巡回群

MATHEMATICS.PDF

2010-06-28

目 次

1 元の位数 **3**

2 巡回群 **8**

3 巡回群の自己同型 **19**

4 $\mathbb{Z}$ について **25**

参考文献

[1] 彌永昌吉, 有馬哲, 浅枝陽: 詳解代数入門, 1990

[2] 桂利行: 代数学 I 群と環, 東京大学出版会, 2004

[3] 藤崎源二郎: 体とガロア理論, 岩波書店, 1991

[4] 松坂和夫: 代数系入門, 岩波書店. 1976

1　元の位数

群 G の元 a について，$a^n = 1$ となる最小の正の整数 n を a の**位数**あるいは**周期**という. また, そのような n が存在するとき, a は**有限位数**であるという. a が有限位数でないとき, a は**無限位数**であるという.

G の元 a について, 明らかに, a の位数が 1 であることと a が G の単位元であることとは同値である.

a が G の有限位数の元であるとき, 2 つの正の整数 n, n' がともに a の位数であれば, $a^n = 1$ かつ $a^{n'} = 1$ であり, 位数の最小性より $n \leq n'$ かつ $n' \leq n$. ゆえに $n = n'$. したがって, a に対して位数は一意的に定まる.

[定理 1.1] G を群, a を G の元とする. a が有限位数であるための必要十分条件は, ある 0 でない整数 n が存在して $a^n = 1$ となることである.

[証明] a が有限位数のとき $a^n = 1$ となる整数 $n \neq 0$ が存在することは有限位数の定義から明らかである.

ある 0 でない整数 n が存在して $a^n = 1$ が成り立つとすると, $a^{-n} = 1$ でもあるから, $n > 0$ としてもよい. このとき, 正の整数からなる集合

$$S = \{k \in \mathbb{Z} \mid k > 0 \text{ かつ } a^k = 1\}$$

は空でないから, 最小元 m が存在する. この m はまさに a の位数である. □

[定理 1.2] G を群, a を G の位数 n の元とする. このとき，整数 m について,

$$a^m = 1 \Leftrightarrow n \mid m$$

が成り立つ.

[証明] ($\Leftarrow$)　$n \mid m$ のとき, ある $q \in \mathbb{Z}$ が存在して $m = nq$. ゆえに $a^m = a^{nq} = 1$.
($\Rightarrow$)　$a^m = 1$ とする. m を n で割ると, ある q, $r \in \mathbb{Z}$ が存在して,

$$m = nq + r, \quad 0 \leq r < n.$$

このとき,

$$a^m = a^{nq+r} = a^{nq}a^r = a^r.$$

ゆえに $a^r = 1$. 位数の定義から，n は $a^n = 1$ となる最小の正の整数だから $r = 0$ でなければならない. ゆえに $n \mid m$. □

[系 1.3] m, n を正の整数とする. a_1, a_2, ..., a_m を群 G の元とし, 積 $a_1a_2\cdots a_m$ の位数は n であるとする. このとき, $i = 2, 3, \ldots, m$ に対して

$$a_ia_{i+1}\cdots a_na_1a_2\cdots a_{i-1}$$

の位数も n である.

とくに, G の任意の元 a, b に対して, ab の位数が n ならば ba の位数も n である.

[証明] $(a_1a_2\cdots a_m)^n = 1$ より,

$$\begin{aligned} &a_1a_2\cdots a_{i-1}(a_ia_{i+1}\cdots a_na_1a_2\cdots a_{i-1})^n \\ &\quad = (a_1a_2\cdots a_m)^n a_1a_2\cdots a_{i-1} = a_1a_2\cdots a_{i-1} \end{aligned}$$

となる[1)]. したがって $a_ia_{i+1}\cdots a_na_1a_2\cdots a_{i-1}$ は有限位数である (定理 1.1). その位数を l とすると, $l \mid n$ である (定理 1.2). 逆に,

$$\begin{aligned} &(a_1a_2\cdots a_m)^l a_1a_2\cdots a_{i-1} \\ &\quad = a_1a_2\cdots a_{i-1}(a_ia_{i+1}\cdots a_na_1a_2\cdots a_{i-1})^l = a_1a_2\cdots a_{i-1}. \end{aligned}$$

ゆえに $(a_1a_2\cdots a_m)^l = 1$. よって $n \mid l$ である (定理 1.1). n, l はともに正の整数なので, $l = n$ が得られる. □

[系 1.4] 群 G のすべての元の位数が 2 以下ならば, G は Abel 群である.

[証明] G の任意の元 a に対して, 仮定より a の位数は 1 または 2 であるから, 定理 1.2 より $a^2 = 1$ が成り立ち, $a^{-1} = a$ となる. したがって, 任意の a, $b \in G$ に対して,

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba.$$

ゆえに G は Abel 群である. □

[定理 1.5] G を群, a を G の位数 n の元とし, k を整数, d を k, n の (正の) 最大公約数とする. このとき, a^k の位数は n/d である.

[1)] 例えば, $m = n = 2$ のときは, $a_1(a_2a_1)(a_2a_1) = (a_1a_2)(a_1a_2)a_1$.

[証明] m を整数とすると,

$$(a^k)^m = 1 \Leftrightarrow a^{km} = 1 \Leftrightarrow n \mid km$$

が成り立つ (定理 1.2).

$$n = dn_1, \quad k = dk_1, \quad \gcd(n_1, k_1) = 1$$

とおけば,

$$n \mid km \Leftrightarrow n_1 \mid k_1 m \Leftrightarrow n_1 \mid m$$

である. 一方,

$$(a^k)^{n_1} = (a^n)^{k_1} = 1.$$

ゆえに n_1 は $(a^k)^{n_1} = 1$ となる最小の正の整数である. すなわち, $n_1 = n/d$ は a^k の位数である. □

[系 1.6] G を群, a を G の位数 n の元とする. k を n と互いに素な整数とするとき, a^k の位数は n である.

[証明] 定理 1.5 における $d = 1$ の場合である. □

[系 1.7] G を群, a を G の位数 n の元とする. このとき, a^{-1} の位数は n である.

[証明] 定理 1.5 における $k = -1$ の場合である. □

[系 1.8] G を群, a を G の位数 n の元とする. このとき, n の任意の正の約数 d に対して, $a^{\frac{n}{d}}$ の位数は d である.

[証明] $k = n/d$ とおく. k は n の正の約数なので, $\gcd(k, n) = k$ である. 定理 1.5 により, a^k の位数は $n/k = d$ である. □

[系 1.9] G を群, a を G の元とする. a の位数は mn であり, m, n は互いに素であるとする. このとき, a に対して位数 m の元 b と位数 n の元 c との組がただ 1 つ存在して, $a = bc = cb$ を満たす.

[証明] 存在することの証明：m, n が互いに素だから，整数 s, t が存在して，

$$ms + nt = 1.$$

ゆえに，

$$a = a^{nt+ms} = a^{nt}a^{ms}.$$

そこで，$b = a^{nt}$, $c = a^{ms}$ とおけば，$a = bc = cb$ となる．

a の位数が mn であるから，a^n の位数は m である (系 1.8)．m, t は互いに素であるから，$b = a^{nt}$ の位数は m である (系 1.6)．同様に，$c = a^{ms}$ の位数は n である．

一意性の証明：$a = b'c' = c'b'$ で，b', c' の位数をそれぞれ m, n とすれば，

$$b = a^{nt} = (b'c')^{nt} = b'^{nt}c'^{nt} = b'^{nt} = b'^{ms}b'^{nt} = b'^{ms+nt} = b'.$$

また，$bc = a = b'c'$ より，$c = c'$．これで b, c の一意性が示された． □

[定理 1.10] G を群，a, b を G の元とし，$ab = ba$ とする．m を a の位数，n を b の位数とする．

(i) ab は有限位数の元であり, その位数は mn の約数である．

(ii) m, n が互いに素であるとき，ab の位数は mn である．

(iii) m, n の最大公約数が ab の位数を割れば, ab の位数は m, n の最小公倍数に一致する．

[証明] (i)　$ab = ba$ と仮定したので，

$$(ab)^{mn} = (a^m)^n(b^n)^m = 1.$$

ab は有限位数である (定理 1.1)．また, ab の位数は mn の約数である (定理 1.2)．

(ii)　ab の位数を r とすると, $ab = ba$ より

$$a^r b^r = (ab)^r = 1.$$

よって $a^r = b^{-r}$．これより

$$a^{rn} = (b^n)^{-r} = 1.$$

a の位数は m であるから，rn は m で割り切れる (定理 1.2). ところが m, n は互いに素だから，m は r を割る. 同様に，n も r を割ることがいえる. m, n は互いに素だから，それらの最小公倍数 mn も r の約数である.

$r \mid mn$ かつ $mn \mid r$ であり, r も mn も正なので, $mn = r$ となる.

(iii)　d を m, n の最大公約数, l を m, n の最小公倍数とする. $m = m_1 d$, $n = n_1 d$ とおくと, $\gcd(m_1, n_1) = 1$ かつ $l = m_1 n_1 d$ が成り立つ.

a^d, b^d の位数はそれぞれ m_1, n_1 である (系 1.8). $ab = ba$ より $(ab)^d = a^d b^d$ なので, (ii) より $(ab)^d$ の位数は $m_1 n_1$ である. 一方, ab の位数を r とすると, $d \mid r$ という仮定と系 1.8 より, $(ab)^d$ の位数は r/d である. ゆえに $r/d = m_1 n_1$. したがって $r = m_1 n_1 d = l$. □

[系 1.11] G を群, $a_1, a_2, \ldots, a_r$ をどの 2 つも互いに可換な G の元とし, $1 \leq i \leq r$ について，a_i の位数を n_i とする. また，$n_1, n_2, \ldots, n_r$ はどの 2 つも互いに素であるとする. このとき，積 $a = a_1 \cdots a_n$ の位数は $n = n_1 \cdots n_r$ である.

[証明] 数学的帰納法により証明する. $r = 2$ のときは定理 1.10 によりすでに示されている.

一般に，$r = k$ のとき，上記の命題が正しいと仮定する. $r = k + 1$ のときを考えると，帰納法の仮定より，$a' = a_1 \cdots a_k$ の位数は $n' = n_1 \cdots n_k$ である. a' と a_{k+1} とは可換であり，n' と n_{k+1} とは互いに素である. よって $r = 2$ の場合から，$a = a' a_{k+1}$ の位数は $n = n' n_{r+1}$ であることがいえる. □

[系 1.12] G を群, $a_1, a_2, \ldots, a_r$ をどの 2 つも互いに可換な G の元とし, $1 \leq i \leq r$ について，a_i の位数を n_i とする. また，n を $n_1, n_2, \ldots, n_r$ の最小公倍数とする. このとき，位数が n であるような G の元 a が存在する.

[証明] $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ を素因数分解とする. $1 \leq j \leq k$ であるような任意の j に対して，ある n_i が存在して $p_j^{s_j} \mid n_i$ となる. そこで，$d_j = n_i / p_j^{s_j}$, $b_j = a_i^{d_j}$ とおけば，b_j の位数は $p_j^{s_j}$ である (系 1.8). したがって，各 j に対して，位数が $p_j^{s_j}$ であるような b_j が存在する. $b_1, b_2, \ldots, b_k$ はどの 2 つも可換だから，$a = b_1 b_2 \cdots b_k$ とおけば，a の位数は n である (系 1.11). □

[定理 1.13] Abel 群 G の有限位数の元の全体は G の部分群である.

[証明] G の有限位数の元の全体を T とする. 任意の $a, b \in T$ に対して, 定理 1.10 より $ab \in T$. また, 任意の $a \in T$ に対して, 系 1.7 より $a^{-1} \in T$. ゆえに T は G の部分群である. □

[注意 1.14] G が非可換群の場合, 2 つの有限位数の元の積は必ずしも有限位数とは限らず, 無限位数になることもある. 例えば, G を 2 次の実正則行列全体からなる乗法群とし,

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

とおくと, $A^2 = B^2 = 1$, $C = AB$ である. とくに, A, B は有限位数である. 一方, 任意の整数 k に対して

$$C^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

が成り立ち, C^k が単位行列になるのは $k = 0$ のとき, またそのときに限る. したがって C は無限位数である (定理 1.1).

2 巡回群

群 G が有限個の元 $a_1, \ldots, a_m$ で生成されるとき，G を

$$\langle a_1, \ldots, a_m \rangle$$

という記号で表す. このとき $a_1, \ldots, a_m$ を G の**生成元**という. とくに，G がただ一つの元 a で生成されるとき，すなわち

$$G = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$$

と表されるとき，G は**巡回群**であるという.

[例 2.1] 加法群 $\mathbb{Z}$ は 1 を生成元とする無限巡回群である.

[例 2.2] 正の整数 n に対して，加法群 $\mathbb{Z}/n\mathbb{Z}$ は 1 を代表元とする剰余類 $1+n\mathbb{Z}$ から生成される位数 n の巡回群である．

[定理 2.3] 巡回群 G は Abel 群である．

[証明] 巡回群 G の生成元を a とする．G の元はすべて a^i $(i \in \mathbb{Z})$ の形で書き表せる．そこで G の 2 つの元を a^i, a^j とすれば

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$$

である． □

[定理 2.4] G を群，a を G の位数 n の元とする．このとき，G の巡回部分群 $\langle a \rangle$ の位数は n であり,

$$\begin{aligned}\langle a \rangle &= \{a^i \mid i \in \mathbb{Z},\, 0 \leq i \leq n-1\} \\ &= \{1,\, a,\, a^2,\, \ldots,\, a^{n-1}\}\end{aligned}$$

が成り立つ.

[証明] 任意の整数 m に対して，整数 q, r の組がただ一つ存在して

$$m = nq + r, \quad 0 \leq r < n$$

が成り立つ．よって $a^m = a^r$．したがって,

$$\langle a \rangle = \{1,\, a,\, a^2,\, \ldots,\, a^{n-1}\}.$$

a の位数は n なので, 整数 i に対して,

$$0 < i < n \Rightarrow a^i \neq 1.$$

さらに, 2 つの整数 i, j に対して,

$$0 \leq i < j < n \Rightarrow 0 < j - i < n \Rightarrow a^{j-i} \neq 1 \Rightarrow a^j \neq a^i.$$

ゆえに $\langle a \rangle$ の元 1, a, a^2, …, a^{n-1} は互いに異なる．したがって $\langle a \rangle$ の位数は n である． □

[系 2.5] 無限巡回群の単位元以外のすべての元は無限位数である.

[証明] G を無限巡回群とし, a を G の生成元とする. すなわち, $G = \langle a \rangle$. もし仮に a が有限位数ならば, 定理 2.4 より $\langle a \rangle$ の位数は有限になってしまい, 矛盾が生じる. ゆえに a は無限位数である.

次に, x を G の単位元以外の元とすると, ある 0 でない整数 i によって $x = a^i$ と表せる. もし x が有限位数ならば, ある正の整数 k が存在して $x^k = 1$. したがって $a^{ik} = 1$ かつ $ik \neq 0$. これは a が無限位数であることに矛盾する (定理 1.1). □

[系 2.6] G を位数 n の有限群, a を G の元とする. このとき, a の位数は n の約数であり, $a^n = 1$ が成り立つ.

[証明] G の巡回部分群 $\langle a \rangle$ の位数は G の位数の約数である[2)]. 定理 2.4 より, a の位数は $\langle a \rangle$ の位数に等しい. ゆえに, a の位数は n の約数である. したがって, $a^n = 1$ が成り立つ (定理 1.2). □

[系 2.7] 素数位数の群は巡回群である.

[証明] G を位数が素数 p の群とする. G の位数は 1 より大きいので, 単位元とは異なる元 a が存在し, その位数を n とおくと $n > 1$ である. 定理 2.4 より, G の巡回部分群 $\langle a \rangle$ の位数は n である. 一般に群 G の部分群の位数は G の位数の約数であるから, $n = p$ でなければならない. $\langle a \rangle \subseteq G$ であり, なおかつ両者の群の位数は一致するので, $G = \langle a \rangle$ となる. □

[定理 2.8] G を巡回群, a を G の元とする. このとき, 次の 3 つの条件は同値である.

(i) a は G の生成元である. すなわち $G = \langle a \rangle$.

(ii) b を G の生成元とするとき, ある整数 k が存在して $b = a^k$.

(iii) G の任意の元 x に対して, ある整数 l が存在して $x = a^l$.

[2)] 有限群の部分群の位数に関する Lagrange の定理より.

[証明] (i)⇒(ii)　$b \in G = \langle a \rangle$ より明らか.

(ii)⇒(iii)　$x \in G$ とすると, b は G の生成元なので, ある整数 i が存在して $x = b^i$ となる. また, (ii) より, ある整数 k が存在して $b = a^k$ となる. ゆえに $x = a^{ik}$. よって $l = ik$ とおけばよい.

(iii)⇒(i)　(iii) は $G \subseteq \langle a \rangle$ を意味する. 逆に, 任意の整数 i に対して $a^i \in G$ だから, $\langle a \rangle \subseteq G$. ゆえに $G = \langle a \rangle$. □

[定理 2.9] G を位数 n の有限群, a を G の元とする. このとき, 次の 2 つの条件は同値である.

(i) G は a を生成元とする巡回群である.

(ii) a の位数は n である.

[証明] (i)⇒(ii)　G の位数は n なので, a, a^2, ..., a^{n+1} の $n+1$ 個の元うち少なくともどれか 2 つは一致する. よって, ある正の整数 i, j が存在して, $a^i = a^j$ かつ $i \neq j$ が成り立つ. このとき, $a^{j-i} = 1$ かつ $j - i \neq 0$ である. ゆえに, a は有限位数である (定理 1.1). a の位数は $G = \langle a \rangle$ の位数 n に一致する (定理 2.4).

(ii)⇒(i)　$H = \langle a \rangle$ とおくと，$H \subseteq G$ である．一方，H は a を生成元とする巡回群である．ゆえに H の位数は n である (定理 2.4)．すなわち H の位数は G の位数に一致する．したがって $H = G$. □

[例 2.10] 有限体 $\mathbb{Z}/41\mathbb{Z}$ の乗法群 $(\mathbb{Z}/41\mathbb{Z})^\times$ は位数 40 の群である．

41 を法としての 2 の冪を計算すると，

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 16, \quad 2^5 \equiv 32, \quad 2^6 \equiv 64 \equiv -18,$$
$$2^7 \equiv -36 \equiv 5, \quad 2^8 \equiv 10, \quad 2^9 \equiv 20, \quad 2^{10} \equiv 40 \equiv -1.$$

ゆえに，$2^{20} \equiv 1 \pmod{41}$ となって，2 の位数は 20 であることがわかる．

次に，41 を法としての 3 の冪を計算すると，

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 27 \equiv -14, \quad 3^4 \equiv -42 \equiv -1.$$

ゆえに，$3^8 \equiv 1 \pmod{41}$ となって，3 の位数は 8 であることがわかる．

さて，$2^{\frac{20}{5}} = 2^4$ の位数は 5 である．5, 8 の最大公約数は 1 だから，

$$2^4 \cdot 3 \equiv 48 \equiv 7 \pmod{41}$$

の位数は 40 である．ゆえに，乗法群 $(\mathbb{Z}/41\mathbb{Z})^\times$ は 7 を代表とする剰余類を生成元にもつ巡回群である．

[定理 2.11] G を無限巡回群とし，a を G の生成元とする．このとき，G の生成元は a, a^{-1} の 2 つしかない．

[証明] k を整数とし，G が a^k によって生成されるとすると，ある整数 x が存在して $a = (a^k)^x$ と書ける．よって $a^{kx-1} = 1$ となる．a は無限位数の元であるから，$kx - 1 = 0$ でなければならない (定理 1.1)．ゆえに $kx = 1$．k, x はともに整数だから，$k = \pm 1$ でなければならない．

逆に, $a = (a^{-1})^{-1}$ だから，a^{-1} は G の生成元である (定理 2.8)． □

[定理 2.12] G を群，a を G の位数 n の元とする．さらに，k を整数，d を k, n の最大公約数とする．このとき，

$$\langle a^k \rangle = \langle a^d \rangle$$

が成り立つ．また，$\langle a^k \rangle$ の位数は n/d である．

[証明] d は k の約数なので，$k = dk_1$ とおくと，

$$a^k = (a^d)^{k_1} \Rightarrow a^k \in \langle a^d \rangle \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle.$$

$\langle a^k \rangle$ の位数と $\langle a^d \rangle$ の位数とは互いに等しく n/d である (定理 1.5，定理 2.4)．とくに有限位数だから，$\langle a^k \rangle = \langle a^d \rangle$ がいえる． □

[系 2.13] G を位数 n の巡回群, a を G の生成元とする．このとき, 整数 k について,

$$a^k \text{ が } G \text{ の生成元} \Leftrightarrow \gcd(k, n) = 1$$

が成り立つ．さらに, 位数 n の巡回群 G の生成元の個数は $\varphi(n)$ である．ただし，$\varphi(n)$ は Euler の関数である．

[証明] ($\Leftarrow$)　定理 2.12 において $d = 1$ の場合を考えれば, $\gcd(k, n) = 1$ より,

$$\langle a^k \rangle = \langle a \rangle = G.$$

($\Rightarrow$)　定理 2.12 において $d > 1$ の場合を考えれば, $\gcd(k, n) > 1$ のとき $\langle a^k \rangle$ の位数は n より小さいから $\langle a^k \rangle \neq G$. よって a^k は G の生成元ではない.

以上より, 系の主張の前半が示された. さらに, G の元は

$$a^k, \quad k \in \mathbb{Z}, \quad 0 \leq k \leq n-1$$

がすべてである (定理 2.4). 主張の前半より, このうちで $\gcd(k, n) = 1$ を満たすもの, またそれのみが G の生成元であり, その個数は $\varphi(n)$ である. □

[定理 2.14] 巡回群 G の部分群 H は巡回群である.

[証明] G の生成元を a，単位元を 1 で表す．H の元はすべて a^i $(i \in \mathbb{Z})$ の形で書き表せる.

$a = 1$ のとき, すなわち G が単位元のみからなる群であるときは明らかである. また, H が単位元 1 のみからなる G の部分群であるとき，H は巡回群である.

$a \neq 1$ とし, H は単位元 1 のほかにも元をもつとする. 正の整数からなる集合

$$S = \{i \in \mathbb{Z} \mid i > 0 \text{ かつ } a^i \in H\}$$

を考える．H についての仮定と

$$a^{-i} \in H \Leftrightarrow a^i \in H$$

とから，S は空集合でないことがわかる．したがって S は最小元 n をもつ.

このとき, $H = \langle a^n \rangle$ が成り立つ．実際，$\langle a^n \rangle \subseteq H$ は明らかである．逆に，H の元を a^m $(m \in \mathbb{Z})$ とする．m を n で割ると, ある整数 q, r の組が一意的に存在して

$$m = nq + r, \quad 0 \leq r < n$$

が成り立つから

$$a^r = a^m a^{-nq} \in H.$$

n の最小性により $r = 0$．ゆえに $m = nq$. これより

$$a^m = a^{nq} \in \langle a^n \rangle$$

がいえる. したがって $H \subseteq \langle a^n \rangle$. □

[定理 2.15] G を位数 n の巡回群とする．n の任意の正の約数 d に対して，G の位数 d の部分群がただ 1 つ存在する．a を G の生成元とすれば, $\langle a^{\frac{n}{d}} \rangle$ がその部分群である.

$$\begin{array}{ccc} n & \longleftarrow & G = \langle a \rangle \\ | & & | \\ d & \longleftarrow & \langle a^{\frac{n}{d}} \rangle \\ | & & | \\ 1 & \longleftarrow & \{e\} \end{array}$$

[証明] a を G の生成元とする．定理 2.9 より, a の位数は n である. 存在：n の約数 $d > 0$ に対して，$\langle a^{\frac{n}{d}} \rangle$ は G の位数 d の部分群である (系 1.8, 定理 2.4).

一意性：H を G の位数 d の部分群とする．H は巡回群 (定理 2.14) なので, ある整数 k が存在して,

$$H = \langle a^k \rangle, \quad 0 \leq k < n$$

となる．k, n の最大公約数を d' とすれば，定理 2.12 より

$$\langle a^k \rangle = \langle a^{d'} \rangle, \quad d = \frac{n}{d'}.$$

ゆえに,

$$H = \langle a^{\frac{n}{d}} \rangle.$$

したがって，G の位数 d の部分群はすべて $\langle a^{\frac{n}{d}} \rangle$ に一致する．これは一意性を示している． □

[例 2.16] G を位数 12 の巡回群とし，生成元のひとつを a とする．このとき，G の元のうちで，生成元になるものは $\varphi(12) = 4$ 個あって

$$a, \quad a^5, \quad a^7, \quad a^{11}$$

である．また，12 の約数 1, 2, 3, 4, 6, 12 に対応する G の部分群はそれぞれ

$$\{e\}, \quad \langle a^6 \rangle, \quad \langle a^4 \rangle, \quad \langle a^3 \rangle, \quad \langle a^2 \rangle, \quad G$$

であり，これらが巡回群 G の部分群のすべてである.

[定理 2.17] G を位数 n の巡回群とする．n の正の約数 d に対して, G に含まれる位数 d の元の個数は $\varphi(d)$ である．さらに,

$$n = \sum_{d|n,\, d>0} \varphi(d)$$

が成り立つ．ただし, $\varphi(n)$ は Euler の関数である．

[証明] a を G の生成元とすると, 定理 2.15 より, n の任意の約数 $d > 0$ に対して $\langle a^{\frac{n}{d}} \rangle$ が G におけるただ 1 つの位数 d の部分群である．x を G に属する位数 d の元とすれば, $\langle x \rangle$ は G の位数 d の巡回部分群となる (定理 2.4)．G における位数 d の部分群はただ 1 つだから, $\langle x \rangle = \langle a^{\frac{n}{d}} \rangle$．よって, $x \in \langle a^{\frac{n}{d}} \rangle$ である．定理 2.9 より, x は $\langle a^{\frac{n}{d}} \rangle$ の生成元である．逆に, $\langle a^{\frac{n}{d}} \rangle$ の生成元はすべて位数 d である (定理 2.9)．ゆえに, G の位数 d の元の全体は $\langle a^{\frac{n}{d}} \rangle$ の生成元の全体に等しい．また, $\langle a^{\frac{n}{d}} \rangle$ の生成元の個数は $\varphi(d)$ である (定理 2.13)．これで定理の前半が示された．さらに, 集合の直和

$$G = \bigcup_{d|n, d>0} \{x \in G \mid x \text{ の位数は } d\}$$

が成り立つ (系 2.6) から,

$$|G| = \sum_{d|n,\, d>0} \#\{x \in G \mid x \text{ の位数は } d\}.$$

これより求める等式が得られる． □

[定理 2.18] G を有限群とする．任意の正の整数 l に対して，$x^l = 1$ となる G の元 x の個数が l 以下ならば，G は巡回群である．

[証明] G の位数を n とする．G のすべての元について, その位数は n の約数である (系 2.6)．n の正の約数 d に対して，G に含まれる位数 d の元の個数を $N_d(G)$ とすれば

$$\sum_{d|n,\, d>0} N_d(G) = n$$

が成り立つ．

$N_d(G) \neq 0$ であるような d に対して，位数 d の元 a が存在する．H を a により生成される G の巡回部分群とする．H の元 x はすべて $x^d = 1$ を満たす．ところが，H の元の個数は d 個 (定理 2.4) だから，仮定より

$$H = \{x \in G \mid x^d = 1\}.$$

したがって G の位数 d の元はすべて H に含まれる．よって $N_d(G) = N_d(H)$．一方，H の生成元，すなわち位数 d の元の個数は $\varphi(d)$ である (系 2.13)．ここで φ は Euler の関数である．よって

$$N_d(G) \neq 0 \Rightarrow N_d(G) = N_d(H) = \varphi(d).$$

したがって, $N_d(G) = 0$ または $\varphi(d)$ である. ところが, もし仮に n のある正の約数 $d_0 > 0$ が存在して $N_{d_0}(G) = 0$ ならば,

$$n = \sum_{d|n,\, d>0} N_d(G) < \sum_{d|n,\, d>0} \varphi(d) = n$$

となり矛盾が生じる (最後の等式は定理 2.15). ゆえに，n のすべての正の約数 d に対して $N_d(G) = \varphi(d)$ でなければならない．とくに

$$N_n(G) = \varphi(n) \neq 0$$

となるから，G は位数 n の元を含む．よって G は巡回群である (定理 2.9)． □

[系 2.19] 巡回群ではない任意の有限群 G に対して, ある正の整数 l が存在して, $x^l = 1$ を満たす $x \in G$ が l 個より多く存在する.

[証明] 定理 2.18 の対偶を考えればよい. □

[系 2.20] 整域 R の単元全体からなる乗法群 $R^\times$ の有限部分群は巡回群である.

[証明] $R^\times$ の有限部分群を G とする．R は整域なので, 任意の正の整数 l に対して，多項式 $X^l - 1 \in R[X]$ の根は l 個以下である．よって G の元 x で $x^l = 1$ となるものは l 個以下である．ゆえに定理 2.18 より G は巡回群である． □

[定理 2.21] G を有限群とし, そのすべての部分群の位数は互いに異なるとする. このとき, G は巡回群である.

[証明] 有限群 G の位数 n に関する数学的帰納法によって証明する.

$n = 1$ のとき, G は単位元だけからなる巡回群となり, 定理の主張は明らかに成り立つ.

$n > 1$ のとき, n より小さい位数の有限群については定理の主張が正しいと仮定する. 単位元とは異なる G の元で位数が最小のものが存在する. それを a とおく. a の位数は素数である. なぜなら, もし a の位数が真の約数 d をもてば, a^d の位数は a の位数の真の約数であり (系 1.8), a の最小性に反する. a の位数を p とおく.

N を a によって生成される G の巡回部分群とする. N の位数は p であり (定理 2.4), p は G の位数 n の約数である. 任意の $x \in G$ に対して xNx^{-1} もまた G の部分群であり, その位数は N の位数に等しい. 定理の仮定より, $N = xNx^{-1}$ となる. すなわち, N は G の正規部分群である. よって, 剰余群 G/N が定まる.

自然な準同型 $\pi : G \to G/N$ により, N を含むような G の部分群全体と G/N の部分群全体とは 1 対 1 に対応し, G の任意の部分群 H に対して $\pi(H) = H/N$ が成り立つ. このことから, G/N のすべての部分群の位数が互いに異なることがいえる. さらに,

$$(G : N) = \frac{|G|}{|N|} < |G|.$$

帰納法の仮定より, G/N は巡回群である. その生成元は, ある $b \in G$ によって bN と表せる.

K を b で生成される G の巡回部分群とする. KN は G の部分群であり, N は KN の正規部分群なので, 剰余群 KN/N が定義できる. $b \in KN$ より $bN \in KN/N$ なので, $G/N \subseteq KN/N$. また, $KN \subseteq G$ より逆の包含関係もいえて, $G/N = KN/N$ となる. 位数を比較すると,

$$\frac{|G|}{|N|} = (G : N) = (KN : N) = \frac{|KN|}{|N|}.$$

ゆえに $|G| = |KN|$ である. KN, G はともに有限集合であり, $KN \subseteq G$ だから, $G = KN$ が成り立つ.

$p \mid |K|$ のとき, K は位数 p の部分群をもつ (定理 2.15) が, 定理の仮定によりそれは N に一致し, $N \subseteq K$ がいえる. よって $KN = K$ が成り立つ. ゆえに $G = K$ となり, G は巡回群である.

$p \nmid |K|$ のとき, $|K|$ と $|N|$ とは互いに素である. もし $x \in K \cap N$ ならば, x の位数は, $|K|$ と $|N|$ との公約数だから, 1 でなければならない. ゆえに $x = 1$. したがって $K \cap N = \{1\}$ である. このとき,

$$|KN| = \frac{|K| \cdot |N|}{|K \cap N|} = |K| \cdot |N|.$$

N が G の正規部分群であることを示したのと同様に K もまた G の正規部分群であることがいえる. このことから, $aba^{-1} \in K$, $ba^{-1}b^{-1} \in N$ がいえるので,

$$aba^{-1}b^{-1} \in K \cap N = \{1\}.$$

これより $ab = ba$ が得られる. a の位数と b の位数は互いに素だから, ab の位数は $|K| \cdot |N|$ に, したがって $|KN|$ に一致する (定理 1.10). ゆえに KN は ab によって生成される (定理 2.9). したがって, G は巡回群である.

以上より, すべての n について定理の主張が証明された. □

[系 2.22] 有限群 G の位数 n の各約数 $d > 0$ に対して, G の位数 d の部分群がただ 1 つだけ存在するならば, G は巡回群である.

[証明] 仮定より, 位数が n の約数であるような 2 つの異なる G の部分群は異なる位数をもつ. 一方, 有限群 G の部分群の位数は常に G の位数の約数である. ゆえに, 任意の 2 つの異なる G の部分群は異なる位数をもつ. したがって定理 2.21 より G は巡回群である. □

[定理 2.23] 自明な部分群しか持たない群 G は $\{1\}$ であるか，または位数が素数の巡回群である.

[証明] $G \neq \{1\}$ と仮定する．G の単位元 1 でない元 a に対して，$\langle a \rangle$ は G の部分群である．$\langle a \rangle \neq \{1\}$ であるから，仮定より $G = \langle a \rangle$．したがって G は巡回群である．もし仮に G が無限群ならば, $\langle a^2 \rangle$ は a を含まない G の巡回部分群になり, G が自明な部分群しかもたないという仮定に反する. したがって, G は有限巡回群である.

G の位数を n とおく. もし仮に n が合成数ならば, ある正の約数 $m > 1$ が存在する．G は巡回群だから, 定理 2.15 より位数 m の部分群が存在する．これは仮定に反する．ゆえに n は素数である. したがって G は巡回群である (系 2.7). □

[系 2.24] 可換な単純群は $\{1\}$ か位数が素数の巡回群である.

[証明] Abel 群の部分群はすべて正規部分群である．よって可換な単純群は自明な部分群しか持たない．このことに注意して定理 2.23 を適用すればよい． □

3 巡回群の自己同型

[定理 3.1] G, G' を群とし, a を G の有限位数の元, $f : G \to G'$ を群の準同型写像とする.

(i) $f(a)$ は有限位数であり, その位数は a の位数の約数である.

(ii) f が同型写像ならば, $f(a)$ の位数は a の位数に一致する.

[証明] a の位数を n とおく.

(i) f の準同型性と $a^n = 1$ より

$$f(a)^n = f(a^n) = 1.$$

定理 1.1 より, $f(a)$ は有限位数である. また, 定理 1.2 より, $f(a)$ の位数は n の約数である.

(ii) $f(a)$ の位数を m とし, $b = f(a)$ とおく. f は同型写像だから, 逆写像 f^{-1} が存在し, f^{-1} は準同型である. よって,

$$a^m = f^{-1}(b)^m = f^{-1}(b^m) = f^{-1}(1) = 1.$$

定理 1.2 より $n \mid m$ である. (i) より $m \mid n$ であり, m, n はともに正の整数だから, $m = n$ となる. □

[定理 3.2] $f : G \to G'$ を群の準同型写像とする．G が巡回群ならば，f の像 $f(G)$ も巡回群である．a を G の生成元とすれば $f(a)$ が $f(G)$ の生成元である.

[証明] $f(G)$ のすべての元は，ある $x \in G$ によって $f(x)$ と表される．また, G の任意の元 x は，ある $i \in \mathbb{Z}$ によって $x = a^i$ と表される．f の準同型性から，

$$f(x) = f(a^i) = f(a)^i.$$

したがって $f(G)$ は $f(a)$ によって生成される巡回群である． □

[系 3.3] 巡回群 G の部分群 H による剰余群 G/H は巡回群である．a を G の生成元とすれば aH が G/H の生成元になる．

[証明] 自然な全射準同型写像

$$G \to G/H, \qquad x \mapsto xH$$

に対して定理 3.2 を適用すればよい． □

[系 3.4] 群 G が巡回群であるための必要十分条件は，全射準同型 $\mathbb{Z} \to G$ が存在することである．

[証明] G が巡回群であるとき，a を G の生成元とし, 写像

$$\mathbb{Z} \to G, \quad i \mapsto a^i$$

を考えれば，これは全射準同型である．逆は定理 3.2 より明らかである． □

[定理 3.5] G を群とする．

(i) G が無限巡回群であるための必要十分条件は，G が加法群 $\mathbb{Z}$ と同型であることである．

(ii) G が位数 n の巡回群であるための必要十分条件は，G が加法群 $\mathbb{Z}/n\mathbb{Z}$ と同型であることである．

[証明] (i)　G を無限巡回群，G の生成元を a とする．準同型写像

$$\mathbb{Z} \to G, \quad i \mapsto a^i$$

は全単射である．実際，上の写像の核はただ 1 つの元からなる．逆は明らか．

(ii)　G を位数 n の巡回群，a を G の生成元とする．このとき，準同型写像

$$\mathbb{Z} \to G, \quad i \mapsto a^i$$

は全射であり, その核は $n\mathbb{Z}$ である (定理 1.2)．よって準同型定理から $G \cong \mathbb{Z}/n\mathbb{Z}$ を得る．逆は明らか．　□

[定理 3.6] G を群, a を G の生成元, f を G から G 自身への準同型写像とする．f が G の自己同型であるための必要十分条件は, $f(a)$ が G の生成元となることである．

[証明] f が G の自己同型ならば, f は全射である．よって $f(G) = G$. 一方, 定理 3.2 により, $f(a)$ は $f(G)$ の生成元である．ゆえに $f(a)$ は G の生成元である．

逆に, $f(a)$ が G の生成元とすれば, 任意の $x \in G$ に対して, ある $k \in \mathbb{Z}$ が存在して

$$x = f(a)^k = f(a^k) \in f(G).$$

よって G のすべての元は $f(G)$ に属する．ゆえに $G \subseteq f(G)$. 逆の包含関係は明らかだから, $f(G) = G$.　□

[定理 3.7] 無限巡回群 $\langle a \rangle$ から群 G への準同型写像は, 各 $x \in G$ に対して

$$f_x : \langle a \rangle \to G, \quad a^k \mapsto x^k \quad (k \in \mathbb{Z})$$

によって定まるものがすべてである．

[証明] a は無限位数なので, 任意の $k, l \in \mathbb{Z}$ に対して

$$a^k = a^l \Rightarrow k = l \Rightarrow x^k = x^l$$

となるから, f_x は well-defined である. また, 任意の $k, l \in \mathbb{Z}$ に対して

$$f_x(a^k)f_x(a^l) = x^k x^l = x^{k+l} = f_x(a^{k+l}) = f_x(a^k a^l).$$

よって f_x は準同型である. さらに, f を任意の準同型写像とするとき, $y = f(a)$ とおけば, 任意の $k \in \mathbb{Z}$ に対して

$$f(a^k) = f(a)^k = y^k = f_y(a^k).$$

ゆえに $f = f_y$. □

[定理 3.8] 位数 n の巡回群 $\langle a \rangle$ から群 G への準同型写像は, $x^n = 1$ をみたす各 $x \in G$ に対して

$$f_x : \langle a \rangle \to G, \quad a^k \mapsto x^k \quad (k \in \mathbb{Z})$$

によって定まるものがすべてである.

[証明] a の位数は n なので, 任意の $k, l \in \mathbb{Z}$ に対して

$$a^k = a^l \Rightarrow k \equiv l \pmod{n} \Rightarrow x^{k-l} = 1 \Rightarrow x^k = x^l$$

となるから, f_x は well-defined である. また, 任意の $k, l \in \mathbb{Z}$ に対して

$$f_x(a^k)f_x(a^l) = x^k x^l = x^{k+l} = f_x(a^{k+l}) = f_x(a^k a^l).$$

よって f_x は準同型である. さらに, f を任意の準同型写像とするとき, $y = f(a)$ とおけば,

$$y^n = f(a)^n = f(a^n) = f(1) = 1.$$

さらに, 任意の $k \in \mathbb{Z}$ に対して

$$f(a^k) = f(a)^k = y^k = f_y(a^k).$$

ゆえに $f = f_y$.

□

[定理 3.9] 巡回群 G の自己同型群 $\mathrm{Aut}\, G$ は Abel 群である.

[証明] 巡回群 G の生成元を a とする. G の任意の自己同型写像 σ に対して, ある整数 n が存在して

$$\sigma(a) = a^n.$$

したがって, τ も G の自己同型写像とすれば, $\tau(a) = a^m$ となる整数 m がある. よって

$$\tau\sigma(a) = (a^m)^n = a^{mn} = (a^n)^m = \sigma\tau(a).$$

G の任意の元 x は生成元 a の冪であるから, 任意の $x \in G$ に対して

$$\sigma\tau(x) = \tau\sigma(x).$$

すなわち $\sigma\tau = \tau\sigma$. □

[定理 3.10] G を巡回群とし, $\mathrm{Aut}\, G$ を自己同型群とする.

(i) $|G| = \infty$ ならば, $\mathrm{Aut}\, G \cong \mathbb{Z}/2\mathbb{Z}$.

(ii) $|G| = d < \infty$ ならば, $\mathrm{Aut}\, G \cong (\mathbb{Z}/d\mathbb{Z})^\times$.

[証明] 巡回群 G の生成元を a とする. 任意の準同型写像 $\sigma : G \to G$ に対して, ある整数 n が存在して, $\sigma(a) = a^n$ と書ける. とくに σ が自己同型ならば, a^n は G の生成元でなければならない (定理 3.6) から

$$(a^n)^l = a$$

となる整数 l が存在する.

(i) $|G| = \infty$ のとき, $nl = 1$ となり, $n = \pm 1$. $\sigma(a) = a^{-1}$ によって定まる準同型写像 σ が $\mathrm{Aut}\, G$ の単位元以外の元となる. ゆえに $\mathrm{Aut}\, G$ は位数 2 の巡回群である.

(ii) $|G| = d < \infty$ のとき,

$$nl \equiv 1 \pmod{d}$$

となるから, n は d と互いに素である. よって写像

$$\Phi : \mathrm{Aut}\, G \to (\mathbb{Z}/d\mathbb{Z})^\times, \quad \sigma \mapsto n \pmod{d}$$

が定まる. ここに n は $\sigma(a) = a^n$ を満たす.

d を法として互いに合同ではない整数 m, n を与えれば, $\sigma(a) = a^n$, $\tau(a) = a^m$ によって定まる 2 つの準同型写像 σ, τ は互いに異なる. これは Φ が単射であることを意味する.

また, n が d と互いに素であれば, a^n は G の生成元となる (定理 2.13). よって $\sigma(a) = a^n$ によって準同型写像 σ を定めると, σ は G の自己同型になる. ゆえに Φ は全射である.

さらに, τ を $\tau(a) = a^m$, $\gcd(m, d) = 1$ で定まる自己同型とすれば

$$\tau\sigma(a) = \tau(a^n) = a^{mn}$$

より

$$\Phi(\tau\sigma) \equiv mn \equiv \Phi(\tau)\Phi(\sigma) \pmod{d}.$$

ゆえに Φ は準同型である. □

[例 3.11] 無限巡回群 G の自己同型写像は

$$\mathrm{id}_G : G \to G, \quad x \mapsto x,$$
$$\sigma : G \to G, \quad x \mapsto x^{-1}$$

の 2 つだけである. このとき

$$\mathrm{Aut}\, G = \{\mathrm{id}_G, \sigma\} = \langle\sigma\rangle, \quad \sigma^2 = \mathrm{id}_G$$

である. $\mathrm{Aut}\, G$ は位数 2 の巡回群である.

[例 3.12] G を素数 p を位数とする巡回群とすれば, Aut G $\cong (\mathbb{Z}/p\mathbb{Z})^\times$ なので, $\mathrm{Aut}\, G$ は位数 $p-1$ の巡回群になる.

[例 3.13] G を位数 8 の巡回群とし, a を G の生成元とする. $\mathrm{Aut}\, G$ の元は

$$\sigma(a) = a^k, \quad \gcd(k, 8) = 1$$

によって定まる準同型 σ である. このとき $k = 1, 3, 5, 7$ であるから,

$$\mathrm{id}_G(a) = a, \quad \sigma_1(a) = a^3, \quad \sigma_2(a) = a^5, \quad \sigma_3(a) = a^7$$

とすれば,

$$\operatorname{Aut} G = \{\mathrm{id}_G,\, \sigma_1,\, \sigma_2,\, \sigma_3\}, \quad \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \mathrm{id}_G$$

となる. ゆえに

$$\operatorname{Aut} G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

とくに, G が巡回群であっても, $\operatorname{Aut} G$ は一般には巡回群ではないことがわかる.

4 $\mathbb{Z}$ について

$m \in \mathbb{Z}$ に対して, m の倍数全体からなる集合を $m\mathbb{Z}$ とおく. すなわち,

$$m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$$

とおく. $m\mathbb{Z}$ は, m によって生成される $\mathbb{Z}$ の巡回部分群である.

$a_1, a_2, \ldots, a_n \in \mathbb{Z}$ で生成される $\mathbb{Z}$ の部分群は,

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_i \in \mathbb{Z}\}$$

である.

[定理 4.1] (i) 加法群 $\mathbb{Z}$ の部分群 H は巡回群であり, ある整数 n が存在して $H = n\mathbb{Z}$ と書ける.

(ii) d を 2 つの整数 a, b の最大公約数とすれば

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

が成り立つ.

(iii) l を 2 つの整数 a, b の最小公倍数とすれば

$$a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z}$$

が成り立つ.

[証明] (i)　定理 2.14 を適用すればよい.

(ii)　(i) より, ある整数 d があって

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

と書ける. $-d\mathbb{Z} = d\mathbb{Z}$ だから, $d > 0$ としてよい.

$a \in d\mathbb{Z}$ より, ある $k \in \mathbb{Z}$ が存在して $a = kd$. よって $d \mid a$. 同様にして $b \mid d$ もいえる. ゆえに, d は a, b の公約数である.

$d \in a\mathbb{Z} + b\mathbb{Z}$ より, ある x, $y \in \mathbb{Z}$ が存在して

$$d = ax + by.$$

したがって, 任意の整数 d_1 に対して,

$$d_1 \mid a,\ d_1 \mid b \Rightarrow d_1 \mid d.$$

ゆえに, d は a, b の公約数のうちで最大のものである.

(iii)　(i) より, ある整数 l があって

$$a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z}$$

と書ける. $-l\mathbb{Z} = l\mathbb{Z}$ だから, $l > 0$ としてよい.

$l \in a\mathbb{Z} \cap b\mathbb{Z}$ より, a, b はともに l を割る. ゆえに, l は a, b の公倍数である.

任意の整数 l_1 に対して,

$$a \mid l_1,\ b \mid l_1 \Rightarrow l_1 \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow l_1 \in l\mathbb{Z} \Rightarrow l \mid l_1.$$

ゆえに, l は a, b の公倍数のうちで最小のものである. □

[定理 4.2] a, b を 0 でない整数, d を a, b の最大公約数, l を a, b の最小公倍数とする. このとき, 同型

$$a\mathbb{Z}/l\mathbb{Z} \cong d\mathbb{Z}/b\mathbb{Z}$$

が成り立つ.

[証明] $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ であり, $l\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ である (定理 4.1) から, 群の第 2 同型定理より,

$$a\mathbb{Z}/l\mathbb{Z} = a\mathbb{Z}/(a\mathbb{Z} \cap b\mathbb{Z}) \cong (a\mathbb{Z} + b\mathbb{Z})/a\mathbb{Z} = d\mathbb{Z}/b\mathbb{Z}$$

が成り立つ. □

[定理 4.3] n, m, d を正の整数とし, $n = dm$ であるとする. このとき, 2 つの同型

$$\mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}, \quad \frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/d\mathbb{Z}$$

が成り立つ.

[証明] $n = dm$ なので, 任意の k, $k' \in \mathbb{Z}$ に対して

$$k \equiv k' \pmod{m} \Leftrightarrow dk \equiv dk' \pmod{n}.$$

よって, 写像

$$f : \mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}, \quad k + m\mathbb{Z} \mapsto dk + n\mathbb{Z}$$

は well-defined かつ単射である. f が全射準同型であることは容易に確かめられる.

d は n の約数なので, 任意の k, $k' \in \mathbb{Z}$ に対して

$$k \equiv k' \pmod{n} \Rightarrow k \equiv k' \pmod{d}.$$

よって, 写像

$$g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}, \quad k + n\mathbb{Z} \mapsto k + d\mathbb{Z}$$

は well-defined である. 全射準同型であることは容易に確かめられる. g の核は

$$\ker g = \{k + n\mathbb{Z} \mid k \in d\mathbb{Z}\} = d\mathbb{Z}/n\mathbb{Z}$$

である. 準同型定理によって, 求める同型が得られる. □

[定理 4.4] m, n を正の整数とし, $d = \gcd(m, n)$, $m = dm'$, $n = dn'$ とする. このとき, m 倍写像

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

について,

$$\ker [m] = n'\mathbb{Z}/n\mathbb{Z}, \quad [m](\mathbb{Z}/n\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$$

が成り立つ.

[証明] 任意の $x \in \mathbb{Z}$ に対して,

$$\begin{aligned} x + n\mathbb{Z} \in \ker[m] &\Leftrightarrow mx + n\mathbb{Z} = 0 + n\mathbb{Z} \\ &\Leftrightarrow mx \equiv 0 \pmod{n} \\ &\Leftrightarrow m'x \equiv 0 \pmod{n'} \\ &\Leftrightarrow x \equiv 0 \pmod{n'} \\ &\Leftrightarrow x + n\mathbb{Z} \in n'\mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

ゆえに, $\ker[m] = n'\mathbb{Z}/n\mathbb{Z}$.

次に, 任意の $x \in \mathbb{Z}$ に対して,

$$mx + n\mathbb{Z} = dm'x + n\mathbb{Z} \in d\mathbb{Z}/n\mathbb{Z}.$$

ゆえに, $[m](\mathbb{Z}/n\mathbb{Z}) \subseteq d\mathbb{Z}/n\mathbb{Z}$. 逆に, 任意の $x \in \mathbb{Z}$ に対して, $\gcd(m', n) = 1$ より, ある $y \in \mathbb{Z}$ が存在して, $m'y \equiv x \pmod{n}$. よって,

$$dx + n\mathbb{Z} = dm'y + n\mathbb{Z} = my + n\mathbb{Z} \in [m](\mathbb{Z}/n\mathbb{Z}).$$

ゆえに, $d\mathbb{Z}/n\mathbb{Z} \subseteq [m](\mathbb{Z}/n\mathbb{Z})$. したがって, $[m](\mathbb{Z}/n\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$ が示された. □

[定理 4.5] p を素数, l, k, v を整数とし,

$$0 \leq l < k \leq v$$

を満たしているとする. このとき, 全射準同型

$$\pi_k : p^l\mathbb{Z}/p^v\mathbb{Z} \to \mathbb{Z}/p^{k-l}\mathbb{Z}, \quad p^l x + p^v\mathbb{Z} \mapsto x + p^{k-l}\mathbb{Z} \quad (x \in \mathbb{Z})$$

が定まる. $\ker \pi_k = p^k\mathbb{Z}/p^v\mathbb{Z}$ であり, 同型

$$\frac{p^l\mathbb{Z}/p^v\mathbb{Z}}{p^k\mathbb{Z}/p^v\mathbb{Z}} \cong \mathbb{Z}/p^{k-l}\mathbb{Z}$$

が成り立つ. 特に, π_v は同型写像であり, 同型

$$p^l\mathbb{Z}/p^v\mathbb{Z} \cong \mathbb{Z}/p^{v-l}\mathbb{Z}$$

が成り立つ.

[証明] $0 \leq l < k \leq v$ のとき, 写像

$$\pi_k : p^l\mathbb{Z}/p^v\mathbb{Z} \to \mathbb{Z}/p^{k-l}\mathbb{Z}, \quad p^l x + p^v\mathbb{Z} \mapsto x + p^{k-l}\mathbb{Z} \quad (x \in \mathbb{Z})$$

を考える. 任意の $x, y \in \mathbb{Z}$ に対して

$$p^l x \equiv p^l y \pmod{p^v} \Rightarrow x \equiv y \pmod{p^{v-l}} \Rightarrow x \equiv y \pmod{p^{k-l}}$$

なので, π_k は well-defined である. 全射準同型であることはすぐにわかる. また,

$$\ker \pi_k = \{p^l x + p^v\mathbb{Z} \mid x \in p^{k-l}\mathbb{Z}\} = \{x + p^v\mathbb{Z} \mid x \in p^k\mathbb{Z}\} = p^k\mathbb{Z}/p^v\mathbb{Z}$$

である. 準同型定理により

$$\frac{p^l\mathbb{Z}/p^v\mathbb{Z}}{p^k\mathbb{Z}/p^v\mathbb{Z}} \cong \mathbb{Z}/p^{k-l}\mathbb{Z}$$

が成り立つ.

特に, 全射準同型 $\pi_v : p^l\mathbb{Z}/p^v\mathbb{Z} \to \mathbb{Z}/p^{v-l}\mathbb{Z}$ は, $\ker \pi_v = 0$ であることから単射, したがって同型である. □

[定理 4.6] p を素数, v を正の整数とする. また, m を正の整数とし, ある負でない整数 k と正の整数 m_1 が存在して

$$m = p^k m_1, \quad \gcd(p, m_1) = 1$$

と表されているものとする. さらに, $k \leq v$ である仮定とする. このとき,

$$m \cdot \mathbb{Z}/p^v\mathbb{Z} = p^k\mathbb{Z}/p^v\mathbb{Z}.$$

が成り立つ.

[証明] まず,

$$p^k\mathbb{Z}/p^v\mathbb{Z} = \{x + p^v\mathbb{Z} \mid x \in p^k\mathbb{Z}\},$$
$$m \cdot \mathbb{Z}/p^v\mathbb{Z} = \{mx + p^v\mathbb{Z} \mid x \in \mathbb{Z}\}$$

はともに $\mathbb{Z}/p^v\mathbb{Z}$ の部分群である. $m = p^k m_1$ より, 任意の $x \in \mathbb{Z}$ に対して

$$mx + p^v\mathbb{Z} = p^k(m_1 x) + p^v\mathbb{Z} \in p^k\mathbb{Z}/p^v\mathbb{Z}.$$

ゆえに $m \cdot \mathbb{Z}/p^v\mathbb{Z} \subseteq p^k\mathbb{Z}/p^v\mathbb{Z}$.

逆に, $\gcd(m_1, p) = 1$ より, 任意の $a \in \mathbb{Z}$ に対して, 1 次合同式

$$m_1 x \equiv a \pmod{p^v}$$

は p^v を法としてただ 1 つの解 $x \equiv x_0 \pmod{p^v}$ をもつ. すなわち

$$a + p^v\mathbb{Z} = m_1 x_0 + p^v\mathbb{Z}.$$

したがって,

$$p^k a + p^v\mathbb{Z} = m x_0 + p^v\mathbb{Z}.$$

ゆえに $p^k\mathbb{Z}/p^v\mathbb{Z} \subseteq m \cdot \mathbb{Z}/p^v\mathbb{Z}$. □

[定理 4.7] p を素数, v を正の整数とする. また, m, n を正の整数とし, ある負でない整数 k, l と正の整数 m_1, n_1 が存在して

$$\begin{aligned} m &= p^k m_1, & \gcd(p, m_1) &= 1, \\ n &= p^l n_1, & \gcd(p, n_1) &= 1 \end{aligned}$$

と表されているものとする. さらに, $l \leq k$ である仮定とする. このとき,

$$\frac{n \cdot \mathbb{Z}/p^v\mathbb{Z}}{m \cdot \mathbb{Z}/p^v\mathbb{Z}} \cong \begin{cases} 0, & k = l \text{ または } v \leq l \text{ のとき} \\ \mathbb{Z}/p^{k-l}\mathbb{Z}, & l < k \leq v \text{ のとき} \\ \mathbb{Z}/p^{v-l}\mathbb{Z}, & l < v < k \text{ のとき} \end{cases} \tag{1}$$

が成り立つ.

[証明] 定理 4.6 より,

$$\begin{aligned} n \cdot \mathbb{Z}/p^v\mathbb{Z} &= p^l\mathbb{Z}/p^v\mathbb{Z}, \\ m \cdot \mathbb{Z}/p^v\mathbb{Z} &= p^k\mathbb{Z}/p^v\mathbb{Z} \end{aligned}$$

が成り立つ.

$k = l$ のとき, $n \cdot \mathbb{Z}/p^v\mathbb{Z} = m \cdot \mathbb{Z}/p^v\mathbb{Z}$ がいえるので, (1) の最初の同型が得られる.

$v \leq l$ のとき, $l \leq k$ という仮定から $v \leq k$ である. よって,

$$n \cdot \mathbb{Z}/p^v\mathbb{Z} = m \cdot \mathbb{Z}/p^v\mathbb{Z} = 0.$$

したがって (1) の最初の同型が成り立つ.

$l < k \leq v$ のとき, 定理 4.5 より同型

$$\frac{p^l\mathbb{Z}/p^v\mathbb{Z}}{p^k\mathbb{Z}/p^v\mathbb{Z}} \cong \mathbb{Z}/p^{k-l}\mathbb{Z}$$

が成り立つ. よって, (1) の 2 番目の同型が得られる.

$l < v < k$ のとき, $m \cdot \mathbb{Z}/p^v\mathbb{Z} = 0$ であるから

$$\frac{n \cdot \mathbb{Z}/p^v\mathbb{Z}}{m \cdot \mathbb{Z}/p^v\mathbb{Z}} \cong n \cdot \mathbb{Z}/p^v\mathbb{Z} = p^l\mathbb{Z}/p^v\mathbb{Z}.$$

定理 4.6 より, $p^l\mathbb{Z}/p^v\mathbb{Z} \cong \mathbb{Z}/p^{v-l}\mathbb{Z}$. ゆえに, (1) の 3 番目の同型が得られる.

□

[定理 4.8] m, n が互いに素な整数であるとき, 写像

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

は群の同型写像である.

[証明] m, n が互いに素であるとする. 写像

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z},\, x + n\mathbb{Z})$$

を考える. 任意の x, $y \in \mathbb{Z}$ に対して

$$x \equiv y \pmod{mn} \Rightarrow x \equiv y \pmod{m} \text{ かつ } x \equiv y \pmod{n}$$

だから, 写像 f は well-defined である. また, 準同型性を確かめることも容易である. $\gcd(m, n) = 1$ より, x が m の倍数かつ n の倍数ならば, x は mn の倍数である. これは f が単射であることを意味する. さらに, 位数を比較すれば, 全射性もいえる. □

[注意 4.9] m, n が互いに素な整数でないときには, $\mathbb{Z}/mn\mathbb{Z}$ と $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ とは決して同型にはならない.

実際, d を m, n の最大公約数とし, $d > 1$ と仮定する.

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

を準同型写像とすると, 加法群 $\mathbb{Z}/mn\mathbb{Z}$ は $1+mn\mathbb{Z}$ を生成元とする巡回群なので, $f(\mathbb{Z}/mn\mathbb{Z})$ は $f(1+mn\mathbb{Z})$ を生成元とする巡回群である. 一方, $f(1+mn\mathbb{Z})$ の位数は $l=mn/d$ 以下である. なぜなら,

$$f(1+mn\mathbb{Z}) = (x+m\mathbb{Z},\, y+n\mathbb{Z})$$

とおくと

$$\begin{aligned} l\cdot f(1+mn\mathbb{Z}) &= (lx+m\mathbb{Z},\, ly+n\mathbb{Z}) \\ &= \left(m\cdot\frac{nx}{d}+m\mathbb{Z},\, n\cdot\frac{my}{d}+n\mathbb{Z}\right) \\ &= 0 \end{aligned}$$

となるからである. $d>1$ と仮定したから $l<mn$. したがって

$$f(\mathbb{Z}/mn\mathbb{Z}) \neq \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$$

となり, f は全射ではない.

[定理 4.10] 加法群 $\mathbb{Z}$ の生成元は $1,\,-1$ のみである.

[証明] 定理 2.11 を適用すればよい. □

[定理 4.11] 加法群 $\mathbb{Z}/n\mathbb{Z}$ の元のうち，生成元になるのは

$$k+n\mathbb{Z},\quad k\in\mathbb{Z},\quad 0\leq k\leq n-1,\quad \gcd(k,n)=1$$

なる形の元であり，それらは $\varphi(n)$ 個ある.

[証明] 系 2.13 を適用すればよい. □

[定理 4.12] 加法群 $\mathbb{Z}$ の任意の自己準同型 f に対して, ある整数 a が存在して, 任意の $n\in\mathbb{Z}$ に対して

$$f(n)=an$$

が成り立つ. さらに, $a=0$ ならば f は零写像であり, $a\neq 0$ ならば f は単射である.

[証明] $a = f(1)$ とおく. $n > 0$ のとき

$$f(n) = an \Rightarrow f(n+1) = f(n) + f(1) = an + n = a(n+1).$$

数学的帰納法により, すべての $n > 0$ について $f(n) = an$ がいえる.

$n < 0$ のとき, $-n > 0$ だから

$$f(n) = -f(-n) = -(a(-n)) = an.$$

$n = 0$ のとき, f は準同型だから, $f(0) = 0$ である.

以上より, すべての n に対して $f(n) = an$ がいえた.

さらに, $a = 0$ ならば, すべての整数 n に対して $f(n) = 0$. よって f は零写像である. $a \neq 0$ ならば

$$f(n) = 0 \Rightarrow an = 0 \Rightarrow n = 0$$

なので, $\ker f = \{0\}$. ゆえに f は単射である. □

[定理 4.13] n を正の整数とし, 加法群 $\mathbb{Z}/n\mathbb{Z}$ の任意の自己準同型 f に対して, ある整数 a が存在して, $0 \leq a \leq n-1$ かつ任意の $k \in \mathbb{Z}$ に対して

$$f(k + n\mathbb{Z}) = ak + n\mathbb{Z}$$

が成り立つ.

[証明] $f(1 + n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$ なので, ある整数 a が存在して,

$$f(1 + n\mathbb{Z}) = a + n\mathbb{Z}, \quad 0 \leq a \leq n-1.$$

このとき, 任意の $k \in \mathbb{Z}$ に対して,

$$f(k + n\mathbb{Z}) = k \cdot f(1 + n\mathbb{Z}) = k \cdot (a + n\mathbb{Z}) = ak + n\mathbb{Z}$$

となる. □