1　p 進整数環

p を素数とし，$\mathbb{Z}/p^i\mathbb{Z}$ を $\mathbb{Z}$ の $p^i\mathbb{Z}$ による剰余環とする．$n \leq m$ なる二つの自然数 m, n に対して，写像 $\phi_{m,n}$ を

$$\phi_{m,n} : \mathbb{Z}/p^{m+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}, \qquad x + p^{m+1}\mathbb{Z} \longmapsto x + p^{n+1}\mathbb{Z}$$

と定義すれば，$\phi_{m,n}$ は環の全射準同型であって

$$\phi_{m,m} = id \text{ (恒等写像)}$$
$$n \leq m \leq l \Longrightarrow \phi_{l,n} = \phi_{m,n} \circ \phi_{l,m}$$

が成り立つ．いま

$$\mathbb{Z}_p = \left\{ (x_i)_{i\in\mathbb{N}} \in \prod_{i=0}^{\infty} \mathbb{Z}/p^{i+1}\mathbb{Z} \;\middle|\; n \leq m \Longrightarrow \phi_{m,n}(x_m) = x_n \right\}$$

とおく．

注意 1.1.　以後，$\mathbb{Z}_p$ の元 $x = (x_i)_{i\in\mathbb{N}}$, $y = (y_i)_{i\in\mathbb{N}}$ に対して，

$$x_i \equiv 0 \,(\mathrm{mod}\, p^{i+1}), \qquad x_i \equiv y_i \,(\mathrm{mod}\, p^{i+1})$$

などを，省略してそれぞれ

$$x_i = 0, \qquad x_i = y_i$$

と書く．

命題 1.2.　$x = (x_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_p$ の元，m を自然数とする．このとき，$x_m = 0$ ならば，$0 \leq n \leq m$ に対して $x_n = 0$ が成り立つ．

証明.　$0 \leq n \leq m$ に対して

$$x_n = \phi_{m,n}(x_m) = \phi_{m,n}(0) = 0$$

となる．□

系 1.3.　$x = (x_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_p$ の元，m を自然数とする．このとき，$x_m \neq 0$ ならば，$k \geq m$ なるすべての自然数 k に対して $x_k \neq 0$ が成り立つ．

証明.　もし仮に $k \geq m$ なる自然数 k で $x_k \neq 0$ なるものがあれば，命題 1.2 より $x_m = 0$ となる．これは仮定に矛盾する．□

$\mathbb{Z}_p$ における和および積を次のように定義する．$\mathbb{Z}_p$ の二つの元 $x = (x_i)_{i\in\mathbb{N}}$, $y = (y_i)_{i\in\mathbb{N}}$ に対して

$$x + y = (x_i + y_i)_{i\in\mathbb{N}}, \qquad xy = (x_i y_i)_{i\in\mathbb{N}}$$

と定める．ここで $x + y \in \mathbb{Z}_p$, $xy \in \mathbb{Z}_p$ であることは，$n \leq m$ ならば

$$\phi_{m,n}(x_m + y_m) = \phi_{m,n}(x_m) + \phi_{m,n}(y_m) = x_m + y_m,$$
$$\phi_{m,n}(x_m y_m) = \phi_{m,n}(x_m)\phi_{m,n}(y_m) = x_m y_m$$

となることからわかる．各 $\mathbb{Z}/p^{i+1}\mathbb{Z}$ が可換環であることから，$\mathbb{Z}_p$ の二つの元 x, y について

$$x+y=(x_i+y_i)_{i\in\mathbb{N}}=(y_i+x_i)_{i\in\mathbb{N}}=y+x,$$
$$xy=(x_iy_i)_{i\in\mathbb{N}}=(y_ix_i)_{i\in\mathbb{N}}=yx$$

したがって $\mathbb{Z}_p$ は可換環である．$\mathbb{Z}_p$ の零元，単位元はそれぞれ

$$0=(0)_{i\in\mathbb{N}},\qquad 1=(1)_{i\in\mathbb{N}}$$

である．

写像

$$f:\mathbb{Z}\longrightarrow\mathbb{Z}_p,\qquad a\longmapsto(a+p^{i+1}\mathbb{Z})_{i\in\mathbb{N}}$$

を考える．f が well-defined であることは

$$n\leq m\Longrightarrow\phi_{m,n}(a+p^m\mathbb{Z})=a+p^n\mathbb{Z}$$

より明らかである．$\phi_{m,n}$ の準同型性から f が環の準同型写像であることがわかる．また，$\mathbb{Z}$ の二つの元 a, b に対して

$$f(a)=f(b)\Longrightarrow a\equiv b\,(\mathrm{mod}\,p^i)\ (\forall i\in\mathbb{N})\Longrightarrow p^i\mid a-b\ (\forall i\in\mathbb{N})\Longrightarrow a-b=0$$

したがって f は単射である．この f により $\mathbb{Z}$ を $\mathbb{Z}_p$ の部分環とみなすことができる．

命題 1.4. $\mathbb{Z}_p$ は整域である．そこで $\mathbb{Z}_p$ を p **進整数環**ということにする．

証明. $x=(x_i)_{i\in\mathbb{N}}$, $y=(y_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_p$ の 0 でない二つの元とする．このときある番号 m, n があって $x_m\not\equiv 0\,(\mathrm{mod}\,p^{m+1})$, $y_n\not\equiv 0\,(\mathrm{mod}\,p^{n+1})$ となる．すなわちある整数 a, b, k, l によって

$$x_m\equiv ap^k\,(\mathrm{mod}\,p^{m+1}),\qquad k<m+1,\qquad (p,a)=1,$$
$$y_n\equiv bp^l\,(\mathrm{mod}\,p^{n+1}),\qquad l<n+1,\qquad (p,b)=1$$

と表せる．このとき

$$x_{m+n+1}y_{m+n+1}\not\equiv 0\pmod{p^{m+n+2}}$$

が示せる．なぜなら

$$\phi_{m+n+1,m}(x_{m+n+1})=x_m\equiv ap^k\pmod{p^{m+1}}$$

より，ある整数 a' が存在して

$$x_{m+n+1}=a'p^k,\qquad k<m+1,\qquad (a',p)=1$$

と書ける．同様にして，ある整数 b' が存在して

$$y_{m+n+1}=b'p^k,\qquad k<n+1,\qquad (b',p)=1$$

と書ける．したがって

$$x_{m+n+1}y_{m+n+1}=a'b'p^{k+l},\qquad k+l<m+n+2,\qquad (a'b',p)=1$$

ゆえに $x_{m+n+1}y_{m+n+1}\not\equiv 0\,(\mathrm{mod}\,p^{m+n+2})$ となる．したがって $xy\neq 0$. □

命題 1.5.

$$\mathbb{Z}_p^\times = \{x = (x_i)_{i\in\mathbb{N}} \in \mathbb{Z}_p \mid x_0 \neq 0\}$$

証明.

($\subseteq$) $x \in \mathbb{Z}_p^\times$ とすると，$\mathbb{Z}_p$ の元 y が存在して $xy = 1$ を満たす．$y = (y_i)_{i\in\mathbb{N}}$ とおくと，$x_0y_0 = 1$. よって $x_0 \neq 0$，したがって $x \neq 0$.

($\supseteq$) $x = (x_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_p$ の元で $x_0 \neq 0$ を満たすものとする．このとき $x_0y_0 = 1$ を満たす $y_0 \in \mathbb{Z}/p\mathbb{Z}$ が存在する．いま

$$x_iy_i \equiv 1 \,(\mathrm{mod}\ p^{i+1}), \qquad y_i \equiv y_{i-1} \,(\mathrm{mod}\ p^i)$$

が成り立つような $y_i \in \mathbb{Z}/p^{i+1}\mathbb{Z}$ が存在すると仮定して

$$x_{i+1}y_{i+1} \equiv 1 \,(\mathrm{mod}\ p^{i+2}), \qquad y_{i+1} \equiv y_i \,(\mathrm{mod}\ p^{i+1}) \tag{1}$$

を満たす $y_{i+1} \in \mathbb{Z}/p^{i+2}\mathbb{Z}$ が存在することを示す．このことが示せれば帰納的に $y = (y_i)_{i\in\mathbb{N}} \in \mathbb{Z}_p$ が定まる．この y は $xy = 1$ を満たす．したがって $x \in \mathbb{Z}_p^\times$ がいえる．

x は $\mathbb{Z}_p$ の元なので

$$x_{i+1} \equiv x_i + sp^{i+1} \pmod{p^{i+2}}$$

なる $s \in \mathbb{Z}$ が存在する．また，(1) の二番目の条件は

$$y_{i+1} \equiv y_i + tp^{i+1} \pmod{p^{i+2}}$$

なる $t \in \mathbb{Z}$ が存在することと同値である．このとき

$$\begin{aligned} x_{i+1}y_{i+1} - 1 &\equiv (x_i + sp^{i+1})(y_i + tp^{i+1}) - 1 \\ &\equiv x_iy_i - 1 + (sy_i + tx_i)p^{i+1} \pmod{p^{i+2}} \end{aligned}$$

よって

$$\begin{aligned} x_{i+1}y_{i+1} = 1 &\iff x_iy_i - 1 + (sy_i + tx_i)p^{i+1} \equiv 0 \,(\mathrm{mod}\ p^{i+2}) \\ &\iff \frac{x_iy_i - 1}{p^{i+1}} + sy_i + tx_i \equiv 0 \,(\mathrm{mod}\ p) \\ &\iff \frac{x_iy_i - 1}{p^{i+1}} + sy_0 + tx_0 \equiv 0 \,(\mathrm{mod}\ p) \end{aligned}$$

ただし最後の同値を示すのに帰納法の仮定を用いている．$x_0 \not\equiv 0 \,(\mathrm{mod}\ p)$ であったから，素数 p を法とする一次合同式の性質より，最後の条件を満たす t は p を法としてただ一つ存在する．したがって (1) を満たす $y_{i+1} \in \mathbb{Z}/p^{i+2}\mathbb{Z}$ が存在する．

□

例 1.6. p を 3 以外の素数とする．このとき $3 \in \mathbb{Z}_p^\times$ が成り立つ．なぜなら，$3 = (3)_{i\in\mathbb{N}}$ だから，とくに最初の成分について $3 \not\equiv 0 \,(\mathrm{mod}\ p)$.

例 1.7. より一般に，p を素数，m を p と互いに素な $\mathbb{Z}$ の元とすれば，例 1.6 と同じような理由で，$m \in \mathbb{Z}_p^\times$ が成り立つ．

2　p 進展開

p を素数とし，$S := \{0, 1, 2, \ldots, p-1\}$ とおく．$(a_i)_{i\in\mathbb{N}}$ を S の元の列とする．すなわち各番号 i に対して a_i は $0, 1, 2, \ldots, p-1$ のいずれかの値をとる．いま，$n = 0, 1, 2, \ldots$ に対して

$$x_n = \sum_{i=0}^{n} a_i p^i$$

とおけば，$(x_n)_{n\in\mathbb{N}}$ は $\mathbb{Z}_p$ の元である．実際

$$x_n \in \mathbb{Z}/p^{n+1}\mathbb{Z} \quad (\forall n \in \mathbb{N})$$

$$n \leq m \Longrightarrow \phi_{m,n}(x_m) = x_n$$

が成り立つ．よって $(x_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$．このとき $(x_n)_{n\in\mathbb{N}}$ を

$$\sum_{i=0}^{\infty} a_i p^i$$

のように表す.

定理 2.1.　p を素数とし，$S := \{0, 1, 2, \ldots, p-1\}$ とおく．$\mathbb{Z}_p$ の各元 x に対して，S の元の列 $(a_i)_{i\in\mathbb{N}}$ がただ一つ存在して

$$x = \sum_{i=0}^{\infty} a_i p^i$$

が成り立つ．$\displaystyle\sum_{i=0}^{\infty} a_i p^i$ を x の p **進展開**という.

証明.　$\mathbb{Z}_p$ の元 $x = (x_n)_{n\in\mathbb{N}}$ に対して，$n = 0, 1, 2, \ldots$ に対する合同式

$$(*)_n \qquad x_n \equiv \sum_{i=0}^{n} a_i p^i \pmod{p^{n+1}}$$

を満たす S の元の列 $(a_i)_{i\in\mathbb{N}}$ が一意的に定まることを示せばよい.

(i)　$n = 0$ のとき．$a_0 \equiv x_0 \pmod{p}$ なる S の元 a_0 はただ 1 つ存在する．

(ii)　いま，$n \geq 1$ に対して，S の元の $a_0, a_1, \ldots, a_{n-1}$ が一意的に定まって，合同式 $(*)_0, (*)_1, \ldots, (*)_{n-1}$ が満たされていると仮定する．このとき $\phi_{n,n-1}(x_n) = x_{n-1}$ より

$$\phi_{n,n-1}(x_n - \sum_{i=0}^{n-1} a_i p^i) = \phi_{n,n-1}(x_n) - \phi_{n,n-1}(\sum_{i=0}^{n-1} a_i p^i) = x_{n-1} - x_{n-1} = 0$$

ゆえに

$$x_n - \sum_{i=0}^{n-1} a_i p^i \in \ker \phi_{n,n-1} = p^n\mathbb{Z}/p^{n+1}\mathbb{Z} \ (\subseteq \mathbb{Z}/p^{n+1}\mathbb{Z})$$

よって，S の元 a_n を適当にとって

$$x_n - \sum_{i=0}^{n-1} a_i p^i \equiv a_n p^n \pmod{p^{n+1}}$$

とできる．このとき数列 $a_0, a_1, \ldots, a_n$ に対して合同式 $(*)_0, (*)_1, \ldots, (*)_n$ が満たされる．

a_n の一意性は次のようにしてわかる．もし S のもう 1 つの元 a'_n に対して

$$x_n \equiv \sum_{i=0}^{n-1} a_i p^i + a'_n p^n \pmod{p^{n+1}}$$

が成り立つとすると

$$p^n(a_n - a'_n) \equiv 0 \pmod{p^{n+1}}$$

よって $a_n - a'_n$ は p の倍数である．一方，a_n, a'_n はともに S の元だから

$$|a_n - a'_n| < p$$

これより $a_n - a'_n = 0$ を得る．

□

系 2.2. n を自然数，x を $\mathbb{Z}_p$ の元とする．$x = \sum_{i=0}^{\infty} a_i p^i$ を x の p 進展開とするとき，列 $(b_i)_{i\in\mathbb{N}}$ を

$$b_i = \begin{cases} 0, & 0 \le i \le n-1 \\ a_{i-n}, & n \le i \end{cases}$$

によって定めれば

$$p^n x = \sum_{i=0}^{\infty} b_i p^i$$

が $p^n x$ の p 進展開になる．

証明. $x = (x_i)_{i\in\mathbb{N}}$ とすると，$p^n x = (p^n x_i)_{i\in\mathbb{N}}$ である．一方，p 進展開の定義から各 i に対して

$$x_i \equiv \sum_{k=0}^{i} a_k p^k \pmod{p^{i+1}}$$

したがって

$$p^n x_i \equiv \sum_{k=0}^{i} a_k p^{n+k} \equiv \sum_{k=0}^{i} b_k p^k \pmod{p^{i+1}}$$

となる． □

系 2.3. n を自然数，x を $\mathbb{Z}_p$ の元とする．このとき

$$p^n x = 0 \Longrightarrow x = 0$$

が成り立つ．

証明. $\mathbb{Z}_p$ が整域であることを認めれば，この事実は自明である．

ここでは，$\mathbb{Z}_p$ が整域であることを仮定せずに，定理 2.1 の系として証明する．$x = \sum_{i=0}^{\infty} a_i p^i$ を x の p 進展開とすると，系 2.2 より

$$\sum_{i=0}^{\infty} b_i p^i = p^n x = 0$$

ただし

$$b_i = \begin{cases} 0, & 0 \le i \le n-1 \\ a_{i-n}, & n \le i \end{cases}$$

p 進展開の一意性により，各 i について $b_i = 0$，したがって $a_i = 0$ を得る．よって $x = 0$. □

命題 2.4. 任意の素数 p について，$\mathbb{Z}_p$ の濃度は $\mathbb{R}$ の濃度に等しい．

証明. 概略を示す．濃度についての一般的な事実は，松坂和夫著「集合・位相入門」(岩波書店) を参照せよ．

集合 A の濃度を $\operatorname{card} A$ とおき，$\mathfrak{a} = \operatorname{card} \mathbb{N}$, $\mathfrak{c} = \operatorname{card} \mathbb{R}$ とおくと，$\mathbb{R}$ は区間 $(0, 1)$ と対等であるから

$$\operatorname{card} (0, 1) = \mathfrak{c}$$

また，区間 $(0, 1)$ に属する実数が二進小数で表せることから

$$\operatorname{card} (0, 1) \le \operatorname{card} \prod_{n=0}^{\infty} \{0, 1\} = 2^{\mathfrak{a}}$$

である．一方，$\mathbb{Z}_p$ の元が p 進展開で表されることと包含関係から

$$\operatorname{card} \prod_{n=0}^{\infty} \{0, 1\} \le \mathbb{Z}_p \le \operatorname{card} \prod_{n=0}^{\infty} \mathbb{Z}$$

がいえる．さらに $\operatorname{card} \mathbb{Z} = \mathfrak{a}$ であるから

$$\operatorname{card} \prod_{n=0}^{\infty} \mathbb{Z} = \mathfrak{a}^{\mathfrak{a}}$$

最後に

$$2^{\mathfrak{a}} = \mathfrak{a}^{\mathfrak{a}} = \mathfrak{c}$$

という事実を認めれば，Bernstein の定理より，$\operatorname{card} \mathbb{Z}_p = \mathfrak{c}$ が示される． □

命題 2.5. $\mathbb{Z}_p$ の 0 でない元 x はすべて

$$x = p^e u, \qquad e \in \mathbb{N}, \qquad u \in \mathbb{Z}_p^{\times}$$

の形で一意的に表される．

証明. $x = (x_i)_{i \in \mathbb{N}} = \sum_{i=0}^{\infty} a_i p^i$ とする．ただし最後の式は x の p 進展開である．$x \neq 0$ より

$$e = \min\{i \in \mathbb{N} \mid x_i \neq 0\}$$

が存在する．

$$u = \sum_{k=0}^{\infty} a_{k+e} p^k$$

とおくと，$x = p^e u$ が成り立つ (系 2.2)．$u = (u_i)_{i \in \mathbb{N}}$ とすると，$u = a_e \neq 0$ がわかる．実際，e の取り方から

$$x_i = 0 \ (0 \le i \le e) \iff a_i = 0 \ (0 \le i < e)$$

p 進展開の定義から

$$0 \neq x_e = \sum_{k=0}^{e} a_e p^e = a_e p^e, \qquad a_e \in \{0, 1, \ldots, p-1\}$$

ゆえに $a_e \neq 0$ を得る．したがって $u \in \mathbb{Z}_p^\times$ である．

次に一意性を示す．

$$x = p^e u = p^{e'} u', \qquad e, e' \in \mathbb{N}, \qquad u, u' \in \mathbb{Z}_p^\times$$

とする．$e \leq e'$ と仮定しても一般性を失わない．このとき

$$p^e(u - p^{e'-e}) = 0$$

系 2.3 から

$$u = p^{e'-e} v$$

を得る．$u \in \mathbb{Z}_p^\times$ だから $e' - e = 0$ でなければならない (命題 1.5). □

注意 2.6. 命題 2.5 と系 2.3 によって，$\mathbb{Z}_p$ が整域であることが再び証明される．

命題 2.7. $\mathbb{Z}_p$ の元 $x = (x_i)_{i\in\mathbb{N}} = \sum_{k=0}^{\infty} a_k p^k$ (p 進展開) に対して，次の条件は同値である．

(i) $x_n = 0$

(ii) $a_0 = a_1 = \cdots = a_n = 0$

(iii) ある $y \in \mathbb{Z}_p$ が存在して $x = p^{n+1} y$

証明.

(i)⇒(ii) 条件 (i) と命題 1.2 より，$0 \leq i \leq n$ なる i に対して

$$\sum_{k=0}^{i} a_k p^k \equiv x_i \equiv 0 \pmod{p^{i+1}}$$

$a_k \in \{0, 1, \cdots, p-1\}$ より

$$0 \leq \sum_{k=0}^{i} a_k p^k \leq \sum_{k=0}^{i} (p-1) p^k = p^i - 1 < p^i \qquad (0 \leq i \leq n)$$

ゆえに (ii) を得る．

(ii)⇒(iii) (ii) が成り立つとき

$$y = \sum_{k=0}^{\infty} a_{k+n+1} p^k$$

とおけば $x = p^{n+1} y$ である (系 2.2).

(iii)⇒(i) $y = (y_i)_{i\in\mathbb{N}}$ とすると

$$x_n \equiv p^{n+1} y \equiv 0 \pmod{p^{n+1}}$$

である．

□

命題 2.8.

$$\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \cong \mathbb{Z}/p^{n+1}\mathbb{Z} \qquad (\forall n \in \mathbb{N})$$

証明. 写像

$$f_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}, \qquad (x_i)_{i\in\mathbb{N}} \longmapsto x_n$$

を考えると，f_n が全射準同型であることはすぐにわかる．

$\mathrm{Ker}\, f_n = p^{n+1}\mathbb{Z}_p$ であることは，命題 2.7 より

$$x \in p^{n+1}\mathbb{Z}_p \Longleftrightarrow x_n = 0$$

であることからわかる． □

例 2.9. $\mathbb{Z}_2$ の元 x に対して

$$x(1+x) \in 2\mathbb{Z}_2$$

が成り立つ．

証明. $x = (x_i)_{i\in\mathbb{N}}$ とすると，$1 + x = (1 + x_i)_{i\in\mathbb{N}}$ である．$x_0 \in \mathbb{Z}/2\mathbb{Z}$ より x_0, $1 + x_0$ のいずれか一方は 0 である．したがって $x_0(1 + x_0) = 0$．ゆえに命題 2.7 より，ある $y \in \mathbb{Z}_p$ があって $x(1 + x) = 2y$ となる． □

定理 2.10. $x = (x_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_2^\times$ の元とする．このとき

$$x \in (\mathbb{Z}_2^\times)^2 \Longleftrightarrow x_2 = 1$$

が成り立つ．

証明.

(⇒) $x = y^2$ なる $y \in \mathbb{Z}_p^\times$ が存在したとする．$y = (y_i)_{i\in\mathbb{N}}$ とおくと $y_0 = 1$ である．よって命題 2.7 より $y - 1 \in 2\mathbb{Z}_2$．そこで $y = 1 + 2z\,(z \in \mathbb{Z}_2)$ とおくと

$$x = y^2 = (1 + 2z)^2 = 1 + 4z(1 + z)$$

ここで例 2.7 より，$z(1 + z) \in 2\mathbb{Z}_2$ であるから

$$x - 1 = 4z(1 + z) \in 8\mathbb{Z}_2$$

一方，$x - 1 = (x_i - 1)_{i\in\mathbb{N}}$ であるから，命題 2.7 より $x_2 - 1 = 0$ を得る．

(⇐) $x_2 = 1$ とする．このとき $x_0 = 1$, $x_1 = 1$ であるから，x の二進展開は

$$x = 1 + \sum_{k=3}^{\infty} a_k 2^k, \qquad a_k \in \{0, 1\}$$

と書ける．いま，$n \geq 3$ に対して，整数列 $(b_i)_{i\in\mathbb{N}}$ が存在して

$$y_{n-1} = 1 + \sum_{k=2}^{n-1} b_k 2^k$$

とおいたとき

$$(*)_n \qquad y_{n-1}^2 \equiv 1 + \sum_{k=3}^{n} a_k 2^k \pmod{2^{n+1}}$$

が満たされていることを，n に関する数学的帰納法で示す．

$n = 3$ のとき．$b_2 = a_3$ とおくと

$$y_2^2 = (1 + 4b_2)^2 = (1 + 4a_3)^2 \equiv 1 + 8a_3 \pmod{2^4}$$

となる．

次に，$n \geq 3$ として，$(*)_n$ を満たす y_{n-1} が上述のように取ることができたと仮定すると，ある $s \in \mathbb{Z}$ によって

$$y_{n-1}^2 = 1 + \sum_{k=3}^{n} a_k 2^k + s2^{n+1}$$

と書ける．任意の整数 $t \in \mathbb{Z}$ に対して

$$\begin{aligned}(y_{n-1} + t2^n)^2 &= (y_{n-1})^2 + ty_{n-1}2^{n+1} + t^2 2^{2n} \\ &\equiv 1 + \sum_{k=3}^{n} a_k 2^k + 2^{n+1}(s + ty_{n-1}) \pmod{2^{n+2}}\end{aligned}$$

が成り立つ．$y_{n-1} \equiv 1 \pmod 2$ だから，t についての一次合同式

$$s + ty_{n-1} \equiv a_{n+1} \pmod 2$$

は解 $b_n \in \mathbb{Z}/2\mathbb{Z}$ を満たす．したがって $y_0 = 1$, $y_1 = 1$ とおき，$y = (y_i)_{i\in\mathbb{N}}$ とおけば $x = y^2$ となる．$x \in \mathbb{Z}_2^\times$ より $y \in \mathbb{Z}_2^\times$ でなければならない．したがって $x \in (\mathbb{Z}_2^\times)^2$.

□

命題 2.11.

$$\mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

証明. $G = \mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2$ とおく．命題 1.5 より $x = (x_i)_{i\in\mathbb{N}} \in \mathbb{Z}_2$ について

$$x \in \mathbb{Z}_2^\times \iff x_0 = 1 \iff x_2 = 1, 3, 5, 7 \iff x_2 \in (\mathbb{Z}/8\mathbb{Z})^\times$$

である．よって写像

$$f : \mathbb{Z}_2^\times \longrightarrow (\mathbb{Z}/8\mathbb{Z})^\times, \qquad (x_i)_{i\in\mathbb{N}} \longmapsto x_2$$

を考えると，f は全射準同型である．定理 2.10 から，$x \in \mathbb{Z}_2$ について

$$x \in \operatorname{Ker} f \iff x_2 = 1 \iff x \in (\mathbb{Z}_2^\times)^2$$

したがって $\operatorname{Ker} f = (\mathbb{Z}_2)^\times$ となり，準同型定理により $G \cong (\mathbb{Z}/8\mathbb{Z})^\times$ を得る．一方，$(\mathbb{Z}/8\mathbb{Z})^\times$ は位数 4 の元であって，すべての元は 2 乗すると単位元に一致するから，$(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. したがって $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

とくに G の生成元として $3, 5, 7 \in \mathbb{Z}_p^\times$ を代表とする同値類のうち任意の 2 つがとれる．実際，それら 3 つの類は互いに異なり，かつ単位類とも一致しない. □

定理 2.12. p を奇素数とし，$x=(x_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_p^\times$ の元とする．このとき

$$x\in(\mathbb{Z}_p^\times)^2 \iff \left(\frac{x_0}{p}\right)=1$$

証明.

($\Rightarrow$)　$x=y^2$ なる $y\in\mathbb{Z}_p^\times$ が存在したとする．$y=(y_i)_{i\in\mathbb{N}}$ とおくと

$$x_i=y_i^2 \qquad (\forall i\in\mathbb{N})$$

が成り立つ．したがって特に $x_0=y_0^2$ が成り立つ．

($\Leftarrow$)　自然数 n に対して，合同式

$$(*)_n \qquad\qquad X^2\equiv x_n \pmod{p^{n+1}}$$

を考える．いま，$\left(\frac{x_0}{p}\right)=1$ ならば，整数列 $(a_k)_{k\in\mathbb{N}}$ が存在して

$$y_n=\sum_{k=0}^{n}a_kp^k$$

とおいたとき y_n が $(*)_n$ の解になることを示す．そうすれば $y=(y_i)_{i\in\mathbb{N}}$ とおいたとき $x=y^2$ が成り立つ．

$n=0$ のとき，$\left(\frac{x_0}{p}\right)=1$ より $a_0^2\equiv x_0 \pmod p$ を満たす $a_0\in\mathbb{Z}/p\mathbb{Z}$ が存在する．$y_0=a_0$ とおけば，y_0 は $(*)_0$ の解となる．

一般の n について，$(*)_n$ の解 $y_n=\sum_{k=0}^{n}a_kp^k$ が存在したと仮定する．このとき，ある $b\in\mathbb{Z}$ によって

$$y_n^2=x_n+bp^{n+1}$$

と書ける．一方，任意の $s\in\mathbb{Z}$ に対して

$$\begin{aligned}(y_n+sp^{n+1})^2&=y_n^2+2y_nsp^{n+1}+s^2p^{2(n+1)}\\&\equiv x_n+p^{n+1}(b+2y_ns) \pmod{p^{n+2}}\end{aligned}$$

となる．p は奇素数，$x\in\mathbb{Z}_p^\times$ だから

$$2y_n\equiv 2y_0=2x_0\not\equiv 0 \pmod p$$

よって s についての一次方程式

$$b+2y_ns\equiv 0 \pmod p$$

は解 $a_{n+1}\in\mathbb{Z}/p\mathbb{Z}$ を持つ．このとき

$$y_{n+1}=y_n+a_{n+1}p^{n+1}=\sum_{k=0}^{n+1}a_kp^k$$

が $(*)_{n+1}$ の解となる．

□

命題 2.13. p を奇素数とする．このとき $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ は位数 2 の群である．

証明. $G = \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ とおく．G の単位元でない元がただ一つ存在することをいえばよい．$x = (x_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_p^\times$ の元とすると，定理 2.12 より

$$x \in (\mathbb{Z}_p^\times)^2 \Longleftrightarrow \left(\frac{x_0}{p}\right) = 1$$

である．p を法とする平方剰余と平方非剰余は 0 を除いてちょうど半々ずつ存在するから，$(\mathbb{Z}_p)^\times$ の元であって，$(\mathbb{Z}_p^\times)^2$ の元でないようなものが存在する．すなわち G は単位元でない元をもつ．

次に，$x = (x_i)_{i\in\mathbb{N}}$, $y = (y_i)_{i\in\mathbb{N}}$ を $\mathbb{Z}_p^\times$ の元で $(\mathbb{Z}_p^\times)^2$ に属さないものとする．このとき $y^{-1} \in \mathbb{Z}_p^\times$ であり，また，上述のことから

$$\left(\frac{x_0}{p}\right) = \left(\frac{y_0}{p}\right) = -1, \qquad \left(\frac{x_0y_0}{p}\right) = \left(\frac{x_0}{p}\right)\left(\frac{y_0}{p}\right) = 1$$

したがって $xy \in (\mathbb{Z}_p^\times)^2$ となる．よって $xy^{-1} \in (\mathbb{Z}_p^\times)^2$ であるから，x, y は $(\mathbb{Z}_p^\times)^2$ を法として同じ同値類に属する．このことは G において，単位元以外の元がただ一つであることを示している．したがって G は位数 2 の群である． □

例 2.14. p を素数とする．このとき，$x^2 + 1 = 0$ を満たす $x \in \mathbb{Z}_p$ が存在するための必要十分条件は $p \equiv 1 \pmod 4$ である．

証明. $(-1)^2 = 1$ より，任意の素数 p に対して $-1 \in \mathbb{Z}_p^\times$ である．

$p = 2$ のとき，$\mathbb{Z}_2$ 内では

$$-1 = (-1,\, -1,\, -1, \ldots) = (1,\, 3,\, 7,\, \ldots)$$

であるから，$-1 = (y_i)_{i\in\mathbb{N}}$ とおくと $y_2 \neq 1$．したがって定理 2.10 より $-1 \notin (\mathbb{Z}_2^\times)^2$．すなわち $x^2 + 1 = 0$ を満たす $x \in \mathbb{Z}_p$ は存在しない．

p が奇素数のとき，$-1 = (y_i)_{i\in\mathbb{N}}$ とすると $y_0 \equiv -1 \pmod p$ である．よって平方剰余の相互法則 (より正確には第一補充法則) と定理 2.12 より

$$\begin{aligned} x^2 + 1 = 0 \text{ を満たす } x \in \mathbb{Z}_p \text{ が存在しない} &\Longleftrightarrow -1 \in (\mathbb{Z}_p^\times)^2 \\ &\Longleftrightarrow \left(\frac{y_0}{p}\right) = 1 \\ &\Longleftrightarrow \left(\frac{-1}{p}\right) = 1 \\ &\Longleftrightarrow p \equiv 1 \pmod 4 \end{aligned}$$

がいえる． □

3 p 進体

$\mathbb{Z}_p$ は整域だから，その商体が存在する．$\mathbb{Z}_p$ の商体を $\mathbb{Q}_p$ で表し，これを p **進体**という．$\mathbb{Z} \subseteq \mathbb{Z}_p$ だから $\mathbb{Q} \subseteq \mathbb{Q}_p$，したがって $\mathbb{Q}_p$ の標数は 0 である．

命題 3.1. $\mathbb{Q}_p$ の濃度は $\mathbb{R}$ の濃度に等しい.

証明. $\mathbb{Q}_p$ が $\mathbb{Z}_p$ の商体であることと命題 2.4 より

$$\operatorname{card} \mathbb{Q}_p \leq \operatorname{card} \mathbb{Z}_p \times \mathbb{Z}_p = \operatorname{card} \mathbb{Z}_p \cdot \operatorname{card} \mathbb{Z}_p = \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$$

一方，命題 2.4 と包含関係により

$$\mathfrak{c} = \operatorname{card} \mathbb{Z}_p \leq \operatorname{card} \mathbb{Q}_p$$

ゆえに Bernstein の定理より，$\mathfrak{c} = \operatorname{card} \mathbb{Q}_p$. □

命題 3.2. $\mathbb{Q}_p$ の 0 でない元 α は

$$(*) \qquad \alpha = p^e u, \qquad e \in \mathbb{Z}, \qquad u \in \mathbb{Z}_p^\times$$

と一意的に書ける.

証明. $\mathbb{Q}_p$ は $\mathbb{Z}_p$ の商体なので，α は

$$\alpha = \frac{y}{x}, \qquad x, y \in \mathbb{Z}_p, \qquad x \neq 0$$

と表すことができる．命題 2.5 より

$$x = p^m v, \qquad y = p^n w, \qquad m, n \in \mathbb{N}, \qquad v, w \in \mathbb{Z}_p^\times$$

と表せるから，$e = n - m$, $u = w/v$ とおけば α は $(*)$ のように表すことができる.

表し方の一意性は命題 2.5 のときと全く同じようにして，系 2.3 と命題 1.5 を用いて証明することができる. □

命題 3.3.

$$\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

証明. 命題 3.2 により，$\mathbb{Q}_2$ の元 α はすべて

$$\alpha = 2^e u, \qquad e \in \mathbb{Z}, \qquad u \in \mathbb{Z}_2^\times$$

と書ける．このとき

$$\alpha \in (\mathbb{Q}_2^\times)^2 \Longleftrightarrow e \equiv 0 \,(\mathrm{mod}\ 2) \text{ かつ } u \in (\mathbb{Z}_2^\times)^2$$

したがって定理 2.10 より

$$\{1, 2, u, v, w, 2u, 2v, 2w\}$$

が $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ の完全代表系である．ただし

$$u, v \in \mathbb{Z}_2^\times, \qquad u, v \notin (\mathbb{Z}_2^\times)^2, \qquad u \not\equiv v, \quad w \equiv uv \pmod{\mathbb{Z}_2^\times}$$

とする．このことから命題の同型を得る.

とくに，$2, u, v$ を代表元とする三つの同値類が $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ の生成元になる．u, v としては 3, 5, 7 のうちいずれか二つを選ぶことができる. □

命題 3.4. p を奇素数とする．このとき

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

が成り立つ．

証明. 命題 3.2 により，$\mathbb{Q}_p$ の元 α はすべて

$$\alpha = p^e u, \qquad e \in \mathbb{Z}, \qquad u \in \mathbb{Z}_p^\times$$

と書ける．このとき

$$\alpha \in (\mathbb{Q}_p^\times)^2 \iff e \equiv 0 \,(\mathrm{mod}\ 2) \text{ かつ } u \in (\mathbb{Z}_p^\times)^2$$

したがって定理 2.12 より

$$\{1,\ p,\ u,\ pu\}$$

が $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ の完全代表系である．ただし

$$u \in \mathbb{Z}_p^\times, \qquad u \notin (\mathbb{Z}_p^\times)^2$$

このことから命題の同型を得る．

とくに $p,\ u$ を代表元とする二つの同値類が $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ の生成元になる． □

4 p 進体の付値

p を素数とし，$\mathbb{Q}_p$ を p 進体，$\mathbb{Z}_p$ を p 進整数環とする．

$\mathbb{Q}_p^\times$ の元 α に対して

$$\alpha = p^e u, \qquad e \in \mathbb{Z}, \qquad u \in \mathbb{Z}_p^\times$$

と表したとき，α の p **進絶対値** $|\alpha|_p$ を

$$|\alpha|_p = p^{-e}$$

によって定める．0 に対しては $|0|_p = 0$ とする．

命題 4.1. $|*|_p$ は非アルキメデス付値をなす．すなわち

(i) $|\alpha| \geq 0$

(ii) $|\alpha|_p = 0 \iff \alpha = 0$

(iii) $|\alpha\beta|_p = |\alpha|_p|\beta|_p$

(iv) $|\alpha+\beta|_p \leq \max\{|\alpha|_p,\ |\beta|_p\}$

ただし $\alpha,\ \beta \in \mathbb{Q}_p$ とする．

証明. (i), (ii) は $|*|_p$ の定義から明らかである．

$$\alpha = p^m u, \qquad \beta = p^n v, \qquad m,\ n \in \mathbb{Z}, \qquad u,\ v \in \mathbb{Z}_p^\times$$

とおくと

$$\alpha\beta = p^{m+n}uv, \qquad m+n \in \mathbb{Z}, \qquad uv \in \mathbb{Z}_p^\times$$

となる．よって

$$|\alpha|_p|\beta|_p = p^{-m}\cdot p^{-n} = p^{-(m+n)} = |\alpha\beta|_p$$

すなわち (iii) が成り立つ．

さらに，$m \le n$ と仮定しても一般性を失わない．$m < n$ のとき

$$\alpha+\beta = p^m(u+p^{n-m}v), \qquad u+p^{n-m}v \in \mathbb{Z}_p^\times$$

$m = n$ のとき

$$\alpha+\beta = p^m(u+v), \qquad u+v \in \mathbb{Z}_p$$

いずれにせよ

$$|\alpha+\beta|_p \le p^{-m} = |\alpha|_p = \max\{|\alpha|_p,\, |\beta|_p\}$$

すなわち (iv) が成り立つ． □

命題 4.2.

(i) $\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \le 1\}$

(ii) 任意の $m \in \mathbb{N}$ に対して $p^{m+1}\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \le p^{-(m+1)}\}$.
とくに $p\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p < 1\}$.

(iii) $\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p = 1\}$

証明. 命題 2.5 より明らかである． □

$\mathbb{Q}_p$ の二つの元 $\alpha,\, \beta$ に対して，$\alpha,\, \beta$ の p **進距離**を

$$\rho_p(\alpha,\, \beta) = |\alpha-\beta|_p$$

と定める．$|*|_p$ は非アルキメデス付値なので，ρ_p は距離の公理を満たし，$(\mathbb{Q}_p,\, \rho_p)$ は距離空間をなす．

$\mathbb{Q}_p^\times$ の元 α に対して，$\mathrm{ord}_p(\alpha) = -\log|\alpha|_p$ と定義する．$\alpha = 0$ のときは $\mathrm{ord}_p(0) = \infty$ と定める．こうして定まる写像 $\mathrm{ord}_p : \mathbb{Q}_p \longrightarrow \mathbb{R}\cup\{\infty\}$ を p **進付値**という．

命題 4.3.

(i) $\mathrm{ord}_p(\alpha) \in \mathbb{Z} \qquad (\alpha \in \mathbb{Q}_p^\times)$

(ii) $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$

(iii) $\mathrm{ord}_p(\alpha+\beta) \ge \min\{\mathrm{ord}_p(\alpha),\, \mathrm{ord}_p(\beta)\}$

証明. p 進付置 ord_p の定義と，命題 4.1 からわかる． □

5　p 進体の元の列の収束について

$\mathbb{Q}_p$ の元の列 $(\alpha_n)_{n\in\mathbb{N}}$ が $\mathbb{Q}_p$ の元 α に**収束する**とは，任意の実数 $\varepsilon > 0$ に対して，ある自然数 N が存在して，自然数 n について

$$n \geq N \Longrightarrow |\alpha_n - \alpha|_p < \varepsilon$$

が成り立つことをいう．このとき α を $(\alpha_n)_{n\in\mathbb{N}}$ の**極限値**という．

命題 5.1.　$\mathbb{Q}_p$ の元の列 $(\alpha_n)_{n\in\mathbb{N}}$ が $\mathbb{Q}_p$ の元 α に収束すれば，$(\alpha_n)_{n\in\mathbb{N}}$ の任意の部分列 $(\alpha_{n_k})_{k\in\mathbb{N}}$ も α に収束する．

証明.　ε を正の実数とする．$(\alpha_n)_{n\in\mathbb{N}}$ は α に収束するので，ある自然数 N が存在して，任意の自然数 n について

$$n \geq N \Longrightarrow |\alpha_n - \alpha|_p < \varepsilon$$

が成り立つ．このとき

$$k \geq N \Longrightarrow n_k \geq N \Longrightarrow |\alpha_{n_k} - \alpha|_p < \varepsilon$$

である．したがって $(\alpha_{n_k})_{k\in\mathbb{N}}$ も α に収束する．　□

命題 5.2.　$\mathbb{Q}_p$ の元の列 $(\alpha_n)_{n\in\mathbb{N}}$ が $\mathbb{Q}_p$ の元 α に収束しているとする．$\alpha \neq 0$ ならば，ある自然数 M が存在して，任意の自然数 n について

$$n \geq M \Longrightarrow |\alpha_n|_p = |\alpha|_p$$

が成り立つ．すなわち，ある番号より大きいところでは $|\alpha_n|_p$ が一定になる．

証明.　$(\alpha_n)_{n\in\mathbb{N}}$ は収束列なので，任意の自然数 m に対して，ある自然数 N が存在して，任意の自然数 n について

$$\begin{aligned} n \geq N &\Longrightarrow |\alpha_n - \alpha|_p < p^{-m} \\ &\Longrightarrow \alpha_n - \alpha \in p^{m+1}\mathbb{Z}_p \\ &\Longrightarrow \alpha_n \in \alpha + p^{m+1}\mathbb{Z}_p \end{aligned}$$

一方，$\alpha \neq 0$ なので

$$\alpha = p^{m_0}u, \qquad m_0 \in \mathbb{Z}, \qquad u \in \mathbb{Z}_p^{\times}$$

と一意的に書ける．よって $m_1 = \max\{m_0, 1\}$ に対して，ある自然数 M をとれば，自然数 n について

$$\begin{aligned} n \geq M &\Longrightarrow \alpha_n \in p^{m_0}\mathbb{Z}_p^{\times} + p^{m_1+1}\mathbb{Z}_p = p^{m_0}\mathbb{Z}_p^{\times} \\ &\Longrightarrow |\alpha_n|_p = p^{-m_0} = |\alpha|_p \end{aligned}$$

が成り立つ．とくに M の取り方は自然数 m には依存しない．　□

命題 5.3.　$(\alpha_n)_{n\in\mathbb{N}}$, $(\beta_n)_{n\in\mathbb{N}}$ をそれぞれ $\mathbb{Q}_p$ の元 α, β に収束する $\mathbb{Q}_p$ の元の列とする．

(i)　$(\alpha_n + \beta_n)_{n\in\mathbb{N}}$ は $\alpha + \beta$ に収束する．

(ii)　$(-\alpha_n)_{n\in\mathbb{N}}$ は $-\alpha$ に収束する．

(iii)　$(\alpha_n\beta_n)_{n\in\mathbb{N}}$ は $\alpha\beta$ に収束する．

(iv)　$\alpha \neq 0$ かつ各 n に対して $\alpha_n \neq 0$ ならば $(1/\alpha_n)_{n\in\mathbb{N}}$ は $1/\alpha$ に収束する．

証明.

(i)
$$|(\alpha_n+\beta_n)-(\alpha+\beta)|_p = |(\alpha_n-\alpha)+(\beta_n-\beta)|_p \leq \max\{|\alpha_n-\alpha|_p,\, |\beta_n-\beta|_p\}$$

(ii)
$$|(-\alpha_n)-(-\alpha)|_p = |-(\alpha_n-\alpha)|_p = |\alpha_n-\alpha|_p$$

(iii)　$|\beta_n|_p \leq 0 (n \leq 0)$ のときは，十分大きな n に対して $|\beta_n|_p < M$ となるような正の実数 M が存在する．そうでないときは，十分大きな n に対して $|\beta_n|_p = |\beta|_p$ になる．そこでこのときは $M = |\beta|_p$ とおく．そうすればいずれの場合も十分大きな n に対して $|\beta_n| \leq M$ となって
$$\begin{aligned}|\alpha_n\beta_n-\alpha\beta|_p &= |(\alpha_n-\alpha)\beta_n+\alpha(\beta_n-\beta)|_p \\ &\leq \max\{|\alpha_n-\alpha|_p|\beta_n|_p,\, |\alpha|_p|\beta_n-\beta|_p\} \\ &\leq \max\{|\alpha_n-\alpha|_pM,\, |\alpha|_p|\beta_n-\beta|_p\}\end{aligned}$$
となる．

(iv)　十分大きい自然数 n に対して，$|\alpha_n|_p = |\alpha|_p$ となって
$$\left|\frac{1}{\alpha_n}-\frac{1}{\alpha}\right|_p = \frac{|\alpha_n-\alpha|_p}{|\alpha|_p|\alpha_n|_p} = \frac{|\alpha_n-\beta|_p}{|\beta|_p^2}$$
となる．

□

定理 5.4.　任意の $\alpha \in \mathbb{Q}_p$ に対し，α に収束する有理数列 $(\alpha_n)_{n\in\mathbb{N}}$ が存在する．

証明.　$\mathbb{Q}_p$ の元 α は
$$\alpha = p^e u, \qquad e \in \mathbb{Z}, \qquad u \in \mathbb{Z}_p^\times$$
と書ける．u を p 進展開して
$$u = \sum_{k=0}^{\infty} a_k p^k$$
とおいたとき，有理数列 $(\alpha_n)_{n\in\mathbb{N}}$ を
$$\alpha_n = \sum_{k=0}^{n} a_k p^{k+e}$$
とおくと，$(\alpha_n)_{n\in\mathbb{N}}$ は α に収束する．実際，自然数 n に対して
$$\begin{aligned}|\alpha_n-\alpha|_p &= \left|p^e\left(u-\sum_{k=0}^{n} a_k p^k\right)\right|_p \\ &= p^{-e}\left|u-\sum_{k=0}^{n} a_k p^k\right|_p \\ &\leq p^{-n-e} \to 0\ (n\to\infty)\end{aligned}$$
となる．

□

$\mathbb{Q}_p$ の元の列 $(\alpha_n)_{n\in\mathbb{N}}$ が $|*|_p$ について **Cauchy 列**をなすとは，任意の実数 $\varepsilon > 0$ に対して，ある自然数 N が存在して，自然数 m, n について

$$m,\, n \geq N \Longrightarrow |\alpha_m - \alpha_n|_p < \varepsilon$$

が成り立つことをいう．

実数体 $\mathbb{R}$ のときと同じような事実が $\mathbb{Q}_p$ についても成り立つ．

命題 5.5. $\mathbb{Q}_p$ の元 $(\alpha_n)_{n\in\mathbb{N}}$ について

$$(\alpha_n)_{n\in\mathbb{N}} \text{ がある } \alpha \in \mathbb{Q}_p \text{ に収束する} \Longleftrightarrow (\alpha_n)_{n\in\mathbb{N}} \text{ が Cauchy 列である}$$

証明.

($\Rightarrow$) 仮定より，実数 ε に対して，ある自然数 N が存在して，自然数 n について

$$n > N \Longrightarrow |\alpha_n - \alpha|_p < \varepsilon$$

とできる．よって，自然数 m, n について

$$m,\, n > N \Longrightarrow |\alpha_m - \alpha_n|_p \leq \max\{|\alpha_m - \alpha|_p,\, |\alpha_n - \alpha|_p\} < \varepsilon$$

が成り立つ．

($\Leftarrow$) まず，$\mathbb{Z}_p$ の元の Cauchy 列 $(\alpha_n)_{n\in\mathbb{N}}$ を考え

$$\alpha_n = \sum_{k=0}^{\infty} a_{n,k} p^k \qquad (p \text{ 進展開})$$

と表す．Cauchy 列の定義から，各自然数 e に対して，ある番号 $N(e)$ が存在して，自然数 m, n に対して

$$m,\, n > N(e) \Longrightarrow |\alpha_m - \alpha_n|_p < \frac{1}{p^e}$$

が成り立つ．一方

$$\begin{aligned} |\alpha_m - \alpha_n|_p < \frac{1}{p^e} &\Longleftrightarrow \alpha_m - \alpha_n \in p^{e+1}\mathbb{Z} \\ &\Longleftrightarrow a_{n,k} = a_{m,k}\ (0 \leq k \leq e) \end{aligned}$$

よって

$$m, n > N(e) \Longrightarrow a_{n,k} = a_{m,k}\ (0 \leq k \leq e)$$

となる．そこで，自然数 e に対して，$N(e)$ より大きい自然数 m について一定になる $a_{m,e}$ を a_e と定めることにする．こうして定まる数列 $(a_k)_{k\in\mathbb{N}}$ に対して

$$\alpha = \sum_{k=0}^{\infty} a_k p^k$$

とおくと，$(\alpha_n)_{n\in\mathbb{N}}$ は α に収束する．実際，任意の実数 $\varepsilon > 0$ に対して，$p^{-e} < \varepsilon$ なる自然数 e を一つとり，先ほどの $N(e)$ をとると α の定め方から

$$n > N(e) \Longrightarrow |\alpha_n - \alpha|_p = \left| \sum_{k=e+1}^{\infty} a_{e+1} p^k \right|_p \leq \frac{1}{p^{e+1}} < \varepsilon$$

が成り立つ．次に，$\mathbb{Q}_p$ の元の Cauchy 列 $(\alpha_n)_{n\in\mathbb{N}}$ について考える．Cauchy 列の定義から，任意の実数 $\varepsilon > 0$ に対して，ある自然数 N があって，自然数 m, n について

$$m, n > N \Longrightarrow |\alpha_m - \alpha_n|_p < \varepsilon$$

が成り立つ．まず，有限個を除いて $|\alpha_m|_p$ が一定である場合を考える．このとき自然数 N をとりなおして

$$m, n > N \Longrightarrow |\alpha_m|_p = |\alpha_n|_p$$

が成り立つとしてよい．そこで N より大きい番号について一定な $|\alpha_m|_p$ の値を p^{-e} とおき

$$\beta_m = \begin{cases} 0, & m \leq N \\ p^{-e}\alpha_m, & m > N \end{cases}$$

によって列 $(\beta_m)_{m\in\mathbb{N}}$ を定める．$(\beta_m)_{m\in\mathbb{N}}$ は Cauchy 列になる．実際，実数 $\varepsilon > 0$ に対して，ある番号 $N_1 > N$ があって

$$m, n > N_1 \Longrightarrow |\alpha_m - \alpha_n|_p < \frac{\varepsilon}{p^e}$$

とできる．したがって

$$m, n > N_1 \Longrightarrow |\beta_m - \beta_n|_p = p^e|\alpha_m - \alpha_n|_p < \varepsilon$$

となる．$(\beta_m)_{m\in\mathbb{N}}$ は $\mathbb{Z}_p$ の元の列なので，先に述べたことから極限値 β をもつ．このとき $\alpha = p^e\beta$ が $(\alpha_n)_{n\in\mathbb{N}}$ の極限値になる．実際，実数 $\varepsilon > 0$ に対して，十分大きい自然数 $N_2 > N$ をとると，自然数 n に対して

$$n > N_2 \Longrightarrow |\alpha_n - \alpha|_p = p^{-e}|\beta_n - \beta|_p < \varepsilon$$

とできる．

次に，$|\alpha_m|_p$ の値が異なるような α_m が無限個あったとする．$(\alpha_n)_{n\in\mathbb{N}}$ からこのようなものを順番に抜き出してできる部分列を $(\alpha_m)_{m\in\mathbb{N}}$ とする．$\alpha'_m \neq \alpha'_n$ ならば，非アルキメデス付値の性質から

$$|\alpha'_m - \alpha'_n|_p = \max\{|\alpha'_m|_p, |\alpha'_n|_p\}$$

よって任意の実数 $\varepsilon > 0$ に対して，ある番号 N があって，自然数 m について

$$m > N \Longrightarrow |\alpha'_m|_p \leq \max\{|\alpha'_m|_p, |\alpha'_{N+1}|_p\} = |\alpha'_m - \alpha'_{N+1}|_p < \varepsilon$$

すなわち $(\alpha'_m)_{m\in\mathbb{N}}$ は 0 に収束する．したがって，十分大きい番号 N_1 をとると，自然数 m, $n > N_1$ に対して

$$|\alpha_n|_p = |(\alpha_n - \alpha'_m) + \alpha'_m|_p \leq \max\{|\alpha_n - \alpha'_m|_p, |\alpha'_m|_p\} < \varepsilon$$

とできる．よって $(\alpha_n)_{n\in\mathbb{N}}$ も 0 に収束する．

□

$\mathbb{Q}_p$ の元の列 $(\alpha_n)_{n\in\mathbb{N}}$ に対し，列 $(\beta_n)_{n\in\mathbb{N}}$ を

$$\beta_n = \sum_{k=0}^{n} \alpha_k$$

によって定める．$(\beta_n)_{n\in\mathbb{N}}$ が極限値をもつとき，その極限値を

$$\sum_{n=0}^{\infty} \alpha_n$$

と表す.

命題 5.6. $\mathbb{Q}_p$ の元の列 $(\alpha_n)_{n\in\mathbb{N}}$ について，次の三つの条件は同値である：

(i) $\displaystyle\sum_{n=0}^{\infty} \alpha_n$ が収束する

(ii) $n \to \infty$ のとき $\mathbb{R}$ の中で $|\alpha_n|_p \to 0$ となる

(iii) $(\alpha_n)_{n\in\mathbb{N}}$ が $\mathbb{Q}_p$ の中で 0 に収束する．

証明.

(i)⇔(ii) $s_n = \displaystyle\sum_{k=0}^{n} \alpha_k$ とおくと，命題 5.5 より $(s_n)_{n\in\mathbb{N}}$ が収束することと $(s_n)_{n\in\mathbb{N}}$ が Cauchy 列であることとは同値である．また，後者は $|\alpha_n|_p \to 0$ $(n \to \infty)$ と同値である．実際，$(s_n)_{n\in\mathbb{N}}$ が Cauchy 列ならば

$$|\alpha_{N+2}|_p = |s_{N+2} - s_{N+1}|_p \to 0 \qquad (n \to \infty)$$

となる．逆に，$|\alpha_n|_p \to 0$ $(n \to \infty)$ ならば

$$|s_m - s_n|_p = |\alpha_m + \cdots + \alpha_{n+1}|_p \leq \max\{|\alpha_m|_p, \ldots, |\alpha_{n+1}|_p\} \to 0 \qquad (n \to \infty)$$

となる.

(ii)⇔(iii) 収束の定義から明らかである.

□

命題 5.7. $\displaystyle\sum_{n=0}^{\infty} \alpha_n$, $\displaystyle\sum_{n=0}^{\infty} \beta_n$ がそれぞれ α, β に収束するとき

$$\gamma_n = \sum_{k=0}^{n} \alpha_k \beta_{n-k}$$

とおくと，$\displaystyle\sum_{n=0}^{\infty} \gamma_n$ は収束し

$$\sum_{n=0}^{\infty} \gamma_n = \alpha\beta$$

が成り立つ.

証明. 命題 5.6 より，$|\alpha_n|_p \to 0$, $|\beta_n|_p \to 0$ $(n \to \infty)$ であるから，$|\alpha_n|_p$, $|\beta_n|_p$ は上に有界である．すなわち，ある正の実数 M が存在して，すべての自然数 n について $|\alpha_n|_p < M$, $|\beta_n|_p < M$ となる．ε を正の実数とすると，ある自然数 N が存在して，任意の自然数 n に対して

$$n \geq N \Longrightarrow |\alpha_n|_p < \frac{\varepsilon}{M}, \quad |\beta_n|_p < \frac{\varepsilon}{M}$$

が成り立つ．このとき，$2N$ よりも大きい自然数 n に対して

$$\begin{aligned}
|\gamma_n|_p &= \left| \sum_{k=0}^{n} \alpha_k \beta_{n-k} \right|_p \\
&\leq \max_{0 \leq k \leq n} |\alpha_k|_p |\beta_{n-k}|_p \\
&< M \max\{|\beta_n|_p, \ldots, |\beta_{[\frac{n+1}{2}]}|_p, |\alpha_{[\frac{n+1}{2}]}|_p, \ldots, |\alpha_n|_p\} \\
&< M \cdot \frac{\varepsilon}{M} = \varepsilon
\end{aligned}$$

が成り立つ．ゆえに $|\gamma_n|_p \to \infty$ $(n \to \infty)$．したがって命題 5.6 より $\displaystyle\sum_{n=0}^{\infty} \gamma_n$ は収束する．

正の整数 m について

$$\begin{aligned}
\left| \sum_{n=0}^{2m} \gamma_n - \sum_{s=0}^{m} \alpha_s \sum_{t=0}^{m} \beta_t \right|_p &= \left| \sum_{t=m+1}^{2m} \sum_{s=0}^{2m-t} \alpha_s \beta_t + \sum_{s=m+1}^{2m} \sum_{t=0}^{2m-s} \alpha_s \beta_t \right|_p \\
&\leq \max\left\{ \left| \sum_{t=m+1}^{2m} \sum_{s=0}^{2m-t} \alpha_s \beta_t \right|_p, \left| \sum_{s=m+1}^{2m} \sum_{t=0}^{2m-s} \alpha_s \beta_t \right|_p \right\}
\end{aligned}$$

一方，命題 5.6 より $|\alpha_s|_p \to 0$ $(s \to \infty)$ であるから，$|\alpha_s|_p$ は上に有界である．その上界を M とおくと

$$\begin{aligned}
\left| \sum_{t=m+1}^{2m} \sum_{s=0}^{2m-t} \alpha_s \beta_t \right|_p &\leq \max_{m+1 \leq t \leq 2m} \left| \sum_{s=0}^{2m-t} \alpha_s \beta_t \right|_p \\
&\leq \max_{\substack{m+1 \leq t \leq 2m \\ 0 \leq s \leq 2m-t}} \{|\alpha_s|_p |\beta_t|_p\} \\
&\leq M \max_{m+1 \leq t \leq 2m} \{|\beta_t|_p\} \to 0 \qquad (m \to \infty)
\end{aligned}$$

ここで，最後の収束は命題 5.6 を用いた．同様にして

$$\left| \sum_{s=m+1}^{2m} \sum_{t=0}^{2m-s} \alpha_s \beta_t \right|_p \to 0 \qquad (m \to \infty)$$

したがって

$$\sum_{n=0}^{2m} \gamma_n - \sum_{s=0}^{m} \alpha_s \sum_{t=0}^{m} \beta_t \to 0 \qquad (m \to \infty)$$

がいえる．したがって

$$\sum_{n=0}^{\infty} \gamma_n = \sum_{n=0}^{\infty} \alpha_n \sum_{n=0}^{\infty} \beta_n$$

が成り立つ． □

6　p 進体の指数関数・対数関数

命題 6.1.　p を素数とする．正の整数 n に対して

$$\mathrm{ord}_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^m} \right]$$

が成り立つ．

証明.　$\left[\dfrac{n}{p^m} \right]$ は 1 から n までの整数のうち p^m で割り切れるものの個数であり，$n > \log_p n$ すなわち $p^m > n$ ならば $\left[\dfrac{n}{p^m} \right] = 0$ である．ゆえに

$$\mathrm{ord}_p(n!) = \mathrm{ord}_p\Big(\prod_{\substack{1 \le x \le n \\ p \mid x}} x \Big) = \sum_{\substack{1 \le x \le n \\ p \mid x}} \mathrm{ord}_p(x) = \sum_{m=1}^{[\log_p n]} \left[\frac{n}{p^m} \right] = \sum_{m=1}^{\infty} \left[\frac{n}{p^m} \right]$$

である．　□

命題 6.2.　c を実数，n を正の整数，p を素数とする．

(i)　$nc - \mathrm{ord}_p(n!) \to \infty \ (n \to \infty) \iff c > \dfrac{1}{p-1}$

(ii)　$nc - \mathrm{ord}_p(n) \to \infty \ (n \to \infty) \iff c > 0$

(iii)　$c \ge \dfrac{1}{p-1} \implies nc - \mathrm{ord}_p(n!) \ge c$

証明.

(i)　$c > \dfrac{1}{p-1}$ と仮定すると

$$nc - \mathrm{ord}_p(n!) \ge nc - \sum_{i=1}^{\infty} \frac{n}{p^i} \ge nc - \frac{n}{p-1} \to \infty \qquad (n \to \infty)$$

である．逆に，$nc - \mathrm{ord}_p(n!) \to \infty \ (n \to \infty)$ とすると

$$p^m c - \mathrm{ord}_p(p^m!) \to \infty \qquad (m \to \infty)$$

が成り立つ．一方，命題 6.1 より

$$p^m c - \mathrm{ord}_p(p^m!) = p^m c - \sum_{i=1}^{m} p^{m-i} = p^m \left(c - \frac{1}{p-1} \right) + \frac{1}{p-1}$$

これが ∞ に発散するためには $c > \dfrac{1}{p-1}$ でなければならない．

(ii)　$\log_p n$ を実数体 $\mathbb{R}$ における p を底とする n の対数とすると，$\mathrm{ord}_p(n) \ge \log_p n$ ゆえ

$$nc - \mathrm{ord}_p(n) \ge nc - \log_p n$$

これは $c > 0$ のとき ∞ に発散する．逆に，$nc - \mathrm{ord}_p(n) \to \infty$ ならば

$$p^m c - \mathrm{ord}_p(p^m) \to \infty \qquad (m \to \infty)$$

一方

$$p^m c - \mathrm{ord}_p(p^m) = p^m c - m = m\left(\frac{p^m}{m}c - 1\right)$$

これが ∞ に発散するためには $c > 0$ であることが必要である．

(iii)　命題 6.1 より

$$\mathrm{ord}_p(n!) = \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right] < \sum_{i=1}^{\infty}\frac{n}{p^i} = \frac{n}{p-1}$$

である．一方，$\dfrac{n}{p-1}$ より小さい整数は $\dfrac{n-1}{p-1}$ 以下であるから

$$\mathrm{ord}_p(n!) \leq \frac{n-1}{p-1}$$

である．よって $c > \dfrac{1}{p-1}$ ならば

$$nc - \mathrm{ord}_p(n!) - c \geq (n-1)\left(c - \frac{1}{p-1}\right) \geq 0$$

となる．

□

命題 6.3.

(i)　$x \in \mathbb{Q}_p$ について

$$\sum_{n=0}^{\infty}\frac{x^n}{n!} \text{ が収束} \iff x \in p^m\mathbb{Z}_p$$

である．ただし p が奇素数のとき $m = 1$, $p = 2$ のとき $m = 2$ とする．

証明．　すべての自然数 n に対して

$$\mathrm{ord}_p\left(\frac{x^n}{n!}\right) = n\,\mathrm{ord}_p(x) - \mathrm{ord}_p(n!)$$

である．したがって命題 6.2 (i) によって

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{x^n}{n!} \text{ が収束する} &\iff \mathrm{ord}_p\left(\frac{x^n}{n!}\right) \to \infty \qquad (n \to \infty)\\ &\iff n\,\mathrm{ord}_p(x) - \mathrm{ord}_p(n!) \to \infty \qquad (n \to \infty)\\ &\iff \mathrm{ord}_p(x) > \frac{1}{p-1}\end{aligned}$$

p が奇素数ならば

$$\mathrm{ord}_p(x) > \frac{1}{p-1} \iff \mathrm{ord}_p(x) \geq 1 \iff x \in p\mathbb{Z}_p$$

$p = 2$ ならば

$$\mathrm{ord}_p(x) > \frac{1}{p-1} \iff \mathrm{ord}_2(x) > 1 \iff \mathrm{ord}_2(x) \geq 2 \iff x \in 4\mathbb{Z}_2$$

である．

□

そこで，p が奇素数のときは $x \in p\mathbb{Z}_p$ に対して，$p = 2$ のときは $x \in 4\mathbb{Z}_2$ に対して

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

とおく．

命題 6.4. x, y がともに exp の収束域に属するならば

$$\exp(x+y) = \exp(x)\exp(y)$$

が成り立つ．

証明. 命題 5.7 より

$$\exp(x)\exp(y) = \sum_{n=0}^{\infty} \gamma_n$$

ただし

$$\gamma_n = \sum_{k=0}^{n} \frac{x^k}{k!}\frac{y^{n-k}}{(n-k)!} = \frac{1}{n!}\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \frac{1}{n!}(x+y)^n$$

したがって

$$\exp(x)\exp(y) = \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \exp(x+y)$$

となる． □

命題 6.5. $x \in \mathbb{Q}_p$ について

$$\sum_{n=0}^{\infty} \frac{(-1)^{n-1}}{n} x^n \text{ が収束} \iff x \in p\mathbb{Z}_p$$

である．

証明. すべての正の整数 n に対して

$$\mathrm{ord}_p\left(\frac{(-1)^{n-1}}{n}x^n\right) = n\,\mathrm{ord}_p(x) - \mathrm{ord}_p(n)$$

である．したがって命題命題 6.2 (i) によって

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n \text{ が収束する} &\iff \mathrm{ord}_p\left(\frac{(-1)^{n-1}}{n}x^n\right) \to \infty \qquad (n \to \infty) \\
&\iff n\,\mathrm{ord}_p(x) - \mathrm{ord}_p(n) \to \infty \qquad (n \to \infty) \\
&\iff \mathrm{ord}_p(x) > 0 \\
&\iff \mathrm{ord}_p(x) \in p\mathbb{Z}_p
\end{aligned}$$

□

そこで，$x - 1 \in p\mathbb{Z}_p$ なる x に対して

$$\log(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(x-1)^n$$

とおく．

補題 6.6 (形式的べき級数の反転). 形式的べき級数

$$f(x) = x + a_2x^2 + \cdots + a_nx^n + \cdots$$

が与えられたとき，$k \geq 2$, $m \geq 2$ に対して

$$\begin{aligned} a_k^{(1)} &= a_k, \\ a_{m+k}^{(m+1)} &= a_k + a_{k-1}a_{m+1}^{(m)} + a_{k-2}a_{m+2}^{(m)} + \cdots + a_2a_{m+k-2}^{(m)} + a_{m+k-1}^{(m)} \end{aligned}$$

とおき

$$\begin{aligned} b_1 &= 1, \\ b_n &= -b_{n-1}a_n^{(n-1)} - b_{n-2}a_n^{(n-2)} - \cdots - a_n^{(1)} \qquad (n \geq 2) \end{aligned}$$

によって形式的べき級数 $g(x) = \sum_{n=1}^{\infty} b_nx^n$ を定めれば

$$f(g(x)) = g(f(x)) = x$$

が成り立つ.

証明. 概略を示す．いま $y = f(x)$ とおき，$m \geq 1$ について

$$y^k = x^k + a_{k+1}^{(k)}x^{k+1} + a_{k+2}^{(k)}x^{k+2} \cdots$$

とおくと，各 $a_n^{(m)}$ は

$$\begin{aligned} a_k^{(1)} &= a_k, \\ a_{m+k}^{(m+1)} &= a_k + a_{k-1}a_{m+1}^{(m)} + a_{k-2}a_{m+2}^{(m)} + \cdots + a_2a_{m+k-2}^{(m)} + a_{m+k-1}^{(m)} \end{aligned}$$

によって計算できる．一方

$$1 = b_1, \qquad 0 = b_n + b_{n-1}a_n^{(n-1)} + \cdots + b_1a_n^{(1)} \ (n \geq 2)$$

であることが

$$x = b_1y + b_2y^2 + \cdots + b_ny^n + \cdots$$

であるための必要十分条件である. □

$f(x) = \exp(x) - 1$, $g(x) = \log(1 + x)$ とおき，上の補題を用いて計算すると

$$\exp(\log(1 + x)) = 1 + x, \qquad \log(\exp(x)) = x$$

が確かめられる.

注意 6.7. 実は，直接確かめるのは簡単ではない．ただし，少なくとも実数における exp と log については，級数が収束する範囲において上の事実は正しいので，形式的べき級数において上の事実が正しくないということはないはずである (実数の場合はまず指数関数 exp を定義し，exp が単調増加連続関数であるという事実から逆関数が存在することが言える．その逆関数を log と定義したのち，Taylor 展開や逆関数の微分を考えることによって上の事実を導く).

定理 6.8. p が奇素数なら $m \geq 1$, $p = 2$ なら $m \geq 2$ とする．このとき exp と log は，群としての互いに逆な同型

$$p^m\mathbb{Z}_p \cong 1 + p^m\mathbb{Z}_p$$

を与える．ただし，$p^m\mathbb{Z}_p$ は加法群，$1 + p^m\mathbb{Z}_p$ は乗法群であるとする．

証明. 命題 6.2 (iii) より，$x \in p^m\mathbb{Z}_p$ ならば，$n \geq 1$ のとき

$$\begin{aligned}\mathrm{ord}_p\left(\frac{x^n}{n!}\right) &= n\,\mathrm{ord}_p(x) - \mathrm{ord}_p(n!)\\ &\geq \mathrm{ord}_p(x)\\ &\geq m\end{aligned}$$

ゆえに

$$x \in p^m\mathbb{Z}_p \Longrightarrow \exp(x) - 1 \in p^m\mathbb{Z}_p$$

また，再び命題 6.2 (iii) より，$x \in 1 + p^n\mathbb{Z}_p$ ならば，$n \geq 1$ のとき

$$\begin{aligned}\mathrm{ord}_p\left((-1)^{n-1}\frac{(x-1)^n}{n}\right) &= n\,\mathrm{ord}_p(x-1) - \mathrm{ord}_p(n)\\ &\geq n\,\mathrm{ord}_p(x-1) - \mathrm{ord}_p(n!)\\ &\geq \mathrm{ord}_p(x-1)\\ &\geq m\end{aligned}$$

ゆえに

$$x \in 1 + p^m\mathbb{Z}_p \Longrightarrow \log(x) \in p^m\mathbb{Z}_p$$

形式的べき級数として $\exp(\log(x)) = x$, $\log(\exp(x)) = x$ が成り立つことはすでに示されている．よって以上で exp, log が互いに逆写像であることが示された．exp が準同型写像であることも既に示されているので，log もまた準同型写像でなければならない．すなわち

$$\log(xy) = \log(x) + \log(y)$$

が成り立つ. □

参考文献

[1] 斎藤秀司：整数論，共立出版株式会社（1997）

[2] 加藤和也，黒川重信，斎藤毅：数論 1，岩波書店（1996）

[3] 松坂和夫：集合・位相入門，岩波書店（1968）