ぐん

群の作用と整数と暗号

縫田　光司（ぬいだ　こうじ）
九州大学 マス・フォア・インダストリ研究所

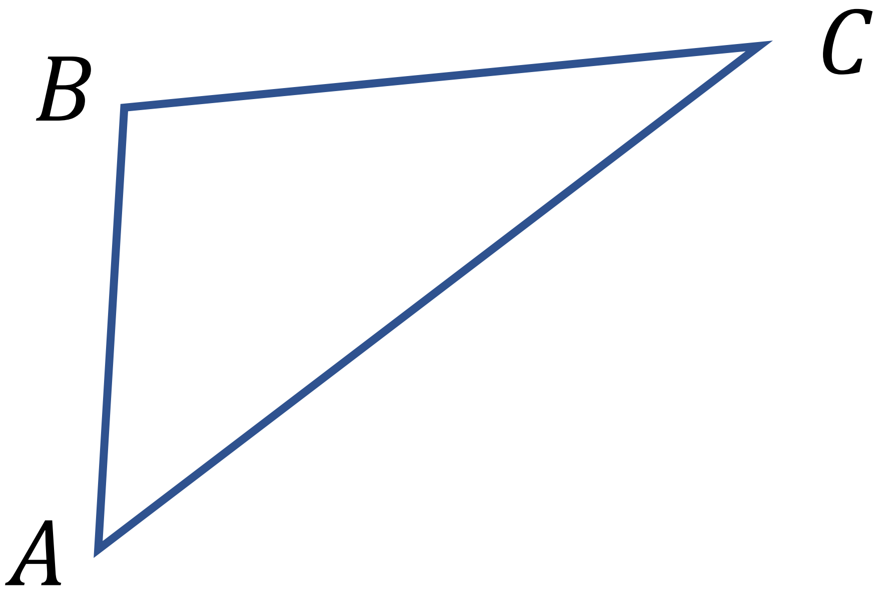
JST数学キャラバン
2023年12月16日　＠中部大学

目次

目次

（例１）

平面の点 A, B の距離を $d(A, B)$ と書くと、

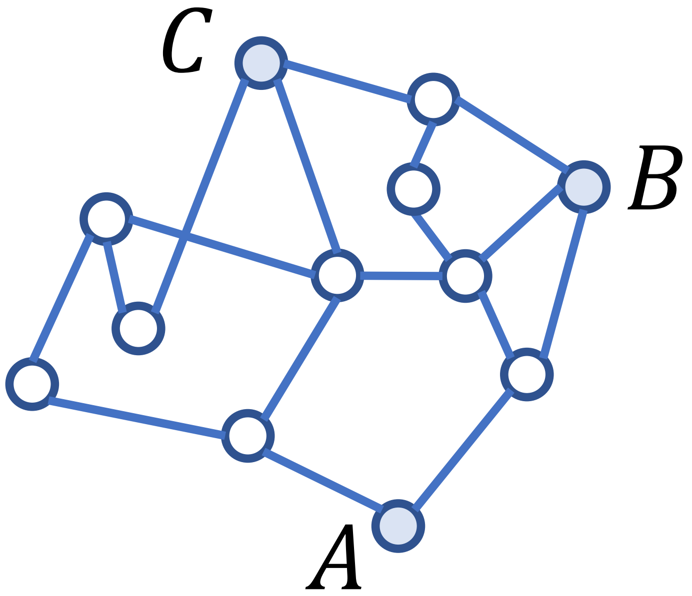


$$\boxed{d(B, A) = d(A, B)}$$

$$\boxed{d(A, C) \leqq d(A, B) + d(B, C)}$$

（例２）

$A \rightarrow B$ で通る線の数の最小値を $d(A,B)$ と書くと、



$$\boxed{d(B,A) = d(A,B)}$$

$$\boxed{d(A,C) \leqq d(A,B) + d(B,C)}$$

（例３）
「１文字書く」「１文字消す」を最小何回で単語 A から B にできるか、を $d(A,B)$ と書くと、

A：すうがく
B：がいこく
C：たいいく

$$\boxed{d(B,A) = d(A,B)}$$

$$\boxed{d(A,C) \leqq d(A,B) + d(B,C)}$$

（例では $d(A,B) = 4,\ d(B,C) = 4,\ d(A,C) = 6$）

	例１ (平面)	例２ (点と線)	例３ (単語)
図形的？	○	○	×
「二つの物のちょうど中間の物」がある？	○	×	×

どの例の「距離」も $|d(A,C)-d(B,C)| \leqq d(A,B)$ を満たすことを、**同じようにして**証明できる

定義は？

	例１ （平面）	例２ （点と線）	例３ （単語）
図形的？	○	○	×
「二つの物のちょうど中間の物」がある？	○	×	×

性質 $\boldsymbol{d(B,A) = d(A,B)}$ と $\boldsymbol{d(A,C) \leqq d(A,B) + d(B,C)}$ **だけ**を使って

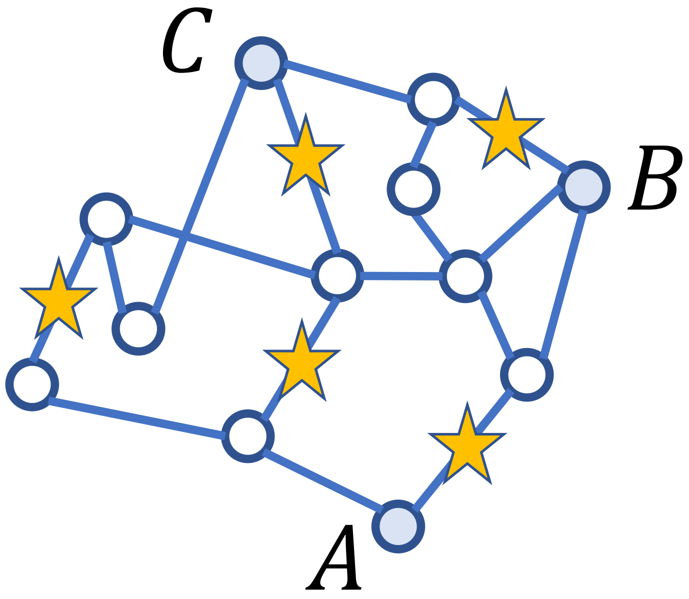
$|d(A,C) - d(B,C)| \leqq d(A,B)$ を

証明できる

本質的な理由
（他の性質は
無関係）

（おまけ：これまでと「似ていない」例）

例２で「☆の線は１本までしか通れない」とすると、

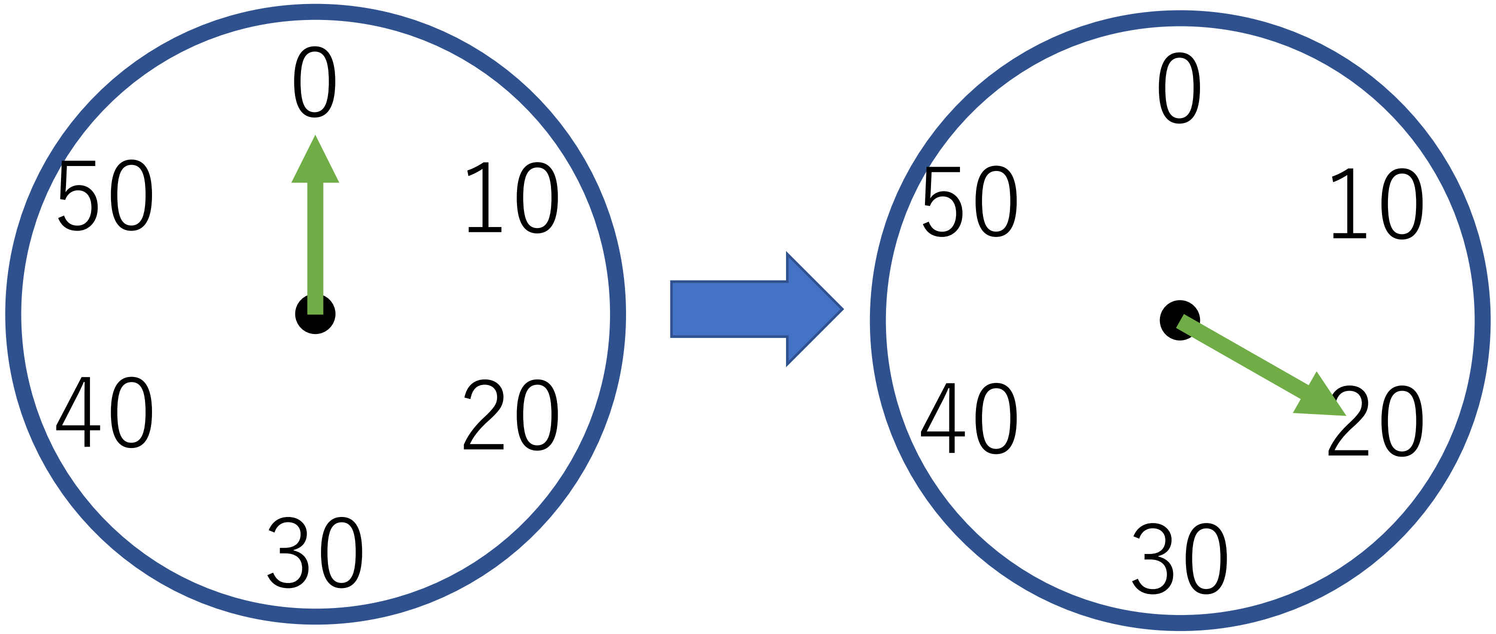


$$d(A,B)=2, d(B,C)=2, d(A,C)=5$$

$$\xcancel{\boxed{d(A,C) \leqq d(A,B)+d(B,C)}}$$

目次

（例Ａ）
時計の秒針を10秒単位で進める進め方（６通り）

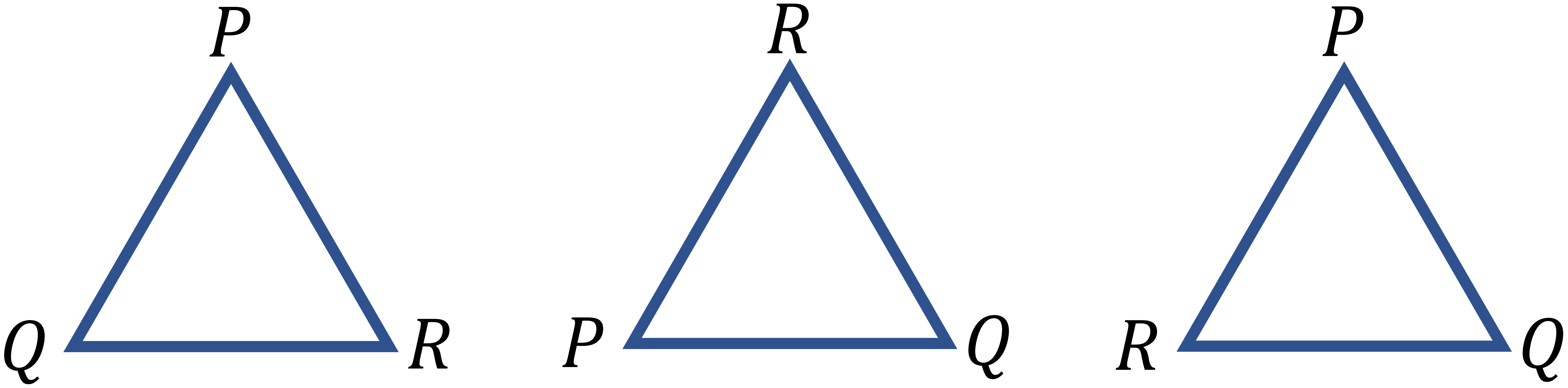


＊「60秒進める」
は
「0秒進める」
と同じと考える

（例Ｂ）

正三角形 PQR の合同変換（裏返しも可）

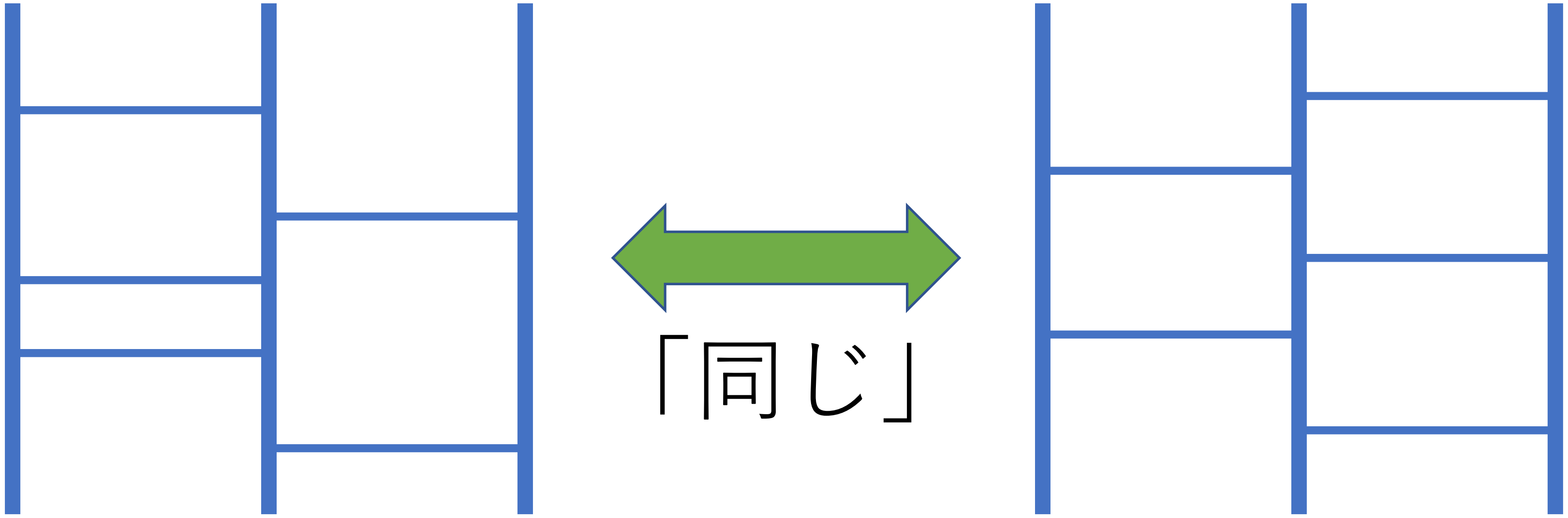
＊「まったく動かさない変換」も含む



（例Ｃ）

縦線が３本のあみだくじ

＊結果が同じあみだくじは「同じ」と考える



「同じ」

例Ａ （時計）	例Ｂ （正三角形）	例Ｃ （あみだくじ）

実はどの例でも、

「**同じものを６回繰り返すと『何もしない』状態になる**」

↑全部「同じようにして」証明できるか？

→「**動かし方の全体**」に注目する

後で「群」と呼ばれるもの

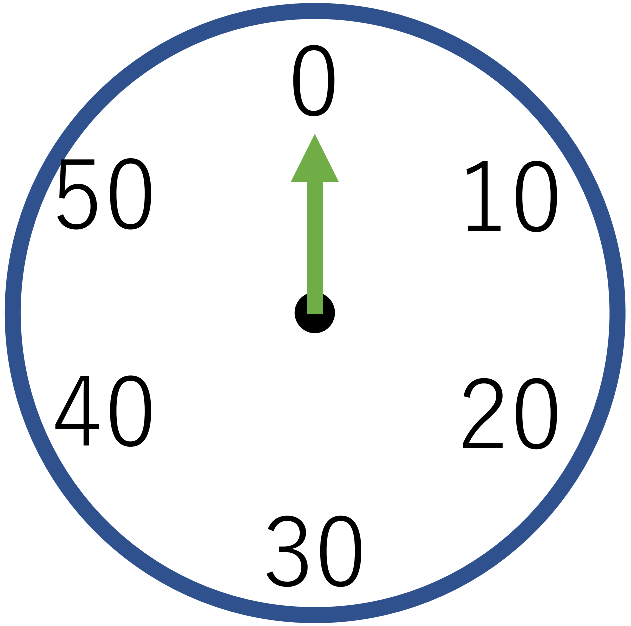
例A（時計）で、「動かし方の全体」は

$$\{\,[+0],[+10],[+20],[+30],[+40],[+50]\,\}$$

（$[+a]$ は「a 秒進める」）

動かし方 g の後に h を続ける、を $h \circ g$ と書く
（注意：右側が先）

$$[+20] \circ [+10] = [+30]$$
$$[+30] \circ [+50] = [+20]$$



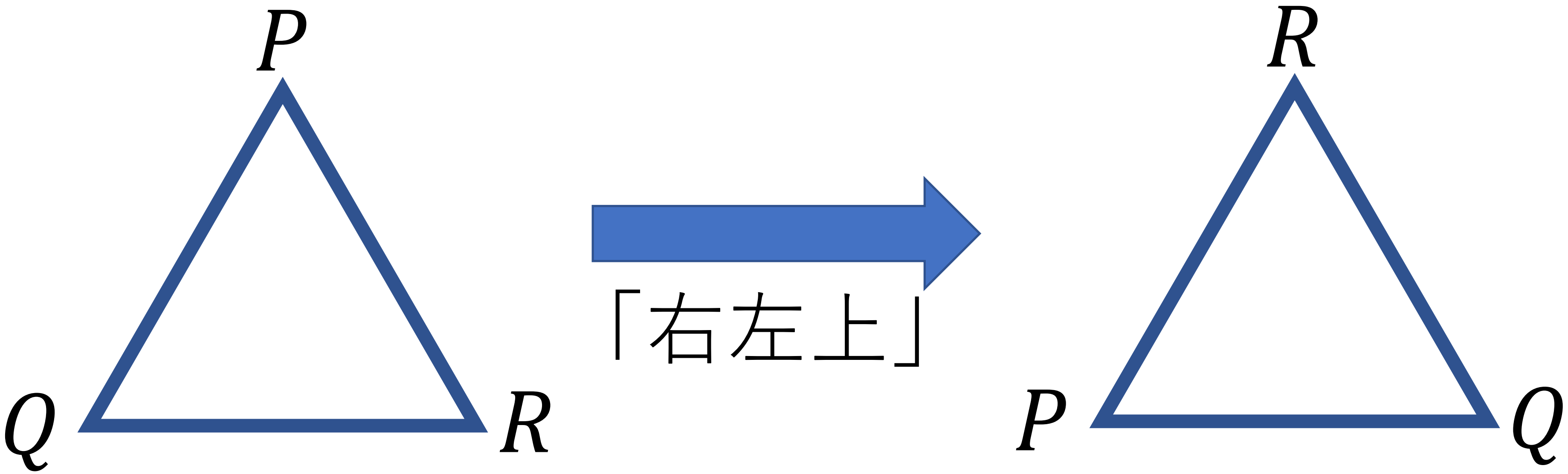
例Aでの $h \circ g$ の表

g

h

	[+0]	[+10]	[+20]	[+30]	[+40]	[+50]
[+0]	[+0]	[+10]	[+20]	[+30]	[+40]	[+50]
[+10]	[+10]	[+20]	[+30]	[+40]	[+50]	[+0]
[+20]	[+20]	[+30]	[+40]	[+50]	[+0]	[+10]
[+30]	[+30]	[+40]	[+50]	[+0]	[+10]	[+20]
[+40]	[+40]	[+50]	[+0]	[+10]	[+20]	[+30]
[+50]	[+50]	[+0]	[+10]	[+20]	[+30]	[+40]

例Ｂ（正三角形）で、左の頂点、上の頂点、右の頂点の行き先を並べて一つの変換を表す



「右左上」

変換 g の後に h を続ける、を $h \circ g$ と書く

例Ｂでの $h \circ g$ の表

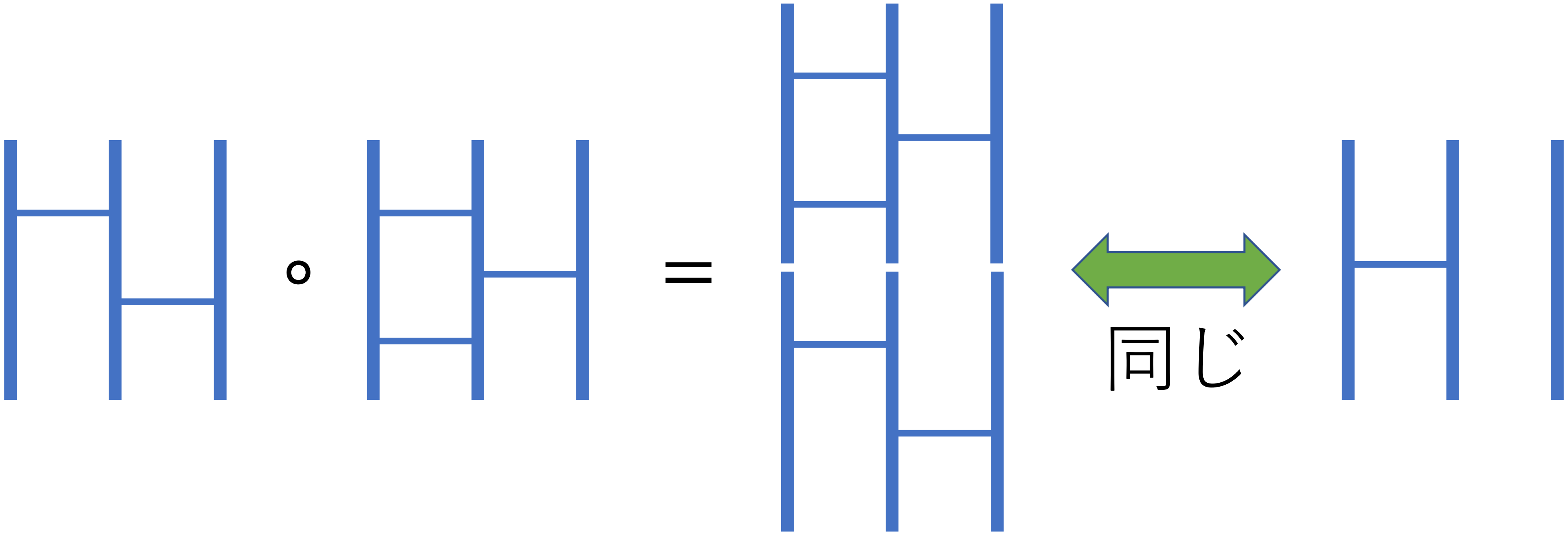
（[左,上,右]の行き先、の順で表示）

g

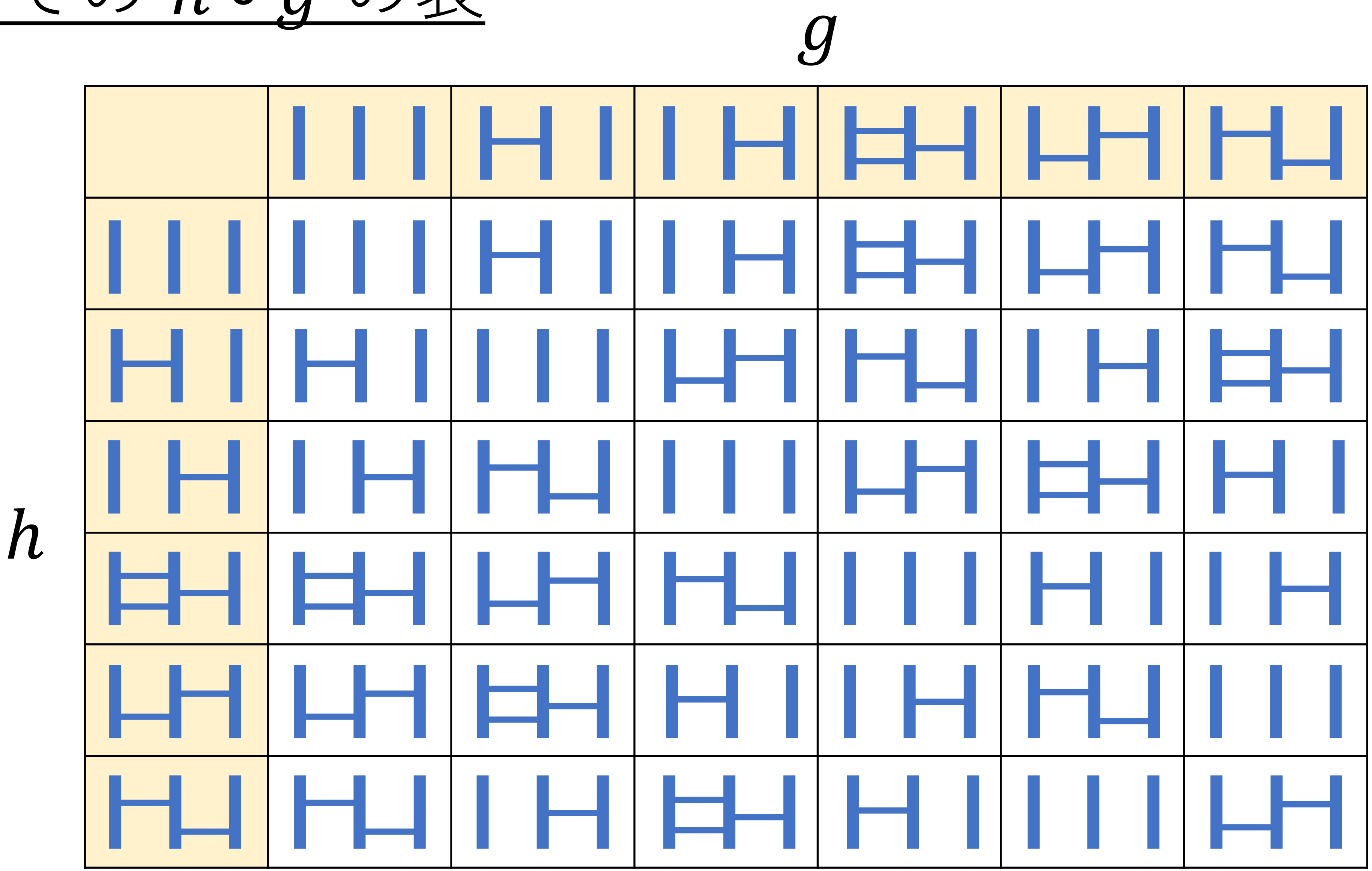
h

	左上右	上左右	左右上	右上左	上右左	右左上
左上右	左上右	上左右	左右上	右上左	上右左	右左上
上左右	上左右	左上右	上右左	右左上	左右上	右上左
左右上	左右上	右左上	左上右	上右左	右上左	上左右
右上左	右上左	上右左	右左上	左上右	上左右	左右上
上右左	上右左	右上左	上左右	左右上	右左上	左上右
右左上	右左上	左右上	右上左	上左右	左上右	上右左

例C（あみだくじ）で、あみだくじ g の下に h をつなげたものを $h \circ g$ と書く



例 C での $h \circ g$ の表



例A、例B、例Cに共通する性質（の一部）：

(1) $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

(2) 「常に $e \circ g = g$ かつ $g \circ e = g$」を
満たす e が（一つだけ）ある

(3) 各 g について、$I(g)$ をうまく選ぶと
「$g \circ I(g) = e$ かつ $I(g) \circ g = e$」

このような集合（と対応関係 $\circ$）を「**群**」と呼ぶ

群の条件(1)(2)(3)は「何を動かしているか」と独立に定義されている

例Ａ、例Ｂ、例Ｃの状況はどれも、
- まず「群」があり、
- 群の各要素が「物をどう動かすか」が定まる

と解釈できる
（作用の条件の説明は省略）

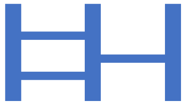
群の「**作用**」

→ 群の性質から作用の性質（の一部）がわかる

例Ｂ（正三角形）の群は
例Ｃ（あみだくじ）の群と<u>同じ構造</u>

「**同型**」

要素の対応関係の表

例Ｂ	左上右	上左右	左右上	右上左	上右左	右左上
例Ｃ						

例Bでの $h \circ g$ の表

（[左,上,右]の行き先、の順で表示）

g

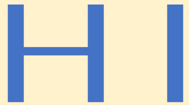
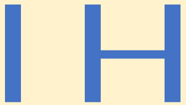
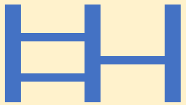
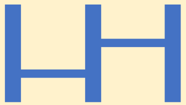
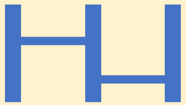
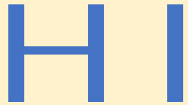
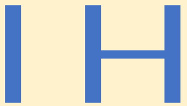
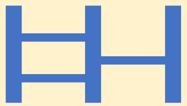
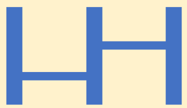
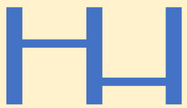
h

	左上右	上左右	左右上	右上左	上右左	右左上
左上右	0	1	2	3	4	5
上左右	1	0	4	5	2	3
左右上	2	5	0	4	3	1
右上左	3	4	5	0	1	2
上右左	4	3	1	2	5	0
右左上	5	2	3	1	0	4

例 C での $h \circ g$ の表

g

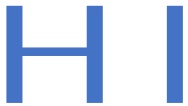
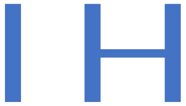
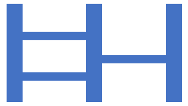
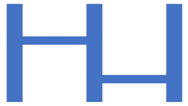
h

						
	0	1	2	3	4	5
	1	0	4	5	2	3
	2	5	0	4	3	1
	3	4	5	0	1	2
	4	3	1	2	5	0
	5	2	3	1	0	4

例Ｂ（正三角形）の群は
例Ｃ（あみだくじ）の群と同じ構造

「**同型**」

要素の対応関係の表

例Ｂ	左上右	上左右	左右上	右上左	上右左	右左上
例Ｃ						

＊例Ａ（時計）の群とは同型ではない
（なぜだろうか？）

群の別の例

整数全体の集合で、$h \circ g = h + g$ と定義

(2) $e = 0$（$g + 0 = 0 + g = g$ なので）
(3) $I(g) = -g$（$g + (-g) = (-g) + g = 0$ なので）

群は「整数」「図形」「順列と組み合わせ」などの性質（の一部）と幅広く関係している

さらに別の例（n を正の整数とする）

$$C_n = \{0, 1, 2, \ldots, n-1\}$$

で、$h + g$ を n で割った余りを $h \circ g$と定義

(2) $e = 0$

(3) $I(g) = n - g$（$g \neq 0$ のとき）、$I(0) = 0$

＊例Ａ（時計）の群は C_6 と同型

→ 例Ａは「群 C_6 の作用」とも考えられる

例Ａ	[+0]	[+10]	[+20]	[+30]	[+40]	[+50]
C_6	0	1	2	3	4	5

一般の群に関する定理

群の要素が全部で有限個（n 個）のとき、

$$\text{常に}\ \underbrace{g \circ g \circ \cdots \circ g}_{n\text{ 個}} = e$$

例Ａ、例Ｂ、例Ｃの群はどれも要素が６個

→ 「**同じものを６回繰り返すと『何もしない』状態（e）になる**」

（おまけ）
正六角形の合同変換の群と、
正三角柱の合同変換の群は同型
（話者の研究テーマの簡単な例）

「コクセター群の同型問題」

目次

- はじめに：数学と抽象化
- 「群」と「作用」の考え方
- **応用：整数の性質**
- 応用：暗号技術

フェルマーの小定理（の言い換え）

素数 p と正の整数 a について、
$a^p - a$ は常に p の倍数

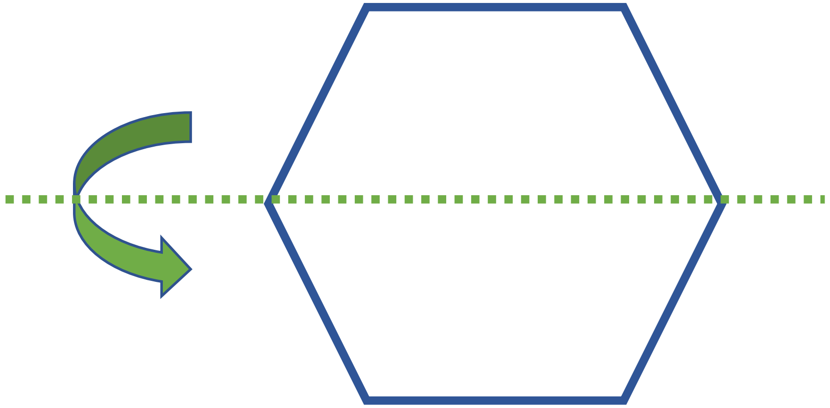
例

$$p = 5,\ a = 3 \rightarrow 3^5 - 3 = 243 - 3 = 240 = 5 \times 48$$

群と作用の考え方で証明してみよう！

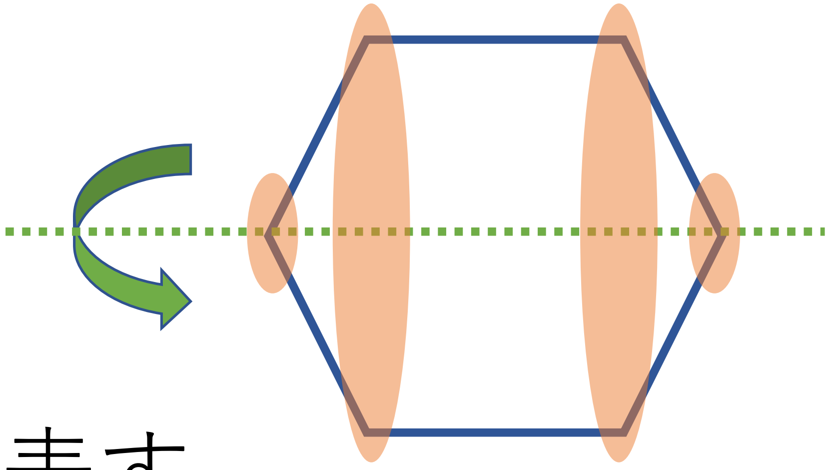
（要素が有限個の）群 G が集合 X に作用しているとする（$x \in X$ の行き先を $g(x)$ と書く）

例：$X = ($正六角形の頂点全体$)$
$G = \{$何もしない, 上下反転$\}$



（要素が有限個の）群 G が集合 X に作用しているとする（$x \in X$ の行き先を $g(x)$ と書く）

例：$X =$ (正六角形の頂点全体)
$G =$ {何もしない，上下反転}



$g(x)$（$g \in G$）全体の集合を $G \cdot x$ で表す

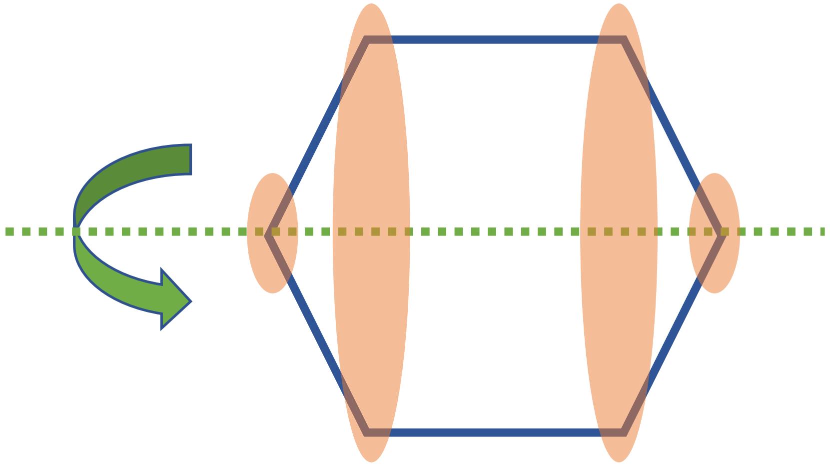
$x \in X$ の「**軌道**」

X 全体は、互いに交わらない軌道たちの和集合になる

（要素が有限個の）群 G が集合 X に作用しているとする（$x \in X$ の行き先を $g(x)$ と書く）

例：$X=$ (正六角形の頂点全体)

$G=$ {何もしない，上下反転}



群の作用に関する定理

$$(G \cdot x \text{ の要素数}) = \frac{(G \text{ の要素数})}{(g(x)=x \text{ となる } g \text{ の個数})}$$

フェルマーの小定理（の言い換え）

素数 p と正の整数 a について、
$a^p - a$ は常に p の倍数

1 から a までの整数 p 個の列全体を X とする
（全部で a^p 個の列）

$G = C_p$ （p で割った余りのなす群）とする
（全部で p 個の要素）

フェルマーの小定理（の言い換え）

素数 p と正の整数 a について、
$a^p - a$ は常に p の倍数

X：1 から a までの整数 p 個の列全体

$G = C_p$ （p で割った余りのなす群）

作用の定義

$g(x) = (x$ を右に g 個巡回的にずらしたもの$)$

例　$2([1,3,6,6,2]) = [6,2,1,3,6]$

フェルマーの小定理（の言い換え）

素数 p と正の整数 a について、
$a^p - a$ は常に p の倍数

$$(G \cdot x \text{ の要素数}) = \frac{(G \text{ の要素数})}{(g(x) = x \text{ となる } g \text{ の個数})}$$

右辺の分母と左辺は整数、右辺の分子は p（素数）

→ 右辺の分母は 1 または p のみ
（左辺は p または 1 のみ）

フェルマーの小定理（の言い換え）

素数 p と正の整数 a について、
$a^p - a$ は常に p の倍数

$$X = (\text{要素数 } p \text{ の軌道たち}) \cup (\text{要素数 } 1 \text{ の軌道たち})$$

a^p 個

要素は全部で
p の倍数個

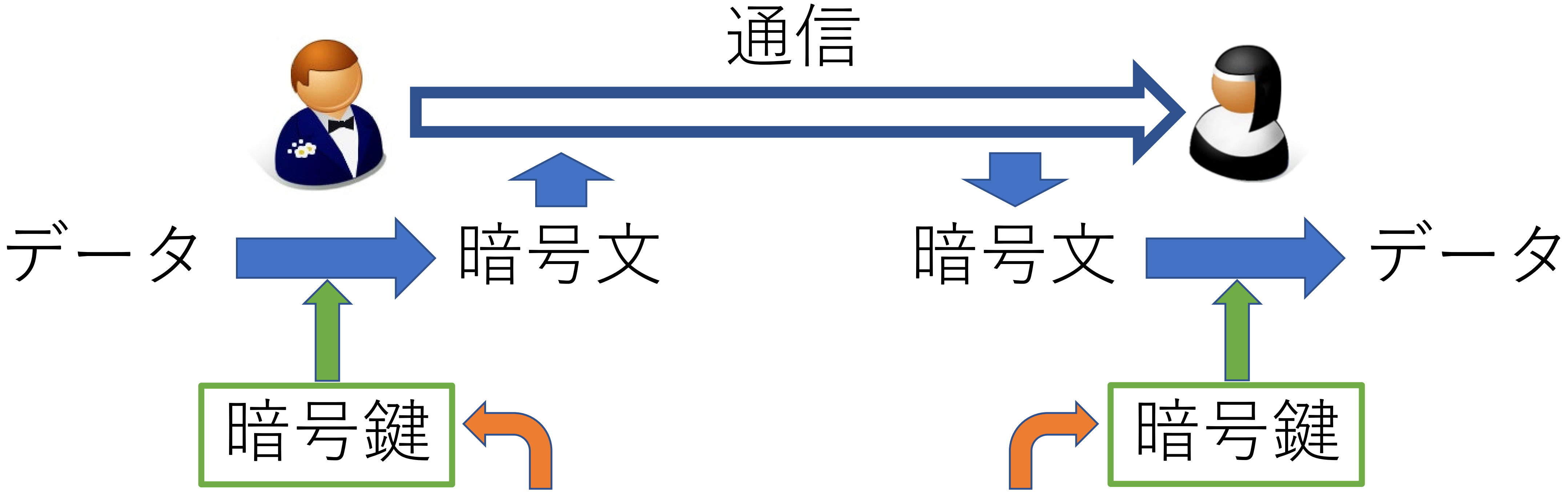
軌道 $G \cdot x$ がこうなるのは
x をどうずらしても x のとき
→ すべて同じ要素（全 a 通り）

→ $a^p = (p \text{ の倍数}) + a$ 【証明終】

目次

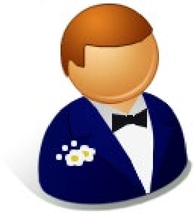
データの通信と暗号化

データを見られないよう暗号化して送る



どう秘密に共有する？

ディフィー・ヘルマン鍵共有（1976年）

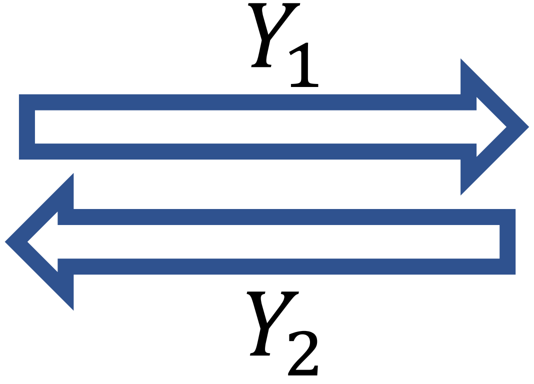


p は素数、 $a \in \{1,2,\ldots,p-1\}$

X_1 ：ランダム

Y_1 ： $a^{X_1} \div p$ の余り

K_1 ： $Y_2^{X_1} \div p$ の余り



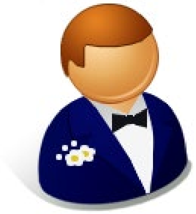
X_2 ：ランダム

Y_2 ： $a^{X_2} \div p$ の余り

K_2 ： $Y_1^{X_2} \div p$ の余り

$\boldsymbol{K_1 = Y_2^{X_1} = a^{X_2 X_1} = a^{X_1 X_2} = Y_1^{X_2} = K_2}$ （「の余り」略）

ディフィー・ヘルマン鍵共有（1976年）



p は素数、 $a \in \{1,2,\ldots,p-1\}$

（例） $p=5, a=2$

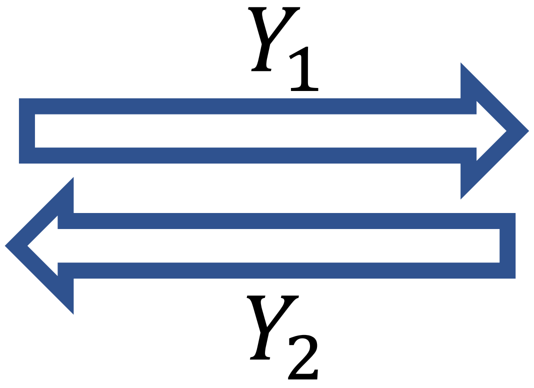
X_1 ：ランダム

Y_1 ：$a^{X_1} \div p$ の余り

（例） $X_1=2, Y_1=4$

K_1 ：$Y_2^{X_1} \div p$ の余り

（例） $K_1=3^2=9\equiv 4$



Y_1

Y_2

X_2 ：ランダム

Y_2 ：$a^{X_2} \div p$ の余り

（例） $X_2=3, Y_2=3$

K_2 ：$Y_1^{X_2} \div p$ の余り

（例） $K_2=4^3=64\equiv 4$

$\mathbf{K_1=Y_2^{X_1}=a^{X_2X_1}=a^{X_1X_2}=Y_1^{X_2}=K_2}$ （「の余り」略）

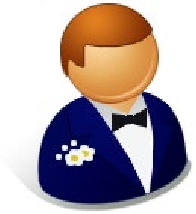
群の作用を用いた一般化

先ほどの方法で、べき乗 z^k を
「k の z への作用」と考える

→ **群とその作用を用いた一般化**のアイデア

（クーベニュー、1997年／2006年）

群の作用を用いた一般化



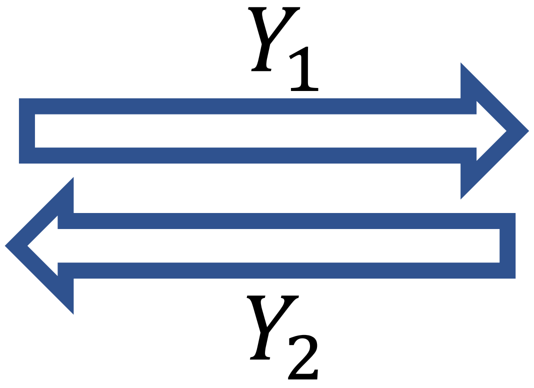
群 G は X へ作用、$a \in X$

G では常に $g \circ h = h \circ g$

$X_1 \in G$：ランダム

$Y_1 = X_1(a)$

$K_1 = X_1(Y_2)$



Y_1

Y_2

$X_2 \in G$：ランダム

$Y_2 = X_2(a)$

$K_2 = X_2(Y_1)$

$$\boldsymbol{K_1 = X_1(Y_2) = X_1 \circ X_2(a) = X_2 \circ X_1(a) = X_2(Y_1) = K_2}$$

群の作用を用いた一般化

先ほどの方法で、べき乗 z^k を

「k の z への作用」と考える

→ 群とその作用を用いた一般化のアイデア

（クーベニュー、1997年／2006年）

→ 安全かつ（そこそこ）効率的な**具体的構成**

（キャストリック 他４名、2018年）

＊とても専門的な数学の理論を使う

（2次拡大体上の超特異楕円曲線に対する構成的Deuring対応）

まとめ

- はじめに：数学と抽象化
  - 数学的性質の「本質的な理由」をとらえる
- 「群」と「作用」の考え方
  - 群の定義、群やその作用の例
- 応用：整数の性質
  - 群と作用を用いたフェルマーの小定理の証明
- 応用：暗号技術
  - 群と作用を用いた暗号鍵共有