Theorem - If $\sigma \in S_n$ then either

① σ can be written as a product of an odd # of transpositions

or

② σ can be written as a product of an even # of transpositions

But it is impossible that σ satisfies both ① & ②.

Sketch of proof: We showed that every perm. can be written as a product of disjoint cycles, and each cycle can be written as a product of transpositions.

$\Rightarrow$ Definitely ① or ② must be true.

Suppose a permutation σ can be written as

$$\sigma = \sigma_1 \cdots \sigma_{2m+1} = \tau_1 \cdots \tau_{2k}$$

for some transpositions σ_j, τ_s where $m, k \in \mathbb{Z}_{\geq 0}$.

If this is true, then

$$\sigma_1 \cdots \sigma_{2m+1} \cdot \tau_{2k}^{-1} \cdots \tau_1^{-1} = e$$

Note the inverse of a transposition is itself, so $\tau_j^{-1} = \tau_j$.

[Note $a \in G$ is called idempotent if $a^2 = e$ = identity.]

We need to show that it is impossible for the product of an odd # of transpositions to be the identity.

Note the transposition (a,b) can be written as a matrix.

The transposition is

$$\begin{pmatrix} 1 \\ 2 \\ \vdots \\ a \\ \vdots \\ b \\ \vdots \\ n \end{pmatrix} \to \begin{pmatrix} 1 \\ 2 \\ \vdots \\ b \\ \vdots \\ a \\ \vdots \\ n \end{pmatrix}$$

This is the same as matrix multiplication

by

$$\begin{array}{c c} & \begin{matrix} \quad\quad a & b \quad \end{matrix} \\ \begin{matrix} \\ a \to \\ b \to \\ \\ \end{matrix} & \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 0 & 1 \\ & & 1 & 0 \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix} \end{array} = M_{(a,b)} \Leftarrow \text{matrix associated with } (a,b).$$

permutation matrix - type of elementary matrix that switches two rows in a linear system.

So a product of an odd # of such matrices gives the matrix of the odd product of transpositions. The result must be the identity matrix.

But $\det(M_{(a,b)}) = -1$ $\quad\quad \det(I) = 1$

$\therefore$ we would get

$$\underbrace{\det(M_{\sigma_1} M_{\sigma_2} \cdots M_{\sigma_{2m+1}} M_{\tau_{2k}} \cdots M_{\tau_1})}_{} = 1$$

since $\operatorname{Det}(AB) = \det(A)\det(B)$,

we get

$$\det(M_{\sigma_1})\det(M_{\sigma_2}) \cdots \cdots \det(M_{\tau_1}) = 1$$

$$(-1)^{2m+1+2k} = 1 \quad \Rightarrow\Leftarrow$$

∴ we can only be written as an odd #
or an even # of permutations.

This shows the power of representation theory.
Given group, you make a group
homomorphism to $GL(V)$
some vector space.

Here $GL(V) = \{$linear functions $f: V \to V$ that are invertible$\}$

If the homomorphism is 1-1, G is isomorphic
to a subgroup of $GL(V)$ —
these are called faithful representations.

Homomorphisms. If G & H are
groups, then a function $\phi: G \to H$ is
a homomorphism if $\forall a, b \in G$

$$\phi(ab) = \phi(a)\phi(b).$$

ϕ is called an isomorphism if $\phi^{-1}: H \to G$
exists (i.e. ϕ is 1-1 and onto) and ϕ^{-1} is
also a homomorphism

Question: Is it possible for a homomorphism to be 1-1 and onto but not be an isomorphism?

i.e. is the last part necessary?

Suppose $c, q \in H$. Consider

$\phi^{-1}(cq)$. We must be able to write $c = \phi(a)$ and $q = \phi(b)$ for unique choices of a & b.

$$\phi^{-1}(cq) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab))$$

$$= ab = \phi^{-1}(c)\,\phi^{-1}(q).$$

Thus if ϕ is a 1-1, onto homomorphism, it is automatically an isomorphism.

If $\phi: G \to H$ is a homomorphism, then $\phi(G) = \{\phi(a) : a \in G\}$ is automatically a subgroup of H (often called "image of G").

<u>Thm</u> (First Isomorphism Theorem)

$$\phi(G) \cong \frac{G}{\ker\phi} = \{\text{right cosets } g(\ker\phi) : g \in G\}.$$

$\ker \phi = \{ g \in G : \phi(g) = e_H \}$

identity in H.

$\ker\phi$ is a normal subgroup.

A subgroup N of G is normal

if $\cdot\ gng^{-1} \in N \quad \forall g \in G, n \in N.$

$\iff gNg^{-1} = N$

$\iff gN = Ng$

$\iff gNg^{-1} \subseteq N$

set of left cosets

$G/N = \{ aN : a \in G \}$

$\parallel$

only for normal subgroup case

$N \backslash G = \{ Nb : b \in G \}$

Set of right cosets

each form a group under multiplication.