1　Hom の計算例

[定理 1] $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})=0$.

[証明] $f\in\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ とする.

任意の $m,n\in\mathbb{Z}$, $n\neq 0$, $\gcd(m,n)=1$ に対して,

$$n\cdot f\left(\frac{m}{n}\right)=f\left(n\cdot\frac{m}{n}\right)=f(m)=m\cdot f(1).$$

$f(\mathbb{Q})\subseteq\mathbb{Z}$ なので, n は $f(1)$ を割る.

特に, $m=1$ とし, n として素数 p をとれば, p は $f(1)$ の約数である. もし仮に $f(1)\neq 0$ ならば, p の取り方は任意なので, $f(1)$ は無数の素因子を持つことになり矛盾する. したがって, $f(1)=0$ でなければならない.

すると, $f(m/n)=0$ がいえる. ゆえに, $f=0$. □

[定理 2] M を可除 $\mathbb{Z}$ 加群とする[1]. このとき, $\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})=0$ が成り立つ.

[証明] $f\in\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$, すなわち, $f:M\to\mathbb{Z}$ を $\mathbb{Z}$ 準同型とする.

M が可除 $\mathbb{Z}$ 加群ならば, $f(M)$ もまた可除 $\mathbb{Z}$ 加群である. 実際, $u\in M$ を任意にとると, M は可除 $\mathbb{Z}$ 加群だから, 任意の $r\in\mathbb{Z}$ に対して, ある $v\in M$ が存在して, $u=rv$. ゆえに,

$$f(u)=f(rv)=r\cdot f(v).$$

よって, 任意の $u\in M$ と任意の素数 p に対して, ある $v\in M$ が存在して, $f(u)=p\cdot f(v)$ となる. $f(v)\in\mathbb{Z}$ だから, $f(u)$ は p で割り切れる. もし仮に $f(u)\neq 0$ ならば, p は任意なので, $f(u)$ は無数の素因子を持つことになり矛盾する. ゆえに, $f(u)=0$ でなければならない. したがって, $f=0$ となる. □

[例 3] $\mathbb{Q}$ は可除 $\mathbb{Z}$ 加群である. 実際, 任意の $x\in\mathbb{Q}$, $r\in\mathbb{Z}$ に対して, $y=x/r$ とおけば, $x=ry$, $y\in\mathbb{Q}$ となる. したがって, 再び $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})=0$ が示された.

[例 4] $\mathbb{Q}/\mathbb{Z}$ は可除 $\mathbb{Z}$ 加群である. 実際, 任意の $x\in\mathbb{Q}$, $r\in\mathbb{Z}$ に対して, $y=x/r$ とおけば,

$$x+\mathbb{Z}=ry+\mathbb{Z}=r\cdot(y+\mathbb{Z})$$

となる. したがって, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z},\mathbb{Z})=0$.

---

[1] すなわち, 任意の $x\in M$, $r\in\mathbb{Z}$ に対して, ある $y\in M$ が存在して, $x=ry$ が成り立つものとする.

[定理 5] R を環とする. 任意の左 R 加群 M に対して, $\mathrm{Hom}_R(R, M) \cong M$.

[証明] $H = \mathrm{Hom}_R(R, M)$ とおく. 写像 φ を

$$\varphi : H \to M, \quad f \mapsto f(1)$$

によって定める.

任意の $f, g \in H$ と $r \in R$ に対して

$$\varphi(f+g) = (f+g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g),$$
$$\varphi(rf) = (rf)(1) = r \cdot f(1) = r \cdot \varphi(f).$$

ゆえに, φ は R 準同型である.

各 $x \in M$ に対して, 写像 $f_x : R \to M$ を, 各 $r \in R$ に対して,

$$f_x(a) = ax$$

とおくことによって定める. 任意の $a, b, r \in R$ に対して,

$$f_x(a+b) = (a+b)x = ax + bx = f_x(a) + f_x(b),$$
$$f_x(ra) = (ra)x = r(ax) = r \cdot f_x(a).$$

ゆえに, f_x は R 準同型である. すなわち, $f_x \in H$. これより, 写像

$$\psi : M \to H, \quad x \mapsto f_x.$$

が定まる.

φ が全単射であることを示すために, ψ が φ の逆写像であることを示す. 任意の $x \in M$ に対して,

$$\varphi \circ \psi(x) = \varphi(f_x) = f_x(1) = 1 \cdot x = x.$$

逆に, 任意の $f \in H$ に対して, $y = f(1)$ とおくと,

$$\psi \circ \varphi(f) = \psi(y) = f_y.$$

一方, 任意の $a \in R$ に対して,

$$f_y(a) = ay = a \cdot f(1) = f(a).$$

ゆえに, $f_y = f$. よって, $\psi \circ \varphi(f) = f$. したがって, ψ は φ の逆写像であり, φ は全単射である.

以上より, φ が R 加群の同型であることが示された. □

[例 6] 任意の環 R に対して, $\mathrm{Hom}_R(R, R) \cong R$.

$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}) \cong \mathbb{Q}$.

m を 2 以上の整数とするとき, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$.

[定理 7] m を正の整数とするとき, 任意の $\mathbb{Z}$ 加群 M に対して, $\mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, M) \cong M$.

[証明] $H = \mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, M)$ とおく. 写像 φ を

$$\varphi : H \to M, \quad f \mapsto f(m)$$

によって定める.

任意の $f, g \in H$ と $r \in \mathbb{Z}$ に対して

$$\varphi(f+g) = (f+g)(m) = f(m) + g(m) = \varphi(f) + \varphi(g),$$
$$\varphi(rf) = (rf)(m) = r \cdot f(m) = r \cdot \varphi(f).$$

ゆえに, φ は $\mathbb{Z}$ 準同型である.

各 $x \in M$ に対して, 写像 $f_x : m\mathbb{Z} \to M$ を, 各 $r \in \mathbb{Z}$ に対して,

$$f_x(ma) = ax$$

とおくことによって定める. 任意の $a, b, r \in \mathbb{Z}$ に対して,

$$f_x(ma + mb) = (a+b)x = ax + bx = f_x(ma) + f_x(mb),$$
$$f_x(r(ma)) = f_x(m(ra)) = (ra)x = r(ax) = r \cdot f_x(ma).$$

ゆえに, f_x は $\mathbb{Z}$ 準同型である. すなわち, $f_x \in H$. これより, 写像

$$\psi : M \to H, \quad x \mapsto f_x.$$

が定まる.

φ が全単射であることを示すために, ψ が φ の逆写像であることを示す. 任意の $x \in M$ に対して,

$$\varphi \circ \psi(x) = \varphi(f_x) = f_x(m) = f_x(m \cdot 1) = 1 \cdot x = x.$$

逆に, 任意の $f \in H$ に対して, $y = f(m)$ とおくと,

$$\psi \circ \varphi(f) = \psi(y) = f_y.$$

一方, 任意の $a \in \mathbb{Z}$ に対して,

$$f_y(ma) = ay = a \cdot f(m) = f(ma).$$

ゆえに, $f_y = f$. よって, $\psi \circ \varphi(f) = f$. したがって, ψ は φ の逆写像であり, φ は全単射である.

以上より, φ が $\mathbb{Z}$ 加群の同型であることが示された. $\square$

[別証] m 倍写像

$$[m] : \mathbb{Z} \to m\mathbb{Z}, \quad x \mapsto mx$$

は $\mathbb{Z}$ 加群の同型であり, その逆写像は

$$[m^{-1}] : m\mathbb{Z} \to \mathbb{Z}, \quad mx \mapsto x$$

である. これより, 任意の $\mathbb{Z}$ 加群 M に対して, $\mathbb{Z}$ 加群の同型

$$\varphi : \mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, M) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M), \quad f \mapsto f \circ [m]$$

が定まる. 実際, $H = \mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, M)$ とおくと, 任意の $f,\, g \in H$ と任意の $r,\, x \in \mathbb{Z}$ に対して,

$$\begin{aligned}
\varphi(f+g)(x) &= ((f+g)\circ[m])(x) = (f+g)(mx) \\
&= f(mx) + g(mx) \\
&= (f\circ[m])(x) + (g\circ[m])(x) \\
&= \varphi(f)(x) + \varphi(g)(x) \\
&= (\varphi(f) + \varphi(g))(x). \\
\varphi(rf)(x) &= ((rf)\circ[m])(x) = (rf)(mx) \\
&= r\cdot f(mx) = r\cdot(f\circ[m])(x) \\
&= r\cdot\varphi(f)(x).
\end{aligned}$$

ゆえに, φ は準同型である. さらに,

$$\psi : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) \to \mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, M), \quad g \mapsto g \circ [m^{-1}]$$

が φ の逆写像になる. 実際, $H' = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M)$ とおくと, 任意の $f \in H$, $g \in H'$ に対して,

$$\begin{aligned}
\psi\circ\varphi(f) &= \psi(f\circ[m]) = (f\circ[m])\circ[m^{-1}] = f\circ([m]\circ[m^{-1}]) = f, \\
\varphi\circ\psi(g) &= \varphi(g\circ[m^{-1}]) = (g\circ[m^{-1}])\circ[m] = g\circ([m^{-1}]\circ[m]) = g.
\end{aligned}$$

ゆえに, φ は全単射である. よって確かに, φ は同型である.

このとき, 同型

$$\mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, M) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) \cong M$$

が成り立つ. □

[例 8] m を正の整数とするとき, $\mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, \mathbb{Q}) \cong \mathbb{Q}$.

m, n を正の整数とするとき, $\mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, n\mathbb{Z}) \cong n\mathbb{Z} \cong \mathbb{Z}$.

m, n を正の整数とするとき, $\mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

[定理 9] R を整域, K をその商体とするとき, $\mathrm{Hom}_R(K, K) \cong K$.

[証明] $H = \mathrm{Hom}_R(K, K)$ とおく. 写像 φ を

$$\varphi : H \to K, \quad f \mapsto f(1)$$

によって定める.

任意の $f, g \in H$ と $r \in R$ に対して

$$\begin{aligned}\varphi(f+g) &= (f+g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g),\\ \varphi(rf) &= (rf)(1) = r \cdot f(1) = r \cdot \varphi(f).\end{aligned}$$

ゆえに, φ は R 準同型である.

各 $a \in K$ に対して, 写像 $f_a : K \to K$ を, 各 $x \in K$ に対して,

$$f_a(x) = ax$$

とおくことによって定めると, 任意の $x, y \in K$, $r \in R$ に対して,

$$\begin{aligned}f_a(x+y) &= a(x+y) = ax + ay = f_a(x) + f_a(y),\\ f_a(rx) &= a(rx) = r(ax) = r \cdot f(x).\end{aligned}$$

ゆえに, f_a は R 準同型である. すなわち, $f_a \in H$. これより, 写像

$$\psi : K \to H, \quad a \mapsto f_a$$

が定まる.

φ が全単射であることを示すために, ψ が φ の逆写像であることを示す. 任意の $a \in K$ に対して,

$$\varphi \circ \psi(a) = \varphi(f_a) = f_a(1) = a.$$

逆に, 任意の $f \in H$ に対して, $b = f(1)$ とおくと,

$$\psi \circ \varphi(f) = \psi(b) = f_b.$$

一方, 任意の $m, n \in R$, $n \neq 0$ に対して,

$$\begin{aligned}n \cdot f_b\left(\frac{m}{n}\right) &= f_b\left(n \cdot \frac{m}{n}\right) = f_b(m) = m \cdot f_b(1) = m(b \cdot 1)\\ &= mb = m \cdot f(1) = f(m) = f\left(n \cdot \frac{m}{n}\right)\\ &= n \cdot f\left(\frac{m}{n}\right).\end{aligned}$$

K は体なので, 両辺を n で割ることにより, $f_b(m/n) = f(m/n)$ が得られる. さらに, K は R の商体だから, K のすべての元は m/n の形で表せる. ゆえに, $f_b = f$ となる. よって, $\psi \circ \varphi(f) = f$. したがって, ψ は φ の逆写像であり, φ は全単射である.

以上より, φ が R 同型であることが示された. □

［例 10］ $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q})\cong\mathbb{Q}$.

［定理 11］ K を整域, R をその部分整域, $\mathfrak{a}$ を R の 0 でないイデアルとするとき, $\mathrm{Hom}_R(R/\mathfrak{a},K)=0$ が成り立つ.

［証明］ $\mathfrak{a}\neq 0$ なので, $a\in\mathfrak{a}$, $a\neq 0$ が存在する.

$f\in\mathrm{Hom}_R(R/\mathfrak{a},K)$ とすると, 任意の $x\in R$ に対して,

$$a\cdot f(x+\mathfrak{a})=f(ax+\mathfrak{a})=f(0+\mathfrak{a})=0.$$

K は整域であり, $a\neq 0$ だから, $f(x+\mathfrak{a})=0$ でなければならない. したがって, $f=0$. □

［例 12］ m を 2 以上の整数とするとき, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\mathbb{Z})=\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\mathbb{Q})=0$.

m, n を 2 以上の整数とするとき, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},n\mathbb{Z})=0$. 実際, もし仮に $\mathbb{Z}/m\mathbb{Z}$ から $n\mathbb{Z}$ への $\mathbb{Z}$ 準同型 f で $f\neq 0$ なるものが存在すれば, 写像 $[n^{-1}]:n\mathbb{Z}\to\mathbb{Z}$, $nx\mapsto x$ は $\mathbb{Z}$ 加群の同型なので, $[n^{-1}]\circ f$ は $\mathbb{Z}/m\mathbb{Z}$ から $\mathbb{Z}$ への 0 でない準同型写像になる. これは $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\mathbb{Z})=0$ に矛盾する.

［定理 13］ m, n を 2 以上の整数, $d=\gcd(m,n)$ とする. このとき, $\mathbb{Z}$ 加群として

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\mathbb{Z}/n\mathbb{Z})\cong\mathbb{Z}/d\mathbb{Z}.$$

［証明］ $m=dm'$, $n=dn'$ とおく. また, $H=\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\,\mathbb{Z}/n\mathbb{Z})$ とおく.

$a\in\mathbb{Z}$ に対して, 写像 $f_a:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ を, 各 $x\in\mathbb{Z}$ に対して,

$$f_a(x+m\mathbb{Z})=n'ax+n\mathbb{Z}$$

とおくことによって定める. f_a は well-defined である. 実際, 任意の x, $x'\in\mathbb{Z}$ に対して,

$$\begin{aligned}x\equiv x'\ (\mathrm{mod}\ m)&\Rightarrow x\equiv x'\ (\mathrm{mod}\ d)\\&\Rightarrow n'a(x-x')\equiv 0\ (\mathrm{mod}\ n)\\&\Rightarrow n'ax\equiv n'ax'\ (\mathrm{mod}\ n)\\&\Rightarrow f_a(x+m\mathbb{Z})=f_a(x'+m\mathbb{Z}).\end{aligned}$$

任意の x, y, $r\in\mathbb{Z}$ に対して,

$$\begin{aligned}f_a((x+m\mathbb{Z})+(y+m\mathbb{Z}))&=f_a((x+y)+m\mathbb{Z})=n'a(x+y)+n\mathbb{Z}\\&=(n'ax+n\mathbb{Z})+(n'ay+n\mathbb{Z})\end{aligned}$$

$$
\begin{aligned}
&= f_a(x+m\mathbb{Z}) + f_a(y+m\mathbb{Z}),\\
f_a(r\cdot(x+m\mathbb{Z})) &= f_a(rx+n\mathbb{Z}) = n'a(rx)+n\mathbb{Z}\\
&= r\cdot(n'ax+n\mathbb{Z})\\
&= r\cdot f(x+m\mathbb{Z}).
\end{aligned}
$$

したがって, f_a は $\mathbb{Z}$ 準同型である．すなわち, $f_a \in H$. これより, 写像

$$\varphi : \mathbb{Z} \to H, \quad a \mapsto f_a$$

が定まる.

任意の a, b, x, $r \in \mathbb{Z}$ に対して,

$$
\begin{aligned}
(\varphi(a) \ \ + \varphi(b))(x+m\mathbb{Z}) &= f_a(x+m\mathbb{Z}) + f_b(x+m\mathbb{Z})\\
&= (n'ax+n\mathbb{Z}) + (n'bx+n\mathbb{Z}) = n'(a+b)x+n\mathbb{Z}\\
&= \varphi(a+b)(x+m\mathbb{Z}),\\
(r\cdot\varphi(a))(x+m\mathbb{Z}) &= r\cdot f_a(x+m\mathbb{Z}) = r\cdot(n'ax+n\mathbb{Z})\\
&= r(n'ax)+n\mathbb{Z} = n'(ra)x+n\mathbb{Z}\\
&= \varphi(ra).
\end{aligned}
$$

ゆえに, φ は $\mathbb{Z}$ 準同型である.

$f \in H$ とする．ある $y \in \mathbb{Z}$ によって $f(1+m\mathbb{Z}) = y+n\mathbb{Z}$ と書ける．このとき,

$$
\begin{aligned}
my+n\mathbb{Z} &= m\cdot(y+n\mathbb{Z}) = m\cdot f(1+m\mathbb{Z})\\
&= f(m+m\mathbb{Z}) = f(0+n\mathbb{Z})\\
&= 0+n\mathbb{Z}.
\end{aligned}
$$

さらに,

$$my+n\mathbb{Z} = 0+n\mathbb{Z} \Rightarrow my \equiv 0 \pmod{n} \Rightarrow m'y \equiv 0 \pmod{n'}.$$

よって, ある $a \in \mathbb{Z}$ が存在して, $m'y = n'a$ と書ける．$\gcd(m', n') = 1$ だから, m' は a を割る. $a = m'a'$ とおくと, $y = n'a'$ となる．このとき, 任意の $x \in \mathbb{Z}$ に対して

$$
\begin{aligned}
f(x+m\mathbb{Z}) &= x\cdot f(1+m\mathbb{Z}) = x\cdot(y+n\mathbb{Z})\\
&= xy+n\mathbb{Z} = n'a'x+n\mathbb{Z}\\
&= f_{a'}(x+m\mathbb{Z}).
\end{aligned}
$$

すなわち, $f = f_{a'} = \varphi(a')$. ゆえに, φ は全射である.

さらに,

$$a \in \mathrm{Ker}(\varphi) \Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } f_a(x+m\mathbb{Z}) = 0+n\mathbb{Z}$$

$$\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } n'ax + n\mathbb{Z} = 0 + n\mathbb{Z}$$
$$\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } n'ax \equiv 0 \pmod{n}$$
$$\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } ax \equiv 0 \pmod{d}$$
$$\Leftrightarrow a \in d\mathbb{Z}.$$

ゆえに, $\mathrm{Ker}(\varphi) = d\mathbb{Z}$.

したがって, 準同型定理により, 同型

$$\mathbb{Z}/d\mathbb{Z} \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}), \quad a + d\mathbb{Z} \mapsto f_a$$

が得られる. □

[別証] $m = m'd$, $n = n'd$, $H = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ とする.

$f \in H$ に対して, a_f を $f(1 + m\mathbb{Z}) = a_f + n\mathbb{Z}$, $0 \leq a_f < n$ によって定めると,

$$\begin{aligned} ma_f + n\mathbb{Z} &= m(a_f + n\mathbb{Z}) = mf(1 + m\mathbb{Z}) \\ &= f(m + m\mathbb{Z}) = f(0 + m\mathbb{Z}) \\ &= 0 + n\mathbb{Z}. \end{aligned}$$

さらに, $\gcd(m', n') = 1$ より,

$$n \mid ma_f \Rightarrow n' \mid m'a_f \Rightarrow n' \mid a_f.$$

したがって, $a_f = n'a'_f$ と表せる. このとき, 写像 φ を

$$\varphi : H \to \mathbb{Z}/d\mathbb{Z}, \quad f \mapsto a'_f + d\mathbb{Z}$$

によって定める.

任意の $f, g \in H$ に対して,

$$f = g \Leftrightarrow a_f \equiv a_g \bmod n \Leftrightarrow a'_f \equiv a'_g \bmod d \Leftrightarrow \varphi(f) = \varphi(g).$$

ゆえに, φ は well-defined かつ単射である.

任意の $f, g \in H$, $r \in \mathbb{Z}$ に対して,

$$(f + g)(1) = f(1) + g(1), \quad (rf)(1) = r \cdot f(1)$$

より,

$$\begin{aligned} &\varphi(f + g) = (a'_f + a'_g) + d\mathbb{Z} = \varphi(f) + \varphi(g), \\ &\varphi(rf) = (ra'_f) + d\mathbb{Z} = r\varphi(f). \end{aligned}$$

ゆえに, φ は $\mathbb{Z}$ 加群の準同型である.

任意の $a \in \mathbb{Z}$ に対して, $f(1+m\mathbb{Z}) = n'a + n\mathbb{Z}$ によって $f \in H$ を定めれば, $\varphi(f) = a + d\mathbb{Z}$ が成り立つ. したがって, φ は全射である.

以上より, φ が $\mathbb{Z}$ 加群の同型であることが示された. $\square$

[注意 14] $m = n$ のとき, 上の定理における $\mathbb{Z}$ 加群の同型

$$\mathbb{Z}/d\mathbb{Z} \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\, \mathbb{Z}/m\mathbb{Z}), \quad a + d\mathbb{Z} \mapsto f_a$$

は, 環としての同型になる. ただし, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\, \mathbb{Z}/m\mathbb{Z})$ の乗法は写像の合成によって定める.

実際, 任意の $a,\, b,\, x \in \mathbb{Z}$ に対して,

$$f_{ab}(x + m\mathbb{Z}) = abx + m\mathbb{Z} = f_a(bx + m\mathbb{Z}) = f_a \circ f_b(x + m\mathbb{Z})$$

となり, 積についても準同型であることがわかる.

[定理 15] $m,\, n$ を 2 以上の整数, $d = \gcd(m, n)$ とする. このとき, $\mathbb{Z}$ 加群として

$$\mathrm{Hom}_{\mathbb{Z}}\left(\frac{1}{m}\mathbb{Z}/\mathbb{Z}, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right) \cong \mathbb{Z}/d\mathbb{Z}.$$

[証明] $m = dm'$, $n = dn'$ とおく. また, $H = \mathrm{Hom}_{\mathbb{Z}}\left(\frac{1}{m}\mathbb{Z}/\mathbb{Z},\, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)$ とおく.

$a \in \mathbb{Z}$ に対して, 写像 $f_a : \frac{1}{m}\mathbb{Z}/\mathbb{Z} \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ を, 各 $x \in \mathbb{Z}$ に対して,

$$f_a\left(\frac{x}{m} + \mathbb{Z}\right) = \frac{n'ax}{n} + \mathbb{Z}$$

とおくことによって定める. f_a は well-defined である. 実際, 任意の $x,\, x' \in \mathbb{Z}$ に対して,

$$\begin{aligned}
x \equiv x' \pmod{m} &\Rightarrow x \equiv x' \pmod{d} \\
&\Rightarrow n'a(x - x') \equiv 0 \pmod{n} \\
&\Rightarrow \frac{n'ax}{n} - \frac{n'ax'}{n} = \frac{n'a(x - x')}{n} \in \mathbb{Z} \\
&\Rightarrow \frac{n'ax}{n} + \mathbb{Z} = \frac{n'ax'}{n} + \mathbb{Z} \\
&\Rightarrow f_a\left(\frac{x}{m} + \mathbb{Z}\right) = f_a\left(\frac{x'}{m} + \mathbb{Z}\right).
\end{aligned}$$

任意の $x,\, y,\, r \in \mathbb{Z}$ に対して,

$$\begin{aligned}
f_a\left(\left(\frac{x}{m} + \mathbb{Z}\right) + \left(\frac{y}{m} + \mathbb{Z}\right)\right) &= f_a\left(\frac{x+y}{m} + \mathbb{Z}\right) = \frac{n'a(x+y)}{n} + \mathbb{Z} \\
&= \left(\frac{n'ax}{n} + \mathbb{Z}\right) + \left(\frac{n'ay}{n} + \mathbb{Z}\right)
\end{aligned}$$

$$
\begin{aligned}
&= f_a\left(\frac{x}{m}+\mathbb{Z}\right)+f_a\left(\frac{y}{m}+\mathbb{Z}\right),\\
f_a\left(r\cdot\left(\frac{x}{m}+\mathbb{Z}\right)\right) &= f_a\left(\frac{rx}{m}+\mathbb{Z}\right)=\frac{n'a(rx)}{n}+\mathbb{Z}\\
&= r\cdot\left(\frac{n'ax}{n}+\mathbb{Z}\right)\\
&= r\cdot f\left(\frac{x}{m}+\mathbb{Z}\right).
\end{aligned}
$$

したがって, f_a は $\mathbb{Z}$ 準同型である. すなわち, $f_a\in H$. これより, 写像

$$
\varphi:\mathbb{Z}\to H,\quad a\mapsto f_a
$$

が定まる.

任意の $a, b, x, r\in\mathbb{Z}$ に対して,

$$
\begin{aligned}
(\varphi(a)\ +\varphi(b))\left(\frac{x}{m}+\mathbb{Z}\right) &= f_a\left(\frac{x}{m}+\mathbb{Z}\right)+f_b\left(\frac{x}{m}+\mathbb{Z}\right)\\
&= \left(\frac{n'ax}{n}+\mathbb{Z}\right)+\left(\frac{n'bx}{n}+\mathbb{Z}\right)=\frac{n'(a+b)x}{n}+\mathbb{Z}\\
&= \varphi(a+b)\left(\frac{x}{m}+\mathbb{Z}\right),\\
(r\cdot\varphi(a))\left(\frac{x}{m}+\mathbb{Z}\right) &= r\cdot f_a\left(\frac{x}{m}+\mathbb{Z}\right)=r\cdot\left(\frac{n'ax}{n}+\mathbb{Z}\right)\\
&= \frac{r(n'ax)}{n}+\mathbb{Z}=\frac{n'(ra)x}{n}+\mathbb{Z}\\
&= \varphi(ra).
\end{aligned}
$$

ゆえに, φ は $\mathbb{Z}$ 準同型である.

$f\in H$ とする. ある $y\in\mathbb{Z}$ によって $f\left(\frac{x}{m}+\mathbb{Z}\right)=y+n\mathbb{Z}$ と書ける. このとき,

$$
\begin{aligned}
\frac{my}{n}+\mathbb{Z} &= m\cdot\left(\frac{y}{n}+\mathbb{Z}\right)=m\cdot f\left(\frac{1}{m}+\mathbb{Z}\right)\\
&= f\left(\frac{m}{m}+\mathbb{Z}\right)=f(0+\mathbb{Z})\\
&= 0+\mathbb{Z}.
\end{aligned}
$$

さらに,

$$
\frac{my}{n}+\mathbb{Z}=0+\mathbb{Z}\Rightarrow my\equiv 0 \pmod{n}\Rightarrow m'y\equiv 0 \pmod{n'}.
$$

よって, ある $a\in\mathbb{Z}$ が存在して, $m'y=n'a$ と書ける. $\gcd(m',n')=1$ だから, m' は a を割る. $a=m'a'$ とおくと, $y=n'a'$ となる. このとき, 任意の $x\in\mathbb{Z}$ に対して

$$
\begin{aligned}
f\left(\frac{x}{m}+\mathbb{Z}\right) &= x\cdot f\left(\frac{1}{m}+\mathbb{Z}\right)=x\cdot\left(\frac{y}{n}+\mathbb{Z}\right)\\
&= \frac{xy}{n}+\mathbb{Z}=\frac{n'a'x}{n}\mathbb{Z}\\
&= f_{a'}\left(\frac{x}{m}+\mathbb{Z}\right).
\end{aligned}
$$

すなわち, $f = f_{a'} = \varphi(a')$. ゆえに, φ は全射である.

さらに,

$$\begin{aligned}
a \in \mathrm{Ker}(\varphi) &\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } f_a\left(\frac{x}{m} + \mathbb{Z}\right) = 0 + n\mathbb{Z} \\
&\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } \frac{n'ax}{n} + \mathbb{Z} = 0 + n\mathbb{Z} \\
&\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } \frac{ax}{d} = \frac{n'ax}{n} \in \mathbb{Z} \\
&\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } ax \in d\mathbb{Z} \\
&\Leftrightarrow a \in d\mathbb{Z}.
\end{aligned}$$

ゆえに, $\mathrm{Ker}(\varphi) = d\mathbb{Z}$.

したがって, 準同型定理により, 同型

$$\mathbb{Z}/d\mathbb{Z} \cong \mathrm{Hom}_{\mathbb{Z}}\left(\frac{1}{m}\mathbb{Z}/\mathbb{Z},\, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right), \quad a + d\mathbb{Z} \mapsto f_a$$

が得られる. □

[別証] $\dfrac{1}{m}\mathbb{Z}/\mathbb{Z} = \left\{ \dfrac{x}{m} + \mathbb{Z} \;\middle|\; x \in \mathbb{Z} \right\}$ より, 写像

$$\varphi_m : \mathbb{Z} \to \frac{1}{m}\mathbb{Z}/\mathbb{Z}, \quad x \mapsto \frac{x}{m} + \mathbb{Z}$$

は全射である. φ_m が $\mathbb{Z}$ 加群の準同型であることはすぐに確かめられる. さらに,

$$x \in \mathrm{Ker}(\varphi_m) \Leftrightarrow \frac{x}{m} \in \mathbb{Z} \Leftrightarrow x \in m\mathbb{Z}.$$

よって, 準同型定理により, $\mathbb{Z}$ 加群の同型

$$\widetilde{\varphi_m} : \mathbb{Z}/m\mathbb{Z} \to \frac{1}{m}\mathbb{Z}/\mathbb{Z}, \quad x + m\mathbb{Z} \mapsto \frac{x}{m} + \mathbb{Z}$$

が得られる. 同様に, n に対しても, $\mathbb{Z}$ 加群の同型

$$\widetilde{\varphi_n} : \mathbb{Z}/n\mathbb{Z} \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}, \quad x + n\mathbb{Z} \mapsto \frac{x}{n} + \mathbb{Z}$$

が得られる. このとき,

$$\mathrm{Hom}_{\mathbb{Z}}\left(\frac{1}{m}\mathbb{Z}/\mathbb{Z},\, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right) \to \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/m\mathbb{Z},\, \mathbb{Z}/n\mathbb{Z}\right), \quad f \mapsto \widetilde{\varphi_n}^{-1} \circ f \circ \widetilde{\varphi_m}$$

は $\mathbb{Z}$ 加群の同型である. したがって,

$$\mathrm{Hom}_{\mathbb{Z}}\left(\frac{1}{m}\mathbb{Z}/\mathbb{Z},\, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right) \cong \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/m\mathbb{Z},\, \mathbb{Z}/n\mathbb{Z}\right) \cong \mathbb{Z}/d\mathbb{Z}.$$

□

[注意 16] $m = n$ のとき, 上の定理における $\mathbb{Z}$ 加群の同型

$$\mathbb{Z}/d\mathbb{Z} \cong \mathrm{Hom}_{\mathbb{Z}}\left(\frac{1}{m}\mathbb{Z}/\mathbb{Z},\, \frac{1}{m}\mathbb{Z}/\mathbb{Z}\right), \quad a + d\mathbb{Z} \mapsto f_a$$

は, 環としての同型になる. ただし, $\mathrm{Hom}_{\mathbb{Z}}\left(\frac{1}{m}\mathbb{Z}/\mathbb{Z},\, \frac{1}{m}\mathbb{Z}/\mathbb{Z}\right)$ の乗法は写像の合成によって定める.

実際, 任意の $a,\, b,\, x \in \mathbb{Z}$ に対して,

$$f_{ab}\left(\frac{x}{m} + \mathbb{Z}\right) = \frac{abx}{m} + \mathbb{Z} = f_a\left(\frac{bx}{m} + \mathbb{Z}\right) = f_a \circ f_b\left(\frac{x}{m} + \mathbb{Z}\right)$$

となり, 積についても準同型であることがわかる.

[定理 17] m を 2 以上の整数とする. このとき, $\mathbb{Z}$ 加群として

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\, \mathbb{C}^{\times}) \cong \mathbb{Z}/m\mathbb{Z}.$$

[証明] ζ を 1 の原始 m 乗根とする. $a \in \mathbb{Z}$ に対して, 写像 $f_a : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}^{\times}$ を, 各 $x \in \mathbb{Z}$ に対して,

$$f_a(x + m\mathbb{Z}) = \zeta^{ax}$$

とおくことによって定める. f_a は well-defined である. 実際, $\zeta^m = 1$ より, 任意の $x,\, x' \in \mathbb{Z}$ に対して,

$$x \equiv x' \pmod{m} \Rightarrow f_a(x + m\mathbb{Z}) = \zeta^{ax} = \zeta^{ax'} = f_a(x' + m\mathbb{Z}).$$

任意の $x,\, y,\, r \in \mathbb{Z}$ に対して,

$$\begin{aligned} f_a((x + m\mathbb{Z}) + (y + m\mathbb{Z})) &= f_a((x+y) + m\mathbb{Z}) = \zeta^{a(x+y)} = \zeta^{ax} \cdot \zeta^{ay} \\ &= f_a(x + m\mathbb{Z}) \cdot f_a(y + m\mathbb{Z}), \\ f_a(r \cdot (x + m\mathbb{Z})) &= f_a(rx + n\mathbb{Z}) = \zeta^{a(rx)} = (\zeta^{ax})^r \\ &= f(x + m\mathbb{Z})^r. \end{aligned}$$

したがって, f_a は $\mathbb{Z}$ 準同型であり, 写像

$$\varphi : \mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\, \mathbb{C}^{\times}), \quad a \mapsto f_a$$

が定まる.

任意の $a,\, b,\, x,\, r \in \mathbb{Z}$ に対して,

$$\begin{aligned} (\varphi(a) \cdot \varphi(b))(x + m\mathbb{Z}) &= f_a(x + m\mathbb{Z}) \cdot f_b(x + m\mathbb{Z}) = \zeta^{ax} \cdot \zeta^{bx} = \zeta^{(a+b)x} \\ &= \varphi(a+b)(x + m\mathbb{Z}), \\ \varphi(a)^r(x + m\mathbb{Z}) &= f_a(x + m\mathbb{Z})^r = (\zeta^{ax})^r = \zeta^{rax} \end{aligned}$$

$$= \varphi(ra).$$

ゆえに, φ は $\mathbb{Z}$ 準同型である.

$f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{C}^{\times})$ とすると,

$$f(1+m\mathbb{Z})^m = f(m+m\mathbb{Z}) = f(0+m\mathbb{Z}) = 1.$$

よって, $f(1+m\mathbb{Z})$ は 1 の m 乗根であるから, ある整数 $a \in \mathbb{Z}$ が存在して, $f(1+m\mathbb{Z}) = \zeta^a$ と書ける. さらに, 任意の $x \in \mathbb{Z}$ に対して,

$$f(x+m\mathbb{Z}) = f(1+m\mathbb{Z})^x = \zeta^{ax} = f_a(x+m\mathbb{Z}).$$

すなわち, $f = f_a = \varphi(a)$. ゆえに, φ は全射である.

さらに,

$$\begin{aligned} a \in \mathrm{Ker}(\varphi) &\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } f_a(x+m\mathbb{Z}) = 1 \\ &\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } \zeta^{ax} = 1 \\ &\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } ax \in m\mathbb{Z} \\ &\Leftrightarrow a \in m\mathbb{Z}. \end{aligned}$$

ゆえに, $\mathrm{Ker}(\varphi) = m\mathbb{Z}$.

したがって, 準同型定理により, 同型

$$\mathbb{Z}/m\mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{C}^{\times}), \quad a+m\mathbb{Z} \mapsto f_a$$

が得られる. □

[定理 18] m を 2 以上の整数とする. このとき, $\mathbb{Z}$ 加群として

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

[証明] $a \in \mathbb{Z}$ に対して, 写像 $f_a : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ を, 各 $x \in \mathbb{Z}$ に対して,

$$f_a(x+m\mathbb{Z}) = \frac{ax}{m} + \mathbb{Z}$$

とおくことによって定める. f_a は well-defined である. 実際, 任意の $x, x' \in \mathbb{Z}$ に対して,

$$\begin{aligned} x \equiv x' \pmod{m} &\Rightarrow \left(\frac{ax}{m} + \mathbb{Z}\right) - \left(\frac{ax'}{m} + \mathbb{Z}\right) = \frac{a(x-x')}{m} + \mathbb{Z} = 0 + \mathbb{Z} \\ &\Rightarrow f_a(x+m\mathbb{Z}) = f_a(x'+m\mathbb{Z}). \end{aligned}$$

任意の $x, y \in \mathbb{Z}$ に対して,

$$f_a((x+m\mathbb{Z}) + (y+m\mathbb{Z})) = f_a((x+y)+m\mathbb{Z}) = \frac{a(x+y)}{m} + \mathbb{Z}$$

$$
\begin{aligned}
&= \left(\frac{ax}{m} + \mathbb{Z}\right) + \left(\frac{ay}{m} + \mathbb{Z}\right) \\
&= f_a(x + m\mathbb{Z}) + f_a(y + m\mathbb{Z}), \\
f_a(r \cdot (x + m\mathbb{Z})) &= f_a(rx + n\mathbb{Z}) = \frac{a(rx)}{m} + n\mathbb{Z} = r \cdot \left(\frac{ax}{m} + n\mathbb{Z}\right) \\
&= r \cdot f(x + m\mathbb{Z}).
\end{aligned}
$$

したがって, f_a は $\mathbb{Z}$ 準同型であり, 写像

$$
\varphi : \mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}), \quad a \mapsto f_a
$$

が定まる.

任意の $a, b, x, r \in \mathbb{Z}$ に対して,

$$
\begin{aligned}
(\varphi(a)\ + \varphi(b))(x + m\mathbb{Z}) &= f_a(x + m\mathbb{Z})\ + f_b(x + m\mathbb{Z}) \\
&= \left(\frac{ax}{m} + \mathbb{Z}\right) + \left(\frac{bx}{m} + \mathbb{Z}\right) = \frac{(a+b)x}{m} + \mathbb{Z} \\
&= \varphi(a + b)(x + m\mathbb{Z}), \\
(r \cdot \varphi(a))(x + m\mathbb{Z}) &= r \cdot f_a(x + m\mathbb{Z}) = \frac{rax}{m} + \mathbb{Z} \\
&= \varphi(ra).
\end{aligned}
$$

ゆえに, φ は $\mathbb{Z}$ 準同型である.

$f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ とする. ある $y \in \mathbb{Q}$ によって $f(1 + m\mathbb{Z}) = y + \mathbb{Z}$ と書ける. このとき,

$$
\begin{aligned}
my + \mathbb{Z} &= m \cdot (y + \mathbb{Z}) = m \cdot f(1 + m\mathbb{Z}) \\
&= f(m + m\mathbb{Z}) = f(0 + m\mathbb{Z}) \\
&= 0 + \mathbb{Z}.
\end{aligned}
$$

ゆえに, $my \in \mathbb{Z}$. そこで, $a = my$ とおくと, 任意の $x \in \mathbb{Z}$ に対して

$$
\begin{aligned}
f(x + m\mathbb{Z}) &= x \cdot f(1 + m\mathbb{Z}) = x \cdot (y + \mathbb{Z}) \\
&= xy + \mathbb{Z} = \frac{ax}{m} + \mathbb{Z} \\
&= f_a(x + m\mathbb{Z}).
\end{aligned}
$$

すなわち, $f = f_a = \varphi(a)$. よって, φ は全射である.

さらに,

$$
\begin{aligned}
a \in \mathrm{Ker}(\varphi) &\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } f_a(x + m\mathbb{Z}) = 0 + \mathbb{Z} \\
&\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } \frac{ax}{m} + \mathbb{Z} = 0 + \mathbb{Z} \\
&\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して, } \frac{ax}{m} \in \mathbb{Z}
\end{aligned}
$$

$$\Leftrightarrow \text{任意の } x \in \mathbb{Z} \text{ に対して}, ax \in m\mathbb{Z}$$
$$\Leftrightarrow a \in m\mathbb{Z}.$$

ゆえに, $\mathrm{Ker}(\varphi) = m\mathbb{Z}$.

　したがって, 準同型定理により, 同型

$$\mathbb{Z}/m\mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}), \quad a + m\mathbb{Z} \mapsto f_a$$

が得られる. □

[定理 19] p を素数, $\mathbb{Z}_p$ を p 進整数環とする. このとき, 環として

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}, \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}\right) \cong \mathbb{Z}_p.$$

ただし,

$$\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{x}{p^n} \,\middle|\, x \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\right\}, \quad \mathbb{Z}_{\geq 0} = \{n \in \mathbb{Z} \mid n \geq 0\}$$

とする.

[証明] $M = \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$, $H = \mathrm{Hom}_{\mathbb{Z}}(M, M)$ とおく.

　各 $\alpha = (\alpha_n \mid n \in \mathbb{Z}_{\geq 0}) \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ と各 $x \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$ に対して,

$$\alpha \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right) = \frac{a_k x}{p^n} + \mathbb{Z}, \quad h = \begin{cases} 0, & x \in p^n\mathbb{Z}, \\ n - \mathrm{ord}_p(x), & x \notin p^n\mathbb{Z}, \end{cases}$$
$$\alpha_h = a_h + p^h\mathbb{Z} \in \mathbb{Z}/p^n\mathbb{Z}, \quad a_h \in \mathbb{Z}$$

によってスカラー倍を定めることにより, M は $\mathbb{Z}_p$ 加群になる.

　実際, まず, 任意の $x, x' \in \mathbb{Z}$, $n, n' \in \mathbb{Z}_{\geq 0}$ に対して,

$$\frac{x}{p^n} - \frac{x'}{p^{n'}} \in \mathbb{Z} \Rightarrow \mathrm{ord}_p\left(\frac{x}{p^n}\right) - \mathrm{ord}_p\left(\frac{x'}{p^{n'}}\right) = 0$$
$$\Rightarrow (\mathrm{ord}_p(x) - n) - (\mathrm{ord}_p(x') - n') = 0$$

であるから, h の値は M に属する類の代表元の取り方によらない. したがって, スカラー倍は well-defined である.

　次に, $\alpha \in \mathbb{Z}_p$ に対して,

$$\alpha = \sum_{i=0}^{\infty} a'_i p^i, \quad a'_i \in \{0, 1, \ldots, p-1\}$$

を p 進展開とするとき,

$$a_n \equiv \sum_{i=0}^{n} a'_i p^i \pmod{p^n}$$

だから, 任意の $k \in \mathbb{Z}_{\geq 0}$ に対して,

$$k \geq h \Rightarrow \frac{(a_k - a_h)x}{p^n} \in \mathbb{Z} \Rightarrow \frac{a_k x}{p^n} + \mathbb{Z} = \frac{a_h x}{p^n} + \mathbb{Z}$$

となることに注意せよ. すると, 任意の $\alpha, \beta \in \mathbb{Z}_p$, 任意の $x, y \in \mathbb{Z}$, $n, m \in \mathbb{Z}_{\geq 0}$ に対して,

$$\alpha = (a_n + p^n\mathbb{Z} \mid n \in \mathbb{Z}_{\geq 0}), \quad \beta = (b_n + p^n\mathbb{Z} \mid n \in \mathbb{Z}_{\geq 0})$$

とおくと,

$$\alpha + \beta = ((a_n + b_n) + p^n\mathbb{Z} \mid n \in \mathbb{Z}_{\geq 0}), \quad \alpha\beta = (a_n b_n + p^n\mathbb{Z} \mid n \in \mathbb{Z}_{\geq 0})$$

であり, 十分大きい $k \in \mathbb{Z}_{\geq 0}$ をとれば,

$$\begin{aligned}
(\alpha\beta) \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right) &= \frac{(a_k b_k)x}{p^n} + \mathbb{Z} = \alpha \cdot \left(\frac{b_k x}{p^n} + \mathbb{Z}\right) \\
&= \alpha \cdot \left(\beta \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right)\right), \\
(\alpha + \beta) \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right) &= \frac{(a_k + b_k)x}{p^n} + \mathbb{Z} \\
&= \left(\frac{a_k x}{p^n} + \mathbb{Z}\right) + \left(\frac{b_k x}{p^n} + \mathbb{Z}\right) \\
&= \alpha \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right) + \beta \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right),
\end{aligned}$$

さらに, $m \leq n$ のとき,

$$\begin{aligned}
\alpha \cdot \left(\left(\frac{x}{p^n} + \mathbb{Z}\right) + \left(\frac{y}{p^m} + \mathbb{Z}\right)\right) &= \alpha \cdot \left(\frac{x + p^{n-m}y}{p^n} + \mathbb{Z}\right) \\
&= \frac{a_k(x + p^{n-m}y)}{p^n} + \mathbb{Z} \\
&= \left(\frac{a_k x}{p^n} + \mathbb{Z}\right) + \left(\frac{a_k p^{n-m} y}{p^n} + \mathbb{Z}\right) \\
&= \alpha \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right) + \alpha \cdot \left(\frac{y}{p^m} + \mathbb{Z}\right).
\end{aligned}$$

$m > n$ のときも同様である. $1_{\mathbb{Z}_p}$, $1_{\mathbb{Z}}$ をそれぞれ $\mathbb{Z}_p$, $\mathbb{Z}$ の単位元とすると,

$$1_{\mathbb{Z}_p} \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right) = \frac{1_{\mathbb{Z}} \cdot x}{p^n} + \mathbb{Z} = \frac{x}{p^n} + \mathbb{Z}.$$

以上より, M は $\mathbb{Z}_p$ 加群をなす.

各 $\alpha \in \mathbb{Z}$ に対して, 写像 $f_\alpha : M \to M$ を, 各 $x \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$ に対して,

$$f_\alpha \left(\frac{x}{p^n} + \mathbb{Z}\right) = \alpha \cdot \left(\frac{x}{p^n} + \mathbb{Z}\right)$$

とおくことによって定める. 任意の $\alpha \in \mathbb{Z}_p$, $x, y \in \mathbb{Z}$, $n, m \in \mathbb{Z}_{\geq 0}$ に対して, スカラー倍の性質により,

$$f_\alpha \left(\left(\frac{x}{p^n} + \mathbb{Z}\right) + \left(\frac{y}{p^m} + \mathbb{Z}\right)\right) = \alpha \cdot \left(\left(\frac{x}{p^n} + \mathbb{Z}\right) + \left(\frac{y}{p^m} + \mathbb{Z}\right)\right)$$

$$
\begin{aligned}
&= \alpha \cdot \left(\frac{x}{p^n} + \mathbb{Z} \right) + \alpha \cdot \left(\frac{y}{p^m} + \mathbb{Z} \right) \\
&= f_\alpha \left(\frac{x}{p^n} + \mathbb{Z} \right) + f_\alpha \left(\frac{y}{p^m} + \mathbb{Z} \right).
\end{aligned}
$$

よって, f_α は $\mathbb{Z}$ 加群としての準同型であり, 写像

$$\varphi : \mathbb{Z}_p \to H, \quad \alpha \mapsto f_\alpha$$

が定まる.

H の積が写像の合成によって定まっているとき, φ は環準同型になる. 実際, 任意の $\alpha, \beta \in \mathbb{Z}_p$ に対して, スカラー倍の性質により,

$$
\begin{aligned}
f_{\alpha+\beta} \left(\frac{x}{p^n} + \mathbb{Z} \right) &= (\alpha + \beta) \cdot \left(\frac{x}{p^n} + \mathbb{Z} \right) = \alpha \cdot \left(\frac{x}{p^n} + \mathbb{Z} \right) + \beta \cdot \left(\frac{x}{p^n} + \mathbb{Z} \right) \\
&= f_\alpha \left(\frac{x}{p^n} + \mathbb{Z} \right) + f_\beta \left(\frac{x}{p^n} + \mathbb{Z} \right), \\
f_{\alpha\beta} \left(\frac{x}{p^n} + \mathbb{Z} \right) &= (\alpha\beta) \cdot \left(\frac{x}{p^n} + \mathbb{Z} \right) = \alpha \cdot \left(\beta \cdot \left(\frac{x}{p^n} + \mathbb{Z} \right) \right) \\
&= f_\alpha \circ f_\beta \left(\frac{x}{p^n} + \mathbb{Z} \right).
\end{aligned}
$$

$f \in H$ とする. 各 $n \in \mathbb{Z}_{\geq 0}$ に対して, $M_n = \dfrac{1}{p^n}\mathbb{Z}$ とおくと, M_n は M の部分 $\mathbb{Z}$ 加群なので, f の M_n への制限 $f_n : M_n \to M$ は $\mathbb{Z}$ 準同型である. 一方, M における p^n 倍写像 $[p^n]$ を考えると,

$$[p^n] \circ f_n(M_n) = f_n(p^n M_n) = f_n(\mathbb{Z}) = \mathbb{Z}$$

であるから,

$$f_n(M_n) \subseteq \mathrm{Ker}([p^n] : M \to M) = M_n.$$

ゆえに, f_n は M_n の自己準同型であり, ある $a_n \in \mathbb{Z}$ が存在して, f_n は M_n における a_n 倍写像である. $\alpha = (a_n + p^n\mathbb{Z} \mid n \in \mathbb{Z}_{\geq 0})$ とおくと, $\alpha \in \mathbb{Z}_p$. さらに, f_α の M_n への制限は f_n に一致する. $M = \displaystyle\bigcup_{n \in \mathbb{Z}_{\geq 0}} M_n$ だから, $f_\alpha = f$ となる. よって, φ は全射である.

$\alpha = (a_n + p^n\mathbb{Z} \mid n \in \mathbb{Z}_{\geq 0}) \in \mathrm{Ker}(\varphi)$ とすると, $\varphi(\alpha) = f_\alpha$ は零写像なので, 任意の $n \in \mathbb{Z}_{\geq 0}$ に対して,

$$\frac{a_n}{p^n} + \mathbb{Z} = \alpha \cdot \left(\frac{1}{p^n} + \mathbb{Z} \right) = f_\alpha \left(\frac{1}{p^n} + \mathbb{Z} \right) = 0 + \mathbb{Z}.$$

よって, $a_n \equiv 0 \pmod{p^n}$. ゆえに, $\alpha = 0$. したがって, φ は単射である.

以上より, φ が環の同型であることが示された. □