We study a wide range of techniques from ALGEB
to answer questions about objects that are COMBINATORIAL, DISCRETE ...

Some examples:

1) How many distinct necklaces can be made from 3 black beads and 13 white beads?

2) How many ways can the faces of a cube be colore so that there are two red faces, one white face, three blue?

3) How many "symmetries" does the dodecahedron have?

4) How many magic squares, latin squares of size $n \times n$ are there?

5) 15 - Puzzle

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

can you move $\rightsquigarrow$ to

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

So we look to COUNT, show EXISTENCE, and sometimes Find OPTIMAL configuration among a (Huge) finite set of possibilities.

PERMUTATIONS: Let $[n] = \{1, 2, \dots, n\}$ then a permutation is a function that is one-to-one and surjective. The set of all permutations is S_n. $\sigma : [n] \longrightarrow [n]$ can be reprasented as a table function

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$$

or as a list or rearrangement $[3\,6\,5\,2\,1\,4] = \sigma$

Here position j of i indicatas $\sigma(j) = i$

Ex: $\sigma(2) = 6$.

Functions can be composed, then we define the "multiplication" of permutations α, β $\beta \cdot \alpha(i) = \beta(\alpha(i))$

Ex:
$$\alpha \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

$$\beta \cdot \alpha \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 5 & 1 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 1 & 1 & 3 & 1 \end{pmatrix}$$

Lemma: $|S_n| = n!$, in fact S_n is a GROUP:

i) if $\pi, \sigma \in S_n \Rightarrow \pi \cdot \sigma \in S_n$

ii) For any $\pi, \sigma, \tau \in S_n$ $(\pi\sigma)\tau = \pi(\sigma\tau)$

iii) The identity permutation is a permutation and $id \cdot \sigma = id \cdot \sigma = \sigma$

iv) Each $\pi \in S_n$ has an inverse $\pi^{-1} \in S_n$ such that $\pi \cdot (\pi^{-1}) = \pi^{-1} \cdot \pi = id$.

S_n is called the SYMMETRIC group

There is a third representation of permutations. Let us motivate with a puzzle

EXAMPLE: A card game: Twelve cards are laid out on a table

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

$\rightarrow$ Then they are picked by row order and redealt in same 3x4 array but by columns $\rightarrow$

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

Question: How many times must this shuffle be repeated before cards reappear in the original position?

ANSWER: Keep track of where cards go!

1, 12 remain fixed

$2 \to 5 \to 6 \to 10 \to 4 \to 2$ ↙ Creates a cycle that repeats itself after 5 times

Shuffle has permutation $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 & 11 & 4 & 8 & 12 \end{pmatrix}$

Its cycle decomposes as

$$(1)\,(2,5,6,10,4)\,(3,9,11,8,7)\,(12)$$

So repeating five times is enough to be back to original position.

Lemma: Every permutation decomposes as the product of cycles that have disjoint elements

Proof: Every permutation π has smallest power K such that $\underbrace{\pi \cdot \pi \cdot \pi \cdots \pi}_{K \text{ time}} = id$ (by finiteness of S_n)

to do the cycle decomposition start with a symbol (say 2) trace effect of π on its successors until we reach symbol 2 again.
These symbols form a cycle.
- choose a new symbol not present in a cycle so far
- repeat procedure until symbols are all touched

Clearly LCM (cycle lengths) = smallest power K $\pi^K = id$.

this is the ORDER of π.

WE WANT TO COUNT PERMUTATIONS OF DIFFERENT KINDS !!

WE WILL DO THIS DURING THE WHOLE COURSE

NOTATION: $\binom{n}{j}$ = # of subsets of cardinality j in an n element set.

$$\binom{n}{j} = \frac{n!}{(n-j)!\,j!} \qquad \binom{5}{2} = 6$$

why? (Easy to prove using induction and $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$)

PROBLEM (ANGRY SECRETARY): A secretary is angry with her boss. To show her anger she inserts n letters in envelopes with addresses and postage without paying attention possibly inserting the wrong letter in a envelope.

What is the probability that she put <u>every</u> letter in an incorrect envelope?

<u>Definition</u>: A permutation with the property $\pi(i) \neq i$ for all $i \in \{1, 2, \dots n\}$ is called a DERANGEMENT

How many derangements are there in S_n?

Theorem (INCLUSION-EXCLUSION Principle) For any sets $B_1, B_2, \dots, B_s$ finite sets (not necessarily disjoints)

$$|B_1 \cup B_2 \cup \dots \cup B_s| = \sum_{i=1}^{s} |B_i| - \sum_{\{i,j\}} |B_i \cap B_j| + \sum_{\{i_1, i_2, i_3\}} |B_{i_1} \cap B_{i_2} \cap B_{i_3}|$$

$$\dots (-1)^k \sum_{\underbrace{\{i_1, \dots, i_k\}}_{k\text{-tuples}}} |B_{i_1} \cap \dots \cap B_{i_k}| + \dots + (-1)^s |B_1 \cap \dots B_s| \qquad ☺$$

<u>proof</u>: Take $x \in B_1 \cup \dots \cup B_s$.

If x belongs to $B_{i_1}, \dots, B_{i_r}$ How many times was x counted in ☺?

x is counted ONCE in the size r intersection

x is counted r times in size $(r-1)$ intersections

THUS x is counted $\binom{r}{j}$ times in size j intersections.

therefore x is counted a TOTAL OF...

☆ $\binom{r}{1} - \binom{r}{2} + \binom{r}{3} - \cdots + (-1)^r \binom{r}{r}$

↑ contribution of x to Right hand side eqration.

Now using $\binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r}$

☆ becomes

$$\left\{\binom{r-1}{0} + \binom{r-1}{1}\right\} - \left\{\binom{r-1}{1} + \binom{r-1}{2}\right\} + \left\{\binom{r-1}{2} + \binom{r-1}{3}\right\}$$

$$- \cdots (-1)^r \cdot \binom{r}{r} = \binom{r-1}{0} + (-1)^{r-1}\binom{r-1}{r-1} + (-1)^r \binom{r}{r}$$

$$= 1 + (-1)^{r-1} + (-1)^r = \underline{1}$$

$\Rightarrow$ Each $x \in B_1 \cup \cdots \cup B_s$ is counted <u>ONCE</u> on the ~~left~~ RHS equation !!! ...

Now we apply this to counting derangements

Let $A_j = \{\pi \in S_n \mid \pi(j) = j\}$ consider

$$\alpha_r = \sum |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}|$$

$\{i_1, \ldots i_r\}$ runs over all r-subsets

What is the value of α_r ? Easy !

- CHOOSE SET OF "FIXED" guys $\{i_1, \ldots, i_r\}$ $\binom{n}{r}$ ways to do it.
- remaining $(n-r)$ can be permuted in any way ! $(n-r)!$

- The two decisions are done independently

$$\Rightarrow \alpha_r = \binom{n}{r}(n-r)! = \frac{n!}{r!}$$

Corollary: Using INCLUSION-EXCLUSION PRINCIPLE we know

$$|A_1 \cup \cdots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \cdots (-1)^n \alpha_n$$

$$= n! - \frac{n!}{2!} + \frac{n!}{3!} - \frac{n!}{4!} + \cdots + (-1)^n \frac{n!}{n!}$$

$$\Rightarrow \# \text{Derangements} = n! - \left(n! - \frac{n!}{2} + \frac{n!}{3} + \cdots + (-1)^n\right)$$

$$= \frac{n!}{2} - \frac{n!}{3} + \frac{n!}{2} \cdots + (-1)^{n+1}$$

NOTICE that that given a permutation π, its cycle decomposition partitions the set $\{1, 2, \ldots, n\}$

Definition: A partition of a set X is a family of non-empty subsets $\{Y_i \mid i \in I\}$ such that

i) $X = \bigcup_{i \in I} Y_i$, (ii) $Y_i \cap Y_j = \phi$

Definition: The type of a permutation π is the Expression $[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$ where α_i is the number of cycles of length i in π

Example: $\pi = (1,2,3)(7,8)(4)(5)(6)$

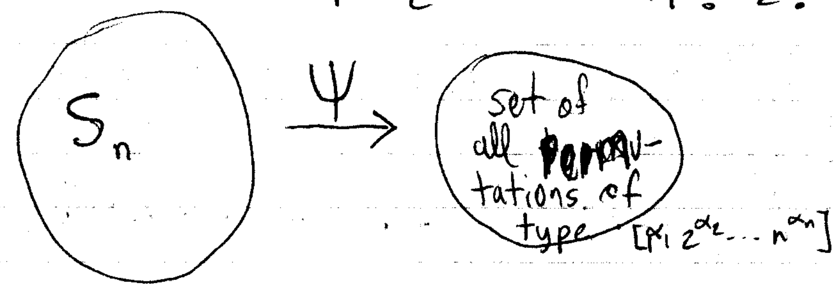
has type $1^3 2^1 3^1$

HOW MANY PERMUTATIONS are there of type $[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$??

Theorem: # of S_n permutations of type $[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$ is

$$\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n} \alpha_1! \alpha_2! \cdots \alpha_n!}$$

proof:



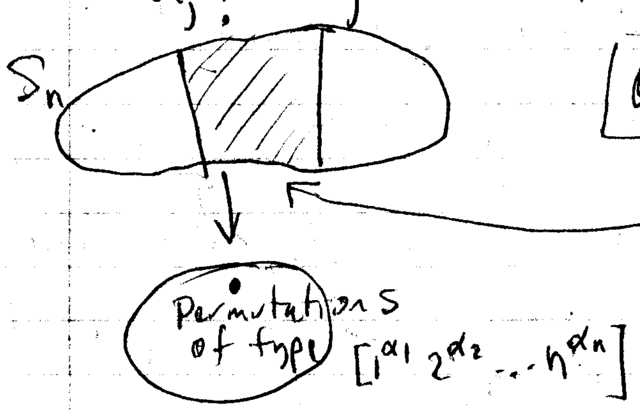
$$\pi(1)\pi(2)\cdots\pi(n) \longmapsto (\pi(1)\pi(2)\,(\cdots)\cdots(\cdots\pi(n))$$

We put the symbols into brackets.

Clearly this map is surjective.
Now this map is not injective!! How many $\pi \in S_n$ map to same cycle decomposition?

1) $(\underbrace{* * \cdots *}_{i\text{-cycle}})$ inside any i-cycle we can shift and make any of the i symbols to be first (i ways to choose who is first)

2) The order in which we put the j-cycles is irrelevant for the purpose of map Ψ
$\alpha_j!$ ways to order them



$\boxed{\alpha_1!\, \alpha_2! \cdots \alpha_n!\; 1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}}$

Cardinality of $\Psi^{-1}(\pi)$

π permutation of type $[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$

Definition: We say two permutations α, β are conjugate if there exist another permutation σ, such that $\sigma \alpha \sigma^{-1} = \beta$ or equivalently $\sigma\alpha = \beta\sigma$

Question: Can two conjugate permutations have different type??

NO!

Theorem: Two permutations α, β have the same type if and only if they are conjugate.

Proof: for each k-cycle of α we can use $\sigma\alpha = \beta\sigma$ to recover a k-cycle of β:

$$\begin{tikzcd} x_1 \arrow[r, "\alpha"] & x_2 \arrow[r, "\alpha"] & x_3 \arrow[r, "\alpha"] & \cdots & x_r \arrow[llll, bend left, "\alpha"] \end{tikzcd}$$

$$\begin{tikzcd} x_1 \arrow[r, "\alpha"] \arrow[d, "\sigma"'] & x_2 \arrow[r, "\alpha"] \arrow[d, "\sigma"] & x_3 \arrow[r] \arrow[d, "\sigma"] & \cdots \\ y_1 \arrow[r, "\beta"'] & y_2 \arrow[r] & y_3 \arrow[r] & \cdots \end{tikzcd}$$

$\Rightarrow$ if $\sigma\alpha = \beta\sigma \Rightarrow$ they have the same type

Now conversely suppose α, β have the same type. How to find σ?

Example: $(1\,3\,6\,2\,4)\ (5\,8\,7)\ (9) = \alpha$
$(1\,5\,8\,6\,2)\ (3\,9\,4)\ (7) = \beta$

WHAT is the natural thing to do?

set-up bijection by aligning cycles of similar sizes!

$$\begin{array}{ccccccccccc} 1&3&6&2&4, & 5&8&7, & 9 \\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow & \downarrow&\downarrow&\downarrow & \downarrow \\ 1&5&8&6&2, & 3&9&4, & 7 \end{array}$$

We get (in example) a permutation
$\sigma = (1)(268974)(35)$ which does the job!

NOTE: σ is not unique.
But this the general way of constructing it.

WE saw permutations are always products of cycles

Definition: A permutation that interchanges two symbols only and leaves the rest unaltered is a TRANSPOSITION (it has type $[1^{n-2}2^1]$

Lemma: Every cycle $(x_1, x_2, \ldots x_{r-1}, x_r)$ can be written as a product of transpositions
$(x_1 x_r)(x_1 x_{r-1})(x_1 x_{r-2}) \ldots (x_1 x_3)(x_1 x_2)$

proof: checking this by ~~[illegible]~~ element element

The only difficult one is $x_r \to x_1$ but this can be seen as consecutive exchanges

$x_1 \; x_2 \; x_3 \; \ldots \; x_{r-1} \; x_r$

$x_2 \; x_1 \; x_3 \; \ldots$

$x_2 \; x_3 \; x_1 \; \ldots \; x_{r-1} \; x_r$

$\vdots$

$x_2 \; x_3 \; x_4 \; \ldots \; x_1 \; x_r$

Corollary: Every permutation can be written as the product of transpositions.

WARNING: Decomposition is not always unique!

$(16)(13)(27)(25)(24) = (15)(35)(36)(57)(14)(27)(1$

Definition: For a permutation of type $[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$ let $C(\pi) = \alpha_1 + \alpha_2 + \cdots + \alpha_n = \#$ of disjoint cycles

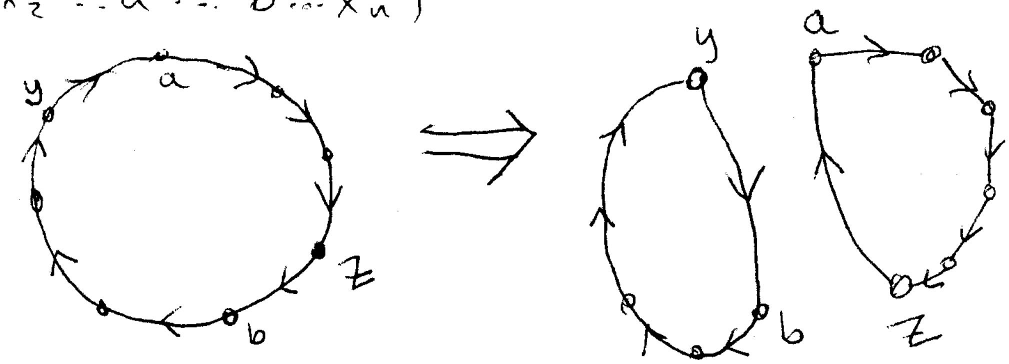
Question: What is the relation between $C(\tau\pi)$ and $C(\pi)$ for τ a transposition?

ANSWER: It changes the # of cycles by one (it either adds a cycle or removes a cycle)

proof: Suppose $\tau(a) = b$, $\tau(b) = a$

Case 1 Both a, b are in the same cycle of π

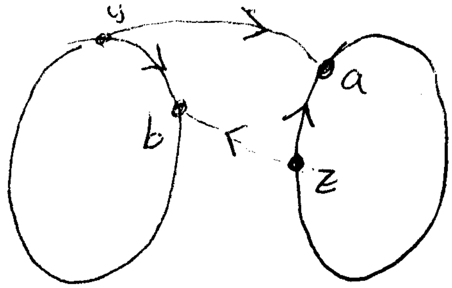
$(x_1\, x_2 \ldots a \ldots b \ldots x_n)$



$\tau\pi(x_i) = \pi(x_i)$ for $x_i \neq y, z$

$\tau\pi(y) = \tau(a) = b$, $\tau\pi(z) = \tau(b) = a$

Case 2: suppose a, b are **in different** cycles



$\tau\pi(y) = \tau(b) = a$

$\tau\pi(z) = \tau(a) = b$

cycles get glued when we apply a transposition!

Theorem: Every two decompositions of a permutation into transpositions have the same parity, namely if

$$\pi = \tau_r \tau_{r-1} \cdots \tau_2 \tau_1 = \sigma_s \sigma_{s-1} \cdots \sigma_2 \sigma_1$$

where τ_i, σ_j are permutations

$\Rightarrow r, s$ are both **even or** both odd.