$Ax=b$ の $\mathbb{Z}$ 上での可解性について考える．

定理 1　$A : m \times n$ 整数行列で $\mathrm{rank}(A)=m$ とすると以下はすべて同値である．

(1) ${}^{\forall}b \in \mathbb{Z}^m$ に対して ${}^{\exists}x \in \mathbb{Z}^n : Ax=b$

(2) $y^{\mathrm{T}}A \in \mathbb{Z}^n \Rightarrow y \in \mathbb{Z}^m$

(3) A の行列式因子 $g_k(A) \cdots k$ 次の小行列式の最大公約数として，$g_m(A)=1$

(4) A のエルミート標準形$=[I_m|0]$

(4) を基準に見ていく．

まず (1) について．Q を単摸行列でエルミート標準形として $Ax=b \Leftrightarrow AQQ^{-1}x=b$

先週より $x \in \mathbb{Z}^n \Leftrightarrow Q^{-1}x \in \mathbb{Z}^n (4 \to 1)$ なので A をエルミート標準形としてよい．

${}^{\forall}b \in \mathbb{Z}^m$ に対して

$$\begin{array}{|c|c|}\hline \begin{matrix} & 0 \\ I & \end{matrix} & 0 \\ \hline \end{array}\ \boxed{x} = \boxed{b}$$

このとき $i(>1)$ 行目で

$$\begin{array}{|c|c|}\hline \begin{matrix} & 0 \\ I & \end{matrix} & 0 \\ \hline \quad a & \\ \hline & \\ \hline \end{array}\ \boxed{x} = \begin{array}{|c|}\hline 0 \\ \vdots \\ b_i \\ \vdots \\ 0 \\ \hline \end{array}$$

1〜$i-1$ 行は解けて $x=\begin{array}{|c|}\hline 0 \\ \vdots \\ x_i \\ \vdots \\ * \\ \hline \end{array} \to ax_i=b_i \in \mathbb{Z}$ なので $a=1$

次に (2) についてみてみる．$y^{\mathrm{T}}A \in \mathbb{Z}^n \Leftrightarrow y^{\mathrm{T}}AQ \in \mathbb{Z}^n(Q$ は単摸行列) なので A をエルミート標準形としてよい．

このとき (2)$\Leftrightarrow \beta_{11}=\beta_{22}=\cdots\beta_{mm}=1$ を示す．

$\Leftarrow$ は明らかである．

$\Rightarrow \beta_{ii} \neq 1$ となる最初の行 (k 行) に注目する．

$$A=\begin{array}{|c|c|}\hline \begin{matrix} & 0 \\ I & \end{matrix} & 0 \\ \hline \begin{matrix} \beta_{k1}\beta_{k2}\cdots & \\ & \beta_{kk} \end{matrix} & \\ \hline & \\ \hline \end{array}$$

$$y^{\mathrm{T}}=\begin{array}{|c|c|c|c|c|}\hline -\beta_{k1}/\beta_{kk} & -\beta_{k2}/\beta_{kk} & \cdots & 1/\beta_{kk} & 0 \\ \hline \end{array}$$

とおくと $y^{\mathrm{T}}A=[0,0\cdots1,0\cdots0]$ となって $y^{\mathrm{T}}A\in\mathbb{Z}^n$ であるが $y\notin\mathbb{Z}^n$

次に (3) について．

準備として $g_k(A)$ は A の $\mathbb{Z}$ 型の列基本変形で不変である．

A に対して $\alpha=1\sim k$ 列の小行列式で $\beta=1\sim k-1,j$ 列の小行列式とし A の j 列を i 列に加えて A' とする．

A' に対して $1\sim k-1,j$ 列の小行列式 $=b$,$1\sim k$ 列の小行列式を a' とする．Laplace 展開を考えると (a_i に関する展開)+(a_j に関する展開) なので $a'=a+b$

準備より Q が単摸なら $g_n(A)=g_m(AQ)$ なので A をエルミート標準形としてよい．$g_m(A)=1\Leftrightarrow\beta_{11}=\cdots=\beta_{mm}=1$

0.1 Smith 標準形

$A\in\mathbb{Z}^{m\times n},\ \mathrm{rank}(A)=r,\ {}^{\exists}P,Q$ を単摸行列とする．

$$PAQ=\begin{array}{|ccc|c|}\hline \alpha_1 & & & \\ & \ddots & & 0 \\ & & \alpha_r & \\ \hline & 0 & & 0 \\ \hline\end{array}$$

$\alpha_1>0,\alpha_2>0\cdots\alpha_r>0$ であり $\alpha_1|\alpha_2\cdots|\alpha_r(\alpha_1\text{は}\alpha_2\text{を割り切る})$

このとき $g_k(A)=g_k(PAQ)=\alpha_1\cdots\alpha_k$

Smith 標準形の作り方を述べる．まず $\min\{|a_{ij}|i=1\cdots m,\ j=1\cdots n\ a_{ij}\neq0\}$ なる (i,j) に注目して a_{ij} を基本変形で (1,1) にもってくる．

次に列基本変形で $0\leq a_{1j}<a_{11}(j=2\cdots n)$ とする．$a_{ij}=q_ja_{11}+r_j(q_j\in\mathbb{Z})$ として ${a_{ij}}'=r_j$ とする．a_{ij} を a_{11} で割り算して余りで更新していく．これを続けて最小 $(\neq0)$ になった a_{ij} を (1,1) にもってくる．そうするといつかは以下のようになる．

$$\begin{array}{|cccc}\hline a_{11} & 0 & \cdots & 0 \\ \hline & & & \\ & & & \end{array}$$

同じことを行基本変形でも行うと以下のようになる．

$$\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & a_{11}\text{の倍数} & \\ 0 & & & \end{array}$$

もし a_{11} の倍数でないなら $a_{ij}\to a_{ij}/a_{11}$ の基本変形ができるので．