

p 進数について (後半)

2021 年 5 月 15 日

1 復習

定義 1.1 (再掲). p を素数とする. $x \in \mathbb{Q}$ に対し, $|x|_p$ を以下で定める:

(1) $x = 0$ のとき, $|0|_p = 0$ と定める.

(2) $x \neq 0$ のとき, $x = p^\ell \frac{a}{b}$ ($\ell, a, b \in \mathbb{Z}$, ただし, a, b は p で割り切れない.) と表す. このとき, $|x|_p = p^{-\ell}$ と定義する.

$|x|_p$ を x の p 進ノルムと呼ぶ.

$$\text{例: } \left| \frac{36}{5} \right|_2 = \left| 4 \cdot \frac{9}{5} \right|_2 = \frac{1}{4}, \quad \left| \frac{27}{40} \right|_2 = \left| \frac{1}{8} \cdot \frac{27}{5} \right|_2 = 8.$$

※ ($\forall x, y \in \mathbb{Q}$) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. 強三角不等式.

本ファイルでは, 断りが無い限り p 進距離に関するコーシー列を単にコーシー列と略す. 有理数からなるコーシー列 $\mathbf{a} = (a_n)_{n \geq 0}$ に対して, $\bar{\mathbf{a}}$ を $\bar{\mathbf{a}} = \{(b_n)_{n \geq 0} \mid (b_n)_{n \geq 0} \text{ は有理数からなるコーシー列, } \lim_{n \rightarrow \infty} |a_n - b_n|_p = 0\}$ で定義した. $\mathbb{Q}_p := \{\bar{\mathbf{a}} \mid \mathbf{a} \text{ は有理数からなるコーシー列}\}$ であった.

$\bar{\mathbf{a}} = \overline{(a_n)_{n \geq 0}} \in \mathbb{Q}_p$ に対して, $|\bar{\mathbf{a}}|_p = \lim_{n \rightarrow \infty} |a_n|_p$. さらに, $\bar{\mathbf{a}} \neq 0$ ならば,

$$\text{十分大きいすべての } n \text{ に対して } |\bar{\mathbf{a}}|_p = |a_n|_p \in \{p^m \mid m \in \mathbb{Z}\} \quad (1.1)$$

であった. なお, $\mathbb{Q}_p$ の具体的なイメージは補足 3.1 で明らかにする予定.

2 $\mathbb{Q}_p$ における和, 積 (補足 3.1 も参照)

$\bar{\mathbf{a}} = \overline{(a_n)_{n \geq 0}}, \bar{\mathbf{b}} = \overline{(b_n)_{n \geq 0}} \in \mathbb{Q}_p$ に対して, 和および積を次で定義する:

$$\bar{\mathbf{a}} + \bar{\mathbf{b}} := \overline{(a_n + b_n)_{n \geq 0}}, \quad \bar{\mathbf{a}} \cdot \bar{\mathbf{b}} := \overline{(a_n \cdot b_n)_{n \geq 0}}. \quad (2.1)$$

これらの演算は, 代表元 $(a_n)_{n \geq 0}, (b_n)_{n \geq 0}$ の選び方に依らない. 実際に, コーシー列 $(a_n)_{n \geq 0}, (b_n)_{n \geq 0}$ および $(a'_n)_{n \geq 0}, (b'_n)_{n \geq 0}$ が $\lim_{n \rightarrow \infty} |a_n - a'_n|_p = 0$ および $\lim_{n \rightarrow \infty} |b_n - b'_n|_p = 0$ を満たすと仮定する. まず, 和を考察する.

$$|(a_n + b_n) - (a'_n + b'_n)|_p \leq \max\{|a_n - a'_n|_p, |b_n - b'_n|_p\} \rightarrow 0 (n \rightarrow \infty)$$

(強三角不等式) となる. よって, $\overline{(a_n + b_n)_{n \geq 0}} = \overline{(a'_n + b'_n)_{n \geq 0}}$ となり, 和が代表元の選び方に依らない. 次に積を考察する. コーシー列の p 進ノルムが有界. つまり, ある正定数 M が存在し, 任意の $n \geq 0$ に対し, $|a_n|_p \leq M, |b'_n|_p \leq M$. すると,

$$\begin{aligned} |a_n b_n - a'_n b'_n|_p &= |a_n(b_n - b'_n) + (a_n - a'_n)b'_n|_p \\ &\leq \max\{|a_n|_p |b_n - b'_n|_p, |a_n - a'_n|_p |b'_n|_p\} \\ &\leq \max\{M |b_n - b'_n|_p, M |a_n - a'_n|_p\} \rightarrow 0 (n \rightarrow \infty) \end{aligned}$$

よって, $\overline{(a_n b_n)_{n \geq 0}} = \overline{(a'_n b'_n)_{n \geq 0}}$ となり, 積も代表元の選び方に依らない. さて, $a \in \mathbb{Q}$ に対して, $(a_n)_{n \geq 0} = (a)_{n \geq 0}$ (恒等的に a をとる数列) と a を同一視することにより, $\mathbb{Q} \subset \mathbb{Q}_p (a \in \mathbb{Q})$. なお, $\bar{a} = \overline{(a_n)_{n \geq 0}} \in \mathbb{Q}_p$ に対して, $\bar{a} \neq 0$ ならば, $\bar{a}^{-1} := \overline{(a_n^{-1})_{n \geq 0}}$ とおけば, $\bar{a} \cdot \bar{a}^{-1} = 1$.

※必要に応じて, 代表元 $(a_n)_{n \geq 0}$ が $(\forall n \geq 0) a_n \neq 0$ を満たすように選べる. なお, $\bar{a}^{-1}$ の定義も代表元の選び方に依らないことを証明できる (省略). まとめ: $\mathbb{Q}_p$ に和, 積を (2.1) により定義すると, $\mathbb{Q}_p$ は (可換) 体である. すなわち, 分配法則などが成り立つ. $\mathbb{Q}_p$ におけるノルムの性質を復習する. 以下, 断りが無い限り $\mathbb{Q}_p$ の元を x, y のように書き,

「 x の代表元 $(a_n)_{n \geq 0}$ をとる ($a_n \in \mathbb{Q}$)」などのように記述する.

命題 2.1. p を素数とする. すると, 以下が成立する. ※式 (1.1) 参照.

- (1) 任意の $x \in \mathbb{Q}_p$ に対して, $|x|_p \geq 0$.
- (2) 任意の $x \in \mathbb{Q}_p$ に対して, 「 $|x|_p = 0 \Leftrightarrow x = 0$ 」.
- (3) 任意の $x, y \in \mathbb{Q}_p$ に対して, $|xy|_p = |x|_p |y|_p$. 特に, $|-x|_p = |x|_p$.
- (4) 任意の $x, y \in \mathbb{Q}_p$ に対して, $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ (強三角不等式).

$x, y \in \mathbb{Q}_p$ に対して, $d_p(x, y) := |x - y|_p$ と定義することにより, $\mathbb{Q}_p$ は距離空間. このとき, $\mathbb{Q}$ は $\mathbb{Q}_p$ の稠密部分集合. 実際に, $x \in \mathbb{Q}_p$ とする. x の代表元 $(a_n)_{n \geq 0}$ を考える ($a_n \in \mathbb{Q}$). さて, $(a_n)_{n \geq 0}$ がコーシー列であるため, $\lim_{m \rightarrow \infty} |x - a_m|_p = 0$ を確認できる.

また, $\mathbb{Q}_p$ は完備距離空間である. 実際に, $\mathbb{Q}_p$ における任意のコーシー列 $(x_m)_{m \geq 0}$ は $\mathbb{Q}_p$ における収束列であることを示す. まず, $\mathbb{Q}$ が $\mathbb{Q}_p$ におい

て稠密より, 各 $m \geq 0$ に対して, $a_m \in \mathbb{Q}$ が存在して, $|x_m - a_m|_p < p^{-m}$.
 さて, $(x_n)_{n \geq 0}$ がコーシー列であることにより, $(a_n)_{n \geq 0}$ もコーシー列であることを確認できる. $y = \overline{(a_n)_{n \geq 0}} \in \mathbb{Q}_p$ とおく. すると,

$$\begin{aligned} |x_m - y|_p &= |(x_m - a_m) + (a_m - y)|_p \\ &\leq \max\{|x_m - a_m|_p, |a_m - y|_p\} \rightarrow 0 (m \rightarrow \infty) \end{aligned}$$

より, $(x_m)_{m \geq 0}$ は y に収束する.

3 $\mathbb{Q}_p$ の元の形 (p 進表示)

この節の目標は, $\mathbb{Q}_p$ の元が以下のように表せることを証明することである: $\sum_{n \geq -R}^{\infty} a_n \cdot p^n$. ただし, R は非負整数であり, 任意の $n \geq 0$ に対して $a_n \in \mathbb{Z}, 0 \leq a_n \leq p-1$.

補題 3.1. 非負整数全体の集合 $\mathbb{Z}_{\geq 0}$ は集合 $A := \{x \in \mathbb{Q} \mid |x|_p \leq 1\}$ において稠密部分集合である.

証明. p 進ノルムの定義から $(\forall n \in \mathbb{Z}_{\geq 0}) |n|_p \leq 1$ である. よって, $\mathbb{Z}_{\geq 0} \subset A$. 稠密性については, 以下を示せばよい: 任意の $x = a/b \in A$ (ただし, a, b は互いに素な整数) を固定する. すると, 任意の正整数 m に対して非負整数 $n(m)$ で $|x - n(m)|_p \leq p^{-m}$ となるものが存在する.

一般性を失わない.

さて, $|x|_p \leq 1$ より, b と p は互いに素. よって $u, w \in \mathbb{Z}$ が存在して, $ub + wp^m = 1$ が成立. すると, 以下が成立:

$$|ua - x|_p = \left| ua - \frac{a}{b} \right|_p = \left| \frac{a}{b} \right|_p |ub - 1|_p \leq |-wp^m|_p \leq p^{-m}.$$

$k \in \mathbb{Z}$ が存在して, $0 \leq ua + kp^m$. さて, $n(m) := ua + kp^m$ とおくと,
 $|n(m) - x|_p = |(ua - x) + kp^m|_p \leq \max\{|ua - x|_p, |kp^m|_p\} \leq p^{-m}$. $\square$

$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ とおく. すると, A は $\mathbb{Z}_p$ の稠密な部分集合である. 実際に, $x \in \mathbb{Z}_p \setminus \{0\}$ およびその代表元 $(a_n)_{n \geq 0}$ を任意に選ぶ. 式 (1.1) より, 十分大きい n に対して $|a_n|_p = |x|_p \leq 1$. よって, $a_n \in A$ である. したがって, $\lim_{n \rightarrow \infty} |x - a_n|_p = 0$ より, A は $\mathbb{Z}_p$ において稠密.
 一方, 補題 3.1 より, $\mathbb{Z}_{\geq 0}$ は A において稠密. 以上により, $\mathbb{Z}_{\geq 0}$ は $\mathbb{Z}_p$ の稠密な部分集合である.

$\mathbb{Z}_p$ の元の形を調べるために, $x \in \mathbb{Z}_p$ を任意に選び固定する. $\mathbb{Z}_{\geq 0}$ は $\mathbb{Z}_p$ の稠密な部分集合であるため, 任意の正整数 m に対して非負整数 $n(m)$ で $|x - n(m)|_p \leq p^{-m}$ となるものが存在する.

※必要に応じて, $n(m)$ から p^m の倍数を引いたものを改めて $n(m)$ と置き直すことにより, $0 \leq n(m) < p^m$ としても一般性を失わない.

$\lim_{m \rightarrow \infty} |x - n(m)|_p = 0$ より,

$$x = \lim_{m \rightarrow \infty} n(m) \quad (3.1)$$

である. まず, $0 \leq n(1) =: a_0 < p$. 次に, $m \geq 2$ に対して $n(m)$ と $n(m-1)$ を比較:

$$\begin{aligned} |n(m) - n(m-1)|_p &= |(n(m) - x) + (x - n(m-1))|_p \\ &\leq \max\{|n(m) - x|_p, |x - n(m-1)|_p\} \leq p^{-(m-1)} \end{aligned}$$

より, $n(m) \equiv n(m-1) \pmod{p^{m-1}}$. さらに, $0 \leq n(m-1) < p^{m-1}$, $0 \leq n(m) < p^m$ より, $n(m) = a_{m-1}p^{m-1} + n(m-1)$ ($0 \leq a_{m-1} \leq p-1$).

よって, (3.1) により, $x = \sum_{m=0}^{\infty} a_m \cdot p^m$ ※ ($\forall m$) $a_m \in \mathbb{Z}$, $0 \leq a_m \leq p-1$.

一方, 任意の $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$ は $|x|_p = p^{-R}$ (R は正整数) と書ける. 実際に $|p^R x|_p = p^{-R}|x|_p = 1$ より, $p^R x \in \mathbb{Z}_p$ である. よって, 以下が成立:

$$\begin{aligned} x &= p^{-R}(p^R x) = p^{-R} \sum_{n=0}^{\infty} a_n \cdot p^n \quad (\forall n, 0 \leq a_n \leq p-1) \\ &= \sum_{n=-R}^{\infty} a_{n+R} \cdot p^n. \end{aligned}$$

$x \in \mathbb{Q}_p$ に対して, 便宜上 $x = \sum_{n=-R}^{\infty} a_n \cdot p^n$ ($\forall n, 0 \leq a_n \leq p-1$) を p 進表示と呼ぶ.

補足 3.1. $x, y \in \mathbb{Q}_p$ に対して, $x = \sum_{n=-R}^{\infty} a_n \cdot p^n$ ($\forall n, 0 \leq a_n \leq p-1$), $y = \sum_{n=-R}^{\infty} b_n \cdot p^n$ ($\forall n, 0 \leq b_n \leq p-1$) とする (R は非負整数). $x \neq y$ のとき, $N = \min\{n \geq -R \mid a_n \neq b_n\}$ とする. すると, $|x - y|_p = p^{-N}$ である. さて, x, y の和と積の計算方法を具体的に述べる. 簡単のために, $x, y \in \mathbb{Z}_p$ の場合を考える. つまり, $R = 0$ である. 和 $x + y$ の”3桁”計算する場合, $(a_0 + a_1p + a_2p^2) + (b_0 + b_1p + b_2p^2)$ を p^3 で割った余りを求めればよい. 同様に積 xy の”3桁”計算する場合, $(a_0 + a_1p + a_2p^2)(b_0 + b_1p + b_2p^2)$ を計算して, p^3 で割った余りを求めればよい.

※ $\mathbb{Z}_p$ の元を p 進整数と呼ぶこともある. $\mathbb{Z}_p$ は $\mathbb{Q}_p$ の部分環.

特に, $x, y \in \mathbb{Z}_p$ ならば, $x + y \in \mathbb{Z}_p$, $xy \in \mathbb{Z}_p$.

4 不定方程式と p 進数

定理 4.1. $f(X, Y) \in \mathbb{Z}[X, Y]$ とする. このとき, 以下の 2 条件は同値:

条件 1 任意の $n \geq 1$ に対し $f(x, y) \equiv 0 \pmod{p^n}$ を満たす $x, y \in \mathbb{Z}$ が存在.

条件 2 $f(x, y) = 0$ を満たす $x, y \in \mathbb{Z}_p$ が存在する.

※前半のファイルで, $f(x, y) = 0$ を満たす整数 x, y が存在する十分条件として, $f(x, y) = 0$ を満たす $x, y \in \mathbb{R}$ が存在することであると述べた. 定理 4.1 の条件 2 ($f(x, y) = 0$ を満たす $x, y \in \mathbb{Z}_p$ が存在) も, 整数解が存在するための十分条件を与えている.

以下, 定理 4.1 の証明を行う.

補題 4.1. $\mathbb{Z}_p$ は $\mathbb{Q}_p$ のコンパクト部分集合. つまり, $\mathbb{Z}_p$ の元からなる任意の数列 $(x^{(n)})_{n \geq 0}$ は収束列である.

証明. $x^{(m)}$ ($m = 0, 1, \dots$) を $\mathbb{Z}_p$ の任意の数列とする. このとき, $x^{(m)}$ の p 進展開を

$$x^{(m)} = \sum_{n=0}^{\infty} a_n^{(m)} p^n = a_0^{(m)} + a_1^{(m)} p + a_2^{(m)} p^2 + \dots$$

($\forall n \geq 0, a_n^{(m)} \in \{0, 1, \dots, p-1\}$) とする. まず, $a_0^{(m)}$ ($m \geq 0$) を考察する. すると, $b_0 \in \{0, 1, \dots, p-1\}$ および非負整数からなる無限集合 S_0 が存在して, 以下を満たす: 任意の $m \in S_0$ に対して, $a_0^{(m)} = b_0$. 特に, $|x^{(m)} - b_0|_p \leq p^{-1}$.

次に, 無限集合 S_0 に対して, $a_1^{(m)}$ ($m \in S_0$) を考察する. すると, $b_1 \in \{0, 1, \dots, p-1\}$ および, S_0 の無限部分集合 S_1 が存在して, 以下を満たす: 任意の $m \in S_1$ に対して, $a_1^{(m)} = b_1$. 特に, $|x^{(m)} - b_0 - b_1 p|_p \leq p^{-2}$.

同様に無限集合 S_1 に対して, $a_2^{(m)}$ ($m \in S_1$) を考察する. すると, $b_2 \in \{0, 1, \dots, p-1\}$ および, S_1 の無限部分集合 S_2 が存在して, 以下を満たす: 任意の $m \in S_2$ に対して, $a_2^{(m)} = b_2$. 特に, $|x^{(m)} - b_0 - b_1 p - b_2 p^2|_p \leq p^{-3}$.

以下, この操作を繰り返すことで, 無限集合の列 $S_0 \supset S_1 \supset \dots \supset S_n \supset \dots$ および $b_n \in \{0, 1, \dots, p-1\}$ ($n \geq 0$) が存在して, 以下を満たす: 任意の $m \in S_n$ に対して $|x^{(m)} - (b_0 + b_1 p + \dots + b_n p^n)|_p \leq p^{-n-1}$. よって, $x = \sum_{k=0}^{\infty} b_k p^k \in \mathbb{Z}_p$ とおけば, 任意の $m \in S_n$ に対して $|x^{(m)} - x|_p \leq p^{-n-1}$. さて, 数列 S_n ($n \geq 0$) は, 任意の $n \geq 0$ に対して $S_n \supset S_{n+1}$ を満たす無

限集合の列であるので、以下のように狭義単調増加数列 $(m(n))_{n \geq 0}$ で、各 $n \geq 0$ 毎に $m(n) \in S_n$ を満たすものが存在する。よって、 $|x^{(m(n))} - x|_p \leq p^{-n-1} \rightarrow 0$ ($n \rightarrow \infty$) である。したがって、 $x^{(m)}$ ($m = 0, 1, \dots$) の部分列 $x^{(m(n))}$ ($n = 0, 1, \dots$) が x に収束することが示された。 $\square$

定理 4.1 の証明:

以下、 $f(X, Y) = \sum_{(i,j) \in \Lambda} A_{i,j} X^i Y^j$ とおく。ただし、 Λ は非負整数の組からなる有限集合であり、各 $(i, j) \in \Lambda$ に対して $A_{i,j} \in \mathbb{Z}$ である。

まず、 $f(x, y) = 0$ を満たす $x, y \in \mathbb{Z}_p$ が存在すると仮定する。このとき、 $x = \sum_{0 \leq m} a_m p^m, y = \sum_{0 \leq m} b_m p^m$, ($\forall m \geq 0, a_m, b_m \in \{0, 1, \dots, p-1\}$) とする。 $n \geq 1$ に対して、 $x_n = \sum_{0 \leq m \leq n-1} a_m p^m, y_n = \sum_{0 \leq m \leq n-1} b_m p^m$ とおく。すると、強三角不等式より以下が成立する:

$$\begin{aligned} |f(x_n, y_n)|_p &= |f(x_n, y_n) - f(x, y)|_p \\ &= \left| \sum_{(i,j) \in \Lambda} A_{i,j} x_n^i y_n^j - \sum_{(i,j) \in \Lambda} A_{i,j} x^i y^j \right|_p \\ &\leq \max \left\{ \left| \sum_{(i,j) \in \Lambda} A_{i,j} x_n^i y_n^j - \sum_{(i,j) \in \Lambda} A_{i,j} x_n^i y^j \right|_p, \left| \sum_{(i,j) \in \Lambda} A_{i,j} x_n^i y^j - \sum_{(i,j) \in \Lambda} A_{i,j} x^i y^j \right|_p \right\}. \end{aligned}$$

さて、 $|x - x_n| \leq p^{-n}$ かつ $|y - y_n|_p \leq p^{-n}$ である。よって、再び強三角不等式より、

$$\begin{aligned} \left| \sum_{(i,j) \in \Lambda} A_{i,j} x_n^i y_n^j - \sum_{(i,j) \in \Lambda} A_{i,j} x_n^i y^j \right|_p &\leq p^{-n}, \\ \left| \sum_{(i,j) \in \Lambda} A_{i,j} x_n^i y^j - \sum_{(i,j) \in \Lambda} A_{i,j} x^i y^j \right|_p &\leq p^{-n} \end{aligned}$$

となる。以上により、 $|f(x_n, y_n)|_p \leq p^{-n}$ となる。 $x_n, y_n \in \mathbb{Z}$ より、 $f(x_n, y_n) \in \mathbb{Z}$ である。特に $f(x_n, y_n) \equiv 0 \pmod{p^n}$ が成立する。

逆に、各 $n \geq 1$ に対して $f(x_n, y_n) \equiv 0 \pmod{p^n}$ を満たす整数 x_n, y_n が存在すると仮定する。つまり、 $|f(x_n, y_n)|_p \leq p^{-n}$ である。補題 4.1 により、適切な $x, y \in \mathbb{Z}_p$ および狭義単調増加列 $(n(m))_{m \geq 0}$ を取ることにより、

$$|x - x_{n(m)}| \leq p^{-n(m)}, \quad |y - y_{n(m)}|_p \leq p^{-n(m)}$$

が成り立つ.

※特に,

$$x = \lim_{m \rightarrow \infty} x_{n(m)}, \quad y = \lim_{m \rightarrow \infty} y_{n(m)}$$

である.

$$|f(x, y)|_p \leq \max\{|f(x, y) - f(x_{n(m)}, y_{n(m)})|_p, |f(x_{n(m)}, y_{n(m)})|_p\}$$

前半部分の証明と同様に, $|f(x, y) - f(x_{n(m)}, y_{n(m)})|_p \leq p^{-n(m)}$ であることを証明できる. さて, $|f(x_{n(m)}, y_{n(m)})|_p \leq p^{n(m)}$ とあわせると, $|f(x, y)|_p \leq p^{n(m)}$ である. m は任意の非負整数であることに着目すると, $|f(x, y)|_p = 0$, すなわち $f(x, y) = 0$ であることがわかる.