有限生成アーベル群の基底定理について

2020 年 6 月
石動高校　片山　喜美

「可換体に含まれる乗法有限部分群（例えば $\mathbb{F}_p^{\times}$）が巡回群になることについて」というレポートで、「有限生成アーベル群の基底定理」を用いた証明にも触れた。「有限生成アーベル群の基底定理」の 2 つの証明をメモしておく。

1　有限生成アーベル群の基底定理の証明　その 1

松村英之　著「代数学」（朝倉書店　数理科学ライブラリー）による証明を以下に記載する。なお、アーベル群の群演算を加法で記載する。従って、次の形の定理を証明する。

有限生成アーベル群の基底定理

G を有限生成アーベル群とすると、次が成り立つ。

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

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

とできる。

定義 1.1　G をアーベル群とする。G の元 $e_1, e_2, \cdots, e_n$ が一次独立であるとは、
$a_1e_1 + a_2e_2 + \cdots + a_ne_n = 0 \quad (a_1, \cdots, a_n \in \mathbb{Z}) \quad \Longrightarrow \quad a_1 = a_2 = \cdots = a_n = 0$
が成り立つこととする。

定義 1.2　G をアーベル群とする。G の元 $e_1, e_2, \cdots, e_n$ が G の基底であるとは、次をみたすこととする。

- $e_1, e_2, \cdots, e_n$ は G を生成する。
- $e_1, e_2, \cdots, e_n$ は一次独立である。

補題 1.3　$e_1, e_2, \cdots, e_n$ が G の基底であるとき、G の任意の元 x は
$x = a_1e_1 + a_2e_2 + \cdots + a_ne_n \quad (a_1, a_2, \cdots, a_n \in \mathbb{Z})$ の形に一通りに表される。

証明）$e_1, e_2, \cdots, e_n$ は基底であることから、x をそのような形に表すことができる。
一意性を示す。
$x = a_1'e_1 + a_2'e_2 + \cdots + a_n'e_n \quad (a_1', a_2', \cdots, a_n' \in \mathbb{Z})$ とも表せたとする。
差し引いて、$0 = (a_1 - a_1')e_1 + (a_2 - a_2')e_2 + \cdots + (a_n - a_n')e_n$
一次独立性より、$a_1 - a_1' = 0, a_2 - a_2 = 0, \cdots, a_n - a_n' = 0$
以上により、x を表す方法は一通りである。//

補題 1.4　$\mathbb{Z}^r$　$(r \in \mathbb{N})$ に同型な群を**自由アーベル群**という。r をその群の**階数**という。

定理 1.5　G ： 階数 r の自由アーベル群、$e_1, e_2, \quad \cdots \quad , e_r$ を G の基底とする。
整数 $a_1, a_2, \quad \cdots \quad , a_r$ について、その最大公約数 $gcd(a_1, a_2, \quad \cdots \quad , a_r)$ が 1 ならば、$e'_1 = a_1e_1 + a_2e_2 + \quad \cdots \quad + a_re_r$ を一員とする G の基底 $e'_1, e'_2, \quad \cdots \quad , e'_r$ が存在する。

証明）r に関する数学的帰納法で示す。

- $r = 1$ のとき

  $G =< e_1 >, a_1 = \pm 1$ であるから、定理は成り立つ。

- $r > 1$ のとき

  $d = gcd(a_2, \quad \cdots \quad , a_r), \quad a_2 = a'_2d, \quad \cdots \quad , a_n = a'_nd$ とする。

  このとき、$gcd(a'_2, \quad \cdots \quad , a'_r) = 1$ であるから、数学的帰納法の仮定より、

  $f_2 = a'_2e_2 + a'_3e_3 + \quad \cdots \quad + a'_re_r$ を一員とする $< e_2, \quad \cdots \quad , e_n >$ の基底 $f_2, \quad \cdots \quad , f_r$ が存在する。このとき、$a_1e_1 + df_2 = e'_1$ が成り立つ。

  ここで、$gcd(a_1, d) = 1$ であるから、 $\exists s, t \in \mathbb{Z}$ s.t. $se_1 + td = 1$ 。

  $$det \begin{pmatrix} a_1 & d \\ -t & s \end{pmatrix} = sa_1 + td = 1$$

であることに注意して、 $e'_2 = -te_1 + sf_2$ とおく。
$se'_1 - de'_2 = s(a_1e_1 + df_2) - d(-te_1 + sf_2) = (sa_1 + td)e_1 + (sd - sd)f_2 = e_1$
$te_1 + a_1e'_2 = t(a_1e_1 + df_2) + a_1(-te_1 + sf_2) = (ta_1 - ta_1)e_1 + (td + sa_1)f_2 = f_2$
と逆に戻れる。従って、$< e_1, f_2 >=< e'_1, e'_2 >$
よって、$G =< e_1, f_2, f_3, \quad \cdots \quad , f_r >=< e'_1, e'_2, f_3, \quad \cdots \quad , f_r >$
ここで、 $e'_3 = f_3, \quad \cdots \quad , e'_r = f_r$ と名前を付け替えると、$e'_1, e'_2, \quad \cdots \quad , e'_n$ が G の基底となることから、定理が成り立つ。//

定義 1.6　G ： 階数 r の自由アーベル群、$e_1, e_2, \quad \cdots \quad , e_r$ はその基底であるとする。
$x \in G$ が $x = a_1e_1 + a_2e_2 + \quad \cdots \quad + a_re_r \quad (a_1, a_2, \quad \cdots \quad , a_r \in \mathbb{Z})$ と表されるとき、$\delta(x) = gcd(a_1, a_2, \quad \cdots \quad , a_r)$ と定義し、「x の大きさ」と呼ぶ。

注意　$\delta(x)$ は基底の選び方によらず、1 つの値として定まる。

証明)$e'_1, e'_2, \quad \cdots \quad , e'_r$ も基底で、$x = a'_1e'_1 + a'_2e'_2 + \quad \cdots \quad + a'_re'_r \quad (a'_1, a'_2, \quad \cdots \quad , a'_r \in \mathbb{Z})$ と表されるものとする。また、$gcd(a_1, a_2, \quad \cdots \quad , a_r) = d$, $gcd((a'_1, a'_2, \quad \cdots \quad , a'_r) = d'$ とする。

$u_{ij} \in \mathbb{Z} \quad (1 \leqq i, j \leqq r)$ が存在して、$e'_i = \sum_{j=1}^{r} u_{ij}e_j$ とできるから、

$$x = \sum_{i=1}^{r} a'_ie'_i = \sum_{i=1}^{r} a'_i \left(\sum_{j=1}^{r} u_{ij}e_j \right) = \sum_{j=1}^{r} \left(\sum_{i=1}^{r} a'_iu_{ij} \right) e_j$$

$\therefore \quad a_j = \sum_{i=1}^{r} a'_i u_{ij}$ となり、$d'|a_j \quad (j = 1, 2, \quad \cdots \quad , r)$ が言える。従って、$d'|d$

全く同様に、$d|a'_j \quad (j = 1, 2, \quad \cdots \quad , r)$、$d|d'$ が言えるので、$d = d'$ //

定理 1.7　G : 階数 r の自由アーベル群、G' を G の部分群とするとき、$0 \leqq r' \leqq r$ をみたす整数 r 、$d_1|d_2, d_2|d_3, \quad \cdots \quad , d_{r'-1}|d_{r'}$ をみたす自然数 $d_1, d_2, \quad \cdots \quad , d_{r'}$ 及び G の基底 $f_1, f_2, \quad \cdots \quad , f_r$ が存在して、$G' =< d_1 f_1, d_2 f_2, \quad \cdots \quad , d_{r'} f_{r'} >$ となる。

証明）$G' = \phi$ のとき、自明である。$G' \neq \phi$ として、r に関する数学的帰納法で示す。

- $r = 1$ のとき

  $G =< e_1 >, G' =< d_1 e_1 >$ となるから、定理は成立する。

- $r > 1$ のとき

  $min\{\delta(x) \mid x \in G'\} = d_1, \quad \delta(x_1) = d_1 \quad (x_1 \in G')$ とする。

  ここで、$x_1 = a_1 e_1 + a_2 e_2 + \quad \cdots \quad + a_r e_r$ とすると、$gcd(a_1, a_2, \quad \cdots \quad , a_r) = d_1$ である。

  $a_1 = a'_1 d_1, a_2 = a'_2 d_1, \quad \cdots \quad , a_r = a'_r d_1$ とすると、$gcd(a'_1, a'_2, \quad \cdots \quad , a'_r) = 1$ である。

  定理1.5 より、$e'_1 = a'_1 e_1 + a'_2 e_2 + \quad \cdots \quad + a'_r e_r$ を一員とする G の基底 $e'_1, e'_2, \quad \cdots \quad , e'_r$ が存在する。このとき、$d_1 e'_1 = x_1$ である。

  $y = c_1 e'_1 + c_2 e'_2 + \quad \cdots \quad + c_r e'_r$ を G' の任意の元とする。

  Claim 1　c_1 は d_1 の倍数である。

  $\because$)　　$gcd(d_1, c_1) = d$ とする。$d|d_1 \quad \cdots$ ① が成り立つ。

  $\exists s, t \in \mathbb{Z} \quad s.t. \quad sd_1 + tc_1 = d$

  $sx_1 + ty = (sd_1 + tc_1)e'_1 + tc_2 e'_2 + \quad \cdots \quad + tc_r e'_r$

  $\qquad = de'_1 + tc_2 e'_2 + \quad \cdots \quad + tc_r e'_r$

  d_1 の最小性より、$d_1 \leqq d \quad \cdots$ ②

  ①, ② より、$d_1 = d = gcd(d_1, c_1)$ 。よって、$d_1|c_1$ //

  $c_1 = qd_1 \quad (q \in \mathbb{Z})$ とすると、$y - qx_1 = c_2 e'_2 + \quad \cdots \quad + c_r e'_r \in G' \cap < e'_2, \quad \cdots \quad , e'_r >$

  従って、$G'' = G' \cap < e'_2, \quad \cdots \quad , e'_r >$ とおくと、$G' =< d_1 e'_1 > \oplus G''$

  $G'' = \phi$ ならば定理は成立する。$G'' \neq \phi$ のとき、数学的帰納法の仮定より、$2 \leqq r' \leqq r$ をみたす自然数 r' 、$< e'_2, \quad \cdots \quad , e'_r >$ の基底 $< f_2, \quad \cdots \quad , f_r >$ 、$d_2|d_3, d_3|d_4, \quad \cdots \quad , d_{r'-1}|d_{r'}$ をみたす自然数 $d_2, \quad \cdots \quad , d_{r'}$ が存在して

  $G'' =< d_2 f_2, d_3 f_3, \quad \cdots \quad , d_{r'} f_{r'} >$ が成り立つ。

  従って、$G' =< d_1 e'_1, d_2 f_2, d_3 f_3, \quad \cdots \quad , d_{r'} f_{r'} >$

Claim 2　$d_1|d_2$ である。

$\because$)　　$gcd(d_1, d_2) = d$ とする。$d|d_1$　　$\cdots$ ① が成り立つ。

$\delta(d_1e_1' + d_2f_2) = d$ である。d_1 の最小性より、 $d_1 \leqq d$　　$\cdots$ ②

①, ② より、$d_1 = d = gcd(d_1, d_1)$ 。よって、$d_1|d_2$ //

この Claim により、$e_1' = f_1$ とすれば、 r のときの定理が成り立つことが言える。

数学的帰納法により、定理は正しいことが証明された。（証明終）

定理 1.8　有限生成アーベル群の基底定理

G を有限生成アーベル群とすると、次が成り立つ。

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

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

とできる。

証明）$x_1, x_2, \quad \cdots \quad x_s$ を G の生成元とする。また、F を階数 s の自由アーベル群、$e_1, e_2, \quad \cdots \quad e_s$ を F の基底とする。このとき、$\varphi : F \to G$ を $\varphi(e_j) = x_j$ で定める。φ は全射である。従って、$Ker(\varphi) = K$ とすると、 $G \cong F/K$ が成り立つ。

定理1.7を F, K に適用すると、$0 \leqq s' \leqq s$ をみたす整数 s 、$d_1|d_2$, $d_2|d_3$, $\quad \cdots \quad$, $d_{s'-1}|d_{s'}$ をみたす自然数 $d_1, d_2, \quad \cdots \quad , d_{s'}$ 及び F の基底 $f_1, f_2, \quad \cdots \quad , f_s$ が存在して、$K =< d_1f_1, d_2f_2, \quad \cdots \quad , d_{s'}f_{s'} >$ となる。

$F \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \quad \cdots \quad \oplus \mathbb{Z}$, $\quad K \cong d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \quad \cdots \quad \oplus d_{s'}\mathbb{Z}$ であるから、

$F/K \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus (\mathbb{Z}/d_2\mathbb{Z}) \oplus \quad \cdots \quad \oplus (\mathbb{Z}/d_{s'}\mathbb{Z}) \oplus \mathbb{Z} \oplus \quad \cdots \quad \oplus \mathbb{Z}$ となる。

このとき、$d_j = 1$ ならば、 $\mathbb{Z}/d_j\mathbb{Z} = \{0\}$ となり、同型右辺の直和から消える。このことを踏まえ、 $d_1, d_2, \quad \cdots \quad , d_{s'}$ のうち、1 ではないものが r 個であるとし、それらを記号をつけ直して $d_1, d_2, \quad \cdots \quad , d_r$ とすれば、

$F/K \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus (\mathbb{Z}/d_2\mathbb{Z}) \oplus \quad \cdots \quad \oplus (\mathbb{Z}/d_r\mathbb{Z}) \oplus \mathbb{Z} \oplus \quad \cdots \quad \oplus \mathbb{Z}$ となる。（ただし、$\mathbb{Z}$ の部分は $s - s'$ 個の直和である。）

以上で定理が証明された。//

2　有限生成アーベル群の基底定理の証明　その2

アルティン「ガロア理論入門」　寺田文行　訳　東京図書株式会社　による証明をメモする。

G をアーベル群として、群演算は加法で書き表すものとする。

定義 2.1　G の元 $e_1, e_2, \quad \cdots \quad , e_k$ が
bf G を生成するとは、

G の任意の元 x に対して、$a_1, a_2, \quad \cdots \quad , a_k \in \mathbb{Z}$ があって、

$x = a_1e_1 + a_2e_2 + \quad \cdots \quad + a_ke_k$ と書き表すことができることである。

定義 2.2

- G の元 $e_1, e_2, \quad \cdots \quad , e_k$ が**一次独立**であるとは、

  $a_1e_1 + a_2e_2 + \quad \cdots \quad + a_ke_k = 0 \implies a_1 = a_2 = \quad \cdots \quad = a_k = 0$

  が成り立つこととする。

  係数がすべて 0 の式を**自明な関係式** という。

- $e_1, e_2, \quad \cdots \quad , e_k$ が一次独立な G の生成元であるとき、$e_1, e_2, \quad \cdots \quad , e_k$ を G **の基底（basis)** という。

- G の元 $e_1, e_2, \quad \cdots \quad , e_k$ が一次独立でないとき、$e_1, e_2, \quad \cdots \quad , e_k$ は**一次従属**であるという。

  このとき、$a_1e_1 + a_2e_2 + \quad \cdots \quad + a_ke_k = 0$ かつ $a_1, a_2, \quad \cdots \quad , a_k$ の中に 0 と異なるものがある。このような式を**非自明な関係式**という。

補題 2.3 $e_1, e_2, \quad \cdots \quad , e_k$ が G の基底 (basis) であるとき、$x \in G$ の $e_1, e_2, \quad \cdots \quad , e_k$ による表し方は一通りである。

証明） $x = a_1e_1 + a_2e_2 + \quad \cdots \quad + a_ke_k = b_1e_1 + b_2e_2 + \quad \cdots \quad + b_ke_k$ であったとする。
$(a_1 - b_1)e_1 + (a_2 - b_2)e_2 + \quad \cdots \quad + (a_k - b_k)e_k = 0$
となるが、$e_1, e_2, \quad \cdots \quad , e_k$ が一次独立であるから、係数は全て 0 である。
よって、 $a_1 = b_1, a_2 = b_2, \quad \cdots \quad , a_k = b_k$ が従うので、表し方は一通りである。//

定義 2.4 （極小生成元）
G の元 $e_1, e_2, \quad \cdots \quad , e_k$ が G の生成元で、かつ、$k-1$ 個以下の G の元では G を生成できないとき、$e_1, e_2, \quad \cdots \quad , e_k$ を G **の極小生成元** という。

命題 2.5 $e_1, e_2, \quad \cdots \quad , e_k$ が G の生成元ならば、$e_1 + me_j, e_2, \quad \cdots \quad , e_k \quad (j = 2, 3, \cdots, k \quad m \in \mathbb{Z})$ も G の生成元である。

証明） $j = 2$ の場合に示す。他の j の場合も同様である。
$x = a_1e_1 + a_2e_2 + a_3e_3 + \quad \cdots \quad + a_ke_k$ のとき、
$x = a_1(e_1 + me_2) + (a_2 - a_1m)e_2 + a_3e_3 + \quad \cdots \quad + a_ke_k$
となるので、$e_1 + me_2, e_2, \quad \cdots \quad , e_k \quad (m \in \mathbb{Z})$ も G の生成元である。//

定義 2.6 G がその部分群 $G_1, G_2, \quad \cdots \quad , G_k$ の直和であるとは、G の任意の元 x に対して、$x_j \in G_j \quad (j = 1, 2, \quad \cdots \quad , k)$ が存在して、$x = x_1 + x_2 + \quad \cdots \quad + x_k$ の形に一意的に表されることをいう。
このとき、 $G = G_1 \oplus G_2 \oplus \quad \cdots \quad \oplus G_k$ と書く。

ここで、アーベル群 G が一次従属な極小生成元 $e_1, e_2, \quad \cdots \quad , e_k$ を持つ場合について考える。

全ての極小生成元について非自明な関係式を考え、その中で最小正の係数が現れるものが、極小生成元 $e_1, e_2, \quad \cdots \quad , e_k$ に関する関係式 $m_1e_1 + m_2e_2 + \quad \cdots \quad + m_ke_k = 0 \quad (m_1, m_2, \cdots, m_k \in \mathbb{Z})$ であるとする。必要なら番号をつけ直して、最小正の係数は m_1 であるとする。

補題 2.7　最小正の係数 m_1 が現れる非自明な関係式 $m_1e_1 + m_2e_2 + \quad \cdots \quad + m_ke_k = 0$ の係数について、 $m_1|m_j \quad (j = 2, 3, \cdots, k)$ が成り立つ。

証明） $j = 2$ の場合に示す。他の j の場合も同様である。

$m_2 = m_1q + r \quad (0 \leqq r < m_1)$ をみたす整数 q, r が存在する。

$0 = m_1e_1 + m_2e_2 + \quad \cdots \quad + m_ke_k = m_1e_1 + (m_1q + r)e_2 + m_3e_3 + \quad \cdots \quad + m_ke_k$

$= m_1(e_1 + qe_2) + re_2 + m_3e_3 + \quad \cdots \quad + m_ke_k$

もし、 $0 < r < m_1$ であったならば、m_1 が最小正の係数であることに反する。従って、$r = 0$ である。すると、 $m_2 = m_1q$ となるので、 $m_1|m_2$ である。//

補題 2.8　$n_1e_1 + n_2e_2 + \quad \cdots \quad + n_ke_k = 0$ が成り立つとき、 $m_1|n_1 \quad (j = 2, 3, \cdots, k)$ が成り立つ。

証明） $n_1 = m_1q + r \quad (0 \leqq r < m_1)$ をみたす整数 q, r が存在する。

$(n_1e_1 + n_2e_2 + \quad \cdots \quad + n_ke_k) - q(m_1e_1 + m_2e_2 + \quad \cdots \quad + m_ke_k) = 0$

$re_1 + (n_2 - qm_2)e_2 + (n_3 - qm_3)e_3 + \quad \cdots \quad + (n_k - qm_k)e_k = 0$

もし、 $0 < r < m_1$ であったならば、m_1 が最小正の係数であることに反する。従って、$r = 0$ である。すると、 $n_1 = m_1q$ となるので、 $m_1|m_2$ である。//

定理 2.9　（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のとき、 $G = G_1 \oplus G_2 \oplus \quad \cdots \quad \oplus G_k$

ただし、

- k は G の極小生成元の個数
- $G_1, \quad \cdots \quad G_k$ のうち $G_1, \quad \cdots \quad G_r$ は有限巡回群で、$^{\#}G_1 = d_1, \quad \cdots \quad , ^{\#}G_r = d_r$ とするとき $d_j|d_{j+1} \quad (j = 1, 2, \cdots, r-1)$
- $G_{r+1}, \quad \cdots \quad , G_k \cong \mathbb{Z}$

である。

※　$r = 0$ の場合もある。このとき、$G \cong \mathbb{Z}^k$ である。

証明）G の極小生成元の個数 k に関する数学的帰納法により証明する。

・ $k = 1$ のとき、G 自身が巡回群であるから正しい。

・$k>1$ のとき　　$e_1,' e_2,\quad \cdots \quad ,e_k$ を G の極小生成元とする。

（ i ）　$e_1,' e_2,\quad \cdots \quad ,e_k$ が一次独立のとき

$G \cong \mathbb{Z}\oplus\mathbb{Z}\oplus \quad \cdots \quad \oplus\mathbb{Z} = \mathbb{Z}^k$ となるから定理は成立する。

（ ii ）$e_1,' e_2,\quad \cdots \quad ,e_k$ が一次従属のとき

全ての極小生成元について非自明な関係式を考え、その中に現れる最小正の係数が m_1 でそれが現れるものが、極小生成元 $e_1, e_2,\quad \cdots \quad ,e_k$ に関する関係式 $m_1e_1 + m_2e_2 + \quad \cdots \quad + m_ke_k = 0 \quad (m_1, m_2, \cdots, m_k \in \mathbb{Z})$ であるとする。

補題 2.7 より、 $m_j = q_jm_1 \quad (q_j \in \mathbb{Z},\ j = 2, 3, \cdots, k)$ とできるので、

ここで、 $\overline{e_1} = e_1 + q_2e_2 + \quad \cdots \quad + q_ke_k$ とおくと、 $\overline{e_1}, e_2,\quad \cdots \quad ,e_k$ は極小生成元である。

また、$m_1\overline{e_1} = 0$ である。

Claim 1　$n_1\overline{e_1} + n_2e_2 + \quad \cdots \quad + n_ke_k = 0 \implies n_1\overline{e_1} = 0$ が成り立つ。

証明）条件式の $\overline{e_1}$ を $e_1,\quad \cdots \quad ,e_k$ で書き表して補題 2.8 を適用すると、 $n_1 = qm_1 \quad (q \in \mathbb{Z})$ とおける。従って、$n_1\overline{e_1} = qm_1\overline{e_1} = 0 \quad //$

Claim 2　$G_1 =< \overline{e_1} >$ は $\overline{e_1}$ で生成される位数 m_1 の巡回群である。

証明） $m_1(e_1 + q_2e_2 + \quad \cdots \quad + q_ke_k) = 0$ が成り立つことは、$\overline{e_1}$ の定義から従う。$0 < n < m_1$ を満たす整数 n が $n\overline{e_1} = 0$ を満たすとすると、$\overline{e_1}$ を $e_1,\quad \cdots \quad ,e_k$ で書き表して、m_1 の最小性に反することがわかる。以上で Claim は正しい。　//

$G_1 =< \overline{e_1} >,\quad G' =< e_2,\quad \cdots \quad ,e_k >$ とする。

Claim 3　$G = G_1 \oplus G'$ （直和）である。

証明）$\forall x \in G$ について、 $x = a_1\overline{e_1} + a_2e_2 + \quad \cdots \quad + a_ke_k = a_1\overline{e_1} + g' \quad (a_1\overline{e_1} \in G_1,\ g' \in G')$ とできる。

$x = a_1\overline{e_1} + g' = a_1'\overline{e_1} + g''$ であるとすると、$(a_1 - a_1')\overline{e_1} + (g' - g'') = 0$

Claim 1 により、$(a_1 - a_1')\overline{e_1} = 0$ となる。すると $g' - g'' = 0$ となる。従って、 x の表し方は 1 通りになる。すなわち、$G = G_1 \oplus G'$ （直和）であるといえる。//

ここで、数学的帰納法の仮定より、 G' は有限位数の元 $\overline{e_2},\quad \cdots \quad ,\overline{e_r}$ で生成される有限巡回群 $G_2,\quad \cdots \quad G_r$ および、 $k-r$ 個の無限巡回群 $G_{r+1} \quad \cdots \quad ,G_k$ の直和となる。ただし、 $t_j =^{\#} G_j \quad j = 2, \cdots, r$ とすると、$t_j | t_{j+1} \quad (j = 2, \cdots, r-1)$ が成り立つ。

$\overline{e_1}, \overline{e_2}$ の位数はそれぞれ m_1, t_2 であったから、 $m_1\overline{e_1} + t_2\overline{e_2} = 0$ が成り立つ。

補題 2.8 を極小生成元 $\overline{e}, \overline{e_2}, \quad \cdots \quad , \overline{e_k}$ に適用して、 $m_1|t_2$ が従う。
以上により、定理が示された。（証明終わり）