

p 進数の初歩

2017 年 4 月 11 日

1 導入

次の式を見てください．

$$\begin{aligned}-1 &= 1 + 2 + 2^2 + 2^3 + 2^4 + \dots \\ -1/2 &= 1 + 3 + 3^2 + 3^3 + 3^4 + \dots \\ \sqrt{-1} &= 2 + 5 + 2 \cdot 5^2 + 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + \dots\end{aligned}$$

実数や複素数として考えるとこの式は間違いです．なぜなら右辺は $+\infty$ に発散するからです．しかし， p 進数の世界ではこれらは完全に正しい式です．一つ目は 2 進数，二つ目は 3 進数，三つ目は 5 進数として成り立ちます．

p 進数とはなんでしょうか．一言でいえば p 進数の全体 \mathbb{Q}_p は有理数全体 \mathbb{Q} を p 進距離と呼ばれる距離によって完備化した空間であり，それに四則演算の構造を入れたものです．ここに p は素数です．

つまり，各素数 p ごとに実数とは異なる数の世界 \mathbb{Q}_p があるのです．各 \mathbb{Q}_p は \mathbb{Q} を含んでいます．

$$\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7, \mathbb{Q}_{11}, \dots \supset \mathbb{Q} \subset \mathbb{R}$$

これから \mathbb{Q}_p を定義し，その性質を見ていきます．この発表が終わる頃には皆さんに最初の 3 つの式を納得していただけるだろうと期待しています．

2 p 進数の定義

p 進数を定義するには， p 進距離を導入する必要があります．そこでまず，数学でいう距離とは何なのか定義します．

定義 1 (距離空間). X を集合， d を $X \times X$ から \mathbb{R} への写像とする．任意の $x, y, z \in X$ について次を満たすものとする．

1. $d(x, y) \geq 0$
2. $d(x, y) = 0 \iff x = y$
3. $d(x, y) = d(y, x)$

$$4. d(x, z) \leq d(x, y) + d(y, z)$$

このとき, d を X 上の距離関数という.

また (X, d) あるいは単に X を距離空間という.

たとえば, \mathbb{R} で $d(x, y) = |x - y|$ と定義すると (\mathbb{R}, d) は距離空間です. 確認しましょう. この距離関数 d をユークリッド距離といい, (\mathbb{R}, d) をユークリッド空間といいます. ユークリッド距離関数を有理数に制限した関数も d と書くことにすると (\mathbb{Q}, d) も距離空間です.

同じ集合でも距離の入れ方は一つとは限りません. 実際, これから \mathbb{Q} に $|x - y|$ とは異なる p 進距離 d_p を定めます.

以下 p を素数とします.

定義 2 (p 進付値). 整数 $n \neq 0$ の素因数分解を

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

とする. このとき n の p 進付値を

$$v_p(n) = \begin{cases} e_i & (\exists i, p = p_i) \\ 0 & (\text{otherwise}) \end{cases}$$

で定める.

有理数 $x = m/n$ ($m, n \in \mathbb{Z}, m, n \neq 0$) の p 進付値を

$$v_p(x) = v_p(m) - v_p(n)$$

で定める. (これは well-defined である)

定義 3 (p 進絶対値). 有理数 $x \neq 0$ の p 進絶対値を

$$|x|_p = p^{-v_p(x)}$$

で定める. 0 に対しては

$$|0|_p = 0$$

と定める.

定義 4 (p 進距離). 有理数 x, y の p 進距離を

$$d_p(x, y) = |x - y|_p$$

で定める.

p 進距離が距離関数になることは確認する必要があります.

しかし, その前に p 進距離がどういう距離か説明します. p 進距離は p でたくさん割れれば割れるほど 0 に近いという距離です. 実際,

$$\begin{aligned}d_2(1, 0) &= 1 \\d_2(2, 0) &= 1/2 \\d_2(4, 0) &= 1/4 \\d_2(8, 0) &= 1/8 \\&\vdots\end{aligned}$$

となります.

命題 5. 任意の $a, b \in \mathbb{Q}$ について

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$

証明. 1 は指数法則から直ちにいえる. 2 は $v_p(a) = e, v_p(b) = e', e \leq e'$ とするとき, $a = p^e n, b = p^{e'} n'$ (n, n' は p と互いに素) と書け,

$$a + b = p^e(n + p^{e'-e}n')$$

となることからわかる. $e > e'$ のときも同様. □

命題 6. 任意の $a, b \in \mathbb{Q}$ について

1. $|a|_p \geq 0$
2. $|a|_p = 0 \iff a = 0$
3. $|ab|_p = |a|_p |b|_p$
4. $|a + b|_p \leq \max\{|a|_p, |b|_p\}$

証明. 1 と 2 は明らかである. 3 と 4 は命題 5 から従う. □

命題 6 の 4 を p 進絶対値の非アルキメデス性といいます.

定理 7. d_p は \mathbb{Q} 上の距離関数である .

証明. 非負値性は命題 6 の 1 より , 非退化性は命題 6 の 2 より従う . 6 の 3 で $a = b = -1$ とすれば $|-1|_p = 1$ を得る . そこで $|-a|_p = |a|_p$ となる . ここから d の対称性が従う . $x, y, z \in \mathbb{Q}$ とするとき命題 6 の 4 において $a = x - y, b = y - z$ とおけば三角不等式より強い次の不等式

$$d(x, z) \leq \max\{d(x, y), d(y, z)\}$$

が得られる . □

問. p が素数でないときも整数 x に対して $v_p(x)$ を

$$v_p(x) = \max\{k \geq 0 \mid x \text{ は } p^k \text{ で割り切れる} \}$$

のように定義できる . このとき同じようにして得られる d_p は距離関数にならない . どこでうまくいかないのか .

\mathbb{Q}_p は \mathbb{Q} を p 進距離によって完備化した空間だと述べました . そこで完備化を説明する必要があります . そのために , 点列の収束 , コーシー列 , 完備性という概念を説明します .

定義 8 (点列の収束). (X, d) を距離空間 , $\{x_n\}_{n \in \mathbb{N}}$ を X の点の列とする . このとき $\alpha \in X$ が存在して

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq N \Rightarrow d(x_n, \alpha) < \epsilon$$

を満たすとき , X の点列 $\{x_n\}_{n \in \mathbb{N}}$ は α に収束するといい ,

$$\lim_{n \rightarrow \infty} x_n = \alpha$$

と書く .

定義 9 (コーシー列). (X, d) を距離空間 , $\{x_n\}_{n \in \mathbb{N}}$ を X の点の列とする .

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq N \Rightarrow d(x_n, x_N) < \epsilon$$

を満たすとき , $\{x_n\}_{n \in \mathbb{N}}$ はコーシー列であるという .

定義より収束列は明らかにコーシー列です .

例. X の任意の距離空間 , $x \in X$ を任意の点としたとき点列 $\{x, x, x, \dots\}$ つまり $x_n = x (\forall n \in \mathbb{N})$ は x に収束する . 実際 , 任意の $\epsilon > 0$ に対して $N = 1$ とすれば $n \geq 1$ のとき $d(x_n, x) = d(x, x) = 0 < \epsilon$. 特にこの点列はコーシー列である .

例. \mathbb{R} をユークリッド空間, $x_n = 1/n$ とするとこれは 0 に収束する. 実際, 任意の $\epsilon > 0$ に対して N を $1/\epsilon$ より大きい自然数とおけば, $n \geq N$ のとき $d(1/n, 0) = 1/n \leq 1/N < \epsilon$. 特にこの点列はコーシー列である.

例. \mathbb{R} をユークリッド空間, $x_n = n$ とするとこれはコーシー列ではない. 実際, 任意の $N \in \mathbb{N}$ に対して $n = N + 1$ とおけば $d(x_N, x_n) = |N - (N + 1)| = 1 \geq 1$. 特にこの点列は収束列でない.

例. d_p を p 進距離として距離空間 (\mathbb{Q}, d_p) を考えると, $x_n = p^n$ は 0 に収束する. 実際, 任意の $\epsilon > 0$ に対して $p^{-N} < \epsilon$ となるよう N をとると, $d_p(p^n, 0) = p^{-n} \leq p^{-N} < \epsilon$ となる.

例. d をユークリッド距離として距離空間 (\mathbb{Q}, d) を考え, 点列

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 1.4 \\ a_3 &= 1.41 \\ a_4 &= 1.414 \\ a_5 &= 1.4142 \\ &\vdots \end{aligned}$$

を考える. この点列はコーシー列だが収束列ではない. (空間を \mathbb{R} とすれば当然 $\sqrt{2}$ に収束する)

問. p と q を異なる素数とするととき (\mathbb{Q}, d_p) において $\{q^n\}$ はコーシー列でないことを示せ.

定義 10 (完備). (X, d) を距離空間とする. X の任意のコーシー列が収束するとき X は完備であるという.

たとえば d をユークリッド距離とすると (\mathbb{R}, d) は完備ですが, (\mathbb{Q}, d) は完備ではありません.

定義 11 (稠密性). (X, d) を距離空間とする. $S \subset X$ が次の条件を満たすとき, S は X において稠密であるという.

$$\forall x \in X, \forall \epsilon > 0, \exists y \in S, d(x, y) < \epsilon$$

S が X において稠密であることは任意の $x \in X$ に対して S の元の列 $\{x_n\}$ であって x に収束するものが存在することと同値です.

完備ではない距離空間も, それに点を付け加えて完備にすることができます. すなわち次が成立します.

定理 12 (完備化). (X, d) を距離空間とする. このとき距離空間 (\tilde{X}, \tilde{d}) であって次を満たすものがある.

1. $X \subset \tilde{X}$
2. \tilde{d} の $X \times X$ への制限は d に等しい

3. \tilde{X} は完備である
4. X は \tilde{X} において稠密である

(\tilde{X}, \tilde{d}) を (X, d) の完備化という .

証明の概略 . X のコーシー列全体を $C(X)$ と書き , $C(X)$ に次の同値関係を入れる .

$$\{x_n\} \sim \{y_n\} \iff \forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq N \Rightarrow d(x_n, y_n) < \epsilon$$

そして $\tilde{X} = C(X)/\sim$ とおく . また

$$\tilde{d}(\{x_n\}, \{y_n\}) = \lim_{n \rightarrow \infty} d(x_n, y_n)$$

とおく . このとき (\tilde{X}, \tilde{d}) が定理の条件を満たす .

なお , X の元 x にコーシー列 $\{x, x, x, \dots\} \in C(X)$ を対応させることで X を \tilde{X} の部分集合だとみなす . (証明の概略終わり)

実は , (\mathbb{Q}, d) を完備化したものが (\mathbb{R}, d) なのであります .

定義 13. (\mathbb{Q}, d_p) の完備化を $(\mathbb{Q}_p, \tilde{d}_p)$ と書く .

これで距離空間としての \mathbb{Q}_p は定義されました . \mathbb{Q}_p の元のことを p 進数といいます . しかし四則演算がまだ定義されていません . 四則演算 (のうち和 ・ 差 ・ 積) は次のように定義します .

定義 14. \mathbb{Q}_p に和 ・ 差 ・ 積を次のように定義する .

$\tilde{x}, \tilde{y} \in \mathbb{Q}_p$ に対して \mathbb{Q} の点列 $\{x_n\}, \{y_n\}$ で $x_n \rightarrow \tilde{x}, y_n \rightarrow \tilde{y} (n \rightarrow \infty)$ となるものをとる . このとき

$$\tilde{x} + \tilde{y} = \lim_{n \rightarrow \infty} (x_n + y_n)$$

$$\tilde{x} - \tilde{y} = \lim_{n \rightarrow \infty} (x_n - y_n)$$

$$\tilde{x}\tilde{y} = \lim_{n \rightarrow \infty} (x_n y_n)$$

と定める .

これらは well-defined です . たとえば和の場合 , $\{x_n\}, \{y_n\}$ が収束するとき $\{x_n + y_n\}$ も収束します . また , \tilde{x}, \tilde{y} に対してそれに収束する $\{x_n\}, \{y_n\}$ の取り方は無数にありますが , その取り方によらず $\lim_{n \rightarrow \infty} (x_n + y_n)$ の値は定まります .

問. このことを示せ .

こうして定義した演算に関して \mathbb{Q}_p は環になります .

定義 15 (環). 集合 A とその上の二項演算 $+, \cdot$ について, 元 $0, 1 \in A$ が存在して次を満たすとき $(A, +, \cdot)$ あるいは単に A を環という.

任意の $x, y, z \in A$ に対して

1. $0 + x = x$
2. $\exists x' \in A, x + x' = 0$
3. $x + (y + z) = (x + y) + z$
4. $x + y = y + x$
5. $1 \cdot x = x$
6. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
7. $x \cdot y = y \cdot x$
8. $x \cdot (y + z) = x \cdot y + x \cdot z$

\mathbb{Q}_p は環であるだけでなく体でもあります.

定義 16 (体). 集合 K が環であって次を満たすとき K を体という.

任意の $x \in A, x \neq 0$ に対して $x \cdot x' = 1$ となる $x' \in K$ がある.

定理 17. \mathbb{Q}_p は体である.

証明. 環であることは \mathbb{Q} が環であることと, \mathbb{Q}_p の演算の定義より出る. たとえば結合法則 $\tilde{x} + (\tilde{y} + \tilde{z}) = (\tilde{x} + \tilde{y}) + \tilde{z}$ は \mathbb{Q} の点列 $\{x_n\}, \{y_n\}, \{z_n\}$ で $x_n \rightarrow \tilde{x}, y_n \rightarrow \tilde{y}, z_n \rightarrow \tilde{z} (n \rightarrow \infty)$ となるものをとるとき

$$\begin{aligned}\tilde{x} + (\tilde{y} + \tilde{z}) &= \lim_{n \rightarrow \infty} (x_n + (y_n + z_n)) \\ &= \lim_{n \rightarrow \infty} ((x_n + y_n) + z_n) \\ &= (\tilde{x} + \tilde{y}) + \tilde{z}\end{aligned}$$

というように示せる.

任意の 0 でない元 \tilde{x} について \tilde{x}' が存在して $\tilde{x}\tilde{x}' = 1$ となることは, $\tilde{x}' = \lim_{n \rightarrow \infty} 1/x_n$ とおけば示せる. (ただしこの極限が存在することを示す必要がある) □

\mathbb{Q} に定義されていた p 進絶対値を \mathbb{Q}_p に拡張します.

定義 18. $\tilde{x} \in \mathbb{Q}_p$ に対して

$$|\tilde{x}|_p = \tilde{d}_p(\tilde{x}, \tilde{0})$$

と定める .

命題 19. 任意の $\tilde{a}, \tilde{b} \in \mathbb{Q}_p$ について

1. $|\tilde{a}|_p \geq 0$
2. $|\tilde{a}|_p = 0 \iff \tilde{a} = \tilde{0}$
3. $|\tilde{a}\tilde{b}|_p = |\tilde{a}|_p |\tilde{b}|_p$
4. $|\tilde{a} + \tilde{b}|_p \leq \max\{|\tilde{a}|_p, |\tilde{b}|_p\}$

証明. 1 と 2 は定義より出る . 3 と 4 は命題 6 の 3 と 4 の極限をとればよい . □

\mathbb{Q}_p において , 和 , 差 , 積 , 商は連続写像になります . このことの証明は省きます .

定義 20. $\mathbb{Z}_p = \{\tilde{x} \in \mathbb{Q}_p \mid |\tilde{x}|_p \leq 1\}$ と定め , \mathbb{Z}_p の元を p 進整数という .

命題 19 より $0, 1$ は p 進整数であり p 進整数同士の和 , 差 , 積は p 進整数となります . よって \mathbb{Z}_p は環となります .

なお「 p 進数」と「 p 進法」は異なる概念であることに注意しましょう . p 進数は \mathbb{Q}_p の元のことですが , p 進法は実数を p を底として小数表示することを言います .

3 p 進数の性質

以降 , \tilde{d}_p をチルダなしの d_p で書き , \mathbb{Q}_p の元も \tilde{x} ではなく x のような文字を使います .

今 , 等比数列の和の公式より

$$(1 - p^{n+1})/(1 - p) = 1 + p + p^2 + \cdots + p^n$$

です . \mathbb{Q}_p において両辺を $n \rightarrow \infty$ とすると $p^{n+1} \rightarrow 0$ なので ,

$$1/(1 - p) = 1 + p + p^2 + \cdots$$

となります . ここに $p = 2, 3$ を代入すると最初の 3 つの式のうちの二つ

$$\begin{aligned} -1 &= 1 + 2 + 2^2 + 2^3 + 2^4 + \cdots \text{ (in } \mathbb{Q}_2\text{)} \\ -1/2 &= 1 + 3 + 3^2 + 3^3 + 3^4 + \cdots \text{ (in } \mathbb{Q}_3\text{)} \end{aligned}$$

が示せました !

非アルキメデス性から次の重要な事実が出ます .

命題 21. $\{a_n\}$ を \mathbb{Q}_p の点列とする . このとき

$$\sum_{n=1}^{\infty} a_n \text{ が収束 } \iff \lim_{n \rightarrow \infty} a_n = 0$$

証明. \Rightarrow は \mathbb{R} のときと同じ証明でよい .

$$\Leftarrow) |a_{m+1} + a_{m+2} + \dots + a_n|_p \leq \max\{|a_{m+1}|_p, |a_{m+2}|_p, \dots, |a_n|_p\} \text{ より出る .}$$

□

命題 21 から次の事実が従います .

命題 22. $k \in \mathbb{Z}$, $a_k, a_{k+1}, \dots \in \mathbb{Z}$, $0 \leq a_i < p-1$ のとき級数

$$\sum_{i=k}^{\infty} a_i p^i \tag{1}$$

は \mathbb{Q}_p において収束する .

$k=0$ である場合 , $\sum_{i=0}^{\infty} a_i p^i$ を $(\dots a_3 a_2 a_1 a_0)_{(p)}$ と書きます . たとえば $-1 = (\dots 1111)_{(2)}$.

\mathbb{Q}_p の元が式 (1) のように表せるとき , その表示を p 進展開といいます .

\mathbb{Q} の元は p 進展開可能であることを見ましょう .

a を p と互いに素な整数とします . このとき初等整数論 (あるいは初等群論) の事実より

$$p^k \equiv 1 \pmod{a}$$

となる $k \in \mathbb{N}$ が存在します . すると

$$p^k - 1 = ab$$

です . これを変形すると

$$\begin{aligned} \frac{1}{a} &= \frac{-b}{1 - p^k} \\ &= -b(1 + p^k + p^{2k} + \dots + p^{nk} + \dots) \end{aligned}$$

となります . $-b$ も p 進展開して積を計算すれば $1/a$ の p 進展開が得られます .

例. $1/5$ の 2 進展開を求める . $2^4 - 1 = 15 = 3 \cdot 5$ である .

$$\begin{aligned} \frac{1}{5} &= \frac{-3}{1 - 2^4} \\ &= -3(1 + 2^4 + 2^8 + \dots + 2^{4n} + \dots) \\ &= -(1 + 2)(1 + 2^4 + 2^8 + \dots + 2^{4n} + \dots) \\ &= -(1 + 2^1 + 2^4 + 2^5 + 2^8 + 2^9 + \dots) \\ &= -(\dots 00110011)_{(2)} \\ &= (\dots 11001101)_{(2)} \\ &= 1 + 2^2 + 2^3 + 2^6 + 2^7 + 2^{10} + 2^{11} + \dots \end{aligned}$$

この例から任意の \mathbb{Q} の元は p 進展開可能であることが推察できます .
 実は次の事実が知られています .

定理 23. 任意の \mathbb{Q}_p の元 ($\neq 0$) は一意的に p 進展開可能 . つまり任意の $x \in \mathbb{Q}_p - \{0\}$ について $k \in \mathbb{Z}$, $a_k, a_{k+1}, \dots \in \mathbb{Z}$, $0 \leq a_i < p-1$, $a_k \neq 0$ が一意的に存在して

$$x = \sum_{i=k}^{\infty} a_i p^i$$

となる . このとき $|x|_p = p^{-k}$.

証明はしません . 証明の鍵となるものは

- p 進絶対値の離散性
- \mathbb{Q} が \mathbb{Q}_p において稠密であること

です .

4 ヘンゼルの補題

定理 24 (ヘンゼルの補題). $F(x)$ を整数係数の多項式 , $x_0 \in \mathbb{Z}$ とする . $\delta_1 = v_p(F(x_0))$, $\delta_2 = v_p(F'(x_0))$ とおく . もし , $\delta_1 > 2\delta$ ならば , $x \in \mathbb{Z}_p$ があり $F(x) = 0$.

証明はしない .

この x は次のように構成される:

$$x_{n+1} = x_n - \frac{F(x_n)}{F'(x_n)}$$

として

$$x = \lim_{n \rightarrow \infty} x_n.$$

しかし , この構成法では , 近似値 x_n は有理数である . 近似値 x_n が整数となるような構成法もあり , 次のようにする .

$$\begin{aligned} F'(x_n) &= p^{\delta_2} y_n \\ y_n z_n &\equiv 1 \pmod{p} \\ x_{n+1} &= x_n - \frac{F(x_n)}{p^{\delta_2}} z_n \end{aligned}$$

として

$$x = \lim_{n \rightarrow \infty} x_n.$$

特に x_n の p 進展開は x の p 進展開と $\delta_1 - \delta_2 + n$ 桁まで一致する .

ヘンゼルの補題を使って, $F(x) = x^2 + 1$ の根 (すなわち $\sqrt{-1}$) が \mathbb{Z}_5 の中にあることを確認して, その p 進展開を求めましょう.

$F(x) = x^2 + 1$ より, $F'(x) = 2x$. $x_0 = 2$ とおけば, $F(2) = 5, F'(2) = 4$ より, $\delta_1 = v_5(F(2)) = 1, \delta_2 = v_5(F'(2)) = 0$. よって定理の仮定を満たします.

$y_0 = 4, z_0 = -1$ であり, $x_1 = 2 - 5 \cdot (-1) = 7 = (12)_{(5)}$.

$y_1 = 14, z_0 = -1$ であり, $x_2 = 7 - 50 \cdot (-1) = 57 = (212)_{(5)}$.

$y_2 = 114, z_0 = -1$ であり, $x_3 = 57 - 3250 \cdot (-1) = 3307 = (101212)_{(5)}$.

$y_2 = 6614, z_0 = -1$ であり, $x_3 = 3307 - 10936250 \cdot (-1) = 10939557 = (10300031212)_{(5)}$.

よって $\sqrt{-1} = (\dots 31212)_{(5)}$ です. 実際に筆算して確かめましょう.

問. \mathbb{Q}_p において $\sqrt[3]{-2}$ すなわち $x^3 + 2$ の根が存在するような p を一つ見つけよ.

参考文献

- [1] 彌永昌吉・彌永健一『集合と位相』岩波書店
- [2] 雪江明彦『整数論 1 初等整数論から p 進数へ』日本評論社