Def: if \( \sigma \in S_n \) can be written as an even (odd) number of transpositions, then we say \( \sigma \) is an even (odd) transposition.
Def: $A_n$ is the set of all even permutations. This (in homework), $A_n$ is a subgroup, called the Alternating group.
Note

\[
\text{odd \cdot odd = even} \\
\text{odd \cdot even = odd} \\
\text{even \cdot even = even}.
\]

\[
|S_n| = n!
\]
Theorem \(|A_n| = \frac{n!}{2}\) for \(n > 2\)

Proof: since \(n > 2\), \((12) \in S_n\) if \(\sigma \in S_n\) is odd

Then \((12)\sigma\) is even

\[
\therefore \text{ # even } \geq \text{ # odds}
\]
if \( \sigma \in S_n \) is even, then

\( (12) \) \( \sigma \) is odd, \ldots

\[ \# \text{ odds} \geq \# \text{ evens}, \]

hence \( \# \text{ odds} = \# \text{ evens} \),

so \( |S_n| = \# \text{ odds} + \# \text{ evens} \)

\[ \Rightarrow \ n^! = 2 \cdot \# \text{ evens} \]

\[ \Rightarrow \ \frac{n^!}{2} = \# \text{ evens} = |A_n| \]
Theorem (not in book)

An m-cycle is an odd permutation if the number m is even.

\( (1\ 2) \) is an odd permutation (even length, \( m = 2 \))

while \((1\ 2\ 3) = (1\ 3)(1\ 2)\) is an even permutation (odd length, \( m = 3 \))
Proof:

Recall

\[(a_1, \ldots, a_m) = (a, m) (a_1, m-1) \cdots (a, a_2)\]

\[\text{length } m\]

\[m \text{ and } m-1 \text{ have opposite parity}\]
Application: check digit scheme

To $a_1, \ldots, a_{n-1}$ add an

5th

$s(a_1) + s(a_2) + \cdots + s(a_n) = 0$

where $s = (01589427)$

and $* $ is in $D_5$
Find the check digit for

\( \sigma = (01589427)(36) \)

\( \sigma(2) = 7 \quad \sigma^2(3) = 3 \quad \sigma^3(4) = 0, \quad \sigma^4(1) = 4 \)

Now we need \( x \) so that \( \sigma^5(x) = b \)

So that \( 7 \times 3 \times 0 \times 4 \times b = 0 \) in \( D_5 \)

\[ 9 \times 4 \times b = 0 \]
\[ 5 \times b = 0 \]

So \( b = 5 \)

So now we need \( x \) so that \( \sigma^5(x) = 5 \)

So \( x = 4 \). Thus the check digit is 4.
Chapter 6

\[ \mathbb{Z}_5 + \{0, 1, 2, 3, 4\} \]

and \( \langle a \rangle = \{ a^0, a^1, a^2, a^3, a^4 \} \)

if \(|a| = 5\)

\[ 1 + 3 \iff a^1 \cdot a^3 \]

\[ 4 \iff a^4 \]
Operation preserving same group table structure
Def. $h$

Isomorphism

A map $\Theta : G \rightarrow H$ where $(G, \ast)$ and $(H, \#)$ are groups is an isomorphism if $\Theta$ is 1-1 and onto and

AND

\[ \Theta(a \ast b) = \Theta(a) \# \Theta(b) \]

\[ \forall a, b \in G \]

\[ \forall \in H \]
If there is such a map,

Then we say \( G \) and \( H \) are isomorphic and write

\[ G \cong H \text{, or } G \simeq H \]