$\mathbb{F}_p^\times$ が巡回群であることについて

2020 年 6〜7 月
石動高校　片山　喜美

素数 p について、$\mathbb{F}_p^\times$ を考えるとき、それが巡回群になること、言い換えれば p を法とする原始根 ($\mathbb{F}_p^\times$ の生成元) が存在することは重要なことである。例えば、ガウス周期に関わるいろいろなことも、原始根の巾で考えていくとうまく示すことができるのである。

$\mathbb{F}_p^\times$ が巡回群になることは、**「体 K に含まれる有限乗法部分は巡回群になる」**という定理に含まれる。この定理の幾通りかの証明について、整理しておく。

0　基礎的な事項の整理

まずは、証明に使う基礎的な事項について述べておく。

命題 0.1　有限乗法群 G の元の個数が n であるとき (このとき、「群 G の位数は n である。」という)、G の任意の元 g について、$g^n = 1$ が成り立つ。

証明）$G = \{g_1, g_2, \cdots, g_n\}$ とする。$\forall g \in G,\quad gg_i = gg_j$ が成り立つとき、両辺に g^{-1} を掛けると $g_i = g_j$ であることがわかる。従って、$gg_1, gg_2, \cdots, gg_n$ は G の相異なる n 個の元であるから $g_1, g_2, \cdots, g_n$ を並び替えただけのものであると言える。故に $(gg_1)(gg_2)\cdot\cdots\cdot(gg_n) = g_1g_2\cdot\cdots\cdot g_n$ であるから、$g^n(g_1g_2\cdot\cdots\cdot g_n) = g_1g_2\cdot\cdots\cdot g_n$。

よって、$g^n = 1$ //

定義 0.2　有限乗法群 G の元 $g(\neq 1)$ が $g^k = 1,\quad g, g^2, \cdots, g^{k-1} \neq 1$ のとき、k を g の位数という。なお、1 の位数は 1 とする。

命題 0.3　g を有限群 G の元とする。g の位数 k は G の元の個数 $n =^{\#} G$ の約数である。

証明）$n = kq + r \qquad (q, r \in \mathbb{Z},\quad 0 \leqq r < k)$ を満たす q, r を取ることができる。

定理 0.1 より、$g^n = 1, \qquad g^{qk+r} = (g^k)^q \cdot g^r = 1, \qquad \therefore g^r = 1$。

もし、$0 < r < k$ であるとすると、k より小さい巾で 1 になることから、k が g の位数であることに反する。従って、$r = 0,\quad n = qk$。すなわち、k は n の約数である。//

命題 0.4　$g \in G$ の位数を k とする。$m \in \mathbb{N}\quad g^m = 1$ ならば、m は k の倍数である。

証明）$m = kq + r\quad (q, r \in \mathbb{Z},\quad 0 \leqq r < k)$ として、前の命題と同様に証明できる。//

定理 0.5　体 K の元を係数とする n 次方程式の K における解の個数は n 個以下である。

証明）

- $n = 1$ のとき

  $ax + b = 0 \quad (a \neq 0)$ の解は $x = -a^{-1}b$ で、解の個数は 1 個であるから定理は正しい。

- $n > 1$ のとき

  n 次の方程式 $f(x) = 0$ が 体 K に解をもたないときは、もちろん定理を満たす。

  $f(x) = 0$ が体 K 内に解 $x = k$ を持つとき、割り算を行って、

  $f(x) = (x - k)Q(x) \quad (Q(x)$ は $n - 1$ 以下の次数の K 係数の整式)

  とできる。このとき、 $Q(x) = 0$ の解の個数が $n - 1$ 以下であると仮定すると、$x(x) = 0$ が体 K 内に持つ解の個数が n 以下になるといえる。

数学的帰納法により、定理が成り立つことが示された。 //

1 G の位数 n の素因数分解から考える方法 その 1

G に含まれる元の位数は、 $n =^{\#} G$ の約数である。例えば、$G = \mathbb{F}_{13}^{\times} = \{1, 2, \cdots, 12\}$ の場合、$n = 12 = 2^2 \cdot 3$ であるから、$\mathbb{F}_{13}^{\times}$ の元の位数は $1, 2, 3, 4, 6, 12$ のいずれかである。

実際に各元の位数を調べてみると

g	1	2	3	4	5	6	7	8	9	10	11	12
位数	1	12	3	6	4	12	12	4	3	6	12	2

位数で分けてみると

位数	1	2	3	4	6	12
元	1	12	3, 9	5, 8	3, 10	2, 6, 7, 11

12 の約数のいずれについても、それを位数とする元がある。

一般に次の補題が成り立つ。

補題 1.1 $a \in G$ の位数を r とし、 d を r の約数とすると、 G には位数 d の元が存在する。

証明） $g = a^{\frac{r}{d}}$ とする。また、g の位数を t とする。 $g^d = a^r = 1$ 従って、命題 0.4 により、t は d の約数である。

t が d の約数のとき、命題 0.4 より、$d = tl \quad (l \in \mathbb{N})$ とできる。ここで、 d が r の約数で、 l は d の約数であるから、 l は r の約数である。

もし、 $l > 1$ であれば、$r' = \dfrac{r}{l}$ とおくとき、 $r' < r$ である。

$a^{r'} = a^{\frac{r}{l}} = (a^{\frac{r}{d}})^{\frac{d}{l}} = g^t = 1$ 。これは、r が a の位数であることに反する。(r より小さい r' 乗で 1 になってしまうから。)

従って、$l = 1$ で、 $t = d$ となるので g の位数は d である。すなわち、位数 d の元の存在が証明された。//

補題 1.2　$a, b \in G$ の位数をそれぞれ r, s とする。 r と s が互いに素であるとき、G に位数 rs の元が存在する。

証明） r と s の最大公約数 $gcd(r, s) = 1$ のとき、 最小公倍数 $lcm(r, s) = t$ とおくと、$t = rs$ である。また、 $c = ab$ とし、c の位数を u とする。

$c^t = (a^r)^s \cdot (b^s)^r = 1^s \cdot 1^r = 1$ 。命題 0.4 より、t は c の位数 u の倍数である。このとき、 $u \leqq t$　$\cdots$①

$c^{us} = a^{us}(b^s)^u = a^{us} \cdot 1^u = a^{us}$ 。また、$c^{us} = (c^u)^s = 1^s = 1$ 。

従って、$a^{us} = 1$ 。命題 0.4 より $r|us$ 。ここで $gcd(r, s) = 1$ であるから、$r|u$　$\cdots$② が成り立つ。

同様に、$c^{ur} = (a^r)^u b^{ur} = 1 \cdot b^{ur} = b^{ur}$ 。また、$c^{ur} = (c^u)^r = 1^r = 1$ 。

従って、$b^{ur} = 1$ 。命題 0.4 より $s|ur$ 。ここで $gcd(r, s) = 1$ であるから、$s|u$　$\cdots$③ が成り立つ。

②, ③ より、u は r, s の公倍数である。従って、u は $t = lcm(r, s)$ の倍数である。このとき、 $t \leqq u$　$\cdots$④

①, ④ より、$u = t$ 。すなわち、 r と s の最小公倍数 t を位数に持つ G の元 c が存在する。//

定理 1.3　$a, b \in G$ の位数をそれぞれ r, s とする。 また、$t = lcm(r, s)$ とする。 G には位数 t の元が存在する。

証明） r, s のいずれか、もしくは両方の素因数分解に現れる素数のすべてを $p_1, p_2, \cdots, p_k$ とする。また、$r = p_1^{e_1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$,　$s = p_1^{f_1} p_2^{f_2} \cdot \cdots \cdot p_k^{f_k}$　　$(e_j, f_j \geqq 0 \quad j = 1, 2, \cdots, k)$ とする。このとき、 $l_j = max(e_j, f_j)$ とおいて、$t = p_1^{l_1} p_2^{l_2} \cdot \cdots \cdot p_k^{l_k}$ が成り立つ。

補題 1.1 により、 r の約数 $p_j^{e_j}$ を位数に持つ G の元および s の約数 $p_j^{f_j}$ を位数に持つ G の元が存在する。従って、$p_j^{l_j}$ を位数に持つ G の元 c_j が存在する。

補題 1.2 を繰り返し適用することにより、$c = c_1 c_2 \cdot \cdots \cdot c_k$ は位数 $p_1^{l_1} p_2^{l_2} \cdot \cdots \cdot p_l^{l_k} = t$ の元である。//

定理 1.4　G には、位数 $n =^{\#} G$ の元が存在する。すなわち、 G は巡回群である。

証明）G の元の位数の最大値を r とする。（G は有限群であるから最大値が存在する。）$0 < r < n$ とするとき、 G の元で $x^r - 1 = 0$ を満たすものは r 個以下しかない。したがって、 G には r の約数ではない位数をもつ元がある。その元の位数を s とする。定理 1.3 により、 G には位数が $t = lcm(r, s)$ の元が存在する。s は r の約数ではないから、$t > r$ となる。それは、 r の最大性に反する。

これにより、 G の元の位数の最大値は n となる。g 位数が n の元であるとすると、$1, g, g^2, \cdots, g^{n-1}$ は相異なる n 個の元であるから、 G に含まれるすべての元を渡る。すなわち、 G は g によって生成される巡回群となる。//

2　G の位数 n の素因数分解から考える方法　その2

$n = p_1^{e_1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$ を n の素因数分解であるとする。

補題 2.1　$j = 1, 2, \cdots, k$ について、 G には位数 $p_j^{e_j}$ の元がある。

証明）　$p_j = p,\ e_j = e$ と略記する。$a^{p^e} = 1,\quad a^{p^{e-1}} \neq 1$ を満たす元を探す。

$\forall b \in G,\quad b^n = 1$ であるから、 $\left(b^{\frac{n}{p}}\right)^p = b^n = 1$

ところで、方程式 $x^{\frac{n}{p}} - 1 = 0$ は G の中に $\dfrac{n}{p}$ 個以下の解しか持たない。$\dfrac{n}{p} < n$ であるから、 G には $x^{\frac{n}{p}} - 1 = 0$ を満たさない元が存在する。その1つを b とする。

$b^{\frac{n}{p}} \neq 1 \quad \cdots \quad ①$

ここで、 $a = b^{\frac{n}{p^e}}$ とする。

$a^{p^e} = \left(b^{\frac{n}{p^e}}\right)^{p^e} = b^n = 1$。従って、$a$ の位数は p^e の約数である。p は素数なので、p^e の約数は $p^l \quad (0 \leqq l \leqq e)$ となる。位数が p^e であることを示すために、p^e の次に大きい巾 p^{e-1} について考える。

$a^{p^{e-1}} = \left(b^{\frac{n}{p^e}}\right)^{p^{e-1}} = b^{\frac{n}{p}} \neq 1 \quad (\because ①より)$。従って, 位数は p^e である。

再び添え字を付け、$a = a_j,\ p = p_j,\ e = e_j$ として、位数　$p_j^{e_j}$ の元 a_j が存在することが示された。 //

定理 2.2　G には位数 n の元がある。

証明）補題 2.1 の $a_j \quad (j = 1, 2, \cdots, k)$ を掛け合わせて $a = a_1 a_2 \cdot \cdots \cdot a_k$ とし、その位数を m とする。m は G の位数 n の約数である。 $n = ml$ で、 $l > 1$ と仮定して矛盾を導く。

l の素因数は、 n の素因数であるから、$p_1, p_2, \cdots, p_k$ の中に含まれる。必要なら番号をつけ直して、 l が p_1 を素因数を持つものとする。

このとき、$a^{\frac{n}{p_1}} = a^{m \cdot \frac{l}{p_1}} = 1$

一方、$\dfrac{n}{p_1} = p_1^{e_1 - 1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$ より、

$a^{\frac{n}{p_1}} = a_1^{p_1^{e_1-1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}} a_2^{p_1^{e_1-1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}} \cdot \cdots \cdot a_k^{p_1^{e_1-1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}}$

上の式で、$a_2, \cdots, a_k$ については、巾に $p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$ が含まれているので、1になる。

従って、 $1 = a_1^{p_1^{e_1-1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}}$　が成り立つ。

a_1 の位数が $p_1^{e_1}$ であることから、 $p_1^{e_1} \mid p_1^{e_1-1} p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$ とならなければならないが、それは不可能である。すなわち、 $l > 1$ と仮定すると矛盾が導かれる。

よって $l = 1$ で、 a の位数は n となる。すなわち、G には位数 n の元がある。 //

3　位数 d の元の個数を数える方法

G の位数を n とし、d を n の約数とする。

このとき、位数が d の元の個数は $\varphi(d) =^{\#} \{1 \leqq x \leqq d \mid gcd(x, d) = 1\}$　(d 以下の自然数で、d と互いに素であるものの個数) であることを示す。

例えば、第1節で $\mathbb{F}_{13}^{\times}$ の元を位数で分けた表を再掲すると

位数	1	2	3	4	6	12
元	1	12	3, 9	5, 8	3, 10	2, 6, 7, 11

$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(6) = 2, \varphi(12) = 4$ で、「位数が d である元の個数は $\varphi(d)$ である」が成り立っている。

特に、位数が n である元の個数が $\varphi(n) \geqq 1$ であるから、主張が正しいことが示されるのである。このことについて、順次示していく。

補題 3.1　d を G の位数 n の約数とする。このとき、$^{\#}\{x \in G \mid x^d - 1 = 0\} = d$ が成り立つ。

証明）$n = kd$ とおくと、 $x^n - 1 = (x^d - 1)(x^{(k-1)d} + x^{(k-2)d} + \cdots + x^d + 1)$

G の n 個の元はすべて $x^n - 1 = 0$ を満たす。すなわち、$x^n - 1 = 0$ は異なる n 個の解を G の中に持つ。従って、上記の等式により、$(x^d-1)(x^{(k-1)d}+x^{(k-2)d}+\cdots+x^d+1) = 0$ は異なる n 個の解を G の中に持つ。

一方、2つの方程式 $x^d - 1 = 0, \quad x^{(k-1)d} + x^{(k-2)d} + \cdots + x^d + 1 = 0$ の解の個数は、定理 0.5 により、それぞれ、 $d, \quad (k-1)d$ 以下である。

$\therefore \quad (x^d - 1)(x^{(k-1)d} + x^{(k-2)d} + \cdots + x^d + 1) = 0$ の解の個数 $\leqq d + (k-1)d = kd \leqq n$ 。

以上のことから、$n \leqq d+(k-1)d = kd = n$ 。これが成り立つには、不等号のところで等号が成立していなければならないので、$x^d-1 = 0, \quad x^d-1)(x^{(k-1)d}+x^{(k-2)d}+\cdots+x^d+1 = 0$ の解の個数 a はそれぞれ、 $d, \quad (k-1)d$ とならなければならない。よって、補題は示された。//

G の元で位数が e のものの個数を $f(e)$ で表す。

G の元で $x^d - 1 = 0$ を満たすものの位数は d の約数であり、逆に位数が d の約数である G の元は $x^d - 1 = 0$ を満たす。

以上により、

$$d =^{\#} \{x \in G \mid x^d - 1 = 0\} = \sum_{e|d} f(e)$$

が成り立つ。

この式から $f(e) = \varphi(e)$ を導くには、 $\varphi(e)$ の満たす性質、およびメビウスの反転公式を用いる。それについて述べる。

補題 3.2　すべての $n \in \mathbb{N}$ について、$\sum_{d|n} \varphi(d) = n$ が成り立つ。

証明）　いくつかの Claim を重ねて証明する。

Claim3.2.1　d を n の約数とする。

$M_d = \{1 \leqq a \leqq n \mid gcd(a, n) = d\}, \quad N_d = \left\{1 \leqq a \leqq n \mid \quad d|a \text{ かつ } gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1\right\}$ とおくと、 $M_d = N_d$　が成り立つ。

証明）　$a \in M_d \quad \Longrightarrow \quad {}^{\exists}a', n' \in \mathbb{N} \quad s.t. \quad a = a'd, n = n'd \quad gcd(a', n') = 1$

$$\Longrightarrow \quad d|a \quad \text{かつ} \quad gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \quad \Longrightarrow \quad a \in N_d \qquad \therefore M_d \subset N_d$$

$$a \in N_d \quad \Longrightarrow \quad a' = \frac{a}{d}, n' = \frac{n}{d} \text{ とおいて、} a = a'd, n = n'd, \quad gcd(a', n') = 1$$

$$\Longrightarrow \quad 1 \leqq a \leqq n, \quad gcd(a, n) = d \quad \Longrightarrow \quad a \in M_d \qquad \therefore N_d \subset M_d$$

以上により、 $M_d = N_d$ //

Claim3.2.2 $\quad \sum_{d|n}{}^{\#} M_d = n$

証明） 定義から、 $d \neq d' \quad \Longrightarrow \quad M_d \cap N_{d'} = \emptyset$

$1 \leqq a \leqq n$ のとき、n の約数 d が唯一つ決まって、 $a \in M_d$ となる。

これらのことから、$\{a \mid 1 \leqq a \leqq n\} = \bigcup_{d|n} M_d$ であり、この和は共通項を持たない和である。 従って、$n = \sum_{d|n}^{\#} M_d$ //

Claim3.2.3 $\quad {}^{\#}N_d = \varphi\left(\frac{n}{d}\right)$

証明） $e \in \mathbb{N}$ について、 $L_e = \{1 \leqq x \leqq e \mid gcd(x, e) = 1\}$ とする。

$a \in N_d$ のとき、 $a' = \frac{n}{d}$ とおくと、 $1 \leqq a' \leqq \frac{n}{d}, \quad gcd\left(a', \frac{n}{d}\right) = 1$ となる。

$\therefore \quad a' \in L_{\frac{n}{d}}$

$a' \in L_{\frac{n}{d}}$ のとき、$a = a'd$ とすると、$a \in N_d$ となることは明らかである。

従って、N_d の元 a に $L_{\frac{n}{d}}$ の元 $a' = \frac{a}{d}$ を対応させる写像は、N_d から $L_{\frac{n}{d}}$ への全単射である。よって ${}^{\#}N_d = {}^{\#} L_{\frac{n}{d}}$

${}^{\#}L_{\frac{n}{d}} = \varphi\left(\frac{n}{d}\right)$ であるから Claim は証明された。 //

補題 3.2 の証明

Claim3.2.1 ～Claim3.2.3 より

$$n = \sum_{d|n} {}^{\#}M_d = \sum_{d|n} {}^{\#}N_d = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$$

ここで、 d が n の約数全体を動くとき $e = \frac{n}{d}$ と対応させると、 e は n の約数全体を動く。従って、最後の和を書き換えて、$n = \sum_{e|n} \varphi(e)$ とできる。 最後の和の値は $\sum_{d|n} \varphi(d)$ と同じである。従って補題は示された。 //

定義 3.3 自然数を定義域とする関数 $\mu(n)$ を次で定義する。（**メビウス関数**と呼ぶ）

$$\mu(n) = \begin{cases} 1 & (n = 1 \text{ のとき}) \\ (-1)^k & (n \text{ が相異なる } k \text{ 個の素数の積のとき}) \\ 0 & (n \text{ がある素数の } 2 \text{ 乗で割り切れるとき}) \end{cases}$$

補題 3.4 $\quad n \geqq 2$ のとき、$\sum_{d|n} \mu(d) = 0$

証明）d がある素数の 2 乗で割り切れるとき、$\mu(d) = 0$ となることから、この補題を $n = p_1 p_2 \cdot \cdots \cdot p_k$ （相異なる k 個の素数の積）の時に示せばよい。

$f(x_1, x_2, \cdots, x_k) = (1 - x_1)(1 - x_2) \cdot \cdots \cdot (1 - x_k)$ とおく。

n の約数 d は、$d = p_{j_1} p_{j_2} \cdot \cdots \cdot p_{j_m}$ の形に表されるので、それに変数 $x_{j_1} x_{j_2} \cdot \cdots \cdot x_{j_m}$ を対応させ、$(d) = x_{j_1} x_{j_2} \cdot \cdots \cdot x_{j_m}$ とする。

$$\begin{aligned} & f(x_1, x_2, \cdots, x_k) \\ & \quad = 1 - (x_1 + x_2 + \cdots + x_k) + (x_1 x_2 + x_1 x_3 + \cdots + x_{k-1} x_k) + \cdots + (-1)^k x_1 x_2 \cdots x_k \\ & \quad = \sum_{d|n} \mu(d) P(d) \end{aligned}$$

$x_1 = x_2 = \cdots = x_k = 1$ とすると、任意の d について $P(d) = 1$ であるから、

$$0 = f(1, 1, \cdots, 1) = \sum_{d|n} \mu(d) \quad //$$

定理 3.5　（メビウスの反転公式）

自然数を定義域にもつ 2 つの関数 $f(x)$, $g(x)$ について、次が成り立つ。

$$\forall n \in \mathbb{N} \text{ について } g(n) = \sum_{d|n} f(d) \quad \Longleftrightarrow \quad \forall n \in \mathbb{N} \text{ について } f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

証明）

$$\Longrightarrow) \quad \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{e|d} f(e) = \sum_{e|n} \left(\sum_{h|\frac{n}{e}} \mu(h) \right) f(e) \quad \cdots ①$$

$$\text{内側の和} = \sum_{h|\frac{n}{e}} \mu(h) = \begin{cases} 1 & \left(\frac{n}{e} = 1 \text{ のとき}\right) \\ 0 & \left(\frac{n}{e} > 1 \text{ のとき}\right) \end{cases}$$

となるので、$① = f(n) \quad //$

$$\Longleftarrow) \quad \sum_{d|n} f(d) = \sum_{d|n} \sum_{e|d} \mu\left(\frac{d}{e}\right) g(e) = \sum_{e|n} \left(\sum_{h|\frac{n}{e}} \mu(h) \right) g(e) = g(n) \quad //$$

定理 3.6　d を G の位数 n の約数とする。G の元で位数が d であるものの個数は $\varphi(d)$ である。特に、位数が n であるものが $\varphi(n)(\geqq 1)$ 個あることから、G は巡回群となる。

証明）補題 3.2 にメビウスの反転公式を適用すると、$\varphi(d) = \sum_{e|d} \mu\left(\frac{d}{e}\right) e$

G の元で位数が e のものの個数を $f(e)$ で表すと、n の約数 d について、$d = \sum_{e|d} f(e)$ が成り立つのであった。メビウスの反転公式より、$f(d) = \sum_{e|d} \mu\left(\frac{d}{e}\right) e$

以上より、 $f(d)=\varphi(d)$ が成り立つ。

特に、$f(n)=\varphi(n)\geqq 1$ である。従って、 G の中に位数 n の元が存在する。すなわち G は巡回群である。　//

4　有限生成アーベル群の基底定理を用いる方法

有限生成アーベル群について、次の定理が成り立つことが知られている。

定理 4.1　　**（有限生成アーベル群の基底定理）**

G が有限生成アーベル群であるとき、次の同型が成り立つ。

$$G\cong(\mathbb{Z}/d_1\mathbb{Z})\otimes(\mathbb{Z}/d_2\mathbb{Z})\otimes\ \cdots\otimes(\mathbb{Z}/d_r\mathbb{Z})\otimes\mathbb{Z}\otimes\ \cdots\ \otimes\mathbb{Z}$$

$$\text{ここで、}d_1,\,d_2,\cdots,d_r\in\mathbb{N}\quad d_j|d_{j+1}\quad(j=1,2,\cdots,r-1)$$

注意：G が有限アーベル群の場合は、$G\cong(\mathbb{Z}/d_1\mathbb{Z})\otimes(\mathbb{Z}/d_2\mathbb{Z})\otimes\ \cdots\otimes(\mathbb{Z}/d_r\mathbb{Z})$

また、$G\cong\mathbb{Z}\otimes\ \cdots\ \otimes\mathbb{Z}$ となる場合もある。

定理 4.1 の証明は後回しにして、それを用いて次の結論を得る。

定理 4.2　G が可換体 K に含まれる有限乗法群ならば、G は巡回群である。

証明）G は有限生成の有限群であるから、有限生成アーベル群の基底定理により、

$$G\cong(\mathbb{Z}/d_1\mathbb{Z})\otimes(\mathbb{Z}/d_2\mathbb{Z})\otimes\cdots\otimes(\mathbb{Z}/d_r\mathbb{Z})\qquad d_1,\,d_2,\cdots,d_r\in\mathbb{N}\quad d_j|d_{j+1}\quad(j=1,2,\cdots,r-1)$$

とできる。ここで $d_1d_2\cdot\ \ \cdots\ \ \cdot d_r=^{\#}G$ である。

一方、$(\mathbb{Z}/d_1\mathbb{Z})\otimes(\mathbb{Z}/d_2\mathbb{Z})\otimes\ \cdots\otimes(\mathbb{Z}/d_r\mathbb{Z})$ の元はすべて $x^{d_r}-1=0$ をみたす。この方程式の解の個数は d_r 以下である。しかるに、$r>1$ のとき $d_r<n$ であるから、矛盾が起こる。よって、$r=1$ であり、$G\cong(\mathbb{Z}/d_1\mathbb{Z})$ となるから、 G は巡回群である。//

有限生成アーベル群の基底定理のいくつかの証明については、別のレポートで自分の学習のためにまとめておく。