

スケジュール 後半 (予定)

- 8 離散確率論：確率の復習と確率不等式 (12/6)
- ★ 中間試験 (12/13)
- 9 離散確率論：確率的離散システムの解析 (12/20)
- 10 離散確率論：乱択データ構造とアルゴリズム (基礎) (1/10)
- 11 離散確率論：乱択データ構造とアルゴリズム (発展) (1/17)
- 12 離散確率論：マルコフ連鎖 (基礎) (1/24)
- 13 離散確率論：マルコフ連鎖 (発展) (1/31)
- ★ 予備日 (2/7)
- ★ 期末試験 (2/14?)

注意：予定の変更もありうる

群の定義

目次

- 1 群の定義
- 2 置換群再考
- 3 群の表示
- 4 群の同型性と準同型性
- 5 今日のまとめ

群の定義

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 ← 今後これを用いていることが多い

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)

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 (10/4)
- ★ 休講 (体育祭) (10/11)
- 2 数え上げの基礎：漸化式の立て方 (10/18)
- 3 数え上げの基礎：漸化式の解き方 (基礎) (10/25)
- 4 数え上げの基礎：漸化式の解き方 (発展) (11/1)
- ★ 休講 (出張) (11/8)
- 5 離散代数：対称群と置換群 (11/15)
- 6 離散代数：有限群 (11/22)
- 7 離散代数：有限群の応用 (11/29)

注意：予定の変更もありうる

今日の目標

今日の目標

有限群に関する基礎的な用語が使えるようになる

- ▶ 群の定義, 単位元, 逆元
- ▶ 群の表示
- ▶ 群の同型性, 準同型性

群の定義

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)										
		...	-4	-3	-2	-1	0	1	2	3	4	...
+	-8	-7	-6	-5	-4	-3	-2	-1	0	...
:-4	-7	-6	-5	-4	-3	-2	-1	0	1	...
-3	-6	-5	-4	-3	-2	-1	0	1	2	...
-2	-5	-4	-3	-2	-1	0	1	2	3	...
-1	-4	-3	-2	-1	0	1	2	3	4	...
0	-3	-2	-1	0	1	2	3	4	5	...
1	-2	-1	0	1	2	3	4	5	6	...
2	-1	0	1	2	3	4	5	6	7	...
3	0	1	2	3	4	5	6	7	8	...
4	1	2	3	4	5	6	7	8	9	...
:	:

群の定義

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										
+		...	-4	-3	-2	-1	0	1	2	3	4	...
...	-8	-7	-6	-5	-4	-3	-2	-1	0	...
-4	...	-8	-7	-6	-5	-4	-3	-2	-1	0	...	
-3	...	-7	-6	-5	-4	-3	-2	-1	0	1	...	
-2	...	-6	-5	-4	-3	-2	-1	0	1	2	...	
-1	...	-5	-4	-3	-2	-1	0	1	2	3	...	
0	...	-4	-3	-2	-1	0	1	2	3	4	...	
1	...	-3	-2	-1	0	1	2	3	4	5	...	
2	...	-2	-1	0	1	2	3	4	5	6	...	
3	...	-1	0	1	2	3	4	5	6	7	...	
4	...	0	1	2	3	4	5	6	7	8	...	

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

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

群の例 (2)

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

		群表				
○		x	y	z	w	
x	x	x	y	z	w	
y	y	y	z	w	x	
z	z	z	w	x	y	
w	w	w	x	y	z	

この表は次の関係を表している

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

群の例 (3)

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

		群表				
○		x	y	z	w	
x	x	x	y	z	w	
y	y	y	x	w	z	
z	z	z	w	x	y	
w	w	w	z	y	x	

この表は次の関係を表している

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

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										
+		...	-4	-3	-2	-1	0	1	2	3	4	...
...	-8	-7	-6	-5	-4	-3	-2	-1	0	...
-4	...	-8	-7	-6	-5	-4	-3	-2	-1	0	...	
-3	...	-7	-6	-5	-4	-3	-2	-1	0	1	...	
-2	...	-6	-5	-4	-3	-2	-1	0	1	2	...	
-1	...	-5	-4	-3	-2	-1	0	1	2	3	...	
0	...	-4	-3	-2	-1	0	1	2	3	4	...	
1	...	-3	-2	-1	0	1	2	3	4	5	...	
2	...	-2	-1	0	1	2	3	4	5	6	...	
3	...	-1	0	1	2	3	4	5	6	7	...	
4	...	0	1	2	3	4	5	6	7	8	...	

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				
○		x	y	z	w	
x	x	x	y	z	w	
y	y	y	z	w	x	
z	z	z	w	x	y	
w	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				
○		x	y	z	w	
x	x	x	y	z	w	
y	y	y	x	w	z	
z	z	z	w	x	y	
w	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, $(y \circ w) \circ z \stackrel{?}{=} y \circ (w \circ z)$)

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

○	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

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

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

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

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** と呼ばれる

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、 $x^n x^m = x^{n+m}$

- 群の定義
- 置換群再考
- 群の表示
- 群の同型性と準同型性
- 今日のまとめ

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

○	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)

有限群とは？

群 (G, \circ) が **有限群** であるとは、 G の要素数が $|G|$ 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 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

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

□

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

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

置換群は群

観察

置換群は写像の合成に関して群である

用語の対応

群	置換群
単位元	恒等置換
逆元	逆置換

置換群の群表 (2)

交代群 A_3 の群表

○	e	(1 2 3)	(1 3 2)
e	e	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	e
(1 3 2)	(1 3 2)	e	(1 2 3)

群の要素を作る

群 G

- ▶ $a \in G$ のとき, $a^2 \in G, a^3 \in G, a^4 \in G, \dots$
- ▶ $a, b \in G$ のとき, $ab \in G, a^2b \in G, aba \in G, \dots$

このように、要素を並べることで、 G の要素がどんどん作れる

群の表示 : 例 (3) を見て

 $G = \{e, a, b, ab\}$

○	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

別の書き方 (群の表示と呼ばれる):

$$G = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle$$

読み方

- ▶ 「 a, b 」を並べることで G の要素はすべて表現できる
- ▶ 並べたとき、「 $a^2 = b^2 = e, ab = ba$ 」と置き換えてよい
- ▶ 置き換える規則は、これら (から導かれるもの) 以外はない

用語

- ▶ $\{a, b\}$ は G の生成系, 「 $a^2 = b^2 = e, ab = ba$ 」は関係式

置換群の群表 (1)

対称群 S_3 の群表

○	e	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
e	e	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	e	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	e	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	e	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	e
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	e	(1 2 3)

目次

- 1 群の定義
- 2 置換群再考
- 3 群の表示
- 4 群の同型性と準同型性
- 5 今日のまとめ

群の表示 : 例 (3) を見て

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

○	x	y	z	w
x	x	y	z	w
y	y	x	w	z
z	z	w	x	y
w	w	z	y	x

- ▶ $yz = w$ が成り立つ
- ▶ つまり、 y と z があれば、 w は復元できる (w はある意味で不要)
- ▶ x は単位元 (e と書く)
- ▶ y は $y^2 = e$ を満たす
- ▶ z は $z^2 = e$ を満たす
- ▶ y と z は $yz = zy$ を満たす (書き換えると $z^{-1}yzy^{-1} = e$)

群の表示 : 例 (3) を見て

$$G = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle$$

簡約の例

$$\begin{aligned} ab^3a^3b &= abbbaaab \\ &= a(bb)b(aa)ab \\ &= aebeab \\ &= abab \\ &= a(ba)b \\ &= a(ab)b \\ &= aabb \\ &= ee \\ &= e \end{aligned}$$

群の表示：群の例 (2)

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

○	x	y	z	w
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y
w	w	x	y	z

関係式

- ▶ 単位元は x (e と書くことにする)
- ▶ $y^2 = z$, $y^3 = zy = w$ (y があれば, z と w は表現できる)
- ▶ $y^4 = wy = e$

巡回群

(有限) 巡回群とは?

位数 n の巡回群とは, 次の表示を持つ群 ($n \geq 0$ は自然数)

$$C_n = \langle a \mid a^n = e \rangle$$

例 (2) は位数 4 の巡回群

注意

- ▶ $C_n = \{e, a, a^2, a^3, \dots, a^{n-1}\}$
- ▶ すなわち, C_n の位数は n
- ▶ C_n はアーベル群 (演習問題)
 - ▶ ヒント: C_n の任意の要素はある自然数 k を用いて a^k と書ける

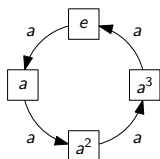
ケーリー・グラフ

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
- ▶ 弧 $(x, y) \in G \times G$ がある \Leftrightarrow ある $z \in S$ が存在して, $y = xz$



群の表示：群の例 (4)

$$G = \{e, a, b, a^2, ab, ba\}$$

○	e	a	b	a ²	ab	ba
e	e	a	b	a ²	ab	ba
a	a	a ²	ab	e	ba	b
b	b	ba	e	ab	a ²	a
a ²	a ²	e	ba	a	b	ab
ab	ab	b	a	ba	e	a ²
ba	ba	ab	a ²	b	a	e

群の表示

$$G = \langle a, b \mid a^3 = b^2 = abab = e \rangle$$

群の表示：群の例 (2)

$$G = \{e, a, a^2, a^3\}$$

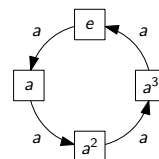
○	e	a	a ²	a ³
e	e	a	a ²	a ³
a	a	a ²	a ³	e
a ²	a ²	a ³	e	a
a ³	a ³	e	a	a ²

群の表示

$$\langle a \mid a^4 = e \rangle$$

ケーリー・グラフ：巡回群

$$C_4 = \langle a \mid a^4 = e \rangle$$



群の表示：群の例 (4)

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

○	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

関係式

- ▶ $a^2 = x$, $ab = y$, $ba = z$ (a, b があれば, x, y, z は表現できる)
- ▶ $a^3 = e$, $b^2 = e$, $abab = e$

群の表示：群の例 (4)

群の表示

$$G = \langle a, b \mid a^3 = b^2 = abab = e \rangle$$

簡約の例

$$\begin{aligned} aba &= ababb \\ &= (abab)b \\ &= eb \\ &= b \end{aligned}$$

$$\begin{aligned} a^2ba^2b &= aabaab \\ &= aabaeab \\ &= aababbab \\ &= a(abab)bab \\ &= aebab \\ &= abab \\ &= e \end{aligned}$$

(有限) 二面体群とは？

位数 $2n$ の二面体群とは、次の表示を持つ群 ($n \geq 0$ は自然数)

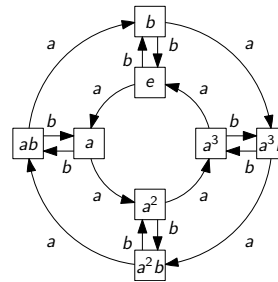
$$D_n = \langle a, b \mid a^n = b^2 = abab = e \rangle$$

例 (4) は位数 6 の二面体群

注意

- ▶ $D_n = \{e, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$
- ▶ すなわち, D_n の位数は $2n$
- ▶ $n \geq 3$ のとき D_n は非可換群 (演習問題)
 - ▶ ヒント: ab と ba を考える

$$D_4 = \langle a, b \mid a^4 = b^2 = abab = e \rangle$$



目次

- 群の定義
- 置換群再考
- 群の表示
- 群の同型性と準同型性
- 今日のまとめ

対称群の表示 (続き)

1 つの表示法

\circ	e	a	b	bab	ba	ab
e	e	a	b	bab	ba	ab
a	a	e	ab	ba	bab	b
b	b	ba	e	ab	a	bab
bab	bab	ab	ba	e	b	a
ba	ba	b	bab	a	ab	e
ab	ab	bab	a	b	e	ba

つまり,

$$\langle a, b \mid a^2 = b^2 = ababab = e \rangle$$

対称群の表示: ここまでのまとめ

3 次の対称群 S_3 に対して, 2 つの表示が得られた

- ▶ $\langle a, b \mid a^2 = b^2 = ababab = e \rangle$
- ▶ $\langle x, y \mid x^2 = y^3 = xyxy = yxyx = xy^2xy^2 = e \rangle$

別の言い方をすると

- ▶ この 2 つの有限群は 3 次の対称群と 同型 である
同型な群は, 本質的に「同じ」である

対称群の表示 (1)

対称群 S_3 の群表

\circ	e	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
e	e	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	e	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	e	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	e	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	e
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	e	(1 2 3)

S_3 の表示は？

対称群の表示 (続き)

別の表示法

\circ	e	x	yx	xy	y	y^2
e	e	x	yx	xy	y	y^2
x	x	e	y^2	y	xy	yx
yx	yx	y	e	y^2	x	xy
xy	xy	y^2	y	e	yx	x
y	y	yx	xy	x	y^2	e
y^2	y^2	xy	x	yx	e	y

つまり,

$$\langle x, y \mid x^2 = y^3 = xyxy = yxyx = xy^2xy^2 = e \rangle$$

群の準同型性と同型性

群 (G, \circ) と群 (H, \star)

群準同型写像とは？

(G, \circ) から (H, \star) への群準同型写像とは,
写像 $\phi: G \rightarrow H$ で, 次を満たすもの

$$\text{任意の } x, y \in G \text{ に対して, } \phi(x \circ y) = \phi(x) \star \phi(y)$$

群同型写像とは？

(G, \circ) から (H, \star) への群同型写像とは,
 (G, \circ) から (H, \star) への群準同型写像で, 全単射であるもの

(G, \circ) から (H, \star) への群同型写像が存在するとき,
 (G, \circ) と (H, \star) は同型であるという

対称群の表示：同型写像 (1)

3 次の対称群 $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ に対して、2 つの表示が得られた

- ▶ $G = \langle a, b \mid a^2 = b^2 = ababab = e \rangle$
- ▶ $H = \langle x, y \mid x^2 = y^3 = xyxy = yxyx = xy^2xy^2 = e \rangle$

写像 $\phi: S_3 \rightarrow G$ として次を考える

$$\begin{aligned} \phi(e) &= e, & \phi((1\ 2)) &= a, & \phi((1\ 3)) &= b, \\ \phi((2\ 3)) &= bab, & \phi((1\ 2\ 3)) &= ba, & \phi((1\ 3\ 2)) &= ab \end{aligned}$$

この ϕ は同型写像である。例えば

$$\phi((1\ 2)(1\ 3)) = \phi((1\ 3\ 2)) = ab = \phi((1\ 2))\phi((1\ 3))$$

対称群の表示：同型写像であることの確認 (1)

$$G = \langle a, b \mid a^2 = b^2 = ababab = e \rangle$$

同型写像であることを確認するためには
関係式を満たすことが確認できればよい

写像 $\phi: S_3 \rightarrow G$ として次を考える

$$\begin{aligned} \phi(e) &= e, & \phi((1\ 2)) &= a, & \phi((1\ 3)) &= b, \\ \phi((2\ 3)) &= bab, & \phi((1\ 2\ 3)) &= ba, & \phi((1\ 3\ 2)) &= ab \end{aligned}$$

このとき、

$$\begin{aligned} a^2 &= \phi((1\ 2))\phi((1\ 2)) = \phi((1\ 2)(1\ 2)) = \phi(e) = e, \\ b^2 &= \phi((1\ 3))\phi((1\ 3)) = \phi((1\ 3)(1\ 3)) = \phi(e) = e, \\ ababab &= \phi((1\ 2))\phi((1\ 3))\phi((1\ 2))\phi((1\ 3))\phi((1\ 2))\phi((1\ 3)) \\ &= \phi((1\ 2)(1\ 3)(1\ 2)(1\ 3)(1\ 2)(1\ 3)) \\ &= \phi((1\ 3\ 2)(1\ 3\ 2)(1\ 3\ 2)) = \phi(e) = e \end{aligned}$$

ゆえに、 ϕ は S_3 から G への群同型写像である

対称群の表示：同型写像 (2)

3 次の対称群 $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ に対して、2 つの表示が得られた

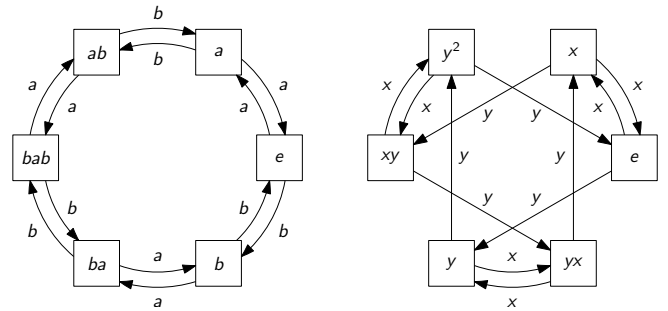
- ▶ $G = \langle a, b \mid a^2 = b^2 = ababab = e \rangle$
- ▶ $H = \langle x, y \mid x^2 = y^3 = xyxy = yxyx = xy^2xy^2 = e \rangle$

写像 $\psi: S_3 \rightarrow H$ として次を考える

$$\begin{aligned} \psi(e) &= e, & \psi((1\ 2)) &= x, & \psi((1\ 3)) &= yx, \\ \psi((2\ 3)) &= xy, & \psi((1\ 2\ 3)) &= y, & \psi((1\ 3\ 2)) &= y^2 \end{aligned}$$

この ψ は同型写像である。(証明は演習問題)

対称群の表示：ケーリー・グラフ



G のケーリー・グラフ

H のケーリー・グラフ

群準同型の性質：単位元

群 (G, \circ) と群 (H, \star) ，群準同型 $\phi: G \rightarrow H$

群準同型の性質 (1)

G の単位元 e_G ， H の単位元 e_H に対して、

$$\phi(e_G) = e_H$$

証明：群準同型の定義より

$$\begin{aligned} \phi(e_G) &= \phi(e_G \circ e_G) = \phi(e_G) \star \phi(e_G) \\ \therefore \phi(e_G) \star \phi(e_G)^{-1} &= \phi(e_G) \star \phi(e_G) \star \phi(e_G)^{-1} \\ \therefore e_H &= \phi(e_G) \end{aligned}$$

□

群準同型の性質：逆元

群 (G, \circ) と群 (H, \star) ，群準同型 $\phi: G \rightarrow H$

群準同型の性質 (2)

任意の $x \in G$ に対して

$$\phi(x^{-1}) = \phi(x)^{-1}$$

証明：演習問題

目次

- 1 群の定義
- 2 置換群再考
- 3 群の表示
- 4 群の同型性と準同型性
- 5 今日のまとめ

今日の目標

今日の目標

有限群に関する基礎的な用語が使えるようになる

- ▶ 群の定義，単位元，逆元
- ▶ 群の表示
- ▶ 群の同型性，準同型性

次回の予告

有限群の応用として，次を扱う

- ▶ 15 パズル
- ▶ タイリング

- ▶ 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