

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 (12/2)
- 9 離散確率論：確率的離散システムの解析 (12/9)
 - * 中間試験 (12/16)
- 10 離散確率論：乱択データ構造とアルゴリズム (基礎) (1/6)
- 11 離散確率論：乱択データ構造とアルゴリズム (発展) (1/13)
- 12 離散確率論：マルコフ連鎖 (基礎) (1/20)
 - * 休講 (海外出張) (1/27)
- 13 離散確率論：マルコフ連鎖 (発展) (2/3)
 - * 期末試験 (2/17?)

注意：予定の変更もありうる

「代数」として思い浮かべるもの

- ▶ モノイド
- ▶ 半群
- ▶ **群**
- ▶ 環
- ▶ 体

- ▶ 半束
- ▶ 束

自然の中の対称性：生物



http://commons.wikimedia.org/wiki/File:Blue_morpho_butterfly.jpg

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 (10/7)
 - * 休講 (体育祭) (10/14)
- 2 数え上げの基礎：漸化式の立て方 (10/21)
- 3 数え上げの基礎：漸化式の解き方 (基礎) (10/28)
- 4 数え上げの基礎：漸化式の解き方 (発展) (11/4)
- 5 **離散代数：群と対称性** (11/11)
- 6 離散代数：部分群と軌道 (11/18)
- 7 離散代数：対称性を考慮した数え上げ (11/25)

注意：予定の変更もありうる

今日の目標

今日の目標

群を用いて物体の対称性を記述できるようになる

- ▶ 群の定義
- ▶ 群の表示
- ▶ 群の作用

自然の中の対称性：雪の結晶



<http://www.its.caltech.edu/~atomic/snowcrystals/>

人工物の対称性：タージ・マハル

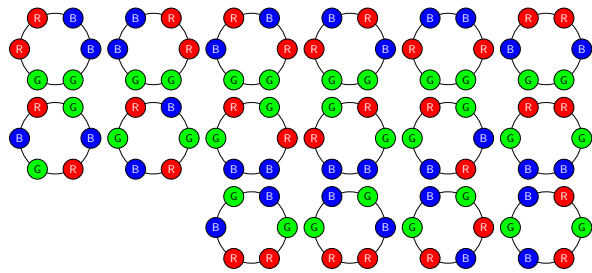


http://en.wikipedia.org/wiki/Taj_Mahal

問題

6個の石を持つネックレスで、その石の色が赤2つ、青2つ、緑2つのものの総数は何か？

ネックレス = 回転して同じものは同じと見なす



16

群の定義

目次

① 群の定義

② 群の表示

③ 群の作用

④ 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)

群の定義

群の例 (1) : 整数と加法 — 1つ目の条件

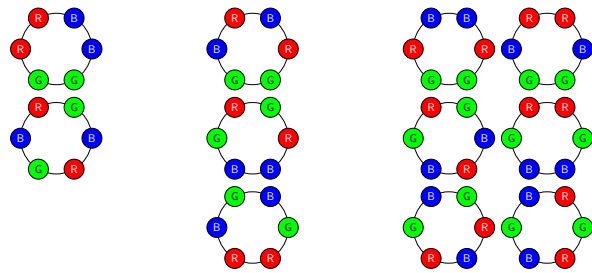
整数全体の集合 \mathbb{Z} は加法 $+$ に関して群となり、その群を $(\mathbb{Z}, +)$ と表す

+	...	-4	-3	-2	-1	0	1	2	3	4	...
...											
-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	...
...											

問題

6個の石を持つブレスレットで、その石の色が赤2つ、青2つ、緑2つのものの総数は何か？

ブレスレット = 回転や鏡映 (裏返し) によって同じものは同じと見なす



11

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

+	...	-4	-3	-2	-1	0	1	2	3	4	...
...											
-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

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

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

群の定義

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

+	...	-4	-3	-2	-1	0	1	2	3	4	...
...											
-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)

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

\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

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

群の例 (3)

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

\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

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

群の例 (4)

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

\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

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

群ではない例

- 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?)
- 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?)
- 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)

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

\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)

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

\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)

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

\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、 $x^n x^m = x^{n+m}$

目次

- 1 群の定義
- 2 群の表示
- 3 群の作用
- 4 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 $z^{-1}zy^{-1} = e$)

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

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

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

□

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) 以外にない

用語

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

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

簡約の例

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

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

○	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

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

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

○	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

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

簡約の例

$$\begin{aligned} aba &= ababb \\ &= (abab)b \\ &= eb \\ &= b \end{aligned} \qquad \begin{aligned} a^2ba^2b &= aabaab \\ &= aabaeb \\ &= aababbab \\ &= a(abab)bab \\ &= aebab \\ &= abab \\ &= e \end{aligned}$$

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

○	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)
- ▶ $y^4 = wy = e$

(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
- ▶ C_n は正 n 角形の回転対称性を表す群 (後述)

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

○	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

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

(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

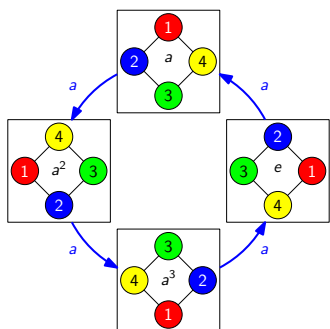
注意

- ▶ $D_n = \{e, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$
- ▶ 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_n は正 n 角形の回転・鏡映対称性を表す群 (後述)

- ① 群の定義
- ② 群の表示
- ③ 群の作用
- ④ 今日のまとめ

正方形の対称性：回転

$C_4 = \langle a \mid a^4 = e \rangle$ が正方形の回転対称性を表す



群の要素の捉え方

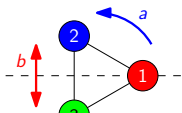
- ▶ 物体の状態
 - ▶ e: 初期状態
 - ▶ a: 90度回転させた状態
 - ▶ a²: 180度回転させた状態
 - ▶ a³: 270度回転させた状態
- ▶ 物体への作用
 - ▶ e: そのままの状態で置く
 - ▶ a: 90度回転させる
 - ▶ a²: 180度回転させる
 - ▶ a³: 270度回転させる

正三角形の対称性：回転と鏡映

$D_3 = \langle a, b \mid a^3 = b^2 = abab = e \rangle$ が正三角形の回転・鏡映対称性を表す

群の要素の捉え方

- ▶ 物体の状態
 - ▶ e: 初期状態
 - ▶ a: 120度回転させた状態
 - ▶ b: x軸に関して鏡映させた状態
 - ▶ ...
- ▶ 物体への作用
 - ▶ e: そのままの状態で置く
 - ▶ a: 120度回転させる
 - ▶ b: x軸に関して鏡映させる
 - ▶ ...

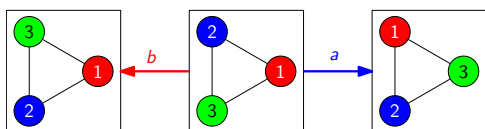


作用することの確認法 (証明法)

- ① 生成系の各要素 (生成元) が定める操作を定義する
- ② 考える物体がその操作により不変であることを確認する
- ③ 各関係式が操作に対しても成り立つことを確認する

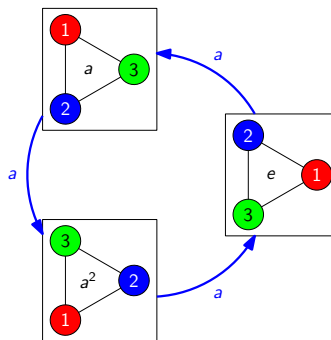
例: $D_3 = \langle a, b \mid a^3 = b^2 = abab = e \rangle$ は正三角形に作用する

- ▶ 原点が正三角形の中心で, x軸の正側に1頂点が置かれるとする
- ▶ aを原点中心反時計回りに120度回転する操作に対応させる
- ▶ bをx軸に関して鏡映する操作に対応させる
- ▶ これら2つの操作により, 正三角形は正三角形にうつる



正三角形の対称性：回転

$C_3 = \langle a \mid a^3 = e \rangle$ が正三角形の回転対称性を表す

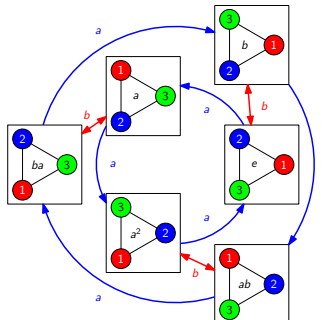


群の要素の捉え方

- ▶ 物体の状態
 - ▶ e: 初期状態
 - ▶ a: 120度回転させた状態
 - ▶ a²: 240度回転させた状態
- ▶ 物体への作用
 - ▶ e: そのままの状態で置く
 - ▶ a: 120度回転させる
 - ▶ a²: 240度回転させる

正三角形の対称性：回転と鏡映

$D_3 = \langle a, b \mid a^3 = b^2 = abab = e \rangle$ が正三角形の回転・鏡映対称性を表す



群の要素の捉え方

- ▶ 物体の状態
 - ▶ e: 初期状態
 - ▶ a: 120度回転させた状態
 - ▶ b: x軸に関して鏡映させた状態
 - ▶ ...
- ▶ 物体への作用
 - ▶ e: そのままの状態で置く
 - ▶ a: 120度回転させる
 - ▶ b: x軸に関して鏡映させる
 - ▶ ...

群の作用：より一般的に書くと...

群 G , 物体 X

- ▶ G の各要素 $g \in G$ を X が住む空間における変換であると見なす
- ▶ $g.x =$ その空間の点 x が g に対応する変換によって動いた先の点

群の作用とは? (直感的な定義)

G が X に作用するとは, 次を満たすこと

- ▶ 任意の $g \in G$ と任意の $x \in X$ に対して, $g.x \in X$
- ▶ 任意の $g, h \in G$ と任意の $x \in X$ に対して, $h.(g.x) = (hg).x$
- ▶ 任意の $x \in X$ に対して, $e.x = x$

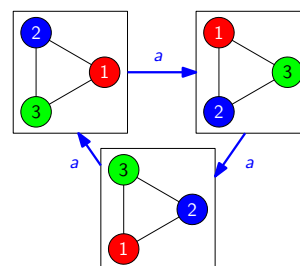
例:

- ▶ C_3 は正三角形に作用する, D_3 は正三角形に作用する
- ▶ C_4 は正方形に作用する, D_4 は正方形に作用する

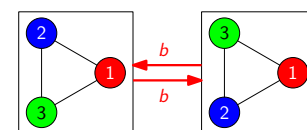
注意 (演習問題): 任意の $g \in G$ に対して, $x \mapsto g.x$ は X 上の全単射

作用することの確認法 (証明法): 続き

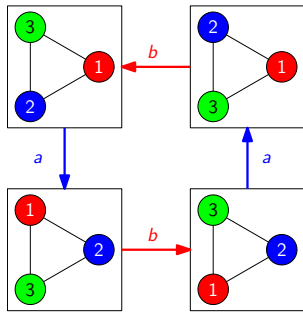
$a^3 = e$ が成り立つことの確認



$b^2 = e$ が成り立つことの確認



$abab = e$ が成り立つことの確認



以上の議論より, D_3 が正三角形に作用することが分かった

- ① 群の定義
- ② 群の表示
- ③ 群の作用
- ④ 今日のまとめ

今日の目標と次回の予告

今日の目標

群を用いて物体の対称性を記述できるようになる

- ▶ 群の定義
- ▶ 群の表示
- ▶ 群の作用

次回の予告

対称性を用いた数え上げを行うための道具の準備

- ▶ 部分群, 剰余群
- ▶ 軌道, 固定部分群