**Def:** The <u>alternating group</u> $A_n \leq S_n$ is the subgroup of $S_n$ consisting of all even permutations.

<u>Why is $A_n$ a group?</u>

- <u>Closure</u>: If $\sigma_1 = \tau_1 \cdots \tau_k$ and $\sigma_2 = \mu_1 \cdots \mu_\ell$, where $\tau_i$ and $\mu_j$ are transpositions, then

$$\sigma_1 \sigma_2 = \tau_1 \cdots \tau_k \mu_1 \cdots \mu_\ell .$$

  If $\sigma_1, \sigma_2 \in A_n$, then $k$ and $\ell$ are both even, so $k+\ell$ is even and $\sigma_1 \sigma_2 \in A_n$.

- <u>Identity</u>: We proved that id is even last time.

- <u>Inverses</u>: If $\sigma = \tau_1 \cdots \tau_k$, where $\tau_i$ are transpositions, then $\sigma^{-1} = \tau_k \cdots \tau_1$, so $\sigma^{-1}$ is even if $\sigma$ is.

<u>**Warm-Up**</u>: List all elements of $A_3$ and $A_4$.

**Thm:** For $n \geq 2$, $|A_n| = \frac{n!}{2}$. That is, exactly half of the permutations in $S_n$ are even, and half are odd.

**Proof:** Define a function

$$f: A_n \to S_n \setminus A_n$$
$$\sigma \mapsto \sigma \cdot (1\ 2).$$

Note that $f$ is well-defined, since $\sigma \cdot (1\ 2)$ is odd if $\sigma$ is even (and $(1\ 2) \in S_n$, since $n \geq 2$).

Then $f$ is injective, since $f(\sigma_1) = f(\sigma_2)$ implies

$$\sigma_1 \cancel{(1\ 2)} = \sigma_2 \cancel{(1\ 2)}$$
$$\sigma_1 = \sigma_2.$$

And $f$ is also surjective: If $\tau \in S_n \setminus A_n$ is odd, then $\tau(1\ 2)$ is even, and

$$f(\tau(1 2)) = \tau(1 2)(1 2) = \tau.$$

Thus, $f$ is a bijection, so $|A_n| = n! - |A_n|$, or $|A_n| = \frac{n!}{2}$. ∎

# Where are we now?

We have compiled a compendium of examples of groups.

| Group | Order | Abelian? |
|---|---|---|
| $\mathbb{Z}_n$ | $n$ | Y |
| $U(n)$ | $\phi(n)$ | Y |
| $\mathbb{Z}$ | $\infty$ | Y |
| $\mathbb{R}$ | $\infty$ | Y |
| $S_n$ | $n!$ | N $(n \geq 3)$ |
| $D_n$ | $2n$ | N |
| $A_n$ | $\frac{n!}{2}$ | N $(n \geq 4)$ |
| $GL_n(\mathbb{R})$ | $\infty$ | N $(n \geq 2)$ |

# Where are we going?

We will prove some general theorems about groups. In doing so, it will be useful to continually refer back to our list of examples.

In particular, here is some "numerology" I'd like to understand:

- $|\mathbb{Z}_n| = n$, and $\mathbb{Z}_n$ has a subgroup of order $d$ for each positive divisor $d | n$.
- $|D_4| = 8$, and $D_4$ has subgroups of orders $1, 2, 4, 8$.
- $|Q_8| = 8$, and $Q_8$ has subgroups of orders $1, 2, 4, 8$.
- $\mathrm{sgn}: S_n \to \{1, -1\}$ has $|\mathrm{sgn}^{-1}(1)| = |A_n| = \frac{|S_n|}{2}$, while $|\{1, -1\}| = 2$ ...