Theorem (cycle decomposition theorem)

If $\sigma \neq e$ is in S_n, then σ is the product of one or more disjoint cycles of length at least 2.

proof

We prove the existence of decomposition by induction on $n \geq 2$ for $\sigma \in S_n$. (Assume the uniqueness).
If $n = 2$ then each permutation has length 2 since $S_2 = \{e, (1\ 2)\}$ and $\sigma \neq e$.
If $n > 2$ assume result true for S_{n-1}.
Let $\sigma \in S_n$. If σ fixes n then $\sigma(n) = n$ and so $\sigma \in S_{n-1}$. By induction hypothesis σ is the product of disjoint cycles of length at least 2.

Assume σ moves n and $\sigma(n) \neq n$. set $m = \sigma^{-1}(n)$ or $\sigma(m) = n$ with $m \neq n$.
Let $\gamma = (m \quad n)$ where $\gamma^2 = e$.
Consider $\tau = \sigma\gamma$. Thus $\tau\gamma = \sigma\gamma^2 = \sigma$.
Moreover, $\tau(n) = \sigma\gamma(n) = \sigma(m) = n$.
Therefore $\tau \in S_{n-1}$ and so τ is the product of disjoint cycles in S_{n-1} of length at least 2 by induction hypothesis.
We consider 2 cases: CASE 1, $\tau(m) = m$ and CASE 2, $\tau(m) \neq m$
CASE 1: $\tau(m) = m$ and $\tau(n) = n$ by above so τ fixes both m and n and τ disjoint from γ.
$\therefore \quad \sigma = \tau\gamma$ is as required.

CASE 2: $\tau(m) \neq m$. Then m is moved by exactly one factor in the decomposition of τ.
say $\tau = \mu(m \quad k_1 \quad k_2 \quad \cdots \quad k_r)$ where μ is the product of cycles that do not move $m \quad k_1 \quad k_2 \quad \cdots \quad k_r$ and n

$$\begin{aligned} \sigma = \tau\gamma &= \mu(m \quad k_1 \quad k_2 \quad \cdots \quad k_r)(m \quad n) \\ &= \mu(m \quad n \quad k_1 \quad k_2 \quad \cdots \quad k_r) \end{aligned}$$

and σ has the required decomposition.
So by principle of induction, the statement is true $\forall n \in \mathbb{N}$ and $n \geq 2$.

Friday

Example

$|S_4| = 24$. List of elements e; $(1 \quad 2)$; $(1 \quad 2)(3 \quad 4)$; $(1 \quad 2 \quad 3)$; $(1 \quad 2 \quad 3 \quad 4)$ etc These are the types of decomposition.