平成15年度 卒業論文

m を法とする既約剰余類群の指数を与えた時の m の上限について

広島大学 理学部 数学科
学生番号 1271021C
小林 智一

平成16 年 2 月 10 日

目 次

1　序文

p を素数とする。p 進整数環 $\mathbf{Z}_p$ の (積に関する) 可逆元全体の群を U と表し、$U_n := 1 + p^n\mathbf{Z}_p$ $(n \geq 1)$ とおく。このとき、U_n は U の正規部分群となり、剰余群 U/U_n を考えることができる。U/U_n の群構造については、「 $U/U_n \cong U_1/U_n \times \mathbf{F}_p^{\times}$, $(\mathbf{Z}/p^n)^{\times} \cong U/U_n$ 」が成り立つ。さらに U_1/U_n については、$p \neq 2, n \geq 1$ のとき、「 $U_1/U_n \cong \mathbf{Z}/p^{n-1}$ 」が成り立ち、$p = 2, n \geq 2$ のとき、「 $U_1/U_n \cong \mathbf{Z}/2^{n-2} \times \mathbf{Z}/2$ 」が成り立つ。

これらの結果を利用すると、$p \neq 2, n \neq 1$ のとき、$(\mathbf{Z}/p^n)^{\times}$ は可約であることが分かる。さらに、2 以上の任意の整数 m に対して m を素因数分解することで、m を法とする既約剰余類群 $(\mathbf{Z}/m)^{\times}$ の群構造が分かる。

本論文では、$2, 3, 4$ 節で上に挙げた関係式を導出し、5 節で $(\mathbf{Z}/m)^{\times}$ の群構造を考察する。その際、「 $(\mathbf{Z}/m)^{\times}$ が巡回群になるための m の必要十分条件 」と「 $(\mathbf{Z}/m)^{\times}$ の指数 (元の最大位数) 」の 2 つについて考えた。そして $6, 7$ 節では、指数に着目し、新しい問題として「$(\mathbf{Z}/m)^{\times}$ の指数 n を与えた時の m の上限」について考えた。

最後になりますが、本論文を書くにあたって指導教官である松本眞先生には多くの助言をいただき、大変お世話になりました。また、榎本彦衛先生にもアドバイスをいただきました。この場を借りて厚く御礼申しあげたいです。

2　定義と準備

この節では環 $\mathbf{Z}_p$ の定義と $\mathbf{Z}_p$ の性質についてみていく。

2.1　定義

p を素数とする。任意の自然数 $n \geq 1$ に対し $A_n = \mathbf{Z}/p^n\mathbf{Z}$ とおく。A_n は p^n を法とする $\mathbf{Z}$ の剰余環である。$x, x' \in \mathbf{Z}$, $x \equiv x' \pmod{p^n} \Rightarrow x \equiv x' \pmod{p^{n-1}}$ だから自然な仕方で環準同型

$$\varphi_n : A_n \longrightarrow A_{n-1}$$

が得られる。(すなわち、標準的射影 $\pi_n : \mathbf{Z} \twoheadrightarrow A_n$ の元を $x \mapsto x_n$ と表したとき、φ_n は $\varphi_n(x_n) := x_{n-1}$ によって定義される写像である。) π_{n-1} は

全射より φ_n は全射である。また φ_n の核は $p^{n-1}A_n$ である。

よって環準同型の列：

$$\cdots \longrightarrow A_n \longrightarrow A_{n-1} \longrightarrow \cdots \longrightarrow A_2 \longrightarrow A_1$$

は射影系を成す。

定義 2.1. 上に定義された系 (A_n, φ_n) の射影的極限 $(\varprojlim(A_n, \varphi_n))$ を p 進整数環と呼び $\mathbf{Z}_p$ と表す。

定義より

$$\varprojlim(A_n, \varphi_n) = \{(\cdots, x_n, \cdots, x_1) \in \prod_{n=1}^{\infty} A_n \mid \varphi_n(x_n) = x_{n-1}(n \geq 2)\}$$

である。

注意． $\mathbf{Z}_p$ の元 $x = (\cdots, x_n, \cdots, x_1), y = (\cdots, y_n, \cdots, y_1)$ に対して以下のような二つの演算を考える。

$$x + y := (\cdots, x_n + y_n, \cdots, x_1 + y_1) \tag{1}$$

$$xy := (\cdots, x_n y_n, \cdots, x_1 y_1) \tag{2}$$

$\varphi_n(x_n + y_n) = \varphi_n(x_n) + \varphi_n(y_n) = x_{n-1} + y_{n-1}$ より $x + y \in \mathbf{Z}_p$ である。一方、$\varphi_n(x_n y_n) = \varphi_n(x_n)\varphi_n(y_n) = x_{n-1}y_{n-1}$ より $xy \in \mathbf{Z}_p$ である。よって上で定義した二つの演算により $\mathbf{Z}_p$ に和 (1)、積 (2) が定義できる。

注意． 上の 2 つの演算に関し、$\mathbf{Z}_p$ は可換環になっている。特に加法逆元については、$x = (x_n) \in \mathbf{Z}_p$ に対して、$x' := (-x_n)$ とおけば $-x = x'$ である。($x + x' = x' + x = 0$ は明らか。また $\varphi_n(-x_n) = -\varphi_n(x_n) = -x_{n-1}$ より $x' \in \mathbf{Z}_p$ が言える。)

命題 2.2. $\mathbf{Z}$ は $\mathbf{Z}_p$ の部分環である。

proof. $x \in \mathbf{Z}$ とすれば、$\varphi_n(\pi_n(x)) = \pi_{n-1}(x)$ だから π を以下のように定める。

$$\pi : \mathbf{Z} \longrightarrow \mathbf{Z}_p, x \longmapsto (\cdots, \pi_n(x), \cdots, \pi_1(x))$$

$$\pi(x + y) = (\pi_n(x + y)) = (\pi_n(x) + \pi_n(y)) = \pi(x) + \pi(y)$$
$$\pi(xy) = (\pi_n(xy)) = (\pi_n(x)\pi_n(y)) = \pi(x)\pi(y)$$
$$\pi(1) = (\pi_n(1)) = 1$$

より π は環準同型。また、

$$\begin{aligned}\ker\pi &= \{x \in \mathbf{Z} \mid (\pi_n(x)) = (0)\} \\ &= \{x \in \mathbf{Z} \mid x \in \bigcap_{n=1}^{\infty} \ker\pi_n\} \\ &= \{x \in \mathbf{Z} \mid x \in p^n\mathbf{Z}, \forall n \geq 1\} \\ &= 0\end{aligned}$$

よって π は単射。ゆえ $\mathbf{Z} \cong \pi(\mathbf{Z}) \subset \mathbf{Z}_p$ より $\mathbf{Z}$ は $\mathbf{Z}_p$ の部分環とみなせる。

□

2.2 $\mathbf{Z}_p$の性質

$\epsilon_n : \mathbf{Z}_p \to A_n$ を、$\mathbf{Z}_p$ の元 $x = (\cdots, x_n, \cdots, x_1)$ に第 n 成分 $x_n \in A_n$ を対応させる写像とする。

命題 2.3.

$$0 \longrightarrow \mathbf{Z}_p \xrightarrow{p^n} \mathbf{Z}_p \xrightarrow{\epsilon_n} A_n \longrightarrow 0$$

は完全系列である。

proof. pによる乗法$p : \mathbf{Z}_p \to \mathbf{Z}_p, x \mapsto px$が単射であることを示す。$\ker p = \{0\}$ を示せばよい。$\forall x \in \ker p$ をとる。$px = 0$ より $\forall n \geq 1$ に対して $px_{n+1} = 0$ である。ゆえに $x_{n+1} = p^n y_{n+1}$ となる $y_{n+1} \in A_{n+1}$ がある。$\varphi_{n+1}(x_{n+1}) = x_n$, $\varphi_{n+1}(p^n y_{n+1}) = 0$ だから $\forall n \geq 1, x_n = 0$ となる。よって $x = 0$ となり、$\ker p \subset \{0\}$ が示された。$\ker p \supset \{0\}$ は明らか。ゆえに $\ker p = \{0\}$ が言えた。p による乗法が単射だから、その合成である p^n による乗法も単射である。

$\ker\epsilon_n = p^n\mathbf{Z}_p$ を示す。
$(\supset)$ を示す。
$\forall x = (x_m) \in p^n\mathbf{Z}_p$ をとる。$x = p^n y$ $(y = (y_m) \in \mathbf{Z}_p)$ と書けるので、$\epsilon_n(x) = p^n y_n = 0$ となり $x \in \ker\epsilon_n$ が言えた。
$(\subset)$ を示す。
$\forall x = (x_m) \in \ker\epsilon_n$ をとる。$x_n = 0$ より $\mathbf{Z}_p$ の定義から $\forall m < n, x_m = 0$ を得る。一方、$\forall m \geq n+1$ に対しては $x_m \equiv 0 \pmod{p^n}$ である。さて $x_m = p^n z_m$ $(z_m \in A_m)$ と書けるが、ここで $y_{m-n} :=$ [z_mの A_{m-n}における像] と

とり、$y := (y_k)$ $(k = m - n)$ とおく。x が $\mathbf{Z}_p$ の元であることと y_k の取り方から y は $\mathbf{Z}_p$ の元である。さらに、$z_m \equiv y_m \pmod{p^{m-n}}$ より $p^n z_m = p^n y_m$ が成り立つ。よって $x_m = p^n y_m$ を得る。従って、

$$\begin{aligned} p^n y &= (\quad \cdots, \quad p^n y_{n+2}, \quad p^n y_{n+1}, \quad p^n y_n, \quad p^n y_{n-1}, \quad \cdots, \quad p^n y_1) \\ &= (\quad \cdots, \quad p^n y_{n+2}, \quad p^n y_{n+1}, \quad 0, \quad 0, \quad \cdots, \quad 0) \\ &= (\quad \cdots, \quad x_{n+2}, \quad x_{n+1}, \quad x_n, \quad x_{n-1}, \quad \cdots, \quad x_1) \\ &= x \end{aligned}$$

ゆえに、$x \in p^n \mathbf{Z}_p$ が言えた。

明らかに ϵ_n は全射である。

□

注意． 命題 2.3 で示された $\ker \epsilon_n = p^n \mathbf{Z}_p$ より

$$\{x = (x_n) \in \mathbf{Z}_p \mid x_n = 0\} = p^n \mathbf{Z}_p \tag{3}$$

である。

命題 2.4. $\mathbf{Z}_p$（または A_n）の元 x が（積に関して）可逆であるための必要十分条件は x が p の倍数とは異なることである。

proof.

- A_n の場合

  x を A_n の可逆元とすると、$xy = yx = 1$ なる $y \in A_n$ が存在する。$\varphi := \varphi_2 \circ \cdots \circ \varphi_n$ とおけば、$\varphi : A_n \to A_1$ を定め、明らかに φ は全射準同型である。特に、$A_1 (= \mathbf{F}_p)$ は体である。$\varphi(xy) = \varphi(x)\varphi(y), \varphi(1) = 1$ より $\varphi(x)\varphi(y) = 1$ だが、もし x が p の倍数であれば、$\varphi(x) = 0$ となり $0 = 1$ となって A_1 が体であることに矛盾する。よって A_n の元 x が可逆ならば x は p の倍数ではない。

  逆に、A_n の元 x が p の倍数でないとすると、$\varphi(x) \neq 0$ である。A_1 は体より $y'\varphi(x) = 1$ なる $y' \in A_1$ が存在する。φ は全射ゆえ $\varphi(y) = y'$ なる $y \in A_n$ が存在する。よって $\varphi(xy) = 1$ となる。ゆえに $xy + pz = 1$ となる $z \in A_n$ が存在する。従って、$xy(1 + pz + \cdots + p^{n-1}z^{n-1}) = 1 - p^n z^n = 1$ だから x は A_n の可逆元である。(逆元 $y(1 + pz + \cdots + p^{n-1}z^{n-1})$ がある。)

- $\mathbf{Z}_p$ の場合

  「$x=(x_n)\in\mathbf{Z}_p$ が可逆 $\Leftrightarrow\forall n\geq 1, x_n\in A_n$ が可逆」を示す。

  ($\Rightarrow$) を示す。

  $x\in\mathbf{Z}_p$ が可逆より、$xy=yx=1$ なる $y=(y_n)\in\mathbf{Z}_p$ が存在する。ゆえ $\forall n\geq 1$ に対して $x_ny_n=y_nx_n=1$ だから $\forall n\geq 1, x_n\in A_n$ は可逆である。

  ($\Leftarrow$) を示す。

  $\forall n\geq 1, x_n\in A_n$ は可逆より、$x_n^{-1}\in A_n$ が存在する。$x':=(x_n^{-1})\in\prod_{n=1}^{\infty}A_n$ とおくと、$xx'=x'x=1$ だからあとは $x'\in\mathbf{Z}_p$ を言えばよい。$\forall n\geq 2$ に対し φ_n は積に関しモノイド準同型なので、$\varphi_n(x_n^{-1})=\varphi_n(x_n)^{-1}=x_{n-1}^{-1}$ となる。ゆえに $x'\in\mathbf{Z}_p$ が言えた。よって $x=(x_n)\in\mathbf{Z}_p$ は可逆である。

  以上のことから

$$\begin{aligned} x=(x_n)\in\mathbf{Z}_p\text{が可逆} &\Leftrightarrow \forall n\geq 1, x_n\in A_n\text{は可逆}\\ &\Leftrightarrow \forall n\geq 1, x_n\in A_n \text{ は } p \text{ の倍数でない}\\ &\Leftrightarrow x_1\neq 0\\ &\Leftrightarrow x=(x_n)\notin p\mathbf{Z}_p\ (\because (3)) \end{aligned}$$

□

命題 2.5. $\mathbf{Z}_p$ の可逆元全体からなる群を U と表せば、$\mathbf{Z}_p$ の零とは異なる任意の元 x に対して一意的に $u\in U, n\geq 0$ が存在し、$x=p^nu$ と書ける。(U の元は p 進単数と呼ばれる。)

proof. $x\in\mathbf{Z}_p, x\neq 0$ ならば $\epsilon_m(x)=0$ を成り立たせる m の最大元 n がある。$x_n=0$ だから (3) より $x=p^nu$ $(u\in\mathbf{Z}_p)$ と書ける。このとき、もし u が p の倍数だとすると、$u=pu'$ $(u'\in\mathbf{Z}_p)$ と書けるので $x=p^{n+1}u'$ である。ところが $\epsilon_{n+1}(x)=\epsilon_{n+1}(p^{n+1}u')=0$ となり n の最大性に反する。従って、u は p の倍数ではないので U の元である。

また、x が $p^nu, p^{n'}u'$ $(n,n'\geq 0, u,u'\in U)$ と 2 通りに表されたとする。$n>n'$ とする。$p^nu=p^{n'}u'$ ゆえ $p^n=p^{n'}u'u^{-1}$ となる。$p^{n'}$ による乗法は単射だから $p^{n-n'}=u'u^{-1}$ が得られ、$p^{n-n'}\notin U$, $u'u^{-1}\in U$ だから矛盾する。一方 $n<n'$ とすると同様にして $p^{n'-n}=uu'^{-1}$ が得られ、矛盾する。

ゆえに $n = n'$ である。従って $p^n u = p^n u'$ となるが p^n による乗法は単射なので $u = u'$ を得る。

□

定義 2.6. x を $\mathbf{Z}_p$ の 0 とは異なる元とし、$x = p^n u$ と表す。整数 n は x の p 進付値と呼び、$v_p(x)$ と記す。

注意 . $v_p(0) = +\infty$ とおく。

命題 2.7. $x, y \in \mathbf{Z}_p, v_p(xy) = v_p(x) + v_p(y)$ が成り立つ。

proof.

- $x, y \neq 0$ のとき

  $x = p^{n_1}u_1, y = p^{n_2}u_2 (n_1, n_2 \geq 0, u_1, u_2 \in U)$ と一意に書ける。よって定義より $v_p(x) = n_1, v_p(y) = n_2$ である。一方、$xy = p^{n_1+n_2}u_1u_2$ で $u_1u_2 \in U$ だから $v_p(xy) = n_1 + n_2$ である。ゆえに $v_p(xy) = v_p(x) + v_p(y)$ が成り立つ。

- x または y が 0 のとき

  $v_p(xy) = v_p(0) = +\infty$, $v_p(x) + v_p(y) = +\infty$ より $v_p(xy) = v_p(x) + v_p(y)$ が成り立つ。

□

系 2.8. $\mathbf{Z}_p$ は整域である。

proof. $x, y \in \mathbf{Z}_p, xy = 0$ とする。$v_p(x) + v_p(y) = v_p(xy) = +\infty$ ゆえ $v_p(x) = +\infty$ または $v_p(y) = +\infty$ である。よって $x = 0$ または $y = 0$ となる。

□

3 単数群のフィルター付け

$U = \mathbf{Z}_p^\times$ を p 進単数群とする。

命題 3.1. 任意の $n \geq 1$ に対して $U_n := 1 + p^n\mathbf{Z}_p$ とおく。

1. $\forall z \in U_n$ に対して、z の表し方は一意である。

2. U_n は準同型 $\epsilon_n|_U : U \longrightarrow (\mathbf{Z}/p^n)^\times$ の核である。

3. $U/U_1 \cong \mathbf{F}_p^\times$

4. $U_n/U_{n+1} \cong \mathbf{Z}/p$,

$\sharp(U_1/U_n) = p^{n-1}$ (ただし $n \geq 1$) , $\sharp(U_2/U_n) = p^{n-2}$ (ただし $n \geq 2$)

1 を示す

proof. $z \in U_n$ が $1 + p^n x$, $1 + p^n y$ $(x, y \in \mathbf{Z}_p)$ と 2 通りに表されたとすると、$1 + p^n x = 1 + p^n y$ より $p^n(x - y) = 0$ が成り立つ。$\mathbf{Z}_p$ は整域であり、$p^n \neq 0$ より $x - y = 0$ である。ゆえ $x = y$ を得る。

□

2 を示す

proof. $\epsilon_n : \mathbf{Z}_p \to A_n$ は環の全射準同型である。ゆえに乗法に関してはモノイド準同型だから $\epsilon_n((\mathbf{Z}_p)^\times) \subset A_n^\times$ である。よって ϵ_n の U による制限写像 $\epsilon_n|_U : U \to A_n^\times$ が定まる。ϵ_n は全射ゆえ $\forall x_n \in A_n^\times$ について $\epsilon_n(x) = x_n$ なる $x = (x_m) \in \mathbf{Z}_p$ が存在する。$x_n \in A_n^\times \Rightarrow x_1 \neq 0 \Rightarrow \forall m \geq 1, x_m \in A_m^\times \Rightarrow x = (x_m) \in \mathbf{Z}_p^\times (= U)$ より、$\epsilon_n|_U$ は全射である。

$\ker \epsilon_n|_U = U_n$ を示す。
$(\supset)$ を示す。
$\forall x \in U_n$ をとる。$x = 1 + p^n y$ $(y = (y_m) \in \mathbf{Z}_p)$ と書ける。$\epsilon_n|_U(x) = 1 + p^n y_n = 1$ より $x \in \ker \epsilon_n|_U$ が言えた。
$(\subset)$ を示す。
$\forall x = (x_m) \in \ker \epsilon_n|_U$ をとると、$x_n = 1$ である。さて、$x, 1 \in \mathbf{Z}_p$ より $x - 1 \in \mathbf{Z}_p$ で、$\epsilon_n(x-1) = x_n - 1 = 0$ だから (3) より $x - 1 = p^n y$ $(y \in \mathbf{Z}_p)$ と書ける。$x = 1 + p^n y$ $(y \in \mathbf{Z}_p)$ より $x \in U_n$ が言えた。

□

3 を示す

proof. $\epsilon_n|_U : U \to A_n^\times$ は全射準同型。2 より $\ker \epsilon_n|_U = U_n$ だから $U_n \triangleleft U$ である。$\epsilon_n|_U$ に群準同型定理を適用すると、$U/U_n \cong A_n^\times$ より、

$$U/U_n \cong (\mathbf{Z}/p^n)^\times \tag{4}$$

を得る。特に $n = 1$ とすると、

$$U/U_1 \cong (\mathbf{Z}/p)^\times = \mathbf{F}_p^\times \tag{5}$$

を得る。

□

4 を示す。

proof. 1 より U_n の任意の元 z に対して、$\mathbf{Z}_p$ の元 x が唯一つ定まる。従って τ を以下のように定める。

$$\tau : U_n \longrightarrow \mathbf{Z}_p, z(= 1 + p^n x) \longmapsto x$$

さて ϕ を以下で定める。

$$\phi : U_n \xrightarrow{\tau} \mathbf{Z}_p \xrightarrow{\epsilon_1} A_1, z \longmapsto x \longmapsto x_1 = (x \pmod p)$$

$n \geq 1$ のとき

$$\begin{aligned}
\phi((1 + p^n x)(1 + p^n y)) &= \phi(1 + p^n(x + y) + p^{2n} xy) \\
&= \phi(1 + p^n(x + y + p(p^{n-1} xy))) \\
&= x + y + p(p^{n-1} xy) \pmod p \\
&= x + y \pmod p \\
&= x \pmod p + y \pmod p \\
&= \phi(1 + p^n x) + \phi(1 + p^n y)
\end{aligned}$$

より ϕ は準同型。

次に、$\ker \phi = U_{n+1}$ を示す。

($\supset$) を示す。

$\forall z \in U_{n+1}$ をとる。$z = 1 + p^{n+1} x$ $(x \in \mathbf{Z}_p)$ と書ける。$\phi(z) = \phi(1 + p^n(px)) = px \pmod p = 0$ より $z \in \ker \phi$ が言えた。

($\subset$) を示す。

$\forall z \in \ker \phi$ をとる。$z = 1 + p^n x$ $(x \in \mathbf{Z}_p)$ と書けるが、$x_1 = x \pmod p = 0$ だから (3) より $x = py$ $(y \in \mathbf{Z}_p)$ と書ける。よって

$$\begin{aligned}
z &= 1 + p^n x \\
&= 1 + p^{n+1} y \quad (y \in \mathbf{Z}_p)
\end{aligned}$$

となるので $z \in U_{n+1}$ が言えた。

従って $\forall n \geq 1$ について $U_{n+1} \triangleleft U_n$ である。また、明らかに ϕ は全射。よって ϕ に群準同型定理を適用すると、$U_n/U_{n+1} \cong A_1$ より、

$$\sharp(U_n/U_{n+1}) = p$$

を得る。これとラグランジュの定理より、$n \geq 1$ のとき

$$\begin{aligned} \sharp(U_1/U_n) &= \sharp(U_1/U_2)\sharp(U_2/U_3)\cdots\sharp(U_{n-1}/U_n) \\ &= p^{n-1} \end{aligned} \tag{6}$$

同様に、$n \geq 2$ のとき

$$\begin{aligned} \sharp(U_2/U_n) &= \sharp(U_2/U_3)\cdots\sharp(U_{n-1}/U_n) \\ &= p^{n-2} \end{aligned} \tag{7}$$

を得る。

□

補題 3.2.

$$0 \xrightarrow{\psi 1} A \xrightarrow{\psi_2} E \xrightarrow{\psi_3} B \xrightarrow{\psi_4} 0$$

を有限加法群の完全系列とし A, B の位数 a, b は互いに素であるとする。B' を $x \in E$ で $bx = 0$ を満たすものの全体からなる E の部分集合とし A を E の部分群と見なすと、E は A と B' の直和であり、しかも B' は E の部分群で B と同型であるような唯一のものである。

proof.

- B' が E の部分群になること

  ψ_b を以下のように定める。

  $$\psi_b : E \longrightarrow E, \ \ x \longmapsto bx$$

  $\psi_b(x+y) = b(x+y) = bx + by = \psi_b(x) + \psi_b(y)$ より、ψ_b は準同型。$\ker \psi_b = \{x \in E \mid bx = 0\}$ より $\ker \psi_b = B'$ である。よって B' は E の (正規) 部分群である。

- $E = A \oplus B'$ であること

  $(A \cap B' = \{0\}$ であること$)$

  もし、$x \in A \cap B'$ ならば、$x \in A$ より $ax = 0$ $(\because \sharp(A) = a)$ である。また $x \in B'$ より $bx = 0$ $(\because B'$ の定義$)$ である。仮定より a, b は互いに素であるが、$\gcd(a, b) = 1 \Leftrightarrow \exists r, \exists s \in \mathbf{Z}$ s.t. $ar + bs = 1$ に注意すると、$x = 1 \cdot x = (ar + bs)x = (ar)x + (bs)x = r(ax) + s(bx) = 0$ となる。よって、$A \cap B' \subset \{0\}$ が示された。$A \cap B' \supset \{0\}$ は明らか。ゆえに $A \cap B' = \{0\}$ が言えた。

  $(E = A + B'$ であること$)$

  $E \supset A + B'$ は自明なので、$\subset$ を示す。
  $\forall x \in E$ をとると、 $x = 1 \cdot x = arx + bsx$ と書ける。以下、$bsx \in A$, $arx \in B'$ を示す。$\forall y \in bE$ をとる。 $y = be$ $(e \in E)$ と書ける。$\psi_3(y) = \psi_3(be) = b\psi_3(e)$, $\psi_3(e) \in B$ より $\psi_3(y) = 0$ である。よって、$y \in \ker \psi_3$ だが $\ker \psi_3 = \mathrm{Im}\psi_2 = \psi_2(A) \cong A$ $(\because \psi_2$ は単射$)$ より $y \in A$ である。従って、$bE \subset A$ である。ところで、$b(sx) \in bE$ だから、$bsx \in A$ が言えた。一方、$E/\ker \psi_3 \cong \mathrm{Im}\psi_3 = B$ $(\because \psi_3$は全射$)$ より、$\sharp(B) = \sharp(E/\ker \psi_3)$ である。$\sharp(E/\ker \psi_3) = \sharp(E)/\sharp(\ker \psi_3) = \sharp(E)/\sharp(\mathrm{Im}\psi_2) = \sharp(E)/\sharp(A)$ だから $\sharp(E) = \sharp(A) \cdot \sharp(B) = ab$ を得る。従って、$abE = \{0\}$ である。ところで、$b(arx) = r(abx) = r \cdot 0 = 0$ だから、$arx \in B'$ が言えた。以上より、$E \subset A + B'$ が示された。

- B' は B と同型であるような唯一のものであること

  $\ker \psi_3|_{B'} = B' \cap \ker \psi_3 = B' \cap \mathrm{Im}\psi_2 = B' \cap A = \{0\}$ より $\psi_3|_{B'}$ は単射。一方、$E = A \oplus B'$ だから $\sharp(E) = \sharp(A) \cdot \sharp(B')$ である。$\sharp(E) = ab$ より $\sharp(B') = b$ を得る。よって、$\psi_3|_{B'} : B' \to B$ は単射で、$\sharp(B') = \sharp(B)$ だから、$\psi_3|_{B'}$ は全射である。従って、$B \cong B'$ である。また、$B'' < E, B'' \cong B$ なる B'' があったとすると、$\sharp(B'') = \sharp(B)$ だから $\sharp(B'') = b$ を得る。よって $bB'' = \{0\}$ だから、$B'' \subset B'$ となる。しかし、$\sharp(B') = b$ だから $B'' = B'$ となり一意性が言えた。

□

命題 3.3. $V_n := \{x \in U/U_n \mid x^{p-1} = 1\}$ とする。
このとき、$U/U_n = U_1/U_n \times V_n$ であり、しかも V_n は U/U_n の部分群で $\mathbf{F}_p^\times$ と同型となる唯一のものである。

proof. $U_n \subset U_1$ より図式

$$\begin{array}{ccc} U & \xrightarrow{id_U} & U \\ {\scriptstyle q_n}\downarrow & & {\scriptstyle q_1}\downarrow \\ U/U_n & \longrightarrow & U/U_1 \end{array}$$

を可換にするような 準同型 $\bar{f} : U/U_n \longrightarrow U/U_1$ が唯一つ存在する。このとき、$\bar{f}$ は $\bar{f}(uU_n) := uU_1$ $(u \in U)$ により定義される。$\bar{f} \circ q_n = q_1 \circ id_U = q_1$ で q_1 が全射だから $\bar{f}$ は全射準同型である。

$U_n \triangleleft U$ で $U_n \subset U_1, U_1 < U$ だから $U_1/U_n < U/U_n$ である。よって自然な単射準同型 $\iota : U_1/U_n \hookrightarrow U/U_n$ がある。

補題 3.2 を次の完全系列に適用すればよい。

$$1 \longrightarrow U_1/U_n \xrightarrow{\iota} U/U_n \xrightarrow{\bar{f}} U/U_1 \longrightarrow 1 \tag{8}$$

(8) が完全系列であることを示す。

$\bar{f}$ は全準同型より U/U_1 で完全。また、ι は単準同型より U_1/U_n で完全。さらに、$\ker \bar{f} = \{uU_n \mid u \in U_1\} = \mathrm{Im}(\iota)$ より U/U_n で完全。

さて、(5),(6) より $\sharp(U_1/U_n) = p^{n-1}, \sharp(U/U_1) = p-1$ で、$\gcd(p^{n-1}, p-1) = 1$ より補題 3.2 の条件は成り立つ。従って、$V_n := \{x \in U/U_n \mid x^{p-1} = 1\}$ とおくと、補題 3.2 より

$$U/U_n = U_1/U_n \times V_n \tag{9}$$

であり、しかも V_n は U/U_n の部分群であって、$\mathbf{F}_p^{\times} (\cong U/U_1)$ と同型であるような唯一のものである。

□

系 3.4. p を素数とする。

1. $\sharp((\mathbf{Z}/p^n)^{\times}) = p^{n-1}(p-1)$
2. $\sharp\{y \in (\mathbf{Z}/p^n)^{\times} \mid y^{p-1} = 1\} = p-1$

注意． 2 は $(\mathbf{Z}/p^n)^{\times}$ に $y^{p-1} = 1$ となる y がちょうど $p-1$ 個あることを意味する。

proof. (4) と (9) より

1. $\sharp((\mathbf{Z}/p^n)^\times) = \sharp(U_1/U_n)\sharp(V_n) = p^{n-1}(p-1)$
2. $\sharp\{y \in (\mathbf{Z}/p^n)^\times \mid y^{p-1} = 1\} = \sharp\{x \in U/U_n \mid x^{p-1} = 1\} = \sharp(V_n) = p-1$

□

4 群U_1の構造

補題 4.1. $x \in U_n - U_{n+1}$ とし $p \neq 2$ のとき $n \geq 1$, $p = 2$ のときは $n \geq 2$ とすると $x^p \in U_{n+1} - U_{n+2}$ である。

proof. 仮定により $x = 1 + kp^n$ (ただし、$k \in \mathbf{Z}_p^\times$)。二項定理により

$$\begin{aligned} x^p &= (1+kp^n)^p \\ &= 1 + \binom{p}{1}kp^n + \cdots + \binom{p}{r}(kp^n)^r + \cdots + (kp^n)^p \\ &= 1 + kp^{n+1} + \cdots + k^p p^{np} \end{aligned}$$

$1 \leq r \leq p-1$ とする。

$$\begin{aligned} \binom{p}{r}(kp^n)^r &= \frac{p(p-1)\cdots(p-r+1)}{r!}k^r p^{nr} \\ &= \frac{(p-1)\cdots(p-r+1)}{r!}k^r p^{nr+1} \end{aligned}$$

二項係数は整数で p は素数であることに注意する。$p \mid r!\binom{p}{r}, \gcd(p, r!) = 1$ だから $p \mid \binom{p}{r}$ となる。従って、$\frac{(p-1)\cdots(p-r+1)}{r!}$ は整数で、また p の倍数ではないので $\frac{(p-1)\cdots(p-r+1)}{r!}$ は $\mathbf{Z}_p^\times$ の元である。ゆえに $\frac{(p-1)\cdots(p-r+1)}{r!}k^r \in \mathbf{Z}_p^\times$ である。このことから $1 \leq r \leq p-1$ のとき、$v_p(\binom{p}{r}(kp^n)^r) = nr+1$ を得る。

1. $p \neq 2$ のとき
   $v_p(\binom{p}{1}kp^n) = n+1$. 一方 $n \geq 1 \Leftrightarrow 2n+1 \geq n+2$ だから $2 \leq r \leq p-1$ のとき $v_p(\binom{p}{r}(kp^n)^r) = nr+1 \geq n+2$. また $np > 2n = n+n \geq n+1$ より $v_p((kp^n)^p) = np \geq n+2$.

2. $p = 2$ のとき
   $v_p(\binom{p}{1}kp^n) = n+1$. また $n \geq 2 \Leftrightarrow 2n \geq n+2$ だから $v_p((kp^n)^p) = np \geq n+2$.

以上より $x^p \equiv 1 + kp^{n+1} \pmod{p^{n+2}}$. ゆえに $x^p \in U_{n+1} - U_{n+2}$.

□

命題 4.2. p を素数とする。

1. $p \neq 2, n \geq 1$ のとき、$U_1/U_n \cong \mathbf{Z}/p^{n-1}$
2. $p = 2, n \geq 2$ のとき、$U_2/U_n \cong \mathbf{Z}/p^{n-2}$, $U_1 = \{\pm 1\} \times U_2$

proof.

1. $p \neq 2, n \geq 1$ のとき

   $\alpha \in U_1 - U_2$ をとる。補題 4.1 より $\alpha^p \in U_2 - U_3$ である。再び補題 4.1 より $\alpha^{p^2} \in U_3 - U_4$ である。以下同様にしていくと $\alpha^{p^i} \in U_{i+1} - U_{i+2}$ を得る。自然な射影 $U_1 \twoheadrightarrow U_1/U_n$ の元を $\beta \mapsto \beta_n$ と書くことにする。$\beta_n = 1 \Leftrightarrow \beta \in U_n$ であることに注意すると、$\alpha^{p^{n-j}} \notin U_n (2 \leq j \leq n)$, $\alpha^{p^{n-1}} \in U_n$ だから

   $$(\alpha^{p^{n-j}})_n = \begin{cases} (\alpha_n)^{p^{n-j}} \neq 1 & (2 \leq j \leq n) \\ (\alpha_n)^{p^{n-1}} = 1 \end{cases} \tag{10}$$

   ラグランジュの定理より $ord(\alpha_n) \mid \sharp(U_1/U_n)$ だが、(6) と (10) より $ord(\alpha_n) = p^{n-1}$ である。さて、$< \alpha_n > \subset U_1/U_n$ だが、$\sharp(< \alpha_n >) = p^{n-1} = \sharp(U_1/U_n)$ より $< \alpha_n > = U_1/U_n$ を得る。ゆえに U_1/U_n は α_n を生成元とする位数 p^{n-1} の有限巡回群となる。したがって

   $$\mathbf{Z}/p^{n-1}\mathbf{Z} \cong U_1/U_n \tag{11}$$

   が得られる。

2. $p = 2, n \geq 2$ のとき

   $\alpha \in U_2 - U_3$ をとる。先と同様の議論から今度は $\alpha^{p^i} \in U_{i+2} - U_{i+3}$ を得る。自然な射影 $U_2 \twoheadrightarrow U_2/U_n$ の元を $\beta \mapsto \beta_n$ と書くことにする。$\beta_n = 1 \Leftrightarrow \beta \in U_n$ であることに注意すると、$\alpha^{p^{n-j}} \notin U_n (3 \leq j \leq n)$, $\alpha^{p^{n-2}} \in U_n$ だから

   $$(\alpha^{p^{n-j}})_n = \begin{cases} (\alpha_n)^{p^{n-j}} \neq 1 & (3 \leq j \leq n) \\ (\alpha_n)^{p^{n-2}} = 1 \end{cases} \tag{12}$$

ラグランジュの定理より $ord(\alpha_n) \mid \sharp(U_2/U_n)$ だが、(7) と (12) より $ord(\alpha_n) = p^{n-2}$ である。さて、$< \alpha_n > \subset U_2/U_n$ だが、$\sharp(< \alpha_n >) = p^{n-2} = ord(\alpha_n)$ より $< \alpha_n > = U_2/U_n$ を得る。ゆえに U_2/U_n は α_n を生成元とする位数 $p^{n-2}(= 2^{n-2})$ の有限巡回群となる。したがって

$$\mathbf{Z}/2^{n-2}\mathbf{Z} \cong U_2/U_n \tag{13}$$

が得られる。

次に $\{\pm 1\} \times U_2 \cong U_1$ を示す。

$\{\pm 1\}, U_2 \triangleleft U_1$ である。$p = 2$ のとき $U_1 = U$ だから ψ を以下のように定める。

$$\psi : \{\pm 1\} \times U_2 \longrightarrow U_1, (\epsilon, u) \longmapsto \varepsilon u$$

$\forall x \in U_1$ をとると $x \equiv 1$ or $-1 \pmod 4$.

(a) $x \equiv 1 \pmod 4$ のとき
$x \in U_2$ だから $(1, x) \in \{\pm 1\} \times U_2$ をとれば $1 \cdot x = x$.

(b) $x \equiv -1 \pmod 4$ のとき
$-x \equiv 1 \pmod 4$ より $-x \in U_2$ だから $(-1, -x) \in \{\pm 1\} \times U_2$ をとれば $(-1) \cdot (-x) = x$.

よって ψ は全射。

また $\{\pm 1\} \cap U_2 = \{1\}$.

以上より

$$\{\pm 1\} \times U_2 \cong U_1 \tag{14}$$

が示された。

□

5 $(\mathbf{Z}/m)^\times$ の群構造

この節では、前節までのことを利用して $(\mathbf{Z}/m)^\times$ の群構造を考える。ただし $m \geq 2$ で考える。ここで利用する最小公倍数や最大公約数については付録を参照されたい。

定義 5.1. 群 G に対し、G の元の最大位数を G の指数と呼ぶ。

補題 5.2. $r \geq 2$ とし、$G_1, \cdots, G_r$ を有限群とする。
　このとき、$G_1 \times \cdots \times G_r$ の任意の元 $(g_1, \cdots, g_r)$ に対して
$ord(g_1, \cdots, g_r) = lcm(ord(g_1), \cdots, ord(g_r))$ である。

proof.

$$\begin{aligned}(g_1, \cdots, g_r)^m = (e_1, \cdots, e_r) &\Leftrightarrow ({g_1}^m, \cdots, {g_r}^m) = (e_1, \cdots, e_r) \\ &\Leftrightarrow {g_1}^m = e_1, \cdots, {g_r}^m = e_r \\ &\Leftrightarrow ord(g_1) \mid m, \cdots, ord(g_r) \mid m \\ &\Leftrightarrow m \text{ は } ord(g_1), \cdots, ord(g_r) \text{ の公倍数}\end{aligned}$$

さて、$ord(g_1, \cdots, g_r) := \min\{m \in \mathbf{N} \mid (g_1, \cdots, g_r)^m = (e_1, \cdots, e_r)\}$ より
$ord(g_1, \cdots, g_r) = lcm(ord(g_1), \cdots, ord(g_r))$ を得る。

□

補題 5.3. $r \geq 2$ とする。
　$\mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$ の指数は $lcm(n_1, \cdots, n_r)$ である。

proof. $\forall (x_1, \cdots, x_r) \in \mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$ をとる。ラグランジュの定理より $ord(x_1) \mid n_1, \cdots, ord(x_r) \mid n_r$ だから

$$lcm(ord(x_1), \cdots, ord(x_r)) \mid lcm(n_1, \cdots, n_r)$$

となる。従って、

$$\begin{aligned}ord(x_1, \cdots, x_r) &= lcm(ord(x_1), \cdots, ord(x_r)) \\ &\leq lcm(n_1, \cdots, n_r)\end{aligned}$$

を得る。一方、$\mathbf{Z}/n_i$ の生成元を a_i とすると $ord(a_1, \cdots, a_r) = lcm(n_1, \cdots, n_r)$
だから指数は $lcm(n_1, \cdots, n_r)$ である。

□

補題 5.4. $\mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$ が巡回群であるための必要十分条件は、
$n_1, \cdots, n_r$ が *pairwise* に互いに素であることである。

proof. $n_1, \cdots n_r$ が *pairwise* に互いに素であるとする。

$$\begin{aligned}&n_i \text{と } n_j \ (i \neq j) \text{ が互いに素} \\ &\Leftrightarrow \exists x, \exists y \in \mathbf{Z} \text{ s.t. } n_i x + n_j y = 1 \\ &\Leftrightarrow (n_i) + (n_j) = \mathbf{Z}\end{aligned}$$

ゆえに

$$\begin{aligned} &n_1, \cdots, n_r \text{が} pairwise \text{に互いに素} \\ \Leftrightarrow\ &(n_1), \cdots, (n_r) \text{が} pairwise \text{に互いに素} \end{aligned}$$

である。従って中国式剰余定理より、

$$\mathbf{Z}/\bigcap_{i=1}^{r}(n_i) \cong \mathbf{Z}/(n_1) \times \cdots \times \mathbf{Z}/(n_r)$$

を得る。また仮定より $\bigcap_{i=1}^{r}(n_i) = (lcm(n_1, \cdots, n_r)) = (n_1 \cdots n_r)$ だから

$$\mathbf{Z}/(n_1 \cdots n_r) \cong \mathbf{Z}/(n_1) \times \cdots \times \mathbf{Z}/(n_r) \tag{15}$$

を得る。ゆえに $\mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$ は巡回群である。

逆に $\mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$ が巡回群とする。このとき n_i と n_j が互いに素でないような i,j が存在したとすると、

$$\mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r \text{の指数} = lcm(n_1, \cdots, n_r) < n_1 \cdots n_r$$

となる。これは矛盾。(もし巡回群なら、生成元となる元の位数は $n_1 \cdots n_r$ であるが、上で見たように $\mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$ にはそのような元はない。) □

さて、前節までのことを利用すると

1. $p \neq 2, n \geq 1$ のとき
   (4) , (9) , (11) より

$$\begin{aligned} (\mathbf{Z}/p^n)^\times &\cong U_1/U_n \times V_n \\ &\cong \mathbf{Z}/p^{n-1} \times \mathbf{Z}/p-1 \quad (\because V_n \cong \mathbf{F}_p^\times \cong \mathbf{Z}/p-1) \end{aligned}$$

2. $p = 2, n \geq 2$ のとき
   (4) , (9) , (13) , (14) より

$$\begin{aligned} (\mathbf{Z}/p^n)^\times &\cong U_1/U_n \times V_n \\ &\cong (\{\pm 1\} \times U_2/\{1\} \times U_n) \times V_n \\ &\cong (\{\pm 1\}/\{1\} \times U_2/U_n) \times V_n (\because \{1\} \lhd \{\pm 1\}, U_n \lhd U_2) \\ &\cong (\{\pm 1\} \times U_2/U_n) \times \{1\} \quad (\because V_n \cong \mathbf{F}_2^\times = \{1\}) \\ &\cong \mathbf{Z}/2 \times \mathbf{Z}/2^{n-2} \end{aligned}$$

以上より

$$(\mathbf{Z}/p^n)^\times \begin{cases} \cong \mathbf{Z}/p^{n-1} \times \mathbf{Z}/p-1 & (p \neq 2, n \geq 1) \\ \cong \mathbf{Z}/2^{n-2} \times \mathbf{Z}/2 & (p = 2, n \geq 2) \\ = \{1\} & (p = 2, n = 1) \end{cases} \tag{16}$$

が得られる。

さらに、$p \neq 2, n \geq 1$ のときは、$\gcd(p^{n-1}, p-1) = 1$ だから

$$\mathbf{Z}/p^{n-1} \times \mathbf{Z}/p-1 \cong \mathbf{Z}/p^{n-1}(p-1) \tag{17}$$

より巡回群となる。

従って、m の素因数分解を ${p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}$ ($p_1, p_2, \cdots, p_s$ は相異なる素数) とすると (15) と各 $\mathbf{Z}/{p_i}^{e^i}$ が積に関しモノイドであることから

$$\begin{aligned} (\mathbf{Z}/m)^\times &= (\mathbf{Z}/{p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s})^\times \\ &\cong (\mathbf{Z}/{p_1}^{e_1} \times \mathbf{Z}/{p_2}^{e_2} \times \cdots \mathbf{Z}/{p_s}^{e_s})^\times \\ &= (\mathbf{Z}/{p_1}^{e_1})^\times \times (\mathbf{Z}/{p_2}^{e_2})^\times \times \cdots \times (\mathbf{Z}/{p_s}^{e_s})^\times \end{aligned} \tag{18}$$

となり、以下 (16) により直積分解が続く。従って、$(\mathbf{Z}/m)^\times$ の群構造を調べる際、(18) の群構造を調べてもよいことが分かる。

例 1.

$(\mathbf{Z}/15)^\times$	$(\mathbf{Z}/16)^\times$	$(\mathbf{Z}/20)^\times$
$= (\mathbf{Z}/3\cdot 5)^\times$	$= (\mathbf{Z}/2^4)^\times$	$= (\mathbf{Z}/2^2\cdot 5)^\times$
$\cong (\mathbf{Z}/3)^\times \times (\mathbf{Z}/5)^\times$	$\cong \mathbf{Z}/2^{4-2} \times \mathbf{Z}/2$	$\cong (\mathbf{Z}/2^2)^\times \times (\mathbf{Z}/5)^\times$
$\cong \mathbf{Z}/2 \times \mathbf{Z}/4$	$\cong \mathbf{Z}/4 \times \mathbf{Z}/2$	$\cong \mathbf{Z}/2 \times \mathbf{Z}/4$

よって $(\mathbf{Z}/15)^\times, (\mathbf{Z}/16)^\times, (\mathbf{Z}/20)^\times$ の群構造は同型の違いを無視すれば同じ構造のものと考えられる。また、指数は $4(= lcm(2,4))$ である。

例 2.

$(\mathbf{Z}/17)^\times$	$(\mathbf{Z}/18)^\times$
$= \mathbf{Z}/16$	$= (\mathbf{Z}/2\cdot 3^2)^\times$
	$\cong (\mathbf{Z}/2)^\times \times (\mathbf{Z}/3^2)^\times$
	$\cong \{1\} \times (\mathbf{Z}/3 \times \mathbf{Z}/2)$
	$\cong \mathbf{Z}/3 \times \mathbf{Z}/2$
	$\cong \mathbf{Z}/6 \quad (\because \gcd(3,2) = 1)$

よって $(\mathbf{Z}/17)^\times, (\mathbf{Z}/18)^\times$ は巡回群になる。また、指数はそれぞれ $16, 6$ である。

さて、$(\mathbf{Z}/m)^\times$ の群構造関し次の主張を証明する。

主張 1. $(\mathbf{Z}/m)^\times$ が巡回群になるための必要十分条件は m が $2, 4, 2p^n, p^n (p$: 奇素数$, n \geq 1)$ となるときである。

proof. m の素因数分解を $\prod_{i=1}^{s} {p_i}^{e_i} (p_i$: 相異なる素数$, e_i \geq 1, s \geq 1)$ とする。$(\mathbf{Z}/m)^\times$ が巡回群であるとする。(16),(18) 及び補題 5.4 に注意する。

1. $2 \nmid m$ のとき

   各 p_i は奇素数であるから、$p_i - 1$ は偶数である。もし、$s > 1$ とすると $1 \leq i, j \leq s\ (i \neq j)$ について、$\gcd(p_i - 1, p_j - 1) \neq 1$ だから $(\mathbf{Z}/m)^\times$ は巡回群にならない。よって $s \leq 1$ であるべき。従って、$m = p_1^{e_1}$ となる。このとき、(17) より $(\mathbf{Z}/m)^\times$ は巡回群になる。ゆえ、$2 \nmid m$ のとき $(\mathbf{Z}/m)^\times$ が巡回群となるための必要十分条件は、$m = p_1^{e_1}$ である。

2. $2 \mid m$ のとき

   $p_1 = 2$ とする。$e_1 > 2$ とすると、$\gcd(2^{e_1 - 2}, 2) \neq 1$ だから $e_1 \leq 2$ であるべき。$2 \leq i \leq s$ では p_i は奇素数である。もし、$s > 2$ とすると $2 \leq i, j \leq s (i \neq j)$ について、$\gcd(p_i - 1, p_j - 1) \neq 1$ だから $s \leq 2$ であるべき。従って、$m = 2, 2p_2^{e_2}, 2^2, 2^2 p_2^{e_2}$ となるが (16) より、

   (a) $m = 2$ のとき
   $(\mathbf{Z}/2)^\times = \{1\}$ より巡回群。

   (b) $m = 2^2$ のとき
   $(\mathbf{Z}/2^2)^\times \cong \mathbf{Z}/2$ より巡回群。

   (c) $m = 2p_2^{e_2}$ のとき
   $(\mathbf{Z}/2p_2^{e_2})^\times \cong \{1\} \times \mathbf{Z}/p_2^{e_2 - 1}(p_2 - 1) \cong \mathbf{Z}/p_2^{e_2 - 1}(p_2 - 1)$
   より巡回群。

   (d) $m = 2^2 p_2^{e_2}$ のとき
   $(\mathbf{Z}/2^2 {p_2}^{e_2})^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/p_2^{e_2 - 1}(p_2 - 1)$
   $\gcd(2, p_2 - 1) \neq 1$ より巡回群でない。

以上より、$2 \mid m$ のとき $(\mathbf{Z}/m)^\times$ が巡回群となるための必要十分条件は、$m = 2, 4, 2p_2^{e_2}$ である。

□

次に、$(\mathbf{Z}/m)^\times$ の指数に関し次の主張を証明する。

主張 2. $\forall m \geq 3$ について $(\mathbf{Z}/m)^\times$ の指数は偶数で、$m = 2$ のとき指数は 1 である。

proof. m の素因数分解を $\prod_{i=1}^{s} {p_i}^{e_i} (p_i$: 相異なる素数$, e_i \geq 1, s \geq 1)$ とする。$e := (\mathbf{Z}/m)^\times$の指数 とおく。

1. $2 \nmid m$ のとき
   各 p_i は奇素数であるから
   $$e = \underset{1 \leq i \leq s}{lcm} ({p_i}^{e_i - 1}, p_i - 1)$$
   $p_1 - 1 \mid e$ より $2 \mid e$ である。よって e は偶数。

2. $2 \mid m$ のとき
   $p_1 = 2$ とする。$i \geq 2$ について p_i は奇素数である。

   (a) $e_1 \geq 2$ のとき
   $$e = \underset{2 \leq i \leq s}{lcm} (2^{e_1 - 2}, 2, p_i^{e_i - 1}, p_i - 1)$$
   s に関わらず $2 \mid e$ だから指数は偶数。

   (b) $e_1 = 1$ のとき

   i. $s > 1$ のとき
   $m = 2 \prod_{i=2}^{s} p_i^{e_1}$ より
   $$e = \underset{2 \leq i \leq s}{lcm} ({p_i}^{e_i - 1}, p_i - 1)$$
   $p_2 - 1 \mid e$ より $2 \mid e$ である。よって e は偶数。

   ii. $s = 1$ のとき
   $m = 2$ だから
   $$(\mathbf{Z}/2)^\times = \{1\}$$
   $ord(1) = 1$ だから指数は 1 である。

□

6　$(\mathbf{Z}/m)^\times$ の指数を与えた時の m の上限 (その１)

前節より、$(\mathbf{Z}/m)^\times$ の m を決めると m を素因数分解することで、群構造が分かり、同時に指数も分かるのであった。逆に指数を先に与えた場合 m のとりうる値について興味がいく。この節では指数を先に与えた時に、m の上限について考察する。

指数を先に与えた時、m について以下の主張を証明する。

主張 3. $e := (\mathbf{Z}/m)^\times$の指数 とおく。このとき、
$\forall n \geq 1, \exists M(n) : n$ の関数 $s.t.\ e \leq n \Rightarrow m \leq M(n).$

($\mathbf{Z}/m)^\times$の指数 に上限 n を与えると、m は n による関数で上からおさえられる。)

proof. $e \leq n$ を仮定する。もし、m の素因数に $p > n+1$ なる p があるとすると、このとき $p \geq 3$ より $e \geq p-1 > n$ となり仮定に反す。ゆえ

$$m \text{ の素因数は全て } n+1 \text{ 以下であるべき} \tag{19}$$

m の素因数分解を $\prod_{i=1}^{s} {p_i}^{e_i} (p_i : \text{相異なる素数}, e_i \geq 1, s \geq 1)$ とする。

1. $n = 1$ のとき

   主張 2 より m の上限は 2 である。

2. $n \geq 2$ のとき

   (a) m の素因数に 2 が入っていない場合

   m の素因数は全て奇素数である。$n \geq e = \underset{1 \leq i \leq s}{lcm} ({p_i}^{e_i-1}, p_i - 1)$
   より $n \geq {p_i}^{e_i-1}, n \geq p_i - 1$ であるべき。

   $n \geq {p_i}^{e_i-1} \Leftrightarrow e_i \leq 1 + \log_{p_i} n \Rightarrow e_i \leq 1 + \log_3 n \overset{e_i \in \mathbf{Z}}{\Leftrightarrow} e_i \leq 1 + [\log_3 n]$
   $n \geq p_i - 1 \Leftrightarrow p_i \leq n + 1$

   一方、(p_i の数) $= s \leq p_s - 2$ であるが (19) より $s \leq n - 1$ で

あるべき。従って

$$\begin{aligned} m &= \prod_{i=1}^{s} {p_i}^{e_i} \\ &\leq \prod_{i=1}^{s} (n+1)^{[\log_3 n]+1} = (n+1)^{([\log_3 n]+1)s} \\ &\leq (n+1)^{([\log_3 n]+1)(n-1)} \end{aligned}$$

(b) m の素因数に 2 が入っている場合

$p_1 = 2$ とする。

$$n \geq e = \begin{cases} \underset{2\leq i\leq s}{lcm}\,(2^{e_1-2}, 2, {p_i}^{e_i-1}, p_i - 1) & (e_1 \geq 2) \\ \underset{2\leq i\leq s}{lcm}\,({p_i}^{e_i-1}, p_i - 1) & (e_1 = 1) \end{cases}$$

$(e_1 \geq 2)$ のとき

$n \geq 2^{e_1-2}$ より $2^{e_1} \leq 4n$ であるべき。$i \geq 2$ では $n \geq {p_i}^{e_i-1}, n \geq p_i - 1$ だから $e_i \leq 1 + [\log_3 n], p_i \leq n+1$ であるべき。一方、(p_i の数) $= s \leq p_s - 1$ であるが (19) より $s \leq n$ であるべき。従って

$$\begin{aligned} m &= 2^{e_1} \prod_{i=2}^{s} {p_i}^{e_i} \\ &\leq 4n \prod_{i=2}^{s} (n+1)^{[\log_3 n]+1} = 4n(n+1)^{([\log_3 n]+1)(s-1)} \\ &\leq 4n(n+1)^{([\log_3 n]+1)(n-1)} \end{aligned}$$

$(e_1 = 1)$ のとき

$i \geq 2$ では e_i, p_i の条件は $e_1 \geq 2$ のときと同じで、s の条件も同じである。従って

$$\begin{aligned} m &= 2 \prod_{i=2}^{s} {p_i}^{e_i} \\ &\leq 2 \prod_{i=2}^{s} (n+1)^{[\log_3 n]+1} = 2(n+1)^{([\log_3 n]+1)(s-1)} \\ &\leq 2(n+1)^{([\log_3 n]+1)(n-1)} \end{aligned}$$

さて

$$(n+1)^{([\log_3 n]+1)(n-1)} < 2(n+1)^{([\log_3 n]+1)(n-1)} < 4n(n+1)^{([\log_3 n]+1)(n-1)}$$

だから、$n \geq 2$ のとき

$$M(n) := 4n(n+1)^{([\log_3 n]+1)(n-1)}$$

とおけば $m \leq M(n)$ となる。

ここで $M(1) = 4$ である。$4 > \{n = 1$ のときの m の上限 $\}$ より $\forall n \geq 1$ に対して $e \leq n$ ならば $m \leq M(n)$ を得る。

□

主張 3 で 指数 n を決めるごとに m は上からおさえられることが分かったので、n を与えたときの m の最大値を求めてみることにする。

主張 2 より $m \geq 3$ のとき、$(\mathbf{Z}/m)^\times$ の指数は常に偶数だったから、$n = 2, 4, 6$ について調べてみる。

$\langle n = 2$ のとき m の最大値を求める $\rangle$

主張 3 より $m \leq M(2) = 24$ であることが分かっている。

1. m の素因数に偶素数 2 があるとする

   $p_1 = 2$ とおく。もし、$e_1 > 3$ とすると $(\mathbf{Z}/2^{e_1})^\times \cong \mathbf{Z}/2^{e_1-2} \times \mathbf{Z}/2$ より、$\mathbf{Z}/2^{e_1-2}$ の元で位数が 2 より大きいものが存在してしまう。よって $e_1 \leq 3$ であるべき。

   $(\mathbf{Z}/2^3)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2$ (位数 1,2 の元がある)
   $(\mathbf{Z}/2^2)^\times \cong \mathbf{Z}/2$ (位数 1,2 の元がある)
   $(\mathbf{Z}/2)^\times = \{1\}$ (位数 1 の元がある)

2. m の素因数に奇素数 p_i があるとする。

   もし、$p_i > 3$ とすると $\mathbf{Z}/p_i - 1$ の元で位数が 2 より大きいものが存在してしまう。よって $p_i \leq 3$ であるべきだがこれを満たす奇素数は 3 のみである。$p_2 = 3$ とおく。もし、$e_2 > 1$ とすると

$(\mathbf{Z}/3^{e_2})^\times \cong \mathbf{Z}/3^{e_2-1} \times \mathbf{Z}/2$ より $\mathbf{Z}/3^{e_2-1}$ の元で位数が 2 より大きいものが存在してしまう。よって $e_2 \leq 1$ であるべき。

$$(\mathbf{Z}/3)^\times \cong \mathbf{Z}/2 \qquad \text{(位数 1,2 の元がある)}$$

従って m の素因数として考えられるのは $2, 3$ でそれぞれの冪の上限は $3, 1$ である。

さて

$$(\mathbf{Z}/2^3)^\times \times (\mathbf{Z}/3)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$$

の指数は $2(= \mathrm{lcm}(2,2,2))$ より求める m は $24(= 2^3 \cdot 3)$ である。

$$(\mathbf{Z}/24)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$$

$\langle n = 4$ のとき m の最大値を求める $\rangle$

主張 3 より $m \leq M(4) = 4 \cdot 4 \cdot 5^6 = 250000$ であることが分かっている。

1. m の素因数に偶素数 2 があるとする

   $p_1 = 2$ とおく。もし、$e_1 > 4$ とすると $(\mathbf{Z}/2^{e_1})^\times \cong \mathbf{Z}/2^{e_1-2} \times \mathbf{Z}/2$ より、$\mathbf{Z}/2^{e_1-2}$ の元で位数が 4 より大きいものが存在してしまう。よって $e_1 \leq 4$ であるべき。

   $$\begin{aligned}
   (\mathbf{Z}/2^4)^\times &\cong \mathbf{Z}/2^2 \times \mathbf{Z}/2 && \text{(位数 1,2,4 の元がある)}\\
   (\mathbf{Z}/2^3)^\times &\cong \mathbf{Z}/2 \times \mathbf{Z}/2 && \text{(位数 1,2 の元がある)}\\
   (\mathbf{Z}/2^2)^\times &\cong \mathbf{Z}/2 && \text{(位数 1,2 の元がある)}\\
   (\mathbf{Z}/2)^\times &= \{1\} && \text{(位数 1 の元がある)}
   \end{aligned}$$

2. m の素因数に奇素数 p_i があるとする。

   もし、$p_i > 5$ とすると $\mathbf{Z}/p_i - 1$ の元で位数が 4 より大きいものが存在してしまう。よって $p_i \leq 5$ であるべき。$p_2 = 3, p_3 = 5$ とおく。

   もし、$e_2 > 2$ とすると $(\mathbf{Z}/3^{e_2})^\times \cong \mathbf{Z}/3^{e_2-1} \times \mathbf{Z}/2$ より $\mathbf{Z}/3^{e_2-1}$ の元で位数が 4 より大きいものが存在してしまう。よって $e_2 \leq 2$ で

あるべき。ところが $e_2 = 2$ のとき $(\mathbf{Z}/3^2)^\times \cong \mathbf{Z}/3 \times \mathbf{Z}/2 \cong \mathbf{Z}/6$ となるので位数が 4 より大きいものが存在してしまう。よって $e_2 \leq 1$ であるべき。

$$(\mathbf{Z}/3)^\times \cong \mathbf{Z}/2 \qquad \text{(位数 1,2 の元がある)}$$

もし、$e_3 > 1$ とすると $(\mathbf{Z}/5^{e_3})^\times \cong \mathbf{Z}/5^{e_3-1} \times \mathbf{Z}/4$ より $\mathbf{Z}/5^{e_3-1}$ の元で位数が 4 より大きいものが存在してしまう。よって $e_3 \leq 1$ であるべき。

$$(\mathbf{Z}/5)^\times \cong \mathbf{Z}/4 \qquad \text{(位数 1,2,4 の元がある)}$$

従って m の素因数として考えられるのは $2, 3, 5$ でそれぞれの冪の上限は $4, 1, 1$ である。

さて

$$(\mathbf{Z}/2^4)^\times \times (\mathbf{Z}/3)^\times \times (\mathbf{Z}/5)^\times \cong \mathbf{Z}/4 \times \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/4$$

の指数は $4(= \mathrm{lcm}(4, 2, 2, 4))$ より求める m は $240(= 2^4 \cdot 3 \cdot 5)$ である。

$$(\mathbf{Z}/240)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/4 \times \mathbf{Z}/4$$

$\langle n = 6$ のとき m の最大値を求める $\rangle$

主張 3 より $m \leq M(6) = 4 \cdot 6 \cdot 7^{10}$ であることが分かっている。

1. m の素因数に偶素数 2 があるとする

   $p_1 = 2$ とおく。もし、$e_1 > 4$ とすると $(\mathbf{Z}/2^{e_1})^\times \cong \mathbf{Z}/2^{e_1-2} \times \mathbf{Z}/2$ より、$\mathbf{Z}/2^{e_1-2}$ の元で位数が 6 より大きいものが存在してしまう。よって $e_1 \leq 4$ であるべき。

   $(\mathbf{Z}/2^4)^\times \cong \mathbf{Z}/2^2 \times \mathbf{Z}/2$ (位数 1,2,4 の元がある)
   $(\mathbf{Z}/2^3)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2$ (位数 1,2 の元がある)
   $(\mathbf{Z}/2^2)^\times \cong \mathbf{Z}/2$ (位数 1,2 の元がある)
   $(\mathbf{Z}/2)^\times = \{1\}$ (位数 1 の元がある)

2. m の素因数に奇素数 p_i があるとする。

もし、$p_i > 7$ とすると $\mathbf{Z}/p_i - 1$ の元で位数が 6 より大きいものが存在してしまう。よって $p_i \leq 7$ であるべき。$p_2 = 3, p_3 = 5, p_4 = 7$ とおく。

もし、$e_2 > 2$ とすると $(\mathbf{Z}/3^{e_2})^\times \cong \mathbf{Z}/3^{e_2-1} \times \mathbf{Z}/2$ より $\mathbf{Z}/3^{e_2-1}$ の元で位数が 6 より大きいものが存在してしまう。よって $e_2 \leq 2$ であるべき。

$$\begin{aligned}(\mathbf{Z}/3^2)^\times &\cong \mathbf{Z}/3 \times \mathbf{Z}/2 \qquad (\text{位数 1,2,3,6 の元がある})\\ &\cong \mathbf{Z}/6\\ (\mathbf{Z}/3)^\times &\cong \mathbf{Z}/2 \qquad (\text{位数 1,2 の元がある})\end{aligned}$$

もし、$e_3 > 2$ とすると $(\mathbf{Z}/5^{e_3})^\times \cong \mathbf{Z}/5^{e_3-1} \times \mathbf{Z}/4$ より $\mathbf{Z}/5^{e_3-1}$ の元で位数が 6 より大きいものが存在してしまう。よって $e_3 \leq 2$ であるべき。ところが $e_3 = 2$ のとき $(\mathbf{Z}/5^2)^\times \cong \mathbf{Z}/5 \times \mathbf{Z}/4 \cong \mathbf{Z}/20$ となるので位数が 6 より大きいものが存在してしまう。よって $e_3 \leq 1$ であるべき。

$$(\mathbf{Z}/5)^\times \cong \mathbf{Z}/4 \qquad (\text{位数 1,2,4 の元がある})$$

もし、$e_4 > 1$ とすると $(\mathbf{Z}/7^{e_4})^\times \cong \mathbf{Z}/7^{e_4-1} \times \mathbf{Z}/6$ より $\mathbf{Z}/7^{e_4-1}$ の元で位数が 6 より大きいものが存在してしまう。よって $e_4 \leq 1$ であるべき。

$$(\mathbf{Z}/7)^\times \cong \mathbf{Z}/6 \qquad (\text{位数 1,2,3,6 の元がある})$$

従って m の素因数として考えられるのは $2, 3, 5, 7$ でそれぞれの冪の上限は $4, 2, 1, 1$ である。

さて $(\mathbf{Z}/7)^\times \times (\mathbf{Z}/5)^\times$ は指数が $12 (= \mathrm{lcm}(6, 4))$ となるので不適。よって、$(2^{e_1(\leq 4)}, 3^{e_2(\leq 2)}, 5, 7)$ のうち $(5, 7)$ を組み合わせない 3 つ以下の組の直積で m が最大となるものを調べる。

(組が 2 つのとき)

直積	指数	m の値
$(\mathbf{Z}/7)^\times \times (\mathbf{Z}/3^2)^\times$	$6(=\mathrm{lcm}(6,6))$	63
$(\mathbf{Z}/7)^\times \times (\mathbf{Z}/2^4)^\times$	$12(=\mathrm{lcm}(6,4,2))$	不適
$(\mathbf{Z}/7)^\times \times (\mathbf{Z}/2^3)^\times$	$6(=\mathrm{lcm}(6,2,2))$	56
$(\mathbf{Z}/5)^\times \times (\mathbf{Z}/3^2)^\times$	$12(=\mathrm{lcm}(4,6))$	不適
$(\mathbf{Z}/5)^\times \times (\mathbf{Z}/3)^\times$	$4(=\mathrm{lcm}(4,2))$	15
$(\mathbf{Z}/5)^\times \times (\mathbf{Z}/2^4)^\times$	$4(=\mathrm{lcm}(4,4,2))$	80
$(\mathbf{Z}/3^2)^\times \times (\mathbf{Z}/2^4)^\times$	$12(=\mathrm{lcm}(6,4,2))$	不適
$(\mathbf{Z}/3^2)^\times \times (\mathbf{Z}/2^3)^\times$	$6(=\mathrm{lcm}(6,2,2))$	72
$(\mathbf{Z}/3)^\times \times (\mathbf{Z}/2^4)^\times$	$4(=\mathrm{lcm}(2,4,2))$	48

(組が 3 つのとき)

$(2^{e_1(\leq 4)}, 3^{e_2(\leq 2)}, 7)$ の組の直積を考える。$2^4 \cdot 3^2 \cdot 7 > 2^3 \cdot 3^2 \cdot 7 > 2^4 \cdot 3 \cdot 7$ だが、上のことより $(2^4, 7)$ の組は不適だから $(2^4, 3^{e_2(\leq 2)}, 7)$ の組も不適。

$(2^{e_1(\leq 4)}, 3^{e_2(\leq 2)}, 5)$ の組の直積を考える。$2^4 \cdot 3^2 \cdot 5 > 2^3 \cdot 3^2 \cdot 5 > 2^4 \cdot 3 \cdot 5$ だが、上のことより $(5, 3^2)$ の組は不適だから $(2^{e_1(\leq 4)}, 3^2, 5)$ の組も不適。

直積	指数	m の値
$(\mathbf{Z}/7)^\times \times (\mathbf{Z}/3^2)^\times \times (\mathbf{Z}/2^3)^\times$	$6(=\mathrm{lcm}(6,6,2,2))$	504
$(\mathbf{Z}/5)^\times \times (\mathbf{Z}/3)^\times \times (\mathbf{Z}/2^4)^\times$	$4(=\mathrm{lcm}(4,2,4,2))$	240

以上のことから求める m は 504 である。

$$(\mathbf{Z}/504)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/6 \times \mathbf{Z}/6$$

7 $(\mathbf{Z}/m)^\times$ の指数を与えた時の m の上限 (その２)

前節より $n = 2, 4, 6$ のとき、$e \leq n$ を満たす m の最大値はそれぞれ $24, 240, 504$ であった。このとき、指数はそれぞれ $2, 4, 6$ だからこれらの

値は、$e = n$ を満たす m の最大値である。この節では $e = n$ を満たす m の最大値についてその存在と値について考察する。

記号． 群 G の指数を $e(G)$ と表す。

記号． $prim(m) := \{m \text{ の素因数 }\}$

補題 7.1. G を有限アーベル群とする。
このとき、$\forall g \in G, ord(g) \mid e(G)$ である。

proof. $e(G) = m$ とする。$m = 1$ のときは、$G = \{1\}$ より明らか。$m \geq 2$ のときを考える。$a \in G$ を G の位数最大元とする。(すなわち、$ord(a) = m$ である。) $ord(b) \nmid m$ となる $b \in G$ が存在したと仮定して矛盾を導く。$ord(b) = n(\neq 1)$ とおく。

1. $prim(n) \nsubseteq prim(m)$ のとき

   このとき、$p \mid n, p \nmid m$ となる素数 p がある。$n = pn'(\exists n' \in \mathbf{Z})$ と書けるので、$ord(b^{n'}) = p$ である。G はアーベル群で $\gcd(p, m) = 1$ だから $ord(ab^n) = mp > m$ となって矛盾。

2. $prim(n) \subset prim(m)$ のとき

   $prim(m) = \{p_1, \cdots, p_t\}$ とする。$m = \prod_{i=1}^{t} p_i^{m_i}\ (m_i \geq 1), n = \prod_{i=1}^{t} p_i^{n_i}\ (n_i \geq 0, n_i$のうち少なくとも一つは$0$でない。$)$ と書ける。仮定より $n \nmid m$ だから $n_j > m_j$ なる j が少なくとも 1 つ存在する。(もし、$\forall i$ について $n_i \leq m_i$ となっていたら $n \mid m$ となって矛盾。) $\prod_{i \neq j} p_i^{m_i}, \prod_{i \neq j} p_i^{n_i}$ をそれぞれ m', n' とおくと、$m = p_j^{m_j} m', n = p_j^{n_j} n'$ で $p_j \nmid m'$, $p_j \nmid n'$ となる。$ord({a^{p_j}}^{m_j}) = m', ord(b^{n'}) = {p_j}^{n_j}$ で $\gcd(m', {p_j}^{n_j}) = 1$ だから $ord({a^{p_j}}^{m_j} b^{n'}) = m' {p_j}^{n_j} > m' {p_j}^{m_j} = m$ となって矛盾。

□

補題 7.2. $r \geq 2$ とし、$G_1, \cdots, G_r$ を有限アーベル群とする。このとき、$lcm(e(G_1), \cdots, e(G_r)) = e(G_1 \times \cdots \times G_r)$ である。

proof. $ord(g_1) = e(G_1), \cdots, ord(g_r) = e(G_r)$ とする。

$$\begin{aligned} lcm(e(G_1), \cdots, e(G_r)) &= lcm(ord(g_1), \cdots, ord(g_r)) \\ &= ord(g_1, \cdots, g_r) \\ &\leq e(G_1 \times \cdots \times G_r) \end{aligned}$$

一方、$ord(g_1, \cdots, g_r) = e(G_1 \times \cdots \times G_r)$ とする。補題 7.1 より、$ord(g_1) \mid e(G_1), \cdots, ord(g_r) \mid e(G_r)$ である。ゆえに、

$$\begin{aligned} e(G_1 \times \cdots \times G_r) &= ord(g_1, \cdots, g_r) \\ &= lcm(ord(g_1), \cdots, ord(g_r)) \\ &\leq lcm(e(G_1), \cdots, e(G_r)) \end{aligned}$$

以上より、$lcm(e(G_1), \cdots, e(G_r)) = e(G_1 \times \cdots \times G_r)$ が示された。

□

系 7.3. $e(G_1 \times \cdots \times G_r) \mid n \Leftrightarrow e(G_1) \mid n, \cdots, e(G_r) \mid n$

proof. 補題 7.2 より

$$e(G_1 \times \cdots \times G_r) \mid n \Leftrightarrow lcm(e(G_1), \cdots, e(G_r)) \mid n$$

であることから言える。

□

系 7.4. $n \geq 1$ とし、m の素因数分解を $\prod_{i=1}^{s} {p_i}^{e_i} (p_i$: 相異なる素数, $e_i \geq 1, s \geq 1)$ とする。このとき、$e((\mathbf{Z}/m)^{\times}) \mid n$ となる必要十分条件は、全ての i に対して $e((\mathbf{Z}/{p_i}^{e_i})^{\times}) \mid n$ となることである。

proof. (18) と系 7.3 より明らか。

□

命題 7.5. $n \geq 1$ とし、$M_1(n) := \max\{m \mid \ e((\mathbf{Z}/m)^{\times}) \mid n\}$ とおく。このとき、

$$M_1(n) = \prod_{p:\text{素数}} p^{\mu(n,p)}$$

ここに、

$$\mu(n,p) = \begin{cases} 1 & if \quad p = 2, v_2(n) = 0 \\ v_2(n) + 2 & if \quad p = 2, v_2(n) \geq 1 \\ v_p(n) + 1 & if \quad p \neq 2, p-1 \mid n \\ 0 & if \quad p \neq 2, p-1 \nmid n \end{cases}$$

である。

proof. 系 7.4 より $e((\mathbf{Z}/m)^\times) \mid n$ を満たす最大の m は、$e((\mathbf{Z}/p^\mu)^\times) \mid n$ を満たすような $\mu(\geq 1)$ が一つでもあるような全ての素数 p に対して、$\mu(n,p) := \max\{\mu \mid e((\mathbf{Z}/p^\mu)^\times) \mid n\}$ とおいたとき、$p^{\mu(n,p)}$ の積をとった値である。

1. $p \neq 2$ のとき

   $e((\mathbf{Z}/p^\mu)^\times) = p^{\mu-1}(p-1)$ より $\mu \geq 1$ について

   $$p^{\mu-1}(p-1) \mid n \Leftrightarrow p-1 \mid n \ , \ p^{\mu-1} \mid n$$

   ゆえに

   (a) $p-1 \nmid n$ のとき

   $\mu(n,p) = 0$

   (b) $p-1 \mid n$ のとき

   $p^{\mu-1} \mid n \Leftrightarrow \mu - 1 \leq v_p(n)$ より $\mu(n,p) = v_p(n) + 1$

   これより、

   $$\begin{cases} p-1 \nmid n \Rightarrow \mu(n,p) = 0 \\ p-1 \mid n \Rightarrow \mu(n,p) = v_p(n) + 1 \end{cases}$$

   を得る。

2. $p = 2$ のとき

   $$e((\mathbf{Z}/2^\mu)^\times) = \begin{cases} 1 & (\mu = 1) \\ 2 & (\mu = 2) \\ 2^{\mu-2} & (\mu \geq 3) \end{cases}$$

   より

   $$e((\mathbf{Z}/2^\mu)^\times) \mid n \Leftrightarrow \begin{cases} 1 \mid n & (\mu = 1) \\ 2 \mid n \Leftrightarrow v_2(n) \geq 1 & (\mu = 2) \\ 2^{\mu-2} \mid n \Leftrightarrow \mu - 2 \leq v_2(n) & (\mu \geq 3) \end{cases}$$

従って、

$$
\begin{aligned}
v_2(n) = 0 &\Rightarrow \mu(n,2) = 1 \\
v_2(n) = 1 &\Rightarrow \mu(n,2) = 3 \\
v_2(n) = 2 &\Rightarrow \mu(n,2) = 4 \\
v_2(n) = 3 &\Rightarrow \mu(n,2) = 5 \\
v_2(n) = 4 &\Rightarrow \mu(n,2) = 6 \\
&\vdots
\end{aligned}
$$

である。これより、

$$
\begin{cases}
v_2(n) = 0 \Rightarrow \mu(n,2) = 1 \\
v_2(n) \geq 1 \Rightarrow \mu(n,2) = v_2(n) + 2
\end{cases}
$$

を得る。

□

系 7.6. $e((\mathbf{Z}/m)^\times) \mid n$ を満たす任意の m に対して、$m \mid M_1(n)$ である。

proof. 命題 7.5 より明らか。

□

系 7.7. $n \geq 1$ とする。
$E_n := \{m \mid e((\mathbf{Z}/m)^\times) = n\}, D_n := \{m \mid e((\mathbf{Z}/m)^\times) \mid n\}$ とし、$M_0(n) := \max E_n, M_1(n) := \max D_n$ とおく。このとき、

1. $e((\mathbf{Z}/M_1(n))^\times) = n \Rightarrow M_1(n) = M_0(n)$
2. $e((\mathbf{Z}/M_1(n))^\times) < n \Rightarrow M_0(n)$ は存在しない

が成り立つ。

proof. $\forall n \geq 1$ に対して、$2 \in D_n$ だから $D_n \neq \phi$ である。よって、$\forall n \geq 1$ に対して、$M_1(n)$ は存在する。

1. を示す。

   $e((\mathbf{Z}/M_1(n))^\times) = n$ とする。このとき、$M_1(n) \in E_n$ である。もし、$m_0 \in E_n$ であって $m_0 > M_1(n)$ となるものがあったとしたら、$M_1(n)$ の最大性に反す。よって、$\forall m \in E_n, m \leq M_1(n)$ である。ゆえに、$M_1(n) = M_0(n)$ である。

2. を示す。

$e((\mathbf{Z}/M_1(n))^\times) < n$ とする。系 7.6 より、$\forall m \in D_n, m \mid M_1(n)$ である。命題 7.5 より $M_1(n) = \prod_{p:\text{素数}} p^{\mu(n,p)}$ だから $m = \prod_{p:\text{素数}} p^{\eta}$ $(\eta \leq \mu(n,p))$ と書ける。よって、$\forall m \in D_n, e((\mathbf{Z}/m)^\times) \leq e((\mathbf{Z}/M_1(n))^\times) < n$ である。ゆえに、仮定の下では $e((\mathbf{Z}/m)^\times) = n$ を満たす m は存在しない。従って、$E_n = \phi$ となり $M_0(n)$ は存在しない。

□

命題 7.5, 系 7.7 を利用して $n = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20$ のとき、$M_0(n), M_1(n)$ を求めてみる。

- $n = 2$ のとき

$$\mu(n, 2) = v_2(n) + 2 = 3$$

一方、2 の約数は $1, 2$ より、$p-1 \mid n$ となる奇素数 p は 3 のみである。

$$\mu(n, 3) = v_3(n) + 1 = 1$$

ゆえに、$M_1(2) = 2^3 \cdot 3 = 24$ である。さて、$(\mathbf{Z}/24)^\times$ の指数は 2 より、$M_0(2) = 24$ である。

- $n = 4$ のとき

$$\mu(n, 2) = v_2(n) + 2 = 4$$

一方、4 の約数は $1, 2, 4$ より、$p-1 \mid n$ となる奇素数 p は $3, 5$ である。

$$\mu(n, 3) = v_3(n) + 1 = 1$$
$$\mu(n, 5) = v_5(n) + 1 = 1$$

ゆえに、$M_1(4) = 2^4 \cdot 3 \cdot 5 = 240$ である。さて、$(\mathbf{Z}/240)^\times$ の指数は 4 より、$M_0(4) = 240$ である。

- $n = 6$ のとき

$$\mu(n, 2) = v_2(n) + 2 = 3$$

一方、6 の約数は $1, 2, 3, 6$ より、$p - 1 \mid n$ となる奇素数 p は $3, 7$ である。

$$\mu(n, 3) = v_3(n) + 1 = 2$$
$$\mu(n, 7) = v_7(n) + 1 = 1$$

ゆえに、$M_1(6) = 2^3 \cdot 3^2 \cdot 7 = 504$ である。さて、$(\mathbf{Z}/504)^\times$ の指数は 6 より、$M_0(6) = 504$ である。

- $n = 8$ のとき

$$\mu(n, 2) = v_2(n) + 2 = 5$$

一方、8 の約数は $1, 2, 4, 8$ より、$p - 1 \mid n$ となる奇素数 p は $3, 5$ である。

$$\mu(n, 3) = v_3(n) + 1 = 1$$
$$\mu(n, 5) = v_5(n) + 1 = 1$$

ゆえに、$M_1(8) = 2^5 \cdot 3 \cdot 5 = 480$ である。

さて、

$$(\mathbf{Z}/480)^\times \cong \mathbf{Z}/8 \times \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/4$$

より、指数は $8(=\mathrm{lcm}(8,2,2,4))$ である。従って、$M_0(8) = 480$ である。

- $n = 10$ のとき

$$\mu(n, 2) = v_2(n) + 2 = 3$$

一方、10 の約数は $1, 2, 5, 10$ より、$p-1 \mid n$ となる奇素数 p は $3, 11$ である。

$$\mu(n, 3) = v_3(n) + 1 = 1$$
$$\mu(n, 11) = v_{11}(n) + 1 = 1$$

ゆえに、$M_1(10) = 2^3 \cdot 3 \cdot 11 = 264$ である。

さて、

$$(\mathbf{Z}/264)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/10$$

より、指数は 10(=lcm(2,2,2,10)) である。従って、$M_0(10) = 264$ である。

- $n = 12$ のとき

$$\mu(n, 2) = v_2(n) + 2 = 4$$

一方、12 の約数は $1, 2, 3, 4, 6, 12$ より、$p-1 \mid n$ となる奇素数 p は $3, 5, 7, 13$ である。

$$\mu(n, 3) = v_3(n) + 1 = 2$$
$$\mu(n, 5) = v_5(n) + 1 = 1$$
$$\mu(n, 7) = v_7(n) + 1 = 1$$
$$\mu(n, 13) = v_{13}(n) + 1 = 1$$

ゆえに、$M_1(12) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 = 65520$ である。

さて、

$$(\mathbf{Z}/65520)^\times \cong \mathbf{Z}/4 \times \mathbf{Z}/2 \times \mathbf{Z}/3 \times \mathbf{Z}/2 \times \mathbf{Z}/4 \times \mathbf{Z}/6 \times \mathbf{Z}/12$$

より、指数は 12(=lcm(4,2,3,2,4,6,12)) である。従って、$M_0(12) = 65520$ である。

- $n = 14$ のとき

$$\mu(n,2) = v_2(n) + 2 = 3$$

一方、14 の約数は $1, 2, 7, 14$ より、$p-1 \mid n$ となる奇素数 p は 3 のみである。

$$\mu(n,3) = v_3(n) + 1 = 1$$

ゆえに、$M_1(14) = 2^3 \cdot 3 = 24$ である。さて、$(\mathbf{Z}/24)^\times$ の指数は 2 より、$M_0(14)$ は存在しない。

- $n = 16$ のとき

$$\mu(n,2) = v_2(n) + 2 = 6$$

一方、16 の約数は $1, 2, 4, 8, 16$ より、$p-1 \mid n$ となる奇素数 p は $3, 5, 17$ である。

$$\mu(n,3) = v_3(n) + 1 = 1$$
$$\mu(n,5) = v_5(n) + 1 = 1$$
$$\mu(n,17) = v_{17}(n) + 1 = 1$$

ゆえに、$M_1(16) = 2^6 \cdot 3 \cdot 5 \cdot 17 = 16320$ である。

さて、

$$(\mathbf{Z}/16320)^\times \cong \mathbf{Z}/16 \times \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/4 \times \mathbf{Z}/16$$

より、指数は16(=lcm(16,2,2,4,16))である。従って、$M_0(16) = 16320$ である。

- $n = 18$ のとき

$$\mu(n,2) = v_2(n) + 2 = 3$$

一方、18 の約数は $1, 2, 3, 6, 9, 18$ より、$p-1 \mid n$ となる奇素数 p は $3, 7, 19$ である。

$$\mu(n, 3) = v_3(n) + 1 = 3$$
$$\mu(n, 7) = v_7(n) + 1 = 1$$
$$\mu(n, 19) = v_{19}(n) + 1 = 1$$

ゆえに、$M_1(18) = 2^3 \cdot 3^3 \cdot 7 \cdot 19 = 28728$ である。

さて、

$$(\mathbf{Z}/28728)^\times \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/9 \times \mathbf{Z}/2 \times \mathbf{Z}/6 \times \mathbf{Z}/18$$

より、指数は $18(=\mathrm{lcm}(2,2,9,2,6,18))$ である。従って、$M_0(18) = 28728$ である。

- $n = 20$ のとき

$$\mu(n, 2) = v_2(n) + 2 = 4$$

一方、20 の約数は $1, 2, 4, 5, 10, 20$ より、$p-1 \mid n$ となる奇素数 p は $3, 5, 11$ である。

$$\mu(n, 3) = v_3(n) + 1 = 1$$
$$\mu(n, 5) = v_5(n) + 1 = 2$$
$$\mu(n, 11) = v_{11}(n) + 1 = 1$$

ゆえに、$M_1(20) = 2^4 \cdot 3 \cdot 5^2 \cdot 11 = 13200$ である。

さて、

$$(\mathbf{Z}/13200)^\times \cong \mathbf{Z}/4 \times \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/5 \times \mathbf{Z}/4 \times \mathbf{Z}/10$$

より、指数は $20(=\mathrm{lcm}(4,2,2,5,4,10))$ である。従って、$M_0(20) = 13200$ である。

以上を表にすると次のようになる。

n	$M_1(n)$	$M_0(n)$
2	24	24
4	240	240
6	504	504
8	480	480
10	264	264
12	65520	65520
14	24	存在しない
16	16320	16320
18	28728	28728
20	13200	13200

n を偶数としたとき、$e((\mathbf{Z}/m)^{\times}) = n$ を満たす m が存在しないような n もあることが分かる。(例：$n = 14$)

8　付録 (最小公倍数と最大公約数について)

この付録は 5 節で証明なしに使った、最小公倍数と最大公約数についてまとめたものである。

正の整数 a, b, c (ただし a, b, c のうち少なくとも一つは 2 以上とする。) に対し、$\{p_1, p_2, \cdots, p_s\} := prim(a) \cup prim(b) \cup prim(c)$ とおく。このとき、$a = \prod_{i=1}^{s} {p_i}^{\alpha_i}, b = \prod_{i=1}^{s} {p_i}^{\beta_i}, c = \prod_{i=1}^{s} {p_i}^{\gamma_i}$ $(\alpha_i, \beta_i, \gamma_i \geq 0, 1 \leq i \leq s)$ と書ける。

注意． $p_1, p_2, \cdots, p_s$ の定義より $\forall i, (\alpha_i, \beta_i, \gamma_i) \neq (0, 0, 0)$ である。

命題 8.1. 最小公倍数と最大公約数について以下が成り立つ。

1. $\gcd(a, b, c) = \prod_{i=1}^{s} p_i^{\min(\alpha_i, \beta_i, \gamma_i)}$
2. $lcm(a, b, c) = \prod_{i=1}^{s} p_i^{\max(\alpha_i, \beta_i, \gamma_i)}$

proof. $\zeta_i := \min(\alpha_i, \beta_i, \gamma_i), \eta_i := \max(\alpha_i, \beta_i, \gamma_i)$ とする。

1. $d := \prod_{i=1}^{s} {p_i}^{\zeta_i}$ とおく。

   (a) $d \mid a, d \mid b, d \mid c$ であること

   $\zeta_i = \min(\alpha_i, \beta_i, \gamma_i) \leq \alpha_i$ より ${p_1}^{\zeta_1}{p_2}^{\zeta_2} \cdots {p_s}^{\zeta_s} \mid {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s}$ だから $d \mid a$。以下同様に $\zeta_i \leq \beta_i, \zeta_i \leq \gamma_i$ だから $d \mid b, d \mid c$ を得る。

   (b) d が a, b, c の約数の中で最大であること

   $d' \mid a, d' \mid b, d' \mid c$ を満たすかってな d' をとる。このとき、d' の素因数において、$p_1, \cdots, p_s$ 以外の素数は現れない。ゆえ $d' = {p_1}^{\zeta'_1}{p_2}^{\zeta'_2} \cdots {p_s}^{\zeta'_s}$ とおくことができる。$d' \mid a$ より $\zeta'_i \leq \alpha_i$ である。以下同様に $\zeta'_i \leq \beta_i, \zeta'_i \leq \gamma_i$ である。従って、$\zeta'_i \leq \min(\alpha_i, \beta_i, \gamma_i)$ より $\zeta'_i \leq \zeta_i$ となる。以上より $d' \mid d$ であるから $d' \leq d$ が得られた。

2. $l := \prod_{i=1}^{s} {p_i}^{\eta_i}$ とおく。

   (a) $a \mid l, b \mid l, c \mid l$ であること

   $\alpha_i \leq \max(\alpha_i, \beta_i, \gamma_i) = \eta i$ より ${p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s} \mid {p_1}^{\eta_1}{p_2}^{\eta_2} \cdots {p_s}^{\eta_s}$ だから $a \mid l$。以下同様に $\beta_i \leq \eta_i, \gamma_i \leq \eta_i$ だから $b \mid l, c \mid l$ を得る。

   (b) l が a, b, c の公倍数の中で最小であること

   $a \mid l', b \mid l', c \mid l'$ を満たすかってな l' をとる。このとき l' は必ず $p_1, \cdots, p_s$ を素因数にもつ。ゆえ $l' = {p_1}^{\eta'_1}{p_2}^{\eta'_2} \cdots {p_s}^{\eta'_s}{p_{s+1}}^{\eta'_{s+1}} \cdots {p_t}^{\eta'_t}$ ($p_{s+1}, \cdots, p_t$ は $p_1, \ldots p_s$ と異なる素数 , $t \geq s$) の形をしている。$a \mid l'$ より $\alpha_i \leq \eta'_i$ $(1 \leq i \leq s)$ である。以下同様に $\beta_i \leq \eta'_i, \gamma_i \leq \eta'_i$ $(1 \leq i \leq s)$ である。従って、$\max(\alpha_i, \beta_i, \gamma_i) \leq \eta'_i$ より $\eta_i \leq \eta'_i$ $(1 \leq i \leq s)$ となる。以上より $l \mid l'$ であるから $l \leq l'$ が得られた。

□

定理 8.2. $\gcd(a, b, c) \leq lcm(a, b, c) \leq abc$

proof. $abc = \prod_{i=1}^{s} {p_i}^{\alpha_i+\beta_i+\gamma_i}$ である。従って、全ての i について

$$\min(\alpha_i, \beta_i, \gamma_i) \leq \max(\alpha_i, \beta_i, \gamma_i) \leq \alpha_i + \beta_i + \gamma_i$$

が成り立つことより言える。

□

定理 8.3. $\gcd(a,b,c) = 1$ となる必要十分条件は、全ての i に対して、$\{\alpha_i, \beta_i, \gamma_i\}$ のうち少なくとも一つは 0 となることである。

proof. $\gcd(a,b,c) = \prod_{i=1}^{s} p_i^{\min(\alpha_i,\beta_i,\gamma_i)}$ より

$$\begin{aligned}
&\gcd(a,b,c) = 1 \\
&\Leftrightarrow \forall i, \min(\alpha_i, \beta_i, \gamma_i) = 0 \\
&\Leftrightarrow \forall i, \{\alpha_i, \beta_i, \gamma_i\} \text{のうち少なくとも一つは} 0
\end{aligned}$$

□

定理 8.4. $lcm(a,b,c) = abc$ となる必要十分条件は、全ての i に対して、$\{\alpha_i, \beta_i, \gamma_i\}$ のうち一つを除いて全て 0 となることである。

proof. $lcm(a,b,c) = \prod_{i=1}^{s} p_i^{\max(\alpha_i,\beta_i,\gamma_i)}$ より

$$\begin{aligned}
&lcm(a,b,c) = abc \\
&\Leftrightarrow \forall i, \max(\alpha_i, \beta_i, \gamma_i) = \alpha_i + \beta_i + \gamma_i \\
&\Leftrightarrow \forall i, \{\alpha_i, \beta_i, \gamma_i\} \text{のうち一つを除いて全て} 0
\end{aligned}$$

□

系 8.5. $lcm(a,b,c) = abc$ であるための必要十分条件は、$\gcd(a,b) = 1, \gcd(b,c) = 1, \gcd(c,a) = 1$ (すなわち a, b, c が *pairwise* に互いに素) となることである。

proof. 定理 8.3 と定理 8.4 より

$$\begin{aligned}
&lcm(a,b,c) = abc \\
&\Leftrightarrow \forall i, \{\alpha_i, \beta_i, \gamma_i\} \text{のうち一つを除いて全て} 0 \\
&\overset{※}{\Leftrightarrow} \forall i, [\min(\alpha_i, \beta_i) = 0, \min(\beta_i, \gamma_i) = 0, \min(\gamma_i, \alpha_i) = 0] \\
&\Leftrightarrow \gcd(a,b) = 1, \gcd(b,c) = 1, \gcd(c,a) = 1
\end{aligned}$$

※の同値を示す。
($\Rightarrow$) は明らか。
($\Leftarrow$) を示す。
$\forall i, [\min(\alpha_i, \beta_i) = 0, \min(\beta_i, \gamma_i) = 0, \min(\gamma_i, \alpha_i) = 0]$ を仮定する。もし、ある i があって $\{\alpha_i, \beta_i, \gamma_i\}$ のうち 0 でないものが 2 つ以上あったとする

と、$[\min(\alpha_i,\beta_i),\min(\beta_i,\gamma_i),\min(\gamma_i,\alpha_i)]$ のうち少なくとも一つは 0 でなくなる。これは仮定に反す。よって $\forall i,\{\alpha_i,\beta_i,\gamma_i\}$ のうち一つを除いて全て 0 である。

□

系 8.6. $lcm(a,b,c) < abc$ であるための必要十分条件は、$\gcd(a,b) \neq 1$ または $\gcd(b,c) \neq 1$ または $\gcd(c,a) \neq 1$ となることである。

proof. 系 8.5 より

$$\begin{aligned} & lcm(a,b,c) \neq abc \\ & \Leftrightarrow \gcd(a,b) \neq 1 \text{ または } \gcd(b,c) \neq 1 \text{ または } \gcd(c,a) \neq 1 \end{aligned}$$

□

定理 8.7. $a \mid n_1, b \mid n_2, c \mid n_3$ ならば $lcm(a,b,c) \mid lcm(n_1,n_2,n_3)$

proof. $\{q_1,q_2,\cdots,q_s\} := \bigcup_{i=1}^{3} prim(n_i)$ とする。このとき、$n_1 = \prod_{i=1}^{s} {q_i}^{\delta_i}$, $n_2 = \prod_{i=1}^{s} {q_i}^{\epsilon_i}$, $n_3 = \prod_{i=1}^{s} {q_i}^{\mu_i}$ $(\delta_i,\epsilon_i,\mu_i \geq 0, 1 \leq i \leq s)$ と書ける。$a \mid n_1, b \mid n_2, c \mid n_3$ より、$a = \prod_{i=1}^{s} {q_i}^{\alpha_i}$ $(\alpha_i \leq \delta_i)$, $b = \prod_{i=1}^{s} {q_i}^{\beta_i}$ $(\beta_i \leq \epsilon_i)$, $c = \prod_{i=1}^{s} {q_i}^{\gamma_i}$ $(\gamma_i \leq \mu_i)$ となる。さて、

$$lcm(a,b,c) = \prod_{i=1}^{s} {q_i}^{\max(\alpha_i,\beta_i,\gamma_i)}$$

$$lcm(n_1,n_2,n_3) = \prod_{i=1}^{s} {q_i}^{\max(\delta_i,\epsilon_i,\mu_i)}$$

であるが、$\alpha_i \leq \delta_i$, $\beta_i \leq \epsilon_i$, $\gamma_i \leq \mu_i$ より

$$\max(\alpha_i,\beta_i,\gamma_i) \leq \max(\delta_i,\epsilon_i,\mu_i)$$

だから $lcm(a,b,c) \mid lcm(n_1,n_2,n_3)$ を得る。

□

注意． 以上の命題、定理、系は整数 $a_1,\cdots,a_r$ $(r \geq 2)$ のときも同様にして示せる。

参考文献

[1] J.-P. セール:「数論講義」岩波書店（邦訳 彌永健一）

[2] 松坂 和夫 著:「代数系入門」岩波書店

[3] 永尾 汎 著:「新数学講座-4 代数学」朝倉書店

[4] 彌永 昌吉・有馬 哲・朝枝 陽 著:「詳解 代数入門」東京図書株式会社

[5] 新妻 弘・木村 哲三 著：「群・環・体 入門」共立出版株式会社

[6] 倉田 吉喜 著：「現代数学ゼミナール 16 代数学」近代科学社