Math 546
Set 7
Permutations
Permutations

**Sym.** A permutation of a set $A$ is a 1-1 + onto fn. from $A$ to $A$.

The set of all perms. of a set $A$ is denoted by $\mathfrak{S}(A)$ or $\mathfrak{S}(A)$ or $\text{Sym}(A)$.

If $A = \{1, 2, \ldots, n\}$ we write $\mathfrak{S}n$ or $\mathfrak{S}^n$ for $\mathfrak{S}(A)$.

[This is symmetric group on $n$ elts.]
Ex. \( n = 5 \)

\[ A = \{1, 2, 3, 4, 5\} \]

Two-line notation

\[ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \]

diagram

One-line or cycle notation

\( (1 \ 4 \ 3 \ 5) \ (2) \)

Diagram of the cycle notation \( (1 \ 4 \ 3 \ 5) \ (2) \).
Prop. $\forall n \ |S_n| = n!$

Pf. Every $\pi \in S_n$ can be represented as

$\pi = (a_1 \ a_2 \ \cdots \ a_n)$,

where $a_1 \in \{1, \ldots, n\}$

$\Rightarrow a_2 \in \{1, \ldots, n\} \setminus \{a_1\}$

$a_3 \in \{1, \ldots, n\} \setminus \{a_1, a_2\}$

$\vdots$

$\Rightarrow \# \pi = (\# a_1) \cdot (\# a_2 \neq a_1) \cdot (\# a_3 \neq a_1, a_2) \cdots \cdot 1$

$= n \ (n-1)! (n-2)! \ldots 1$

$= n!$

\[\forall \pi \in S_n \quad n \leq 4\]
"Multiplying" Perms.

The product of two perms. in $S(A)$ is their composition as functions.

Ex. $\pi$ as above +

$\rho \in S_5 : \rho = (1 \ 2 \ 3 \ 4 \ 5)$

$\rho \circ \pi$

$\rho \circ \pi = (1 \ 2 \ 3 \ 4 \ 5) \in S_5$

We write $\rho \pi$ for $\rho \circ \pi$.

IMPT: Go R to L in working out a product.

$\pi(i) = \rho(\pi(i))$
order matters in general

\[ \pi \rho = (1\ 2\ 3\ 4\ 5) \cdot \rho \pi \]

def. a cycle in \( S(A) \) is a perm. which in one-line (cycle) notation is \((a, a_2 a_3 \ldots a_r)\).

\[ \begin{array}{cccc}
  & a_1 & \rightarrow & a_2 \\
  \downarrow & & & \downarrow \\
  a_r & \rightarrow & & a_3 \\
 & & & \rightarrow \\
 & & & \ldots
\end{array} \]

r-cycle

Ex. \( \pi \) above is a 4-cycle in \( S_5 \): \( \pi = (1\ 4\ 3\ 5) \).

\text{IMPT: Go L to R in the circle}
A product of disjoint cycles is easy:

\[ \text{Ex. } (1435)(27) \in S_8 \]
\[ = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \]
\[ = (4\ 7\ 5\ 3\ 1\ 6\ 2\ 8) \]
\[ = (27)(1435) \]
\[ = (72)(3514) \]
\[ = (5143)(72)(8) \]

For the product of disjoint cycles, it doesn't matter what order the cycles are in.

But it does if the cycles intersect!
Ex. \[ (1453) (251) \]
\[ = (12345)(12345) \]
\[ = (23154) = (123)(45) \]

one-line

\[ (123)(45) \]

In this fashion we multiply any product of cycles (one-line).

Also, we see that

Thm. Every \( \pi \in S_n \)

is a product of disjoint cycles.
pf. WLOG

\[\pi = (1 \ z \ 3 \ 4 \ \ldots \ \ n) = (a_1\ a_2\ \ldots\ a_n)\]

See where 1 goes: \[\pi^2(1) = \pi(\pi(1)) = \pi(1) = a_1\]

\[1 \rightarrow a_1 = \pi(a_1) \rightarrow \pi^3(1) = \pi(\pi(\pi(1))) = \pi(1) = a_1\]

Eventually you return to 1, since \(\pi\) is a perm, you have a cycle.

Then take an elt not in the cycle, see where it goes, etc.

\ldots until all of \(1, \ldots, n\) are accounted for:

\[\pi = (1\ a_1\ \pi(a_1)\ \ldots)(b\ \ldots)(c\ \ldots)\]

\[a_1\ \ldots\ \ a_1 \leftrightarrow \ \ldots \leftrightarrow c\]
Ex. \( \pi = (15342) \in S_5 \) is one 5-cycle.

\[ \sigma = (15)(2)(34) \in S_5 \]

Power of Perms. \( \sigma \in \mathfrak{S}(A), \ n \in \mathbb{Z}_+ \)

\[ \sigma^n = 0 \sigma \cdots \sigma \]

Ex. \( \sigma \) above

\[ \sigma^2 = (1)(2)(3)(4)(5)(15)(2)(34)(15)(2)(34) = \text{the identity} \]

Defn. The \( \mathfrak{S}(A) \) \text{ is the identity map.}
Defn. $\sigma^0 = 1$

Defn. **The inverse** of $\sigma \in S(A)$ is the **inverse** fn., denoted by $\sigma^{-1}$ (not $\sigma^{-1}$). $(\sigma^n)^{-1} = \sigma^{-n} = \text{inverse of } \sigma^n = (\sigma^{-1})^n$.

**The Laws of Exponents work!**

Ex. $\sigma^4 \sigma^{-3} \sigma^5 = \sigma^6$

Ex.: $\sigma = (1\ 6\ 4\ 2\ 3\ 5)$ 6-cycle

$\sigma^2 = (1\ 4\ 3)\ (2\ 5\ 6)$

$\sigma^3 = (1\ 2)\ (3\ 6)\ (4\ 5)$

$\sigma^4 = (1\ 3\ 4)\ (2\ 6\ 5)$

$\sigma^5 = (1\ 5\ 3\ 2\ 4\ 6) = \sigma^{-1}$

$\sigma^6 = 1$  $\sigma$ has order 6
Define. The order of $\sigma \in S(A)$ is the smallest power $n > 0$ s.t. $\sigma^n = 1$.

\[ \sigma^{-2} \cdot \sigma^{-6} = \sigma^{-8} \]
\[ \sigma^4 = \sigma^{-2} \quad (\sigma^3)^{-1} = \sigma^{-3} \]
\[ (\sigma^4)^{-1} = \sigma^{-4} = \sigma^2 \]

If $A$ is finite, every $\sigma \in S(A)$ has some order $\sigma, \sigma^2, \sigma^3, \ldots$ must repeat eventually because $S(A)$ is finite. Say $\sigma^i = \sigma^j$; $i < j$. Say $\sigma^i = \sigma^{i+j}$. $i < j$. $i+j > 0$. 

\[ \sigma^{-2} \cdot \sigma^{-6} = \sigma^{-8} \]
so some positive power of $c$ is that it, $c$ appears in the sequence. Then the order $n$ is the first power $p$ s.t. $c^p = c$.

has order 1

$\exists! \sigma = (164235)$

$\sigma, \sigma^2, \ldots, \sigma^6, \sigma^7, \ldots, \sigma^{12}$

order 6
We can see from our 6-cycle example that if $\sigma_r$ is an $r$-cycle, then $\sigma_r^i = c$ $\iff$ $r/i$.

The reason is that $b_j \rightarrow b_{j+1} \rightarrow \ldots$

$\sigma_r^i(b_j) = b_{j+i \mod r}$

$+ b_{j+i} = b_j$

$\therefore i$ is a multiple of $r$.

\[ \therefore \text{An } r\text{-cycle has order } r. \]
Example: \[ \sigma = (1439 \ 12 \ 2) \ \ (5678) \]
\[ \chi_1 = 6 \ \ \ \ \chi_2 = 4 \]
\[ \text{LCM}(6, 4) = 12 \]

\[ \sigma^2 = (1 \ 3 \ 12) \ (249) \ (57) \ (68) \]

\[ \sigma_1^2 = 1 \]
\[ \sigma_2 \text{ order } 12. \]

\[ \sigma_{98} = (\sigma_1^2)^8 \sigma^2 = \sigma_2^2 \]
\[ 98 = 8 \cdot 12 + 2 \]
\[ 98 \equiv 2 \mod 12 \]

\[ \text{i.e., } -97 = \sigma_1^{11} = \sigma_1^{-1} \]
\[ -97 = -9 \cdot 12 + 11 \]

\[ \sigma^2 = (12 \ 12 \ 9 \ 34) \ (5678) \]

\[ \text{LCM}(3, 3, 2, 2) = 6. \]
Defn. A transposition is a 2-cycle, \((ij)\).

Ex. \((12)(13) = (132)\)

So \((132)\) is a product of transpositions.

Thm. If \(\pi \in S_n\), then \(\pi\) can be written as the product of at most \(n-1\) transpositions.
Thm. If \( \sigma \) is a product of disjoint cycles of lengths \( l_1, l_2, \ldots, l_s \), then

\[
\sigma^n = e \iff \frac{\text{lcm}(l_1, \ldots, l_s)}{n} \mid n
\]

Thus, the order of \( \sigma \) is \( \text{lcm}(l_1, \ldots, l_s) \).

Pf. Say \( \sigma = \tau_1 \tau_2 \ldots \tau_s \)

where \( \tau_i \) is a cycle of length \( l_i \) - \( s \) cycles

Then \( \sigma^n = \tau_1^n \tau_2^n \ldots \tau_s^n \) since \( \tau_i \) are disjoint.

\[
\Rightarrow \forall i \quad \frac{n}{l_i} \mid n \quad \text{since } \tau_i \text{ is an } l_i \text{-cycle}
\]

\[
\Rightarrow \text{lcm}(l_1, \ldots, l_s) \mid n.
\]
Then. A perm. \( \pi \in S_n \) which is the product of \( R \) disjoint cycles can be written as the product of \( n - R \) transpositions.
Ex.

\[ \pi = (18\ 54)\ (36\ 2)\ (7) \]

or

\[ \pi = (18)\ (85)\ (54)\ (36)\ (62) \]

\[ (4+3)-2 = 5 \text{ transps.} \]

or

\[ (14)\ (15)\ (18)\ (32)\ (36) \]

Pf.

For an r-cycle

\[ (a_1\ a_2\ \ldots\ a_r) = (a_1\ a_2)\ (a_2\ a_3)\ \ldots \]

\[ \text{can be written as a product of } r-1 \text{ transposes.} \]

Thus, a perm. with disjoint cycles of lengths \( \ell_1, \ell_2, \ldots, \ell_k \)

\[ \text{can be written as a product of } \sum_{i=1}^{k} (\ell_i - 1) \]

\[ = \sum_{i=1}^{k} \ell_i - k = n - k \leq n-1 \]
Defn. An orbit of an elt. under a perm. is the set of els. it reaches by successive appln. of the perm.

[An orbit is an equivalence class under the relation ~ of # 14.]

Ex: \( n = 12 \)

\( \tau = (1 \ 4 \ 3 \ 9 \ 12 \ 2)(568) \)

Orbits are:

\( \{1, 4, 3, 9, 12, 2\} \)
\( \{5, 6, 8\} \)
\( \{3\} \)
\( \{103\} \)
\( \{1113\} \)
Multiplying by a Transposition

1. Multiply on the left

Let \( \sigma \in S_n \)

\[
\sigma = \begin{pmatrix}
1 & 2 & \cdots & n \\
\sigma(1) & \sigma(2) & \cdots & \sigma(n)
\end{pmatrix}
\]

Transposition

\( \tau = (i \, j), \; 1 \leq i < j \leq n \)

\[
\begin{align*}
\tau \sigma &= (ij) \sigma \\
&= (ij) \begin{pmatrix}
1 & 2 & \cdots & n \\
\sigma(1) & \sigma(2) & \cdots & \sigma(n)
\end{pmatrix} \\
&= \begin{pmatrix}
1 & 2 & \cdots & n \\
\sigma(1) & \sigma(2) & \cdots & \sigma(n)
\end{pmatrix}
\end{align*}
\]

\( \tau \) switches entries \( i \) \& \( j \) in the second row.

\[\text{Ex.: } (46) \cdot (154)(26) \rightarrow (15624)\]
2. Multiply on the right

\[ \sigma \tau = (\sigma_0 \cdots \sigma_n) (i_0 \cdots i_n) \]

This time, \( \tau = (i_j) \) switches entries \( \sigma(i) \) and \( \sigma(j) \).

**Example**

\[ (154)(26) \cdot (46) \]

\[ = (42615) \]

\[ \sigma = (5 \ 6 \ 3 \ 1 \ 4 \ 2) \]

\[ \sigma \tau = (5 \ 6 \ 1 \ 4 \ 2) \]

\[ = (15426) \]
3. Combining (1) and (2) we see that
\[ \sigma \tau = \sigma(i \cdot j) \]
\[ = \text{swap } \sigma(i) + \sigma(j) \text{ in second line} \]
\[ = (\sigma(i) \sigma(j)) \sigma \]
\[ \text{trans} \]

\[ \text{Ex. } \sigma \tau = \]
\[ = (154)(26) \cdot (46) \]
\[ = (1 2) (154)(26) \]
\[ = (154 2 6) \]
Parity Thm.

Let \( \alpha \in S_n \) be written two ways as a product of transpositions:

\[ \alpha = T_1 T_2 \ldots T_j = \sigma_1 \sigma_2 \ldots \sigma_k \]

Then \( j \equiv k \pmod{2} \).

Define the parity of a perm. \( \alpha \in S_n \) is "even" or "odd" according as \( j \) is even or odd.

\[ \pi = (1854)(362) \quad \text{5 trans. is odd perm.} \]

\[ \lambda = (1) \ldots (n) \quad 0 \text{ trans. is even} \]
The product of two odd primes is even.
\[ \text{odd} \times \text{odd} = \text{even} \]
Ex.

\[(5, 7, 4, 1)(2, 8)\]
\[(6)(3, 142)(46, 37, 29, 18)\]

\[= (5, 7)(7, 4)(4, 1)(2, 8)(3, 142)\]
\[(46, 37)(37, 29)(29, 18)\]

\[\#\text{trans.} = 8 \quad \text{even perm.}\]
Proof: Define a polynomial in variables \( x_1, \ldots, x_n \):

\[
P(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)
\]

\( \text{Ex., } n = 3 \)

\[
P(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3) \cdot (x_2 - x_3)
\]

\[
= x_1^2x_2 - x_1^2x_3 + \ldots
\]

\[
\text{degree 3}
\]

\[
2 \cdot 2 \cdot 2 = 8 \text{ terms}
\]

\( n = 4 \)

\[
P(x_1, x_2, x_3, x_4)
\]

\[
= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \cdot (x_2 - x_3)(x_2 - x_4)(x_3 - x_4)
\]

\[
\text{degree 6}
\]

\[
64 \text{ terms}
\]
\[ P(x_1, \ldots, x_n) \text{ degree } (\frac{n}{2}) \]

We say \( \pi \in S_n \) acts on \( P(x_1, \ldots, x_n) \):

\[ \pi P(x_1, \ldots, x_n) = P(x_{\pi(1)}, \ldots, x_{\pi(n)}) \]

**Example:** \( \pi = (1 \, 3 \, 2) \) \( n = 3 \)

\[ \pi P(x_1, x_2, x_3) = P(x_3, x_1, x_2) \]

\[ = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) \]

\[ = (-1)(x_1 - x_3)(-1)(x_2 - x_3)(x_1 - x_2) \]

\[ = (-1)^2 P(x_1, x_2, x_3) \]

\[ = P(x_1, x_2, x_3) \]

We'll see in general that for \( \pi P(x_1, \ldots, x_n) = \pm P(x_1, \ldots, x_n) \)

**+ depends only on \( \pi \)**
Claim: If $T \in S_n$ is a transposition, then
\[ \tau P(x_1, \ldots, x_n) = -P(x_1, \ldots, x_n) \]

Proof. Let $T = (k \; l)$, $k < l$.

\[ \tau P(x_1, \ldots, x_n) = P(x_1, \ldots, x_l, \ldots, x_k, \ldots, x_n) \]

\[ = (x_1 - x_l) \cdots (x_i - x_k) \cdots (x_n - x) \]

We get the same $\binom{n}{2}$ factors as before, except $x_i - x_j$ as before, except $x_i - x_j$ as before, except $x_i - x_j$. Some are reversed, $x_j - x_i$.

Consider what $T$ does to a term $(x_i - x_j)$.
\[
\begin{align*}
\text{in } P & \quad \rightarrow \quad \text{in } TP \\
X_i - X_j, \ i \neq j, i \leq l & \quad X_i - X_j \\
X_k - X_l & \quad X_k - X_l \\
(X_i - X_k)(X_i - X_l), \ i < k & \quad \Rightarrow (X_i - X_l)(X_i - X_k) \\
(X_k - X_i)(X_k - X_i), \ i > l & \quad \Rightarrow (X_k - X_i)(X_k - X_i) = \\
(X_k - X_i)(X_i - X_l), \ k < i < l & \quad \Rightarrow (X_k - X_i)(X_i - X_k) = \\
\text{So we see altogether} & \quad \Rightarrow P(x_1, \ldots, x_m) = -P(x_1, \ldots, x_n), \\
\text{we shall apply the claim} & \quad \Rightarrow \text{Claim:} \\
\text{to arbitrary } \pi \in S_n \quad \Rightarrow \text{to prove the thm.}
\end{align*}
\]
Apply the claim with \( \pi = \alpha \) to \( P(x_1, \ldots, x_n) \):

1. \( \alpha P(x_1, \ldots, x_n) = T_i \cdots T_j P(x_1, \ldots, x_n) \)
   \( = (-1)^{i-1} \cdots (-1)^{j-1} P(x_1, \ldots, x_n) \)
   \( = (-1)^{j-i} P(x_1, \ldots, x_n) \)

2. \( \alpha P(x_1, \ldots, x_n) = \sigma_1 \cdots \sigma_k P \)
   \( = (-1)^{i-1} \cdots (-1)^{k-1} P \)
   \( = (-1)^{i-k} P(x_1, \ldots, x_n) \)

\( \Rightarrow (-1)^{j-i} = (-1)^{i-k} \)

\( \Rightarrow j \equiv k \pmod{2} \)

\( \Rightarrow \text{Them.} \)