2 数学的帰納法と帰納的定義

• 2-1 ： 数学的帰納法

自然数全体 $\mathbb{N}$ をドメインとする命題関数 $P(x)$ があるとき, 無限個の命題 $P(1), P(2), P(3), \ldots$ が得られる. これら無限個の命題が真であることを証明したいとき, 命題をひとつひとつ検証していればきりがない. 数学的帰納法は, すべての $n \in \mathbb{N}$ に対して, $P(n)$ が真であることを証明する方法である.

定理 2.1 (帰納法の原理)**.** 整数 $a \in \mathbb{Z}$ をとる. $\mathbb{Z}$ の部分集合 $A = \{n \in \mathbb{Z} \mid n \geq a\}$ をドメインとする命題関数 $P(n)$ が次の 2 条件を満たすとする.

(i) $P(a) = \mathsf{T}$ である.
(ii) $k \in A$ について $P(k) = \mathsf{T}$ と仮定するとき, $P(k+1) = \mathsf{T}$ である.

このとき, 全称命題「$\forall n \in A, P(n)$」の真理値は T である.

証明. 背理法を使って証明しよう. A の部分集合 M を

$$M := \{n \in A \mid P(n) = \mathsf{F} \text{ である. }\}$$

と定め, $M \neq \varnothing$ であると仮定する.

m を M の元のなかで最小の整数とする. 条件 (i) より, $m > a$ であるから $m - 1 \in A$ である. m の最小性から $P(m-1) = \mathsf{T}$ となる. このとき,

$$P(m) = P((m-1)+1)$$

であるから, 条件 (ii) より $P(m) = \mathsf{T}$ となるが, これは $m \in M$ に矛盾する. 以上で $M = \varnothing$ となり, 全称命題「$n \in A, P(n)$」の真理値は T である. □

条件 (i) を数学的帰納法の **第一段階**, 条件 (ii) を **第二段階** と呼ぶ.

• 2-2 ： 累積帰納法

数学的帰納法に基づき, $\mathbb{Z}$ の部分集合 $A = \{n \in \mathbb{Z} \mid n \geq a\}$ をドメインとする命題関数 $P(n)$ に関する全称命題「$\forall n \in A, P(n)$」を証明しようとするとき, 第一段階が A に属する整数の最小値 a の場合だけでは不十分な場合がある. 例えば, 次のような問題を考えてみよう.

> 各項が正の数列 $\{a_n\}$ は, すべての自然数に対して
>
> $$(a_1 + a_2 + \cdots + a_n)^2 = a_1^3 + a_2^3 + \cdots + a_n^3$$
>
> を満たしているとき, 数列 $\{a_n\}$ の一般項は $a_n = n$ で与えられることを示せ.

具体的にいくつか計算して成り立つことを確認してみる. まず, $n = 1$ のときは

$$a_1^2 = a_1^3 \iff a_1^2(a_1 - 1) = 0$$

であり, $a_1 > 0$ なので, $a_1 = 1$ である. 次に $n = 2$ のとき, $a_1 = 1$ だったので

$$(1 + a_2)^2 = 1 + a_2^3 \iff a_2(a_2 + 1)(a_2 - 2) = 0$$

であり, $a_2 > 0$ なので, $a_2 = 2$ である. 続いて, $n = 3$ のときは, $a_1 = 1$, $a_2 = 2$ だったので

$$(1 + 2 + a_3)^2 = 1 + 8 + a_3^3 \iff a_3(a_3 + 2)(a_3 - 3) = 0$$

であり, $a_3 > 0$ なので, $a_3 = 3$ である. 以下, 同様に計算していけば $a_4 = 4$, $a_5 = 5, \ldots$ となることがわかる.

ここでポイントとなるのは, $a_3 = 3$ を導くのに **$a_1 = 1$, $a_2 = 2$ のどちらも用いているという点** である. もちろん, $a_4 = 4$ を導くのに **$a_1 = 1$, $a_2 = 2$, $a_3 = 3$ の全てを用いる** ことに気づくだろう. つまり $a_n = n$ を示すために, 全ての $1 \leq k < n$ に対して $a_k = k$ を用いる必要がある.

では, 実際に $a_n = n$ が成り立つことを証明してみよう.

(i) $n = 1$ のとき, $a_1 = 1$ となることは既に示した.

(ii) $n > 1$ のとき, **全ての $1 \leq k < n$ に対して** $a_k = k$ であることを仮定する. このとき, 条件から

$$(a_1 + a_2 + \cdots + a_n)^2 = a_1^3 + a_2^3 + \cdots + a_n^3$$

であり, 仮定から $k = 1, 2, \ldots, n-1$ に対して $a_k = k$ であるから上式は

$$\begin{aligned}
& (1 + 2 + \cdots + (n-1) + a_n)^2 = 1^3 + 2^3 + \cdots + (n-1)^3 + a_n^3 \\
\iff & \left(\frac{1}{2}(n-1)n + a_n\right)^2 = \frac{1}{4}(n-1)^2 n^2 + a_n^3 \\
\iff & (n-1)na_n + a_n^2 = a_n^3 \\
\iff & a_n(a_n + n - 1)(a_n - n) = 0
\end{aligned}$$

ここで, $a_n > 0$ なので $a_n = n$ であることが示された.

以上のように, 全称命題「$\forall n \in A, P(n)$」を証明を数学的帰納法で示そうとするとき, ある番号まですべて正しいと仮定するような帰納法を **累積帰納法** と呼ぶ.

定理 2.2 (帰納法の原理 (2))**.** 整数 $a \in \mathbb{Z}$ をとる. $\mathbb{Z}$ の部分集合 $A = \{n \in \mathbb{Z} \mid n \geq a\}$ をドメインとする命題関数 $P(n)$ が次の 2 条件を満たすとする.

(i) $P(a) = \mathsf{T}$ である.

(ii) $k \in A$ について, 全ての $a \leq m \leq k$ で $P(m) = \mathsf{T}$ と仮定するとき, $P(k+1) = \mathsf{T}$ である.

このとき, 全称命題「$\forall n \in A, P(n)$」の真理値は T である.

- **2-3： 間違った数学的帰納法の使い方**

世の中には, 数学的（累積）帰納法を誤った使い方をすることで「意味不明」な主張をしているようなものが存在する. 数学の証明は, 一部でも間違っていれば全体として崩壊する. 正しい証明を与えるためには, 正しくない証明を見抜く力も必要である. 正しくない証明の典型例と, 何が問題かを示しておく.

主張：日立市の天気は常に晴である.

（証明） 日立市に降る雨粒の数に関する帰納法で証明する. ある日に日立市に降った雨粒の数を n とおく.

(i) $n = 0$ のとき, 明らかにその日は晴である.

(ii) $n = k$ のとき, 晴であると仮定すれば, $n = k + 1$ のとき晴の日に 1 粒雨粒が増えてもやはり晴である.

以上より, 全ての n に対して日立市は常に晴であるから証明が完了した.

この主張は **何粒雨が降れば晴ではなくなるのかという定義が与えられていないので,** そもそも命題ではない. また, 仮に晴の定義を具体的に与えたところで, **ある n 粒から $n+1$ 粒で晴ではなくなる** ので, やはり証明にならない.

主張：全ての猫は同じ顔である.

（証明） 猫の数 n に関する帰納法で証明する

(i) $n=1$ のとき, 1 匹しかいないので同じ顔をしている.

(ii) $n=k$ に対して, これらの k 匹の猫が同じ顔をしていると仮定する. $k+1$ 匹目の猫を考えると, k 匹の猫からなる 2 通りのグループを以下のように作ることができる.

$$\underbrace{\text{猫 }1,\ \text{猫 }2,\ \text{猫 }3,\ \ldots,\ \text{猫 }n}_{k\text{ 匹の猫：グループ A}},\ \text{猫 }n+1,\quad \text{猫 }1,\ \underbrace{\text{猫 }2,\ \text{猫 }3,\ \ldots,\ \text{猫 }n,\ \text{猫 }n+1}_{k\text{ 匹の猫：グループ B}}$$

仮定より, それぞれのグループ A, B に属している k 匹の猫は同じ顔である. よって, $k+1$ 匹目の猫も同じ顔をしている.

以上より, 全ての猫は同じ顔であることが証明された.

この証明は **$n+1=2$ のときに, 猫 1 と猫 2 が同じ顔であることを保証していないので証明が崩壊する.**

- **2-3： 帰納的定義**

あるものを定義するときに, それ自身を使って自己参照をすることで定義する方法を **帰納的定義**, あるいは **再帰的定義** という.

例 2-1 数列の漸化式は帰納的定義の代表例である. 例えば,

$$a_1=1,\quad a_{n+1}=2\cdot a_n+1\ \ (n\geq 1)$$

から定まる数列 $\{a_n\}_{n=1,2,\ldots}$ は

$$a_1=1,\quad a_2=2\cdot a_1+1=3,\quad a_3=2\cdot a_2+1=7,\quad a_4=2\cdot a_3+1=15,\ldots$$

と次の項をそれまでの項の値を参照することで定めている.

例 2-2 アッカーマン関数 $A(m,n)$ は, 次のようにして二重帰納的に定義される関数である.

(i) $A(0,n)=n+1$.

(ii) $A(m+1,0)=A(m,1)$.

(iii) $A(m+1,n+1)=A(m,A(m+1,n))$.

例えば, $A(2,0)$ の値は次のようにして求めることができる:

$$A(2,0)\overset{\text{(ii)}}{=}A(1,1)\overset{\text{(iii)}}{=}A(0,A(1,0))\overset{\text{(i)}}{=}A(1,0)+1\overset{\text{(ii)}}{=}A(0,1)+1\overset{\text{(i)}}{=}2+1=3.$$

定義 2.3. 集合 A の **帰納的定義** とは, A が以下のステップを踏んで得られる集合であるときをいう.

(I) はじめに, いくつかの要素は A に属すると定める. これらの要素を **基礎** という.

(II) A に属する要素を用いて, 新たに A に属する要素を決定する規則を定める. この規則を **帰納** と呼ぶ.

(III) A の要素は, (II) で定められる規則を施して得られるもののみであると定める. このルールを **限定（句）** と呼ぶ.

例 2-3 5 で割り切れる正の整数全体の集合 X は次のように帰納的に定義される.

(I) $5 \in X$.
(II) $(x \in X) \land (y \in X) \Longrightarrow x + y \in X$.
(III) 集合 X は, (I), (II) の手続きを繰り返し適用して得られる全ての要素だけからなる.

まず, 基礎によって $5 \in X$ である. 次に, $x = y = 5$ として (II) を適用すると $x + y = 10 \in X$ である. また, $x = 5$, $y = 10$ として (II) を適用すると $x + y = 15 \in X$ となる. 以下, このように繰り返していけば, $\{5n \mid n \in \mathbb{N}\} \subset X$ となる. 限定句の規則 (III) により, (I), (II) のルール以外のものは X に属さないので $X = \{5n \mid n \in \mathbb{N}\}$ である.

帰納的に定義されるアルゴリズムも存在する. これは, アルゴリズムの処理ステップで, 自身のアルゴリズムでの結果を参照するようなアルゴリズムである.

例 2-4 2 つの正の整数 x, y $(x \geq y)$ が与えられたとき, x と y の最大公約数は Euclid の互除法と呼ばれる次の手続きで求めることができる.

(i) r を, x を y で割った余りであると定義する.
(ii) $r = 0$ ならば, y を出力する.
(iii) $r \neq 0$ のとき, x に y を, y に r を代入して (i) に戻る.

例えば, $x = 3024$, $y = 1620$ として最大公約数を求めてみよう.

- $3024 \div 1620 = 1 \cdots 1404$ なので, $r = 1404$.
- $r \neq 0$ なので, $x = 1620$, $y = 1404$ として (i) に戻る.
- $1620 \div 1404 = 1 \cdots 216$ なので, $r = 216$.
- $r \neq 0$ なので, $x = 1404$, $y = 216$ として (i) に戻る.
- $1404 \div 216 = 6 \cdots 108$ なので, $r = 216$.
- $r \neq 0$ なので, $x = 216$, $y = 108$ として (i) に戻る.
- $216 \div 108 = 2$ なので, $r = 0$.
- $r = 0$ なので, 3024 と 1404 の最大公約数は 108 である.

小テスト 2-1 次の帰納的定義によって定義される集合 X の説明としてそれぞれ適切なものを選べ.

(1) (I) $1 \in X$.
(II) $x \in X \Longrightarrow x+3 \in X$.
(III) 集合 X は, (I), (II) の手続きを繰り返し適用して得られる全ての要素だけからなる.

(2) (I) $1 \in X$, $2 \in X$.
(II) $(x \in X) \wedge (y \in X) \Longrightarrow xy \in X$.
(III) 集合 X は, (I), (II) の手続きを繰り返し適用して得られる全ての要素だけからなる.

小テスト 2-2 次の問に答えよ.

(1) アッカーマン関数 $A(m,n)$ において, $A(3,1)$ の値を求めよ.

(2) 7539 と 22976 の最大公約数を Euclid の互除法を用いて以下のように求めた. このとき, (r_1, r_2, r_3) の組として最も適切な組み合わせを選べ.
- $22976 \div 7539 = 3 \cdots r_1$ なので, $r = r_1$ とおく.
- $7539 \div r = r_2$ である.
- よって, 22976 と 7539 の最大公約数は r_3 である.

演習問題 2-1 次の命題を数学的帰納法で証明せよ.

$$\forall n \in \mathbb{N}, \quad \sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$$

演習問題 2-2 次にように帰納的に定義されている関数 f に対して, $f(3)$, $f(4)$, $f(5)$ を求めよ.

$$f(0) = -1, \quad f(1) = 2, \quad f(n+1) = \frac{f(n-1)}{f(n)} + f(n)$$

演習問題 2-3 長さ n のビット列とは, 0 および 1 だけからなる n 文字列である, 例えば, 01 は長さ 2 のビット列, 111 は長さ 3 のビット列という具合である. 集合 B を, 00 というビット列を含まないようなビット列全体の集合とする. 例えば, $10110 \in B$ であるが, $10010 \notin B$ である. 長さ 0 のビット列を空文といい, ε で表す. $\varepsilon \in B$ であるとする. このとき, 以下の問に答えよ.

(1) 集合 B を, 含まれているビット列の長さ n について帰納的に定義せよ.

(2) B に属する長さ n のビット列全体の集合を $B(n)$ をおく. $|B(0)|$, $|B(1)|$, $|B(2)|$, $|B(3)|$, $|B(4)|$ を求めよ.

- **2-A：Euclid の互除法の証明**

Euclid の互除法が成り立つことを証明しておこう.

定理 (Euclid の互除法)**.** $a, b \in \mathbb{N}$ を $a \geq b$ とする. a を b で割った余りを r とおくと, a と b の最大公約数は b と r の最大公約数に等しい.

証明. a を b で割った商を q, 余りを r とすると $a = bq + r$ とかける. a と b の最大公約数を g_1, b と r の最大公約数を g_2 とおく. すると, ある整数 $x, y \in \mathbb{Z}$ が存在して $a = xg_1$, $b = yg_1$ と表せるので,

$$r = a - bq = xg_1 - yg_1 q = g_1(x - yq)$$

となり, g_1 は r の約数である. 従って, g_1 は b と r の公約数である. 一方, g_2 が b と r の最大公約数なので, $g_1 \leq g_2$ である.

逆の不等号 $g_2 \leq g_1$ を示そう. g_2 は b と r の公約数なので, ある整数 $z, w \in \mathbb{Z}$ が存在して $b = zg_2$, $r = wg_2$ と表せるので,

$$a = bq + r = zg_2 q + wg_2 = g_2(zq + w)$$

となり, g_2 は a の約数である. 従って, g_2 は a と b の公約数であるから, $g_2 \leq g_1$ が成り立つ.

以上で, $g_1 = g_2$ となることが示された. □

自然数 a, b $(a \geq b)$ に対して, a を b で割った余りを r とすれば, 必ず $0 \leq r < b$ となるので, Euclid の互除法のアルゴリズムは必ず有限回で終了する.