LINEAR ALGEBRA -II

B V Rajarama Bhat

Indian Statistical Institute, Bangalore

References

- Basic references:

References

- Basic references:
- Linear Algebra, A. Ramachandra Rao and P. Bhimasankaram.

References

- Basic references:
- Linear Algebra, A. Ramachandra Rao and P. Bhimasankaram.
- Algebra, Michael Artin.

References

- Basic references:
- Linear Algebra, A. Ramachandra Rao and P. Bhimasankaram.
- Algebra, Michael Artin.
- Linear Algebra, Henry Helson.

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:
- `https://lorecioni.github.io/fifteen-puzzle-game/`

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:
- https://lorecioni.github.io/fifteen-puzzle-game/
- Information on the Wikipedia :
  https://en.wikipedia.org/wiki/15_puzzle

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:
- `https://lorecioni.github.io/fifteen-puzzle-game/`
- Information on the Wikipedia :
  `https://en.wikipedia.org/wiki/15_puzzle`
- Question : Consider the initial configuration as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{bmatrix}$$

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:
- `https://lorecioni.github.io/fifteen-puzzle-game/`
- Information on the Wikipedia : `https://en.wikipedia.org/wiki/15_puzzle`
- Question : Consider the initial configuration as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{bmatrix}$$

- Can we re-arrange it to the natural order by moves permitted by the game?

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:
- https://lorecioni.github.io/fifteen-puzzle-game/
- Information on the Wikipedia : https://en.wikipedia.org/wiki/15_puzzle
- Question : Consider the initial configuration as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{bmatrix}$$

- Can we re-arrange it to the natural order by moves permitted by the game?
- Some rich man offered a lot of money for people to come up with a solution.

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:
- https://lorecioni.github.io/fifteen-puzzle-game/
- Information on the Wikipedia :
  https://en.wikipedia.org/wiki/15_puzzle
- Question : Consider the initial configuration as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{bmatrix}$$

- Can we re-arrange it to the natural order by moves permitted by the game?
- Some rich man offered a lot of money for people to come up with a solution.
- But there was no solution!

Lecture 1: Permutations

- Here is a well-known game, called fifteen puzzle:
- https://lorecioni.github.io/fifteen-puzzle-game/
- Information on the Wikipedia : https://en.wikipedia.org/wiki/15_puzzle
- Question : Consider the initial configuration as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{bmatrix}$$

- Can we re-arrange it to the natural order by moves permitted by the game?
- Some rich man offered a lot of money for people to come up with a solution.
- But there was no solution!
- The Rubik's cube is a toy very you see a lot of 'permutations' in action.

Definition

- Definition 1.1: Let S be a finite set. Then a bijective function $\sigma : S \to S$ is said to be a permutation of S.

Definition

- Definition 1.1: Let S be a finite set. Then a bijective function $\sigma : S \to S$ is said to be a permutation of S.
- Example 1.2: Take $S = \{s_1, s_2, \ldots, s_n\}$.

Definition

- Definition 1.1: Let S be a finite set. Then a bijective function $\sigma : S \to S$ is said to be a permutation of S.
- Example 1.2: Take $S = \{s_1, s_2, \ldots, s_n\}$.
- Define $\sigma_1 : S \to S$ by

$$\sigma_1(s_j) = \begin{cases} s_{j+1} & \text{if } \ 1 \leq j < n \\ s_1 & \text{if } \ j = n. \end{cases}$$

Definition

- Definition 1.1: Let S be a finite set. Then a bijective function $\sigma : S \to S$ is said to be a permutation of S.
- Example 1.2: Take $S = \{s_1, s_2, \ldots, s_n\}$.
- Define $\sigma_1 : S \to S$ by

$$\sigma_1(s_j) = \begin{cases} s_{j+1} & \text{if } \; 1 \le j < n \\ s_1 & \text{if } \; j = n. \end{cases}$$

- Assume $n \geq 3$. Define $\sigma_2 : S \to S$ by

$$\sigma_2(s_j) = \begin{cases} s_3 & \text{if } \; j = 1 \\ s_1 & \text{if } \; j = 3 \\ s_j & \text{otherwise.} \end{cases}$$

Definition

- Definition 1.1: Let S be a finite set. Then a bijective function $\sigma : S \to S$ is said to be a permutation of S.
- Example 1.2: Take $S = \{s_1, s_2, \ldots, s_n\}$.
- Define $\sigma_1 : S \to S$ by

$$\sigma_1(s_j) = \begin{cases} s_{j+1} & \text{if } \ 1 \leq j < n \\ s_1 & \text{if } \ j = n. \end{cases}$$

- Assume $n \geq 3$. Define $\sigma_2 : S \to S$ by

$$\sigma_2(s_j) = \begin{cases} s_3 & \text{if } \ j = 1 \\ s_1 & \text{if } \ j = 3 \\ s_j & \text{otherwise.} \end{cases}$$

- Then σ_1, σ_2 are permutations.

Notation

- One way to display the permutation is to write it down explicitly:

Notation

- One way to display the permutation is to write it down explicitly:
- We may show σ_1 above by:

$$\begin{pmatrix} s_1 & s_2 & \dots & s_{n-1} & s_n \\ s_2 & s_3 & \dots & s_n & s_1 \end{pmatrix}$$

Notation

- One way to display the permutation is to write it down explicitly:
- We may show σ_1 above by:

$$\begin{pmatrix} s_1 & s_2 & \dots & s_{n-1} & s_n \\ s_2 & s_3 & \dots & s_n & s_1 \end{pmatrix}$$

- Similarly σ_2 is displayed as:

$$\begin{pmatrix} s_1 & s_2 & s_3 & s_4 & \dots & s_n \\ s_3 & s_2 & s_1 & s_4 & \dots & s_n \end{pmatrix}$$

Group property

- Theorem 1.3: Let S be a finite set. Let G be the collection of all permutations of S.

Group property

- Theorem 1.3: Let S be a finite set. Let G be the collection of all permutations of S.
- If σ, τ are elements of G, then $\sigma \circ \tau$ is also an element of G and the operation $\circ$ has the following properties:

Group property

- Theorem 1.3: Let S be a finite set. Let G be the collection of all permutations of S.
- If σ, τ are elements of G, then $\sigma \circ \tau$ is also an element of G and the operation $\circ$ has the following properties:
- (i) Associativity: $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$ for all $\sigma_1, \sigma_2, \sigma_3$ in G.

Group property

- Theorem 1.3: Let S be a finite set. Let G be the collection of all permutations of S.
- If σ, τ are elements of G, then $\sigma \circ \tau$ is also an element of G and the operation $\circ$ has the following properties:
- (i) Associativity: $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$ for all $\sigma_1, \sigma_2, \sigma_3$ in G.
- (ii) Existence of identity: There exists $\iota \in G$ such that $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in G$.

Group property

- Theorem 1.3: Let S be a finite set. Let G be the collection of all permutations of S.
- If σ, τ are elements of G, then $\sigma \circ \tau$ is also an element of G and the operation $\circ$ has the following properties:
- (i) Associativity: $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$ for all $\sigma_1, \sigma_2, \sigma_3$ in G.
- (ii) Existence of identity: There exists $\iota \in G$ such that $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in G$.
- (iii) Existence of inverse: For $\sigma \in G$, there exists σ^{-1} in G such that $\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = \iota$.

Group property

- Theorem 1.3: Let S be a finite set. Let G be the collection of all permutations of S.
- If σ, τ are elements of G, then $\sigma \circ \tau$ is also an element of G and the operation $\circ$ has the following properties:
- (i) Associativity: $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$ for all $\sigma_1, \sigma_2, \sigma_3$ in G.
- (ii) Existence of identity: There exists $\iota \in G$ such that $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in G$.
- (iii) Existence of inverse: For $\sigma \in G$, there exists σ^{-1} in G such that $\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = \iota$.
- Proof. Take ι as the identity map and then properties (i) to (iii) should be clear.

cycles

- In the following we always take the finite set S under consideration as $\{1, 2, \ldots, n\}$ for some fixed $n \in \mathbb{N}$.

cycles

- In the following we always take the finite set S under consideration as $\{1, 2, \ldots, n\}$ for some fixed $n \in \mathbb{N}$.
- Example 1.4: Suppose $S = \{1, 2, \ldots 7\}$. Consider the permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 4 & 2 & 6 & 1 \end{pmatrix}$$

cycles

- In the following we always take the finite set S under consideration as $\{1, 2, \ldots, n\}$ for some fixed $n \in \mathbb{N}$.
- Example 1.4: Suppose $S = \{1, 2, \ldots 7\}$. Consider the permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 4 & 2 & 6 & 1 \end{pmatrix}$$

- We see $1 \dashrightarrow 3 \dashrightarrow 7 \dashrightarrow 1$. This we call as a cycle. It is a cycle of length 3.

cycles

- In the following we always take the finite set S under consideration as $\{1, 2, \ldots, n\}$ for some fixed $n \in \mathbb{N}$.
- Example 1.4: Suppose $S = \{1, 2, \ldots 7\}$. Consider the permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 4 & 2 & 6 & 1 \end{pmatrix}$$

- We see $1 \dashrightarrow 3 \dashrightarrow 7 \dashrightarrow 1$. This we call as a cycle. It is a cycle of length 3.
- This permutation also has $2 \dashrightarrow 5 \dashrightarrow 2$, a cycle of length 2.

cycles

- In the following we always take the finite set S under consideration as $\{1, 2, \ldots, n\}$ for some fixed $n \in \mathbb{N}$.
- Example 1.4: Suppose $S = \{1, 2, \ldots 7\}$. Consider the permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 4 & 2 & 6 & 1 \end{pmatrix}$$

- We see $1 \dashrightarrow 3 \dashrightarrow 7 \dashrightarrow 1$. This we call as a cycle. It is a cycle of length 3.
- This permutation also has $2 \dashrightarrow 5 \dashrightarrow 2$, a cycle of length 2.
- It also has $4 \dashrightarrow 4$ and $6 \dashrightarrow 6$, cycles of length 1.

cycles

- In the following we always take the finite set S under consideration as $\{1, 2, \ldots, n\}$ for some fixed $n \in \mathbb{N}$.
- Example 1.4: Suppose $S = \{1, 2, \ldots 7\}$. Consider the permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 4 & 2 & 6 & 1 \end{pmatrix}$$

- We see $1 \dashrightarrow 3 \dashrightarrow 7 \dashrightarrow 1$. This we call as a cycle. It is a cycle of length 3.
- This permutation also has $2 \dashrightarrow 5 \dashrightarrow 2$, a cycle of length 2.
- It also has $4 \dashrightarrow 4$ and $6 \dashrightarrow 6$, cycles of length 1.
- For distinct $k_1, k_2, \ldots, k_r$ in $\{1, 2, \ldots, n\}$ (with $r \in \mathbb{N}$) we denote the cycle $k_1 \dashrightarrow k_2 \dashrightarrow \cdots \dashrightarrow k_r \dashrightarrow k_1$ simply as $(k_1, k_2, \ldots, k_r)$.

Cycle decomposition of permutations

- For any permutation σ, σ^2 denotes $\sigma \circ \sigma$ and more generally for any natural number r, $\sigma^r = \sigma \circ \sigma \circ \cdots \circ \sigma \quad (r \ \text{ times})$.

Cycle decomposition of permutations

- For any permutation σ, σ^2 denotes $\sigma \circ \sigma$ and more generally for any natural number r, $\sigma^r = \sigma \circ \sigma \circ \cdots \circ \sigma \quad (r \ \text{ times})$.
- Lemma 1.5: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then for any $k_1 \in S$, there exists $r \in \mathbb{N}$ such that $\sigma^r(k_1) = k_1$.

Cycle decomposition of permutations

- For any permutation σ, σ^2 denotes $\sigma \circ \sigma$ and more generally for any natural number r, $\sigma^r = \sigma \circ \sigma \circ \cdots \circ \sigma \quad (r \ \text{ times})$.
- Lemma 1.5: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then for any $k_1 \in S$, there exists $r \in \mathbb{N}$ such that $\sigma^r(k_1) = k_1$.
- Proof. Take $k_2 = \sigma(k_1)$. If $k_2 = k_1$, we can take $r = 1$, and we are done.

Cycle decomposition of permutations

- For any permutation σ, σ^2 denotes $\sigma \circ \sigma$ and more generally for any natural number r, $\sigma^r = \sigma \circ \sigma \circ \cdots \circ \sigma \quad (r \text{ times})$.
- Lemma 1.5: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then for any $k_1 \in S$, there exists $r \in \mathbb{N}$ such that $\sigma^r(k_1) = k_1$.
- Proof. Take $k_2 = \sigma(k_1)$. If $k_2 = k_1$, we can take $r = 1$, and we are done.
- If $k_2 \neq k_1$, take $k_3 = \sigma(k_2)$. If $k_3 = k_1$, we can take $r = 2$ and we are done.

Cycle decomposition of permutations

- For any permutation σ, σ^2 denotes $\sigma \circ \sigma$ and more generally for any natural number r, $\sigma^r = \sigma \circ \sigma \circ \cdots \circ \sigma \quad (r \ \text{times})$.
- Lemma 1.5: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then for any $k_1 \in S$, there exists $r \in \mathbb{N}$ such that $\sigma^r(k_1) = k_1$.
- Proof. Take $k_2 = \sigma(k_1)$. If $k_2 = k_1$, we can take $r = 1$, and we are done.
- If $k_2 \neq k_1$, take $k_3 = \sigma(k_2)$. If $k_3 = k_1$, we can take $r = 2$ and we are done.
- $k_3 = k_2$ is not possible, as this would mean that $k_2 = \sigma(k_1) = \sigma(k_2)$ and contradicting injectivity of σ.

Continuation

- Continuing this way, by induction if we get distinct $k_1, k_2, \ldots, k_s$ with $k_1 \dashrightarrow k_2 \dashrightarrow \cdots \dashrightarrow k_s$, we take $k_{s+1} = \sigma(k_s)$. If $k_{s+1} = k_1$, we can take $r = s$ and we are done.

Continuation

- Continuing this way, by induction if we get distinct $k_1, k_2, \ldots, k_s$ with $k_1 \dashrightarrow k_2 \dashrightarrow \cdots \dashrightarrow k_s$, we take $k_{s+1} = \sigma(k_s)$. If $k_{s+1} = k_1$, we can take $r = s$ and we are done.
- For any $2 \leq t \leq s$, $k_{s+1} = k_t = \sigma(k_{t-1})$ is not possible due to injectivity of σ.

Continuation

- Continuing this way, by induction if we get distinct $k_1, k_2, \ldots, k_s$ with $k_1 \dashrightarrow k_2 \dashrightarrow \cdots \dashrightarrow k_s$, we take $k_{s+1} = \sigma(k_s)$. If $k_{s+1} = k_1$, we can take $r = s$ and we are done.
- For any $2 \leq t \leq s$, $k_{s+1} = k_t = \sigma(k_{t-1})$ is not possible due to injectivity of σ.
- If $k_1, \ldots, k_{s+1}$ are all distinct, we can continue the induction process.

Continuation

- Continuing this way, by induction if we get distinct $k_1, k_2, \ldots, k_s$ with $k_1 \dashrightarrow k_2 \dashrightarrow \cdots \dashrightarrow k_s$, we take $k_{s+1} = \sigma(k_s)$. If $k_{s+1} = k_1$, we can take $r = s$ and we are done.
- For any $2 \leq t \leq s$, $k_{s+1} = k_t = \sigma(k_{t-1})$ is not possible due to injectivity of σ.
- If $k_1, \ldots, k_{s+1}$ are all distinct, we can continue the induction process.
- This process has to terminate after some steps as the set S is finite. In fact S has exactly n distinct elements and so we will have $r \leq n$.

Continuation

- Continuing this way, by induction if we get distinct $k_1, k_2, \ldots, k_s$ with $k_1 \dashrightarrow k_2 \dashrightarrow \cdots \dashrightarrow k_s$, we take $k_{s+1} = \sigma(k_s)$. If $k_{s+1} = k_1$, we can take $r = s$ and we are done.
- For any $2 \leq t \leq s$, $k_{s+1} = k_t = \sigma(k_{t-1})$ is not possible due to injectivity of σ.
- If $k_1, \ldots, k_{s+1}$ are all distinct, we can continue the induction process.
- This process has to terminate after some steps as the set S is finite. In fact S has exactly n distinct elements and so we will have $r \leq n$.
- Exercise 1.6: Show that there exists some $t \in \mathbb{N}$ such that $\sigma^t(j) = j$ for all $j \in S$.

Products of cycles

- We have seen that a permutation may have several cycles.

Products of cycles

- We have seen that a permutation may have several cycles.
- We may write down the permutation by listing the cycles it has.

Products of cycles

- We have seen that a permutation may have several cycles.
- We may write down the permutation by listing the cycles it has.
- For instance, the permutation of Example 1.4, is written as $(1, 3, 7)(2, 5)(4)(6)$.

Products of cycles

- We have seen that a permutation may have several cycles.
- We may write down the permutation by listing the cycles it has.
- For instance, the permutation of Example 1.4, is written as $(1,3,7)(2,5)(4)(6)$.
- We may also write it as $(3,7,1)(4)(2,5),(6)$ or as $(7,1,3)(5,2)(6)(4)$. In other words, in what order we write these cycles does not matter.

Products of cycles

- We have seen that a permutation may have several cycles.
- We may write down the permutation by listing the cycles it has.
- For instance, the permutation of Example 1.4, is written as $(1, 3, 7)(2, 5)(4)(6)$.
- We may also write it as $(3, 7, 1)(4)(2, 5), (6)$ or as $(7, 1, 3)(5, 2)(6)(4)$. In other words, in what order we write these cycles does not matter.
- Some authors do not write down 1-cycles at all. It is understood that elements of S which are not written down form 1-cycles.

Products of cycles

- We have seen that a permutation may have several cycles.
- We may write down the permutation by listing the cycles it has.
- For instance, the permutation of Example 1.4, is written as $(1,3,7)(2,5)(4)(6)$.
- We may also write it as $(3,7,1)(4)(2,5),(6)$ or as $(7,1,3)(5,2)(6)(4)$. In other words, in what order we write these cycles does not matter.
- Some authors do not write down 1-cycles at all. It is understood that elements of S which are not written down form 1-cycles.
- With this notation this permutation is simply $(1,3,7),(2,5)$ or $(3,7,1)(5,2)$ etc.

Products of cycles continued

- Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.

Products of cycles continued

- Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.
- Then $(k_1, k_2, \ldots, k_r)$ denotes the permutation:

$$k_1 \dashrightarrow k_2 \dashrightarrow k_3 \dashrightarrow \ldots \dashrightarrow k_r \dashrightarrow k_1, j \dashrightarrow j \ \text{ otherwise.}$$

Products of cycles continued

- Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.
- Then $(k_1, k_2, \ldots, k_r)$ denotes the permutation:

$$k_1 \dashrightarrow k_2 \dashrightarrow k_3 \dashrightarrow \ldots \dashrightarrow k_r \dashrightarrow k_1, j \dashrightarrow j \ \text{ otherwise.}$$

Products of cycles continued

- Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.
- Then $(k_1, k_2, \ldots, k_r)$ denotes the permutation:

$$k_1 \dashrightarrow k_2 \dashrightarrow k_3 \dashrightarrow \ldots \dashrightarrow k_r \dashrightarrow k_1, j \dashrightarrow j \quad \text{otherwise.}$$

Products of cycles continued

- Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.
- Then $(k_1, k_2, \ldots, k_r)$ denotes the permutation:

$$k_1 \dashrightarrow k_2 \dashrightarrow k_3 \dashrightarrow \ldots \dashrightarrow k_r \dashrightarrow k_1, j \dashrightarrow j \quad \text{otherwise.}$$

- More generally if $k_{11}, k_{12}, \ldots, k_{1r_1},\ k_{21}, k_{22}, \ldots, k_{2r_2}, k_{31}, k_{32}, \ldots, k_{3r_3}, \ldots, k_{m1}, k_{m2}, \ldots k_{mr_m}$ are distinct elements of S, then

$$(k_{11}, k_{12}, \ldots, k_{1r_1})(k_{21}, k_{22}, \ldots, k_{2r_2}) \cdots (k_{m1}, k_{m2}, \ldots, k_{mr_m})$$

is a 'product' of cycles, with

$$\sigma(k_{11}) = k_{12}, \sigma(k_{12}) = k_{13}, \ldots, \sigma(k_{1r_1}) = k_{11},$$

$$\sigma(k_{21}) = k_{22}, \ldots, \sigma(k_{2r_2}) = k_{21}, \ldots,$$

$$\sigma(k_{m1}) = k_{m2} \ldots, \sigma(k_{mr_m}) = k_{m1}, \sigma(j) = j, \quad \text{otherwise.}$$

Products of cycles theorem

- Theorem 1.7: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ Suppose σ is a permutation of S. Then S decomposes uniquely as a product of cycles.

Products of cycles theorem

- Theorem 1.7: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ Suppose σ is a permutation of S. Then S decomposes uniquely as a product of cycles.
- Proof. Take $k_1 = 1$. Then by Lemma 1.3, and its proof, σ has a cycle $(k_1, k_2, \ldots, k_r)$ with $k_1 = 1$.

Products of cycles theorem

- Theorem 1.7: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ Suppose σ is a permutation of S. Then S decomposes uniquely as a product of cycles.
- Proof. Take $k_1 = 1$. Then by Lemma 1.3, and its proof, σ has a cycle $(k_1, k_2, \ldots, k_r)$ with $k_1 = 1$.
- If $S = \{k_1, k_2, \ldots, k_r\}$, we are done. If not, take any $j \in \{k_1, k_2, \ldots, k_r\}^c$, and we can get a cycle $(j_1, j_2, \ldots)$ with elements distinct from $\{k_1, k_2, \ldots, k_r\}$. Continuing this way, we can exhaust whole of S, as S is a finite set.

Products of cycles theorem

- Theorem 1.7: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ Suppose σ is a permutation of S. Then S decomposes uniquely as a product of cycles.
- Proof. Take $k_1 = 1$. Then by Lemma 1.3, and its proof, σ has a cycle $(k_1, k_2, \ldots, k_r)$ with $k_1 = 1$.
- If $S = \{k_1, k_2, \ldots, k_r\}$, we are done. If not, take any $j \in \{k_1, k_2, \ldots, k_r\}^c$, and we can get a cycle $(j_1, j_2, \ldots)$ with elements distinct from $\{k_1, k_2, \ldots, k_r\}$. Continuing this way, we can exhaust whole of S, as S is a finite set.
- Clearly then, the permutation σ is a product of cycles. The uniqueness should also be clear as these cycles determine σ.

Products of cycles theorem

- Theorem 1.7: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ Suppose σ is a permutation of S. Then S decomposes uniquely as a product of cycles.
- Proof. Take $k_1 = 1$. Then by Lemma 1.3, and its proof, σ has a cycle $(k_1, k_2, \ldots, k_r)$ with $k_1 = 1$.
- If $S = \{k_1, k_2, \ldots, k_r\}$, we are done. If not, take any $j \in \{k_1, k_2, \ldots, k_r\}^c$, and we can get a cycle $(j_1, j_2, \ldots)$ with elements distinct from $\{k_1, k_2, \ldots, k_r\}$. Continuing this way, we can exhaust whole of S, as S is a finite set.
- Clearly then, the permutation σ is a product of cycles. The uniqueness should also be clear as these cycles determine σ.
- For i, j in S, write $i \sim j$ if $j = \sigma^r(i)$ for some $r \in \{0, 1, \ldots\}$.

Products of cycles theorem

- Theorem 1.7: Let $S = \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$ Suppose σ is a permutation of S. Then S decomposes uniquely as a product of cycles.
- Proof. Take $k_1 = 1$. Then by Lemma 1.3, and its proof, σ has a cycle $(k_1, k_2, \dots, k_r)$ with $k_1 = 1$.
- If $S = \{k_1, k_2, \dots, k_r\}$, we are done. If not, take any $j \in \{k_1, k_2, \dots, k_r\}^c$, and we can get a cycle $(j_1, j_2, \dots)$ with elements distinct from $\{k_1, k_2, \dots, k_r\}$. Continuing this way, we can exhaust whole of S, as S is a finite set.
- Clearly then, the permutation σ is a product of cycles. The uniqueness should also be clear as these cycles determine σ.
- For i, j in S, write $i \sim j$ if $j = \sigma^r(i)$ for some $r \in \{0, 1, \dots\}$.
- Then $\sim$ is an equivalence relation. (Exercise).

Products of cycles theorem

- Theorem 1.7: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ Suppose σ is a permutation of S. Then S decomposes uniquely as a product of cycles.
- Proof. Take $k_1 = 1$. Then by Lemma 1.3, and its proof, σ has a cycle $(k_1, k_2, \ldots, k_r)$ with $k_1 = 1$.
- If $S = \{k_1, k_2, \ldots, k_r\}$, we are done. If not, take any $j \in \{k_1, k_2, \ldots, k_r\}^c$, and we can get a cycle $(j_1, j_2, \ldots)$ with elements distinct from $\{k_1, k_2, \ldots, k_r\}$. Continuing this way, we can exhaust whole of S, as S is a finite set.
- Clearly then, the permutation σ is a product of cycles. The uniqueness should also be clear as these cycles determine σ.
- For i, j in S, write $i \sim j$ if $j = \sigma^r(i)$ for some $r \in \{0, 1, \ldots\}$.
- Then $\sim$ is an equivalence relation. (Exercise).
- It maybe seen that i, j are in the same cycle if and only if $i \sim j$. In other words, the equivalence classes form different cycles of the permutation.

Signature of a permutation

- Definition 1.8: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then the signature of σ is defined as the number

$$\epsilon(\sigma) = (-1)^{n-p}$$

where p is the number of cycles (including cycles of length 1) in the cycle decomposition of σ.

Signature of a permutation

- Definition 1.8: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then the signature of σ is defined as the number
$$\epsilon(\sigma) = (-1)^{n-p}$$
where p is the number of cycles (including cycles of length 1) in the cycle decomposition of σ.
- For instance for the permutation σ of Example 1.3, $\epsilon(\sigma) = (-1)^{7-4} = (-1)^3 = -1$.

Signature of a permutation

- Definition 1.8: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then the signature of σ is defined as the number
$$\epsilon(\sigma) = (-1)^{n-p}$$
where p is the number of cycles (including cycles of length 1) in the cycle decomposition of σ.
- For instance for the permutation σ of Example 1.3, $\epsilon(\sigma) = (-1)^{7-4} = (-1)^3 = -1$.
- Note that the signature of identity permutation is always 1.

Signature of a permutation

- Definition 1.8: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then the signature of σ is defined as the number

$$\epsilon(\sigma) = (-1)^{n-p}$$

where p is the number of cycles (including cycles of length 1) in the cycle decomposition of σ.
- For instance for the permutation σ of Example 1.3, $\epsilon(\sigma) = (-1)^{7-4} = (-1)^3 = -1$.
- Note that the signature of identity permutation is always 1.
- A cycle $(k_1, k_2, \ldots, k_r)$ can be identified with the permutation σ defined by

$$\sigma(k_1) = k_2, \sigma(k_2) = k_3, \ldots, \sigma(k_r) = k_1$$

and $\sigma(j) = j$ for $j \notin \{k_1, k_2, \ldots, k_r\}$.

Signature of a permutation

- Definition 1.8: Let $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and let σ be a permutation of S. Then the signature of σ is defined as the number
$$\epsilon(\sigma) = (-1)^{n-p}$$
where p is the number of cycles (including cycles of length 1) in the cycle decomposition of σ.
- For instance for the permutation σ of Example 1.3, $\epsilon(\sigma) = (-1)^{7-4} = (-1)^3 = -1$.
- Note that the signature of identity permutation is always 1.
- A cycle $(k_1, k_2, \ldots, k_r)$ can be identified with the permutation σ defined by
$$\sigma(k_1) = k_2, \sigma(k_2) = k_3, \ldots, \sigma(k_r) = k_1$$
and $\sigma(j) = j$ for $j \notin \{k_1, k_2, \ldots, k_r\}$.
- Therefore the signature of a cycle is defined as $(k_1, k_2, \ldots, k_r) = (-1)^{n-(1+(n-r))} = (-1)^{r-1}$.

Continuation

- Cycles of length two are known as transpositions. We see that transpositions have signature (-1).

Continuation

- Cycles of length two are known as transpositions. We see that transpositions have signature (-1).
- Permutations with signature $(+1)$ are known as even permutations and those with signature (-1) are known as odd permutations.

Continuation

- Cycles of length two are known as transpositions. We see that transpositions have signature (-1).
- Permutations with signature $(+1)$ are known as even permutations and those with signature (-1) are known as odd permutations.
- END OF LECTURE 1.