§2.3 Permutations

Shaoyun Yi

MATH 546/701I

University of South Carolina

May 12, 2020

Review

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b]$ $\dashrightarrow$ $\gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- gcd(a, b) **vs.** $\mathrm{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b)|(am + bn)$, linear combination of a and b

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b) | (am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\operatorname{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \operatorname{lcm}[a, b] = ab$
- $(a, b)|(am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n|(a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b)|(am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n|(a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^\times) \Rightarrow c \equiv d \pmod{n}$

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b) | (am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n | (a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^\times)$ $\Rightarrow c \equiv d \pmod{n}$
- Linear congruences $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n) | b$

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\operatorname{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \operatorname{lcm}[a, b] = ab$
- $(a, b) | (am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n | (a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^\times)$ $\Rightarrow c \equiv d \pmod{n}$
- Linear congruences $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n) | b$
- System of congruences: Chinese Remainder Theorem

Review

- Division Algorithm ⇢ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b]$ ⇢ $\gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b) | (am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n | (a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^\times)$ $\Rightarrow c \equiv d \pmod{n}$
- Linear congruences $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n) | b$
- System of congruences: Chinese Remainder Theorem
- $[a]_n = [b]_n \Leftrightarrow a \equiv b \pmod{n}$

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b) | (am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n | (a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^\times) \Rightarrow c \equiv d \pmod{n}$
- Linear congruences $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n) | b$
- System of congruences: Chinese Remainder Theorem
- $[a]_n = [b]_n \Leftrightarrow a \equiv b \pmod{n}$
- Divisor of zero **vs.** Unit in $\mathbf{Z}_n$ (Cancellation law ✓)

Review

- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b] \dashrightarrow \gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b) | (am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n | (a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^\times)$ $\Rightarrow c \equiv d \pmod{n}$
- Linear congruences $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n) | b$
- System of congruences: Chinese Remainder Theorem
- $[a]_n = [b]_n \Leftrightarrow a \equiv b \pmod{n}$
- Divisor of zero **vs.** Unit in $\mathbf{Z}_n$ (Cancellation law ✓)
- For $(a, n) = 1$, find $[a]_n^{-1}$:
  (i) the Euclidean algorithm; (ii) successive powers; (iii) trial and error

Review

- Division Algorithm⇢ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b]$⇢$\gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b)|(am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n|(a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^{\times})$ $\Rightarrow c \equiv d \pmod{n}$
- Linear congruences $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n)|b$
- System of congruences: Chinese Remainder Theorem
- $[a]_n = [b]_n \Leftrightarrow a \equiv b \pmod{n}$
- Divisor of zero **vs.** Unit in $\mathbf{Z}_n$ (Cancellation law ✓)
- For $(a, n) = 1$, find $[a]_n^{-1}$:
  (i) the Euclidean algorithm; (ii) successive powers; (iii) trial and error
- Euler's totient function $\varphi(n) = |\mathbf{Z}_n^{\times}|$

Review

- Division Algorithm ⇢ The Euclidean Algorithm (Matrix form)
- $\gcd(a, b)$ **vs.** $\mathrm{lcm}[a, b]$ ⇢ $\gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$
- $(a, b)|(am + bn)$, linear combination of a and b
- Relatively prime $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- $a \equiv b \pmod{n} \Leftrightarrow n|(a - b) \Leftrightarrow a = b + nq$ for some $q \in \mathbf{Z}$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ $(a \in \mathbf{Z}_n^\times)$ $\Rightarrow c \equiv d \pmod{n}$
- Linear congruences $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n)|b$
- System of congruences: Chinese Remainder Theorem
- $[a]_n = [b]_n \Leftrightarrow a \equiv b \pmod{n}$
- Divisor of zero **vs.** Unit in $\mathbf{Z}_n$ (Cancellation law ✓)
- For $(a, n) = 1$, find $[a]_n^{-1}$:
  (i) the Euclidean algorithm; (ii) successive powers; (iii) trial and error
- Euler's totient function $\varphi(n) = |\mathbf{Z}_n^\times|$
- Euler's theorem ⇢ Fermat's "little" theorem

Definitions and Notations

Definition 1

Let S be a set. A function $\sigma : S \to S$ is called a **permutation** of S if σ is one-to-one and onto.
The set of all permutations of S will be denoted by $\mathrm{Sym}(S)$.
The set of all permutations of the set $\{1, 2, \ldots, n\}$ will be denoted by S_n.

Definitions and Notations

Definition 1

Let S be a set. A function $\sigma : S \to S$ is called a **permutation** of S if σ is one-to-one and onto.

The set of all permutations of S will be denoted by $\mathrm{Sym}(S)$.

The set of all permutations of the set $\{1, 2, \ldots, n\}$ will be denoted by S_n.

Proposition. 1

(i) *if* $\sigma, \tau \in \mathrm{Sym}(S)$, *then* $\tau\sigma \in \mathrm{Sym}(S)$;

(ii) $1_S \in \mathrm{Sym}(S)$;

(iii) *if* $\sigma \in \mathrm{Sym}(S)$, *then* $\sigma^{-1} \in \mathrm{Sym}(S)$.

Definitions and Notations

Definition 1

Let S be a set. A function $\sigma : S \to S$ is called a **permutation** of S if σ is one-to-one and onto.
The set of all permutations of S will be denoted by $\mathrm{Sym}(S)$.
The set of all permutations of the set $\{1, 2, \ldots, n\}$ will be denoted by S_n.

Proposition. 1

(i) *if* $\sigma, \tau \in \mathrm{Sym}(S)$*, then* $\tau\sigma \in \mathrm{Sym}(S)$*;*

(ii) $1_S \in \mathrm{Sym}(S)$*;*

(iii) *if* $\sigma \in \mathrm{Sym}(S)$*, then* $\sigma^{-1} \in \mathrm{Sym}(S)$*.*

Notation: Given $\sigma \in S_n$,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

where under each integer i we write the image of i.

Example

Example. 1

If $S = \{1, 2, 3\}$ *and* $\sigma : S \to S$ *is given by* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Example

Example. 1

If $S = \{1, 2, 3\}$ *and* $\sigma : S \to S$ *is given by* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Proposition. 2

S_n *has* $n!$ *elements.*

Example

Example. 1

If $S = \{1, 2, 3\}$ *and* $\sigma : S \to S$ *is given by* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Proposition. 2

S_n *has* $n!$ *elements.*

Proof.

$$S_n = \left\{ \sigma \;\middle|\; \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. \right\}$$

Example

Example. 1

If $S = \{1, 2, 3\}$ *and* $\sigma : S \to S$ *is given by* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$ *:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Proposition. 2

S_n *has* $n!$ *elements.*

Proof.

$$S_n = \left\{ \sigma \;\middle|\; \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} . \right\}$$

For $\sigma(1)$, there are n choices.

Example

Example. 1

If $S = \{1, 2, 3\}$ *and* $\sigma : S \to S$ *is given by* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Proposition. 2

S_n *has* $n!$ *elements.*

Proof.

$$S_n = \left\{ \sigma \;\middle|\; \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. \right\}$$

For $\sigma(1)$, there are n choices.
For $\sigma(2)$, there are $n-1$ choices since the element that is assigned to $\sigma(1)$ cannot be used again.

Example

Example. 1

If $S = \{1, 2, 3\}$ *and* $\sigma : S \to S$ *is given by* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Proposition. 2

S_n *has* $n!$ *elements.*

Proof.

$$S_n = \left\{ \sigma \;\middle|\; \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. \right\}$$

For $\sigma(1)$, there are n choices.
For $\sigma(2)$, there are $n-1$ choices since the element that is assigned to $\sigma(1)$ cannot be used again.
For $\sigma(3)$, there are $n-2$ choices, etc. $|S_n| = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1 = n!$. □

Composition

Suppose that

$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$.

Then to compute the **composition**

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}.$$

Composition

Suppose that

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}.$$

Then to compute the **composition**

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}.$$

Example. 2

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ *and* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. *Compute* $\sigma\tau$ *and* $\tau\sigma$.

Composition

Suppose that

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}.$$

Then to compute the **composition**

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}.$$

Example. 2

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ *and* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. *Compute* $\sigma\tau$ *and* $\tau\sigma$.

$\sigma\tau(1) : 1 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3 \Rightarrow \sigma\tau(1) = 3$, *etc. We obtain* $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$.

Composition

Suppose that

$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$.

Then to compute the **composition**

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}.$$

Example. 2

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ *and* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. *Compute* $\sigma\tau$ *and* $\tau\sigma$.

$\sigma\tau(1) : 1 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3 \Rightarrow \sigma\tau(1) = 3$, *etc. We obtain* $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$.

$\tau\sigma(1) : 1 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 1 \Rightarrow \sigma\tau(1) = 1$, *etc. We obtain* $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

Inverse

Given $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ in S_n, it is easy to compute σ^{-1}.

Inverse

Given $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ in S_n, it is easy to compute σ^{-1}.

Key idea: If $\sigma(i) = j$, then $i = \sigma^{-1}(j)$. This can be accomplished easily by simply turning the two rows of σ upside down and then rearranging terms.

Inverse

Given $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ in S_n, it is easy to compute σ^{-1}.

Key idea: If $\sigma(i) = j$, then $i = \sigma^{-1}(j)$. This can be accomplished easily by simply turning the two rows of σ upside down and then rearranging terms.

Example. 3

If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, *then* $\sigma^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$.

Cycle

Another notation: For example, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$.

Now writing $\sigma = (1342)$ since $\sigma(1) = 3, \sigma(3) = 4, \sigma(4) = 2$, and $\sigma(2) = 1$. In the new notation we do not need to mention $\sigma(5)$ since $\sigma(5) = 5$.

Cycle

Another notation: For example, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$.

Now writing $\sigma = (1342)$ since $\sigma(1) = 3, \sigma(3) = 4, \sigma(4) = 2$, and $\sigma(2) = 1$. In the new notation we do not need to mention $\sigma(5)$ since $\sigma(5) = 5$.

Definition 2

Let S be a set, and let $\sigma \in \mathrm{Sym}(S)$. Then σ is called a **cycle of length** k if there exist elements $a_1, a_2, \ldots, a_k \in S$ such that
$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$, and
$\sigma(x) = x$ for all other elements $x \in S$ with $x \neq a_i$ for $i = 1, 2, \ldots, k$.
In this case we write $\sigma = (a_1 a_2 \cdots a_k)$.

Cycle

Another notation: For example, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$.

Now writing $\sigma = (1342)$ since $\sigma(1) = 3, \sigma(3) = 4, \sigma(4) = 2$, and $\sigma(2) = 1$.
In the new notation we do not need to mention $\sigma(5)$ since $\sigma(5) = 5$.

Definition 2

Let S be a set, and let $\sigma \in \mathrm{Sym}(S)$. Then σ is called a **cycle of length** k if there exist elements $a_1, a_2, \ldots, a_k \in S$ such that
$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$, and
$\sigma(x) = x$ for all other elements $x \in S$ with $x \neq a_i$ for $i = 1, 2, \ldots, k$.
In this case we write $\sigma = (a_1 a_2 \cdots a_k)$.

We can also write $\sigma = (a_2 a_3 \cdots a_k a_1)$ or $\sigma = (a_3 \cdots a_k a_1 a_2)$, etc.

Cycle

Another notation: For example, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$.

Now writing $\sigma = (1342)$ since $\sigma(1) = 3, \sigma(3) = 4, \sigma(4) = 2$, and $\sigma(2) = 1$.
In the new notation we do not need to mention $\sigma(5)$ since $\sigma(5) = 5$.

Definition 2

Let S be a set, and let $\sigma \in \mathrm{Sym}(S)$. Then σ is called a **cycle of length** k if there exist elements $a_1, a_2, \ldots, a_k \in S$ such that
$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$, and
$\sigma(x) = x$ for all other elements $x \in S$ with $x \neq a_i$ for $i = 1, 2, \ldots, k$.
In this case we write $\sigma = (a_1 a_2 \cdots a_k)$.

We can also write $\sigma = (a_2 a_3 \cdots a_k a_1)$ or $\sigma = (a_3 \cdots a_k a_1 a_2)$, etc.
The notation for a cycle of length $k \geq 2$ can thus be written in k different ways, depending on the starting point.

Cycle

Another notation: For example, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$.

Now writing $\sigma = (1342)$ since $\sigma(1) = 3, \sigma(3) = 4, \sigma(4) = 2$, and $\sigma(2) = 1$. In the new notation we do not need to mention $\sigma(5)$ since $\sigma(5) = 5$.

Definition 2

Let S be a set, and let $\sigma \in \mathrm{Sym}(S)$. Then σ is called a **cycle of length** k if there exist elements $a_1, a_2, \ldots, a_k \in S$ such that
$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$, and
$\sigma(x) = x$ for all other elements $x \in S$ with $x \neq a_i$ for $i = 1, 2, \ldots, k$.
In this case we write $\sigma = (a_1 a_2 \cdots a_k)$.

We can also write $\sigma = (a_2 a_3 \cdots a_k a_1)$ or $\sigma = (a_3 \cdots a_k a_1 a_2)$, etc.
The notation for a cycle of length $k \geq 2$ can thus be written in k different ways, depending on the starting point.

We will use (1) to denote the identity permutation (or just use 1_S).

Examples

Example. 4

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$ *is a cycle of length* 3, *written* (134).

Examples

Example. 4

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$ *is a cycle of length* 3, *written* (134).

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5$ *is not a cycle, written* (134)(25).

Example. 5

Let $\sigma = (1425)$ *and* $\tau = (263)$ *be cycles in* S_6. *Compute the product* $\sigma\tau$.

Examples

Example. 4

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$ *is a cycle of length* 3, *written* (134).

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5$ *is not a cycle, written* $(134)(25)$.

Example. 5

Let $\sigma = (1425)$ *and* $\tau = (263)$ *be cycles in* S_6. *Compute the product* $\sigma\tau$.

$1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 4 \Rightarrow \sigma\tau(1) = 4$, *etc.* $\Longrightarrow \sigma\tau = (1425)(263) = (142635)$.

Example. 4

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$ *is a cycle of length* 3, *written* (134).

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5$ *is not a cycle, written* (134)(25).

Example. 5

Let $\sigma = (1425)$ *and* $\tau = (263)$ *be cycles in* S_6. *Compute the product* $\sigma\tau$.
$1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 4 \Rightarrow \sigma\tau(1) = 4$, *etc.* $\implies \sigma\tau = (1425)(263) = (142635)$.

It is NOT true in general that the product of two cycles is again a cycle.

Examples

Example. 4

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5 \text{ is a cycle of length 3, written } (134).$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5 \text{ is not a cycle, written } (134)(25).$$

Example. 5

Let $\sigma = (1425)$ *and* $\tau = (263)$ *be cycles in* S_6*. Compute the product* $\sigma\tau$*.*
$1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 4 \Rightarrow \sigma\tau(1) = 4$, *etc.* $\Longrightarrow \sigma\tau = (1425)(263) = (142635)$.

It is NOT true in general that the product of two cycles is again a cycle.

Example. 6

Consider $(1425) \in S_6$, *we have* $(1425)(1425) = (12)(3)(45)(6) = (12)(45)$.

Disjoint cycles

Definition 3

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$, for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Disjoint cycles

Definition 3

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$, for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Remark. 1

It often happens that $\sigma\tau \neq \tau\sigma$ for two permutations σ, τ.
For example, in S_3 we have $(12)(13) = (132) \neq (123) = (13)(12)$.
If $\sigma\tau = \tau\sigma$, then we say that σ and τ **commute**.

Disjoint cycles

Definition 3

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$, for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Remark. 1

It often happens that $\sigma\tau \neq \tau\sigma$ *for two permutations* σ, τ.
For example, in S_3 *we have* $(12)(13) = (132) \neq (123) = (13)(12)$.
If $\sigma\tau = \tau\sigma$, *then we say that* σ *and* τ ***commute***.

Proposition. 3

Let S *be any set. If* σ *and* τ *are disjoint cycles in* $\mathrm{Sym}(S)$, *then* $\sigma\tau = \tau\sigma$.

Disjoint cycles

Definition 3

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$, for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Remark. 1

It often happens that $\sigma\tau \neq \tau\sigma$ for two permutations σ, τ.
For example, in S_3 we have $(12)(13) = (132) \neq (123) = (13)(12)$.
If $\sigma\tau = \tau\sigma$, then we say that σ and τ ***commute****.*

Proposition. 3

Let S be any set. If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Proof. Let $\sigma = (a_1 \cdots a_k)$ and $\tau = (b_1 \cdots b_m)$ be disjoint.

Disjoint cycles

Definition 3

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$, for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Remark. 1

It often happens that $\sigma\tau \neq \tau\sigma$ for two permutations σ, τ.
For example, in S_3 we have $(12)(13) = (132) \neq (123) = (13)(12)$.
If $\sigma\tau = \tau\sigma$, then we say that σ and τ **commute**.

Proposition. 3

Let S be any set. If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Proof. Let $\sigma = (a_1 \cdots a_k)$ and $\tau = (b_1 \cdots b_m)$ be disjoint. For $j < k$, then

$\sigma\tau(a_j) = \sigma(a_j) = a_{j+1} = \tau(a_{j+1}) = \tau(\sigma(a_j))$ because τ leaves $a_1, \ldots, a_k$ fixed.

In case $j = k$, we use $\sigma(a_j) = a_1 = \tau(a_1)$.

Disjoint cycles

Definition 3

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$, for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Remark. 1

It often happens that $\sigma\tau \neq \tau\sigma$ for two permutations σ, τ.
For example, in S_3 we have $(12)(13) = (132) \neq (123) = (13)(12)$.
If $\sigma\tau = \tau\sigma$, then we say that σ and τ ***commute****.*

Proposition. 3

Let S be any set. If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Proof. Let $\sigma = (a_1 \cdots a_k)$ and $\tau = (b_1 \cdots b_m)$ be disjoint. For $j < k$, then

$\sigma\tau(a_j) = \sigma(a_j) = a_{j+1} = \tau(a_{j+1}) = \tau(\sigma(a_j))$ because τ leaves $a_1, \ldots, a_k$ fixed.

In case $j = k$, we use $\sigma(a_j) = a_1 = \tau(a_1)$. A similar computation can be given for b_j.

Disjoint cycles

Definition 3

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$, for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Remark. 1

It often happens that $\sigma\tau \neq \tau\sigma$ for two permutations σ, τ.
For example, in S_3 we have $(12)(13) = (132) \neq (123) = (13)(12)$.
If $\sigma\tau = \tau\sigma$, then we say that σ and τ ***commute****.*

Proposition. 3

Let S be any set. If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Proof. Let $\sigma = (a_1 \cdots a_k)$ and $\tau = (b_1 \cdots b_m)$ be disjoint. For $j < k$, then

$\sigma\tau(a_j) = \sigma(a_j) = a_{j+1} = \tau(a_{j+1}) = \tau(\sigma(a_j))$ because τ leaves $a_1, \ldots, a_k$ fixed.

In case $j = k$, we use $\sigma(a_j) = a_1 = \tau(a_1)$. A similar computation can be given for b_j. If i appears in neither cycle, then both σ and τ leave it fixed. □

Permutation in S_n

For any set S, let $\sigma \in \mathrm{Sym}(S)$. Taking the composition of σ with itself any number of times still gives us a permutation; i.e., $\sigma^i = \sigma\sigma \cdots \sigma$.

Permutation in S_n

For any set S, let $\sigma \in \mathrm{Sym}(S)$. Taking the composition of σ with itself any number of times still gives us a permutation; i.e., $\sigma^i = \sigma\sigma\cdots\sigma$. Define $\sigma^0 = (1) = 1_S$ and $\sigma^{-n} = (\sigma^n)^{-1}$. For all integers m, n, we have

$$\sigma^m\sigma^n = \sigma^{m+n} \qquad \text{and} \qquad (\sigma^m)^n = \sigma^{mn}.$$

Theorem 4

Permutation in S_n

For any set S, let $\sigma \in \mathrm{Sym}(S)$. Taking the composition of σ with itself any number of times still gives us a permutation; i.e., $\sigma^i = \sigma\sigma \cdots \sigma$. Define $\sigma^0 = (1) = 1_S$ and $\sigma^{-n} = (\sigma^n)^{-1}$. For all integers m, n, we have

$$\sigma^m \sigma^n = \sigma^{m+n} \qquad \text{and} \qquad (\sigma^m)^n = \sigma^{mn}.$$

Theorem 4

Every permutation in S_n can be written as a product of disjoint cycles. The cycles of length ≥ 2 that appear in the product are unique.

Permutation in S_n

For any set S, let $\sigma \in \mathrm{Sym}(S)$. Taking the composition of σ with itself any number of times still gives us a permutation; i.e., $\sigma^i = \sigma\sigma \cdots \sigma$. Define $\sigma^0 = (1) = 1_S$ and $\sigma^{-n} = (\sigma^n)^{-1}$. For all integers m, n, we have

$$\sigma^m \sigma^n = \sigma^{m+n} \qquad \text{and} \qquad (\sigma^m)^n = \sigma^{mn}.$$

Theorem 4

Every permutation in S_n can be written as a product of disjoint cycles. The cycles of length ≥ 2 that appear in the product are unique.

Sketch of proof: Let $S = \{1, 2, \ldots, n\}$ and let $\sigma \in S_n = \mathrm{Sym}(S)$.

Permutation in S_n

For any set S, let $\sigma \in \mathrm{Sym}(S)$. Taking the composition of σ with itself any number of times still gives us a permutation; i.e., $\sigma^i = \sigma\sigma\cdots\sigma$. Define $\sigma^0 = (1) = 1_S$ and $\sigma^{-n} = (\sigma^n)^{-1}$. For all integers m, n, we have

$$\sigma^m\sigma^n = \sigma^{m+n} \qquad \text{and} \qquad (\sigma^m)^n = \sigma^{mn}.$$

Theorem 4

Every permutation in S_n can be written as a product of disjoint cycles. The cycles of length ≥ 2 that appear in the product are unique.

Sketch of proof: Let $S = \{1, 2, \ldots, n\}$ and let $\sigma \in S_n = \mathrm{Sym}(S)$. Consider $1, \sigma(1), \sigma^2(1), \ldots$: Since S has only n elements, we can find the least positive exponent r such that $\sigma^r(1) = 1$. Then $1, \sigma(1), \ldots, \sigma^{r-1}(1)$ are all distinct, giving us a cycle of length r: $(1\,\sigma(1)\,\sigma^2(1)\cdots\sigma^{r-1}(1))$.

Permutation in S_n

For any set S, let $\sigma \in \mathrm{Sym}(S)$. Taking the composition of σ with itself any number of times still gives us a permutation; i.e., $\sigma^i = \sigma\sigma\cdots\sigma$. Define $\sigma^0 = (1) = 1_S$ and $\sigma^{-n} = (\sigma^n)^{-1}$. For all integers m, n, we have

$$\sigma^m\sigma^n = \sigma^{m+n} \qquad \text{and} \qquad (\sigma^m)^n = \sigma^{mn}.$$

Theorem 4

Every permutation in S_n can be written as a product of disjoint cycles. The cycles of length ≥ 2 that appear in the product are unique.

Sketch of proof: Let $S = \{1, 2, \ldots, n\}$ and let $\sigma \in S_n = \mathrm{Sym}(S)$. Consider $1, \sigma(1), \sigma^2(1), \ldots$: Since S has only n elements, we can find the least positive exponent r such that $\sigma^r(1) = 1$. Then $1, \sigma(1), \ldots, \sigma^{r-1}(1)$ are all distinct, giving us a cycle of length r: $(1\,\sigma(1)\,\sigma^2(1)\cdots\sigma^{r-1}(1))$.

- If $r < n$, let a be the least integer not in $(1\,\sigma(1)\,\sigma^2(1)\cdots\sigma^{r-1}(1))$ and form the cycle $(a\,\sigma(a)\,\sigma^2(a)\cdots\sigma^{s-1}(a))$ in which s is the least positive integer such that $\sigma^s(a) = a$.

Permutation in S_n

For any set S, let $\sigma \in \mathrm{Sym}(S)$. Taking the composition of σ with itself any number of times still gives us a permutation; i.e., $\sigma^i = \sigma\sigma\cdots\sigma$. Define $\sigma^0 = (1) = 1_S$ and $\sigma^{-n} = (\sigma^n)^{-1}$. For all integers m, n, we have

$$\sigma^m\sigma^n = \sigma^{m+n} \qquad \text{and} \qquad (\sigma^m)^n = \sigma^{mn}.$$

Theorem 4

Every permutation in S_n can be written as a product of disjoint cycles. The cycles of length ≥ 2 that appear in the product are unique.

Sketch of proof: Let $S = \{1, 2, \ldots, n\}$ and let $\sigma \in S_n = \mathrm{Sym}(S)$. Consider $1, \sigma(1), \sigma^2(1), \ldots$: Since S has only n elements, we can find the least positive exponent r such that $\sigma^r(1) = 1$. Then $1, \sigma(1), \ldots, \sigma^{r-1}(1)$ are all distinct, giving us a cycle of length r: $(1\,\sigma(1)\,\sigma^2(1)\cdots\sigma^{r-1}(1))$.

- If $r < n$, let a be the least integer not in $(1\,\sigma(1)\,\sigma^2(1)\cdots\sigma^{r-1}(1))$ and form the cycle $(a\,\sigma(a)\,\sigma^2(a)\cdots\sigma^{s-1}(a))$ in which s is the least positive integer such that $\sigma^s(a) = a$.
- If $r + s < n$, etc. We continue in this way until we have exhausted S. □

Examples

We have given an algorithm in the proof for finding the necessary cycles.

Example. 7

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 7 & 6 & 3 & 8 & 1 & 4 \end{pmatrix} \overset{\textit{Applying the algorithm}}{\longrightarrow} \sigma = (1537)(468).$

Examples

We have given an algorithm in the proof for finding the necessary cycles.

Example. 7

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 7 & 6 & 3 & 8 & 1 & 4 \end{pmatrix} \overset{\textit{Applying the algorithm}}{\longrightarrow} \sigma = (1537)(468).$

Example. 8

Consider the cycles (25143) *and* (462) *in* S_6*:*

Examples

We have given an algorithm in the proof for finding the necessary cycles.

Example. 7

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 7 & 6 & 3 & 8 & 1 & 4 \end{pmatrix} \xrightarrow{\text{Applying the algorithm}} \sigma = (1537)(468).$

Example. 8

Consider the cycles (25143) *and* (462) *in* S_6*:* $(25143)(462) = (1465)(23).$

Order of a permutation, I

If $\sigma = (a_1 a_2 \cdots a_m)$ is a cycle of length m, then applying σ m times to any $a_i, i = 1, 2, \ldots, m$ gives a_i. Thus $\sigma^m = (1)$.

Order of a permutation, I

If $\sigma = (a_1 a_2 \cdots a_m)$ is a cycle of length m, then applying σ m times to any $a_i, i = 1, 2, \ldots, m$ gives a_i. Thus $\sigma^m = (1)$.
Furthermore, m is the smallest positive power of σ that equals the identity, since $\sigma^k(a_1) = a_{k+1}$ for $1 \leq k < m$.

Definition 5

Order of a permutation, I

If $\sigma = (a_1 a_2 \cdots a_m)$ is a cycle of length m, then applying σ m times to any $a_i, i = 1, 2, \ldots, m$ gives a_i. Thus $\sigma^m = (1)$.
Furthermore, m is the smallest positive power of σ that equals the identity, since $\sigma^k(a_1) = a_{k+1}$ for $1 \leq k < m$.

Definition 5

Let $\sigma \in S_n$. The least positive integer m such that $\sigma^m = (1)$ is called the **order** of σ.

Order of a permutation, I

If $\sigma = (a_1 a_2 \cdots a_m)$ is a cycle of length m, then applying σ m times to any $a_i, i = 1, 2, \ldots, m$ gives a_i. Thus $\sigma^m = (1)$.
Furthermore, m is the smallest positive power of σ that equals the identity, since $\sigma^k(a_1) = a_{k+1}$ for $1 \leq k < m$.

Definition 5

Let $\sigma \in S_n$. The least positive integer m such that $\sigma^m = (1)$ is called the **order** of σ.

It follows from the above definition that a cycle of length m has order m.

Proposition. 4

Order of a permutation, I

If $\sigma = (a_1 a_2 \cdots a_m)$ is a cycle of length m, then applying σ m times to any $a_i, i = 1, 2, \ldots, m$ gives a_i. Thus $\sigma^m = (1)$.
Furthermore, m is the smallest positive power of σ that equals the identity, since $\sigma^k(a_1) = a_{k+1}$ for $1 \leq k < m$.

Definition 5

Let $\sigma \in S_n$. The least positive integer m such that $\sigma^m = (1)$ is called the **order** of σ.

It follows from the above definition that a cycle of length m has order m.

Proposition. 4

Let $\sigma \in S_n$ have order m. Then for all integers i, j we have $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{m}$.

Order of a permutation, I

If $\sigma = (a_1 a_2 \cdots a_m)$ is a cycle of length m, then applying σ m times to any $a_i, i = 1, 2, \ldots, m$ gives a_i. Thus $\sigma^m = (1)$.
Furthermore, m is the smallest positive power of σ that equals the identity, since $\sigma^k(a_1) = a_{k+1}$ for $1 \leq k < m$.

Definition 5

Let $\sigma \in S_n$. The least positive integer m such that $\sigma^m = (1)$ is called the **order** of σ.

It follows from the above definition that a cycle of length m has order m.

Proposition. 4

Let $\sigma \in S_n$ have order m. Then for all integers i, j we have $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{m}$.

Proof:($\Leftarrow$) $i = j + mt$ for some $t \in \mathbf{Z}$. Hence $\sigma^i = \sigma^{j+mt} = \sigma^j(\sigma^m)^t = \sigma^j$.

Order of a permutation, I

If $\sigma = (a_1 a_2 \cdots a_m)$ is a cycle of length m, then applying σ m times to any $a_i, i = 1, 2, \ldots, m$ gives a_i. Thus $\sigma^m = (1)$.
Furthermore, m is the smallest positive power of σ that equals the identity, since $\sigma^k(a_1) = a_{k+1}$ for $1 \leq k < m$.

Definition 5

Let $\sigma \in S_n$. The least positive integer m such that $\sigma^m = (1)$ is called the **order** of σ.

It follows from the above definition that a cycle of length m has order m.

Proposition. 4

Let $\sigma \in S_n$ have order m. Then for all integers i, j we have $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{m}$.

Proof:($\Leftarrow$) $i = j + mt$ for some $t \in \mathbf{Z}$. Hence $\sigma^i = \sigma^{j+mt} = \sigma^j(\sigma^m)^t = \sigma^j$.
($\Rightarrow$) $\sigma^{i-j} = (1)$, write $i - j = mq + r$. So $(1) = \sigma^{mq+r} = \sigma^r \Rightarrow r = 0$. □

Order of a permutation, II

Proposition. 5

Order of a permutation, II

Proposition. 5

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its disjoint cycles.

Order of a permutation, II

Proposition. 5

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its disjoint cycles.

Proof: Let $\sigma = (a_1 \cdots a_m)$ with order m. And $\sigma^k = (1)$ if and only if $m|k$.

Order of a permutation, II

Proposition. 5

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its disjoint cycles.

Proof: Let $\sigma = (a_1 \cdots a_m)$ with order m. And $\sigma^k = (1)$ if and only if $m|k$.

If $\sigma = (a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_r)$ is a product of two disjoint cycles, then $\sigma^j = (a_1 \cdots a_m)^j (b_1 \cdots b_r)^j$ since $(a_1 \cdots a_m)$ commutes with $(b_1 \cdots b_r)$.

Order of a permutation, II

Proposition. 5

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its disjoint cycles.

Proof: Let $\sigma = (a_1 \cdots a_m)$ with order m. And $\sigma^k = (1)$ if and only if $m|k$.

If $\sigma = (a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_r)$ is a product of two disjoint cycles, then $\sigma^j = (a_1 \cdots a_m)^j (b_1 \cdots b_r)^j$ since $(a_1 \cdots a_m)$ commutes with $(b_1 \cdots b_r)$.

If $\sigma^j = (1)$, then $(a_1 \cdots a_m)^j = (b_1 \cdots b_r)^j = (1)$ since $(a_1 \cdots a_m)^j$ fixes each b_i and $(b_1 \cdots b_r)^j$ fixes each a_i.

Order of a permutation, II

Proposition. 5

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its disjoint cycles.

Proof: Let $\sigma = (a_1 \cdots a_m)$ with order m. And $\sigma^k = (1)$ if and only if $m|k$.

If $\sigma = (a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_r)$ is a product of two disjoint cycles, then $\sigma^j = (a_1 \cdots a_m)^j (b_1 \cdots b_r)^j$ since $(a_1 \cdots a_m)$ commutes with $(b_1 \cdots b_r)$.

If $\sigma^j = (1)$, then $(a_1 \cdots a_m)^j = (b_1 \cdots b_r)^j = (1)$ since $(a_1 \cdots a_m)^j$ fixes each b_i and $(b_1 \cdots b_r)^j$ fixes each a_i. This holds if and only if $m|j$ and $r|j$, and then $[m, r]|j$.

Order of a permutation, II

Proposition. 5

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its disjoint cycles.

Proof: Let $\sigma = (a_1 \cdots a_m)$ with order m. And $\sigma^k = (1)$ if and only if $m|k$.

If $\sigma = (a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_r)$ is a product of two disjoint cycles, then $\sigma^j = (a_1 \cdots a_m)^j (b_1 \cdots b_r)^j$ since $(a_1 \cdots a_m)$ commutes with $(b_1 \cdots b_r)$.

If $\sigma^j = (1)$, then $(a_1 \cdots a_m)^j = (b_1 \cdots b_r)^j = (1)$ since $(a_1 \cdots a_m)^j$ fixes each b_i and $(b_1 \cdots b_r)^j$ fixes each a_i. This holds if and only if $m|j$ and $r|j$, and then $[m, r]|j$. The smallest such j is thus $[m, r]$. $\dashrightarrow$ the general case.

Order of a permutation, II

Proposition. 5

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its disjoint cycles.

Proof: Let $\sigma = (a_1 \cdots a_m)$ with order m. And $\sigma^k = (1)$ if and only if $m|k$.

If $\sigma = (a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_r)$ is a product of two disjoint cycles, then $\sigma^j = (a_1 \cdots a_m)^j (b_1 \cdots b_r)^j$ since $(a_1 \cdots a_m)$ commutes with $(b_1 \cdots b_r)$.

If $\sigma^j = (1)$, then $(a_1 \cdots a_m)^j = (b_1 \cdots b_r)^j = (1)$ since $(a_1 \cdots a_m)^j$ fixes each b_i and $(b_1 \cdots b_r)^j$ fixes each a_i. This holds if and only if $m|j$ and $r|j$, and then $[m, r]|j$. The smallest such j is thus $[m, r]$. $\dashrightarrow$ the general case.

Example. 9

$(1537)(284)$ *has order* 12 *in* S_8. $(153)(284697)$ *has order* 6 *in* S_9.

Inverse revisited

We merely reverse the order of the cycle to compute the inverse of a cycle:

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

Inverse revisited

We merely reverse the order of the cycle to compute the inverse of a cycle:

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

The inverse of the product $\sigma\tau$ of two permutations is $\tau^{-1}\sigma^{-1}$ since

$$(\sigma\tau)(\tau^{-1}\sigma^{-1}) = \sigma(\tau\tau^{-1})\sigma^{-1} = \sigma(1)\sigma^{-1} = \sigma\sigma^{-1} = (1)$$

and similarly

$$(\tau^{-1}\sigma^{-1})(\sigma\tau) = (1).$$

Inverse revisited

We merely reverse the order of the cycle to compute the inverse of a cycle:

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

The inverse of the product $\sigma\tau$ of two permutations is $\tau^{-1}\sigma^{-1}$ since

$$(\sigma\tau)(\tau^{-1}\sigma^{-1}) = \sigma(\tau\tau^{-1})\sigma^{-1} = \sigma(1)\sigma^{-1} = \sigma\sigma^{-1} = (1)$$

and similarly

$$(\tau^{-1}\sigma^{-1})(\sigma\tau) = (1).$$

Thus we have

$$[(a_1 \cdots a_r)(b_1 \cdots b_m)]^{-1} = (b_m \cdots b_1)(a_r \cdots a_1).$$

Inverse revisited

We merely reverse the order of the cycle to compute the inverse of a cycle:

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

The inverse of the product $\sigma\tau$ of two permutations is $\tau^{-1}\sigma^{-1}$ since

$$(\sigma\tau)(\tau^{-1}\sigma^{-1}) = \sigma(\tau\tau^{-1})\sigma^{-1} = \sigma(1)\sigma^{-1} = \sigma\sigma^{-1} = (1)$$

and similarly

$$(\tau^{-1}\sigma^{-1})(\sigma\tau) = (1).$$

Thus we have

$$[(a_1 \cdots a_r)(b_1 \cdots b_m)]^{-1} = (b_m \cdots b_1)(a_r \cdots a_1).$$

Note that if the cycles are disjoint, then they commute, and so the inverses do not need to be written in reverse order.

Transposition

Definition 6

Transposition

Definition 6

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Proposition. 6

Transposition

Definition 6

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Proposition. 6

Any permutation in S_n, where $n \geq 2$, can be written as a product of transpositions.

Transposition

Definition 6

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Proposition. 6

Any permutation in S_n, where $n \geq 2$, can be written as a product of transpositions.

Proof: Any σ can be expressed as a product of disjoint cycles $\Rightarrow$ only need to show that any cycle can be expressed as a product of transpositions.

Transposition

Definition 6

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Proposition. 6

Any permutation in S_n, where $n \geq 2$, can be written as a product of transpositions.

Proof: Any σ can be expressed as a product of disjoint cycles $\Rightarrow$ only need to show that any cycle can be expressed as a product of transpositions.
The identity $(1) = (12)(21)$.

Transposition

Definition 6

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Proposition. 6

Any permutation in S_n, where $n \geq 2$, can be written as a product of transpositions.

Proof: Any σ can be expressed as a product of disjoint cycles $\Rightarrow$ only need to show that any cycle can be expressed as a product of transpositions.
The identity $(1) = (12)(21)$.
For any other permutation, we can give an explicit computation:

$$\begin{aligned}(a_1 a_2 \cdots a_{r-1} a_r) =&(a_{r-1} a_r)(a_{r-2} a_r) \cdots (a_3 a_r)(a_2 a_r)(a_1 a_r)\\ =&(a_1 a_2)(a_2 a_3) \cdots (a_{r-2} a_{r-1})(a_{r-1} a_r).\end{aligned}$$

Example. 10

Transposition

Definition 6

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Proposition. 6

Any permutation in S_n, where $n \geq 2$, can be written as a product of transpositions.

Proof: Any σ can be expressed as a product of disjoint cycles $\Rightarrow$ only need to show that any cycle can be expressed as a product of transpositions.
The identity $(1) = (12)(21)$.
For any other permutation, we can give an explicit computation:

$$\begin{aligned}(a_1 a_2 \cdots a_{r-1} a_r) =& (a_{r-1} a_r)(a_{r-2} a_r) \cdots (a_3 a_r)(a_2 a_r)(a_1 a_r) \\ =& (a_1 a_2)(a_2 a_3) \cdots (a_{r-2} a_{r-1})(a_{r-1} a_r).\end{aligned}$$

Example. 10

$(25378) = (78)(38)(58)(28) = (25)(53)(37)(78)$.

Transposition

Definition 6

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Proposition. 6

Any permutation in S_n, where $n \geq 2$, can be written as a product of transpositions.

Proof: Any σ can be expressed as a product of disjoint cycles $\Rightarrow$ only need to show that any cycle can be expressed as a product of transpositions.
The identity $(1) = (12)(21)$.
For any other permutation, we can give an explicit computation:

$$\begin{aligned}(a_1 a_2 \cdots a_{r-1} a_r) =& (a_{r-1} a_r)(a_{r-2} a_r) \cdots (a_3 a_r)(a_2 a_r)(a_1 a_r) \\ =& (a_1 a_2)(a_2 a_3) \cdots (a_{r-2} a_{r-1})(a_{r-1} a_r).\end{aligned}$$

Example. 10

$(25378) = (78)(38)(58)(28) = (25)(53)(37)(78)$.
$(1) = (123)(132) = (12)(23)(13)(32) = (23)(13)(32)(12)$.

Even permutation vs. Odd permutation

Example. 11

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

A permutation σ is called
even if it can be written as a product of an even number of transpositions.
odd if it can be written as a product of an odd number of transpositions.

Example. 12

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

A permutation σ is called
even if it can be written as a product of an even number of transpositions.
odd if it can be written as a product of an odd number of transpositions.

Example. 12

$(12), (4321)$ *are odd, and* $(123), (25378)$ *are even.*

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

A permutation σ is called
even if it can be written as a product of an even number of transpositions.
odd if it can be written as a product of an odd number of transpositions.

Example. 12

$(12), (4321)$ *are odd, and* $(123), (25378)$ *are even. The identity* (1) *is even.*

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

A permutation σ is called
even if it can be written as a product of an even number of transpositions.
odd if it can be written as a product of an odd number of transpositions.

Example. 12

$(12), (4321)$ *are odd, and* $(123), (25378)$ *are even. The identity* (1) *is even.*

Note that a cycle of odd length is even and a cycle of even length is odd.

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

A permutation σ is called
even if it can be written as a product of an even number of transpositions.
odd if it can be written as a product of an odd number of transpositions.

Example. 12

$(12), (4321)$ *are odd, and* $(123), (25378)$ *are even. The identity* (1) *is even.*

Note that a cycle of odd length is even and a cycle of even length is odd.
If σ is an even (resp. odd) permutation, then σ^{-1} is also even (resp. odd).

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

A permutation σ is called

even if it can be written as a product of an even number of transpositions.

odd if it can be written as a product of an odd number of transpositions.

Example. 12

$(12), (4321)$ *are odd, and* $(123), (25378)$ *are even. The identity* (1) *is even.*

Note that a cycle of odd length is even and a cycle of even length is odd.

If σ is an even (resp. odd) permutation, then σ^{-1} is also even (resp. odd).

The product of *two* even (or odd) permutations is again even;

Even permutation vs. Odd permutation

Example. 11

$(123) = (23)(13)$ *or* $(123) = (12)(23)$; *also* $(123) = (12)(13)(12)(13)$.

Theorem 7

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Definition 8

A permutation σ is called
even if it can be written as a product of an even number of transpositions.
odd if it can be written as a product of an odd number of transpositions.

Example. 12

$(12), (4321)$ *are odd, and* $(123), (25378)$ *are even. The identity* (1) *is even.*

Note that a cycle of odd length is even and a cycle of even length is odd.
If σ is an even (resp. odd) permutation, then σ^{-1} is also even (resp. odd).
The product of *two* even (or odd) permutations is again even; o.w. is odd.

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions.

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m} \delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions. Suppose that $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. (o.w. $\rho_1 \cdots \rho_k(a) = b$)

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions. Suppose that $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. (o.w. $\rho_1 \cdots \rho_k(a) = b$) *Among all products of length k that are equal to* (1), *and such that a appears in the transposition on the extreme left, we assume that $\rho_1 \cdots \rho_k$ has the fewest number of a's.*

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \dots \tau_{2m}, \delta_1, \dots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions. Suppose that $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. (o.w. $\rho_1 \cdots \rho_k(a) = b$)
Among all products of length k that are equal to (1), and such that a appears in the transposition on the extreme left, we assume that $\rho_1 \cdots \rho_k$ has the fewest number of a's.

Let a, u, v, r be distinct:

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions. Suppose that $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. (o.w. $\rho_1 \cdots \rho_k(a) = b$)

Among all products of length k that are equal to (1), and such that a appears in the transposition on the extreme left, we assume that $\rho_1 \cdots \rho_k$ has the fewest number of a's.

Let a, u, v, r be distinct: $(uv)(ar) = (ar)(uv)$ and $(uv)(av) = (au)(uv)$.

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \dots \tau_{2m}, \delta_1, \dots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions. Suppose that $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. (o.w. $\rho_1 \cdots \rho_k(a) = b$)
Among all products of length k that are equal to (1), and such that a appears in the transposition on the extreme left, we assume that $\rho_1 \cdots \rho_k$ has the fewest number of a's.
Let a, u, v, r be distinct: $(uv)(ar) = (ar)(uv)$ and $(uv)(av) = (au)(uv)$.
Hence we can move a transposition with entry a to the second position without changing the number of a's that appear $\Rightarrow$ say $\rho_2 = (ac), c \neq a$.

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions. Suppose that $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. (o.w. $\rho_1 \cdots \rho_k(a) = b$) *Among all products of length k that are equal to (1), and such that a appears in the transposition on the extreme left, we assume that $\rho_1 \cdots \rho_k$ has the fewest number of a's.*

Let a, u, v, r be distinct: $(uv)(ar) = (ar)(uv)$ and $(uv)(av) = (au)(uv)$. Hence we can move a transposition with entry a to the second position without changing the number of a's that appear $\Rightarrow$ say $\rho_2 = (ac), c \neq a$. If $c = b$, then $\rho_1\rho_2 = (1)$, and so $(1) = \rho_3 \cdots \rho_k$. (*contradiction*)

Proof of Theorem 7

Proof by contradiction: Suppose that the conclusion of the thm is false:

$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \quad \tau_1, \ldots \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ are transpositions.

Since $\delta_j = \delta_j^{-1}$ for $1 \leq j \leq 2n+1$, we have $\sigma^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\delta_{2n+1} \cdots \delta_1. \quad \Rightarrow$ The identity permutation is odd.

Suppose that $(1) = \rho_1 \cdots \rho_k (k \geq 3)$ is the *shortest* product of an odd number of transpositions. Suppose that $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. (o.w. $\rho_1 \cdots \rho_k(a) = b$)
Among all products of length k that are equal to (1), and such that a appears in the transposition on the extreme left, we assume that $\rho_1 \cdots \rho_k$ has the fewest number of a's.
Let a, u, v, r be distinct: $(uv)(ar) = (ar)(uv)$ and $(uv)(av) = (au)(uv)$.
Hence we can move a transposition with entry a to the second position without changing the number of a's that appear $\Rightarrow$ say $\rho_2 = (ac), c \neq a$.
If $c = b$, then $\rho_1\rho_2 = (1)$, and so $(1) = \rho_3 \cdots \rho_k$. (*contradiction*)
If $c \neq b$, $(ab)(ac) = (ac)(bc) \Rightarrow (1) = (ac)(bc)\rho_3 \cdots \rho_k$. (*contradiction*)