Thm.: No permutation in $S_n$ ($n \in \mathbb{N}$) can be written both as a product of an odd number of transpositions and as a product of an even number of transpositions.

Proof #2: We already handled the case $n < 2$.

If $n \geq 2$, then we show: Let $\sigma \in S_n$ and let $\tau = (i, j)$ be a transposition in $S_n$. Then:

\[(\text{# of orbits in } \sigma) - (\text{# of orbits in } \sigma \tau) = \pm 1.\]

Case I: Assume $i$ and $j$ are in different orbits of $\sigma$.

Writing $\sigma$ as a product of disjoint cycles, we have

\[\sigma = (i, a_1, a_2, \ldots, a_r)(j, b_1, b_2, \ldots, b_s). \quad \text{(other cycles)}\]

Then also

\[\sigma \tau = (i, a_1, \ldots, a_r, j, b_1, \ldots, b_s). \quad \text{(other cycles)}\]

Here we used:

\[(i, a_1, \ldots, a_r)(j, b_1, \ldots, b_s)(i, j) = (i, a_1, \ldots, a_r, j, b_1, \ldots, b_s) \quad \text{(this is true even if } r = 0 \text{ or } s = 0 \text{ on both)}\]

So $\sigma \tau$ has one less orbit than $\sigma$.

Case II: Assume $i$ and $j$ are in the same orbit of $\sigma$.

Then the identity

\[\sigma \tau = (i, a_1, \ldots, a_r, j, b_1, \ldots, b_s)(i, j) = (i, a_1, \ldots, a_r)(j, b_1, \ldots, b_s)\]

leads to the conclusion that $\sigma \tau$ has one more orbit than $\sigma$. (The argument is similar.)
Therefore, by induction on m (starting with m = 0, in which case \( \sigma = e \) has n orbits):

If \( \sigma \) can be written as a product of m transpositions, then \( (n - (\# \text{ of orbits of } \sigma)) \) has the same parity as m.

This number \( (n - (\# \text{ of orbits of } \sigma)) \) depends only on \( \sigma \), so no matter how you write \( \sigma \) as a product of transpositions, the number of transpositions must be:

- even if \( (n - (\# \text{ of orbits of } \sigma)) \) is even,
- odd if \( n - (\# \text{ of orbits of } \sigma) \) is odd.

So it can't be both (for different expressions as a product of transpositions).

\[ \text{Def: An element of } S_n \text{ is even or odd, depending on whether it can be written as a product of an even or odd number of transpositions.} \]

\[ \text{Def: For all } n \geq 0, \ An = \{ \sigma \in S_n : \sigma \text{ is even} \}. \]

It is a subgroup of \( S_n \), called the alternating group (on n letters).

If \( n = 0 \) or 1, then \( An = S_n = \{ e \} \), so \( |A_n| = 1 = |S_n| = 1 \).

If \( n > 1 \), then \( |An| = |S_n \setminus An| \), because \( \sigma \mapsto \sigma \circ (1, 2) \) is a bijection from \( An \) to \( S_n \setminus An \) (with inverse \( \varrho \mapsto \varrho \circ (1, 2) \)).

So \( |An| = \frac{|S_n|}{2} = \frac{n!}{2} \) for all \( n \geq 2 \).

\[ \text{Example: } S_3 = \{ e, (1), (1, 2, 3), (3, 2, 1), (2, 3), (1, 3), (1, 2) \} \]

\[ P_0 \quad P_1 \quad P_2 \quad P_3 \quad \varrho \quad \tau_2 \quad \tau_3 \]

even permutations = \( A_3 \).

\[ \text{Challenge: } |A_4| = \frac{4!}{2} = \frac{1 \cdot 2 \cdot 3 \cdot 4}{2} = \frac{24}{2} = 12. \text{ List all } 12 \text{ elements.} \]
Cosets

Def.: Let \( H \) be a subgroup of a group \( G \). A left coset of \( H \) in \( G \) is a subset of \( G \) of the form

\[
    aH = \{ ah : h \in H \}
\]

For some \( a \in G \).

In additive notation: \( a+H = \{ a+h : h \in H \} \).

Example: \( G = \mathbb{Z} \), \( H = 3\mathbb{Z} \)

Then \( 1+H = \{ 1+3n : n \in \mathbb{Z} \} = \{ -2, -1, 0, 1, 2, 3, 4, \ldots \} = 4+H \)

Example: The triangles in the Cayley diagram for \( A_4 \) on p.95 are cosets of the subgroup \( H = \langle (1,2,3) \rangle \).

Thm: Let \( H \leq G \). Then the collection of all left cosets of \( H \) in \( G \) is a partition of \( G \).

Proof #1: Define an equivalence relation (see the book).

Proof #2: Show it directly.

The union of all cosets of \( H \) is \( G \) because \( H \subseteq G \), and for all \( a \in G \), \( aH \neq \emptyset \), so \( a \in \text{the union} \). The union of \( H \) is \( G \).

Also all cosets are nonempty, because \( a \in H \) for all \( a \in G \).

Finally, suppose \( aH \cap bH = \emptyset \), so say \( c \notin aH \cap bH \). Then \( c = ah = bh \) with \( h, h' \in H \) and \( a = bh \). Since \( h = h', \) the group gives \( a \in bH \).

Then \( aH \subseteq bH \) because \( a = bh \) with \( h, h' \in H \); \( a \) \ in \( bH \) for all \( h \in H \). Similarly, \( bH \subseteq aH \) is a left coset. Thus, \( aH = bH \).

So two cosets are either equal or disjoint. It's a partition.

You can do all of the above with right cosets instead of left cosets. Right cosets are \( Ha = \{ ha : h \in H \} \) or \( H + a = \{ h+a : h \in H \} \) in additive notation.
Observations: Let $H \leq G$. Then all (left or right) cosets of $H$ in $G$ have the same cardinality.

Proof: For left cosets: fix $a \in G$, and define $\varphi: H \rightarrow aH$ by $\varphi(h) = ah$. Then $\varphi$ is onto by definition of $aH$, and is 1-1 by cancellation ($ah = ah' \Rightarrow h = h'$). Let $|aH| = |H| \forall a \in G$.

Similarly, $|Ha| = |H| \forall a \in G$.

Thm (La Grange): Let $G$ be a finite group and let $H \leq G$.

Then $|H|$ divides $|G|$.

Proof: Let $n = |G|$, $m = |H|$, and let $r$ be the number of left cosets of $H$ in $G$. Then $n = rm$, so $m | n$.

(We've already seen this if $G$ is cyclic.)

Note: In general, if $|G| = n$ and $m | n$ ($m > 0$), then $G$ might not have a subgroup of order $m$.

Or, it may have more than one subgroup of order $m$.

Example: $\langle (1, 2) \rangle \neq \langle (2, 3) \rangle$ are subgroups of $S_3$ of order 2.

Cor: Let $G$ be a finite group and let $a \in G$. Then the order of $a$ divides $|G|$.

Proof: Since $\langle a \rangle$ is a subgroup of $G$, it's order divides $|G|$.

But $|a| = |\langle a \rangle|$, so $|a|$ divides $|G|$.

Cor 2: Every group of prime order is cyclic, and is abelian.

Proof: Let $G$ be a group of order $p$, with $p$ prime.

Let $a \in G$ be an element with $a \neq e$. Then $|a|$ divides $p$ and $|a| \neq 1$, so $|a| = p$; \therefore $\langle a \rangle = G$, so $G$ is cyclic.

Cor 3: All groups of order $< 6$ are abelian.

Proof: Let $G$ be a group with $|G| < 6$. If $|G| = 1$ then $G$ is the trivial group. $(G \text{ cyclic } \iff \langle e \rangle)$, if $|G| = 2, 3, 4, 5$, then it's also cyclic. If $|G| = 4$ then it's either $\mathbb{Z}_4$ or $V$. 