

論理的思考法を身につけるための数学

1. 序

論理的思考法を身につけることは、現在の情報溢れの社会で生き残るための、必要条件である。論理的思考には、狭い意味の記号論理から、広い意味の、説得のための弁論法や、人の言うことを鵜呑みにしないための批判的思考法まで、色々な意味がある。しかし、厳密な論理展開は、基礎能力として確りと身につけるべきである。

厳密な論理展開を身につける手段として、数学の証明を学ぶことは、有効である。パースが指摘したように、数学は、前提になるものが、数学の世界だけであるので、論理の正しさを厳密に定義できる。このように、とりあえず理想的な世界で、議論する手法を身につけてから、複雑な一般世界での議論に応用を拡げるべきである。

数学にも、色々な分野がある。従来は、論理的な証明と言えば、ユークリッド以来の伝統ある幾何学で学ぶことが多かった。しかし、ここでは整数論を例にとる。整数論は、検討対象が誰もが使っている **1,2,3** などの数値であるので、勉強していてもイメージがわきやすい。そして、今まで直感的に使っていた整数の性質にも、きちんとした証明があるということを知ることが、思考方法の改善に効果大である。

なお、整数論の勉強の手法は以下のとおりである。

- 1) データを集める。具体的な数値が多いが、抽象的なものもある。
- 2) データを調べてパターンや関係性を見出す。
- 3) パターンや関係式を説明できる予想を式にする。
- 4) 更にデータを集めて予想を確かめ、予想にあうことを確認する。
- 5) 予想が正しいことを示す根拠を示す。(証明する)
- 6) できるならば応用事例に適用する

1)~3)までの段階で、比較的具体的な例から一般的な、規則を見出すのは帰納的な思考法である。一方、5)の段階で、公理や既知の定理から証明するのは、演繹的な思考法である。なお、数学的帰納法と言うのは、数値の順序的な構造を使った、演繹的な手法であり、証明段階でよく使っている。

2. 初等整数論の証明例

2-1 記号の説明

$\mathbf{N} = \{1, 2, 3, \dots\}$ 自然数全体の集合

$\mathbf{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ 整数全体の集合

\mathbf{N} を 0 とマイナスの数値にまで拡張したもの。

$\mathbf{Q} = \{n/m \mid m, n \in \mathbf{Z}, n \neq 0\}$ 有理数全体の集合

\mathbf{N} を分数の世界まで拡張し、四則演算が全てできるようにした。

\mathbf{R} = 実数全体の集合

有理数と有理数の間には、無限に多くの無理数がある。

$\mathbf{C} = \{a+b\sqrt{-1} \mid a, b \in \mathbf{R}\}$ 複素数全体の集合

複素数の世界で、方程式の解は全て求めることができる。

2-2 割り算議論

整数の割り算は、通常割り切れないので、商と余りが出る。このことを厳密に議論してみよう。

例えば $30 \div 7 = 4 \cdots (\text{余り})2$

まず、自然数の性質として、大小関係と、正の最小整数の存在を公理として述べておく。例えば、2 より大きい自然数ならば、最小値の 3 がある。

公理 1 \mathbf{N} の空でない部分集合には、最小の正の整数がある

この結果、自然数の部分集合は、無限に小さくなる数列は存在しない。

次に、議論を便利にするための定義を行う。

定義 2 $a (\neq 0), b$ を整数とする。 $ax = b$ をみたす $x \in \mathbf{Z}$ があるとき a は b の約数である。あるいは b は a の倍数である。このとき $a \mid b$ とあらわす。

そして、整数の割り算について、厳密な議論を行う。

定理 3(整数の除法の定理)

任意の整数 a と自然数 b に対して、

$$a = bq + r, 0 \leq r < b$$

を満たす整数 q, r がただ一組決まる。これは

「 a を b で割ると商 q と余り r が決まり、余り r は割る数 b よりも小さくなる。」

を数式で表現したものである。

[証明]

q を有理数 a/b 以下の最大の整数とする。このような数は、公理 1 で存在することが保証されている。r = a - bq とおく。このとき a = bq + r が成立する。q の取り方から

a/b - 1 < q ≤ a/b であるが、b > 0 と合わせて a - b < bq ≤ a を得る。これから 0 ≤ r = a - bq < b を得る。

次に q, r の一意性を示す。a = bq' + r' (0 ≤ r' < b) と書けたとする。ここで、前の式からこの式を引くと b(q - q') + (r - r') = 0 となる。ここで、|r - r'| の絶対値は b より小さいから、b(q - q') は絶対値が b より小さい b の倍数となり、b(q - q') = 0 しかありえない。従って、q = q' となり、r = r' となる。

[証明終]

2-3 最大公約数

次に 2 つの数の共通の約数、特に最大のものを考えてみる。

定義 4 公約数、最大公約数、互いに素

a1, a2, ..., an を 0 でない整数とする。1 ≤ i ≤ n の全てに対して、d | ai を満たす整数 d を a1, a2, ..., an の公約数と言う。さらに a1, a2, ..., an の正の公約数 d が a1, a2, ..., an の任意の公約数 c に対して c | d を満たすとき、d を a1, a2, ..., an の最大公約数と言い gcd(a1, a2, ..., an) または (a1, a2, ..., an) とあらわす。gcd(a1, a2, ..., an) = 1 のとき a1, a2, ..., an は互いに素であると言う。

例えば、30 と 18 の最大公約数は、6 である。一方、31 と 18 は互いに素である。

定理 5(ユークリッドの互除法) a, b を正の整数とする。a0 = a、a1 = b とおき、N ≥ 1 に対し

a_{n-1} = a_n q_n + a_{n+1} (1)

0 ≤ a_{n+1} < a_n (2)

で数列 {a_n} を定義する。つまり a_{n-1} を a_n で割った余りが a_{n+1} となる。この時ある自然数 N があって a_{N+1} = 0 となり、

a_N = gcd(a, b)

が成立する。

[証明] まず(1)式が成立すると、(a_{n-1}, a_n) = (a_n, a_{n+1}) を示す。

d = (a_{n-1}, a_n)、d' = (a_n, a_{n+1})

とする。d | a_{n-1}, d | a_n だから (1) より d | a_{n+1}。従って、d は a_n, a_{n+1} の公約数であり、最大公約数の定義から、d | d' である。同様に d' | d も言えるので d = d' となる。これを繰り返し使うと、公約数は保存されているが (2) より {a_n} は単調減少するので有限回で 0 となる。これを N + 1 とすると、a_{N-1} = a_N q_N が成立し、(a_{N-1}, a_N) = a_N となる。

上と合わせて

(a, b) = a_N

である。

[証明終]

[計算例]

a_0 = 30、a_1 = 18 で考える。

30 = 18 × 1 + 12

18 = 12 × 1 + 6

12 = 6 × 3

[例終]

2-4 素数

整数論の中で、1 とそれ自身しか約数が無い素数は、重要な役割を果たす。

定義 6(素数) 2 より大きくて、1 とそれ自身しか約数が存在しない、正の自然数を、素数と言う。

2, 3, 5, 7, 11, 13, 17, 19, 23... は素数である。このような素数が、無数に多く存在することは、簡単に証明できる。

定理 7 無限に多くの素数が存在する

[証明] p_1 = 2 < p_2 = 3 < ... < p_r が素数の全てと仮定する。

P = p_1 p_2 ... p_r + 1

とし、P を割り切る素数を、p とする。p は、p_1, p_2, ..., p_r のいずれも割り切ることにはできない。そうでないと、p は P - p_1 p_2 ... p_r = 1 を割り切ることになり矛盾する。従って、p_1, p_2, ..., p_r が素数の全てと言う仮定は間違っており。素数は無限に存在する。

[証明終]

この証明では、 p_r が最大の素数と仮定したことが、矛盾を呼んでいる。この場合、最大の素数が存在するか、それより大きい素数が無限に存在するかは、どちらかしかないので、この証明方法に問題は無い。なお、このような P は全て素数になるのではと考えるかもしれないが、 P は p_r より十分大きいので、その間に素数が介在している。

例えば、11 が最大の素数と仮定すると

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 \cdots \text{これは素数}$$

しかし、13 を最大と仮定するならば

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30043 = 59 \times 509$$

と 59 という比較的大きい約数が見つかる。

素数の大切な役割は、以下に示すように任意の数を、素数の組み合わせで示すことである。

例えば

$$60 = 2^2 \times 3 \times 5$$

と言う形に表現できる。

定理 8 算術の基本定理 全ての $n \geq 2$ の整数は素数の積

$$n = p_1 p_2 \cdots p_r$$

に、順序の違いを除いて一意的に分解できる。

[証明]この中には2つの主張がある

主張# 1 整数 n は素数の積に表すことが可能である

主張# 2 そのような分解は一通りである

主張# 1 の証明

帰納法で証明する。まず、 $2=2, 3=3, 4=2^2, 5=5$ と分解できる。次に、数 N までに主張# 1 までに証明されているとする。全ての整数 $n \leq N$ に対して素数の積に分解できているとする。次に $N+1$ について考える。

可能性第1は、 $N+1$ が素数の場合である。この場合は、それ自身が素数の積である。

可能性第2は、合成数の場合である。この場合には2つの整数

$$2 \leq n_1, n_2 \leq N \text{ が存在し、}$$

$$N+1 = n_1 n_2$$

と表せる。 $n_1 n_2$ は両者とも N 以下なので、主張# 1 が成立する。従って、 n_1 と n_2 は素数の積で表すことができ、これを掛け合わせて $N+1$ は素数の積

に分解できる。

主張# 2 の証明

整数 n が2通りの素数の積に表されているとする。

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

このような分解は一通りであることを示す。まず、 $p_1 | q_1 q_2 \cdots q_s$ と言う事実から始める。このように素数で割る時には、どれかの素数を割り切る必要がある。つまり $q_1 q_2 \cdots q_s$ のどれか一つを割り切る。これを、番号付けを替えて、 q_1 とする。この時、素数の性質より $p_1 = q_1$ である。従って式の両辺から $p_1 = q_1$ を消去する。

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

これを繰り返して、 p_i が全てなくなるまで続ける。この時、左辺が1になるので、 q_i が残ることは不可能である。つまり、 p と q の個数は同じである。以上をまとめると、素数の積への分解は、素数の個数は同じであり、それぞれの番号を付け替えることで、全ての素数が同じにすることができる。つまり、分解的は一意的である。

[証明終わり]