三年生の代数学

第 12 回 単項イデアル整域上の加群と単因子論

第 13 回 有限生成加群の構造定理 講義中に指示する

第 14 回 ジョルダンの標準形

http://www.math.titech.ac.jp/~shanekelly/\%E4\%BB\%A3\%E6\%95\%B0\%E5\%AD\%A6.html

Shane Kelly

東京工業大学

2020 年 7 月 29 日

1 Smith normal form

定理 1. R を単項イデアル整域とし、$A = [a_{ij}]_{1\leq i\leq n, 1\leq j\leq m}$ を $n \times m$ 行列とする。そのとき、ある可逆行列 $P \in GL_n(R)$ と $Q \in GL_m(R)$ が存在して、PAQ が次の形になる。

$$PAQ = \begin{pmatrix} e_1 & & & & \\ & e_2 & & & \\ & & \ddots & & \\ & & & e_s & \\ & & & & \end{pmatrix}$$

ここに、空白は 0 をあらわす。

注意 2. 上の形だと正方行列っぽく見えるが実は $n \times m$ 行列である。

上記の定理の証明のために、$a \in R$ に対して、$\delta(a) = (a$ の素因数の個数$)$ と定義する。すなわち、a を素元の積 $a = p_1^{i_1} p_2^{i_2} \dots p_n^{i_n}$ として書けば、

$$\delta(p_1^{i_1} p_2^{i_2} \dots p_n^{i_n}) = i_1 + i_2 + \cdots + i_n.$$

$$\delta(0) = \infty$$

とおく。

命題 3. R を単項イデアル整域とする、任意の $a, b \in R \setminus \{0\}$ に対して、可逆行列 $P \in GL_2(R)$ が存在して、

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

さらに、$\delta(gcd(a, b)) = \delta(a)$ の時、$P = \left[\begin{smallmatrix} 1 & 0 \\ * & * \end{smallmatrix}\right]$ と選べる.

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

$$P = \begin{pmatrix} 1 & 0 \\ \frac{-b}{a} & 1 \end{pmatrix}$$

とおけば良い。その他、$ad + bc = g$ 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、行列

$$P = \begin{pmatrix} d & c \\ \frac{-b}{g} & \frac{a}{g} \end{pmatrix}$$

が補題の条件をみたす：

$$\det P = d\tfrac{a}{g} - c\tfrac{-b}{g} = \tfrac{ad+bc}{g} = \tfrac{g}{g} = 1$$

■

命題 4. R を単項イデアル整域とする。任意の行列

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{i-1,1} & a_{i-1,2} & \dots & a_{i-1,m} \\ a_{i1} & a_{i2} & \dots & a_{im} \\ 0 & a_{i+1,2} & \dots & a_{i+1,m} \\ \vdots & \vdots & \dots & \vdots \\ 0 & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

に対して、$P \in GL_n(R)$ が存在して、

$$PA = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{i-1,1} & a_{i-1,2} & \dots & a_{i-1,m} \\ 0 & b_{i,2} & \dots & b_{i,m} \\ 0 & a_{i+1,2} & \dots & a_{i+1,m} \\ \vdots & \vdots & \dots & \vdots \\ 0 & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

さらに、

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

か

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

のどちらかをみたす P を選ぶことができる。

証明. 三つの場合を対処する。

$a_{i,1} = 0$ のとき、何もしなくても良い。

$a_{1,1} = 0$ のとき、1 行目と i 行目を入れ替え行列

$$\begin{pmatrix} 1 & & 0 & \\ & Id_{i-2} & & \\ 0 & & 1 & \\ & & & Id_{n-i} \end{pmatrix}.$$

を選ぶ。ここに、空白は 0 をあらわし、$Id_j \in GL_j(R)$ は単位行列である。

$a_{11} \neq 0$ かつ $a_{1i} \neq 0$ のとき、命題 3 において a_{11}, a_{1i} に対応する行列 $P = \left[\begin{smallmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{smallmatrix}\right]$ を用い、

$$\begin{pmatrix} p_{11} & & p_{12} & \\ & Id_{i-2} & & \\ p_{21} & & p_{22} & \\ & & & Id_{n-i} \end{pmatrix}.$$

を選ぶ。 ■

命題 5. R を単項イデアル整域とする、任意の行列

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

に対して、$P \in GL_n(R)$ が存在して、

$$PA = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ 0 & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \dots & b_{nm} \end{pmatrix}.$$

さらに、

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

か

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

のどちらかをみたす P を選ぶことができる。

証明. 命題 4 から従う。 ■

命題 6. R を単項イデアル整域とする、任意の行列

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

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

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

証明. 命題 5 とそれの転置を用いると、

$$B_1 = P_1 A, \qquad B_2 = P_1 A Q_1, \qquad B_3 = (P_2 P_1) A Q_1, \qquad B_4 = (P_2 P_1) A (Q_1 Q_2), \qquad \dots$$

が与えられる。左上成分の δ が減るから、ある N に対して、$B_N = B_{N+1} = B_{N+2} = \dots$ で、これらが命題の PAQ の形になる。 ■

命題 7. R を単項イデアル整域とする、任意の行列

$$A = \begin{pmatrix} a_{11} & & & & & \\ & \ddots & & & & \\ & & a_{ii} & a_{i,i+1} & \dots & a_{im} \\ & & a_{i+1,i} & a_{i+1,i+1} & \dots & a_{i+1,m} \\ & & \vdots & \vdots & & \vdots \\ & & a_{ni} & a_{n,i+1} & \dots & a_{n,m} \end{pmatrix}.$$

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

$$PAQ = \begin{pmatrix} a_{11} & & & & & \\ & \ddots & & & & \\ & & a_{i+1,i+1} & & & \\ & & & a_{i+2,i+2} & \dots & a_{i+2,m} \\ & & & \vdots & & \vdots \\ & & & a_{n,i+2} & \dots & a_{n,m} \end{pmatrix}.$$

証明.

$$\begin{pmatrix} a_{ii} & a_{i,i+1} & \dots & a_{im} \\ a_{i+1,i} & a_{i+1,i+1} & \dots & a_{i+1,m} \\ \vdots & \vdots & & \vdots \\ a_{ni} & a_{n,i+1} & \dots & a_{nm} \end{pmatrix}$$

に対して命題 6 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。 ■

定理の証明. 命題 7 から従う。 ■

2 PID 上の加群

定理 8. M を単項イデアル整域 R 上有限生成加群とする. 同型

$$M \cong R^{\oplus d} \oplus \bigoplus_{\text{素元 } p \in R} \left(\left(\frac{R}{(p)}\right)^{\oplus e_{p,1}} \oplus \left(\frac{R}{(p)^2}\right)^{\oplus e_{p,2}} \oplus \left(\frac{R}{(p)^3}\right)^{\oplus e_{p,3}} \oplus \dots \right)$$

が存在する。ここに、$d, e_{p,j} \in \mathbb{N}$、有限個を除いて $e_{p,j}$ がゼロである. さらに、$d, e_{p,j}$ は一意に定まる.

例 9. *1.* $R = \mathbb{Z}$ とき、有限生成アーベル群の基本定理になる.

2. R が離散付値環で、$\langle \pi \rangle$ が極大イデアルであれば、(例えば、

$$R = \mathbb{C}[[t]] = \{\sum_{i=0}^{\infty} a_i t^i \mid a_i \in \mathbb{C}\}, \qquad \pi = t$$

とか

$$R = \mathbb{Z}_{(p)} = \{\tfrac{a}{b} \mid b, p \text{ 互いに素 }\}, \qquad \pi = p$$

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

命題 10. $N \subseteq R^{\oplus n}$ 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
$$\pi : R^{\oplus n} \to R; \qquad (b_1, \ldots, b_n) \mapsto b_n$$
を考えよう．その核は
$$ker(\pi) = \{(b_1, b_2, \ldots, b_{n-1}, 0) \mid b_i \in R\}$$
である。
$$N' = N \cap ker(\pi) = \{(b_1, b_2, \ldots, b_n) \in N \mid b_n = 0\}$$
とおく．帰納法によって N' を生成する
$$\begin{aligned} a_1 &= (a_{1,1}, \ldots, a_{1,n_1}, 0, \ldots, 0, \ldots, 0, \ldots, 0) \\ a_2 &= (a_{2,1}, \ldots, a_{2,n_1}, \ldots, a_{2,n_2}, 0, \ldots, 0, \ldots, 0) \\ &\vdots \\ a_m &= (a_{m,1}, \ldots, a_{m,n_1}, \ldots, a_{m,n_2}, \ldots, a_{m,n_m}, 0, \ldots, 0) \end{aligned}$$
が存在する．ここに、$a_{ij} \in R$, $a_{i,n_i} \neq 0$, $n_1 < n_2 < \cdots < n_m$. もし $N' = N$ であれば、以上です．$N/N' \neq \{0\}$ 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 が PID). したがって、$c + N'$ が R 加群として N/N' を生成する $c = (c_1, \ldots, c_{n-1}, c_n) \in R^{\oplus n}$ が存在する．

そうすると、
$$\begin{aligned} a_1 &= (a_{1,1}, \ldots, a_{1,n_1}, 0, \ldots, 0, \ldots, 0, \ldots, 0) \\ a_2 &= (a_{2,1}, \ldots, a_{2,n_1}, \ldots, a_{2,n_2}, 0, \ldots, 0, \ldots, 0) \\ &\vdots \\ a_m &= (a_{m,1}, \ldots, a_{m,n_1}, \ldots, a_{m,n_2}, \ldots, a_{m,n_m}, 0, \ldots, 0) \\ c &= (c_1, \ldots, c_{n-1}, c_n) \end{aligned}$$
が N を R 加群として生成する：$n \in N$ をとって、$c + N'$ が N/N' を生成するから、ある $b \in R$ について $bc + N' = n + N'$. すなわち、$bc - n \in N'$. 元 a_i が N' を生成するので、ある $b_1, \ldots, b_m$ について $bc - n = \sum_{i=1}^m b_i a_i$. したがって、 $n = bc + \sum_{i=1}^m b_i a_i$. ■

注意 11. ツォルンの補題を用いると、上記の補題の有限生成仮定を外すことができて、M と N が一般な自由加群になる．

定理の証明. M が有限生成加群とは全射 $\pi : R^{\oplus n} \to M$ が存在することである．命題によって、π の核が $R^{\oplus m}$ に同型である．すなわち、単射 $\iota : R^{\oplus m} \to R^{\oplus n}$ が存在して、
$$0 \to R^{\oplus m} \xrightarrow{\iota} R^{\oplus n} \xrightarrow{\pi} M \to 0$$
が「完全系列」になる。

定義 12. R 加群準同型

$$M_{i_0} \to \ldots \to M_{i-1} \xrightarrow{\phi_i} M_i \xrightarrow{\phi_{i+1}} M_{i+1} \to \cdots \to M_{i_n}$$

が完全系列であるとは、任意の i に対して、

$$im(\phi_i) = ker(\phi_{i+1})$$

が成立することである

自由加群の準同型 ι に対応する $n \times m$ 行列 A を考えよう．可逆行列 P, Q が存在して、

$$PAQ = \begin{pmatrix} e_1 & & & & \\ & e_2 & & & \\ & & \ddots & & \\ & & & e_m & \\ & & & & \end{pmatrix}.$$

そうすると、行が完全系列である可換図式を得られる．

$$(b_1, \ldots, b_m) \quad \mapsto \quad (e_1 b_1, \ldots, e_m b_m, 0, \ldots, 0)$$

$$\begin{tikzcd}
0 \arrow[r] & R^{\oplus m} \arrow[r, "PAQ"] & R^{\oplus n} \arrow[r] & \left(\oplus_{i=1}^m R/\langle e_m \rangle\right) \oplus R^{\oplus n-m} \arrow[r] & 0 \\
0 \arrow[r] & R^{\oplus m} \arrow[r, "A"'] \arrow[u, "Q^{-1}"] & R^{\oplus n} \arrow[r] \arrow[u, "P"] & M \arrow[r] & 0
\end{tikzcd}$$

$$b \qquad \mapsto \qquad Ab$$

ここに、$e_1, \ldots, e_m$ はゼロや可逆元である可能性もある。

P と Q が同型を誘導するから、「図式追跡」によって、同型

$$M \cong \left(\oplus_{i=1}^m R/\langle e_m \rangle\right) \oplus R^{\oplus n-m}$$

が存在する．もしくは準同型定理によって、P が同型のおかげで、誘導される準同型

$$\frac{R^{\oplus n}}{\phi(R^{\oplus m})} \xrightarrow{P} \frac{R^{\oplus n}}{\iota(R^{\oplus m})}$$

は同型である．ここに、ι は A に対応する準同型で、ϕ は PAQ に対応する準同型である．

最後に、各 e_i を素元の積 $e_i = p_1^{j_1} p_2^{j_2} \ldots p_n^{j_\nu}$ として書けば、中国の剰余定理によって、同型

$$R/\langle e_i \rangle \cong \left(\frac{R}{\langle p_1^{j_{i1}} \rangle}\right) \oplus \left(\frac{R}{\langle p_2^{j_{i2}} \rangle}\right) \oplus \cdots \oplus \left(\frac{R}{\langle p_\nu^{j_{i\nu}} \rangle}\right)$$

となる．

一意性を証明するために同型

$$R^{\oplus d} \oplus \bigoplus_{\substack{\text{素元} \\ p \in R}} \bigoplus_{j \geq 1} \bigoplus_{i=1}^{e_{p,j}} \frac{R}{(p^j)} \cong M$$

$$\cong M' \cong R^{\oplus d'} \oplus \bigoplus_{\substack{\text{素元} \\ p \in R}} \bigoplus_{j \geq 1} \bigoplus_{i=1}^{e'_{p,j}} \frac{R}{(p^j)}$$

とし、素元 p において $R/\langle p \rangle$ ベクトル空間 $p^n M/p^{n+1}M$ を考えろう．素元 p, q は違えば、$R/\langle q \rangle$ で p が可逆元になる．ゆえに、

$$p^n \frac{R}{\langle q^j \rangle} / p^{n+1} \frac{R}{\langle q^j \rangle} \cong \frac{R}{\langle q^j \rangle} / \frac{R}{\langle q^j \rangle} = 0 \tag{1}$$

さらに、$n \geq j$ のとき、$p^n \frac{R}{\langle p^j \rangle} \cong 0$ で、

$$p^n \frac{R}{\langle p^j \rangle} / p^{n+1} \frac{R}{\langle p^j \rangle} = 0, \qquad n \geq j \tag{2}$$

となる．p^n と掛けれる準同型 ϕ_{p^n} は $R/\langle p \rangle$ 同型

$$\phi_{p^n} : R/\langle p \rangle \xrightarrow{\sim} p^n R/p^{n+1}R; \quad a + pR \mapsto p^n a + p^{n+1}R \tag{3}$$

となる．同様に、$n < j$ の場合に、

$$\phi_{p^n} : R/\langle p \rangle \xrightarrow{\sim} p^n \frac{R}{\langle p^j \rangle} / p^{n+1} \frac{R}{\langle p^j \rangle}, \qquad n < j \tag{4}$$

したがって、ある N に対して, 上記の R 同型 (1)、(2)、(3)、(4) は $R/\langle p \rangle$ 同型

$$p^n M/p^{n+1}M \cong \left(\frac{R}{\langle p \rangle}\right)^{\oplus d} \oplus \bigoplus_{j>n} \left(\frac{R}{\langle p \rangle}\right)^{\oplus e_{p,j}}$$

になる. 同様に、

$$p^n M'/p^{n+1}M' \cong \left(\frac{R}{\langle p \rangle}\right)^{\oplus d'} \oplus \bigoplus_{j>n} \left(\frac{R}{\langle p \rangle}\right)^{\oplus e'_{p,j}}$$

同型なベクトル空間の次元が等しいですので、任意の p, n に対して

$$\begin{aligned} &d + e_{p,n+1} + e_{p,n+2} + e_{p,n+3} + \dots \\ =&d' + e'_{p,n+1} + e'_{p,n+2} + e'_{p,n+3} + \dots \end{aligned}$$

がわかる．したがって、$d = d'$, $e_{p,j} = e'_{p,j}\ \forall p, j$. ■

3 Jordan 標準形

定理 13. V を代数閉体 k 上の有限次元ベクトル空間とし、$\phi : V \to V$ を線型写像とする。同伴な行列が次の形になる基底が存在する。

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_n \end{pmatrix}$$

ここに、空白は 0 をあらわし、ある λ_i に対し、J_i は次の形になる正方行列である.

$$\begin{pmatrix} \lambda_i & 1 & & \\ & \lambda_i & 1 & \\ & & \ddots & 1 \\ & & & \lambda_i \end{pmatrix}.$$

証明. スカラー倍

$$k[T] \times V \mapsto V; \qquad (\sum_{i=1}^{n} a_i T^i, v) \mapsto \sum_{i=1}^{n} a_i \phi^i(v)$$

を定義すると、V は $k[T]$ 加群になる. ここに、$\phi^i = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_{i\ 部数}$. k ベクトル空間 V は有限次元ですので、$k[T]$ 加群 V は有限生成である. したがって、$k[T]$ 加群同型

$$V \cong k[T]^{\oplus d} \oplus \left(\bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \bigoplus_{k=1}^{e_{i,j}} \frac{k[T]}{(p_i(T))^j} \right)$$

が存在する. ここに、$p_i(T) \in k[T]$ は既約元である. k が代数閉体であるから、ある $\lambda_i \in k$ に対して $p_i(T) = T - \lambda_i$. 上記の同型は k ベクトル空間同型でもある. 左側の次元は有限ですので、右側の次元も有限である. ゆえに、$d = 0$. ゆえに、

$$V \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \bigoplus_{k=1}^{e_{i,j}} \frac{k[T]}{(T - \lambda_i)^j}$$

右側の自己準同型 $f \mapsto Tf$ を ϕ_T と表そう.

$$\begin{array}{ccc} V & \cong & \bigoplus_{i,j,k} \frac{k[T]}{(T-\lambda_i)^j} \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_T} \\ V & \cong & \bigoplus_{i,j,k} \frac{k[T]}{(T-\lambda_i)^j} \end{array}$$

は可換図式ですので、ϕ_T の行列が

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_n \end{pmatrix}$$

になる右側の基底を見つけたら良い. 明らかに、$\frac{k[T]}{\langle T-\lambda \rangle^j}$ の場合を扱えば良い. k ベクトル空間として, 元

$$\overline{(T-\lambda)^{j-1}}, \overline{(T-\lambda)^{j-2}}, \ldots, \overline{T-\lambda}, \overline{1}, \in \frac{k[T]}{\langle T-\lambda \rangle^j}$$

が基底をなす. この基底に対して線型写像

$$\phi_T : \frac{k[T]}{\langle T - \lambda \rangle^j} \to \frac{k[T]}{\langle T - \lambda \rangle^j}; \qquad \overline{f(T)} \mapsto \overline{Tf(T)}$$

に対応する行列は

$$\begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

である. ■

注意 14. $n \times n$ 行列

$$J = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

は $(T - \lambda \cdot Id_n)^n = 0$ をみたす. より一般に行列

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_n \end{pmatrix} \quad \text{（ここに、}J_i = \begin{pmatrix} \lambda_i & 1 & & \\ & \lambda_i & 1 & \\ & & \ddots & 1 \\ & & & \lambda_i \end{pmatrix}\text{）}$$

の固有値は $\lambda_1, \dots, \lambda_n$ で、最小多項式は $(T - \lambda_1)^{j_1} \dots (T - \lambda_n)^{j_n}$ である. ここに、$j_i = J_i$ の大きさである.