finite!

$$\Rightarrow g^m = g^n \quad \text{for some } m, n \in \mathbb{N}. \quad (\text{say } m < n)$$

$$\Rightarrow g^m g^{-m} = g^n g^{-m}$$

$$\Rightarrow e = g^{n-m}$$

So we have found a positive power of g which gives e.

The order of g ($\text{ord}(g)$) is the smallest positive power of g which gives e.

$$\langle g \rangle = \{g^m \mid m \in \mathbb{N}\}$$ has size $\text{ord}(g)$,

and is a subgroup of G.

By Lagrange's Theorem

$$\text{ord}(g) = |\langle g \rangle| \mid |G|$$

$$\boxed{\text{ord}(g) \mid |G|}$$

$\text{Perm}(\{1,2,3,4\}) = 24$

eg (1234) has order 4 $\quad 4 \mid 24$

(123) has order 3 $\quad 3 \mid 24$

(24) has order 2 $\quad 2 \mid 24$

$5! = |\text{Perm}(\{1,2,3,4,5\})|$

eg $(123)(45)$ has order 6 $\quad 6 \mid 120$

(12345) has order 5 $\quad 5 \mid 120$

---

eg We have seen that if p is a prime number, then $(\mathbb{Z}_p - \{0\}, \times)$ is a group.

→ $\mathbb{Z}_p - \{0\}$ has $p-1$ elements

→ if $a \in \mathbb{Z}_p - \{0\}$ then

$$\text{ord}(a) \mid |\mathbb{Z}_p - \{0\}|$$

$$\text{ord}(a) \mid (p-1)$$

Look at specific examples in class

$\Rightarrow a^{p-1} =$ identity in $(\mathbb{Z}_p - \{0\}, \times)$

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow a^p \equiv a \pmod{p}$

Also $0^p \equiv 0 \pmod{p}$

Therefore, for all residues $a \in \{0, \ldots, p-1\}$ we have seen

$$a^p \equiv a \pmod{p}$$

$\Rightarrow$ for all integers m

$$m^p \equiv m \pmod{p}$$

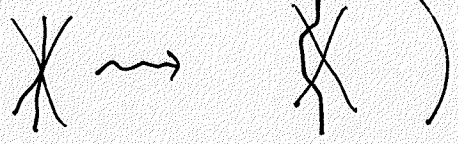
OR

$$p \mid (m^p - m) \qquad \text{for all integers } m.$$

Think back on our case-by-case proofs of this fact for $p=5$, $p=7$, $p=11$, etc...!

This example shows you the power of Lagrange's Theorem!

Misc. cool results about permutations

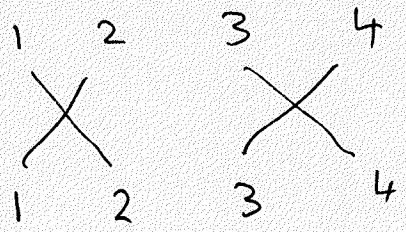
Sign Given a permutation $f \in \mathrm{Perm}(\{1, \ldots, n\})$, write down a braid picture for f. Count the number of crossings "$\times$" of braid strands (making sure to perturb any triple intersections or higher )

Define

$\mathrm{sign}(f) \equiv$ number of crossings $\pmod 2$.

---

eg $(12)(34)$

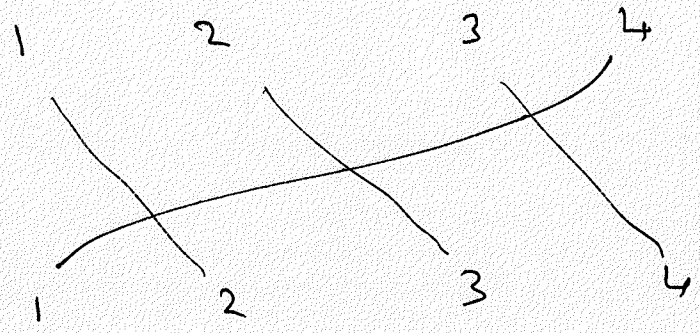


$\mathrm{sign}\big((12)(34)\big) = 2 \pmod 2$

$\equiv 0 \pmod 2$.

$\mathrm{sign}\big((12)(34)\big) = 0$

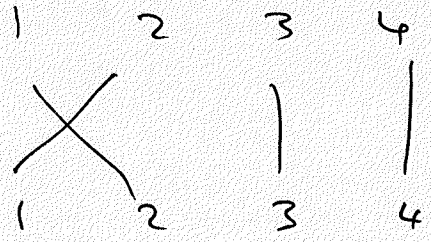
eg $\text{sign}\ (1\,2\,3\,4) = 3 \pmod 2 \equiv 1 \pmod 2$



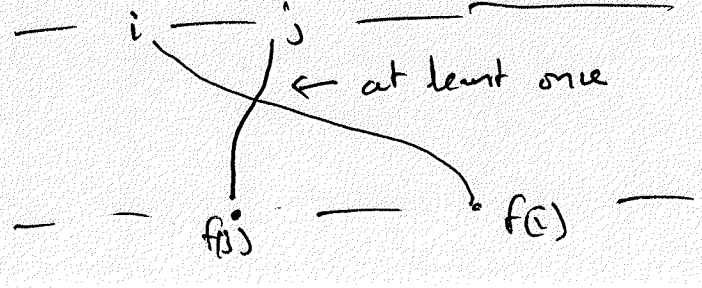
$\text{Sign}\ (1234) = 1$

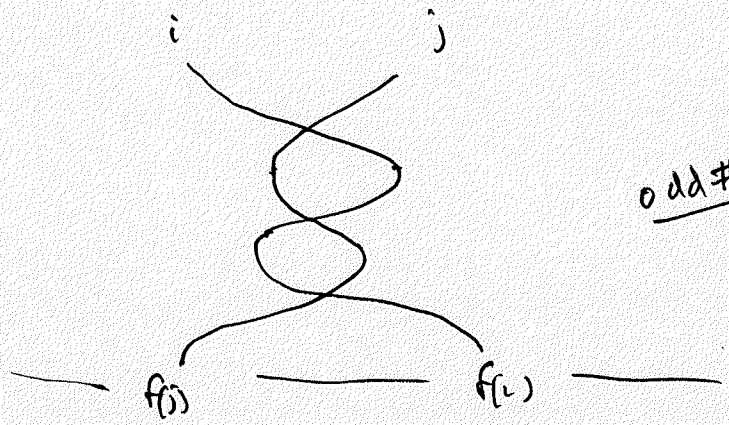
---

eg $\text{Sign}\ ((12)) = 1$



Note It does it matter how you draw the braided strands → The key fact is if $i < j$ yet $f(i) > f(j)$ then the i & j strands (counted at the top) will have to cross at least once, & will have to cross an odd number of times



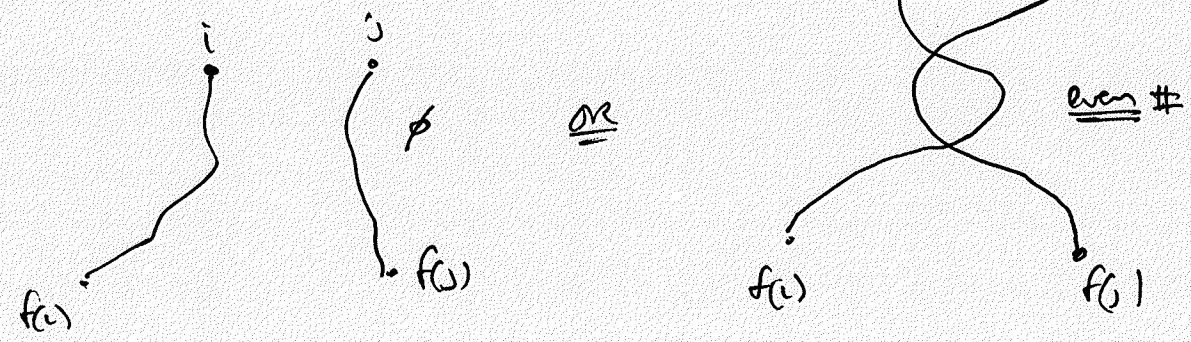


Key observation the $(j, f(j))$ – strand has to cross from the right side of the $(i, f(i))$ – strand to the left side of this strand. Therefore it must cross an odd number of times! $\equiv 1 \pmod 2$.

If $i < j$ & $f(i) < f(j)$

then the ~~strand~~ $(j, f(j))$ strand has to endup on the right side of the $(i, f(i))$ strand. $\Rightarrow$ it crosses 0 times OR must cross an even # of times

$\equiv 0 \pmod 2$

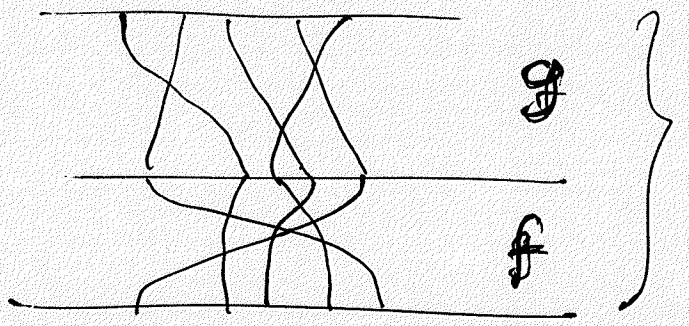


So here is another way to define sign(f).

$$\text{sign}(f) = \left(\begin{array}{l}\text{number of pairs } i<j \\ \text{so that } f(i) > f(j)\end{array}\right) \pmod 2.$$

Properties of sign

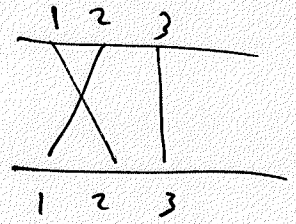
(1) $\text{Sign}(f \circ g) = \text{sign}(f) + \text{sign}(g) \pmod 2$



add crossings to get the (Mod 2) count for $f \circ g$

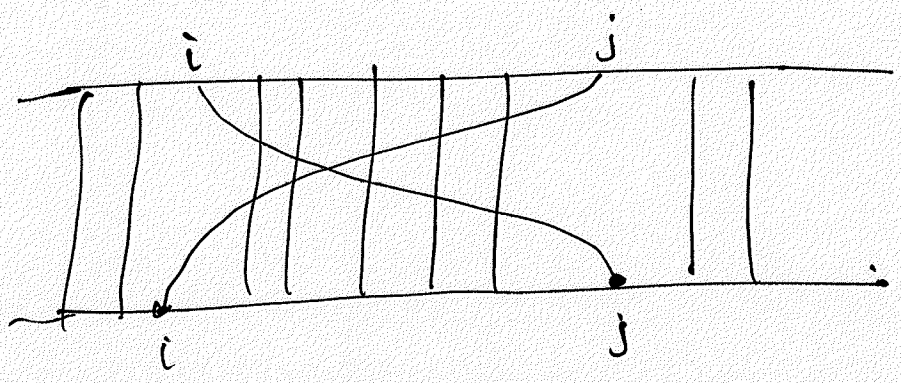
(2) Sign (transposition) = 1

eg



sign (12) = 1 is easy!

In general ---→



(ij)

The i & j strands cross once.

each i & j strands cross all the strands in the middle $(j-i-1)$ of them.

So # crossings $= 1 + 2(j-i-1)$

$\equiv 1 \pmod 2$ ∎

Applications of sign.

① permutations with sign $= 0$ form a subgroup called the Alternating group, A_n

$A_n < \text{Perm}(\{1, \ldots, n\})$

A_n has $\frac{n!}{2}$ elements.

eg $n=3$ $\quad A_3 = \{1, (123), (132)\}$

$n=4$ $\quad A_4 = \{1, (123), (124), (134), (132), (142), (143)$
$(234), (243), (12)(34), (14)(23), (13)(24)\}$

(2) Determinants

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

(2 terms, $2 = 2!$)

↑ Hmm---!?

↓

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}$$

(6 terms, $6 = 3!$)

↓ generalization??

permutations and their signs give the general definition of determinant.

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

eg $n=2$ $\quad \mathrm{Perm}(\{1,2\}) = \{\mathbb{1}, f\}$, $f = (12)$

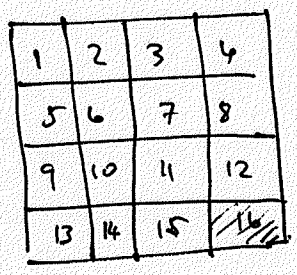
$\mathrm{sign} = 0$ for $\mathbb{1}$, $\mathrm{sign} = 1$ for f

$$\det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = (-1)^0 a_{11}a_{22} + (-1)^1 a_{12}a_{21}$$

$\mathbb{1}(1)=1$, $\mathbb{1}(2)=2$, $f(1)=2$, $f(2)=1$

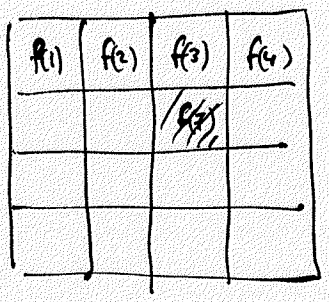
Yes!!

The 15-puzzle.



Unscrambled puzzle

Scrambled puzzle



← eg $f(7) = 16$

Comes with a permutation $f \in \text{Perm}(\{1, \ldots, 16\})$

telling you that square $f(i)$ is now in position i

There is also an integer n telling you how many slides moves the empty square is from its original position (position 16).

Claim $\quad \text{sign}(f) + n \pmod 2$

is an invariant of a slide move.

(in class proof)

Consequence There are two classes of scrambled 15 puzzles — ones which can be solved. (0) ; and ones which can't (1) invar. invar.