代数学概論 B 演習

教師用　(計算問題の略解付き)

黒木 玄　(東北大学大学院理学研究科数学専攻)

2008 年 5 月 26 日 (月)

目 次

1　行列の単因子論

この節の目標は次の定理を証明することである.

定理 1.1 (行列の単因子論) $\mathbb{Z}$ の元を成分に持つ (m,n) 型行列 $A \in M_{m,n}(\mathbb{Z})$ を任意に取る. このとき行列の基本変形によって A を

$$\begin{bmatrix} e_1 & & & & & & 0 \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_s & & & \\ & & & & 0 & & \\ 0 & & & & & \ddots & \end{bmatrix}$$

の形の行列で次をみたすものに変形できる:

$$e_1 \mid e_2 \mid \cdots \mid e_s, \qquad e_s \neq 0.$$

しかもこのような $e_1,\dots,e_s$ は ± 1 倍を除いて一意に定まる. $e_1,\dots,e_s$ を行列 A の**単因子 (elementary divisors)** と呼ぶ[1]. (単因子として正のものを選ぶことにすれば単因子は行列 A から一意に定まる.) □

[1]任意の可換環において $0 \in R$ は任意の $a \in R$ で割り切れる (なぜならば $0 = 0 \cdot a$). よって $N = \min\{m,n\}$, $e_{s+1} = \cdots = e_N = 0$ と置けば $e_1 \mid e_2 \mid \cdots \mid e_N$ が成立する. したがって 0 を例外扱いする必要はなく, 0 も単因子に含めておいても問題は生じない.

証明を後回しにして例をひとつ挙げておこう.

例 1.2 行列 A を次のように定める:

$$A = \begin{bmatrix} 0 & 1 & 5 & 1 \\ 2 & 1 & 19 & 5 \\ 6 & -1 & 43 & 11 \end{bmatrix}.$$

このとき行列の基本変形を $\to$ で表わすと,

$$\begin{aligned} &\begin{bmatrix} 0 & 1 & 5 & 1 \\ 2 & 1 & 19 & 5 \\ 6 & -1 & 43 & 11 \end{bmatrix} \xrightarrow{\text{第 1,2 列を交換}} \begin{bmatrix} 1 & 0 & 5 & 1 \\ 1 & 2 & 19 & 5 \\ -1 & 6 & 43 & 11 \end{bmatrix} \\ &\xrightarrow[\text{(第 4 列)}-\text{(第 1 列)}]{\text{(第 3 列)}-5\times\text{(第 1 列)}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 14 & 4 \\ -1 & 6 & 48 & 12 \end{bmatrix} \xrightarrow[\text{(第 3 行)}+\text{(第 1 行)}]{\text{(第 2 行)}-\text{(第 1 行)}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 14 & 4 \\ 0 & 6 & 48 & 12 \end{bmatrix} \\ &\xrightarrow[\text{(第 4 列)}-2\times\text{(第 2 列)}]{\text{(第 3 列)}-7\times\text{(第 2 列)}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 6 & 6 & 0 \end{bmatrix} \xrightarrow{\text{(第 4 行)}-3\times\text{(第 2 行)}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{bmatrix}. \end{aligned}$$

このとき $1 \mid 2 \mid 6$ が成立しているので $1, 2, 6$ は行列 A の単因子である. □

行列の単因子の存在の証明 1. m に関する帰納法. $A = 0$ ならば何もすることはない. よって $A \neq 0$ と仮定して良い. A に基本変形をほどこした結果全体の集合を $\mathcal{E}$ と書き, ある $B \in \mathcal{E}$ の成分になっているような $\mathbb{Z}$ の元全体の集合を $\mathcal{F}$ と書くことにする. $\mathcal{F}$ に含まれる 0 でない元の中で絶対値が最小のものを e_1 とする. e_1 を第 $(1,1)$ 成分とする $B \in \mathcal{E}$ が存在する. B の第 1 列と第 1 行における第 $(1,1)$ 成分以外の成分の中に e_1 で割り切れないものが存在するとすれば, 基本変形によってその割り切れない成分から e_1 の整数倍を引き去ることによって e_1 よりも絶対値が小さい 0 でない整数を構成できるので e_1 の絶対値の最小性に反する. したがって 第 1 列と第 1 行のすべての成分は e_1 で割り切れる. そのことから行列の基本変形によって, 第 $(1,1)$ 成分の e_1 を変えずにそれ以外の第 1 列と第 1 行の成分を 0 にできることがわかる. その結果を $C = \begin{bmatrix} e_1 & 0 \\ 0 & C' \end{bmatrix}$ と書くことにする. ここで C' は $(m-1, n-1)$ 型行列である. もしも C' の成分の中に e_1 で割り切れない成分が存在するとすればその成分を含む C の列を第 1 列に加えてから上と同様の議論を行なうことによって, e_1 の絶対値の最小性に矛盾することがわかる. よって C' のすべての成分は e_1 で割り切れる. あとは C' に帰納法の仮定を適用すれば証明が終わる. C' の基本変形で「C' のすべての成分が e_1 で割り切れる」という性質が保たれることに注意せよ. □

注意 1.3 上の証明 1 はそのままでは行列の単因子を計算するためのアルゴリズム (有限時間ステップで必ず終わる計算手続き) を与えない. なぜならば無限集合 $\mathcal{E}, \mathcal{F}$ を扱ってしまっているからである. しかし下の証明 2 はアルゴリズムを与える. □

行列の単因子の存在の証明 2. $A = [a_{ij}] \in M_{m,n}(R)$ に以下の手続きで基本変形をほどこす:

1. $A = 0$ ならば手続きを終了する.

2. 行と列の置換によって, A の 0 でない絶対値が最小の成分を第 $(1,1)$ 成分に持って来て, 改めてその行列を A として次に進む.

3. 以下のサブルーチンを実行する:

   (a) $a_{21},\dots,a_{m1}$ のすべてが a_{11} で割り切れるならば第 1 行の整数倍を第 $2,\dots,m$ 行に加えて第 $(2,1),\dots,(m,1)$ 成分をすべて 0 にする．その結果を改めて A として次に進む.

   (b) $a_{21},\dots,a_{m1}$ のどれかが a_{11} で割り切れないならば行の基本変形を用いて第 1 列に Euclid の互除法を適用して A を次の形に変形する:

   $$\begin{bmatrix} a & b \\ 0 & B \end{bmatrix}, \qquad 0 \neq a \in R, \quad b \in M_{1,n-1}(R), \quad B \in M_{m-1,n-1}(R).$$

   ここで a は A の第 1 列の最大公約数であり, $|a| < |a_{11}|$ が成立している. 変形した結果を改めて A として次に進む.

   (c) $a_{12},\dots,a_{1n}$ のすべてが a_{11} で割り切れるならば第 1 列の整数倍を第 $2,\dots,m$ 列に加えて第 $(1,2),\dots,(1,n)$ 成分をすべて 0 にする. その結果を改めて A として次に進む.

   (d) $a_{12},\dots,a_{1n}$ のどれかが a_{11} で割り切れないならば列の基本変形を用いて第 1 行に Euclid の互除法を適用して A を次の形に変形する:

   $$\begin{bmatrix} a & 0 \\ c & B \end{bmatrix}, \qquad 0 \neq a \in R, \quad c \in M_{m-1,1}(R), \quad B \in M_{m-1,n-1}(R).$$

   ここで a は A の第 1 行の最大公約元であり, $|a| < |a_{11}|$ が成立している. その結果を改めて A として次に進む.

   (e) もしも A が次の形をしていたらこのサブルーチンを終了する:

   $$\begin{bmatrix} a & 0 \\ 0 & B \end{bmatrix}, \qquad 0 \neq a \in R, \quad B \in M_{m-1,n-1}(R). \tag{$\sharp$}$$

   このサブルーチンは必ず有限ステップで終了する. なぜならば, a_{11} で第 1 列もしくは第 1 行のどれかの成分が割り切れないならば $|a_{11}|$ が小さくなって行くからである. そして a_{11} で第 1 列と第 1 行の両方の成分がすべて割り切れるならば A は $(\sharp)$ の形に変形されてしまう.

4. この時点で A は $(\sharp)$ の形をしている. もしも B のある成分が a で割り切れないならば, その成分が存在する列もしくは行を第 1 列もしくは第 1 行に加える. その結果を改めて A としてステップ 3 に戻る.

5. B のすべての成分が a で割り切れるならば B に対してこの手続き自身を再帰的 (帰納的) に適用する. (行列 B を基本変形しても「B のすべての成分が a で割り切れる」という性質が保たれることに注意せよ.)

6. この手続きの全体を終了する. この手続き全体は必ず有限ステップで終了する. なぜならば, ステップ 3 の終了時に B のある成分が a で割り切れないならばステップ 4 を経由してステップ 3 に戻り, ステップ (b) で $|a_{11}|$ が小さくなって行くからである.

以上のようにして行列 A を行列の基本変形によって定理 1.1 の形に変形できることがわかる. $\square$

整数を成分の持つ (m,n) 型行列 $A \in M_{m,n}(\mathbb{Z})$ に対して A のすべての i 次小行列式[2]の最大公約数を $d_i(A)$ と書き, A の**行列式因子 (determinantal divisors)** と呼ぶ[3].

補題 1.4 (行列式因子の基本変形による不変性) 行列式因子は基本変形によって (± 1 倍を除いて) 不変である.

証明. 行列 B は以下のどれかであるとする：

(1) B は A のある行 (または列) を ± 1 倍したものである.

(2) B は A のある行 (または列) の整数倍を他の行 (または列) に加えてできる行列である.

(3) B は A の二つの異なる行 (または列) を交換したものである.

行列の基本変形はこれらの基本操作の有限回の繰り返しのことなので, 以上の場合について $d_i(A)$ と $d_i(B)$ が等しいことを示せばよい. さらに行列の基本変形は逆変形を持ち, 逆変形も基本変形なので, $d_i(B)$ が $d_i(A)$ で割り切れることを示せば十分である. そのためには B の i 次の小行列式が $d_i(A)$ で割り切れることを示せばよい.

(1) と (3) の場合. B の i 次の小行列式は A の i 次の小行列式の ± 1 倍になるので, B の i 次の小行列式は $d_i(A)$ で割り切れる.

(2) の場合. B の i 次の小行列式は A の i 次の小行列式の整数倍の和の形になるので $d_i(A)$ で割り切れる. $\square$

次の命題を証明すれば定理 1.1 の証明が完了する.

命題 1.5 (単因子と行列式因子の関係) 行列 $A \in M_{m,n}(\mathbb{Z})$ の単因子を $e_1, \dots, e_s$ と書き, 行列式因子を $d_1, \dots, d_k$ ($k = \min\{m,n\}$) と書くとき, 必要ならばそれぞれを適切に ± 1 倍することによって次が成立する:

$$d_1 = e_1,\ d_2 = e_1 e_2,\ \dots,\ d_s = e_1 e_2 \cdots e_s, \qquad d_i = 0 \quad (i > s).$$

これは次と同値なので行列 A の単因子は A から ± 1 倍を除いて一意に定まることもわかる:

$$e_1 = d_1,\ e_2 = d_2/d_1,\ \dots,\ e_s = d_s/d_{s-1}, \qquad 0 = d_i/d_{i-1} \quad (i > s).$$

証明. 行列 A を基本変形することによって次の形の行列 B が得られたとする:

$$B = \begin{bmatrix} e_1 & & & & & 0 \\ & e_2 & & & & \\ & & \ddots & & & \\ & & & e_s & & \\ & & & & 0 & \\ 0 & & & & & \ddots \end{bmatrix}, \qquad e_1 \mid e_2 \mid \cdots \mid e_s, \quad e_s \neq 0.$$

補題 1.4 より, 必要なら適当に ± 1 倍すれば $d_i(A) = d_i(B)$ である. しかし, $d_i(B)$ は容易に計算できる: $d_1(B) = e_1$, $d_2(B) = e_1 e_2$, ..., $d_r(B) = e_1 e_2 \cdots e_s$, $d_i(B) = 0$ $(i > s)$. $\square$

[2] (m,n) 型行列の i 次小行列式は $\binom{m}{i}\binom{n}{i}$ 通り存在する.

[3] 単因子の記号 e_i は elementary divisor の頭文字を取っており, 行列式因子の記号 d_i は determinantal divisor の頭文字を取っている. 堀田 [1] では単因子は d_i と表わされ, 行列式因子を $\varDelta_i$ と表わされているので混乱しないように注意せよ.

2　有限生成 Abel 群の基本定理

以下 Abel 群を加法群として扱う.

有限個の Abel 群 $M_1, M_2, \dots, M_k$ の直積 $M_1 \times M_2 \times \cdots \times M_k$ を直和の記号を用いて $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ と書くことにする. このとき $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ の元 v は

$$v = v_1 + v_2 + \cdots + v_k, \qquad v_i \in M_i$$

と一意に表わされる (これが直和の定義だと考えてよい).

Abel 群 M が **有限生成 (finitely generated)** であるとはある $v_1, \dots, v_n \in M$ で

$$M = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$$

を満たすものが存在することであると定める. このとき, M は $v_1, \dots, v_n$ から生成されると言い, $v_1, \dots, v_n$ を M の生成元と呼ぶ. そのとき任意の $v \in M$ は

$$v = a_1 v_1 + \cdots + a_n v_n, \qquad a_1, \dots, a_n \in \mathbb{Z}$$

と表わされるが, この表示の一意性が成立するとは限らないことには注意せよ. 表示の一意性が成立するときには群の同型

$$M = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n \cong \mathbb{Z}^n, \qquad v = a_1 v_1 + \cdots + a_n v_n \leftrightarrow (a_1, \dots, a_n)$$

が成立している. このとき M は有限生成**自由** Abel 群であると言い, $v_1, \dots, v_n$ を M の**自由基底**と呼ぶ.

この節の目標は次の定理の証明の概略と応用例について説明することである.

定理 2.1 (有限生成 Abel 群の基本定理 1) M は有限生成 Abel 群であるとする. このとき 2 以上の整数 $e_1, \cdots, e_s$ と 0 以上の整数 r で次を満たすものが一意に存在する:

$$M \cong (\mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_s\mathbb{Z}) \oplus \mathbb{Z}^r \quad (\text{加法群の同型}), \qquad e_1 \mid \cdots \mid e_s. \quad \square$$

一般に正の整数 n が $n = p_1^{m_1} \cdots p_k^{m_k}$ (p_i は互いに異なる素数, m_ν は正の整数) と素因数分解されているとき, 中国式剰余定理

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_k^{m_k}\mathbb{Z}) \quad (\text{加法群の同型})$$

が成立している. したがって上の定理における各 e_i を素因数分解することによって次の結果が得られる (詳しい証明は略).

定理 2.2 (有限生成 Abel 群の基本定理 2) M は有限生成 Abel 群であるとする. このとき素数 $p_1, \dots, p_N$ (重複を許す) と正の整数 $m_1, \dots, m_N$ と 0 以上の整数 r で次を満たすものが存在する:

$$M \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_N^{m_N}\mathbb{Z}) \oplus \mathbb{Z}^r \quad (\text{加法群の同型}).$$

しかも r は M から一意に定まり, $(p_1^{m_1}, \dots, p_N^{m_N})$ は並べる順序を除いて M から一意に定まる. $\square$

例 2.3 n が 2 以上の整数のとき $M = \mathbb{Z}/n\mathbb{Z}$ は $\bar{1} = 1 + n\mathbb{Z}$ から生成される有限生成 Abel 群である. $M = \mathbb{Z}/n\mathbb{Z}$ に対する定理 2.1 の s, e_i, r は $s = 1$, $e_1 = n$, $r = 0$ となる. $\square$

例 2.4 n が 0 の整数のとき $M = \mathbb{Z}^n$ は標準基底 $e_1, \ldots, e_n$ から生成される有限生成 Abel 群である．ここで e_i は第 i 成分だけが 1 で他の成分はすべて 0 のベクトルである (定理 2.1 の e_i との区別に注意せよ)．$\mathbb{Z}^0 = \{0\}$ と考える．$M = \mathbb{Z}^n$ に対する定理 2.1 の s, e_i, r は $s = 0$, $r = n$ となる． □

例 2.5 $\mathbb{Z}^2$ の部分群 N を $N = \{\,(x,y) \in \mathbb{Z}^2 \mid x + y = 0\}$ と定め，$M = \mathbb{Z}^2/N$ とおく．このとき M は $v_1 = (1,0) \bmod N\,(= (1,0)+N)$, $v_2 = (0,1) \bmod N\,(= (0,1)+N)$ から生成される有限生成 Abel 群である．$M \cong \mathbb{Z}$ を次のようにして証明できる．加法群の準同型 $f : M \to \mathbb{Z}$ を $f(x,y) = x + y$ $((x,y) \in \mathbb{Z}^2)$ と定める．このとき任意の $a \in \mathbb{Z}$ に対して $f(a,0) = a$, $(a,0) \in \mathbb{Z}^2$ なので f は全射である．さらに $(x,y) \in \mathbb{Z}^2$ に対して $f(x,y) = 0 \iff x + y = 0$ なので $\operatorname{Ker} f = N$ であることもわかる．よって群の準同型定理より $M = \mathbb{Z}^2/N \cong \mathbb{Z}$ となる．$M = \mathbb{Z}^2/N$ に対する定理 2.1 の s, e_i, r は $s = 0$, $r = 1$ となる． □

例 2.6 n は 2 以上の整数であるとし，$\mathbb{Z}^2$ の部分群 N を $N = \{\,(x,y) \mid x = y \equiv 0 \bmod n\,\}$ と定め，$M = \mathbb{Z}^2/N$ とおく．このとき M は $v_1 = (1,0) \bmod N\,(= (1,0)+N)$, $v_2 = (0,1) \bmod N\,(= (0,1)+N)$ から生成される有限生成 Abel 群である．$M \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}$ を次のようにして証明できる．加法群の準同型 $f : M \to \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}$ を $f(x,y) = (x \bmod n, y - x)$ $((x,y) \in \mathbb{Z}^2)$ と定める．このとき任意の $a, b \in \mathbb{Z}$ に対して $f(a, a+b) = (a \bmod n, b)$, $(a, a+b) \in \mathbb{Z}^2$ なので f は全射である．さらに $(x,y) \in \mathbb{Z}^2$ に対して $f(x,y) = (0 \bmod n, 0) \iff x = y \equiv 0 \bmod n$ なので $\operatorname{Ker} f = N$ であることもわかる．よって群の準同型定理より $M = \mathbb{Z}^2/N \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}$ となる．$M = \mathbb{Z}^2/N$ に対する定理 2.1 の s, e_i, r は $s = 1$, $e_1 = n$, $r = 1$ となる． □

例 2.7 $M = (\mathbb{Z}/20\mathbb{Z}) \oplus (\mathbb{Z}/30\mathbb{Z})$ とおく．$20 \nmid 30$ に注意せよ．このとき中国式剰余定理と $20 = 2^2 \cdot 5$, $30 = 2 \cdot 3 \cdot 5$, $2^2 \cdot 3 \cdot 5 = 60$, $2 \cdot 5 = 10$ より

$$\begin{aligned} M &\cong ((\mathbb{Z}/2^2\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})) \oplus ((\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})) \\ &\cong ((\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})) \oplus ((\mathbb{Z}/2^2\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})) \\ &\cong (\mathbb{Z}/10\mathbb{Z}) \oplus (\mathbb{Z}/60\mathbb{Z}). \end{aligned}$$

$10 \mid 60$ に注意せよ．よって M に対する定理 2.1 の s, e_i, r は $s = 2$, $e_1 = 10$, $e_2 = 60$, $r = 0$ となる． □

定理 2.1 の証明の概略. 1. M は $w_1', \ldots, w_m'$ から生成される有限生成 Abel 群であると仮定する．このとき群の全射準同型 $f : \mathbb{Z}^m \to M$ を $f(a_1, \ldots, a_m) = a_1 w_1' + \cdots + a_m w_m'$ $(a_i \in \mathbb{Z})$ と定めることができる．よって $N = \operatorname{Ker} f$ とおくと群の準同型定理より $M \cong \mathbb{Z}^m/N$ である．

2. N は m 個以下の元 $w_1, \ldots, w_n \in \mathbb{Z}^m$ $(n \leqq m)$ から生成される (要証明)．よって群の準同型 $g : \mathbb{Z}^n \to \mathbb{Z}^m$ を $g(b_1, \ldots, b_n) = b_1 w_1 + \cdots + b_n w_n$ $(b_i \in \mathbb{Z})$ と定めると $\operatorname{Im} g = N$ が成立している．$\mathbb{Z}^n$, $\mathbb{Z}^m$ の元を列 (縦) ベクトルで表わすことにし，$w_j \in \mathbb{Z}^m$ を第 j 列ベクトルに持つ (m,n) 型行列を A と書くと，$g(x) = Ax$ $(x \in \mathbb{Z}^n)$ が成立している (簡単なことだが要確認)．

3. 定理 1.1(行列の単因子論) の結果より，行列 A は基本変形によって次の形に変形さ

れる:

$$B = \begin{bmatrix} e_1 & & & & & & 0 \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_s & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & \end{bmatrix}, \qquad \begin{cases} e_1 = e_2 = \cdots = e_l = 1, \\ e_{l+1} \mid e_{l+1} \mid \cdots \mid e_s, \\ e_{l+1}, \ldots, e_s \text{ は 2 以上の整数.} \end{cases}$$

そして行列の列に関する基本変形を与える行列は $\mathbb{Z}^n$ の自由基底を取り換え, 行列の行に関する基本変形を与える行列は $\mathbb{Z}^m$ の自由基底を取り換える (簡単なことだが要確認). よって適当に取り換えられた自由基底に関する準同型 g の行列表示が B であると考えてよい. すなわち, $\mathbb{Z}^n$ のある自由基底 $u_1, \ldots, u_n$ と $\mathbb{Z}^m$ のある自由基底 $v_1, \ldots, v_m$ が存在して次が成立している:

$$g(u_1) = e_1 v_1, \quad \ldots, \quad g(u_s) = e_s v_s, \quad g(u_{s+1}) = \cdots = g(u_n) = 0.$$

したがって $N = \operatorname{Im} g = \mathbb{Z} e_1 v_1 \oplus \cdots \oplus \mathbb{Z} e_s v_s$.

4. $M \cong \mathbb{Z}^m/N$ は次のように計算される (要証明):

$$\begin{aligned} M \cong \mathbb{Z}^m/N &= \frac{\mathbb{Z} \quad v_1 \oplus \cdots \oplus \mathbb{Z} \quad v_s \oplus \mathbb{Z} v_{s+1} \oplus \cdots \oplus \mathbb{Z} v_m}{\mathbb{Z} e_1 v_1 \oplus \cdots \oplus \mathbb{Z} e_s v_s} \\ &\cong (\mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_s\mathbb{Z}) \oplus \mathbb{Z}^{m-s}. \end{aligned}$$

さらに $e_1 = \cdots = e_l = 1$ と $\mathbb{Z}/1\mathbb{Z} = \mathbb{Z}/\mathbb{Z} \cong 0$ より

$$M \cong (\mathbb{Z}/e_{l+1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_s\mathbb{Z}) \oplus \mathbb{Z}^{m-s}.$$

ここで $e_{l+1} \mid \cdots \mid e_s$ でかつ $e_{l+1}, \ldots, e_s$ は 2 以上の整数であることに注意すれば定理 2.1 の同型の存在が示されたことがわかる. 同型の右辺の一意性の証明については略. □

注意 2.8 上の証明は行列の単因子を求めることによって定理 2.1 の同型の右辺を計算する方法を与えている. 一般に $\mathbb{Z}$ の元を成分に持つ (m, n) 型行列 A が行列の基本変形によって

$$\begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & \ddots \end{bmatrix}$$

の形に変形されるとき, A の n 本の列ベクトルから生成される $\mathbb{Z}^m$ の部分群を N と書き, $M = \mathbb{Z}^m/N$ とおくと,

$$M \cong \begin{cases} \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_m\mathbb{Z} & (m \leqq n), \\ \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z} \oplus \mathbb{Z}^{m-n} & (m \geqq n). \end{cases} \quad \square$$

例 2.9 例 1.2 の行列 A を考える. A の第 j 列ベクトルを $w_j \in \mathbb{Z}^3$ と書き, w_1, w_2, w_3, w_4 から生成される $\mathbb{Z}^3$ の部分群を N と書き, $M = \mathbb{Z}^3/N$ とおく. 例 1.2 の結果より次が成立していることがわかる:

$$M \cong (\mathbb{Z}/1\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}).$$

最後の同型で中国式剰余定理を使った. □

3 ねじれ部分

Abel 群 (加法群) M に対してその**ねじれ部分 (torsion part)** M_{tor} を

$$M_{\mathrm{tor}} = \{\, v \in M \mid \text{ある } 0 \text{ でない } a \in \mathbb{Z} \text{ が存在して } av = 0 \,\}$$

と定める. M_{tor} は M の部分群になる (要証明).

定理 3.1 M が有限生成 Abel 群であるとき以下が成立している:

1. M/M_{tor} は有限生成自由 Abel 群である.
2. M は自由 $\iff$ $M_{\mathrm{tor}} = 0$.
3. M は有限 $\iff$ $M = M_{\mathrm{tor}}$.

証明. 有限生成 Abel 群の基本定理より $M = (\mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_s\mathbb{Z}) \oplus \mathbb{Z}^r$ $(e_i \geqq 2)$ と仮定してよい (なぜか?). このとき $M_{\mathrm{tor}} = (\mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_s\mathbb{Z})$ である. よって, $M/M_{\mathrm{tor}} \cong \mathbb{Z}^r$ が有限生成自由 Abel 群であることと M は有限 $\iff$ $M = M_{\mathrm{tor}}$ であることがわかる. さらに有限生成 Abel 群の基本定理の一意性の主張より, M は自由 $\iff$ $M = \mathbb{Z}^r \iff M_{\mathrm{tor}} = 0$. □

4 問題

問題 1. $\mathbb{Z}$ の元を成分として持つ行列 $A = \begin{bmatrix} 4 & 2 & 4 & 4 \\ 3 & 1 & 3 & 3 \\ 7 & 5 & 3 & 11 \\ 7 & 1 & 11 & 3 \end{bmatrix}$ を行列の基本変形によって $B = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{bmatrix}$ $(a \mid b \mid c \mid d,\ a, b, c, d \geqq 0)$ の形に変形せよ. 行列 A の 4 本の列ベクトルから生成される $\mathbb{Z}^4$ の部分群を N と書き, $M = \mathbb{Z}^4/N$ とおく. 有限生成 Abel 群の基本定理の意味で M の構造を決定せよ. □

問題 2. $M = (\mathbb{Z}/40\mathbb{Z}) \oplus (\mathbb{Z}/18\mathbb{Z}) \oplus (\mathbb{Z}/12\mathbb{Z})$ とおく. $M \cong (\mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/e_s\mathbb{Z})$, $e_1 \mid \cdots \mid e_s$, $e_i \geqq 2$ を満たす e_i たちを求めよ. □

参考文献

[1] 堀田良之, 代数入門—群と加群, 数学シリーズ, 裳華房, 1987