# 離散数理工学　第 5 回
# 離散代数：対称群と置換群

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2017 年 11 月 14 日

最終更新：2017 年 11 月 13 日　11:31



## スケジュール 前半 (予定)



注意：予定の変更もありうる



## スケジュール 後半 (予定)



注意：予定の変更もありうる



## 今日の目標

**今日の目標**

置換群に関する基礎的な用語が使えるようになる
- 置換，二行記法，巡回記法，互換
- 偶置換，奇置換
- 置換群，対称群，交代群
- 生成系





## 目次





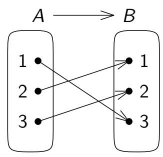


## 置換

有限集合 $X$

**置換とは？**

$X$ 上の置換とは，$X$ から $X$ への全単射のこと




$\{1, 2, 3\}$ 上の置換



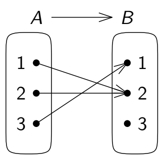


## 復習：全単射

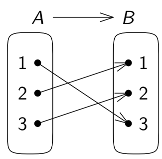
集合 $A, B$ と写像 $f\colon A \to B$

**全単射とは？**

$f$ が全単射であるとは，全射であり，かつ，単射であること




全単射ではない




全単射である





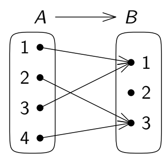
## 復習：全射

集合 $A, B$ と写像 $f\colon A \to B$

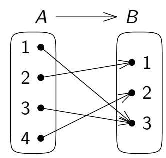
**全射とは？**

$f$ が全射であるとは，次を満たすこと

任意の $b \in B$ に対して，ある $a \in A$ が存在して $b = f(a)$




全射ではない




全射である

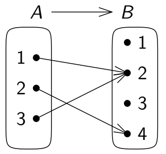
## 復習：単射

集合 $A, B$ と写像 $f\colon A \to B$

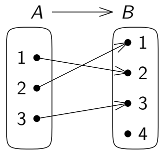
**単射とは？**

$f$ が単射であるとは，次を満たすこと

$$\text{任意の } a, a' \in A \text{ に対して，} \quad f(a) = f(a') \text{ ならば } a = a'$$




単射ではない




単射である





## 復習：写像の合成

集合 $A, B, C$ と写像 $f\colon A \to B$, $g\colon B \to C$

**写像の合成とは？**

写像 $f$ と $g$ の合成を $g \circ f\colon A \to C$ と表記し，任意の $x \in A$ に対して

$$(g \circ f)(x) = g(f(x))$$

とすることで定義する

注意：$f$ の終域と $g$ の始域が同じでないといけない
(同じでないときは合成を定義できない)





## 復習：写像の合成：例

- $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$, $C = \{8, 9\}$
- 写像 $f\colon A \to B$ を次で定義
  - $f(1) = 5$, $f(2) = 4$, $f(3) = 7$
- 写像 $g\colon B \to C$ を次で定義
  - $g(4) = 8$, $g(5) = 9$, $g(6) = 9$, $g(7) = 8$

このとき，$g \circ f\colon A \to C$ を考えると，

$$(g \circ f)(3) = g(f(3)) = g(7) = 8$$

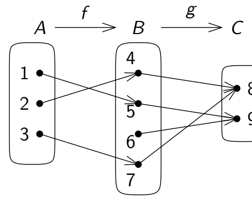


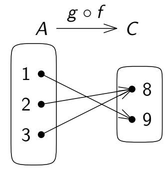


## 復習：写像の合成：例 (続)

- $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$, $C = \{8, 9\}$
- 写像 $f\colon A \to B$ を次で定義
  - $f(1) = 5$, $f(2) = 4$, $f(3) = 7$
- 写像 $g\colon B \to C$ を次で定義
  - $g(4) = 8$, $g(5) = 9$, $g(6) = 9$, $g(7) = 8$

このとき，$g \circ f\colon A \to C$ を考えると，





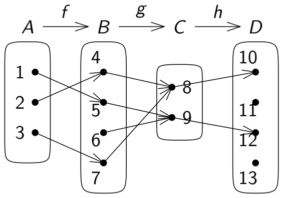



## 写像の合成の性質 (1)

集合 $A, B, C, D$ と写像 $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$

**演習問題 (結合法則)**

写像として，$h \circ (g \circ f) = (h \circ g) \circ f$




この性質より，$h \circ (g \circ f)$ や $(h \circ g) \circ f$ を $h \circ g \circ f$ と書くことが
正当化される



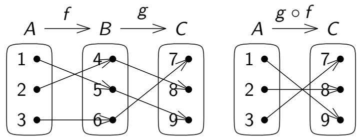


## 写像の合成の性質 (2)

集合 $A, B, C$ と写像 $f\colon A \to B$, $g\colon B \to C$

**演習問題 (全単射の合成も全単射)**

$f$ と $g$ が全単射 $\Rightarrow$ $g \circ f$ も全単射








## 復習：恒等写像

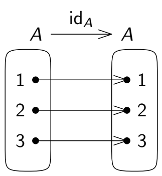
集合 $A$ と写像 $f\colon A \to A$

**恒等写像とは？**

$f$ が恒等写像であるとは，任意の $a \in A$ に対して $a = f(a)$ であること

- $A \to A$ の恒等写像を $\mathrm{id}_A$ と書くこともある
- 例：$A = \{1, 2, 3\}$ のとき $f\colon A \to A$ で

$$f(1) = 1, \quad f(2) = 2, \quad f(3) = 3$$




注：恒等写像は置換である



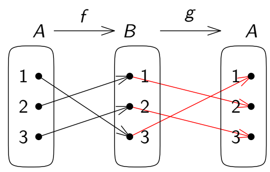


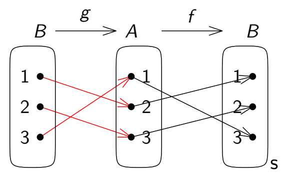
## 復習：逆写像

集合 $A, B$ と写像 $f\colon A \to B$

**逆写像とは？**

$f$ の逆写像とは，写像 $g\colon B \to A$ で，$g \circ f = \mathrm{id}_A$ かつ $f \circ g = \mathrm{id}_B$ を
満たすもの　　　　($\mathrm{id}_A\colon A \to A$，$\mathrm{id}_B$ は恒等写像)




この $f$ の逆写像は存在する

**記法**

$f$ の逆写像が存在するとき，それを $f^{-1}$ で表す

## 復習：逆写像の性質

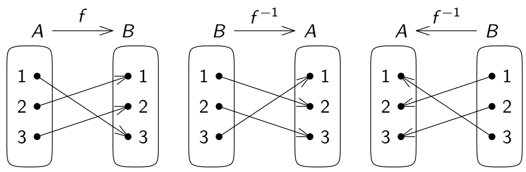
集合 $A, B$，写像 $f\colon A \to B$

### 逆写像が存在するための必要十分条件

写像 $f$ の逆写像が存在する $\Leftrightarrow$ $f$ が全単射

### 逆写像の性質

全単射 $f$ の逆写像 $f^{-1}$ も全単射





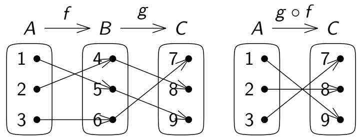


## 写像の合成の性質 (3)

集合 $A, B, C$ と全単射 $f\colon A \to B$, $g\colon B \to C$

### 演習問題 (合成の逆写像は逆写像の合成)

写像として，$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$







## 置換の性質 (ここまでのまとめ)

有限集合 $X$

### ここまでのまとめ

1. 恒等写像 $\mathrm{id}_X$ は $X$ 上の置換
2. $\pi$ が $X$ 上の置換 $\Rightarrow$ $\pi^{-1}$ も $X$ 上の置換
3. $\pi, \rho$ が $X$ 上の置換 $\Rightarrow$ $\pi \circ \rho$ も $X$ 上の置換

置換の文脈では以下の用語・記法も使う

- $\mathrm{id}_X$ は $X$ 上の恒等置換で，$e$ と書くことがある
- 置換 $\pi$ に対して，$\pi^{-1}$ を $\pi$ の逆置換
- 置換の合成を置換の積とも言う
- $\pi \circ \rho$ を $\pi\rho$ とも書く
- $\pi \circ \pi$ を $\pi^2$ とも書く ($\pi^3, \pi^4$ なども使う)
- $\pi^{-1} \circ \pi^{-1}$ を $\pi^{-2}$ とも書く ($\pi^{-3}, \pi^{-4}$ なども使う)
  - 注：$(\pi^2)^{-1} = (\pi^{-1})^2$

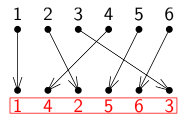




## 置換を見て何を思うか？

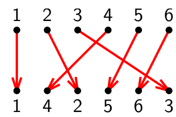
### 置換を見て何を思うか？ (1)

順列としての置換　(静的な見方)



### 置換を見て何を思うか？ (2)

全単射としての置換 (動的な見方)



2 つの見方を柔軟に使い分けることができるとよい





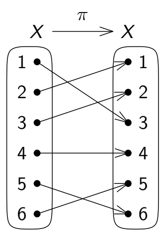
## 置換の二行記法

有限集合 $X = \{1, 2, \ldots, n\}$

### 置換の二行記法

$X$ 上の置換 $\pi$ を次のように書くことがある

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



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

注意

- 二行記法で用いる括弧は必ず丸括弧
- $X = \{1, 2, \ldots, n\}$ でなくても，同じ記法を用いることができる





## 二行記法に慣れる

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}$ のとき，

$$\begin{aligned}
\pi \circ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 4 & 3 & 1 & 6 & 2 & 5 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix}, \\
\pi^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 3 & 1 & 2 & 4 & 6 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}.
\end{aligned}$$





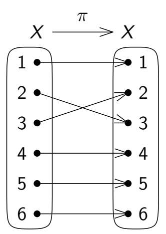
## 特殊な置換：隣接互換 (基本互換)

有限集合 $X = \{1, 2, \ldots, n\}$

### 隣接互換とは？

$X$ 上の置換 $\pi$ が隣接互換であるとは，ある $i$ を用いて次のように書けること

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ 1 & 2 & \cdots & i+1 & i & \cdots & n \end{pmatrix}$$



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





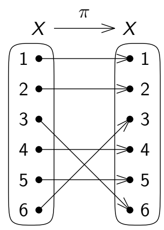
## 特殊な置換：互換

有限集合 $X = \{1, 2, \ldots, n\}$

### 互換とは？

$X$ 上の置換 $\pi$ が互換であるとは，ある $i, j$ を用いて次のように書けること

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$



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

注意

- 隣接互換は互換である

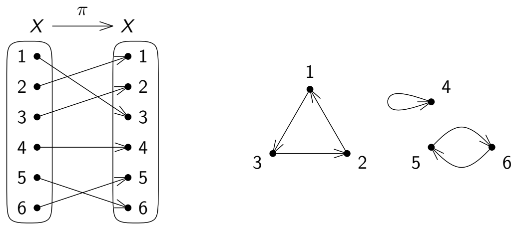
## 目次







## 置換の巡回記法：直感




二行記法：$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$　　巡回記法：$\pi = (1\ 3\ 2)(5\ 6)$





## 置換の巡回置換

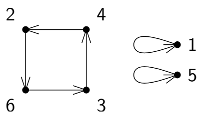
有限集合 $X = \{1, 2, \dots, n\}$

**巡回置換とは？**

$X$ 上の置換 $\pi$ が巡回互換であるとは，
ある $x \in X$ と自然数 $k \geq 2$ が存在して，次が成り立つこと

- $x, \pi(x), \pi^2(x), \dots, \pi^{k-1}(x)$ がすべて異なり，
- $x = \pi^k(x)$ であり，
- 任意の $y \in X - \{x, \pi(x), \dots, \pi^{k-1}(x)\}$ に対して，$y = \pi(y)$

巡回置換を $\pi = (x\ \pi(x)\ \pi^2(x)\ \cdots\ \pi^{k-1}(x))$ とも表す　(巡回記法)




$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 5 & 3 \end{pmatrix} = (2\ 6\ 3\ 4)$$

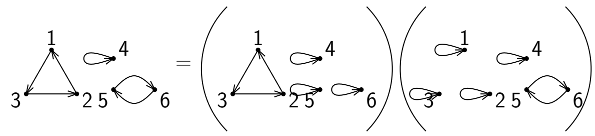




## 置換の巡回記法

**巡回記法とは？**

置換を互いに素な巡回置換の積 (合成) として表したもの




$$\pi = (1\ 3\ 2)(5\ 6)$$





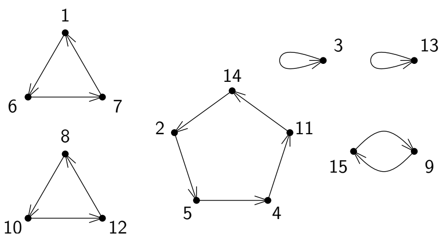
## 巡回記法に慣れる (1)

- 二行記法

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

- 巡回記法

$$(1\ 6\ 7)(2\ 5\ 4\ 11\ 14)(8\ 10\ 12)(9\ 15)$$








## 巡回記法に慣れる (2)

$X = \{1, 2, 3, 4\}$ 上の置換をすべて考えてみる

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = ()$　(or, $e$)　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 2)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (3\ 4)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (2\ 3)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 3)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (2\ 3\ 4)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 4\ 3)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 2\ 4)$





## 巡回記法に慣れる (3)

$X = \{1, 2, 3, 4\}$ 上の置換をすべて考えてみる

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\ 3\ 2)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (1\ 4\ 2)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\ 3)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (1\ 4\ 3)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (2\ 3\ 4)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = (1\ 4)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1\ 4\ 2\ 3)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1\ 3\ 2\ 4)$　　$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$

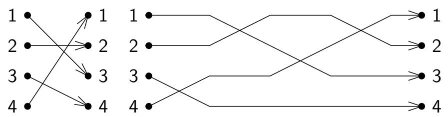




## 目次

## 置換を互換の積として表してみる

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 3)(1\ 2)(3\ 4)$$

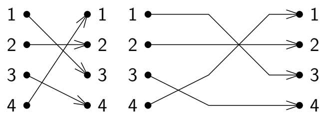






## 置換を互換の積として表してみる：Part 2

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3)(3\ 4)$$







## 置換を互換の積として表してみる：互換の数の偶奇性

**ここまでのまとめ**

- 任意の置換は，いくつかの互換の積 (合成) として表せる
- その表し方は，一通りではない

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 3)(1\ 2)(3\ 4) = (1\ 3)(3\ 4)$$

しかし，次が (一般的に) 言える

**性質：互換の数の偶奇性**

任意の有限集合 $X$ 上の任意の置換 $\pi$ に対して，
$\pi$ を互換の積として表したとき，現れる互換の数の偶奇は必ず等しい





## 互換の数の偶奇性：証明 (1)

**性質：互換の数の偶奇性 (再掲)**

任意の有限集合 $X$ 上の任意の置換 $\pi$ に対して，
$\pi$ を互換の積として表したとき，現れる互換の数の偶奇は必ず等しい

証明：背理法による

- $\pi$ を偶数個の互換の積，奇数個の互換の積として表せると仮定
- このとき，$\pi^{-1}$ も偶数個の互換の積，奇数個の互換の積として表せる
- $\pi \circ \pi^{-1} = e$ なので，恒等置換 $e$ は奇数個の互換の積で表せる

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} &= (1\ 3)(3\ 4) \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}^{-1} &= ((1\ 3)(3\ 4))^{-1} = (3\ 4)^{-1}(1\ 3)^{-1} = (4\ 3)(3\ 1) \end{aligned}$$





## 互換の数の偶奇性：証明 (2)

**補題**

奇数個の互換の積は恒等置換 $e$ にならない
(これが証明できれば，矛盾が得られる)

補題の証明：次を数学的帰納法により証明する

任意の自然数 $k \geq 0$ に対して，
$e$ が $2k+1$ 個の互換の積として書けると，矛盾が導かれる

- $k = 0$ のとき，$e = (i\ j)$ であるとすると，
$e(i) = j$ となり，$e$ が恒等置換であることに矛盾
- 任意の $k \geq 0$ を考え，$e$ が $2k+1$ 個の互換の積で書けないと仮定する
- $e = (a_1\ b_1) \cdots (a_{2k+3}\ b_{2k+3})$ と $e$ が $2k+3$ 個の互換の積で書けるとする
- そのような互換の積の中で,「$a_1$ の出現回数」が最小のものを考える
(最小性論法)





## 互換の数の偶奇性：証明 (3)

- $a_1 \in \{a_i, b_i\}$ となる最小の $i \geq 2$ を考える
- 注：そのような $i$ は必ず存在する (なぜ？)
- このとき，$e$ は次のように書き換えられる

$$e = (a_1\ b_1)(a_i\ b_i)(a_2\ b_2) \cdots (a_{i-1}\ b_{i-1})(a_{i+1}\ b_{i+1}) \cdots (a_{2k+3}\ b_{2k+3})$$

- ここで場合分け
- $\boxed{\text{場合 1}}$：$|\{a_1, b_1\} \cap \{a_i, b_i\}| = 2$ のとき
- このとき，$(a_1\ b_1) = (a_i\ b_i)$ であるので，$(a_1\ b_1)(a_i\ b_i) = e$ であり，

$$e = (a_2\ b_2) \cdots (a_{i-1}\ b_{i-1})(a_{i+1}\ b_{i+1}) \cdots (a_{2k+3}\ b_{2k+3})$$

となる
- つまり，$e$ は $2k+1$ 個の互換の積となり，帰納法の仮定に矛盾



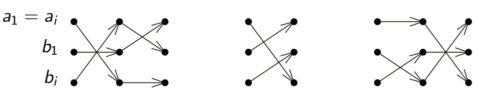


## 互換の数の偶奇性：証明 (4)

- $\boxed{\text{場合 2}}$：$|\{a_1, b_1\} \cap \{a_i, b_i\}| = 1$ のとき
- 例えば，$a_1 = a_i, b_1 \neq b_i$ とする ($a_1 = b_i, b_1 \neq a_i$ のときも同様)
- このとき，$(a_1\ b_1)(a_i\ b_i) = (a_1\ b_1)(a_1\ b_i) = (a_1\ b_i)(b_1\ b_i)$
- したがって，

$$e = (a_1\ b_i)(b_1\ b_i) \cdots (a_{i-1}\ b_{i-1})(a_{i+1}\ b_{i+1}) \cdots (a_{2k+3}\ b_{2k+3})$$

- これは，先ほどの表現が $a_1$ の出現回数を最小にしていたことに矛盾 □




$(a_1\ b_1)(a_1\ b_i)$ $(a_1\ b_i\ b_1)$ $(a_1\ b_i)(b_1\ b_i)$





## 偶置換と奇置換

**性質：互換の数の偶奇性 (再掲)**

任意の有限集合 $X$ 上の任意の置換 $\pi$ に対して，
$\pi$ を互換の積として表したとき，現れる互換の数の偶奇は必ず等しい

この性質をもとにして，次の用語を定義する

**偶置換，奇置換とは？**

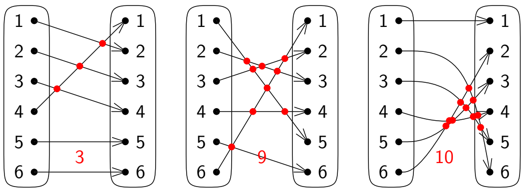
偶置換とは，偶数個の互換の積として表せる置換のこと
奇置換とは，奇数個の互換の積として表せる置換のこと

例：

- 恒等置換 $e$ は偶置換
- 巡回置換 $(1\ 2\ 3\ 4)$ は奇置換 $((1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4))$

## 偶置換か奇置換か，簡単に判別するには？

「交点の数」の偶奇を調べればよい








## 目次







## 置換群とは？

有限集合 $X$

**置換群とは？**

$X$ 上の置換群とは，$X$ 上の置換の集合 $S$ で以下を満たすもの

1. $e \in S$ (恒等置換を持つ)
2. $\pi, \sigma \in S$ ならば $\pi\sigma \in S$ (積で閉じている)
3. $\pi \in S$ ならば $\pi^{-1} \in S$ (逆置換も持つ)





## 代表的な置換群 (1)：対称群

有限集合 $X$

**対称群とは？**

$X$ 上の対称群とは，$X$ 上の置換をすべて集めた集合

- $S(X)$, $\mathcal{S}(X)$, $\mathfrak{S}(X)$ と書くことが多い
- $|X| = n$ のときは，$n$ 次の対称群 ($n$ 次対称群) と呼ばれ，$S_n$, $\mathcal{S}_n$, $\mathfrak{S}_n$ と書くことが多い

例：$X = \{1, 2, 3\}$ のとき

$$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

注：$|S_n| = n!$





## 代表的な置換群 (2)：交代群

有限集合 $X$

**交代群とは？**

$X$ 上の交代群とは，$X$ 上の偶置換をすべて集めた集合

- $A(X)$, $\mathcal{A}(X)$, $\mathfrak{A}(X)$ と書くことが多い
- $|X| = n$ のときは，$n$ 次の交代群 ($n$ 次交代群) と呼ばれ，$A_n$, $\mathcal{A}_n$, $\mathfrak{A}_n$ と書くことが多い

例：$X = \{1, 2, 3\}$ のとき

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

注：$|A_n| = n!/2$





## 目次

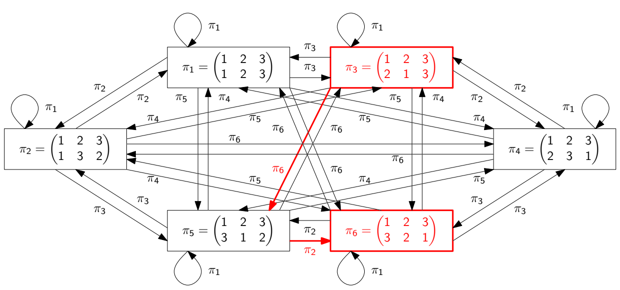






## 対称群の生成 (1)

ケーリー・グラフ (定義は後ほど)



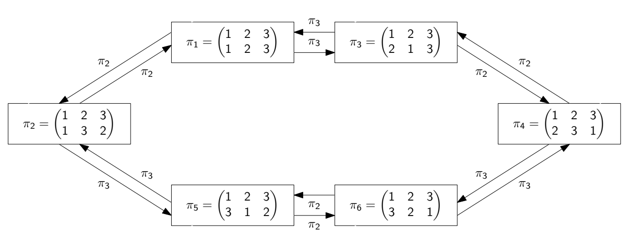
$\pi_3\pi_6\pi_2 = \pi_6$





## 対称群の生成 (2)

ケーリー・グラフ (定義は後ほど)



$\pi_2, \pi_3$ は対称群 $S_3$ を生成する

## 置換群を生成する (1)

**例題 1**

$X = \{1, 2, 3\}$ 上の置換群で，$\pi = (1\ 2\ 3)$ が生成するものを $G$ とすると，$G$ は何？

よって，$G = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$

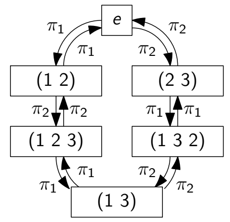




## 置換群を生成する (2)

**例題 2**

$X = \{1, 2, 3\}$ 上の置換群で，
$\pi_1 = (1\ 2)$ と $\pi_2 = (2\ 3)$ が生成するものを $G$ とすると，$G$ は何？




よって，$G = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} = S_3$





## 置換群の生成系

有限集合 $X = \{1, 2, \ldots, n\}$

**置換の集合が生成する置換群とは？**

$X$ 上の置換の集合 $S$ に対して，$S$ が生成する $X$ 上の置換群とは，
$X$ 上の置換群で，$S$ を含むような最小のもの
$\langle S \rangle$ と書く

先ほどの例：$X = \{1, 2, 3\}$ のとき

- $\langle \{(1\ 2\ 3)\} \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$
- $\langle \{(1\ 2), (2\ 3)\} \rangle = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

注：$\langle \{(1\ 2), (2\ 3)\} \rangle$ と書かず，$\langle (1\ 2), (2\ 3) \rangle$ と書くことも多い

**用語**

置換群 $G$ に対して，$G = \langle S \rangle$ であるとき，
$S$ を $G$ の生成系と呼ぶ (ことがある)





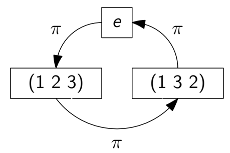
## ケーリー・グラフ

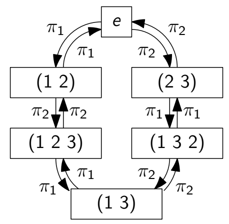
置換群 $G$ とその生成系 $S$

**ケーリー・グラフとは？**

$(G, S)$ のケーリー・グラフとは，次で定義される有向グラフ

- 頂点集合は $G$
- 孤 $(\pi, \pi') \in G \times G$ がある $\Leftrightarrow$ ある $\sigma \in S$ が存在して，$\pi' = \pi\sigma$








## 目次







## 今日の目標

**今日の目標**

置換群に関する基礎的な用語が使えるようになる

- 置換，二行記法，巡回記法，互換
- 偶置換，奇置換
- 置換群，対称群，交代群
- 生成系





## 残った時間の使い方

- 演習問題をやる
  - 相談推奨 (ひとりでやらない)
- 質問をする
  - 教員と TA は巡回
- 退室時，小さな紙に感想など書いて提出する ← 重要
  - 内容は何でも OK
  - 匿名で OK