

p 進数の初歩

2017 年 4 月 7 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 進数とはなんのでしょうか。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{Q} で $d(x, y) = |x - y|$ と定義すると (\mathbb{Q}, d) は距離空間です。確認しましょう。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 指数). 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 指数を

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

で定める。

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

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

で定める。(これは well-defined である)

定義 3 (p 進付値). 有理数 $x \neq 0$ の p 進付値を

$$v_p(x) = p^{-e_p(x)}$$

で定める。0 に対しては

$$v_p(0) = 0$$

と定める。

定義 4 (p 進距離). 有理数 x, y の p 進距離を

$$d_p(x, y) = v_p(x - y)$$

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、

$$d_2(1, 0) = 1, d_2(2, 0) = 1/2, d_2(4, 0) = 1/4, d_2(8, 0) = 1/8 \dots$$

となります。

命題 5. 任意の $a, b \in \mathbb{Q}$ について

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

証明. あとで

□

命題 6. 任意の $a, b \in \mathbb{Q}$ について

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

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 が成り立つことを v_p は非アルキメデスの付値であるといいます。

定理 7. d_p は \mathbb{Q} 上の距離関数である。

証明. あとで

□

\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。しかし逆は成り立つとは限りません。

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。

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。

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

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。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} 上稠密である

(\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。 \square

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。

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 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

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

このように示せる。

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) \square

\mathbb{Q} に定義されていた p 進付値を \mathbb{Q}_p に拡張します。

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

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

と定める。

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

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

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。 \square

\tilde{v}_p のことも p 進付値と言います。

\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. $\mathbb{Z}_p = \{\tilde{x} \in \mathbb{Q}_p \mid \tilde{v}_p(\tilde{x}) \leq 1\}$ 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。

3 p 進数の性質

以降、 \tilde{d}_p, \tilde{v}_p をチルダなしの d_p, v_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

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

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、

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

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

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

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 $v_p(a_{m+1} + a_{m+2} + \dots + a_n) \leq \max\{v_p(a_{m+1}), v_p(a_{m+2}), \dots, v_p(a_n)\}$ 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 (2) 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

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

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。

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

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 $k \in \mathbb{Z}$, $a_k, a_{k+1}, \dots \in \mathbb{Z}$, $0 \leq a_i < p - 1$, $a_k \neq 0$ が一意に存在して

$$x = \sum_{i=k}^{\infty} a_i p^i \quad (2)$$

となる。このとき $v_p(x) = p^{-k}$ 。

証明はしません。証明の鍵となるものは

- p 進付値の離散性
- \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

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