Recall: Let $n \in \mathbb{Z}^+$, $n > 1$, then every element in S_n is a product of the transpositions:

$$(1 2), (1 3), \dots, (1 n).$$

In particular if $\sigma = (a_1 \cdots a_r)$ a cycle of length r, then:

$$\sigma = (a_{r-1}\, a_r)(a_{r-2}\, a_r)\cdots(a_2\, a_r)(a_1\, a_r) = (a_1 a_2)(a_2 a_3)\cdots(a_{r-2}\, a_{r-1})(a_{r-1}\, a_r).$$

Remark: The decomposition of a permutation into a product of transpositions is <u>not</u> unique.

Recall that we have group homomorphisms:

$$\begin{array}{ccccc} S_n & \xrightarrow{\Theta} & \mathrm{Perm}_n(\mathbb{R}) & \xrightarrow{\det} & \{\pm 1\}. \\ \sigma & \longmapsto & [T_\sigma]_{S_n} & \longmapsto & \det([T_\sigma]_{S_n}). \end{array}$$

where S_n is the standard basis for $\mathbb{R}^n$ and $\mathrm{Perm}_n(\mathbb{R})$ are the permutation matrices.

Define $A_n := \mathrm{Ker}(\det \circ \Theta) \trianglelefteq S_n$, we have $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ and $[S_n : A_n] = 2$.

For a transposition $\tau \in S_n$, since τ permutes two columns of the identity matrix, we have $\det([T_\tau]_{S_n}) = -1$. Hence if $\sigma \in S_n$ is a product of r transpositions and a product of s transpositions for some $r, s \in \mathbb{Z}^+$, then $(-1)^r = (-1)^s$ so $r \equiv s \mod 2$.

Thus by the Proposition above, for σ an r-cycle, it decomposes into the product of $r-1$ transpositions, so $\det([T_\sigma]_{S_n}) = (-1)^{r-1}$. We have $\sigma \in A_n$ for r odd and $\sigma \in S_n \setminus A_n$ for r even. We conclude:

$$A_n = \{ \sigma \in S_n \mid \sigma \text{ is a product of an even number of transpositions} \}.$$

$$S_n \setminus A_n = \{ \sigma \in S_n \mid \sigma \text{ is a product of an odd number of transpositions} \}.$$

__Definition:__ An element in A_n is called an __even permutation__. An element in $S_n \setminus A_n$ is called an __odd permutation__.

__Definition:__ Let $\sigma \in S_n$, suppose that $\sigma = \sigma_1 \cdots \sigma_r$ is the full cycle decomposition of σ. We define the __signum__ of σ as: $\mathrm{sgn}(\sigma) = (-1)^{n-r}$.

__Remark:__ Since the full cycle decomposition of σ is unique, this defines a function:

$$\mathrm{sgn}: S_n \longrightarrow \{\pm 1\}.$$

__Proposition:__ The function $\mathrm{sgn}: S_n \longrightarrow \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ is a group homomorphism.

__Corollary:__ The group homomorphisms $\det \circ \theta : S_n \to \{\pm 1\}$ and $\mathrm{sgn}: S_n \longrightarrow \{\pm 1\}$ coincide.

__Corollary:__ The alternating group A_n is equal to the kernel of the signum $\ker(\mathrm{sgn})$.

__Proposition:__ Let $n \in \mathbb{Z}^+$, $n \geq 3$. Then the alternating group A_n is generated by the 3-cycles:

$$(123), (124), \cdots, (12n).$$

__Lemma:__ Let K be a normal subgroup of A_n, if K contains a 3-cycle then $K = A_n$.

__Theorem:__ (Abel's Theorem) Let $n \in \mathbb{Z}^+$, $n \neq 4$, then the alternating group A_n is simple.

__Remark:__ Recall that a subgroup of a solvable group is solvable, and that a non-abelian simple group cannot be solvable, so a group containing a non-abelian simple group cannot be solvable.

Hence S_n is <u>not</u> solvable for $n>5$.

<u>Proposition:</u> Let $n\in\mathbb{Z}^+$, $n\geq 5$. Then A_n is the only subgroup of S_n of index two.

<u>Theorem:</u> The alternating group A_5 is, up to isomorphism, the only simple group of order 60.

<u>Proposition:</u> Let $n\in\mathbb{Z}^+$, $n\geq 5$, H a normal subgroup of S_n. Then $H=\{1\}$ or $H=A_n$ or $H=S_n$.

<u>Proposition:</u> Let G be a finite group of order $2n$, n odd. Then G contains a normal subgroup of index two. In particular if $n>1$ then G is <u>not</u> simple.

<u>Theorem:</u> Let G be a finite group of order $2^r\cdot m$, m odd, $r\in\mathbb{Z}^+$. If G contains a cyclic Sylow 2-subgroup then there exists a normal subgroup of G of order 2^r. In particular if $m>1$ or $n>1$ then G is <u>not</u> simple.