Theorem: (sign is well-defined) Let $\sigma \in S_n$. Then σ is either even or odd, but not both. Consequently, ε is a well-defined homomorphism.

Proof: (Miller) Suppose $\sigma \in S_n$ is both even and odd, and let e denote the identity of S_n. Then σ^{-1} is both even and odd, since we can write σ^{-1} as the product of transpositions in σ, only in reverse order:

If $\sigma = (x_1\, x_2)(x_3\, x_4)$

$x_i \in \{1, 2, \cdots, n\}$, $1 \le i \le 4$

with $x_1 \neq x_2$, $x_3 \neq x_4$,

then

$\sigma^{-1} = (x_3\, x_4)(x_1\, x_2)$ since

by uniqueness of inverse,

$\sigma\ (x_3 x_4)(x_1 x_2)$

$= (x_1 x_2)(x_3 x_4)(x_3 x_4)(x_1 x_2)$

e

$= (x_1 x_3)(x_1 x_3)$

$= e$.

Therefore, $\sigma^{-1} = (x_3 x_4)(x_1 x_2)$

Now assume that if σ can be expressed as the product of k transpositions, then σ^{-1} can be expressed as the product of the same transpositions, written in reverse order. Let $\gamma \in S_n$ and suppose γ is the product of $k+1$ transpositions:

$$\gamma = (x_1 x_2)(x_3 x_4) \cdots (x_{2k-1} x_{2k})(x_{2k+1} x_{2k+2})$$

with $x_{2i-1} \neq x_{2i}$ $\forall$ $1 \leq i \leq k+1$.

Then

$$\gamma \cdot (x_{2n+1}\, x_{2n+2})(x_{2n-1}\, x_{2n}) \cdots (x_3 x_4)(x_1 x_2)$$

$$= (x_1 x_2)(x_3 x_4) \cdots (x_{2n-1} x_{2n})(x_{2n+1} x_{2n+2})$$

$$\cdot (x_{2n+1} x_{2n+2})(x_{2n-1} x_{2n}) \cdots (x_3 x_4)(x_1 x_2)$$

$$= \Big((x_1 x_2)(x_3 x_4) \cdots (x_{2n-1} x_{2n})\Big) \cdot (x_{2n-1} x_{2n}) \cdot$$

$$\cdots (x_3 x_4)(x_1 x_2)$$

Let $\sigma = (x_1 x_2)(x_3 x_4) \cdots (x_{2n-1} x_{2n})$.

Then by induction,

$$\sigma^{-1} = (x_{2n-1} x_{2n}) \cdots (x_3 x_4)(x_1 x_2),$$

So the above product is equal to e.

Therefore,

$$\sigma^{-1} = (x_{2n+2}\, x_{2n+1})(x_{2n}\, x_{2n-1}) \cdots (x_4 x_3)(x_2 x_1)$$

From this, we see that if σ is both even and odd, then we can write σ as

$$\sigma = (x_1 x_2)(x_3 x_4) \cdots (x_{4k-1}\, x_{4k}) \quad \text{even}$$

$$\sigma = (y_1 y_2)(y_3 y_4) \cdots (y_{4l-3}\, y_{4l-2}) \quad \text{odd}$$

for $k, l \in \mathbb{N}$ and transpositions

(x_{2i-1}, x_{2i}) $\quad 1 \le i \le 2k$

(y_{2j-1}, y_{2j}) $\quad 1 \le j \le 2l-1$

Then

$$e = \sigma\sigma^{-1}$$

$$= (x_1 x_2)(x_3 x_4) \cdots (x_{4u-1} x_{4u}) \quad \text{even}$$

$$\cdot (y_{4\ell-3} y_{4\ell-2}) \cdots (y_3 y_4)(y_1 y_2) \quad \text{odd}$$

$$= (x_1 x_2)(x_3 x_4) \cdots (x_{4u-1} x_{4u}) \quad \text{even}$$

$$(x_{4u-1} x_{4k}) \cdots (x_3 x_4)(x_1 x_2) \quad \text{even}$$

$\Rightarrow$ e is both even and odd.

Conversely, if e is both even and odd, then by multiplying any permutation σ by e and using either the even or odd representation, σ is both even and odd.

This says we can reduce to showing that the identity permutation cannot be odd, since we know

$(12)(12) = e$.

Idea: If e was odd, there will always be a "lonely" transposition, with an element in it not common to any other transposition in the decomposition of e. Then this element cannot be mapped back to itself, so the decomposition doesn't yield the identity!

Approach: Prove that any decomposition of e via transpositions can always be reduced by removing two transpositions.

To that end,

write

$$e = (x_1 x_2)(x_3 x_4)\cdots(x_{2k-1} x_{2k})$$

with $k \geq 3$, $k \in \mathbb{N}$ and

$(x_{2i-1}\ x_{2i})$ is a transposition $\forall\ 1 \leq i \leq k$.

Choose $m \in \{1, 2, \ldots, n\}$.

Let $(x_{2j-1}\ x_{2j})$ for $1 \le j \le k$

be the first transposition in which

m appears. Write

$$(x_{2j-1}\ x_{2j}) = (m\ a)$$

for some $a \in \{1, 2, \cdots, n\}$, $a \neq m$.

Note $j = k$ is impossible, for then

$e(a) = m \neq a$, and so the

decomposition cannot give the identity.

Cases: 1) $(x_{2j+1}\ x_{2j+2}) = (m\ a)$

then we cancel

$$(x_{2j-1}\ x_{2j})(x_{2j+1}\ x_{2j+2})$$

$$= (ma)(ma)$$

$$= e$$

and we have reduced the number of transpositions by 2, as desired.

2) $(x_{2j+1}\ x_{2j+2}) = (b\ c)$

with $b \neq a, m \neq c$.

Then $(x_{2j+1}\ x_{2j+2})$ and $(x_{2j-1}\ x_{2j})$ are disjoint.

So the transpositions commute, and we can write

$$(x_{2j-1}\ x_{2j})(x_{2j+1}\ x_{2j+2}) = (x_{2j+1}\ x_{2j+2})(x_{2j-1}\ x_{2j}).$$

In this way, we move the first transposition containing m one spot to the right.

3) Without loss of generality, $x_{2j+1} = m$, $x_{2j+2} = c \neq a$

Then

$$(x_{2j-1}, x_{2j})(x_{2j+1}, x_{2j+2})$$

$$= (m\ a)(m\ c)$$

$$= ((a\ m)$$

$$= ((\ a)(a\ m)$$

$$= (c\ a)(m\ a)$$

We have again pushed $(m\ a)$ one spot to the right - Note: $c \neq m$

Since $(m\ c)$ is a transposition.

4) Without loss of generality,

$$x_{a_{j+1}} = a \quad , \quad x_{a_{j+2}} = c \neq m$$

Then

$$(x_{a_{j-1}}\ x_{a_j})(x_{a_{j+1}}\ x_{a_{j+2}})$$

$$= (m\ a)(a\ c)$$

$$= (m\ a\ c)$$

$$= (a\ c\ m)$$

$$= (a\ c)(c\ m)$$

and we have again pushed the first transposition one spot to the right.

This covers all cases

In cases 2) - 4), we move the first transposition containing m one spot to the right. Either we encounter $(m\ a)$ one spot to the right, and then we are in case 1), or we do not. In the latter case, we can push to $(x_{2k-1}\ x_{2k}) = (m\ c)$ for some $c \in \{1, 2, \ldots, n\}$, $c \neq m$ as the first transposition containing m, so the decomposition cannot yield the identity.

Therefore, we are always in case 1):
every transposition can be paired,
and therefore, e cannot be odd.

Notation: (A_n) $\quad A_n \leq S_n$,

$A_n = \ker(\xi)$

A_n = all even permutations in S_n.

A_5 = smallest-order simple nonabelian group.