Number Theory

p-進数の入門から基礎まで

October 2026

$\mathbb{Z}$undamϕrphism

Contents

Chapter 1 p-進数の基礎 **3**

1.1 完備性 3

1.2 p-進数 9

References **11**

(i) 本コンテンツに関する著作権その他の知的財産権は，すべて著作者に帰属します．著作権法で認められている私的利用の範囲を超えて，本コンテンツの全部または一部を無断で複製，転載，改変，販売，配布する等の行為は一切禁止しております．
(ii) 権利者の許諾なく (i) に違反する行為またはこれに準ずる行為が行われていることが発覚した場合には，法的措置をとらせていただく場合がございます．
(iii) 万が一内容の誤りによって損害やトラブルが発生した場合でも，当方では責任を負いかねます．
(iv) 誤植やご意見等ございましたら，zundamorphism@icloud.com までご連絡いただけますと幸いです．

Chapter 1

p-進数の基礎

1.1　完備性

$\mathbb{Q}$ に無限小数を追加したものが $\mathbb{R}$ でした．この追加操作のことを完備化と言います．実は，任意の距離空間は完備化することが可能です．この節では完備化を厳密に定義し，距離空間の完備化を構成することが目標です．

まず，距離空間の定義から確認していきましょう．

定義 1.1.1. **距離空間**とは，空でない集合 X と写像 $d\colon X \times X \to \mathbb{R}$ の組 (X, d) で，

(i) $d(x, y) \geq 0$.

(ii) $d(x, y) = 0 \iff x = y$.

(iii) $d(x, y) = d(y, x)$.

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

を満たすもののことである．

距離空間では，集合の 2 点 x, y の間の距離を関数 d によって測ることができます．

距離関数は，非アルキメデス付値から自然に定めることができます．

定義 1.1.2. 体 K の**非アルキメデス付値**とは，写像 $|\cdot|\colon K \to \mathbb{R}$ で，

(i) $|x| \geq 0$.

(ii) $|x| = 0 \iff x = 0$.

(iii) $|xy| = |x||y|$.

(iv) $|x + y| \leq \max\{|x|, |y|\}$.

を満たすもののことである．

定義 1.1.3. 体 K 上の非アルキメデス付値 $|\cdot|$ に対し，d を

$$d(x,y) \stackrel{\text{def}}{=} |x-y|$$

と定義すれば，これは K 上の距離となる．このとき，d を $|\cdot|$ によって誘導される**超距離**と言う．

次に，点列の挙動が徐々に収まっていくような数列を導入します．

定義 1.1.4. 距離空間 (X,d) における点列 $\{x_n\}$ が，

$$^\forall\varepsilon > 0, {}^\exists N > 0, {}^\forall n,m \in \mathbb{N}, \quad n,m > N \implies d(x_n,x_m) < \varepsilon$$

を満たすとき，$\{x_n\}$ は **Cauchy 列**であると言う．

要するに，$N+1$ 項目以降は振幅が ε 未満になっているような数列のことです．

もし集合 X に “隙間” があれば，X における Cauchy 列の極限値はその “隙間” に収束してしまうかもしれないので，X 内で必ず収束するとは限りません．

例 1.1.5. $\mathbb{Q}$ の数列 $\{a_n\}_{n=0}^\infty \subseteq \mathbb{Q}$ を

$$a_n \stackrel{\text{def}}{=} 10^{-n} \cdot \lfloor 10^n \pi \rfloor$$

で定める．これは

$$a_0 = 3,\ a_1 = 3.1,\ a_2 = 3.14,\ a_3 = 3.141,\ a_4 = 3.1415, \ldots$$

という数列である．$\lim_{n\to\infty} a_n = \pi \notin \mathbb{Q}$ より，この数列は $\mathbb{Q}$ で収束しない．

ここまでの議論から，次の定義は妥当であると言えるでしょう．

定義 1.1.6. 距離空間 (X,d) において，その任意の Cauchy 列が X で収束するとき，(X,d) は**完備**であると言う．

例 1.1.7. Euclid 距離に関して，$\mathbb{R}$ は完備であるが，$\mathbb{Q}$ は完備でない．

冒頭で述べた $\mathbb{Q}$ と $\mathbb{R}$ の関係は次のように一般化されます．

定義 1.1.8. $(X,d),(\widehat{X},\widehat{d})$ を距離空間とし，$X \subseteq \widehat{X}$ であるとする．このとき，

(i) X は $\widehat{X}$ で稠密

(ii) $\widehat{d}$ の $X \times X$ への制限が d

(iii) $\widehat{X}$ は完備

であるならば，$\widehat{X}$ は X の**完備化**であると言う．

例 1.1.9. Euclid 距離に関して，$\mathbb{R}$ は $\mathbb{Q}$ の完備化である．

次の定理は，完備化の作り方を与えます．

定理 1.1.10. (X,d) を距離空間，$C(X)$ を (X,d) における Cauchy 列全体の集合とする．また，$\{x_n\},\{y_n\}\in C(X)$ に対し，$C(X)$ 上の同値関係 $\sim$ を，

$$\{x_n\}\sim\{y_n\} \overset{\text{def}}{\iff} \lim_{n\to\infty} d(x_n,y_n)=0$$

で定義し，$\{x_n\}$ の同値類を $[x_n]$ と書く．このとき，$\widehat{X}\overset{\text{def}}{=}C(X)/\sim$ と定義する．

さらに，$[x_n],[y_n]\in\widehat{X}$ に対し，$\{x_n\}\in[x_n],\{y_n\}\in[y_n]$ を任意に選び，写像 $\widehat{d}\colon \widehat{X}\times\widehat{X}\to\mathbb{R}$ を，

$$\widehat{d}([x_n],[y_n])\overset{\text{def}}{=}\widehat{d}(\{x_n\},\{y_n\})=\lim_{n\to\infty} d(x_n,y_n)$$

で定義する．このとき，距離空間 $(\widehat{X},\widehat{d})$ は (X,d) の**完備化**である．

ポイント 1.1.11. 以下の順に確認していきます．

(1) $\sim$ が同値関係であること

(i) $\{x_n\}\sim\{x_n\}$.

(ii) $\{x_n\}\sim\{y_n\} \implies \{y_n\}\sim\{x_n\}$.

(iii) $\{x_n\}\sim\{y_n\},\{y_n\}\sim\{z_n\} \implies \{x_n\}\sim\{z_n\}$.

(2) $\widehat{d}$ が well-defined であること

(i) $\{x_n\},\{y_n\}\in C(X) \implies {}^{\exists}\lim_{n\to\infty} d(x_n,y_n)$.

(ii) $\{x_n\}\sim\{x'_n\},\{y_n\}\sim\{y'_n\} \implies \widehat{d}([x_n],[y_n])=\widehat{d}([x'_n],[y'_n])$.

(3) $\widehat{d}$ が距離関数であること

(i) $\widehat{d}([x_n],[y_n])\geq 0$.

(ii) $\widehat{d}([x_n],[y_n])=0 \iff [x_n]=[y_n]$.

(iii) $\widehat{d}([x_n],[y_n])=\widehat{d}([y_n],[x_n])$.

(iv) $\widehat{d}([x_n],[z_n])\leq\widehat{d}([x_n],[y_n])+\widehat{d}([y_n],[z_n])$.

(4) 埋め込み i が等長写像であること

(i) 単射 $i\colon X\to\widehat{X}$ に対し，$x,y\in X \implies d(x,y)=\widehat{d}(i(x),i(y))$.

(5) $\overline{X}=\widehat{X}$ であること

(i) 任意の $[x_n] \in \widehat{X}$ に対し，$[x_n]$ に収束する $i(X)$ の点列が存在する．

(6) $\widehat{X}$ が完備であること

(i) 任意の $\widehat{X}$ の Cauchy 列 $\{[x_n]_m\}$ が $\widehat{X}$ で収束する．

注意 1.1.12. $x_n \in \{x_n\} \in [x_n] \in \{[x_n]_m\}$ に注意してください．

補題 1.1.13. (X, d) を距離空間とする．このとき，$x, y, z \in X$ に対し，

$$|d(x, y) - d(x, z)| \leq d(y, z)$$

が成り立つ．

証明. $d(x, y) \leq d(x, z) + d(z, y)$ から，$d(x, y) - d(x, z) \leq d(y, z)$ である．y と z を交換すると $d(x, z) - d(x, y) \leq d(z, y)$ を得る．これらから与式を得る． □

定理 *1.1.10* の証明. ポイント 1.1.11 に従って示していく．

(1) $\sim$ が同値関係であること

(i) $\{x_n\} \sim \{x_n\}$.

$d(x_n, x_n) = 0$ から明らか.

(ii) $\{x_n\} \sim \{y_n\} \implies \{y_n\} \sim \{x_n\}$.

$d(x_n, y_n) = d(y_n, x_n)$ から明らか.

(iii) $\{x_n\} \sim \{y_n\}, \{y_n\} \sim \{z_n\} \implies \{x_n\} \sim \{z_n\}$.

$d(x_n, z_n) \leq d(x_n, y_n) + d(y_n, z_n)$ から明らか.

(2) $\widehat{d}$ が well-defined であること

(i) $\{x_n\}, \{y_n\} \in C(X) \implies {}^{\exists} \lim_{n\to\infty} d(x_n, y_n)$.

まず，$\{x_n\}, \{y_n\} \in C(X)$ ならば，$\{d(x_n, y_n)\}$ が Cauchy 列であることを示す．

仮定から，

$$^{\forall}\varepsilon > 0, {}^{\exists}N > 0, {}^{\forall}n, m \in \mathbb{N}, \quad n, m > N \implies d(x_n, x_m), d(y_n, y_m) < \varepsilon$$

である．ここで補題 1.1.13 より，

$$\begin{aligned} |d(x_n, y_n) - d(x_m, y_m)| &= |d(x_n, y_n) - d(x_m, y_n) + d(x_m, y_n) - d(x_m, y_m)| \\ &\leq |d(y_n, x_n) - d(y_n, x_m)| + |d(x_m, y_n) - d(x_m, y_m)| \\ &\leq d(x_n, x_m) + d(y_n, y_m) < 2\varepsilon \end{aligned}$$

を得る．ゆえに，$\lim_{n\to\infty} d(x_n, y_n)$ が存在することが分かる．

(ii) $\{x_n\} \sim \{x'_n\}, \{y_n\} \sim \{y'_n\} \implies \widehat{d}([x_n], [y_n]) = \widehat{d}([x'_n], [y'_n])$.

$n \to \infty$ のとき $d(x_n, x'_n) \to 0$ なので，補題 1.1.13 より，$|d(x_n, y_n) - d(x'_n, y_n)| \leq$

$d(x_n, x'_n) \to 0$ である．よって，$d(x_n, y_n)$ と $d(x'_n, y_n)$ は同じ値に収束する．したがって，$\{x_n\} \sim \{x'_n\}$ ならば $\widehat{d}([x_n],[y_n]) = \widehat{d}([x'_n],[y_n])$ である．

$\{y_n\}$ に関しても同様である．

(3) $\widehat{d}$ が距離関数であること

(i) $\widehat{d}([x_n],[y_n]) \geq 0.$

$d(x_n, y_n) \geq 0$ で $n \to \infty$ とすればよい．

(ii) $\widehat{d}([x_n],[y_n]) = 0 \iff [x_n] = [y_n].$

($\Longleftarrow$) は明らか．($\Longrightarrow$) は $\sim$ の定義から明らか．

(iii) $\widehat{d}([x_n],[y_n]) = \widehat{d}([y_n],[x_n]).$

$d(x_n, y_n) = d(y_n, x_n)$ で $n \to \infty$ とすればよい．

(iv) $\widehat{d}([x_n],[z_n]) \leq \widehat{d}([x_n],[y_n]) + \widehat{d}([y_n],[z_n]).$

$d(x_n, z_n) \leq d(x_n, y_n) + d(y_n, z_n)$ で $n \to \infty$ とすればよい．

(4) 埋め込み i が等長写像であること

(i) 単射 $i\colon X \to \widehat{X}$ に対し，$x, y \in X \implies d(x,y) = \widehat{d}(i(x), i(y)).$

$x \in X$ とする．全ての n に対し $x_n = x$ とした点列 $\{x\}$ の同値類を $i(x)$ とする．$x \neq y \in X$ ならば $d(x,y) > 0$ であり，全ての n に対し $x_n = x, y_n = y$ ならば $d(x_n, y_n) = d(x,y)$ であるから，$\{d(x_n, y_n)\}$ は $d(x,y) \neq 0$ に収束する．ゆえに，$i\colon X \to \widehat{X}$ は単射で，$x, y \in X \implies d(x,y) = \widehat{d}(i(x), i(y))$ が成り立つ．

(5) $\overline{X} = \widehat{X}$ であること

(i) 任意の $[x_n] \in \widehat{X}$ に対し，$[x_n]$ に収束する $i(X)$ の点列が存在する．

任意の $[x_n] \in \widehat{X}$ とその元 $\{x_n\} \in [x_n]$ を取る．$\{x_n\}$ は Cauchy 列だから，n, m を十分大きく取れば，$d(x_n, x_m) < \varepsilon$ とできる．よって，$i(x_n)$ を考えると，$\varepsilon > 0$ に対し $\widehat{d}([x_n], i(x_n)) < \varepsilon$ とできる．したがって，$i(x_n)$ は $[x_n]$ に収束するから，X は $\widehat{X}$ で稠密である．

(6) $\widehat{X}$ が完備であること

(i) 任意の $\widehat{X}$ の Cauchy 列 $\{[x_n]_m\}$ が $\widehat{X}$ で収束する．

Cauchy 列 $\{[x_n]_m\} \in \widehat{X}$ を任意に取る．この Cauchy 列の収束先が $\widehat{X}$ に存在することを示せばよい．同値類の代表の取り方は議論に影響しないことは既に示した通りなので，以下，同値類 $[x_n^m]$ の代わりにそれから適当な代表元 $\{x_n^m\} \in C(X)$ を取って，直接数列の距離を評価していく．

$$^{\forall}\varepsilon > 0, {}^{\exists}N > 0, {}^{\forall}m_1, m_2 \in \mathbb{N}, \quad m_1, m_2 > N \implies \widehat{d}(\{x_n^{m_1}\}, \{x_n^{m_2}\}) < \varepsilon$$

である．また，

$$^{\forall}m, {}^{\forall}\varepsilon > 0, {}^{\exists}N_m > N, {}^{\forall}n_1, n_2 \in \mathbb{N}, \quad n_1, n_2 > N_m \implies d(x_{n_1}^m, x_{n_2}^m) < \varepsilon$$

である．ただし，N_m を定義する際の ε としては，$\varepsilon < \dfrac{1}{m}$ を満たすようなものを取るようにする．

すると，この m と N_m を用いて表される点列 $\{x^m_{N_m+1}\}$ の同値類 $[x^m_{N_m+1}]$ は，$\{[x_n]_m\}$ の収束先である．

$\widehat{d}(\{x^{m_1}_n\},\{x^{m_2}_n\}) = \lim_{n\to\infty} d(x^{m_1}_n, x^{m_2}_n)$ であるから，n を十分大きく取れば，

$$\left|\widehat{d}(\{x^{m_1}_n\},\{x^{m_2}_n\}) - d(x^{m_1}_n, x^{m_2}_n)\right| < \varepsilon$$

とできるから，$m_1, m_2 > N$ のとき，

$$d(x^{m_1}_n, x^{m_2}_n) < \widehat{d}(\{x^{m_1}_n\},\{x^{m_2}_n\}) + \varepsilon < 2\varepsilon$$

と抑えられる．

今，十分大きい $n > N_{m_1}, N_{m_2}$ を取れば，

$$\begin{aligned} d(x^{m_1}_{N_{m_1}+1}, x^{m_2}_{N_{m_2}+1}) &\le d(x^{m_1}_{N_{m_1}+1}, x^{m_1}_n) + d(x^{m_1}_n, x^{m_2}_n) + d(x^{m_2}_n, x^{m_2}_{N_{m_2}+1}) \\ &< 4\varepsilon \end{aligned}$$

となる．

したがって，$\{x^m_{N_m+1}\} \in \widehat{X}$ は Cauchy 列である．

$m > N_n$ に対して，

$$\begin{aligned} d(x^m_{N_m+1}, x^n_m) &\le d(x^m_{N_m+1}, x^n_{N_n+1}) + d(x^n_{N_n+1}, x^n_m) \\ &< 5\varepsilon \end{aligned}$$

であり，$\widehat{d}(\{x^m_{N_m+1}\},\{x^n_m\}) = \lim_{m\to\infty} d(x^m_{N_m+1}, x^n_m)$ であるから，n に対して m を十分大きく取れば，

$$\left|\widehat{d}(\{x^m_{N_m+1}\},\{x^n_m\}) - d(x^m_{N_m+1}, x^n_m)\right| < \varepsilon$$

とできる．

ゆえに，$n > N$ のとき，

$$\widehat{d}(\{x^m_{N_m+1}\},\{x^n_m\}) \le 6\varepsilon$$

を得る．したがって，$[x^n_m] \to [x^m_{N_m+1}]$ となり，$\widehat{X}$ は完備である．

□

定理 1.1.14. 距離空間の完備化は一意的である．すなわち，$(X_1, d_1), (X_2, d_2)$ が (X, d) の完備化であるとき，全単射 $\phi\colon X_1 \to X_2$ が存在して，

(i) ϕ は X の任意の元を固定する

(ii) $^\forall x, y \in X_1, \quad d_1(x,y) = d_2(\phi(x), \phi(y))$

を満たす．

証明. 任意の $x \in X_1$ に対し，x に収束する X の Cauchy 列 $\{x_n\}$ を取れる．X_2 は完備なので，

$$x_n \to \phi(x) \quad (n \to \infty)$$

となる $\phi(x) \in X_2$ が存在する．このようにして ϕ を定めると，ϕ は well-defined である．

$x \in X$ なら，全ての n に対し $x_n = x$ である点列 $\{x\}$ の同値類 $[x]$ を X_1 からも X_2 からも取れるので，ϕ は X の元を固定することが分かる．

$x, y \in X_1$ に対し，

$$x_n \to x, \quad y_n \to y \qquad (n \to \infty)$$

となる $x_n, y_n \in X$ を取る．

$d_1(x_n, x) \to 0$，$d_1(y_n, y) \to 0$ であるから，

$$\begin{aligned} |d_1(x,y) - d_1(x_n,y_n)| &= |d_1(x,y) - d_1(x,y_n) + d_1(x,y_n) - d_1(x_n,y_n)| \\ &\le |d_1(x,y) - d_1(x,y_n)| + |d_1(x,y_n) - d_1(x_n,y_n)| \\ &\le d_1(y,y_n) + d_1(x,x_n) \end{aligned}$$

であり，$d_1(y, y_n) + d_1(x, x_n) \to 0 \quad (n \to \infty)$ であることから，

$$d(x_n, y_n) = d_1(x_n, y_n) \to d_1(x, y) \qquad (n \to \infty)$$

が従う．

同様にして $d(x_n, y_n) \to d_2(\phi(x), \phi(y)) \quad (n \to \infty)$ となるので，ϕ は等長写像である．ϕ は単射であり，X は X_2 で稠密なので全射でもある． □

1.2 p-進数

定義 1.2.1. 素数 p を固定する．$x \neq 0$ を有理数とする．p と互いに素な整数 a, b 及び整数 n を使って，x を $x = p^n \dfrac{a}{b}$ と表したとき，x の**オーダー** $\mathrm{ord}_p(x)$ を，

$$\mathrm{ord}_p(x) \stackrel{\mathrm{def}}{=} n$$

と定義する．ただし，$x = 0$ の場合は，$\mathrm{ord}_p(0) = +\infty$ とする．

オーダーは，次の性質を持ちます．

命題 1.2.2.

(i) $\mathrm{ord}_p(x) = +\infty \iff x = 0$

(ii) $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$

(iii) $\mathrm{ord}_p(x + y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$

証明. 後日公開. □

定義 1.2.3. $x \in \mathbb{Q}$ と素数 p に対し，x の ***p* 進付値**を次のように定義する．

$$|x|_p \overset{\text{def}}{=} \begin{cases} p^{-\operatorname{ord}_p(x)} & (x \neq 0) \\ 0 & (x = 0) \end{cases}$$

定義 1.2.4. p 進付値は非アルキメデス付値である．p 進付値によって誘導される超距離を ***p* 進距離**と言う．

これでやっと p 進体を定義できます．p 進体は，$\mathbb{Q}$ を p 進距離によって完備化したものです．

定義 1.2.5. $\mathbb{Q}$ の p 進距離による完備化を $\mathbb{Q}_p$ と書き，***p* 進体**と言う．また，$\mathbb{Q}_p$ の元を ***p* 進数**と言う．

定理 1.2.6. $\mathbb{Q}_p$ には $\mathbb{Q}$ の演算を拡張した演算が定義されて，位相体となる．

定義 1.2.7. $\mathbb{Q}_p$ の部分環 $\mathbb{Z}_p$ を

$$\mathbb{Z}_p \overset{\text{def}}{=} \{x \in \mathbb{Q}_p \mid \operatorname{ord}_p(x) \geq 0\}$$

で定義し，***p* 進整数環**と言う．

p 進整数環に関して，ヘンゼルの補題と呼ばれる重要な定理が知られています．

定理 1.2.8 (ヘンゼルの補題)**.** p を素数とする．$f \in \mathbb{Z}_p[x]$ と $a \in \mathbb{Z}_p$ が

$$f(a) \equiv 0 \pmod{p}, \quad f'(a) \not\equiv 0 \pmod{p}$$

を満たすとき，$\alpha \in \mathbb{Z}_p$ がただ 1 つ存在して，

$$f(\alpha) = 0, \quad \alpha \equiv a \pmod{p}$$

となる．

注意 1.2.9. この定理に限った話ではないですが，ヘンゼルの補題には色々なバリエーションがあるので，参考にした書籍によっては全く見た目が違うかもしれません．

この定理を使えば，例えば f として 2 次多項式を選ぶことで $\mathbb{Z}_p$ の平方根の存在を簡単に判定できたりします．

References

[1] KEITH CONRAD, HENSEL'S LEMMA, https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf.

[2] 松坂和夫，集合・位相入門，岩波書店

[3] 雪江明彦，整数論 1，初等整数論から p 進数へ，日本評論社

[4] 雪江明彦，代数学 1，群論入門，日本評論社

[5] 雪江明彦，代数学 2，環と体とガロア理論，日本評論社

[6] 雪江明彦，代数学 3，代数学のひろがり，日本評論社

10242026 Ver.1.5

Copyright (c) 2026 Zundamorphism All Rights Reserved.