鳩はどこへ行った？

新井 敏康（東京大学数理科学研究科）

概要

ひとつ, ふたつ, みっつというように子どもの頃からものの数（個数）を数えることに私たちは慣れてきました．すると

「巣穴が n 個あり, ハトが $(n+1)$ 羽いる．ハトはこの巣穴のいずれかに入る．このとき 2 羽以上のハトが入る巣穴がひとつはある」

ということは当たり前の事実に思えます．これを「鳩の巣原理」と呼びます．ここではこの原理を証明することの難しさを考えてみようと思います.

1　鳩の巣原理 Pigenohole principle

巣穴が n 個あり, ハトが $(n+1)$ 羽いる．ハトはこの巣穴のいずれかに入る．このとき 2 羽以上のハトが入る巣穴がひとつはある．

この原理は, ディリクレ (J. P. G. L. Dirichlet 1805-1859, 「ジリクレ」ではない) が初めて明確に原理として述べて証明に用いたことから「ディリクレの抽き出し論法 Dirichlet's drawer principle, Schubfachprinzip, 1834」「箱入れ論法 box principle」とか「部屋割り論法」とも呼ばれている.

部屋の数が n であるとき, $n+1$ 人以上の人間に対して部屋割りをしようとすれば, 必ずある部屋は 2 人以上が割り当てられる.

この事実は自明であるが, この論法はときに極めて強力で, 部屋割り論法あるいは鳩の巣論法と呼ばれる. 歴史的には, ディリクレがこの論法を用いて数論の結果を導いて以来, 多くの問題に使われている.（後略）

（岩波 数学入門辞典 部屋割り論法の項より, 引用者による下線）

1.1　個数の確定

鳩の巣原理は自明であると考えられている．それはなぜだろうか？もちろん

> ハトの個数 $(n+1)$ のほうが巣穴の個数 (n) より多いから，一つ（一羽）ずつ一つの巣穴に入れていくと一つ（一羽）は余ってしまうから

であるが，そもそも，ものの個数はなぜ確定するのだろうか？

（有限）集合 A が与えられたときに, その要素の個数を数えるには, ひとつ a_1, ふたつ $a_2 \notin \{a_1\}$, みっつ $a_3 \notin \{a_1, a_2\}$, $\ldots$ と一度, 数えたものを取り除きながら, ひとつずつその要素を数 $1, 2, 3, \ldots$ と対応させていく.

$$a_1 \mapsto 1,\ a_2 \mapsto 2,\ a_3 \mapsto 3,\ \ldots$$

こうしてすべての要素を数え終わったときに, 最後に対応した数 $a_n \mapsto n$ こそが<u>集合 A の要素の個数</u>と呼ばれる数である.

これを数学の言葉では集合 A と集合 $\{1, 2, \ldots, n\}$ との間に<u>全単射</u>（一対一対応）をつくったという. またこの対応（写像ともいう）を一つの文字 f で表して $f : A \to \{1, 2, \ldots, n\}$, $f : a_i \mapsto i$ と書き表す.

一般に二つの集合 A, B について, A の各要素 $a \in A$ に B のひとつの要素 $f(a) = b \in B$ が対応させられているとき, この対応 f を集合 A から集合 B への写像といって $f : A \to B$ と書き表す.

写像 $f : A \to B$ が, 異なる A の要素を必ず異なる B の要素に対応させている ($a_1 \neq a_2$ ならば $f(a_1) \neq f(a_2)$) とき, f は単射であるという.

$$\begin{tikzcd} a_1 \arrow[d, mapsto, "f"'] & \neq & a_2 \arrow[d, mapsto, "f"] \\ f(a_1) & \neq & f(a_2) \end{tikzcd}$$

また, どの B の要素 $b \in B$ についても $f(a) = b$ となる A の要素 a が少なくともひとつは存在するときには f は<u>全射</u>であるという.

$$A \ni a \overset{}{\underset{f}{\dashrightarrow}} b \in B$$

写像が全単射であるのは, 丁度, f が全射かつ単射であるときである. つまり写像 $f : A \to B$ が A から B への（A と B の間の）全単射であるのは, A の要素 a と B の要素 b が, $f(a) = b$ という関係により丁度ひとつずつ互いに結び付けられているときである.

$$A \ni a \underset{f}{\longleftrightarrow} b \in B$$

すると鳩の巣原理が述べていることは以下で言い表わせる.

定理 1.1 （写像版の鳩の巣原理）
集合 $\{1, 2, \ldots, n, n+1\}$ から集合 $\{1, 2, \ldots, n\}$ への単射は存在しない.

$(n+1)$ 羽のハトのそれぞれが n 個ある巣穴のいずれか一つに入る入り方が, 丁度, 写像 $f : \{1, 2, \ldots, n, n+1\} \to \{1, 2, \ldots, n\}$ を定め, 逆にそのような写像 f が与えられれば, ハトの巣穴への行き先がひとつ指定される.

$$
\begin{aligned}
& \{1, 2, \ldots, n, n+1\} \text{ から } \{1, 2, \ldots, n\} \text{ への単射が存在しない} \\
\Leftrightarrow\quad & \text{どの写像 } f : \{1, 2, \ldots, n, n+1\} \to \{1, 2, \ldots, n\} \text{ も単射ではない} \\
\Leftrightarrow\quad & \text{どの巣穴にも複数のハトがいないような入り方はない}
\end{aligned}
$$

集合の要素の個数がそれぞれの（有限）集合ごとに確定する，つまりその数え方によらないのは次の事実から分かる：

定理 1.2 二つの自然数 n, m に対して全単射 $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ が存在すれば，$n = m$.

なぜならば，いま集合 A から集合 $\{1, 2, \ldots, n\}$ への，および集合 $\{1, 2, \ldots, m\}$ への全単射 $f : A \to \{1, 2, \ldots, n\}$, $g : A \to \{1, 2, \ldots, m\}$ がそれぞれ与えられているとする.

$$\begin{array}{ccccc} \{1, 2, \ldots, n\} & & A & & \{1, 2, \ldots, m\} \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ x & \xleftarrow[f]{\qquad\qquad} & a & \xrightarrow[g]{\qquad\qquad} & y \end{array}$$

$$\begin{tikzcd}
\{1,2,\ldots,n\} & A & \{1,2,\ldots,m\} \\
x \arrow[u, phantom, sloped, "\in"] \arrow[r, "f^{-1}"] & a \arrow[u, phantom, sloped, "\in"] \arrow[r, "g"'] & y \arrow[u, phantom, sloped, "\in"]
\end{tikzcd}$$

各 $x \in \{1,2,\ldots,n\}$ に対して $f(a) = x$ となる $a \in A$ が丁度一つあるので, この a を x に対応させることで写像 $f^{-1} : \{1,2,\ldots,n\} \to A$（$f$ の逆写像）が作られる.

このとき $x \in \{1,2,\ldots,n\}$ に対して, 先ず $f(a) = x$ となる $a = f^{-1}(x)$ を対応させて, その後でこの a に $y = g(a) \in \{1,2,\ldots,m\}$ を対応させることで合成写像 $g \circ f^{-1} : \{1,2,\ldots,n\} \to \{1,2,\ldots,m\}$, $(g \circ f^{-1})(x) = g(f^{-1}(x))$, $x \mapsto a \mapsto g(a)$, が定義される.

$$\begin{array}{ccccc} \{1,2,\ldots,n\} & & A & & \{1,2,\ldots,m\} \\ \rotatebox[origin=c]{-90}{$\in$} & & \rotatebox[origin=c]{-90}{$\in$} & & \rotatebox[origin=c]{-90}{$\in$} \\ x & \xrightarrow{\quad f^{-1} \quad} & a & \xrightarrow[\quad g \quad]{} & y \end{array}$$

すると先ず全単射 f の逆写像 f^{-1} も全単射になることが分かる.

そしてともに全単射である二つの写像 f^{-1} と g を合成して作った合成写像 $g \circ f^{-1} : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ も全単射になることが分かる.

そこで定理 1.2 により $n = m$ であり, 集合 A の要素の個数は, 写像 f, g が定める数え方によらずに確定することが分かった.

ところがこの事実（定理 1.2）は鳩の巣原理から示されるのである.

二つの自然数 n, m の間に全単射 $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ が与えられているとして, $n \neq m$ であると仮定する. いま一般性を失うことなく $n > m$ であるとしてよい. つまり $n \geq m + 1$.

写像 f を集合 $\{1, 2, \ldots, m + 1\}$ に制限して得られる写像 $g(i) = f(i)$, $g : \{1, 2, \ldots, m + 1\} \to \{1, 2, \ldots, m\}$ を考える. するとこの写像 g は集合 $\{1, 2, \ldots, m + 1\}$ から集合 $\{1, 2, \ldots, m\}$ への単射となり, 鳩の巣原理の写像版である定理 1.1 に矛盾する. よって $n = m$ でなければならない.

結局, 鳩の巣原理を, 集合の要素の個数の大小を比較することによって自明であるとするのは, 集合の要素の個数そのものが鳩の巣原理によって決まるので, 循環していると考えられる.

注意 1 定理 1.2 は集合 $\{1, 2, \ldots, n\}, \{1, 2, \ldots, m\}$ がともに有限だから成り立つ.

無限集合 X と Y では, X が Y の真部分集合であっても X と Y の間に全単射は作れる（ガリレオ・ガリレイ）

例えば自然数全体の集合 $\mathbb{N} = \{1, 2, \ldots\}$ とそこに入っていない要素 $a \notin \mathbb{N}$ について集合 $\mathbb{N} \subsetneq \mathbb{N} \cup \{a\}$ を考える. $f(n) = n + 1\,(n \in \mathbb{N})$, $f(a) = 1$ とすれば写像 $f : \mathbb{N} \cup \{a\} \to \mathbb{N}$ は全単射.

$$\begin{tikzcd}
\mathbb{N} \cup \{a\} & a \arrow[dr] & 1 \arrow[dr] & 2 \arrow[dr] & 3 \arrow[dr] & \cdots & \\
\mathbb{N} & & 1 & 2 & 3 & 4 & \cdots
\end{tikzcd}$$

2　鳩の巣原理を証明する

鳩の巣原理あるいは定理 1.1 は, 本質的には自然数に関する命題であるから数学的帰納法で証明してみよう. 定理 1.1 の命題

> 集合 $\{1, 2, \ldots, n, n+1\}$ から集合 $\{1, 2, \ldots, n\}$ への単射は存在しない.

あるいは同じことだが

> 任意の写像 $f : \{1, 2, \ldots, n, n+1\} \to \{1, 2, \ldots, n\}$ は単射ではない.

を $A(n)$ と書いて, これを自然数 n に関する数学的帰納法で証明しよう.

まず $n=1$ のときを考える．写像 $f:\{1,2\}\to\{1\}$ は $f(1)=1=f(2)$ であるから単射ではない．よって $A(1)$ は成立．

次に $A(n)$ が正しいと仮定して $A(n+1)$ を導こう．

写像 $f:\{1,2,\ldots,n+1,n+2\}\to\{1,2,\ldots,n,n+1\}$ が与えられている．いまこの f が単射であると仮定する．

場合 1．初めに $n+1$ が f の値域に入っていないとする．つまりどの $i\in\{1,2,\ldots,n+1,n+2\}$ についても $f(i)\neq n+1$ である．このとき写像 f を $\{1,2,\ldots,n+1\}$ に制限して得られる写像 $g:\{1,2,\ldots,n+1\}\to\{1,2,\ldots,n\}$ が単射となり帰納法の仮定 $A(n)$ に反する．

$[f : \{1, 2, \dots, n+1, n+2\} \to \{1, 2, \dots, n, n+1\}$ は単射$]$

以下, $n+1$ が f の値域に入っている場合を考える. $i_0 \in \{1, 2, \dots, n+1, n+2\}$ を $f(i_0) = n+1$ となるように取る. f が単射であるから, このような i_0 は一意に決まる.

場合 2. もしも $i_0 = n+2$ であるなら, $i \in \{1, 2, \dots, n+1\}$ について $f(i) \in \{1, 2, \dots, n\}$ であるから, 再び写像 f を $\{1, 2, \dots, n+1\}$ に制限して得られる写像 $g : \{1, 2, \dots, n+1\} \to \{1, 2, \dots, n\}$ が単射となり帰納法の仮定 $A(n)$ に反する.

$$\begin{tikzcd}
n+2 \arrow[dr] & n+1 \arrow[drr] & n & \cdots \\
 & n+1 & n & \cdots
\end{tikzcd}$$

場合 3. ある $i_0 \in \{1, 2, \ldots, n+1\}$ について $f(i_0) = n+1$. このとき f が単射であるから, $f(n+2) = j_0$ は $j_0 \neq n+1$, つまり $j_0 \in \{1, 2, \ldots, n\}$. このとき以下の写像 $g : \{1, 2, \ldots, n+1\} \to \{1, 2, \ldots, n\}$ が単射となる.

$$g(i) = \begin{cases} f(i) & i \neq i_0 \text{ のとき} \\ j_0 & i = i_0 \text{ のとき} \end{cases}$$

$$\begin{tikzcd}
f: & n+2 \arrow[drrrrr] & n+1 & \cdots & i_0 \arrow[dll] & \cdots & j_0 & \cdots \\
& & n+1 & \cdots & i_0 & \cdots & j_0 & \cdots
\end{tikzcd}$$

$$\begin{tikzcd}
g: & n+1 & \cdots & i_0 \arrow[drr] & \cdots & j_0 & \cdots \\
& & \cdots & i_0 & \cdots & j_0 & \cdots
\end{tikzcd}$$

よってすべての場合において, $A(n)$ と単射 $f:\{1,2,\dots,n+1,n+2\}\to\{1,2,\dots,n,n+1\}$ の存在は矛盾するので, $A(n)$ ならばこのような単射は存在せず, 従って $A(n+1)$ が正しい.

上記により自然数 n に関する数学的帰納法により, 任意の自然数 n について命題 $A(n)$ が正しいことが分かった. $\square$

3　証明の難しさをなぜ問題にするか？

上記の命題 $A(n)$ には「任意の写像 $f:\{1,2,\dots,n,n{+}1\}\to\{1,2,\dots,n\}$」という対象を含んでいる. そのような写像は n^{n+1} 個あり, これだけたくさんあるモノ（写像）すべてを完全に見通して把握し切れない.

計算機がする証明では, 形式的対象に関する機械的な規則にのみ従って, 推論が進行する. 本質的には命題 A, B について, 以下のかたちの推論のみ行われる：

$$(A \text{ または } B) \text{ かつ } (A \text{ または } (B \text{ でない})) \text{ ならば } A$$

鳩の巣原理 $A(n)$ を機械可読な形 $A'(n)$ に書き換えてやれば, この極めて単純な命題の操作の繰り返しによって, 各 n ごとに $A'(n)$ は証明される. しかしその証明に要する命題操作の回数は 2^n のオーダーを持たざるを得ないことが分かっている (A. Haken, 1985).

数学の証明を計算機にさせようとするときに, 指数関数 2^n あるいは鳩の巣原理は一つの障壁となる.

4　証明できないことをどうやって証明するか？

いくつかの原理（公理）からある命題が導けないことを示す方法の一つは, それらの原理を満たしながらその命題を満たさないモデル（構造）の存在をいうことである．この方法による古典的な例は, ユークリッドの原論における第五公準（平行線公理）が他の公準から導けないことの証明であった．

例えば球面上の大円を「直線」とみなせば, ユークリッドの初めの四つの公準はすべて満たされるが, 第五公準は, 成り立たない．

他方では第五公準は平面上では成立するから, 第五公準は他の公準から独立な（肯定も否定もできない）命題であることになる．

5　鳩の巣原理の独立性

自然数に関する公理で最も重要な「数学的帰納法」の公理は, 以下のように述べられる. 自然数に n に関する命題 $B(n)$ について

> $B(1)$ が正しくて, かつ任意の自然数 n について, $B(n)$ ならば $B(n+1)$ が成り立てば, 任意の自然数 n について $B(n)$ が成立する.

この数学的帰納法での $B(n)$ として上記の $A(n)$ を取れば鳩の巣原理は証明できた. この命題 $A(n)$ には「任意の写像 $f : \{1, 2, \ldots, n, n+1\} \to \{1, 2, \ldots, n\}$」という概念が含まれており, n を変えると考えるべき写像の個数 n^{n+1} も変わって行く.

鳩の巣原理を証明するために, 指数関数 2^n あるいは「任意の写像 $f : \{1, 2, \ldots, n, n+1\} \to \{1, 2, \ldots, n\}$」という概念が絶対に必要かどうかが問題となってくる.

そこで, そのような概念の使用を禁止した公理系からは鳩の巣原理が独立なのではないか？と予想できる.

先ずは適当な公理系を導入する. 自然数 n と自然数上の写像 f に関する命題 $B(n, f)$ を考える. $B(n, f)$ に含まれる「任意の自然数 m について」や「ある自然数 m が存在して」において, m が動く範囲を n のある自然数係数の多項式に制限する.

m が動く範囲が n のある自然数係数の多項式

$$p(n) = a_d n^d + a_{d-1} n^{d-1} + \cdots + a_1 n + a_0 \, (d, a_d, a_{d-1}, \ldots, a_1, a_0 \in \mathbb{N} \cup \{0\})$$

に限定されているとき, つまり「任意の自然数 $m \leq p(n)$ について」や「ある自然数 $m \leq p(n)$ が存在して」と探す範囲が $p(n)$ で抑えられているとき, $B(n, f)$ を $\Delta_0(f)$-命題という.

自然数に関する公理の中で, 数学的帰納法を $\Delta_0(f)$-命題に制限して得られる公理系を $I\Delta_0(f)$ と書き表す.

数学的帰納法は任意に固定された自然数上の写像 f とこの $\Delta_0(f)$-命題 $B(n,f)$ について

> $B(1,f)$ が正しくて, かつ任意の自然数 n について, $B(n,f)$ ならば $B(n+1,f)$ が成り立てば, 任意の自然数 n について $B(n,f)$

定理 5.1 (M. Ajtai 1988)
$I\Delta_0(f)$ では, 写像 f に関する鳩の巣原理は証明できない：

> 任意の n について, f の $\{1,2,\ldots,n,n+1\}$ への制限は, $\{1,2,\ldots,n\}$ への（全）単射ではない

証明の粗筋.

まず「自然数」の概念を変更する.

ある集合 $M = \mathbb{N} \cup \{a_1, a_2, \ldots\}$ で, f を含まない自然数に関する命題については数学的帰納法が成立するという意味で自然数 $\mathbb{N} = \{1, 2, \ldots\}$ とよく似ているが, すべての自然数よりも大きい要素 $1 < a, 2 < a, \ldots$ を含むようなものを作る.

このような集合 M を自然数の公理の超準モデルと言って, すべての自然数より大きい要素を超準要素と言う.

自然数に関するペアノの公理の内で数学的帰納法以外の公理を考える．集合 M とその一つの要素 $1 \in M$ および M 上の写像 $S : M \to M$ の組が以下を満たすときに, その組を仮に自然数体系と呼ぶ：

1. S は M 上の単射である：$x \neq y \in M$ について $S(x) \neq S(y)$.

2. 写像 S の値域は $\{x \in M | x \neq 1\}$ である.

二つ目の公理が述べているのは, まず $1 \in M$ は写像 S の値域に入らない, 任意の $x \in M$ について $S(x) \neq 1$ であり, また任意の $1 \neq x \in M$ について $S(y) = x$ となる $y \in M$ が存在するということ．一つの目の公理と併せると写像 S を $S : M \to \{x \in M | x \neq 1\}$ とみなせば, この S が全単射になっているということを述べている.

$$S : M \to \{x \in M | x \neq 1\} \text{ は全単射}$$

$M = \mathbb{N}$, $S(x) = x+1$ と思えば上記の公理は満たされるが $\mathbb{N}$ だけが上記を満たす自然数体系ではない. 例えば, 直和 $M = \mathbb{N} \coprod \mathbb{Z}$. $n \neq (1, n), (1, -n)$ として

$$M = 1, 2, 3, \ldots \ldots, (1, -3), (1, -2), (1, -1), (1, 0), (1, 1), (1, 2), (1, 3), \ldots$$

写像 $S : M \to M$ を, 自然数 $n \in \mathbb{N}$ については $S(n) = n + 1$ として, それ以外では $S((1, n)) = (1, n + 1)$ $(n \in \mathbb{Z})$ と定める. $1 \in M$ は自然数の 1. するとこの S について M がやはり自然数体系であることが容易に分かる.

超準要素 $a \in M$ については $\{x \in M | x < a\}$ は無限集合なので, 注意 1 により, $\{x \in M | x < a+1\} = \{x \in M | x < a\} \cup \{a\}$ から $\{x \in M | x < a\}$ への全単射 G が存在する.

問題なのは, このような全単射 G による $\Delta_0(G)$-命題 $B(n, G)$ に適用された数学的帰納法を成立させるためには, G を上手に構成しなければいけないこと.

例えば $G : M \to M$ を, 自然数 $n \in \mathbb{N}$ に対しては $G(n) = n$ として, 超準要素 $b \in M$ で, ある自然数 n について $b < a + n$ となっている b については $G(b) = b - 1$ とし, それ以外の b については $G(b) = a + b$.

$$
\begin{tikzcd}
1 \arrow[d] & \cdots & a-1 \arrow[dl] & a \arrow[dl] & \cdots & b \arrow[drr] & \cdots & \cdots & \cdots \\
1 & \cdots & a-1 & a & \cdots & b & \cdots & a+b & \cdots
\end{tikzcd}
$$

G を集合 $\{x \in M | x < a + 1\}$ に制限した写像 H は全単射 $H : \{x \in M | x < a + 1\} \to \{x \in M | x < a\}$ を与える.

$$
\begin{tikzcd}
1 \arrow[d] & \cdots & a-1 \arrow[dl] & a \arrow[dl] & \cdots & b \arrow[drr] & \cdots & \cdots & \cdots \\
1 & \cdots & a-1 & a & \cdots & b & \cdots & a+b & \cdots
\end{tikzcd}
$$

命題 $B(x,f) :\Leftrightarrow f(x) < a+x$ を考えると

$B(x,G)(\Leftrightarrow G(x) < a+x) \Leftrightarrow x < a+n$ となる自然数 $n \in \mathbb{N}$ が存在する

$x+1 < a+(n+1), n+1 \in \mathbb{N}$ より「$B(x,G)$ ならば $B(x+1,G)$」が任意の $x \in M$ で成立. しかし例えば $b = 2a$ とすると任意の自然数 $n \in \mathbb{N}$ について $b \not< a+n$ なので $B(b,G)$ は正しくない. よって上記の G について命題 $B(n,G)$ に適用した数学的帰納法は成立しない.

超準モデル M の存在を示すには,「コンパクト性定理」と呼ばれる数学基礎論の定理を用いる. 互いに矛盾しない命題が無限個与えられたら, それらすべてを満たすモデルの存在を保証するのが「コンパクト性定理」

数学的帰納法が成立するような全単射 G を構成するには強制法という手法を用いる. 強制法は元々 P. Cohen, 1963-64 が, 選択公理と連続体仮説という集合論の命題の集合論からの独立性証明のために考案した方法.