第十二回

Smith normal form

[定理] RをPIDとし、$A=[a_{ij}]$を$n\times m$行列とする($a_{ij}\in R$)。
可逆行列$P\in GL_n(R)$、$Q\in GL_m(R)$が存在して、
PAQが次の形になる。

$$PAQ = \left.\underbrace{\begin{pmatrix} e_1 & & & & & \\ & e_2 & & & & \\ & & e_3 & & & \\ & & & \ddots & & \\ & & & & e_s & \\ & & & & & \end{pmatrix}}_{n}\right\} m$$

ここに、空白は0をあらわす。

$a\in R$に対して、$\delta(a)=$(aの素因数の個数)と定義する。
すなわち、$a=p_1^{i_1}p_2^{i_2}\cdots p_n^{i_n}$ (p_j 素元)として書けば、

$$\delta(a) = i_1+i_2+\cdots+i_n$$
$$\delta(0) = \infty$$

[命題1] RをPIDとする。$\forall a,b\in R\setminus\{0\}$に対して、$P\in GL_2(R)$が存在して

$$P\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \gcd(a,b) \\ 0 \end{pmatrix}$$

さらに $\delta(\gcd(a,b))=\delta(a)$ のとき、$P=\begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix}$と選べる。

[命題1] R を PID とする。$\forall a, b \in R \setminus \{0\}$ に対して、$P \in GL_2(R)$ が存在して

$$P \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \gcd(a,b) \\ 0 \end{pmatrix}$$

さらに $\delta(\gcd(a,b)) = \delta(a)$ のとき、$P = \begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix}$ と選べる。

証明。$g = \gcd(a,b)$ をおく。$\delta(g) = \delta(a)$ とは $a \mid b$ である。
そのとき、

$$P = \begin{pmatrix} 1 & 0 \\ -b/a & 1 \end{pmatrix}$$ とおけばよい。

そのほか、$ad + bc = g$ がみたす $c, d \in R$ を選ぶ（R が PID ですので $\langle a, b \rangle = \langle g \rangle$）。そして

$$P = \begin{pmatrix} d & c \\ -b/g & a/g \end{pmatrix}$$ とおけばよい。

□

[命題2] R をPIDとする。$\forall$

$$A = \begin{pmatrix} a_{11} & & \cdots & a_{1m} \\ \vdots & & & \vdots \\ a_{i-1,1} & & & \vdots \\ a_{i,1} & a_{i,2} & & \vdots \\ 0 & a_{i+1,2} & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & a_{n,2} & \cdots & a_{n,m} \end{pmatrix}$$

に対して、$P \in GL_n(R)$ が存在して、

$$PA = \begin{pmatrix} b_{11} & & \cdots & b_{1m} \\ a_{21} & & & a_{2m} \\ \vdots & & & \vdots \\ a_{i-1,1} & & & a_{i-1,m} \\ 0 & b_{i,2} & \cdots & b_{im} \\ 0 & a_{i+1,2} & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & a_{n,2} & \cdots & a_{n,m} \end{pmatrix}$$

さらに、

$$\delta(b_{11}) < \delta(a_{11})$$

か

$$a_{11} = b_{11}, \quad a_{12} = b_{12}, \quad \cdots \quad a_{1m} = b_{1m}$$

のどちらかをみたす P を選ぶことができる。

証明。

$a_{i1} = 0$ のとき、 $P = Id_n$

$a_{11} = 0$ のとき、 1行目と i 行目を入れ替え行列を選ぶ。

$$P = \begin{pmatrix} 0 & & 1 & & \\ & 1 & & & \\ & & \ddots & & \\ 1 & & & 0 & \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

$a_{11} \neq 0$、$a_{i1} \neq 0$ のとき、[命題1] において a_{11}、a_{i1} に対応する
$P = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$ を用い、

$$\begin{pmatrix} p_{11} & & p_{12} & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ p_{21} & & p_{22} & & \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

を選ぶ。

□

[命題3] RをPIDとする。$\forall$

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,m} \end{pmatrix}$$

に対して、$P \in GL_n(R)$が存在して、

$$PA = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ 0 & b_{21} & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \cdots & b_{nm} \end{pmatrix}$$

さらに、

$$S(b_{11}) < S(a_{11})$$

か

$$a_{11} = b_{11}, \quad a_{12} = b_{12}, \quad \cdots \quad a_{1m} = b_{1m}$$

のどちらかをみたすPを選ぶことができる。

証明。[命題2]から従う。 $\square$

[命題4] R を PID とする。$\forall$

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$$

に対して、$P \in GL_n(R)$, $Q \in GL_m(R)$ が存在して、

$$PAQ = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{n2} & \cdots & b_{nm} \end{pmatrix}$$

証明。[命題3]とそれの転置(transpose)を用いると、

$B_1 = P_1 A$, $B_2 = P_1 A Q_1$, $B_3 = P_2 P_1 A Q_1$, $B_4 = P_2 P_1 A Q_1 Q_2$, $\cdots$

が与えられる。左上成分の δ が減るから、ある N に対して

$B_N = B_{N+1} = B_{N+2} = \cdots$ で、これらが命題の PAQ の形になる。$\square$

[命題5] R を PID とする. $\forall$

$$A = \begin{pmatrix} a_{11} & & & & \\ & \ddots & & & \\ & & a_{i-1,i-1} & & \\ & & & a_{ii} & \cdots & a_{im} \\ & & & \vdots & & \vdots \\ & & & a_{ni} & \cdots & a_{nm} \end{pmatrix}$$

に対して、$P \in GL_n(R)$, $Q \in GL_m(R)$ が存在して、

$$PAQ = \begin{pmatrix} a_{11} & & & & & \\ & \ddots & & & & \\ & & a_{i-1,i-1} & & & \\ & & & b_{ii} & & \\ & & & & b_{i+1,i+1} & \cdots & b_{i+1,m} \\ & & & & \vdots & & \vdots \\ & & & & b_{n,i+1} & \cdots & b_{nm} \end{pmatrix}$$

証明。
$$\begin{pmatrix} a_{ii} & \cdots & a_{im} \\ \vdots & & \vdots \\ a_{ni} & \cdots & a_{nm} \end{pmatrix}$$
に対して [命題4] の P', Q' を用いると、

$$\begin{pmatrix} Id_i & \\ & P' \end{pmatrix} A \begin{pmatrix} Id_i & \\ & Q' \end{pmatrix}$$

が正しい形になる。 $\square$

[定理] RをPIDとし、$A = [a_{ij}]$ を $n \times m$ 行列とする($a_{ij} \in R$)。可逆行列 $P \in GL_n(R)$、$Q \in GL_m(R)$ が存在して、PAQが次の形になる。

$$PAQ = \underbrace{\left.\begin{pmatrix} e_1 & & & & & \\ & e_2 & & & & \\ & & e_3 & & & \\ & & & \ddots & & \\ & & & & e_s & \\ & & & & & \end{pmatrix}\right\} m}_{n}$$

ここに、空白は0をあらわす。

証明。[命題5]から従う。 $\square$

PID上の加群

[定理] M を PID R 上有限生成加群とする。同型

$$M \cong R^{\oplus d} \oplus \bigoplus_{\substack{\text{素元}\\ p\in R}} \left(\left(\frac{R}{p}\right)^{\oplus e_{p_1}} \oplus \left(\frac{R}{p^2}\right)^{\oplus e_{p_2}} \oplus \left(\frac{R}{p^3}\right)^{\oplus e_{p_3}} \oplus \cdots \right)$$

が存在する。ここに $d, e_{p_j} \in \mathbb{N}$、有限個を除いて e_{p_j} が 0である。
さらに、d、e_{p_j} は一意に定まる。

[記号] 一般な R 加群 M で、$n \in \mathbb{N}$、

$$M^n = M^{\oplus n} = \bigoplus_{i=1}^{n} M = \{(m_1, \ldots, m_n) \mid m_i \in M\}$$

[例] 1) $R = \mathbb{Z}$ のとき、有限生成アーベル群の基本定理になる。
2) R が離散付値環 (discrete valuation ring) で、
$\langle \pi \rangle$ が極大イデアルであれば、(例えば

$$R = \mathbb{C}[[t]] = \left\{ \sum_{i=0}^{\infty} a_i t^i \;\middle|\; a_i \in \mathbb{C} \right\} \qquad \pi = t$$

とか

$$R = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; b, p \text{ 互いに素} \right\} \qquad \pi = p$$

とか)、

$$M \cong R^{\oplus d} \oplus \left(\frac{R}{\pi}\right)^{\oplus e_1} \oplus \left(\frac{R}{\pi^2}\right)^{\oplus e_2} \oplus \left(\frac{R}{\pi^3}\right)^{\oplus e_3} \oplus \cdots \oplus \left(\frac{R}{\pi^N}\right)^{\oplus e_N}$$

[定義] PIDと $\operatorname{Spec} R = \{(0), (\pi)\}$ 　 $\exists\, \pi \neq 0$

$\operatorname{Spec} \mathbb{C}[[t]] = \{(0), (t)\}$

$\operatorname{Spec} \mathbb{Z}_{(p)} = \{(0), (p)\}$

[命題] $N \subseteq R^{\oplus n}$ が部分加群であれば、ある $m \leq n$ について R加群同型

$$N \cong R^{\oplus m}$$

が存在する。

証明。射影

$$\pi : R^{\oplus n} \to R \qquad (b_1, \dots, b_n) \mapsto b_n$$

を考えよう。その核は

$$\ker(\pi) = \{(b_1, \dots, b_{n-1}, 0) \mid b_i \in R\}$$

である。

$$N' = N \cap \ker(\pi) = \{(b_1, \dots, b_n) \in N \mid b_n = 0\}$$

とおく。帰納法によって N' を生成する

$$a_1 = (a_{11}, \dots, \underset{\neq 0}{a_{1n_1}}, 0, \dots, 0, 0, \dots, 0, 0, \dots, 0)$$

$$a_2 = (a_{21}, \dots, a_{2n_1}, a_{2n_1+1}, \dots, \underset{\neq 0}{a_{2n_2}}, 0, \dots, 0, 0, \dots, 0)$$

$$\vdots$$

$$a_m = (a_{m1}, \dots, a_{mn_1}, a_{mn_1+1}, \dots, a_{mn_2}, a_{mn_2+1}, \dots, \underset{\neq 0}{a_{mn_m}}, 0, \dots, 0)$$

がある。ここに、$a_{ij} \in R$、$a_{in_i} \neq 0$、$n_1 < n_2 < \dots < n_m$。

もし $N' = N$ であれば、以上です。

$$\left(\begin{array}{ll} R^m \to N & \\ (b_1, \dots, b_m) \mapsto \sum b_i a_i & \end{array} \quad \text{同型：} \begin{array}{l} \text{単} \\ \text{全} \end{array} \right)$$

$N/N' \neq \{0\}$ であれば、$\pi(N) \neq \{0\} \subseteq R$ となって、R加群として、$\pi(N)$ を生成する $0 \neq c_n \in R$ が存在する（Rの部分加群はイデアル、R PID）。したがって、$c + N'$ がR加群として N/N' を生成する $c = (c_1, \dots, c_n) \in R^n$ が存在する。

$$a_1, \dots, a_m, (c_1, \dots, c_n)$$

が N を R加群として生成する：

($n \in N$ をとって、 $\pi(N) = \{bc + N' \mid b \in R\} \subset N/N' \quad \exists c$

$\pi(N) = \langle c + N' \rangle \Rightarrow \exists b \in R,\ bc + N' = n + N' \Rightarrow bc - n \in N'$

$N' = \langle a_1, \dots, a_m \rangle \Rightarrow \exists b_1, \dots, b_m \in R \quad bc - n = \sum b_i a_i$

$\Rightarrow n = bc - \sum b_i a_i$) $\square$

$N \subset R^3$

$\theta : R^3 \to R^2 \qquad (a_1, a_2, a_3) \mapsto (a_2, a_3)$

$\pi : R^3 \to R \qquad \mapsto a_3$

$N_1 := N \cap \ker(\theta) = \{(a_1, 0, 0) \in N\}$

$N_2 := N \cap \ker(\pi) = \{(a_1, a_2, 0) \in N\}$

$N_3 = N$

$N_1 \subset \{(a, 0, 0) \in R^3 \mid a \in R\} \cong R$

$\Rightarrow \quad N_1 = \langle (c_{11}, 0, 0) \rangle \subseteq R^3$

$\cdot\ \phi : R^3 \to R \qquad (a_1, a_2, a_3) \mapsto a_2.$

$\phi(N_2) \subset R$

$= \langle c_{22} \rangle$

$$\begin{array}{ccccccccc} 0 & \to & N_1 & \hookrightarrow & N_2 & \twoheadrightarrow & N_2/N_1 & \to & 0 \\ & & \cap & & \cap & & \cap & & \\ 0 & \to & R & \hookrightarrow & R^2 & \twoheadrightarrow & R & \to & 0 \end{array}$$

$N_2 = \langle (c_{11}, 0, 0), (c_{12}, c_{22}, 0) \rangle$

$\pi(N) \subset R$

$= \langle c_{33} \rangle$

$N = N_3 = \langle (c_{11}, 0, 0), (c_{12}, c_{22}, 0), (c_{31}, c_{32}, c_{33}) \rangle$