

- 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

スケジュール 後半 (予定)

今日の目標

- 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

今日の目標

群の構造，特に部分群を深く理解する

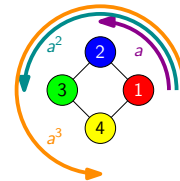
- ▶ 部分群，剰余類
- ▶ ラグランジュの定理
- ▶ 軌道，固定部分群

「対称性を考慮した数え上げ」に対する準備

群の作用：補足

目次

- 1 群の作用：補足
- 2 部分群とラグランジュの定理
- 3 剰余類とラグランジュの定理の証明
- 4 軌道と固定部分群
- 5 今日のまとめ



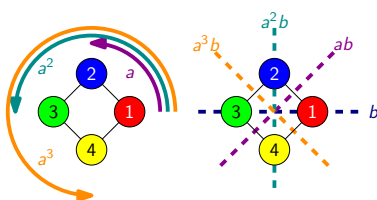
巡回群 C_n の各要素は正 n 角形の回転を表す

$C_n = \{e, a, a^2, \dots, a^{n-1}\}$ であり，
▶ a^k は $360^\circ k/n$ 回転を表す

群の作用：補足

二面体群による作用

二面体群 D_n の各要素は正 n 角形の回転・鏡映を表す

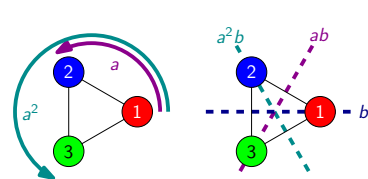


$D_n = \{e, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$ であり，
▶ a^k は $360^\circ k/n$ 回転を表す
▶ $a^k b$ は傾き $180^\circ k/n$ の直線に関する鏡映を表す

群の作用：補足

二面体群による作用 (2)

二面体群 D_n の各要素は正 n 角形の回転・鏡映を表す



$D_n = \{e, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$ であり，
▶ a^k は $360^\circ k/n$ 回転を表す
▶ $a^k b$ は傾き $180^\circ k/n$ の直線に関する鏡映を表す

- ① 群の作用：補足
- ② 部分群とラグランジュの定理
- ③ 剰余類とラグランジュの定理の証明
- ④ 軌道と固定部分群
- ⑤ 今日のまとめ

部分群：例

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

群表	○	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

次のそれぞれは部分群か？

- 1 $H_1 = \{e, a, a^2\}$
- 2 $H_2 = \{e, a\}$
- 3 $H_3 = \{e, a^2\}$
- 4 $H_4 = \{e\}$

部分群：例

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

群表	○	e	a
	e	e	a
	a	a	a^2

- 2 $H_2 = \{e, a\}$

▶ $a \circ a = a^2 \notin H_2$ なので、 H_2 は G の部分群ではない
(これだけが理由である、というわけではない)

部分群：例

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

群表	○	e
	e	e

- 4 $H_4 = \{e\}$

(自明な部分群とも呼ばれる)

H_4 は G の部分群

部分群

群 (G, \circ) , $H \subseteq G$

部分群とは？

(H, \circ) が群であるとき、 H を G の部分群と呼ぶ

注意： (G, \circ) と (H, \circ) における演算は同一

部分群とは？: 定義の言い換え

H が G の部分群であるとは、

- ▶ $x, y \in H \Rightarrow x \circ y \in H$ (演算の保存)
- ▶ G の単位元 e に対して、 $e \in H$ (単位元の保存)
- ▶ $x \in H \Rightarrow G$ における x の逆元 x^{-1} に対して $x^{-1} \in H$ (逆元の保存)

部分群：例

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

群表	○	e	a	a^2
	e	e	a	a^2
	a	a	a^2	a^3
	a^2	a^2	a	e

- 1 $H_1 = \{e, a, a^2\}$

▶ $a \circ a^2 = a^3 \notin H_1$ なので、 H_1 は G の部分群ではない
(これだけが理由である、というわけではない)

部分群：例

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

群表	○	e	a^2
	e	e	a^2
	a^2	a^2	e

- 3 $H_3 = \{e, a^2\}$

- ▶ $e \in H$
- ▶ $e \circ e = a^2 \circ a^2 = e \in H$
- ▶ $e \circ a^2 = a^2 \circ e = a^2 \in H$
- ▶ G における e の逆元は e で、 $e \in H$
- ▶ G における a^2 の逆元は a^2 で、 $a^2 \in H$

したがって、 H_3 は G の部分群

部分群であるための必要十分条件

群 (G, \circ) , 部分集合 $H \subseteq G$, $H \neq \emptyset$

部分群であるための必要十分条件

H が G の部分群である \Leftrightarrow 任意の $a, b \in H$ に対して、 $a^{-1}b \in H$

\Rightarrow の証明： H が G の部分群であると仮定する

- ▶ 任意の $a, b \in H$ を考える
- ▶ H は G の部分群なので、 $a^{-1} \in H$
- ▶ H は G の部分群で、 $a^{-1}, b \in H$ なので、 $a^{-1}b \in H$ □

群 (G, \circ) , 部分集合 $H \subseteq G, H \neq \emptyset$

部分群であるための必要十分条件

H が G の部分群である \Leftrightarrow 任意の $a, b \in H$ に対して, $a^{-1}b \in H$

\Leftarrow の証明: 任意の $a, b \in H$ に対して $a^{-1}b \in H$ であると仮定する

▶ このとき, 「演算の保存」, 「単位元の保存」, 「逆元の保存」を確認する

単位元の保存

▶ $H \neq \emptyset$ なので, ある $x \in G$ が存在して $x \in H$

▶ 仮定において $a = b = x$ とすると, $x^{-1}x \in H$ が得られる

▶ 逆元の定義より, $x^{-1}x = e$ なので, $e \in H$ □

ラグランジュの定理

G : 有限群 H : G の部分群 $\Rightarrow |H|$ は $|G|$ の約数 ($|G|/|H|$ は整数)

証明は次の節で

- ① 群の作用: 補足
- ② 部分群とラグランジュの定理
- ③ 剰余類とラグランジュの定理の証明
- ④ 軌道と固定部分群
- ⑤ 今日のまとめ

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

\circ	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

部分群 $H = \{e, a^2\}$

- ▶ $eH = \{ee, ea^2\} = \{e, a^2\}$
- ▶ $aH = \{ae, aa^2\} = \{a, a^3\}$
- ▶ $a^2H = \{a^2e, a^2a^2\} = \{a^2, e\} = \{e, a^2\}$
- ▶ $a^3H = \{a^3e, a^3a^2\} = \{a^3, a\} = \{a, a^3\}$

観察: $eH = a^2H, aH = a^3H, eH \cap aH = \emptyset$

群 (G, \circ) , 部分集合 $H \subseteq G, H \neq \emptyset$

部分群であるための必要十分条件

H が G の部分群である \Leftrightarrow 任意の $a, b \in H$ に対して, $a^{-1}b \in H$

\Leftarrow の証明 (続):

逆元の保存: $x \in H$ とする

▶ 仮定において $a = x, b = e$ とすると, $x^{-1}e \in H$ が得られる

▶ 単位元の定義より, $x^{-1}e = x^{-1}$ なので, $x^{-1} \in H$ □

演算の保存: $x, y \in H$ とする

▶ 仮定において, $a = x^{-1}, b = y$ とすると, $(x^{-1})^{-1}y \in H$ が得られる

▶ 演習問題 5.11 より, $(x^{-1})^{-1} = x$ なので, $xy \in H$ となる □

これで 3 つの性質の成立が確かめられた □

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

\circ	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

次のそれぞれは部分群か?

- 1 $H_1 = \{e, a, a^2\}$ ← ラグランジュの定理に反するので, 部分群ではない
- 2 $H_2 = \{e, a\}$
- 3 $H_3 = \{e, a^2\}$
- 4 $H_4 = \{e\}$

$|G| = 4$ なので, ラグランジュの定理より

H が G の部分群ならば, $|H| \in \{1, 2, 4\}$

群 G , 部分群 $H \subseteq G$, 要素 $g \in G$

H の (左) 剰余類とは?

g に関する H の (左) 剰余類とは,

$$gH = \{gh \mid h \in H\}$$

群 G , 部分群 $H \subseteq G$

G 上の二項関係 \sim を次で定義

任意の $a, b \in G$ に対して

$$a \sim b \Leftrightarrow aH = bH$$

先ほどの例: $e \sim a^2, a \sim a^3$

命題 1

上で定義した \sim は G 上の同値関係, つまり, 次の 3 つを満たす

- ▶ 任意の $a \in G$ に対して, $aH = aH$ (反射性)
- ▶ 任意の $a, b \in G$ に対して, $aH = bH$ ならば $bH = aH$ (対称性)
- ▶ 任意の $a, b, c \in G$ に対して, $aH = bH$ かつ $bH = cH$ ならば $aH = cH$ (推移性)

これが成り立つことはすぐ分かる

剰余類と同値分割

群 G , 部分群 $H \subseteq G$

G 上の二項関係 \sim を次で定義

任意の $a, b \in G$ に対して

$$a \sim b \iff aH = bH$$

これは G 上の同値関係なので, G の同値分割を与える

つまり,

$G / \sim = \{gH \mid g \in G\}$ は G の分割

この同値分割を G/H と書く (注: $\frac{G}{H}$ とは書かない)

先ほどの例: $G = \{e, a, a^2, a^3\}, H = \{e, a^2\}$

$eH = a^2H = \{e, a^2\}, aH = a^3H = \{a, a^3\}$ なので,

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

剰余類の要素数: 証明

有限群 G , 部分群 $H \subseteq G$

命題 2 (剰余類の要素数)

任意の $a, b \in G$ に対して, $|aH| = |bH|$

証明: aH から bH への全単射が存在することを示せばよい

復習: 関数 $f: aH \rightarrow bH$ が全単射であるとは

- ▶ 任意の $y \in bH$ に対して, ある $x \in aH$ が存在して, $f(x) = y$ (全射性)
- ▶ 任意の $x, x' \in aH$ に対して, $f(x) = f(x')$ ならば $x = x'$ (単射性)

f の構成: 任意の $x \in aH$ に対して, $f(x) = ba^{-1}x$ とする

剰余類の要素数: 証明 (続 2)

単射性の証明

- ▶ $x, x' \in aH$ とし, $f(x) = f(x')$ であると仮定する
- ▶ すなわち, ある $h, h' \in H$ に対して, $x = ah, x' = ah'$
- ▶ このとき, $f(x) = ba^{-1}x = ba^{-1}ah = bh$
- ▶ 同様に, $f(x') = ba^{-1}x' = ba^{-1}ah' = bh'$
- ▶ 仮定より, $bh = bh'$
- ▶ この両辺に左から b^{-1} をかけると, $h = h'$
- ▶ この両辺に左から a をかけると, $ah = ah'$
- ▶ したがって, $x = x'$
- ▶ つまり, f は単射である □

以上より, f は全単射であり, $|aH| = |bH|$ となる □

ラグランジュの定理: 補足

ラグランジュの定理

G : 有限群
 H : G の部分群 $\Rightarrow |H|$ は $|G|$ の約数 ($|G|/|H|$ は整数)

記法: 剰余類による分割

$$G/H = \{gH \mid g \in G\}$$

先ほどの証明から得られる帰結

$$|G/H| = |G|/|H|$$

剰余類の要素数

有限群 G , 部分群 $H \subseteq G$

命題 2 (剰余類の要素数)

任意の $a, b \in G$ に対して, $|aH| = |bH|$

先ほどの例: $G = \{e, a, a^2, a^3\}, H = \{e, a^2\}$

- ▶ $eH = a^2H = \{e, a^2\}$: 要素数 2
- ▶ $aH = a^3H = \{a, a^3\}$: 要素数 2

証明の方針: aH から bH への全単射が存在することを示せばよい

剰余類の要素数: 証明 (続 1)

全射性の証明

- ▶ 任意の $y \in bH$ を考える
- ▶ すなわち, ある $h \in H$ が存在して, $y = bh$
- ▶ $x = ab^{-1}y$ とすると, $x = ab^{-1}bh = ah$ なので, $x \in aH$
- ▶ また,

$$\begin{aligned} f(x) &= ba^{-1}x && (f \text{ の定義}) \\ &= ba^{-1}ab^{-1}y && (x = ab^{-1}y \text{ より}) \\ &= bb^{-1}y && (a^{-1}a = e \text{ より}) \\ &= y && (bb^{-1} = e \text{ より}) \end{aligned}$$

- ▶ したがって, f は全射である □

定義の復習: $bH = \{bh \mid h \in H\}$

ラグランジュの定理: 証明

ラグランジュの定理

G : 有限群
 H : G の部分群 $\Rightarrow |H|$ は $|G|$ の約数 ($|G|/|H|$ は整数)

証明: 命題 1 より, G は H の剰余類によって分割できる

- ▶ すなわち, ある $a_1, \dots, a_{r-1} \in G$ が存在して

$$G = H \cup a_1H \cup \dots \cup a_{r-1}H$$

と G を分割できる

- ▶ したがって, $|G| = |H| + |a_1H| + \dots + |a_{r-1}H|$
- ▶ 命題 2 より, $|H| = |a_1H| = \dots = |a_{r-1}H|$
- ▶ すなわち, $|G| = r|H|$ であり, $|G|/|H|$ は自然数 r □

目次

- ① 群の作用: 補足
- ② 部分群とラグランジュの定理
- ③ 剰余類とラグランジュの定理の証明
- ④ 軌道と固定部分群
- ⑤ 今日のまとめ

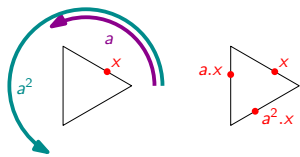
群の作用と軌道

群 G が集合 X に作用

軌道とは？

要素 $x \in X$ の軌道とは,

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

例：正三角形に作用する C_3 (回転)

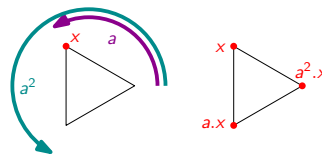
群の作用と軌道

群 G が集合 X に作用

軌道とは？

要素 $x \in X$ の軌道とは,

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

例：正三角形に作用する C_3 (回転)

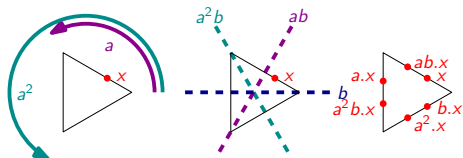
群の作用と軌道

群 G が集合 X に作用

軌道とは？

要素 $x \in X$ の軌道とは,

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

例：正三角形に作用する D_3 (回転・鏡映)

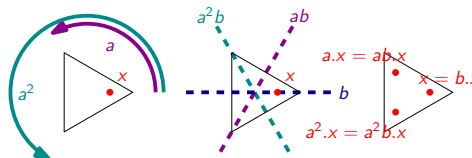
群の作用と軌道

群 G が集合 X に作用

軌道とは？

要素 $x \in X$ の軌道とは,

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

例：正三角形に作用する D_3 (回転・鏡映)

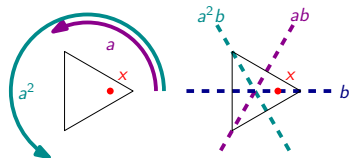
固定部分群

群 G が集合 X に作用

固定部分群とは？

要素 $x \in X$ の固定部分群 (または, 安定化群) とは,

$$\text{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$$

例：正三角形に作用する D_3 (回転・鏡映)

$$\text{Stab}_G(x) = \{e, b\}$$

固定部分群は部分群

群 G が集合 X に作用

補題

任意の $x \in X$ に対して, 固定部分群 $\text{Stab}_G(x)$ は G の部分群証明：任意の $a, b \in \text{Stab}_G(x)$ に対して, $a^{-1}b \in \text{Stab}_G(x)$ となることを示す (すなわち, $(a^{-1}b) \cdot x = x$ となることを示す)

- ▶ $a, b \in \text{Stab}_G(x)$ とする
- ▶ すなわち, $a \cdot x = x$ かつ $b \cdot x = x$
- ▶ 作用の定義より, $a^{-1} \cdot x = a^{-1} \cdot (a \cdot x) \stackrel{*}{=} (a^{-1}a) \cdot x = e \cdot x \stackrel{*}{=} x$
(* の等号で, 作用の定義を用いた)
- ▶ このとき, 作用の定義より, $(a^{-1}b) \cdot x \stackrel{*}{=} a^{-1} \cdot (b \cdot x) = a^{-1} \cdot x = x$
- ▶ したがって, $a^{-1}b \in \text{Stab}_G(x)$ □

軌道固定部分群定理

群 G が集合 X に作用

軌道固定部分群定理 (群作用の基本定理とも呼ばれる)

任意の $x \in X$ に対して, $|G/\text{Stab}_G(x)| = |G \cdot x|$ ラグランジュの定理より, $|G|/|\text{Stab}_G(x)| = |G/\text{Stab}_G(x)|$ なので,

$$|G|/|\text{Stab}_G(x)| = |G \cdot x|$$

となり, すなわち, 任意の $x \in X$ に対して

$$|G| = |G \cdot x| |\text{Stab}_G(x)|$$

- ▶ 次回：証明
- ▶ 今回：とりあえず使い方の一例をしてみる

軌道固定部分群定理：使い方 (1)

例題 1

正 n 角形の回転対称性を表す群の位数は何か？解答例：考える群を G とし, 正 n 角形の 1 頂点を x とする

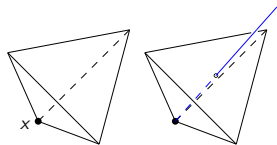
- ▶ このとき, $|G \cdot x| = n$
- ▶ また, $\text{Stab}_G(x) = \{e\}$ であるので, $|\text{Stab}_G(x)| = 1$
- ▶ したがって, $|G| = |G \cdot x| |\text{Stab}_G(x)| = n$ □

例題 2

正四面体の回転対称性を表す群の位数は何か？

解答例：考える群を G とし、正四面体の 1 頂点を x とする

- ▶ G の作用により、 x は正四面体の任意の頂点にうつるので、
 $|G \cdot x| = 4$
- ▶ x を固定する G の作用は、 x とその対面の中心を結ぶ直線の周りの回転のみなので、それは巡回群 C_3 の作用と同一視でき、
 $|\text{Stab}_G(x)| = |C_3| = 3$
- ▶ したがって、 $|G| = |G \cdot x| |\text{Stab}_G(x)| = 4 \cdot 3 = 12$ □



- ① 群の作用：補足
- ② 部分群とラグランジュの定理
- ③ 剰余類とラグランジュの定理の証明
- ④ 軌道と固定部分群
- ⑤ 今日のまとめ

今日の目標と次回の予告

今日の目標

群の構造，特に部分群を深く理解する

- ▶ 部分群，剰余類
- ▶ ラグランジュの定理
- ▶ 軌道，固定部分群

次回の予告

次の 2 つの定理の証明

- ▶ 軌道固定部分群定理
- ▶ コーシー・フロベニウスの定理 (バーンサイドの補題)

$$|\{G \cdot x \mid x \in X\}| = \frac{1}{|G|} \sum_{x \in X} |\text{Stab}_G(x)| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}_X(g)|$$

これを用いて「対称性を考慮した数え上げ」を行う