離散数理工学　第 6 回
離散代数：有限群

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2019 年 11 月 12 日

最終更新：2019 年 11 月 12 日　15:07

スケジュール 前半 (予定)

1. 数え上げの基礎：二項係数と二項定理 (10/1)
2. 数え上げの基礎：漸化式の立て方 (10/8)
3. 数え上げの基礎：漸化式の解き方 (基礎) (10/15)
- ⋆ 休み (祝日) (10/22)
4. 数え上げの基礎：漸化式の解き方 (発展) (10/29)
5. 離散代数：図形とグラフの対称性 (11/5)
6. 離散代数：有限群 (11/12)
7. 離散代数：有限群の構造 (11/19)
8. 離散代数：グラフの対称性と有限群 (11/26)

注意：予定の変更もありうる

スケジュール 後半 (予定)

9 離散確率論：確率的離散システムの解析 (基礎) (12/3)

⋆ 中間試験 (12/10)

10 離散確率論：確率的離散システムの解析 (発展) (12/17)

11 離散確率論：乱択データ構造とアルゴリズム (基礎) (1/7)

12 離散確率論：乱択データ構造とアルゴリズム (発展) (1/14)

13 離散確率論：マルコフ連鎖 (基礎) (1/21)

14 離散確率論：マルコフ連鎖 (発展) (1/28)

⋆ 授業等調整日 (2/4)

⋆ 期末試験 (2/18?)

注意：予定の変更もありうる

今日の目標

群の定義を理解し，群の簡単な性質を証明できる

- 群の定義：単位元，逆元，結合性
- 群の同型性

2 つの群が同型でないことを証明する方法の 1 つを体得する

- 位数を用いる方法

目次

群の例 (1)：整数と加法

整数全体の集合 $\mathbb{Z}$ は加法 $+$ に関して群となり，その群を $(\mathbb{Z}, +)$ と表す

群表 (ケーリー表とも呼ばれる)

$+$	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
$\vdots$											
-4	$\cdots$	-8	-7	-6	-5	-4	-3	-2	-1	0	$\cdots$
-3	$\cdots$	-7	-6	-5	-4	-3	-2	-1	0	1	$\cdots$
-2	$\cdots$	-6	-5	-4	-3	-2	-1	0	1	2	$\cdots$
-1	$\cdots$	-5	-4	-3	-2	-1	0	1	2	3	$\cdots$
0	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
1	$\cdots$	-3	-2	-1	0	1	2	3	4	5	$\cdots$
2	$\cdots$	-2	-1	0	1	2	3	4	5	6	$\cdots$
3	$\cdots$	-1	0	1	2	3	4	5	6	7	$\cdots$
4	$\cdots$	0	1	2	3	4	5	6	7	8	$\cdots$
$\vdots$											

群の構成要素

群は 2 つのものから定義される

- 集合 G
- G 上の演算 $\circ$
  - $x, y \in G$ に対する演算結果が $x \circ y$
  - 演算は他の記号 (例えば，$*$，$\cdot$，$\times$，$+$ など) で表すことも多い
  - $x \circ y$ を単に xy と書くことも多い　← 今後これを用いることが多い

ただし，この G と $\circ$ は次の条件を満たす必要がある

この 2 つを組にして，$(G, \circ)$ と群を表記する
(「$\circ$」を省略して,「G」だけで表記する場合も多い)

群の定義

群とは？

集合 G と G 上の演算 $\circ$ の組 $(G, \circ)$ が群であるとは，次を満たすこと

1. ある要素 $e \in G$ が存在して，任意の $x \in G$ に対して

$$x \circ e = e \circ x = x$$

2. 任意の要素 $x \in G$ に対して，ある要素 $y \in G$ が存在して

$$x \circ y = y \circ x = e$$

3. 演算 $\circ$ は次の結合性を満たす：任意の $x, y, z \in G$ に対して

$$(x \circ y) \circ z = x \circ (y \circ z)$$

群の例 (1)：整数と加法 — 1 つ目の条件

整数全体の集合 $\mathbb{Z}$ は加法 $+$ に関して群となり，その群を $(\mathbb{Z}, +)$ と表す

群表

$+$	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
$\vdots$											
-4	$\cdots$	-8	-7	-6	-5	-4	-3	-2	-1	0	$\cdots$
-3	$\cdots$	-7	-6	-5	-4	-3	-2	-1	0	1	$\cdots$
-2	$\cdots$	-6	-5	-4	-3	-2	-1	0	1	2	$\cdots$
-1	$\cdots$	-5	-4	-3	-2	-1	0	1	2	3	$\cdots$
0	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
1	$\cdots$	-3	-2	-1	0	1	2	3	4	5	$\cdots$
2	$\cdots$	-2	-1	0	1	2	3	4	5	6	$\cdots$
3	$\cdots$	-1	0	1	2	3	4	5	6	7	$\cdots$
4	$\cdots$	0	1	2	3	4	5	6	7	8	$\cdots$
$\vdots$											

群の例 (1)：整数と加法 — 2 つ目の条件

整数全体の集合 $\mathbb{Z}$ は加法 $+$ に関して群となり，その群を $(\mathbb{Z}, +)$ と表す

群表

$+$	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
$\vdots$											
-4	$\cdots$	-8	-7	-6	-5	-4	-3	-2	-1	0	$\cdots$
-3	$\cdots$	-7	-6	-5	-4	-3	-2	-1	0	1	$\cdots$
-2	$\cdots$	-6	-5	-4	-3	-2	-1	0	1	2	$\cdots$
-1	$\cdots$	-5	-4	-3	-2	-1	0	1	2	3	$\cdots$
0	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
1	$\cdots$	-3	-2	-1	0	1	2	3	4	5	$\cdots$
2	$\cdots$	-2	-1	0	1	2	3	4	5	6	$\cdots$
3	$\cdots$	-1	0	1	2	3	4	5	6	7	$\cdots$
4	$\cdots$	0	1	2	3	4	5	6	7	8	$\cdots$
$\vdots$											

群の定義：単位元と逆元

群とは？

集合 G と G 上の演算 $\circ$ の組 $(G, \circ)$ が群であるとは，次を満たすこと

1. ある要素 $e \in G$ が存在して，任意の $x \in G$ に対して

$$x \circ e = e \circ x = x$$

2. 任意の要素 $x \in G$ に対して，ある要素 $y \in G$ が存在して

$$x \circ y = y \circ x = e$$

3. 演算 $\circ$ は次の結合性を満たす：任意の $x, y, z \in G$ に対して

$$(x \circ y) \circ z = x \circ (y \circ z)$$

群の定義：単位元と逆元

群とは？

集合 G と G 上の演算 $\circ$ の組 $(G, \circ)$ が群であるとは，次を満たすこと

1. ある要素 $e \in G$ が存在して，任意の $x \in G$ に対して

$$x \circ e = e \circ x = x$$

この e を G の単位元と呼ぶ

2. 任意の要素 $x \in G$ に対して，ある要素 $y \in G$ が存在して

$$x \circ y = y \circ x = e$$

3. 演算 $\circ$ は次の結合性を満たす：任意の $x, y, z \in G$ に対して

$$(x \circ y) \circ z = x \circ (y \circ z)$$

群の定義：単位元と逆元

群とは？

集合 G と G 上の演算 $\circ$ の組 $(G, \circ)$ が群であるとは，次を満たすこと

1. ある要素 $e \in G$ が存在して，任意の $x \in G$ に対して

$$x \circ e = e \circ x = x$$

この e を G の単位元と呼ぶ

2. 任意の要素 $x \in G$ に対して，ある要素 $y \in G$ が存在して

$$x \circ y = y \circ x = e$$

この y を G における x の逆元と呼び，x^{-1} で表すことが多い

3. 演算 $\circ$ は次の結合性を満たす：任意の $x, y, z \in G$ に対して

$$(x \circ y) \circ z = x \circ (y \circ z)$$

群ではない例

1. 整数全体の集合 $\mathbb{Z}$ は乗法 $\times$ に関して群になる？
   - ならない (なぜ？)
2. 有理数全体の集合 $\mathbb{Q}$ は乗法 $\times$ に関して群になる？
   - ならない (なぜ？)
3. 実数全体の集合 $\mathbb{R}$ は減算 $-$ に関して群になる？
   - ならない (なぜ？)

群の例 (2)

$G = \{x, y, z, w\}$

群表

$\circ$	x	y	z	w
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y
w	w	x	y	z

この表は次の関係を表している

$$
\begin{array}{llll}
x \circ x = x, & x \circ y = y, & x \circ z = z, & x \circ w = w, \\
y \circ x = y, & y \circ y = z, & y \circ z = w, & y \circ w = x, \\
z \circ x = z, & z \circ y = w, & z \circ z = x, & z \circ w = y, \\
w \circ x = w, & w \circ y = x, & w \circ z = y, & w \circ w = z
\end{array}
$$

群の例 (2)

$G = \{x, y, z, w\}$

群表

$\circ$	x	y	z	w
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y
w	w	x	y	z

これが群であるための条件を満たしていることを確認

- 単位元は？
- x の逆元は？ y の逆元は？ z の逆元は？ w の逆元は？
- 結合性は？ (例えば，$(y \circ w) \circ z \stackrel{?}{=} y \circ (w \circ z)$)

群の例 (3)

$G = \{x, y, z, w\}$

群表

$\circ$	x	y	z	w
x	x	y	z	w
y	y	x	w	z
z	z	w	x	y
w	w	z	y	x

この表は次の関係を表している

$$
\begin{array}{llll}
x \circ x = x, & x \circ y = y, & x \circ z = z, & x \circ w = w, \\
y \circ x = y, & y \circ y = x, & y \circ z = w, & y \circ w = z, \\
z \circ x = z, & z \circ y = w, & z \circ z = x, & z \circ w = y, \\
w \circ x = w, & w \circ y = z, & w \circ z = y, & w \circ w = x
\end{array}
$$

群の例 (3)

$G = \{x, y, z, w\}$

群表

$\circ$	x	y	z	w
x	x	y	z	w
y	y	x	w	z
z	z	w	x	y
w	w	z	y	x

これが群であるための条件を満たしていることを確認

- 単位元は？
- x の逆元は？ y の逆元は？ z の逆元は？ w の逆元は？
- 結合性は？ (例えば，$(y \circ w) \circ z \stackrel{?}{=} y \circ (w \circ z)$)

群の例 (4)

$G = \{e, a, b, x, y, z\}$

群表

$\circ$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	x	y	e	z	b
b	b	z	e	y	x	a
x	x	e	z	a	b	y
y	y	b	a	z	e	x
z	z	y	x	b	a	e

この表は次の関係を表している

$$
\begin{array}{llllll}
e \circ e = e, & e \circ a = a, & e \circ b = b, & e \circ x = x, & e \circ y = y, & e \circ z = z, \\
a \circ e = a, & a \circ a = x, & a \circ b = y, & a \circ x = e, & a \circ y = z, & a \circ z = b, \\
b \circ e = b, & b \circ a = z, & b \circ b = e, & b \circ x = y, & b \circ y = x, & b \circ z = a, \\
x \circ e = x, & x \circ a = e, & x \circ b = z, & x \circ x = a, & x \circ y = b, & x \circ z = y, \\
y \circ e = y, & y \circ a = b, & y \circ b = a, & y \circ x = z, & y \circ y = e, & y \circ z = x, \\
z \circ e = z, & z \circ a = y, & z \circ b = x, & z \circ x = b, & z \circ y = a, & z \circ z = e
\end{array}
$$

群の例 (4)

$G = \{e, a, b, x, y, z\}$

群表

$\circ$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	x	y	e	z	b
b	b	z	e	y	x	a
x	x	e	z	a	b	y
y	y	b	a	z	e	x
z	z	y	x	b	a	e

これが群であるための条件を満たしていることを確認

- 単位元は？
- G の各要素の逆元は？
- 結合性は？ (例えば，$(x \circ y) \circ z \stackrel{?}{=} x \circ (y \circ z)$)

注意：$a \circ y \neq y \circ a$ (可換性を満たさない)

アーベル群

アーベル群とは？

群 $(G, \circ)$ がアーベル群であるとは，次の性質を満たすこと

$$\text{任意の } x, y \in G \text{ に対して，} \quad x \circ y = y \circ x$$

この性質を可換性 (交換性) と呼ぶ

- アーベル群は可換群とも呼ばれる
- アーベル群ではない場合，群は非可換群 (非アーベル群) と呼ばれる

有限群と位数

有限群とは？

群 $(G, \circ)$ が有限群であるとは，G の要素数 $|G|$ が有限であること

有限群の位数とは？

有限群 $(G, \circ)$ の位数とは，$|G|$ のこと

今までの例

- 例 (1)：有限群ではない (アーベル群)
- 例 (2)：有限群であり，位数は 4 (アーベル群)
- 例 (3)：有限群であり，位数は 4 (アーベル群)
- 例 (4)：有限群であり，位数は 6 (非可換群)

この講義の焦点は有限群

群の要素の表記法

群 $(G, \circ)$

- $x \circ y$ とは書かずに，xy と書くことが多い
- $x \circ x$ とは書かずに，x^2 と書くことが多い
- $(x \circ y) \circ z$ と $x \circ (y \circ z)$ は同じなので，
  これらを $x \circ y \circ z$ と書き，もっと省略して xyz と書くことが多い
- xxx とは書かずに，x^3 と書くことが多い
- x を n 個並べたものは x^n と書くことが多い
- x の逆元は x^{-1} と書くことが多い
- x^{-1} を n 個並べたものは x^{-n} と書くことが多い
- x^0 は単位元 e を表す

このとき，次の指数法則が成り立つ

観察

任意の $x \in G$ と任意の整数 n, m に対して，$x^n x^m = x^{n+m}$

練習問題

群 G

例題

任意の $x, y \in G$ に対して，$(xy)^{-1} = y^{-1}x^{-1}$

証明：

- 逆元の定義より，$(xy)(xy)^{-1} = e$ (ただし，e は G の単位元)
- この式の両辺に左から x^{-1} をかけると

$$\begin{aligned} x^{-1}(xy)(xy)^{-1} &= x^{-1}e \\ (x^{-1}x)y(xy)^{-1} &= x^{-1} \\ y(xy)^{-1} &= x^{-1} \end{aligned}$$

- 今得られた式の両辺に左から y^{-1} をかけると

$$\begin{aligned} y^{-1}y(xy)^{-1} &= y^{-1}x^{-1} \\ \therefore \quad (xy)^{-1} &= y^{-1}x^{-1} \end{aligned}$$

□

目次

観察したいこと

観察したいこと

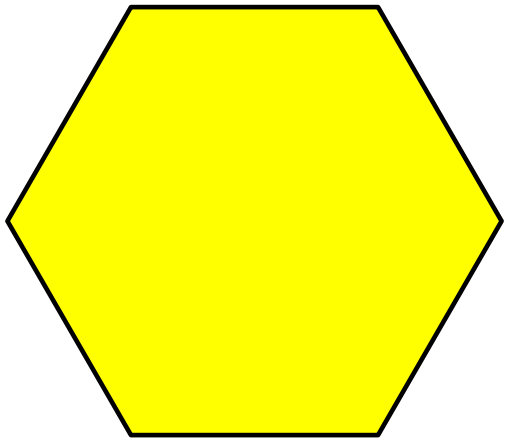
前回,「対称性」として登場した例が群であること

- 正六角形の回転対称性
- 正六角形の回転・鏡映対称性
- 正四面体の回転対称性
- グラフの自己同型性

正六角形の回転対称性：例

問題

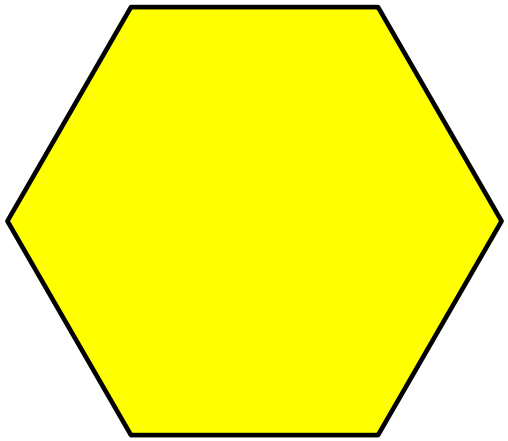
次の図形 (正六角形) を反時計回りに回転させるとき，
回転前と回転後の図形が一致する回転は何か？



正六角形の回転対称性：例

問題

次の図形 (正六角形) を反時計回りに回転させるとき，
回転前と回転後の図形が一致する回転は何か？



前回の解答

反時計回り 60° 回転を r と書くと，正六角形の回転対称性は
集合として $\{1, r, r^2, r^3, r^4, r^5\}$ で表される

これを記号で，$\langle r \mid r^6 = 1 \rangle$ と書く　　(← 群の表示)

正六角形の回転対称性：群表

「変換の合成」を演算と見なすことで，群表が書ける

	1	r	r^2	r^3	r^4	r^5
1	1	r	r^2	r^3	r^4	r^5
r	r	r^2	r^3	r^4	r^5	1
r^2	r^2	r^3	r^4	r^5	1	r
r^3	r^3	r^4	r^5	1	r	r^2
r^4	r^4	r^5	1	r	r^2	r^3
r^5	r^5	1	r	r^2	r^3	r^4

これが群であるための条件を満たしていることを確認

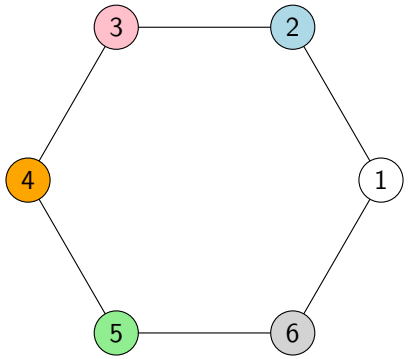
- 単位元は？
- 各要素の逆元は？
- 結合性は？

アーベル群であるか？

正六角形の回転・鏡映対称性：例

問題

正六角形を回転と直線を軸とした鏡映の合成で同じ図形に変換する方法は何通りあるか？(ただし，同じ配置に戻るものは別にして数えない)



前回の解答

正六角形の回転・鏡映対称性は集合として
$\{1, r, r^2, r^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, r^5s\}$ で表される

これを記号で，$\langle r, s \mid r^6 = 1, s^2 = 1, rsrs = 1 \rangle$ と書く　　(← 群の表示)

正六角形の回転・鏡映対称性：群表

変換の合成を演算として，群表が書ける

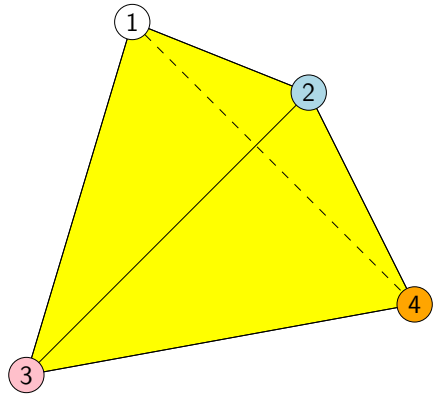
	1	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
1	1	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
r	r	r^2	r^3	r^4	r^5	1	rs	r^2s	r^3s	r^4s	r^5s	s
r^2	r^2	r^3	r^4	r^5	1	r	r^2s	r^3s	r^4s	r^5s	s	rs
r^3	r^3	r^4	r^5	1	r	r^2	r^3s	r^4s	r^5s	s	rs	r^2s
r^4	r^4	r^5	1	r	r^2	r^3	r^4s	r^5s	s	rs	r^2s	r^3s
r^5	r^5	1	r	r^2	r^3	r^4	r^5s	s	rs	r^2s	r^3s	r^4s
s	s	r^5s	r^4s	r^3s	r^2s	rs	1	r^5	r^4	r^3	r^2	r
rs	rs	s	r^5s	r^4s	r^3s	r^2s	r	1	r^5	r^4	r^3	r^2
r^2s	r^2s	rs	s	r^5s	r^4s	r^3s	r^2	r	1	r^5	r^4	r^3
r^3s	r^3s	r^2s	rs	s	r^5s	r^4s	r^3	r^2	r	1	r^5	r^4
r^4s	r^4s	r^3s	r^2s	rs	s	r^5s	r^4	r^3	r^2	r	1	r^5
r^5s	r^5s	r^4s	r^3s	r^2s	rs	s	r^5	r^4	r^3	r^2	r	1

群の定義を満たしていることを確認できる (アーベル群であるか？)

正四面体の回転対称性：例

問題

正四面体を回転で同じ図形に変換する方法は何通りあるか？
(ただし，同じ配置に戻るものは別にして数えない)



前回の解答

正四面体の回転対称性は集合として
$\{1, a, a^2, b, ab, a^2b, ba, aba, a^2ba, ba^2, aba^2, a^2ba^2\}$ で表される

これを記号で，$\langle a, b \mid a^3 = 1, b^2 = 1, ababab = 1 \rangle$ と書く

正四面体の回転対称性：群表

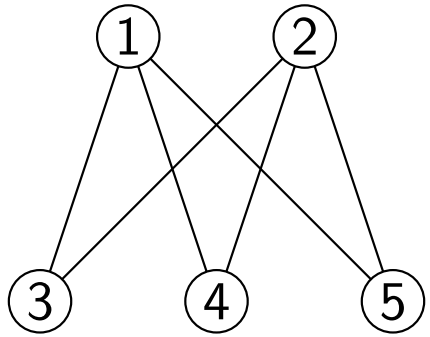
変換の合成を演算として，群表が書ける

	1	a	a^2	b	ab	a^2b	ba	aba	a^2ba	ba^2	aba^2	a^2ba^2
1	1	a	a^2	b	ab	a^2b	ba	aba	a^2ba	ba^2	aba^2	a^2ba^2
a	a	a^2	1	ab	a^2b	b	aba	a^2ba	ba	aba^2	a^2ba^2	ba^2
a^2	a^2	1	a	a^2b	b	ab	a^2ba	ba	aba	a^2ba^2	ba^2	aba^2
b	b	ba	ba^2	1	a^2ba^2	aba	a	a^2b	aba^2	a^2	a^2ba	ab
ab	ab	aba	aba^2	a	ba^2	a^2ba	a^2	b	a^2ba^2	1	ba	a^2b
a^2b	a^2b	a^2ba	a^2ba^2	a^2	aba^2	ba	1	ab	ba^2	a	aba	b
ba	ba	ba^2	b	a^2ba^2	aba	1	a^2b	aba^2	a	a^2ba	ab	a^2
aba	aba	aba^2	ab	ba^2	a^2ba	a	b	a^2ba^2	a^2	ba	a^2b	1
a^2ba	a^2ba	a^2ba^2	a^2b	aba^2	ba	a^2	ab	ba^2	1	aba	b	a
ba^2	ba^2	b	ba	aba	1	a^2ba^2	aba^2	a	a^2b	ab	a^2	a^2ba
aba^2	aba^2	ab	aba	a^2ba	a	ba^2	a^2ba^2	a^2	b	a^2b	1	ba
a^2ba^2	a^2ba^2	a^2b	a^2ba	ba	a^2	aba^2	ba^2	1	ab	b	a	aba

群の定義を満たしていることを確認できる (アーベル群であるか？)

$K_{2,3}$ の自己同型写像

次のグラフには いくつ自己同型写像が あるか？



f をこのグラフの自己同型写像とする

- 各頂点の次数を見ると，f によって，
  $\{1,2\}$ は $\{1,2\}$ に写され，$\{3,4,5\}$ は $\{3,4,5\}$ に写される

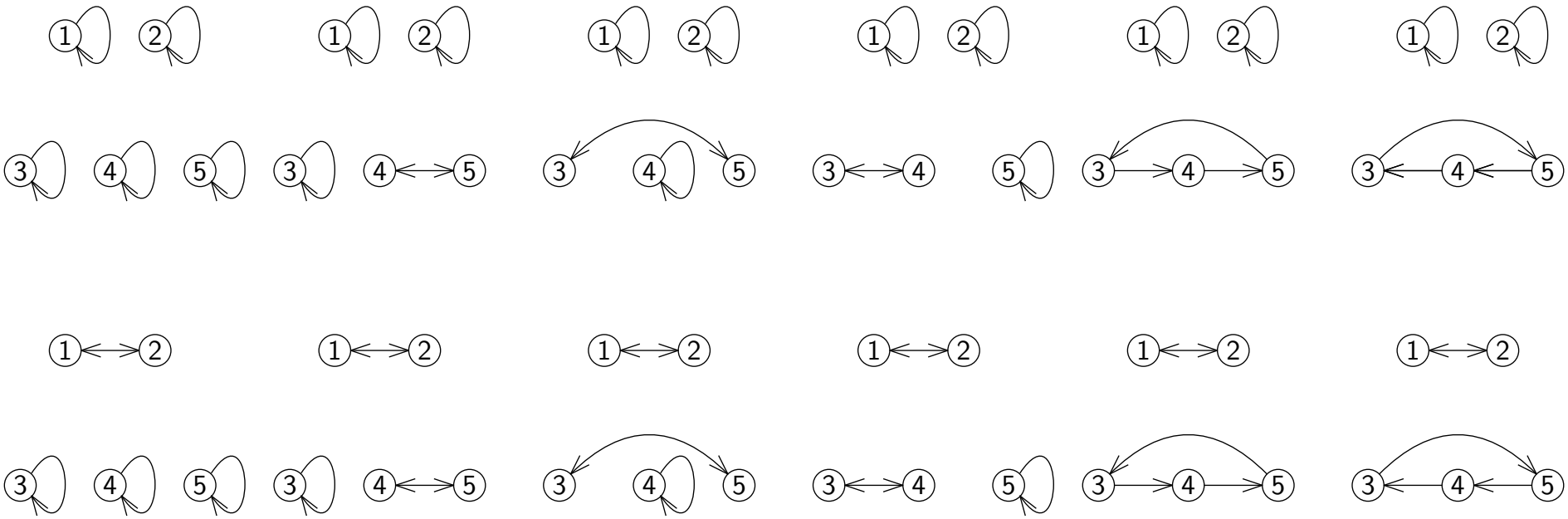
$\therefore$ 自己同型写像の総数 $\leq 2! \cdot 3! = 2 \cdot 6 = 12$

- また，そのように写したものは，すべて自己同型写像である
  (確認せよ)

$\therefore$ 自己同型写像の総数 $= 12$

$K_{2,3}$ の自己同型写像

自己同型写像をすべて描いてみた



$K_{2,3}$ の自己同型写像：群表 (1)

置換の合成はまた置換なので，群表が書ける

	12345	12354	12435	12453	12534	12543
12345	12345	12354	12435	12453	12534	12543
12354	12354	12345	12453	12435	12543	12534
12435	12435	12534	12345	12543	12354	12453
12453	12453	12543	12354	12534	12345	12435
12534	12534	12435	12543	12345	12453	12354
12543	12543	12453	12534	12354	12435	12345
21345	21345	21354	21435	21453	21534	21543
21354	21354	21345	21453	21435	21543	21534
21435	21435	21534	21345	21543	21354	21453
21453	21453	21543	21354	21534	21345	21435
21534	21534	21435	21543	21345	21453	21354
21543	21543	21453	21534	21354	21435	21345

(次ページに続く)

$K_{2,3}$ の自己同型写像：群表 (続)

置換の合成はまた置換なので，群表が書ける

	21345	21354	21435	21453	21534	21543
12345	21345	21354	21435	21453	21534	21543
12354	21354	21345	21453	21435	21543	21534
12435	21435	21534	21345	21543	21354	21453
12453	21453	21543	21354	21534	21345	21435
12534	21534	21435	21543	21345	21453	21354
12543	21543	21453	21534	21354	21435	21345
21345	12345	12354	12435	12453	12534	12543
21354	12354	12345	12453	12435	12543	12534
21435	12435	12534	12345	12543	12354	12453
21453	12453	12543	12354	12534	12345	12435
21534	12534	12435	12543	12345	12453	12354
21543	12543	12453	12534	12354	12435	12345

群の定義を満たしていることを確認できる (アーベル群であるか？)

グラフの自己同型写像全体は群 (1)

無向グラフ $G = (V, E)$，G の自己同型写像全体の集合を $\mathrm{Aut}(G)$ と書く

性質：自己同型写像全体は群

$(\mathrm{Aut}(G), \circ)$ は群　　($\circ$ は写像の合成)

証明：まず，$f, g \in \mathrm{Aut}(G)$ に対して，$f \circ g \in \mathrm{Aut}(G)$ を示す

- f, g が自己同型写像なので，任意の $u, v \in V$ に対して次が成立

$$\{u, v\} \in E \quad \Leftrightarrow \quad \{f(u), f(v)\} \in E \tag{1}$$
$$\{u, v\} \in E \quad \Leftrightarrow \quad \{g(u), g(v)\} \in E \tag{2}$$

- したがって，任意の $u, v \in V$ に対して

$$\{u, v\} \in E \overset{(2)}{\Longleftrightarrow} \{g(u), g(v)\} \in E \overset{(1)}{\Longleftrightarrow} \{f(g(u)), f(g(v))\} \in E$$

- したがって，$f \circ g$ も G の自己同型写像

グラフの自己同型写像全体は群 (2)

無向グラフ $G = (V, E)$，G の自己同型写像全体の集合を $\mathrm{Aut}(G)$ と書く

性質：自己同型写像全体は群

$(\mathrm{Aut}(G), \circ)$ は群　　($\circ$ は写像の合成)

証明 (単位元の存在性)：

- 恒等写像を $\mathrm{id}\colon V \to V$ とすると，id は置換である
- また，id は G の自己同型写像である

$$\because \quad \{u, v\} \in E \quad \Leftrightarrow \quad \{\mathrm{id}(u), \mathrm{id}(v)\} = \{u, v\} \in E$$

- さらに，G の任意の自己同型写像 $f \in \mathrm{Aut}(G)$ に対して，

$$f \circ \mathrm{id} = \mathrm{id} \circ f = f$$

- $\therefore$ id は $(G, \circ)$ の単位元

グラフの自己同型写像全体は群 (3)

無向グラフ $G = (V, E)$，G の自己同型写像全体の集合を $\mathrm{Aut}(G)$ と書く

性質：自己同型写像全体は群

$(\mathrm{Aut}(G), \circ)$ は群　　($\circ$ は写像の合成)

証明 (逆元の存在性)：

- G の自己同型写像 $f \in \mathrm{Aut}(G)$ は全単射なので，逆写像 f^{-1} が存在
- つまり，$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$
- $f^{-1} \colon V \to V$ は G の自己同型写像であることが次のように分かる
  - 任意の $u, v \in V$ を考えると，f は自己同型写像なので，

$$\{f^{-1}(u), f^{-1}(v)\} \in E \Leftrightarrow \{f(f^{-1}(u)), f(f^{-1}(v))\} \in E$$

  - $f \circ f^{-1} = \mathrm{id}$ なので，$\{f^{-1}(u), f^{-1}(v)\} \in E \Leftrightarrow \{u, v\} \in E$
- $\therefore f^{-1}$ は f の逆元

グラフの自己同型写像全体は群 (4)

無向グラフ $G = (V, E)$，G の自己同型写像全体の集合を $\mathrm{Aut}(G)$ と書く

性質：自己同型写像全体は群

$(\mathrm{Aut}(G), \circ)$ は群　　($\circ$ は写像の合成)

証明 (結合性の成立)：

- G の自己同型写像 $f, g, h \in \mathrm{Aut}(G)$ は全単射なので

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

- したがって，$\circ$ は結合性を満たす　□

グラフの自己同型群

無向グラフ G

定義：グラフの自己同型群とは？

無向グラフ G の自己同型群全体の集合を $\mathrm{Aut}(G)$ と書くとき，
群 $(\mathrm{Aut}(G), \circ)$ を G の自己同型群と呼ぶ

グラフの自己同型群については，第 8 回講義でより深く議論する

目次

前回からの疑問

つまり，次の 3 種類の対称性はどれも「12 個の要素」を持つと分かった

- 正六角形の回転・鏡映対称性
- 正四面体の回転対称性
- グラフ $K_{2,3}$ の自己同型

疑問?

この 3 つの「対称性」は本質的に同じものなのか？

$\rightsquigarrow$ いまから，この疑問に答える

群の同型性

「群 G, G' が本質的に同じ」ことを「G, G' が同型である」こととする

定義：群の同型性

群 $(G, \circ)$ と $(G', \circ')$ が同型であるとは，
次を満たす全単射 $f\colon G \to G'$ が存在すること

$$\text{任意の } x, y \in G \text{ に対して，} \quad f(x \circ y) = f(x) \circ' f(y)$$

このような f を $(G, \circ)$ から $(G', \circ')$ への同型写像と呼ぶ

$G = \{x, y, z, w\}$

$\circ$	x	y	z	w
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y
w	w	x	y	z

$G' = \{1, 2, 3, 4\}$

$\circ'$	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

$f(x) = 1, f(y) = 2,$
$f(z) = 3, f(w) = 4$ とすると，
$(G, \circ)$ と $(G', \circ')$ が同型であると分かる

群の同型性

「群 G, G' が本質的に同じ」ことを「G, G' が同型である」こととする

定義：群の同型性

群 $(G, \circ)$ と $(G', \circ')$ が同型であるとは，
次を満たす全単射 $f\colon G \to G'$ が存在すること

$$\text{任意の } x, y \in G \text{ に対して，} \quad f(x \circ y) = f(x) \circ' f(y)$$

このような f を $(G, \circ)$ から $(G', \circ')$ への同型写像と呼ぶ

$G = \{x, y, z, w\}$

$\circ$	x	y	z	w
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y
w	w	x	y	z

$G' = \{1, 2, 3, 4\}$

$\circ'$	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

$f(x) = 1, f(y) = 2,$
$f(z) = 3, f(w) = 4$ と
すると，
$(G, \circ)$ と $(G', \circ')$ が
同型であると
分かる

同型写像の性質：単位元

群 $(G, \circ)$ (単位元は e), 群 $(G', \circ')$，同型写像 $f\colon G \to G'$

性質：同型写像と単位元

$f(e)$ は G' の単位元

証明：任意の要素 $x' \in G'$ を考える

- f は同型写像なので，ある要素 $x \in G$ が存在して，$f(x) = x'$
- このとき，次が成り立つ

$$\begin{aligned} x' \circ' f(e) &= f(x) \circ' f(e) && (x' = f(x)) \\ &= f(x \circ e) && (f \text{ が同型写像}) \\ &= f(x) && (e \text{ が } G \text{ の単位元}) \\ &= x' && (f(x) = x') \end{aligned}$$

- 同様に，$f(e) \circ' x' = f(e) \circ' f(x) = f(e \circ x) = f(x) = x'$
- $\therefore$ $f(e)$ は G' の単位元

□

2 つの群が同型であるか？同型ではないか？

2 つの群が同型であることを証明するには？

同型写像 f を見つければよい

2 つの群が同型ではないことを証明するには？

同型写像 f が存在しないことを言えればよい

問題点

- 候補となる全単射の数は膨大
- 「候補を全部試して，見つかりませんでした」では納得できる証明にならない

つまり，存在しない証拠をうまく示してみたい

要素の位数

群 $(G, \circ)$，単位元 $e \in G$，任意の要素 $x \in G$，

定義：群の要素の位数とは？

x の位数とは，$x^k = e$ となる最小の正整数 k

$G = \{x, y, z, w\}$

$\circ$	x	y	z	w
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y
w	w	x	y	z

- $x^1 = x$ — x の位数は 1
- $y^1 = y$，$y^2 = z$, $y^3 = w$, $y^4 = x$ — y の位数は 4
- $z^1 = z$, $z^2 = x$ — z の位数は 2
- $w^1 = w$, $w^2 = z$, $w^3 = y$，$w^4 = x$ — w の位数は 4

単位元は x

注意：「群の位数」と「群の要素の位数」は異なる概念

同型性と位数 (1)

群 $(G, \circ), (G', \circ')$ と $(G, \circ)$ から $(G', \circ')$ への同型写像 f

性質：同型性と位数

任意の $x \in G$ に対して，

$$G \text{ における } x \text{ の位数} = G' \text{ における } f(x) \text{ の位数}$$

証明：e を $(G, \circ)$ の単位元，e' を G' の単位元とする

- G における x の位数を k とする
- つまり，$x^k = e$，かつ，任意の正整数 $\ell < k$ に対して，$x^\ell \neq e$

証明したいこと

1. $f(x)^k = e'$
2. 任意の正整数 $\ell < k$ に対して，$f(x)^\ell \neq e'$

同型性と位数 (2)

1 の証明：f が同型写像であるから

$$e' = f(e) = f(x^k) = f(x)^k$$

2 の証明：背理法を使ってみる

- ある正整数 $\ell < k$ に対して，$f(x)^\ell = e'$ であると仮定する
- f は同型写像なので，逆写像 f^{-1} が存在し，$f(e) = e'$ を満たす

$$\begin{aligned}
\therefore \quad e &= f^{-1}(f(e)) && (f^{-1} \text{ の定義}) \\
&= f^{-1}(e') && (f(e) = e') \\
&= f^{-1}(f(x)^\ell) && (e' = f(x)^\ell) \\
&= f^{-1}(f(x^\ell)) && (f \text{ は同型写像}) \\
&= x^\ell && (f^{-1} \text{ の定義})
\end{aligned}$$

- これは，$x^\ell \neq e$ に矛盾

証明のまとめ：したがって，G' における $f(x)$ の位数は k □

同型性と位数：帰結 (1)

つまり，次の 3 種類の対称性はどれも「12 個の要素」を持つと分かった

- 正六角形の回転・鏡映対称性
- 正四面体の回転対称性
- グラフ $K_{2,3}$ の自己同型

疑問?

この 3 つの「対称性」は本質的に同じものなのか？

$\rightsquigarrow$ とりあえず，各要素の位数を計算してみる (群表から分かる)

同型性と位数：帰結 (2)

正六角形の
回転・鏡映対称性

要素	位数
1	1
r	6
r^2	3
r^3	2
r^4	3
r^5	6
s	2
rs	2
r^2s	2
r^3s	2
r^4s	2
r^5s	2

正四面体の
回転対称性

要素	位数
1	1
a	3
a^2	3
b	2
ab	3
a^2b	3
ba	3
aba	3
a^2ba	2
ba^2	3
aba^2	2
a^2ba^2	3

$K_{2,3}$ の自己同型性

要素	位数
12345	1
12354	2
12435	2
12453	3
12534	3
12543	2
21345	2
21354	2
21435	2
21453	6
21534	6
21543	2

同型性と位数：帰結 (3)

要素の位数を小さい方から (重複を除かずに) 並べると

正六角形の回転・鏡映対称性	1, 2, 2, 2, 2, 2, 2, 2, 3, 3, 6, 6
正四面体の回転対称性	1, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3
$K_{2,3}$ の自己同型性	1, 2, 2, 2, 2, 2, 2, 2, 3, 3, 6, 6

つまり,

- 正六角形の回転・鏡映対称性を表す群 は
  正四面体の回転対称性を表す群 と同型ではない
- $K_{2,3}$ の自己同型性を表す群 は
  正四面体の回転対称性を表す群 と同型ではない

注意：正六角形の回転・鏡映対称性を表す群 と
$K_{2,3}$ の自己同型性を表す群 が同型かどうか まだ分からない

目次

今日のまとめ

今日の目標

群の定義を理解し，群の簡単な性質を証明できる

- 群の定義：単位元，逆元，結合性
- 群の同型性

2 つの群が同型でないことを証明する方法の 1 つを体得する

- 位数を用いる方法

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

目次