§3.6 Permutation Groups

Shaoyun Yi

MATH 546/701I

University of South Carolina

June 3-4, 2020

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\Bigg\{$

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \end{cases}$

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$:

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n \text{, then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.
  - $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$.
  - $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$.
- Subgroups of $\mathbf{Z}_n$:

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.
  - $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$.
  - $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$.
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.
  - $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$.
  - $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$.
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  $\bullet\ m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m.$ $\quad \bullet\ m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n.$
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.
    (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^{\times}$.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  • $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$. • $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$.
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.
    (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^\times$.
    (ii) If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.

  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  • $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$. • $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$.
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*

  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

  (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^{\times}$.

  (ii) If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.

  (iii) If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  $\bullet\ m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m. \qquad \bullet\ m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n.$
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.
    (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^\times$.
    (ii) If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
    (iii) If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.
- $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_m})$

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  $\bullet\ m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m. \qquad \bullet\ m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n.$
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.
  (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^{\times}$.
  (ii) If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
  (iii) If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.
- $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_m})$
- Let G be a finite abelian group. Let N be the **exponent** of G.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  $\bullet\ m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m. \qquad \bullet\ m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n.$
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.
    (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^\times$.
    (ii) If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
    (iii) If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.
- $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_m})$
- Let G be a finite abelian group. Let N be the **exponent** of G.
  (a) $N = \max\{o(a) \mid a \in G\}$.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  $\bullet\ m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m. \qquad \bullet\ m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n.$
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.
    (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^{\times}$.
    (ii) If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
    (iii) If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.
- $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_m})$
- Let G be a finite abelian group. Let N be the **exponent** of G.
  (a) $N = \max\{o(a) \mid a \in G\}$.
  (b) The group G is cyclic $\Leftrightarrow N = |G|$.

Review from Section 3.5

- Every *subgroup* of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- (a) Any two infinite cyclic groups are isomorphic to each other.
  (b) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

  • $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$. • $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$.
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d]_n \rangle \rightsquigarrow$ *subgroup diagram*
  (a) Let $d = \gcd(m, n)$: $\langle [m]_n \rangle = \langle [d]_n \rangle$ & $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.
    (i) $\langle [k]_n \rangle = \mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n^\times$.
    (ii) If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle \Leftrightarrow d_2|d_1$.
    (iii) If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.
- $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_m})$
- Let G be a finite abelian group. Let N be the **exponent** of G.
  (a) $N = \max\{o(a) \mid a \in G\}$.
  (b) The group G is cyclic $\Leftrightarrow N = |G|$.
- For small n, check $\mathbf{Z}_n^\times$ cyclic or not without using *primitive root thm*.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*:

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle σ of length m has order m, i.e., $o(\sigma) = m$.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle σ of length m has order m, i.e., $o(\sigma) = m$.
- The order of σ is the **lcm** of the *lengths* (*orders*) of its disjoint cycles.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle σ of length m has order m, i.e., $o(\sigma) = m$.
- The order of σ is the **lcm** of the *lengths* (*orders*) of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle σ of length m has order m, i.e., $o(\sigma) = m$.
- The order of σ is the **lcm** of the *lengths* (*orders*) of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a (NOT unique) product of transpositions.

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle σ of length m has order m, i.e., $o(\sigma) = m$.
- The order of σ is the **lcm** of the *lengths* (*orders*) of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a (NOT unique) product of transpositions.
- Product of transpositions: Even permutation *vs.* Odd permutation

Review from Section 2.3

- A **permutation** σ of a set S is a function from S to S that is both one-to-one and onto.
- *Notation*: $\mathrm{Sym}(S) = \{\sigma \mid \sigma : S \to S\}$ or write S_n if $S = \{1, 2, \ldots, n\}$.
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Let $\sigma \in \mathrm{Sym}(S)$. Then $\sigma = (a_1 a_2 \cdots a_k)$ is a cycle of length k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle σ of length m has order m, i.e., $o(\sigma) = m$.
- The order of σ is the **lcm** of the *lengths* (*orders*) of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a (NOT unique) product of transpositions.
- Product of transpositions: Even permutation *vs.* Odd permutation
- A cycle of odd length is even. & A cycle of even length is odd.

Definition

Definition 1

Any subgroup of the symmetric group $\mathrm{Sym}(S)$ on a set S is called a **permutation group**.

Note 1 (Let G be a finite group.)

Definition

Definition 1

Any subgroup of the symmetric group $\mathrm{Sym}(S)$ on a set S is called a **permutation group**.

Note 1 (Let G be a finite group.)

As we have observed, each row in the multiplication table represents a permutation of the group elements.

Definition

Definition 1

Any subgroup of the symmetric group $\mathrm{Sym}(S)$ on a set S is called a **permutation group**.

Note 1 (Let G be a finite group.)

As we have observed, each row in the multiplication table represents a permutation of the group elements. Furthermore, each row corresponds to multiplication by a given element,

Definition

Definition 1

Any subgroup of the symmetric group $\mathrm{Sym}(S)$ on a set S is called a **permutation group**.

Note 1 (Let G be a finite group.)

As we have observed, each row in the multiplication table represents a permutation of the group elements. Furthermore, each row corresponds to multiplication by a given element, and so there is a natural way to assign a permutation to each element $a \in G$.

Definition

Definition 1

Any subgroup of the symmetric group $\mathrm{Sym}(S)$ on a set S is called a **permutation group**.

Note 1 (Let G be a finite group.)

As we have observed, each row in the multiplication table represents a permutation of the group elements. Furthermore, each row corresponds to multiplication by a given element, and so there is a natural way to assign a permutation to each element $a \in G$.

In fact, this natural way will be important in the proof of Cayley's theorem.

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one:

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto:

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G.

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined.

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

(i) Closure:

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

(i) Closure: For any $\lambda_a, \lambda_b \in G_\lambda$ with $a, b \in G$, *to show* $\lambda_a \lambda_b \in G_\lambda$.

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

(i) Closure: For any $\lambda_a, \lambda_b \in G_\lambda$ with $a, b \in G$, *to show* $\lambda_a \lambda_b \in G_\lambda$.

$$\lambda_a \lambda_b(x) = \lambda_a(\lambda_b(x)) = \lambda_a(bx) = a(bx) = (ab)x = \lambda_{ab}(x),$$

for all $x \in G$.

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

(i) Closure: For any $\lambda_a, \lambda_b \in G_\lambda$ with $a, b \in G$, *to show* $\lambda_a \lambda_b \in G_\lambda$.

$$\lambda_a\lambda_b(x) = \lambda_a(\lambda_b(x)) = \lambda_a(bx) = a(bx) = (ab)x = \lambda_{ab}(x),$$

for all $x \in G$. This implies that $\lambda_a\lambda_b = \lambda_{ab} \in G_\lambda$. (Why?)

(ii) Identity:

Cayley's Theorem

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

(i) Closure: For any $\lambda_a, \lambda_b \in G_\lambda$ with $a, b \in G$, *to show* $\lambda_a\lambda_b \in G_\lambda$.

$$\lambda_a\lambda_b(x) = \lambda_a(\lambda_b(x)) = \lambda_a(bx) = a(bx) = (ab)x = \lambda_{ab}(x),$$

for all $x \in G$. This implies that $\lambda_a\lambda_b = \lambda_{ab} \in G_\lambda$. (Why?)

(ii) Identity: λ_e. For any $\lambda_a \in G_\lambda$, $\lambda_a\lambda_e = \lambda_{ae} = \lambda_a$ & $\lambda_e\lambda_a = \lambda_{ea} = \lambda_a$.

(iii) Inverses:

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

(i) Closure: For any $\lambda_a, \lambda_b \in G_\lambda$ with $a, b \in G$, *to show* $\lambda_a\lambda_b \in G_\lambda$.

$$\lambda_a\lambda_b(x) = \lambda_a(\lambda_b(x)) = \lambda_a(bx) = a(bx) = (ab)x = \lambda_{ab}(x),$$

for all $x \in G$. This implies that $\lambda_a\lambda_b = \lambda_{ab} \in G_\lambda$. (Why?)

(ii) Identity: λ_e. For any $\lambda_a \in G_\lambda$, $\lambda_a\lambda_e = \lambda_{ae} = \lambda_a$ & $\lambda_e\lambda_a = \lambda_{ea} = \lambda_a$.

(iii) Inverses: $\lambda_{a^{-1}}$. It is easy to see that $(\lambda_a)^{-1} = \lambda_{a^{-1}}$. (Check it!)

Theorem 2 (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$, for all $x \in G$.

- λ_a is one-to-one: if $\lambda_a(x_1) = \lambda_a(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$. (Why?)
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. (Why?)

Thus, λ_a is a permutation of G. This shows that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined. *Claim:* $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

(i) Closure: For any $\lambda_a, \lambda_b \in G_\lambda$ with $a, b \in G$, *to show* $\lambda_a \lambda_b \in G_\lambda$.

$$\lambda_a\lambda_b(x) = \lambda_a(\lambda_b(x)) = \lambda_a(bx) = a(bx) = (ab)x = \lambda_{ab}(x),$$

for all $x \in G$. This implies that $\lambda_a\lambda_b = \lambda_{ab} \in G_\lambda$. (Why?)

(ii) Identity: λ_e. For any $\lambda_a \in G_\lambda$, $\lambda_a\lambda_e = \lambda_{ae} = \lambda_a$ & $\lambda_e\lambda_a = \lambda_{ea} = \lambda_a$.

(iii) Inverses: $\lambda_{a^{-1}}$. It is easy to see that $(\lambda_a)^{-1} = \lambda_{a^{-1}}$. (Check it!)

Thus, $G_\lambda = \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$.

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined:

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products:

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b).$$

- ϕ is one-to-one:

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b).$$

- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b).$$

- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.

  For all $x \in G$, $\phi(a) = \phi(b) \Rightarrow$

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(ab) = \lambda_{ab} = \lambda_a\lambda_b = \phi(a)\phi(b).$$

- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.

  For all $x \in G$, $\phi(a) = \phi(b) \Rightarrow \lambda_a(x) = \lambda_b(x) \Rightarrow$

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b).$$

- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.

  For all $x \in G$, $\phi(a) = \phi(b) \Rightarrow \lambda_a(x) = \lambda_b(x) \Rightarrow ax = bx \Rightarrow$

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

  $$\phi(ab) = \lambda_{ab} = \lambda_a\lambda_b = \phi(a)\phi(b).$$
- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.

  For all $x \in G$, $\phi(a) = \phi(b) \Rightarrow \lambda_a(x) = \lambda_b(x) \Rightarrow ax = bx \Rightarrow a = b$.
- ϕ is onto:

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.
  $$\phi(ab) = \lambda_{ab} = \lambda_a\lambda_b = \phi(a)\phi(b).$$
- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.
  For all $x \in G$, $\phi(a) = \phi(b) \Rightarrow \lambda_a(x) = \lambda_b(x) \Rightarrow ax = bx \Rightarrow a = b$.
- ϕ is onto: Trivial. By the definition of $G_\lambda = \phi(G)$.

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b).$$

- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.

  For all $x \in G$, $\phi(a) = \phi(b) \Rightarrow \lambda_a(x) = \lambda_b(x) \Rightarrow ax = bx \Rightarrow a = b$.
- ϕ is onto: Trivial. By the definition of $G_\lambda = \phi(G)$.

Thus, ϕ is a group isomorphism.

Proof of Cayley's Theorem cont.: *To show* $G \cong G_\lambda$.

Define $\phi : G \to G_\lambda$ by $\phi(a) = \lambda_a$. *To show* ϕ is a group isomorphism.

- well-defined: Trivial. ✓
- ϕ preserves products: For any $a, b \in G$, *to show* $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b).$$

- ϕ is one-to-one: If $\phi(a) = \phi(b)$ for $a, b \in G$, then it is *to show* $a = b$.

  For all $x \in G$, $\phi(a) = \phi(b) \Rightarrow \lambda_a(x) = \lambda_b(x) \Rightarrow ax = bx \Rightarrow a = b$.
- ϕ is onto: Trivial. By the definition of $G_\lambda = \phi(G)$.

Thus, ϕ is a group isomorphism.

So, $G \cong G_\lambda$, where G_λ is a subgroup of $\mathrm{Sym}(G)$, i.e., a permutation group.

Example: Rigid motions of a square

Definition 3 (Rigid Motion:)

a change in position where the distance between points is preserved and figures remain congruent (having the same size and shape). It may be

- a translation (slide)
- a reflection (flip)
- a rotation (turn)
- or a combination of these.

Example: Rigid motions of a square

Definition 3 (Rigid Motion:)

a change in position where the distance between points is preserved and figures remain congruent (having the same size and shape). It may be

- a translation (slide)
- a reflection (flip)
- a rotation (turn)
- or a combination of these.

Each of the rigid motions determines a permutation of the vertices of the square,

Example: Rigid motions of a square

Definition 3 (Rigid Motion:)

a change in position where the distance between points is preserved and figures remain congruent (having the same size and shape). It may be

- a translation (slide)
- a reflection (flip)
- a rotation (turn)
- or a combination of these.

Each of the rigid motions determines a permutation of the vertices of the square, and the permutation notation gives a convenient way to describe these motions.

Example: Rigid motions of a square

Definition 3 (Rigid Motion:)

a change in position where the distance between points is preserved and figures remain congruent (having the same size and shape). It may be

- a translation (slide)
- a reflection (flip)
- a rotation (turn)
- or a combination of these.

Each of the rigid motions determines a permutation of the vertices of the square, and the permutation notation gives a convenient way to describe these motions.

There are a total of **eight** rigid motions of a square. (Why?)

Example: Rigid motions of a square

Definition 3 (Rigid Motion:)

a change in position where the distance between points is preserved and figures remain congruent (having the same size and shape). It may be

- a translation (slide)
- a reflection (flip)
- a rotation (turn)
- or a combination of these.

Each of the rigid motions determines a permutation of the vertices of the square, and the permutation notation gives a convenient way to describe these motions.

There are a total of **eight** rigid motions of a square. (Why?)

- There are **four** choices of a position in which to place first vertex A,

Example: Rigid motions of a square

Definition 3 (Rigid Motion:)

a change in position where the distance between points is preserved and figures remain congruent (having the same size and shape). It may be

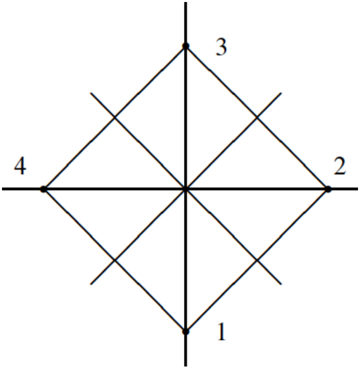
- a translation (slide)
- a reflection (flip)
- a rotation (turn)
- or a combination of these.

Each of the rigid motions determines a permutation of the vertices of the square, and the permutation notation gives a convenient way to describe these motions.

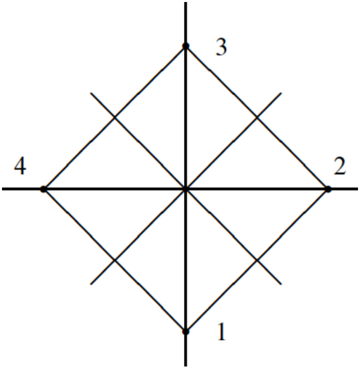
There are a total of **eight** rigid motions of a square. (Why?)

- There are **four** choices of a position in which to place first vertex A,
- and then **two** choices for second vertex since it must be adjacent to A.

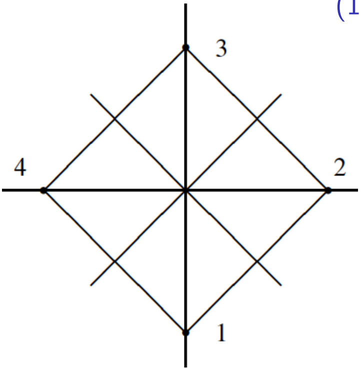
Example cont.: Rigid motions of a square



Example cont.: Rigid motions of a square

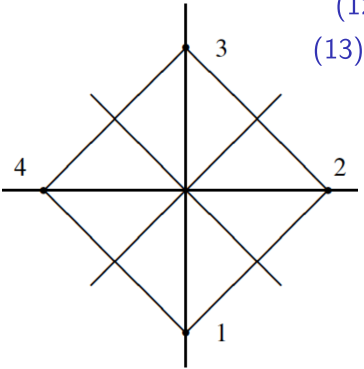


Example cont.: Rigid motions of a square



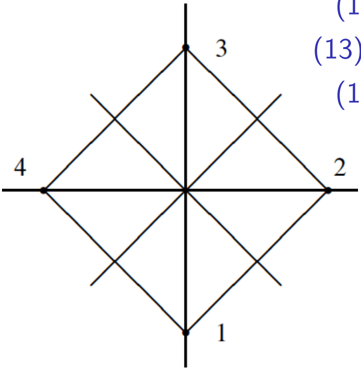
(1234) counterclockwise rotation through 90°

Example cont.: Rigid motions of a square



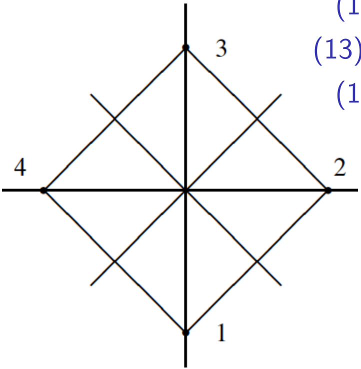
(1234)	counterclockwise rotation through 90°
(13)(24)	counterclockwise rotation through 180°

Example cont.: Rigid motions of a square



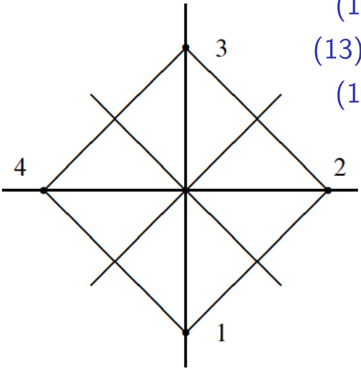
(1234)	counterclockwise rotation through 90°
(13)(24)	counterclockwise rotation through 180°
(1432)	counterclockwise rotation through 270°

Example cont.: Rigid motions of a square



(1234)	counterclockwise rotation through 90°
(13)(24)	counterclockwise rotation through 180°
(1432)	counterclockwise rotation through 270°
(1)	counterclockwise rotation through 360°

Example cont.: Rigid motions of a square



(1234) counterclockwise rotation through 90°

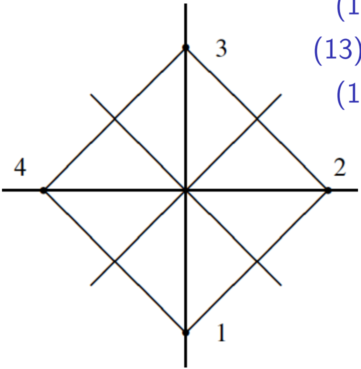
(13)(24) counterclockwise rotation through 180°

(1432) counterclockwise rotation through 270°

(1) counterclockwise rotation through 360°

(24) flip about vertical axis

Example cont.: Rigid motions of a square



(1234) counterclockwise rotation through 90°

(13)(24) counterclockwise rotation through 180°

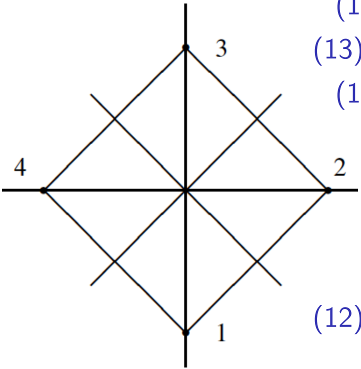
(1432) counterclockwise rotation through 270°

(1) counterclockwise rotation through 360°

(24) flip about vertical axis

(13) flip about horizontal axis

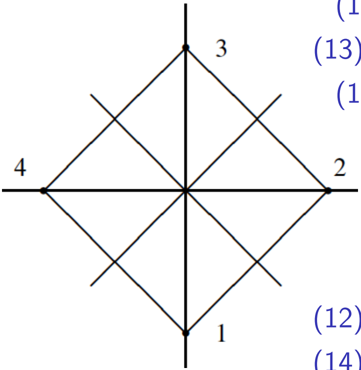
Example cont.: Rigid motions of a square



(1234) counterclockwise rotation through 90°
(13)(24) counterclockwise rotation through 180°
(1432) counterclockwise rotation through 270°
(1) counterclockwise rotation through 360°

(24) flip about vertical axis
(13) flip about horizontal axis
(12)(34) flip about diagonal

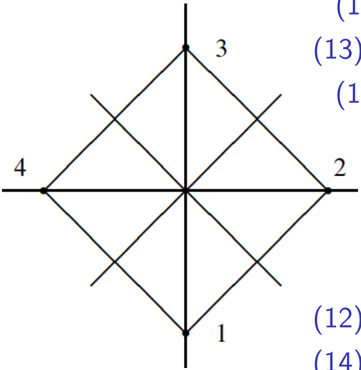
Example cont.: Rigid motions of a square



(1234)	counterclockwise rotation through 90°
(13)(24)	counterclockwise rotation through 180°
(1432)	counterclockwise rotation through 270°
(1)	counterclockwise rotation through 360°
(24)	flip about vertical axis
(13)	flip about horizontal axis
(12)(34)	flip about diagonal
(14)(23)	flip about diagonal

Note 2

Example cont.: Rigid motions of a square



(1234) counterclockwise rotation through 90°
(13)(24) counterclockwise rotation through 180°
(1432) counterclockwise rotation through 270°
(1) counterclockwise rotation through 360°

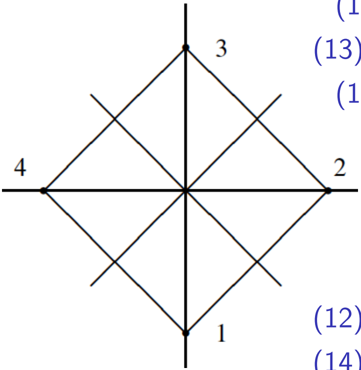
(24) flip about vertical axis
(13) flip about horizontal axis

(12)(34) flip about diagonal
(14)(23) flip about diagonal

Note 2

Note that we do not obtain all elements of S_4 as rigid motion, since, for example,

Example cont.: Rigid motions of a square



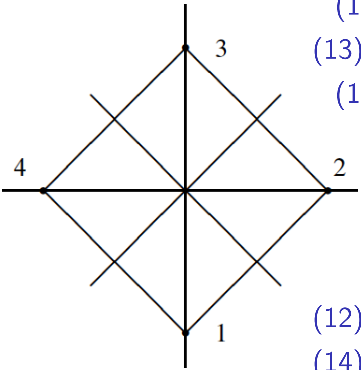
(1234)	counterclockwise rotation through 90°
(13)(24)	counterclockwise rotation through 180°
(1432)	counterclockwise rotation through 270°
(1)	counterclockwise rotation through 360°
(24)	flip about vertical axis
(13)	flip about horizontal axis
(12)(34)	flip about diagonal
(14)(23)	flip about diagonal

Note 2

Note that we do not obtain all elements of S_4 as rigid motion, since, for example, (12) would represent an impossible configuration.

Question 1

Example cont.: Rigid motions of a square



(1234)	counterclockwise rotation through 90°
(13)(24)	counterclockwise rotation through 180°
(1432)	counterclockwise rotation through 270°
(1)	counterclockwise rotation through 360°
(24)	flip about vertical axis
(13)	flip about horizontal axis
(12)(34)	flip about diagonal
(14)(23)	flip about diagonal

Note 2

Note that we do not obtain all elements of S_4 as rigid motion, since, for example, (12) would represent an impossible configuration.

Question 1

What is the order of each rigid motion?

Rigid motions of a square: Multiplication table

Rigid motions of a square: Multiplication table

	(1)	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)
(1)	(1)	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)
(1234)	(1234)	(13)(24)	(1432)	(1)	(12)(34)	(13)	(14)(23)	(24)
(13)(24)	(13)(24)	(1432)	(1)	(1234)	(13)	(14)(23)	(24)	(12)(34)
(1432)	(1432)	(1)	(1234)	(13)(24)	(14)(23)	(24)	(12)(34)	(13)
(24)	(24)	(14)(23)	(13)	(12)(34)	(1)	(1432)	(13)(24)	(1234)
(12)(34)	(12)(34)	(24)	(14)(23)	(13)	(1234)	(1)	(1432)	(13)(24)
(13)	(13)	(12)(34)	(24)	(14)(23)	(13)(24)	(1234)	(1)	(1432)
(14)(23)	(14)(23)	(13)	(12)(34)	(24)	(1432)	(13)(24)	(1234)	(1)

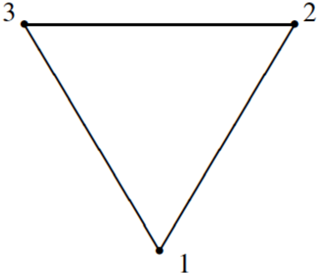
Example: Rigid motions of an equilateral triangle

Proposition 1

Example: Rigid motions of an equilateral triangle

Proposition 1

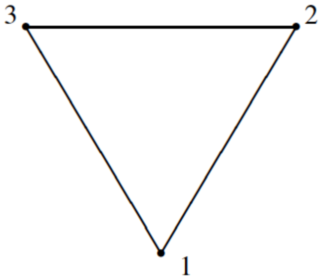
The rigid motions of an equilateral triangle yield the group S_3.



Example: Rigid motions of an equilateral triangle

Proposition 1

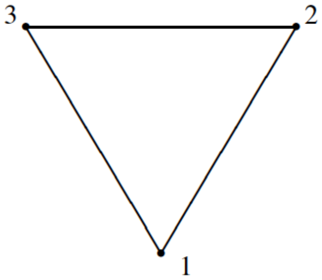
The rigid motions of an equilateral triangle yield the group S_3.



Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.

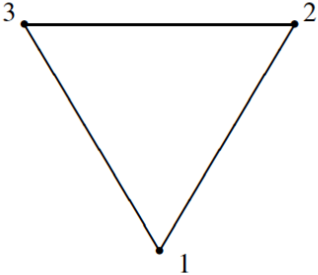


(123) counterclockwise rotation through 120°

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.



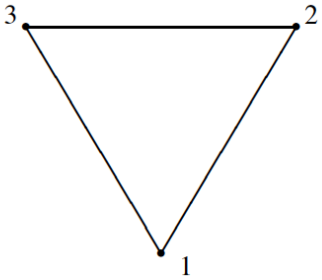
(123) counterclockwise rotation through 120°

(132) counterclockwise rotation through 240°

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.

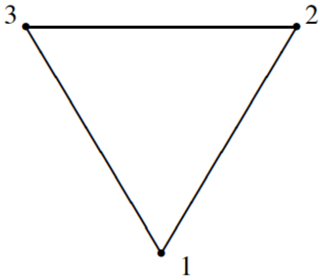


- (123) counterclockwise rotation through 120°
- (132) counterclockwise rotation through 240°
- (1) counterclockwise rotation through 360°

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.



(123) counterclockwise rotation through 120°

(132) counterclockwise rotation through 240°

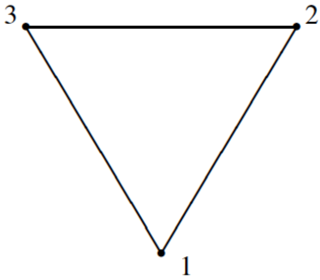
(1) counterclockwise rotation through 360°

(23) flip about vertical axis

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.

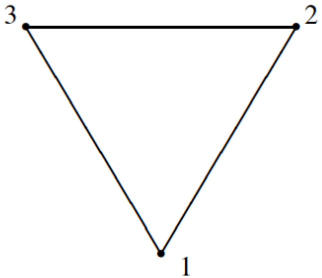


- (123) counterclockwise rotation through 120°
- (132) counterclockwise rotation through 240°
- (1) counterclockwise rotation through 360°
- (23) flip about vertical axis
- (13) flip about angle bisector

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.



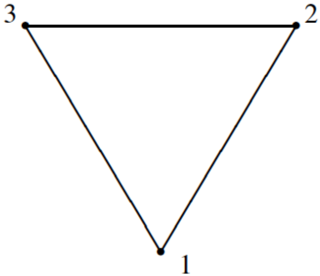
(123)	counterclockwise rotation through 120°
(132)	counterclockwise rotation through 240°
(1)	counterclockwise rotation through 360°
(23)	flip about vertical axis
(13)	flip about angle bisector
(12)	flip about angle bisector

Note 3 (Another notion for describing S_3 in §3.3)

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.



(123) counterclockwise rotation through 120°

(132) counterclockwise rotation through 240°

(1) counterclockwise rotation through 360°

(23) flip about vertical axis

(13) flip about angle bisector

(12) flip about angle bisector

Note 3 (Another notion for describing S_3 in §3.3)

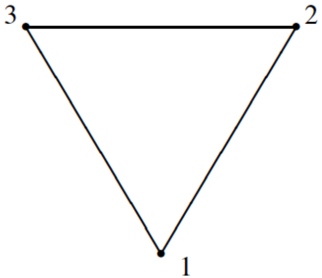
$S_3 = \{e, a, a^2, b, ab, a^2b\}$, *where* $a^3 = e$, $b^2 = e$, $ba = a^2b = a^{-1}b$.

Note 4 (Another notion for describing Rigid Motions of a Square)

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.



(123) counterclockwise rotation through 120°

(132) counterclockwise rotation through 240°

(1) counterclockwise rotation through 360°

(23) flip about vertical axis

(13) flip about angle bisector

(12) flip about angle bisector

Note 3 (Another notion for describing S_3 in §3.3)

$S_3 = \{e, a, a^2, b, ab, a^2b\}$, *where* $a^3 = e$, $b^2 = e$, $ba = a^2b = a^{-1}b$.

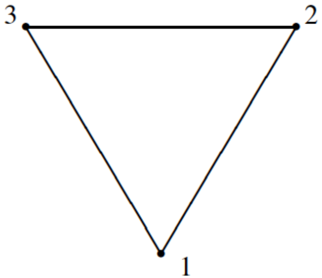
Note 4 (Another notion for describing Rigid Motions of a Square)

Let $a = (1234)$ *and* $b = (24)$. *It can be shown that* $ba = a^3b$.

Example: Rigid motions of an equilateral triangle

Proposition 1

The rigid motions of an equilateral triangle yield the group S_3.



- (123) counterclockwise rotation through 120°
- (132) counterclockwise rotation through 240°
- (1) counterclockwise rotation through 360°
- (23) flip about vertical axis
- (13) flip about angle bisector
- (12) flip about angle bisector

Note 3 (Another notion for describing S_3 in §3.3)

$S_3 = \{e, a, a^2, b, ab, a^2b\}$, *where* $a^3 = e$, $b^2 = e$, $ba = a^2b = a^{-1}b$.

Note 4 (Another notion for describing Rigid Motions of a Square)

Let $a = (1234)$ *and* $b = (24)$. *It can be shown that* $ba = a^3b$. *The group* $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, *where* $a^4 = e$, $b^2 = e$, $ba = a^3b = a^{-1}b$.

Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

i) There are n choices of a position in which to place first vertex A,

Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

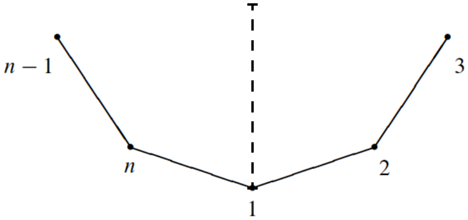
i) There are n choices of a position in which to place first vertex A,
ii) and then two choices for second vertex since it must be adjacent to A.

Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

i) There are n choices of a position in which to place first vertex A,
ii) and then two choices for second vertex since it must be adjacent to A.



i)

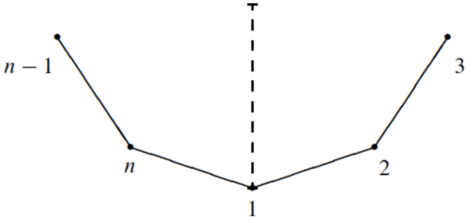
Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

i) There are n choices of a position in which to place first vertex A,

ii) and then two choices for second vertex since it must be adjacent to A.



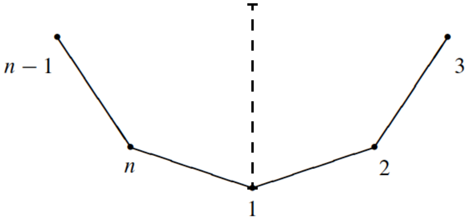
i) Let a be a counterclockwise rotation about the center, through $360/n$ degrees.

Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

i) There are n choices of a position in which to place first vertex A,
ii) and then two choices for second vertex since it must be adjacent to A.



i) Let a be a counterclockwise rotation about the center, through $360/n$ degrees. Thus a is a the cycle $(123 \cdots n)$ of length n and has order n.
ii)

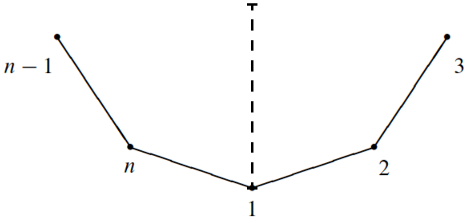
Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

i) There are n choices of a position in which to place first vertex A,

ii) and then two choices for second vertex since it must be adjacent to A.



i) Let a be a counterclockwise rotation about the center, through $360/n$ degrees. Thus a is a the cycle $(123 \cdots n)$ of length n and has order n.

ii) Let b be a flip about the line of symmetry through position number 1.

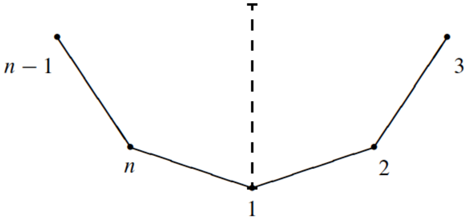
Example: Rigid motions of a regular polygon (n-gon)

Proposition 2

There are $2n$ rigid motions of a regular n-gon.

i) There are n choices of a position in which to place first vertex A,

ii) and then two choices for second vertex since it must be adjacent to A.



i) Let a be a counterclockwise rotation about the center, through $360/n$ degrees. Thus a is a the cycle $(123 \cdots n)$ of length n and has order n.

ii) Let b be a flip about the line of symmetry through position number 1. Thus b has order 2 and is given by the product of transpositions $(2n)(3\ n-1)\cdots$.

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [a^k does NOT flip the n-gon]

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [a^k does NOT flip the n-gon]

Thus, $|S| = 2n$, and so $G = S$.

Note 5 (Notion for describing Rigid Motions of a regular n-gon)

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [a^k does NOT flip the n-gon]

Thus, $|S| = 2n$, and so $G = S$.

Note 5 (Notion for describing Rigid Motions of a regular n-gon)

$G = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{n-1} b = a^{-1} b.$

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [a^k does NOT flip the n-gon]

Thus, $|S| = 2n$, and so $G = S$.

Note 5 (Notion for describing Rigid Motions of a regular n-gon)

$G = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e$, $b^2 = e$, $ba = a^{n-1} b = a^{-1} b$.

Goal: *To show* $ba = a^{-1} b$.

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [a^k does NOT flip the n-gon]

Thus, $|S| = 2n$, and so $G = S$.

Note 5 (Notion for describing Rigid Motions of a regular n-gon)

$G = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{n-1}b = a^{-1}b.$

Goal: *To show* $ba = a^{-1}b$. **Note:** $a^{-1} = a^{n-1}$ (Why?)&

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [a^k does NOT flip the n-gon]

Thus, $|S| = 2n$, and so $G = S$.

Note 5 (Notion for describing Rigid Motions of a regular n-gon)

$G = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{n-1}b = a^{-1}b.$

Goal: *To show* $ba = a^{-1}b$. **Note:** $a^{-1} = a^{n-1}$ (Why?)& $b^{-1} = b$ (Why?)

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \le k < n\}$ of rigid motions.

- The elements a^k for $0 \le k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \le k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \ne a^j b$ for all $0 \le k, j < n$. (Why?) [a^k does NOT flip the n-gon]

Thus, $|S| = 2n$, and so $G = S$.

Note 5 (Notion for describing Rigid Motions of a regular n-gon)

$G = \{a^k, a^k b \mid 0 \le k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{n-1}b = a^{-1}b.$

Goal: *To show* $ba = a^{-1}b$. **Note:** $a^{-1} = a^{n-1}$ (Why?)& $b^{-1} = b$ (Why?)

That is, *to show* $bab = a^{-1}$.

Example cont.: Rigid motions of a regular polygon (n-gon)

Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions.

- The elements a^k for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- The elements $a^k b$ for $0 \leq k < n$ are all distinct. (Why?) [$o(a) = n$]
- $a^k \neq a^j b$ for all $0 \leq k, j < n$. (Why?) [a^k does NOT flip the n-gon]

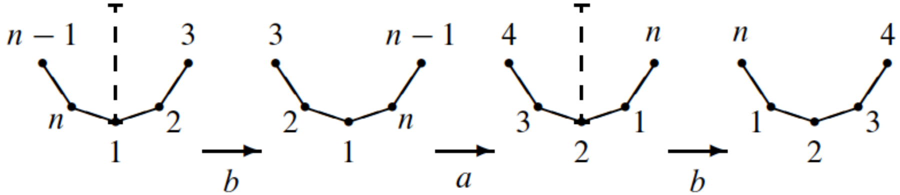
Thus, $|S| = 2n$, and so $G = S$.

Note 5 (Notion for describing Rigid Motions of a regular n-gon)

$G = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e$, $b^2 = e$, $ba = a^{n-1} b = a^{-1} b$.

Goal: *To show* $ba = a^{-1} b$. **Note:** $a^{-1} = a^{n-1}$ (Why?)& $b^{-1} = b$ (Why?)

That is, *to show* $bab = a^{-1}$.



Dihedral group D_n

Definition 4

Dihedral group D_n

Definition 4

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

Proposition 3 (Note 5)

Dihedral group D_n

Definition 4

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

Proposition 3 (Note 5)

$D_n = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{-1}b$.

Remark 1 (Let $n \geq 4$.)

Dihedral group D_n

Definition 4

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

Proposition 3 (Note 5)

$D_n = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{-1}b.$

Remark 1 (Let $n \geq 4$.)

- *We will not list all the subgroups of S_n. (Why?) [*

Dihedral group D_n

Definition 4

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

Proposition 3 (Note 5)

$D_n = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{-1}b$.

Remark 1 (Let $n \geq 4$.)

- *We will not list all the subgroups of S_n. (Why?) [there are too many!!]*

Dihedral group D_n

Definition 4

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

Proposition 3 (Note 5)

$D_n = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{-1}b$.

Remark 1 (Let $n \geq 4$.)

- *We will not list all the subgroups of S_n. (Why?) [there are too many!!]*
- *The "simple" subgroups of S_n: cyclic subgroup generated by $\sigma \in S_n$.*

Dihedral group D_n

Definition 4

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

Proposition 3 (Note 5)

$D_n = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{-1}b$.

Remark 1 (Let $n \geq 4$.)

- *We will not list all the subgroups of S_n. (Why?) [there are too many!!]*
- *The "simple" subgroups of S_n: cyclic subgroup generated by $\sigma \in S_n$.*
- *The dihedral group D_n is one important example of subgroups of S_n.*

Dihedral group D_n

Definition 4

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

Proposition 3 (Note 5)

$D_n = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{-1}b$.

Remark 1 (Let $n \geq 4$.)

- *We will not list all the subgroups of S_n. (Why?) [there are too many!!]*
- *The "simple" subgroups of S_n: cyclic subgroup generated by $\sigma \in S_n$.*
- *The dihedral group D_n is one important example of subgroups of S_n.*
- *The alternating group A_n is another one important example. (soon!)*

Example: Subgroups of $D_3 = S_3$

Proposition 4

Example: Subgroups of $D_3 = S_3$

Proposition 4

If $G = S_3$, then every proper subgroup of S_3 is cyclic. (Why?)

Example: Subgroups of $D_3 = S_3$

Proposition 4

If $G = S_3$, then every proper subgroup of S_3 is cyclic. (Why?)

By Lagrange's theorem, a proper subgroup of S_3 must have order $1, 2$, or 3.

Example: Subgroups of $D_3 = S_3$

Proposition 4

If $G = S_3$, then every proper subgroup of S_3 is cyclic. (Why?)

By Lagrange's theorem, a proper subgroup of S_3 must have order $1, 2$, or 3. And subgroups of order 2 or 3 must be cyclic. (Why?) &

Example: Subgroups of $D_3 = S_3$

Proposition 4

If $G = S_3$, then every proper subgroup of S_3 is cyclic. (Why?)

By Lagrange's theorem, a proper subgroup of S_3 must have order $1, 2$, or 3. And subgroups of order 2 or 3 must be cyclic. (Why?) & $\{e\}$ is trivial.✓

The subgroup diagram of S_3 :

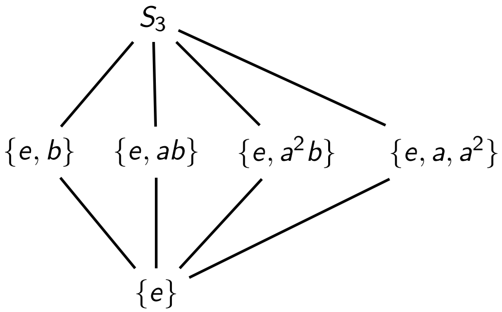
Example: Subgroups of $D_3 = S_3$

Proposition 4

If $G = S_3$, then every proper subgroup of S_3 is cyclic. (Why?)

By Lagrange's theorem, a proper subgroup of S_3 must have order $1, 2$, or 3. And subgroups of order 2 or 3 must be cyclic. (Why?) & $\{e\}$ is trivial.✓

The subgroup diagram of S_3 :

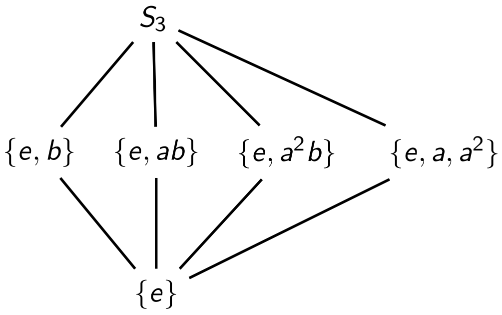


Example: Subgroups of $D_3 = S_3$

Proposition 4

If $G = S_3$, then every proper subgroup of S_3 is cyclic. (Why?)

By Lagrange's theorem, a proper subgroup of S_3 must have order $1, 2$, or 3. And subgroups of order 2 or 3 must be cyclic. (Why?) & $\{e\}$ is trivial.✓
The subgroup diagram of S_3 :



Note that $D_3 = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e, ba = a^2b$.

Subgroups of D_4

Note:

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e$, $b^2 = e$, $ba = a^3b$.

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.
II. The cyclic (proper) subgroups:

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:

   (a) a has order 4. In fact,

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:

  (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:

   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)

   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic?

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.
II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)
III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:

   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)

   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)

   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
   (ii) Any non-identity element of H has order 2. (Why?)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
   (ii) Any non-identity element of H has order 2. (Why?)
   (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
   (ii) Any non-identity element of H has order 2. (Why?)
   (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
   (iv) Consider all possible pairs of elements of order 2 to find all such H's.
   (v) In fact,

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
  (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
  (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
  (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
  (ii) Any non-identity element of H has order 2. (Why?)
  (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
  (iv) Consider all possible pairs of elements of order 2 to find all such H's.
  (v) In fact, there are two such groups. (Check it!)

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
  - (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
  - (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
  - (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
  - (ii) Any non-identity element of H has order 2. (Why?)
  - (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
  - (iv) Consider all possible pairs of elements of order 2 to find all such H's.
  - (v) In fact, there are two such groups. (Check it!)
    - (1) $H_1 = \{e, a^2, b, a^2b\}$:

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
  (a) a has order 4. In fact, $\langle a\rangle = \langle a^3\rangle = \{e, a, a^2, a^3\}$. (Why?)
  (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
  (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
  (ii) Any non-identity element of H has order 2. (Why?)
  (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
  (iv) Consider all possible pairs of elements of order 2 to find all such H's.
  (v) In fact, there are two such groups. (Check it!)
    (1) $H_1 = \{e, a^2, b, a^2b\}$: $ba^2 = (ba)a = a^3(ba) = a^3(a^3b) = a^2b$ ✓

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
   (ii) Any non-identity element of H has order 2. (Why?)
   (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
   (iv) Consider all possible pairs of elements of order 2 to find all such H's.
   (v) In fact, there are two such groups. (Check it!)
      (1) $H_1 = \{e, a^2, b, a^2b\}$: $ba^2 = (ba)a = a^3(ba) = a^3(a^3b) = a^2b$ ✓
      (2) $H_2 = \{e, a^2, ab, a^3b\}$:

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
   (ii) Any non-identity element of H has order 2. (Why?)
   (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
   (iv) Consider all possible pairs of elements of order 2 to find all such H's.
   (v) In fact, there are two such groups. (Check it!)
      (1) $H_1 = \{e, a^2, b, a^2b\}$: $ba^2 = (ba)a = a^3(ba) = a^3(a^3b) = a^2b$ ✓
      (2) $H_2 = \{e, a^2, ab, a^3b\}$: $(ab)a^2 = a(ba)a = a(a^3b)a = ba = a^3b$ ✓

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a\rangle = \langle a^3\rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
   (ii) Any non-identity element of H has order 2. (Why?)
   (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
   (iv) Consider all possible pairs of elements of order 2 to find all such H's.
   (v) In fact, there are two such groups. (Check it!)
      (1) $H_1 = \{e, a^2, b, a^2b\}$: $ba^2 = (ba)a = a^3(ba) = a^3(a^3b) = a^2b$ ✓
      (2) $H_2 = \{e, a^2, ab, a^3b\}$: $(ab)a^2 = a(ba)a = a(a^3b)a = ba = a^3b$ ✓
   (vi) A cyclic subgroup is the smallest subgroup containing the generator;

Subgroups of D_4

Note: $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b$.
The possible orders of proper subgroups of D_4 are 1, 2, or 4. (Why?)

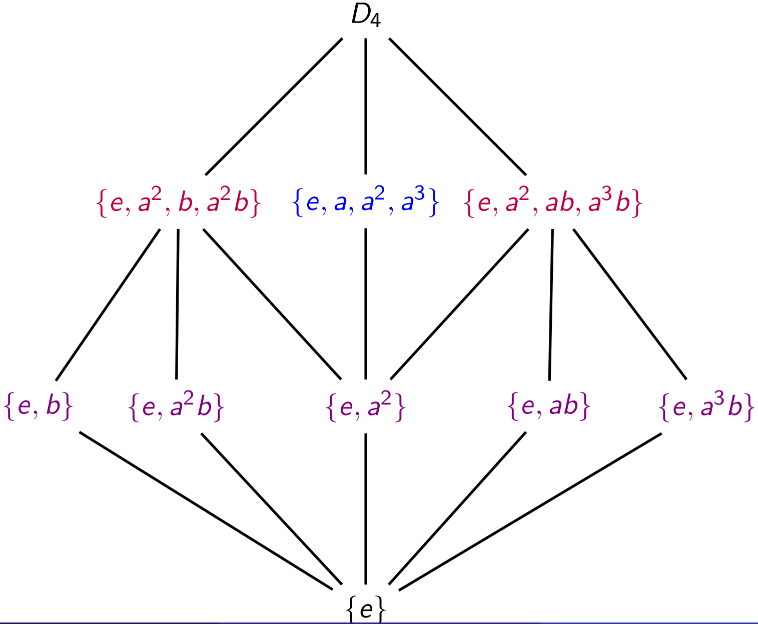
I. The trivial subgroups: $\{e\}, D_4$.

II. The cyclic (proper) subgroups:
   (a) a has order 4. In fact, $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$. (Why?)
   (b) Each of the elements a^2, b, ab, a^2b, a^3b has order 2. (Check it!)

III. Are there (proper) subgroups of D_4 that are not cyclic? Yes! (How?)
   (i) If H is a non-cyclic (proper) subgroup, then $|H| = 4$. (Why?)
   (ii) Any non-identity element of H has order 2. (Why?)
   (iii) $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: Say, $H = \{e, x, y, xy\}$, and so $yx = xy$. (Why?)
   (iv) Consider all possible pairs of elements of order 2 to find all such H's.
   (v) In fact, there are two such groups. (Check it!)
      (1) $H_1 = \{e, a^2, b, a^2b\}$: $ba^2 = (ba)a = a^3(ba) = a^3(a^3b) = a^2b$ ✓
      (2) $H_2 = \{e, a^2, ab, a^3b\}$: $(ab)a^2 = a(ba)a = a(a^3b)a = ba = a^3b$ ✓
   (vi) A cyclic subgroup is the smallest subgroup containing the generator; these subgroups H's are the smallest ones containing the two elements used to construct it.

Subgroups of D_4 cont.: Subgroup diagram

Subgroups of D_4 cont.: Subgroup diagram



Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

(i) Nonempty:

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

(i) Nonempty: The identity permutation is even. (Why?) [

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

(i) Nonempty: The identity permutation is even. (Why?) $[(1) = (12)(21)]$

(ii) Closure:

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

(i) Nonempty: The identity permutation is even. (Why?) [$(1) = (12)(21)$]

(ii) Closure: If σ and τ are even permutations, so is $\tau\sigma$. (Why?) □

Definition 5

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

(i) Nonempty: The identity permutation is even. (Why?) $[(1) = (12)(21)]$

(ii) Closure: If σ and τ are even permutations, so is $\tau\sigma$. (Why?) □

Definition 5

The set of all even permutations of S_n is called the **alternating group** on n elements, and will be denoted by A_n.

Theorem 6 (Let $n > 1$.)

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

(i) Nonempty: The identity permutation is even. (Why?) [$(1) = (12)(21)$]

(ii) Closure: If σ and τ are even permutations, so is $\tau\sigma$. (Why?) □

Definition 5

The set of all even permutations of S_n is called the **alternating group** on n elements, and will be denoted by A_n.

Theorem 6 (Let $n > 1$.)

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Alternating group A_n

Recall that a permutation is called **even** if it can be expressed as an even number of transpositions, and **odd** otherwise.

Proposition 5

The set of all even permutations of S_n is a subgroup of S_n.

Since S_n is a finite set, we can apply Corollary 8 in §3.2. In particular,

(i) Nonempty: The identity permutation is even. (Why?) [$(1) = (12)(21)$]

(ii) Closure: If σ and τ are even permutations, so is $\tau\sigma$. (Why?) □

Definition 5

The set of all even permutations of S_n is called the **alternating group** on n elements, and will be denoted by A_n.

Theorem 6 (Let $n > 1$.)

$|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$. *This is the largest possible cardinality for a proper subgroup.*

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note:

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

We have $S_n = A_n \bigsqcup O_n$ (Why?),

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

We have $S_n = A_n \bigsqcup O_n$ (Why?), so $|S_n| = |A_n| + |O_n|$.

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

$$\text{We have } S_n = A_n \bigsqcup O_n \text{ (Why?), so } |S_n| = |A_n| + |O_n|.$$

I. For each odd permutation σ, the permutation $(12)\sigma$ is even. (Why?)

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

We have $S_n = A_n \bigsqcup O_n$ (Why?), so $|S_n| = |A_n| + |O_n|$.

I. For each odd permutation σ, the permutation $(12)\sigma$ is even. (Why?) If σ and τ are two distinct odd permutations, then $(12)\sigma \neq (12)\tau$.

Proof by contradiction:

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

We have $S_n = A_n \bigsqcup O_n$ (Why?), so $|S_n| = |A_n| + |O_n|$.

I. For each odd permutation σ, the permutation $(12)\sigma$ is even. (Why?)
If σ and τ are two distinct odd permutations, then $(12)\sigma \neq (12)\tau$.

Proof by contradiction: Suppose $(12)\sigma = (12)\tau$, then $\sigma \overset{!}{=} \tau$. (Why?)

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

We have $S_n = A_n \bigsqcup O_n$ (Why?), so $|S_n| = |A_n| + |O_n|$.

I. For each odd permutation σ, the permutation $(12)\sigma$ is even. (Why?)
If σ and τ are two distinct odd permutations, then $(12)\sigma \neq (12)\tau$.

Proof by contradiction: Suppose $(12)\sigma = (12)\tau$, then $\sigma \overset{!}{=} \tau$. (Why?)

Thus, $|A_n| \geq |O_n|$. (Why?)

II. Similarly,

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

We have $S_n = A_n \bigsqcup O_n$ (Why?), so $|S_n| = |A_n| + |O_n|$.

I. For each odd permutation σ, the permutation $(12)\sigma$ is even. (Why?)
If σ and τ are two distinct odd permutations, then $(12)\sigma \neq (12)\tau$.

Proof by contradiction: Suppose $(12)\sigma = (12)\tau$, then $\sigma \overset{!}{=} \tau$. (Why?)

Thus, $|A_n| \geq |O_n|$. (Why?)

II. Similarly, we can show that $|O_n| \geq |A_n|$.

Proof of Theorem 6: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ for $n > 1$.

Let O_n be the set of odd permutations in S_n. Note: O_n is not a subgroup. (Why?)

We have $S_n = A_n \bigsqcup O_n$ (Why?), so $|S_n| = |A_n| + |O_n|$.

I. For each odd permutation σ, the permutation $(12)\sigma$ is even. (Why?) If σ and τ are two distinct odd permutations, then $(12)\sigma \neq (12)\tau$.

Proof by contradiction: Suppose $(12)\sigma = (12)\tau$, then $\sigma \overset{!}{=} \tau$. (Why?)

Thus, $|A_n| \geq |O_n|$. (Why?)

II. Similarly, we can show that $|O_n| \geq |A_n|$.

III. Therefore, $|A_n| = |O_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. (Why?)

Example: List all the elements of A_3 and A_4.

- Recall that

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then we have
$$A_3 = \{(1), (123), (132)\}. \text{ (Why?)}$$

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then we have
$$A_3 = \{(1), (123), (132)\}. \text{ (Why?)}$$
- $|S_4| = 4! = 24$:

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1),(12),(13),(23),(123),(132)\}$, then we have
$$A_3 = \{(1),(123),(132)\}. \text{ (Why?)}$$
- $|S_4| = 4! = 24$: List all the possible *decomposition types* of elements.

Definition 7

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1),(12),(13),(23),(123),(132)\}$, then we have
  $$A_3 = \{(1),(123),(132)\}.\ \text{(Why?)}$$
- $|S_4| = 4! = 24$: List all the possible *decomposition types* of elements.

Definition 7

The **decomposition type** of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.

Upshot: Possible decomposition types of permutations of S_4: (Check it!)

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then we have
$$A_3 = \{(1), (123), (132)\}. \text{ (Why?)}$$
- $|S_4| = 4! = 24$: List all the possible *decomposition types* of elements.

Definition 7

The **decomposition type** of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.

Upshot: Possible decomposition types of permutations of S_4: (Check it!)

(i) a single cycle of length $1, 2, 3$ or 4

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then we have
$$A_3 = \{(1), (123), (132)\}. \text{ (Why?)}$$
- $|S_4| = 4! = 24$: List all the possible *decomposition types* of elements.

Definition 7

The **decomposition type** of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.

Upshot: Possible decomposition types of permutations of S_4: (Check it!)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

Question 2

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then we have
$$A_3 = \{(1), (123), (132)\}. \text{ (Why?)}$$
- $|S_4| = 4! = 24$: List all the possible *decomposition types* of elements.

Definition 7

The **decomposition type** of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.

Upshot: Possible decomposition types of permutations of S_4: (Check it!)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

Question 2

Which of these are even permutations?

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then we have
$$A_3 = \{(1), (123), (132)\}. \text{ (Why?)}$$
- $|S_4| = 4! = 24$: List all the possible *decomposition types* of elements.

Definition 7

The **decomposition type** of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.

Upshot: Possible decomposition types of permutations of S_4: (Check it!)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

Question 2

Which of these are even permutations?

(a) single cycles of length 1 and 3

Example: List all the elements of A_3 and A_4.

- Recall that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, then we have
$$A_3 = \{(1), (123), (132)\}. \text{ (Why?)}$$
- $|S_4| = 4! = 24$: List all the possible *decomposition types* of elements.

Definition 7

The **decomposition type** of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.

Upshot: Possible decomposition types of permutations of S_4: (Check it!)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

Question 2

Which of these are even permutations?

(a) single cycles of length 1 and 3

(b) two disjoint cycles of length 2

Example cont.: List all the elements of A_4, $|A_4| = 12$

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1:

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3:

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

$$\binom{4}{3} = \text{Four choices:}$$

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

$$\binom{4}{3} = \text{Four choices:} \qquad 123 \qquad 124 \qquad 134 \qquad 234$$

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

$$\binom{4}{3} = \text{Four choices:} \qquad 123 \qquad 124 \qquad 134 \qquad 234$$

For each choice, there are **two** ways to make a cycle. (Why?)

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $\binom{4}{3} =$ Four choices: 123 124 134 234

  For each choice, there are **two** ways to make a cycle. (Why?)

  The following is the list of all cycles of length 3 in S_4:

  $(123), (132), \quad (124), (142), \quad (134), (143), \quad (234), (243)$
- two disjoint cycles of length 2:

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $\binom{4}{3} =$ Four choices: 123 124 134 234

  For each choice, there are **two** ways to make a cycle. (Why?)

  The following is the list of all cycles of length 3 in S_4:

  $(123), (132)$, $(124), (142)$, $(134), (143)$, $(234), (243)$
- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $\binom{4}{3} =$ Four choices: 123 124 134 234

  For each choice, there are **two** ways to make a cycle. (Why?)

  The following is the list of all cycles of length 3 in S_4:

  $(123), (132),$ $(124), (142),$ $(134), (143),$ $(234), (243)$
- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $\binom{4}{2} =$ Six choices:

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $$\binom{4}{3} = \text{Four choices:} \qquad 123 \qquad 124 \qquad 134 \qquad 234$$

  For each choice, there are **two** ways to make a cycle. (Why?)
  The following is the list of all cycles of length 3 in S_4:

  $$(123), (132), \qquad (124), (142), \qquad (134), (143), \qquad (234), (243)$$

- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $$\binom{4}{2} = \text{Six choices:} \qquad 12 \qquad 13 \qquad 14 \qquad 23 \qquad 24 \qquad 34$$

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $\binom{4}{3} =$ Four choices: 123 124 134 234

  For each choice, there are **two** ways to make a cycle. (Why?)

  The following is the list of all cycles of length 3 in S_4:

  $(123), (132),$ $(124), (142),$ $(134), (143),$ $(234), (243)$
- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $\binom{4}{2} =$ Six choices: 12 13 14 23 24 34

  Each pair of two numbers listed above gives rise to a transposition.

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $$\binom{4}{3} = \text{Four choices:} \qquad 123 \qquad 124 \qquad 134 \qquad 234$$

  For each choice, there are **two** ways to make a cycle. (Why?)
  The following is the list of all cycles of length 3 in S_4:

  $$(123), (132), \qquad (124), (142), \qquad (134), (143), \qquad (234), (243)$$

- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $$\binom{4}{2} = \text{Six choices:} \qquad 12 \qquad 13 \qquad 14 \qquad 23 \qquad 24 \qquad 34$$

  Each pair of two numbers listed above gives rise to a transposition. The other two numbers form another transposition, which is disjoint from the first one.

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $\binom{4}{3}$ = Four choices: 123 124 134 234

  For each choice, there are **two** ways to make a cycle. (Why?)

  The following is the list of all cycles of length 3 in S_4:

  $(123), (132)$, $(124), (142)$, $(134), (143)$, $(234), (243)$
- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $\binom{4}{2}$ = Six choices: 12 13 14 23 24 34

  Each pair of two numbers listed above gives rise to a transposition. The other two numbers form another transposition, which is disjoint from the first one. The order doesn't matter.(Why?)

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $$\binom{4}{3} = \text{Four choices:} \qquad 123 \qquad 124 \qquad 134 \qquad 234$$

  For each choice, there are **two** ways to make a cycle. (Why?)
  The following is the list of all cycles of length 3 in S_4:

  $$(123), (132), \qquad (124), (142), \qquad (134), (143), \qquad (234), (243)$$

- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $$\binom{4}{2} = \text{Six choices:} \qquad 12 \qquad 13 \qquad 14 \qquad 23 \qquad 24 \qquad 34$$

  Each pair of two numbers listed above gives rise to a transposition. The other two numbers form another transposition, which is disjoint from the first one. The order doesn't matter.(Why?) *This implies that there are* **three** *different products of two disjoint transpositions*:

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $$\binom{4}{3} = \text{Four choices:} \qquad 123 \qquad 124 \qquad 134 \qquad 234$$

  For each choice, there are **two** ways to make a cycle. (Why?)
  The following is the list of all cycles of length 3 in S_4:

  $$(123), (132), \qquad (124), (142), \qquad (134), (143), \qquad (234), (243)$$

- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $$\binom{4}{2} = \text{Six choices:} \qquad 12 \qquad 13 \qquad 14 \qquad 23 \qquad 24 \qquad 34$$

  Each pair of two numbers listed above gives rise to a transposition. The other two numbers form another transposition, which is disjoint from the first one. The order doesn't matter.(Why?) *This implies that there are* **three** *different products of two disjoint transpositions*:
  Pick any pair of two numbers: 6 choices;

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $$\binom{4}{3} = \text{Four choices:} \quad 123 \quad 124 \quad 134 \quad 234$$

  For each choice, there are **two** ways to make a cycle. (Why?)
  The following is the list of all cycles of length 3 in S_4:

  $$(123), (132), \quad (124), (142), \quad (134), (143), \quad (234), (243)$$

- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $$\binom{4}{2} = \text{Six choices:} \quad 12 \quad 13 \quad 14 \quad 23 \quad 24 \quad 34$$

  Each pair of two numbers listed above gives rise to a transposition. The other two numbers form another transposition, which is disjoint from the first one. The order doesn't matter.(Why?) *This implies that there are* **three** *different products of two disjoint transpositions*: Pick any pair of two numbers: 6 choices; the other pair is determined. (Why?)

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $$\binom{4}{3} = \text{Four choices:} \quad 123 \quad 124 \quad 134 \quad 234$$

  For each choice, there are **two** ways to make a cycle. (Why?)
  The following is the list of all cycles of length 3 in S_4:

  $$(123), (132), \quad (124), (142), \quad (134), (143), \quad (234), (243)$$

- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $$\binom{4}{2} = \text{Six choices:} \quad 12 \quad 13 \quad 14 \quad 23 \quad 24 \quad 34$$

  Each pair of two numbers listed above gives rise to a transposition. The other two numbers form another transposition, which is disjoint from the first one. The order doesn't matter.(Why?) *This implies that there are* **three** *different products of two disjoint transpositions*: Pick any pair of two numbers: 6 choices; the other pair is determined. (Why?) The order doesn't matter $\Rightarrow$ 3 different products. (Why?)

Example cont.: List all the elements of A_4, $|A_4| = 12$

- single cycle of length 1: the identity permutation (1)
- single cycles of length 3: Choose any 3 of the numbers $1, 2, 3, 4$:

  $$\binom{4}{3} = \text{Four choices:} \qquad 123 \qquad 124 \qquad 134 \qquad 234$$

  For each choice, there are **two** ways to make a cycle. (Why?)
  The following is the list of all cycles of length 3 in S_4:

  $$(123), (132), \qquad (124), (142), \qquad (134), (143), \qquad (234), (243)$$

- two disjoint cycles of length 2: Choose any two of the #s 1, 2, 3, 4

  $$\binom{4}{2} = \text{Six choices:} \qquad 12 \qquad 13 \qquad 14 \qquad 23 \qquad 24 \qquad 34$$

  Each pair of two numbers listed above gives rise to a transposition. The other two numbers form another transposition, which is disjoint from the first one. The order doesn't matter.(Why?) *This implies that there are* **three** *different products of two disjoint transpositions*: Pick any pair of two numbers: 6 choices; the other pair is determined. (Why?) The order doesn't matter $\Rightarrow$ 3 different products. (Why?)

  $$(12)(34), \qquad (13)(24), \qquad (14)(23)$$

Example: The converse of Lagrange's theorem is false

Upshot:

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4,

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 *is a divisor of* $|A_4| = 12$*,* A_4 *has no subgroup of order* 6*.*

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), $(12)(34)$, $(13)(24)$, $(14)(23)$.

Proposition 6

Although 6 *is a divisor of* $|A_4| = 12$, A_4 *has no subgroup of order* 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction:

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

-

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 *is a divisor of* $|A_4| = 12$, A_4 *has no subgroup of order* 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
-

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 *is a divisor of* $|A_4| = 12$*,* A_4 *has no subgroup of order* 6*.*

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.

Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$.

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.

Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.

Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)

And then $xy = yx$. (Why?) [

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.

Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)

And then $xy = yx$. (Why?) [$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.]

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 *is a divisor of* $|A_4| = 12$, A_4 *has no subgroup of order* 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.

Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)

And then $xy = yx$. (Why?) [$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.]

Hence $\{e, x, y, xy\}$ is a subgroup of H of order 4, a contradiction. (Why?)

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 *is a divisor of* $|A_4| = 12$, A_4 *has no subgroup of order* 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.
Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)
And then $xy = yx$. (Why?) [$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.]
Hence $\{e, x, y, xy\}$ is a subgroup of H of order 4, a contradiction. (Why?)

This implies that H must contain an element of the form (abc) and an element of the form $(ab)(cd)$.

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 *is a divisor of* $|A_4| = 12$, A_4 *has no subgroup of order* 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.
Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)
And then $xy = yx$. (Why?) [$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.]
Hence $\{e, x, y, xy\}$ is a subgroup of H of order 4, a contradiction. (Why?)

This implies that H must contain an element of the form (abc) and an element of the form $(ab)(cd)$. Then H contains $(abc)(ab)(cd) = (acd)$ and

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.
Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)
And then $xy = yx$. (Why?) [$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.]
Hence $\{e, x, y, xy\}$ is a subgroup of H of order 4, a contradiction. (Why?)

This implies that H must contain an element of the form (abc) and an element of the form $(ab)(cd)$. Then H contains $(abc)(ab)(cd) = (acd)$ and $(ab)(cd)(abc) = (bdc)$. $\rightsquigarrow$

Example: The converse of Lagrange's theorem is false

Upshot: The following is the list of elements in A_4: (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).

Proposition 6

Although 6 is a divisor of $|A_4| = 12$, A_4 has no subgroup of order 6.

In A_4, all elements different from the identity have the form (abc) or $(ab)(cd)$ for distinct a, b, c, d.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

- It must contain an element of order 2. (Why?) [since $|H| = 6$ is even]
- It must contain an element of order 3. [Proof by contradiction:]

Assume every non-identity element of H has order 2.

Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$. (Why?)

And then $xy = yx$. (Why?) [$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.]

Hence $\{e, x, y, xy\}$ is a subgroup of H of order 4, a contradiction. (Why?)

This implies that H must contain an element of the form (abc) and an element of the form $(ab)(cd)$. Then H contains $(abc)(ab)(cd) = (acd)$ and $(ab)(cd)(abc) = (bdc)$. $\rightsquigarrow$ H has six elements of order 3. (Why?) □

Standard approach to the definition of even and odd permutations

Definition 8

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$.

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$. Because of such sign changes, we either have $\sigma(\Delta_n) = \Delta_n$ or $\sigma(\Delta_n) = -\Delta_n$.

Example 9 ($\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$)

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$. Because of such sign changes, we either have $\sigma(\Delta_n) = \Delta_n$ or $\sigma(\Delta_n) = -\Delta_n$.

Example 9 ($\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$)

Let $\sigma = (123)$ acts on Δ_3:

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$. Because of such sign changes, we either have $\sigma(\Delta_n) = \Delta_n$ or $\sigma(\Delta_n) = -\Delta_n$.

Example 9 ($\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$)

Let $\sigma = (123)$ acts on Δ_3: $\sigma(\Delta_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) =$

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$. Because of such sign changes, we either have $\sigma(\Delta_n) = \Delta_n$ or $\sigma(\Delta_n) = -\Delta_n$.

Example 9 ($\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$)

Let $\sigma = (123)$ acts on Δ_3: $\sigma(\Delta_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta_3$.

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$. Because of such sign changes, we either have $\sigma(\Delta_n) = \Delta_n$ or $\sigma(\Delta_n) = -\Delta_n$.

Example 9 ($\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$)

Let $\sigma = (123)$ acts on Δ_3: $\sigma(\Delta_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta_3$.
Let $\tau = (12)$ acts on Δ_3:

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$. Because of such sign changes, we either have $\sigma(\Delta_n) = \Delta_n$ or $\sigma(\Delta_n) = -\Delta_n$.

Example 9 ($\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$)

Let $\sigma = (123)$ acts on Δ_3: $\sigma(\Delta_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta_3$.
Let $\tau = (12)$ acts on Δ_3: $\tau(\Delta_3) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) =$

Standard approach to the definition of even and odd permutations

Definition 8

Let Δ_n be the polynomial in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Any permutation $\sigma \in S_n$ acts on Δ_n by permuting the subscripts, and we write

$$\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $i < j$ and $\sigma(i) < \sigma(j)$, then the factors $x_i - x_j$ and $x_{\sigma(i)} - x_{\sigma(j)}$ have the same sign, but if $\sigma(i) > \sigma(j)$ then $x_{\sigma(i)} - x_{\sigma(j)} = -(x_{\sigma(j)} - x_{\sigma(i)})$. Because of such sign changes, we either have $\sigma(\Delta_n) = \Delta_n$ or $\sigma(\Delta_n) = -\Delta_n$.

Example 9 ($\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$)

Let $\sigma = (123)$ acts on Δ_3: $\sigma(\Delta_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta_3$.
Let $\tau = (12)$ acts on Δ_3: $\tau(\Delta_3) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta_3$.

Theorem 10

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim:

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1\le i<j\le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1\le i<j\le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1\le i<j\le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \neq r, s$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1\le i<j\le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1\le i<j\le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1\le i<j\le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \neq r, s$.

(1) if $i > s : (x_{\rho(r)} - x_i)(x_{\rho(s)} - x_i) = (x_s - x_i)(x_r - x_i) = (x_r - x_i)(x_s - x_i)$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \ne r, s$.

(1) if $i > s : (x_{\rho(r)} - x_i)(x_{\rho(s)} - x_i) = (x_s - x_i)(x_r - x_i) = (x_r - x_i)(x_s - x_i)$.
(2) if $r < i < s : (x_{\rho(r)} - x_i)(x_i - x_{\rho(s)}) = (x_s - x_i)(x_i - x_r) = (x_r - x_i)(x_i - x_s)$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \neq r, s$.

(1) if $i > s : (x_{\rho(r)} - x_i)(x_{\rho(s)} - x_i) = (x_s - x_i)(x_r - x_i) = (x_r - x_i)(x_s - x_i)$.
(2) if $r < i < s : (x_{\rho(r)} - x_i)(x_i - x_{\rho(s)}) = (x_s - x_i)(x_i - x_r) = (x_r - x_i)(x_i - x_s)$.
(3) if $i < r : (x_i - x_{\rho(r)})(x_i - x_{\rho(s)}) = (x_i - x_s)(x_i - x_r) = (x_i - x_r)(x_i - x_s)$.

Thus

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \neq r, s$.

(1) if $i > s : (x_{\rho(r)} - x_i)(x_{\rho(s)} - x_i) = (x_s - x_i)(x_r - x_i) = (x_r - x_i)(x_s - x_i)$.
(2) if $r < i < s : (x_{\rho(r)} - x_i)(x_i - x_{\rho(s)}) = (x_s - x_i)(x_i - x_r) = (x_r - x_i)(x_i - x_s)$.
(3) if $i < r : (x_i - x_{\rho(r)})(x_i - x_{\rho(s)}) = (x_i - x_s)(x_i - x_r) = (x_i - x_r)(x_i - x_s)$.

Thus $\widehat{\rho}(\Delta_n) = -\Delta_n$.

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \neq r, s$.

(1) if $i > s : (x_{\rho(r)} - x_i)(x_{\rho(s)} - x_i) = (x_s - x_i)(x_r - x_i) = (x_r - x_i)(x_s - x_i)$.
(2) if $r < i < s : (x_{\rho(r)} - x_i)(x_i - x_{\rho(s)}) = (x_s - x_i)(x_i - x_r) = (x_r - x_i)(x_i - x_s)$.
(3) if $i < r : (x_i - x_{\rho(r)})(x_i - x_{\rho(s)}) = (x_i - x_s)(x_i - x_r) = (x_i - x_r)(x_i - x_s)$.

Thus $\widehat{\rho}(\Delta_n) = -\Delta_n$. Given any $\sigma \in S_n$, we can write $\sigma = \rho_1\rho_2\cdots\rho_k$.
Then

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \neq r, s$.

(1) if $i > s$: $(x_{\rho(r)} - x_i)(x_{\rho(s)} - x_i) = (x_s - x_i)(x_r - x_i) = (x_r - x_i)(x_s - x_i)$.
(2) if $r < i < s$: $(x_{\rho(r)} - x_i)(x_i - x_{\rho(s)}) = (x_s - x_i)(x_i - x_r) = (x_r - x_i)(x_i - x_s)$.
(3) if $i < r$: $(x_i - x_{\rho(r)})(x_i - x_{\rho(s)}) = (x_i - x_s)(x_i - x_r) = (x_i - x_r)(x_i - x_s)$.

Thus $\widehat{\rho}(\Delta_n) = -\Delta_n$. Given any $\sigma \in S_n$, we can write $\sigma = \rho_1\rho_2 \cdots \rho_k$.
Then $\widehat{\sigma}(\Delta_n) = (-1)^k \Delta_n$. (Why?)

Theorem 10

A permutation σ in S_n is even (i.e., $\sigma \in A_n$) if and only if $\sigma(\Delta_n) = \Delta_n$.

Set $X = \{\Delta_n, -\Delta_n\}$. For $\sigma \in S_n$, we define $\widehat{\sigma} : X \to X$ by

$$\widehat{\sigma}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \text{ and } \widehat{\sigma}(-\Delta_n) = -\prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

It is easy to check that $\widehat{\sigma\tau}(\Delta_n) = \widehat{\sigma}(\widehat{\tau}(\Delta_n))$ for any two $\sigma, \tau \in S_n$.
Let $\rho = (rs)$ be any transposition. Claim: $\widehat{\rho}(\Delta_n) = -\Delta_n$.
Assume that $r < s$. By definition, $\widehat{\rho}(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\rho(i)} - x_{\rho(j)})$. We have

$x_{\rho(r)} - x_{\rho(s)} = x_s - x_r = -(x_r - x_s)$ and $x_{\rho(i)} - x_{\rho(j)} = x_i - x_j$ for $i, j \neq r, s$.

(1) if $i > s : (x_{\rho(r)} - x_i)(x_{\rho(s)} - x_i) = (x_s - x_i)(x_r - x_i) = (x_r - x_i)(x_s - x_i)$.
(2) if $r < i < s : (x_{\rho(r)} - x_i)(x_i - x_{\rho(s)}) = (x_s - x_i)(x_i - x_r) = (x_r - x_i)(x_i - x_s)$.
(3) if $i < r : (x_i - x_{\rho(r)})(x_i - x_{\rho(s)}) = (x_i - x_s)(x_i - x_r) = (x_i - x_r)(x_i - x_s)$.

Thus $\widehat{\rho}(\Delta_n) = -\Delta_n$. Given any $\sigma \in S_n$, we can write $\sigma = \rho_1 \rho_2 \cdots \rho_k$.
Then $\widehat{\sigma}(\Delta_n) = (-1)^k \Delta_n$. (Why?) This completes the proof. (Why?) □