線形代数学演習

黒木玄 2005 年 6 月 20 日 (教師用)

目 次

14　必修問題

14.1　正規行列

複素正方行列 A が**正規 (normal)** であるとは $A^*A = AA^*$ が成立することである. たとえば Hermite 行列 ($A^* = A$) や反 Hermite 行列 ($A^* = -A$) やユニタリ行列 ($A^* = A^{-1}$) は正規行列である.

ユニタリ行列による相似変換で対角化可能な複素正方行列は正規であることは容易に確かめられる ([**192**]). これの逆が成立する ([**194**]).

定理 14.1 (Toeplitz の定理) 任意の正規行列はユニタリ行列による相似変換で対角化可能である. □

例 14.2 複素正方行列 $A = \begin{bmatrix} 1 & i & 0 \\ -i & 2 & -i \\ 0 & i & 1 \end{bmatrix}$ は Hermite 行列なので正規行列である. よって Toeplitz の定理より, ユニタリ行列で対角化可能である. そのことを確かめよう.

A の特性多項式は $p_A(t) = |tE - A| = t(t-1)(t-3)$ なので A の固有値は $t = 0, 1, 3$ である. (一般に Hermite 行列の固有値はすべて実数になる.)

固有値 $0, 1, 3$ のそれぞれに属する単位固有ベクトル[1] u_1, u_2, u_3 として以下が取れることがわかる:

$$u_1 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ i \\ 1 \end{bmatrix}, \quad u_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \quad u_3 = \frac{1}{\sqrt{6}} \begin{bmatrix} 1 \\ -2i \\ 1 \end{bmatrix}.$$

これらは互いに直交するので行列 $U = [u_1, u_2, u_3]$ はユニタリ行列である.

このとき

$$A = U \operatorname{diag}(0, 1, 3) U^{-1} = U \operatorname{diag}(0, 1, 3) U^*$$

が成立している. □

[**149**] **(5 点)** 上の例の計算が正しいことを確かめよ. □

[**150**] **(15 点)** 次の行列が正規であることを確かめ, ユニタリ行列で対角化せよ:

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & i & 0 \\ i & 2 & 2i \\ 0 & 2i & 2 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & -i & 1 \\ i & 1 & i \\ 1 & -i & 1 \end{bmatrix}. \quad \square$$

ヒント. B が正規であることは $B - 2E$ が反 Hermite 行列であることに気付けば容易に確かめられる. C の固有値の一つは重複しているので, 固有空間の正規直交基底を Schmidt の正規直交化法などの方法で作らなければいけない. □

略解. A は対称行列なので直交行列で対角化できる. A の固有値は $1, 2, 4$ であり, それぞれに属する単位固有ベクトルとして以下が取れる:

$$\frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}, \quad \frac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}, \quad \frac{1}{\sqrt{6}} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}.$$

[1] ノルムが 1 の固有ベクトルのこと.

一般に n 次の正規行列 X と n 次の単位行列 E と複素数 c に対して $X+cE$ も正規行列になることが容易に確かめらる. $B-2E$ は反 Hermite 行列なので正規である. よって B 自身も正規である. B の固有値は $2, 2+\sqrt{5}i, 2-\sqrt{5}i$ であり, それぞれに属する単位固有ベクトルとして次が取れる:

$$\frac{1}{\sqrt{5}}\begin{bmatrix}2\\0\\-1\end{bmatrix},\quad \frac{1}{\sqrt{10}}\begin{bmatrix}1\\\sqrt{5}\\2\end{bmatrix},\quad \frac{1}{\sqrt{10}}\begin{bmatrix}1\\-\sqrt{5}\\2\end{bmatrix}.$$

C は Hermite 行列なので正規行列である. C の固有値は 0 (重複度 2) と 3 である. 固有値 0 に属する固有空間の正規直交基底 u_1, u_2 と固有値 3 に属する単位固有ベクトル u_3 として次が取れる:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}i\\1\\0\end{bmatrix},\quad \frac{1}{\sqrt{6}}\begin{bmatrix}1\\i\\-2\end{bmatrix},\quad \frac{1}{\sqrt{3}}\begin{bmatrix}1\\i\\1\end{bmatrix}.\quad \square$$

[151] (5 点) 以下を示せ:

1. Hermite 行列と実対称行列の固有値は実数である.
2. 反 Hermite 行列と実交代行列の固有値は純虚数[2]である.
3. ユニタリー行列と実直交行列の固有値の絶対値は 1 である. $\square$

ヒント. 実対称行列, 実交代行列, 実直交行列のそれぞれは Hermite 行列, 反 Hermite 行列, ユニタリー行列の特別な場合である. A は複素 n 次行列であり, $\alpha\in\mathbb{C}$ は A の固有値であり, $Au=\alpha u$, $u\in\mathbb{C}^n$, $u\neq 0$ と仮定する. A が Hermite ($A^*=A$) ならば

$$\overline{\alpha}(u,u)=(Au,u)=\text{以下略}$$

よって $\overline{\alpha}=\alpha$ となり, α は実数になる. A が反 Hermite ($A^*=-A$) ならば

$$\overline{\alpha}(u,u)=(Au,u)=\text{以下略}$$

よって $\overline{\alpha}=-\alpha$ となり, α は純虚数になる. A がユニタリ ($A^*A=AA^*=E$) ならば

$$|\alpha|^2(u,u)=(Au,Au)=\text{以下略}$$

よって $|\alpha|^2=1$ となり, α の絶対値は 1 になる. $\square$

[152] (5 点) Hermite 行列 A の異なる固有値に属する固有ベクトルは互いに直交する. $\square$

ヒント. A は n 次の Hermite 行列であるとし, $\mathbb{C}^n$ の標準的な内積を $(u,v)=u^*v$ ($u,v\in\mathbb{C}^n$) と書くことにする. A の固有値はすべて実数である. A の互いに異なる固有値 $\alpha,\beta\in\mathbb{R}$ とそれぞれに属する固有ベクトル u,v を任意に取る. このとき

$$\alpha(u,v)=(Au,v)=\text{以下略}$$

$\alpha\neq\beta$ であるから $(u,v)=0$. $\square$

[2]虚数単位の実数倍を純虚数と呼ぶ.

[153] (5 点) 任意の正規行列は互いに可換な Hermite 行列と反 Hermite 行列の和で一意に表わされる. □

ヒント. A が正規行列ならば $A_\pm = (A \pm A^*)/2$ は……. □

参考 14.3 上の問題の結果は任意の複素数が実数と純虚数の和で一意に表わされることの一般化になっている. □

固有値がすべて非負の実数であるような Hermite 行列を非負の Hermite 行列と呼ぶことにする.

[154] (5 点) 任意の正規行列は互いに可換な非負の Hermite 行列とユニタリ行列の積で表わされる. □

ヒント. 正規行列 A は Toeplitz の定理より, あるユニタリ行列 P と A の固有値を対角成分に持つ対角行列 A_0 によって $A = PA_0P^{-1} = PA_0P^*$ と表わされる. A_0 は対角成分が非負の実数である対角行列 H_0 と対角成分が絶対値 1 の複素数である対角行列 U_0 によって $A_0 = H_0U_0 = U_0H_0$ と表わされる. $H = \cdots, U = \cdots$ と置く. そのとき……. □

参考 14.4 上の問題の結果は任意の複素数が非負の実数と絶対値が 1 の複素数の積で表わされることの一般化になっている. □

14.2 Sylvester の慣性法則

実対称行列 $A = [a_{ij}]$ から

$$Q(x) = \sum_{i,j=1}^{n} a_{ij}x_ix_j = (x, Ax) \qquad (x = {}^t(x_1, \ldots, x_n) \in \mathbb{R}^n)$$

によって定められた函数 $Q(x)$ を実二次形式と呼ぶ. ここで $(\ ,\ )$ は $\mathbb{R}^n$ の標準的な内積である. (座標不変な定義の仕方もあるが, ここでは簡単のためこのように定義しておく.)

二つの実二次形式 $Q_1(x)$, $Q_2(x)$ が同値であるとはある可逆な実正方行列 $T \in GL_n(\mathbb{R})$ で $Q_2(x) = Q_1(Tx)$ を満たすものが存在することである.

実対称行列 A の固有値 $\alpha_1, \ldots, \alpha_n$ はすべて実数であり, A はある (実) 直交行列 K によって対角化される:

$$A = KA_0K^{-1} = KA_0\,{}^tK, \qquad A_0 := \mathrm{diag}(\alpha_1, \ldots, \alpha_n).$$

よって実二次形式 $Q(x) = (x, Ax)$ は次の二次形式と同値になる:

$$Q(Kx) = (Kx, AKx) = (x, K^{-1}AKx) = (x, A_0x) = \alpha_1x_1^2 + \cdots + \alpha_nx_n^2.$$

必要ならば順番を並べ変えて $\alpha_1, \ldots, \alpha_p > 0$, $\alpha_{p+1}, \ldots, \alpha_{p+q} < 0$, $\alpha_{p+q+1} = \cdots = \alpha_n = 0$ と仮定できる. このとき

$$D = \mathrm{diag}(|\alpha_1|^{-1/2}, \ldots, |\alpha_{p+q}|^{-1/2}, 1, \ldots, 1)$$

と置けば D は可逆な実対角行列であり,

$$Q(KDx) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2.$$

これを $Q(x)$ の標準形と呼び, (p,q) を $Q(x)$ の**符号数 (signature)** と呼ぶことにする. 以上の議論では任意の実二次形式はある標準形と同値であることしか証明されておらず, 標準形の一意性 (符号数の一意性) も標準形が等しい二つの実二次形式が同値であることも証明されていない. しかしそれらの結果は成立しており, その結果は **Sylvester の慣性法則 (Sylvester's law of inertia)** と呼ばれている. 以上の結果をまとめておこう.

定理 14.5 (Sylvester, 実二次形式の分類) 任意の実二次形式 $Q(x)$ に対してある非負の整数の組 (p,q) が存在して $Q(x)$ は次の標準形に同値になる:

$$Q_{p,q}(x) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2.$$

しかも (p,q) は $Q(x)$ から一意的に定まり, 二つの実二次形式が同値になるための必要十分条件はそれぞれの (p,q) が一致することである. □

[155] (10 点) つぎの実二次形式の符号数を求めよ:

(1) $f(x,y,z) = x^2 + y^2 + 4z^2 + 2xy + 4xz + 8yz$,

(2) $g(x,y,z) = 4xy - 8xz + 4yz$. □

ヒント: 文字 $x, y, \ldots$ について順次「平方完成」を実行し, 最終的に一次式の平方の一次結合の形に変形する. その一次結合の正の係数の個数と負の係数の個数の組が符号数である. たとえば

$$\begin{aligned} &x^2 - y^2 - 4z^2 + 2xy + 2xz - 2yz \\ &= x^2 + 2(y+z)x - y^2 - 4z^2 - 2yz = (x+y+z)^2 - (y+z)^2 - y^2 - 4z^2 - 2yz \\ &= (x+y+z)^2 - 2y^2 - 4yz - 5z^2 = (x+y+z)^2 - 2(y+z)^2 - 3z^2 \end{aligned}$$

の符号数は $(1,2)$ である. ただし $(X,Y,Z) = (x+y+z, x+y, z)$ という変数変換が可逆で重要である. たとえば $x^2 + y^2 - x^2$ の符号数は $(2,-1)$ ではなく $(1,0)$ である.

平方項 (x^2, y^2, z^2 のような項) がない場合には公式 $xy = [(x+y)^2 - (x-y)^2]/4$ を用いて計算を先に進める. もしくは $x = (X+Y)/2$, $y = (X-Y)/2$ (すなわち $X = x+y$, $Y = x-y$) と置いて計算を先に進める. □

略解. (1) x について平方完成し, $4yz = (y+z)^2 - (y-z)^2$ を使うと,

$$f(x,y,z) = x^2 + y^2 + 4z^2 + 2xy + 4xz + 8yz = (x+y+2z)^2 + (y+z)^2 - (y-z)^2.$$

よって符号数は $(2,1)$ である.

(2) $x = (X+Y)/2$, $y = (X-Y)/2$ と置くと

$$\begin{aligned} g(x,y,z) &= 4xy - 8xz + 4yz = (X+Y)(X-Y) - 4(X+Y)z + 2(X-Y)z \\ &= X^2 - Y^2 - 2zX - 6zY = (X-z)^2 - z^2 - Y^2 - 6zY \\ &= (X-z)^2 - (Y+3z)^2 + 9z^2 - z^2 = (X-z)^2 - (Y+3z)^2 + 8z^2 \\ &= (x+y-z)^2 - (x-y+3z)^2 + 8z^2. \end{aligned}$$

よって符号数は $(2,1)$. □

[156] (5 点) $Q(x,y)$ は変数 x,y に関する実二次形式であるとする．任意の実数 $h \in \mathbb{R}$ に対してある実数 $a,b \in \mathbb{R}$ で $Q(a,b) = h$ となるものが存在すると仮定する．このとき $Q(x,y)$ の符号数は $(1,-1)$ である． □

ヒント. $Q(x,y)$ の符号数が $(1,-1)$ 以外のとき, $Q(x,y)$ が問題の条件を満たさないことを確認せよ． □

[157] (10 点) 変数 x,y に関する二次形式 $Q(x,y)$ の符号数が $(2,0)$, $(1,1)$, $(0,2)$ のそれぞれの場合において, $\mathbb{R}^2$ 上の函数 $z = Q(x,y)$ のグラフの概形はどのような形になるかを図を描いて説明せよ． □

ヒント. 函数 $z = Q(x,y)$ のグラフは xy 平面上の曲面になる．(x,y) 座標を適当に回転して得られる座標を (X,Y) とすると, $Q(x,y)$ は $Q(x,y) = \alpha X^2 + \beta Y^2$ と表わされる．$Q(x,y)$ の符号数が $(2,0)$ ならば $\alpha,\beta > 0$ であり, $(0,2)$ の場合には $\alpha,\beta < 0$ であり, $(1,1)$ の場合には必要ならば (X,Y) 座標をさらに 90 度回転することによって $\alpha > 0$, $\beta < 0$ と仮定できる．X,Y 座標で函数 $z = Q(x,y) = \alpha X^2 + \beta Y^2$ のグラフの概形を描け． □

14.3 Jordan 標準形の計算

2 次および 3 次行列の Jordan 標準形を計算する問題 [**42**], [**56**] は必修であるとする．

[158] (各 A_i ごとに 10 点) 以下の実正方行列 A_i の Jordan 標準形 J_i と $P_i^{-1}A_iP_i = J_i$ を満たす正則行列 P_i の例を一つ求めよ:

$$A_1 = \begin{bmatrix} -25 & 6 & -7 & 21 \\ 9 & -2 & 2 & -5 \\ 21 & -4 & 4 & -17 \\ -23 & 6 & -7 & 19 \end{bmatrix}, \quad A_2 = \begin{bmatrix} -17 & 12 & 0 & -12 \\ 0 & 7 & -8 & -24 \\ -72 & 36 & 17 & 0 \\ 24 & -10 & -8 & -7 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 12 & -8 & 11 & 3 \\ 9 & -8 & 9 & 0 \\ -5 & 2 & -4 & -3 \\ -8 & 5 & -8 & -2 \end{bmatrix},$$

$$A_4 = \begin{bmatrix} -4 & -6 & 5 & 5 \\ -4 & 7 & -9 & -11 \\ -24 & -9 & 1 & -3 \\ 16 & 12 & -7 & -6 \end{bmatrix}, \quad A_5 = \begin{bmatrix} -5 & 8 & -6 & 4 \\ -3 & 5 & -5 & 4 \\ -2 & 4 & -5 & 4 \\ -1 & 2 & -2 & 1 \end{bmatrix}, \quad A_6 = \begin{bmatrix} -12 & 2 & -3 & 9 \\ 22 & -5 & 6 & -18 \\ 22 & -4 & 5 & -18 \\ -11 & 2 & -3 & 8 \end{bmatrix}. \quad \square$$

ヒント: 固有値がすべて整数になるように問題を作ってある．がんばって計算しましょう．実は 4×4 の Jordan 標準形のパターンをできるだけ網羅するように問題が作ってある．単なる計算問題だが点数を高めに設定した．(サービス!) □

略解: 以下のように J_i, P_i を定めると $P_i^{-1}A_iP_i = J_i$ である:

$$J_1 = \begin{bmatrix} -2 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad J_2 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad J_3 = \begin{bmatrix} -2 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$P_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ -2 & -1 & 0 & 1 \\ -2 & -1 & -3 & 0 \\ 1 & 0 & -1 & 1 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 3 & 0 & 4 & 2 \\ 6 & -1 & 4 & 4 \\ 0 & 2 & 9 & 0 \\ 2 & -1 & -2 & 1 \end{bmatrix}, \quad P_3 = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & 3 & 1 & 1 \\ -1 & 0 & 0 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix},$$

$$J_4=\begin{bmatrix}-2&1&0&0\\0&-2&0&0\\0&0&1&1\\0&0&0&1\end{bmatrix},\qquad J_5=\begin{bmatrix}-1&1&0&0\\0&-1&0&0\\0&0&-1&1\\0&0&0&-1\end{bmatrix},\quad J_6=\begin{bmatrix}-1&1&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&-1\end{bmatrix},$$

$$P_4=\begin{bmatrix}-1&0&-2&-1\\2&1&5&2\\0&2&3&0\\2&-1&1&1\end{bmatrix},\quad P_5=\begin{bmatrix}4&3&2&1\\3&3&2&1\\2&2&2&1\\1&1&1&1\end{bmatrix},\qquad P_6=\begin{bmatrix}1&0&1&1\\-2&-1&1&1\\-2&-1&-3&0\\1&0&0&1\end{bmatrix}.$$

A_i の最小多項式を $\varphi_i(\lambda)$ と書くと,

$$\varphi_1(\lambda)=(\lambda+2)^3(\lambda-2),\quad \varphi_2(\lambda)=(\lambda+1)(\lambda-1),\quad \varphi_3(\lambda)=(\lambda+2)^2(\lambda-1),$$
$$\varphi_4(\lambda)=(\lambda+2)^2(\lambda-1)^2,\quad \varphi_5(\lambda)=(\lambda+1)^2,\qquad \varphi_6(\lambda)=(\lambda+1)^2,$$

A_5 と A_6 の最小多項式は等しいのに Jordan 標準形は異なることに注意せよ. そのようなことは 3 次行列では起こり得ない. 3 次以下の行列では最小多項式だけで Jordan 標準形がわかってしまう. □

計算問題の作り方: 上のような問題を作るのときには, まず正則行列 P を色々作る. Jordan 標準形 J を任意に用意して $A=PJP^{-1}$ を計算して「A の Jordan 標準形を求めよ」とすれば計算問題のいっちょあがりである. 問題は逆行列の計算が易しい P を系統的に生成することである. 逆行列の分母には $\det P$ が登場する. だから A を整数だけで構成された行列にしたければ分母の $\det P$ が 1 であることが望ましい. その場合は逆行列の計算も易しくなる.

行列式が 1 の n 次正方行列全体の集合 $SL_n(K)$ は群をなし, その任意の元は $E+aE_{ij}$ $(a\in K, i\neq j)$ の形の行列を有限個かけ合わせたもので表わせる. (E_{ij} は (i,j) 成分だけが 1 で他の成分が 0 であるような正方行列であり, 行列単位と呼ばれている.) 成分を整数に制限した $SL_n(\mathbb{Z})$ の場合もその任意の元は $E+nE_{ij}$ $(n\in K, i\neq j)$ の形の行列を有限個かけ合わせたもので表わせる. この事実を使えば整数を成分に持つ行列式が 1 の行列を系統的に生成できる. 実は $SL_n(\mathbb{Z})$ の任意の元は $E\pm E_{i,i+1}$, $E\pm E_{i+1,i}$ の有限個の積で表示できる. □

15　Zornの補題の応用の追加

[159] (10 点) Zornの補題を用いて次を示せ. K は任意の体であり, U, V は K 上の任意のベクトル空間であるとし, W は V の任意の部分空間であるとする. このとき任意の線形写像 $f : W \to U$ に対してある線形写像 $g : V \to U$ で g の W 上への制限が f に等しいものが存在する. □

ヒント. V の部分空間 A と線形写像 $g : A \to U$ の組 (A, g) 全体の集合に「写像の拡張になっているか否か」で順序関係を入れてZornの補題を適用せよ. □

[160] (10 点) Zornの補題を用いて次を示せ. K は任意の体であり, V は K 上の任意のベクトル空間であるとし, W は V の任意の部分空間であるとする. このとき V のある部分空間 W' で $V = W \oplus W'$ (すなわち $V = W + W'$ かつ $W \cap W' = \{0\}$) を満たすものが存在する. □

ヒント. V の部分空間 W' で $W \cap W' = \{0\}$ を満たすもの全体の集合に包含関係で順序を入れ, Zornの補題を適用せよ. □

注意 15.1 以上の結果は「ベクトル空間 V の任意の一次独立な部分集合を V の基底に拡張できる」というZornの補題を使って証明できる結果を使えば容易に証明できる. □

16　内積とノルム

16.1　内積とノルムの基本性質

複素 $m \times n$ 行列 A に対して, その転置行列を ${}^tA$ と書き, A の各成分の複素共役を取ってできる行列を $\overline{A}$ と書く. A の**随伴行列 (adjoint matrix)** A^* を

$$A^* := \overline{{}^tA} = {}^t\overline{A}$$

と定める. すなわち,

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \implies A^* = \begin{bmatrix} \overline{a_{11}} & \overline{a_{21}} & \cdots & \overline{a_{m1}} \\ \overline{a_{12}} & \overline{a_{22}} & \cdots & \overline{a_{m2}} \\ \vdots & \vdots & & \vdots \\ \overline{a_{1n}} & \overline{a_{2n}} & \cdots & \overline{a_{mn}} \end{bmatrix}.$$

たとえば, x が縦ベクトルならば x^* は横ベクトルになり, 逆も成立する:

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \implies x^* = \begin{bmatrix} \overline{x_1} & \cdots & \overline{x_n} \end{bmatrix}.$$

[161] (5 点) A, A_1, A_2 は複素 $l \times m$ 行列であり, B は複素 $m \times n$ 行列であるとし, $a_1, a_2 \in \mathbb{C}$ とすると以下が成立する:

1. $(AB)^* = B^*A^*$.

2. $(a_1A_1 + a_2A_2)^* = \overline{a_1}A_1^* + \overline{a_2}A_2^*$. □

縦ベクトルからなる n 次元複素ベクトル空間 $\mathbb{C}^n$ に標準的な内積 $\langle\ ,\ \rangle$ を次のように定める:

$$\langle x, y\rangle := x^*y = \sum_{i=1}^{n} \overline{x_i}y_i, \qquad \left(x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}, \quad x_i, y_i \in \mathbb{C} \right).$$

横ベクトル × 縦ベクトル がスカラーになることに注意せよ.

[162] (内積の基本性質, 5 点) $x, x_1, x_2, y, y_1, y_2 \in \mathbb{C}^n$ と $a_1, a_2, b_1, b_2 \in \mathbb{C}$ に対して以下が成立する:

1. $\langle y, x\rangle = \overline{\langle x, y\rangle}$.
2. $\langle x, b_1y_1 + b_2y_2\rangle = b_1\langle x, y_1\rangle + b_2\langle x, y_2\rangle$ **(線形性)**.
3. $\langle a_1x_1 + a_2x_2, y\rangle = \overline{a_1}\langle x_1, y\rangle + \overline{a_2}\langle x_2, y\rangle$ **(反線形性)**.
4. $\langle x, x\rangle \geq 0$ であり, 等号が成立するための必要十分条件は $x = 0$ である.

これらを内積の基本性質と呼ぶことにする. □

一般に複素ベクトル空間 V に問題 **[162]** の性質を満たす写像 $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$ が与えられているとき, V を**前 Hilbert 空間 (pre-Hilbert space)** と呼び[3], $\langle\ ,\ \rangle$ を**内積 (inner product, scalar product)** と呼ぶ. 問題 **[162]** の結果より, 標準的な内積を入れた $\mathbb{C}^n$ は pre-Hilbert 空間である.

V が pre-Hilbert 空間であるとき, $x \in V$ のノルム $||x||$ を次のように定義する:

$$||x|| := \sqrt{\langle x, x\rangle}.$$

たとえば, $V = \mathbb{C}^n$ のとき $x = {}^t[x_1\ \cdots\ x_n]$ ならば

$$||x|| = \left(\sum_{i=1}^{n} |x_i|^2 \right)^{1/2}.$$

前 Hilbert 空間の 2 つのベクトル x, y が $\langle x, y\rangle = 0$ を満たしているとき, x と y は直交していると言う. ノルムが 1 に等しいベクトルは単位ベクトルと呼ばれる. 前 Hilbert 空間 V の基底 $\{v_i\}_{i\in I}$ が

$$\langle v_i, v_j\rangle = \delta_{ij} \qquad (i, j \in I)$$

を満たしているとき, $\{v_i\}_{i\in I}$ は V の**正規直交基底 (orthonormal basis)** であると言う. ここで δ_{ij} は Kronecker のデルタである. すなわち, $i = j$ ならば $\delta_{ij} = 1$ であり, $i \neq j$ ならば $\delta_{ij} = 0$ である. たとえば, $\mathbb{C}^n$ における標準的な基底

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

[3] **Hilbert 空間 (Hilbert space)** とは完備な pre-Hilbert 空間のことである. 完備であるとは任意の Cauchy 列が収束することである. この段階では完備性の有無については気にしなくて良い. 意識を集中して欲しいのは内積の基本性質 (公理) だけを用いて, どれだけの結論を導き出せるかについてである.

は $\mathbb{C}^n$ の正規直交基底である. 正規直交基底の理論は Fourier 解析の理論の抽象化とみなせる.

[163] (10 点) $f(z)$ が z に関する複素 Laurent 多項式であるとは,

$$f(z) = \sum_{k=-m}^{n} a_k z^k \qquad (a_k \in \mathbb{C},\ m, n \in \mathbb{Z}_{\geq 0})$$

と表示可能な有理式であることである. 複素 Laurent 多項式全体の集合を $\mathbb{C}[z, z^{-1}]$ と書く. 写像 $\langle\ ,\ \rangle : \mathbb{C}[z, z^{-1}] \times \mathbb{C}[z, z^{-1}] \to \mathbb{C}$ を

$$\langle f, g \rangle := \int_0^1 \overline{f(e^{2\pi i x})} g(e^{2\pi i x})\, dx \qquad \big(f, g \in \mathbb{C}[z, z^{-1}]\big)$$

と定めると, $\langle\ ,\ \rangle$ は内積の基本性質を満たしており, $\mathbb{C}[z, z^{-1}]$ は pre-Hilbert 空間になる. さらに, $\{z^k\}_{k\in\mathbb{Z}}$ は $\mathbb{C}[z, z^{-1}]$ の正規直交基底になる. □

[164] (10 点) 複素係数の 1 変数多項式全体の集合を $V = \mathbb{C}[x]$ と書く. $\mathbb{C}[x]$ は自然に複素ベクトル空間とみなせる. 各多項式 $f(x) \in V$ は自然に $\mathbb{R}$ 上の函数とみなせる. 写像 $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$ を

$$\langle f, g \rangle := \int_{-\infty}^{\infty} \overline{f(x)} g(x)\, e^{-x^2} dx \qquad \big(f, g \in V\big)$$

と定めると, $\langle\ ,\ \rangle$ は内積の基本性質を満たしており, $V = \mathbb{C}[x]$ は pre-Hilbert 空間になる. $\{x^k\}_{k\in\mathbb{Z}_{\geq 0}}$ は $V = \mathbb{C}[x]$ の基底であるが, 正規直交基底ではない. □

[165] (10 点) 閉区間 $[a, b]$ 上の複素数値連続函数全体の空間を $C([a, b])$ と書くことにする. $C([a, b])$ は自然に複素ベクトル空間をなす. 写像 $\langle\ ,\ \rangle : C([a, b]) \times C([a, b]) \to \mathbb{C}$ を

$$\langle f, g \rangle := \int_a^b \overline{f(x)} g(x)\, dx \qquad \big(f, g \in C([a, b])\big)$$

と定めると, $C([a, b])$ は pre-Hilbert 空間をなす[4]. □

[166] (Cauchy-Schwarz の不等式, 10 点) V は pre-Hilbert 空間であるとする. このとき, 任意の $x, y \in V$ に対して,

$$|\langle x, y \rangle| \leq ||x|| \cdot ||y||\,.$$

等号が成立するための必要十分条件は x, y のどちらかがもう一方の複素数倍になっていることである. □

ヒント: $x \neq 0$ と仮定して良い (それはどうしてか?). $z = y - ax$ が x と直交するように $a \in \mathbb{C}$ を定め, y のノルムの 2 乗を x と z で表わしてみよ. □

略解: $a = \langle x, y \rangle / \langle x, x \rangle$ であるから,

$$||y||^2 = \langle z + ax, z + ax \rangle = \langle z, z \rangle + |a|^2 \langle x, x \rangle \geq |a|^2 \langle x, x \rangle = \frac{|\langle x, y \rangle|^2}{||x||^2}.$$

ここで, 2 つ目の等号で x と z が直交することを用いた. 途中の不等号で等号が成立するための必要十分条件は $z = 0$ すなわち $y = ax$ である. □

[4] $C([a, b])$ を完備化することによって得られる Hilbert 空間を $[a, b]$ 上の L_2 空間と呼び, $L_2([a, b])$ のように表わす.

[167] (ノルムの基本性質, 10 点) V が pre-Hilbert 空間であるとき, $x, y \in V$ と $a \in \mathbb{C}$ に対して以下が成立する:

1. $||x|| \geq 0$ であり, 等号が成立するための必要十分条件は $x = 0$ である.
2. $||ax|| = |a| \cdot ||x||$.
3. $||x + y|| \leq ||x|| + ||y||$ **(三角不等式)**. □

ヒント: 三角不等式の証明には Cauchy-Schwarz の不等式と $\mathrm{Re}\langle x, y\rangle \leq |\langle x, y\rangle|$ を使う. □

参考: pre-Hilbert 空間の場合には次も成立している: 三角不等式において等号が成立するための必要十分条件は x, y のどちらかがもう一方の非負の実数倍になっていること (直観的には x, y が同じ方向を向いていること) である. 余裕があればこの事実も示してみよ. □

略解: 三角不等式のみを証明しよう. $x, y \in V$ に対して,

$$(||x|| + ||y||)^2 - ||x + y||^2 = 2(||x|| \cdot ||y|| - \mathrm{Re}\langle x, y\rangle) \leq 2(||x|| \cdot ||y|| - |\langle x, y\rangle|) \leq 0.$$

1 つ目の不等号は $\mathrm{Re}\langle x, y\rangle \leq |\langle x, y\rangle|$ より. 2 つ目の不等号は Cauchy-Schwarz の不等式より. $x \neq 0$ のとき, 2 つの不等号が共に等号になるための必要十分条件はある $a \in \mathbb{C}$ が存在して $y = ax$ かつ $\mathrm{Re}\, a = |a|$ が成立することである. □

一般に, 複素ベクトル空間 V に問題 **[167]** の性質を持つ写像 $||\ ||: V \to \mathbb{R}$ が与えられているとき, V を**ノルム空間 (normed vector space)** と呼び, $||\ ||$ を**ノルム (norm)** と呼ぶ.

複素ベクトル空間 V における 2 つのノルム $||\ ||_1$, $||\ ||_2$ が**同値 (equivalent)** であるとはある定数 $A, B > 0$ が存在して, 任意の $x \in V$ に対して $A\,||x||_1 \leq ||x||_2 \leq B\,||x||_1$ が成立することであると定義する.

[168] (10 点) $\mathbb{C}^n$ にノルム $||\ ||_1$, $||\ ||_\infty$ を次のように定めることができることを示せ[5]:

$$||x||_1 := \sum_{i=1}^{n} |x_i|, \quad ||x||_\infty := \max_{1 \leq i \leq n} |x_i| \qquad \left(x = {}^t[x_1\ \cdots\ x_n] \in \mathbb{C}^n\right).$$

このときさらにこれら 2 つのノルムが互いに同値であることを証明せよ. より詳しくは $||x||_\infty \leq ||x||_1 \leq n\,||x||_\infty$ が成立することを証明せよ. □

V がノルム空間であるとき V 内の点列 $\{v_n\}_{n=1}^{\infty}$ が **Cauchy 列 (Cauchy sequence)** もしくは **基本列 (fundamental sequence)** であるとは $||v_m - v_n|| \to 0\ (m, n \to \infty)$

[5]実は任意の $p \geq 0$ に対してノルムを次のように定めることができる:

$$||x||_p := \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}.$$

$\mathbb{C}^n$ の標準的なノルムは $||\ ||_2$ である. しかし, 後で説明されるようにすべてのノルムは互いに同値になるので不等式を評価するときにどのノルムを用いても本質的に変わりはない.

となることである[6]. ノルム空間 V が**完備 (complete)** であるとは V における任意の Cauchy 列が収束することである[7]. たとえば $\mathbb{R}$ 上の 1 次元ベクトル空間 $\mathbb{R}$ にノルムを絶対値で定めれば実数体の完備性より $\mathbb{R}$ は完備なノルム空間になる.

一般に**完備なノルム空間 (complete normed vector space)** を **Banach 空間 (Banach space)** と呼ぶ.

たとえば有限次元ノルム空間は常に完備になるので Banach 空間である. 有限次元複素ベクトル空間に入るノルムは互いにすべて同値になり, どのノルムに関しても $\mathbb{C}^n$ は完備になる.

[169] (20 点) $\mathbb{C}^n$ におけるノルムはすべて互いに同値になることを証明せよ. □

ヒント: 問題 **[168]** の $||\ ||_1$ と $\mathbb{C}^n$ における任意のノルム $||\ ||$ が同値であることを示せば良い. $||\ ||$ に関する三角不等式を用いて, $||x|| \leq B\,||x||_1$ の側が証明される. $||x|| \geq A\,||x||_1$ の側を証明するためには $||\ ||_1$ の定める位相に関してコンパクトな集合 $\{\, x \in \mathbb{C}^n \mid ||x||_1 = 1 \,\}$ 上の実数値連続函数 $||\ ||$ が最小値を持つことを使えば良い. 函数解析 (位相解析) の教科書を見れば答が書いてあるはず. □

略解: $B = \max_{1\leq i\leq n} ||e_i|| > 0$ と置くと,

$$||x|| \leq \sum_{i=1}^{n} |x_i|\ ||e_i|| \leq B \sum_{i=1}^{n} |x_i| = B\,||x||_1 .$$

これより $||\ ||$ は $||\ ||_1$ から定まる位相に関して連続になることもわかる. したがって, $||\ ||$ はコンパクト集合 $\{\, x \in \mathbb{C}^n \mid ||x||_1 = 1 \,\}$ 上で最小値 $A > 0$ を持つ. このとき, $x \neq 0$ ならば

$$||x|| = \left|\left| \frac{x}{||x||_1} \right|\right| ||x||_1 \geq A\,||x||_1 . \quad \square$$

[170] (10 点) $\mathbb{C}^n$ は標準的なノルムに関して完備であることを証明せよ. □

ヒント. $\mathbb{C}$ 自身が完備であることと問題 **[168]** の結果を自由に用いてよい. □

[171] (10 点) pre-Hilbert 空間においてノルムは内積を用いて定義されたが, 逆にノルムを用いて内積を表示することもできる:

$$4\langle x, y\rangle = ||x+y||^2 - ||x-y||^2 - i\,||x+iy||^2 + i\,||x-iy||^2 . \quad \square$$

---

[6] 「$||v_m - v_n|| \to 0\ (m,n \to \infty)$」が成立するとは「任意に $\varepsilon > 0$ が与えられても十分に N 大きくすれば $||v_m - v_n|| \leq \varepsilon\ (m,n \geq N)$ が成立する」ということである. これは「どんなに小さな $\varepsilon > 0$ が与えられても点列のあるところから先の部分 $v_N, v_{N+1}, v_{N+2}, \ldots$ は直径 ε の範囲内に分布している」と言い直すことができる.

直観的に Cauchy 列はある点に収束して行くように見える点列のことである. しかし無限次元の場合には収束先がもとの空間内に存在するとは限らない. 収束しているように見える点列が常に収束しているという条件を仮定しておかないと不便な場合が多い. 次の「完備性 (completeness)」の定義を見よ.

[7] 「V における点列 $\{v_n\}_{n=1}^{\infty}$ が $v \in V$ に収束する」とは「任意に $\varepsilon > 0$ が与えられても十分に N を大きくすれば $||v - v_n|| \leq \varepsilon\ (n \geq N)$ が成立する」ということである. これは「許容できる誤差の上限 $\varepsilon > 0$ をどんなに小さくしても, 点列のあるところから先の部分 $v_N, v_{N+1}, v_{N+2}, \ldots$ はどれも v を誤差 ε 以内で近似している」と言い換えることができる. 収束性の厳密の定義は「いくらでも近似できる」という直観を正確に言い直しただけである.

参考: 複素 $m \times n$ 行列全体の集合を $M_{m,n}(\mathbb{C})$ と書くことにする (M は Matrix の頭文字). このとき, $A, B \in M_{m,n}(\mathbb{C})$ に対して,

$$\langle A, B \rangle := \mathrm{tr}(A^* B), \qquad ||A|| := \sqrt{\langle A, A \rangle}$$

と定めると,

$$\langle A, B \rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} \overline{a_{ij}} b_{ij}, \qquad ||A|| = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} |a_{ij}|^2 \right)^{1/2}$$

が成立している. これによって, $M_{m,n}(\mathbb{C})$ も pre-Hilbert 空間をなす[8]. □

16.2 Schmidt の正規直交化法と岩沢分解

[172] (Schmidt の正規直交化法, 20 点) V は pre-Hilbert 空間であり, $x_1, \ldots, x_n \in V$ は一次独立であると仮定し, $k = 1, \ldots, n$ に対して $v_k, p_k \in V$ を帰納的に,

$$v_k := x_k - \sum_{i=1}^{k-1} \langle p_i, x_k \rangle p_i, \quad p_k := v_k / ||v_k|| \qquad (k = 1, \ldots, n).$$

と定める. (特に, $v_1 = x_1$, $p_1 = x_1 / ||x_1||$.) このとき, $p_1, \ldots, p_n$ の張る V の部分空間は $x_1, \ldots, x_n$ の張る V の部分空間は等しく,

$$\langle p_k, p_l \rangle = \delta_{kl} \qquad (k, l = 1, \ldots, n)$$

が成立する. ここで δ_{kl} は Kronecker のデルタである. 特に $V = \mathbb{C}^n$ のとき $p_1, \ldots, p_n$ は V の正規直交基底である. □

ヒント: 数学的帰納法. □

複素 n 次正方行列全体のなす複素ベクトル空間を $M_n(\mathbb{C})$ と書くことにする. $M_n(\mathbb{C})$ の部分集合 $GL_n(\mathbb{C})$, $U(n)$, A_n, $N_n(\mathbb{C})$ を以下のように定義する:

$$GL_n(\mathbb{C}) := \{ A \in M_n(\mathbb{C}) \mid \det A \neq 0 \},$$
$$U(n) := \{ A \in M_n(\mathbb{C}) \mid A^* A = A A^* = E \},$$
$$A_n := \{ \mathrm{diag}(a_1, \ldots, a_n) \mid a_i > 0 \},$$
$$N_n(\mathbb{C}) := \left\{ \left. \begin{bmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ & 1 & a_{23} & \cdots & a_{2n} \\ & & 1 & \ddots & \vdots \\ & & & \ddots & a_{n-1,n} \\ 0 & & & & 1 \end{bmatrix} \right| a_{ij} \in \mathbb{C} \right\}.$$

ここで, $\mathrm{diag}(a_1, \ldots, a_n)$ は $a_1, \ldots, a_n$ を対角成分とする対角行列である. $N_n(\mathbb{C})$ は対角成分がすべて 1 の上三角行列全体の集合である. 後で群の定義を習えばすぐにわかるように, 以上で定義した行列の集合はすべて行列の積に関して群をなす. $GL_n(\mathbb{C})$ は n 次の**複素一般線形群 (complex general linear group)** と呼ばれ, $U(n)$ は n 次の**ユニタリー群 (unitary group)** と呼ばれている. $U(n)$ に含まれる行列は**ユニタリー行列 (unitary matrix)** と呼ばれる.

[8] 一般に有限次元の pre-Hilbert 空間は Hilbert 空間になる. よって, $M_{m,n}(\mathbb{C})$ は Hilbert 空間になる.

[173] (5 点) $P \in M_n(\mathbb{C})$ の中の n 本の列ベクトルを左から $p_1, \ldots, p_n$ と書くことにする. すなわち $P = [p_1 \ \cdots \ p_n]$. このとき,

$$P \in U(n) \iff p_1, \ldots, p_n \text{ は } \mathbb{C}^n \text{ の正規直交基底.} \quad \square$$

以上の準備のもとで $\mathbb{C}^n$ の基底への Schmidt の正規直交化法の適用を次のように言い直すことができる.

[174] (複素一般線形群の岩沢分解, 15 点) 次の写像は全単射である:

$$U(n) \times A_n \times N_n(\mathbb{C}) \to GL_n(\mathbb{C}), \quad (K, A, N) \mapsto X = KAN.$$

この結果を $GL_n(\mathbb{C})$ の岩沢分解と呼ぶ. $\square$

ヒント: 逆写像の構成の仕方. $X \in GL_n(\mathbb{C})$ の中の n 本の列ベクトル $x_1, \ldots, x_n$ は $\mathbb{C}^n$ の基底をなす. その基底に Schmidt の正規直交化法を適用すると,

$$x_k = \langle p_1, x_k \rangle p_1 + \cdots + \langle p_{k-1}, x_k \rangle p_{k-1} + ||v_k||\, p_k \qquad (k = 1, \ldots, n)$$

であるから, これを書き直すと,

$$X = [x_1 \ \cdots \ x_n] = [p_1 \ \cdots \ p_n] \begin{bmatrix} ||v_1|| & \langle p_1, x_2 \rangle & \langle p_1, x_3 \rangle & \cdots & \langle p_1, x_n \rangle \\ & ||v_2|| & \langle p_2, x_3 \rangle & \cdots & \langle p_2, x_n \rangle \\ & & ||v_3|| & \ddots & \vdots \\ & & & \ddots & \langle p_{n-1}, x_n \rangle \\ 0 & & & & ||v_n|| \end{bmatrix}.$$

複素一般線形群の岩沢分解は任意の正則な複素 n 次正方行列がユニタリー行列と対角成分が正の実数であるような上三角行列の積に一意的に分解されることと同値である. $\square$

参考: 位相について習えばすぐに証明できるようになることだが, $U(n)$ はコンパクト群であり, A_n は $\mathbb{R}^n$ と同相であり, $N_n(\mathbb{C})$ は $\mathbb{R}^{n(n-1)}$ と同相である. 複素一般線形群の岩沢分解は $GL_n(\mathbb{C})$ が位相空間としてコンパクト群とユークリッド空間 $\mathbb{R}^{n^2}$ の直積に同相であることを意味している. $\square$

[175] (15 点) 実数の範囲内での Schmidt の正規直交化法と実一般線形群の岩沢分解を定式化して証明せよ. $\square$

ヒント: ${}^tAA = A\,{}^tA = E$ を満たす実 n 次正方行列全体のなす集合を $O(n)$ と書いて**直交群 (orthogonal group)** と呼び, $O(n)$ の元を**直交行列 (orthogonal matrix)** と呼ぶ. このとき, 行列の積の定める写像

$$O(n) \times A_n \times N_n(\mathbb{R}) \to GL_n(\mathbb{R}), \quad (K, A, N) \mapsto X = KAN.$$

は全単射になる. $\square$

[176] (10 点) 問題 **[164]** の状況を考える. $1, x, x^2, x^3, x^4 \in V$ に Schmidt の正規直交化法を適用してみよ. $\square$

ヒント: 内積の計算については次の問題 [**177**] を見よ. 正規直交化の結果を v_0, v_1, v_2, v_3, v_4 と書くと, 各 v_n は (最高次の係数が 2^n の整数係数多項式)$/\sqrt{2^n n!\sqrt{\pi}}$ の形になる. しかも v_0, v_2, v_4 は偶函数になり, v_1, v_3 は奇函数になる. □

参考: 問題 [**164**], [**176**] は実は Hermite の多項式の理論の一部分になっている. Hermite の多項式に関しては[9]. □

略解: 実は Hermite の多項式 $H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}$ をそのノルム $\sqrt{2^n n!\sqrt{\pi}}$ で割ったものが答になる. 問題 [**176**] に解答するためには $n = 4$ まで計算すれば良い:

$$\begin{aligned}
&H_0(x) = 1, && ||H_0||^2 = 2^0 \cdot 0!\sqrt{\pi} = \sqrt{\pi},\\
&H_1(x) = 2x, && ||H_1||^2 = 2^1 \cdot 1!\sqrt{\pi} = 2\sqrt{\pi},\\
&H_2(x) = 4x^2 - 2, && ||H_2||^2 = 2^2 \cdot 2!\sqrt{\pi} = 8\sqrt{\pi},\\
&H_3(x) = 8x^3 - 12x, && ||H_3||^2 = 2^3 \cdot 3!\sqrt{\pi} = 48\sqrt{\pi},\\
&H_4(x) = 16x^4 - 48x^2 + 12, && ||H_4||^2 = 2^4 \cdot 4!\sqrt{\pi} = 384\sqrt{\pi}.
\end{aligned}$$

よって, $1, x, x^2, x^3, x^4$ を正規直交化した結果 v_0, v_1, v_2, v_3, v_4 は次のようになる:

$$\begin{aligned}
v_0(x) &= H_0(x)/\,||H_0|| = \pi^{-1/4},\\
v_1(x) &= H_1(x)/\,||H_1|| = \pi^{-1/4}\sqrt{2}x,\\
v_2(x) &= H_2(x)/\,||H_2|| = \pi^{-1/4}\left(\sqrt{2}x^2 - \frac{\sqrt{2}}{2}\right),\\
v_3(x) &= H_3(x)/\,||H_3|| = \pi^{-1/4}\left(\frac{2\sqrt{3}}{3}x^3 - \sqrt{3}x\right),\\
v_4(x) &= H_4(x)/\,||H_4|| = \pi^{-1/4}\left(\frac{\sqrt{6}}{3}x^4 - \sqrt{6}x^2 + \frac{\sqrt{6}}{4}\right).
\end{aligned}$$

直接的に Schmidt の正規直交化法を適用するとかなり面倒な計算が必要になるが, 結果は以上と一致することが確かめられる. □

[**177**] **(10 点)** $I_n = \int_{-\infty}^{\infty} x^n e^{-x^2} dx \quad (n = 0, 1, 2, \ldots)$ を計算せよ. □

ヒント: n が偶数の場合は $I(a) = \int_{-\infty}^{\infty} e^{-ax^2} dx \quad (a > 0)$ を計算して, a で微分すれば良い. n が奇数の場合は $I_n = 0$ となる. □

略解: $I(a) = \sqrt{\pi} a^{-1/2}$ である. なぜならば

$$I(a)^2 = \int_{\mathbb{R}^2} e^{-a(x^2+y^2)}\, dx\, dy = \int_0^{2\pi} d\theta \int_0^{\infty} e^{-ar^2} r\, dr = \frac{\pi}{a}.$$

I_{2k} は次のように計算される:

$$I_{2k} = \left(-\frac{d}{da}\right)^k I(a)\bigg|_{a=1} = \frac{1 \cdot 3 \cdots (2k-1)}{2^k}\sqrt{\pi}. \quad \square$$

[9]実はこの参考が問題 [**176**] の最大のヒントになっている. 岩沢分解 [**174**] より,

$$v_n(x) = a_{0n} + a_{1n}x + \cdots + a_{nn}x^n, \qquad a_{mn} \in \mathbb{R}, \quad a_{nn} > 0$$

の形の $v_0, \ldots, v_4$ で $\langle v_m, v_n \rangle = \delta_{mn}$ を満たすものを見付ければ良い. そのような v_n たちは Hermite の多項式に関する結果をよく眺めると見付かってしまう.

ガンマ函数 $\Gamma(s)$ は次のように定義されたのであった:

$$\Gamma(s) := \int_0^\infty y^{s-1}e^{-y}\,dy \qquad (\mathrm{Re}\, s > 0).$$

そして, ガンマ函数は次の函数等式を満たしているのであった:

$$\Gamma(s+1) = s\Gamma(s).$$

$y = x^2$ と変数変換すれば $I_{2k} = \Gamma(k+\frac{1}{2})$ であることがわかる. よって, 函数等式と $\Gamma(1/2) = \sqrt{\pi}$ から I_{2k} を計算することもできる.

[178] (10 点) $\mathrm{Re}\, s > 0$ においてガンマ函数の定義式の右辺の積分が絶対収束することおよびガンマ函数の函数等式を証明せよ. さらに, $\Gamma(n+1) = n!$ $(n \in \mathbb{Z}_{\geq 0})$, $\Gamma(1/2) = \sqrt{\pi}$ を示せ. □

16.3 Cauchy-Schwarz の不等式について

Cauchy-Schwarz の不等式 **[166]** について解説を追加しておく.

Cauchy-Schwarz の不等式がまだ「ああやってもこうやっても明らか」に見えていない人は難しく考え過ぎているからである. 特殊な場合における Cauchy-Schwarz の不等式を様々なやり方で証明しておけば段々「これは当然成立すべき不等式であり, 必要最小限どれだけの条件があれば Cauchy-Schwarz の不等式が成立するかは内積の公理の形にまとめられている」ということが納得できてくるはずである. しかし, そのためには様々な場合について時間をかけて色々考えてみる必要がある. どういうことに時間をかけるべきかについての実例を以下に示すことにする.

実 2 次元の場合に $a = {}^t[a_1, a_2], b = {}^t[b_1, b_2] \in \mathbb{R}^2$ の内積が

$$\langle a, b\rangle = a_1b_1 + a_2b_2$$

と定義されている場合は

$$\begin{aligned}\langle a, a\rangle\langle b, b\rangle - \langle a, b\rangle^2 &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) - (a_1b_1 + a_2b_2)^2 \\ &= (a_1^2b_1^2 + a_1^2b_2^2 + a_2^2b_1^2 + a_2^2b_2^2) - (a_1^2b_1^2 + 2a_1b_1a_2b_2 + a_2^2b_2^2) \\ &= a_1^2b_2^2 - 2a_1b_1b_2b_2 + a_2^2b_1^2 \\ &= (a_1b_2 - a_2b_1)^2 \geq 0.\end{aligned}$$

よって次の Cauchy-Schwarz の不等式が成立する:

$$\langle a, b\rangle^2 \leq \langle a, a\rangle\langle b, b\rangle \quad \text{すなわち} \quad |\langle a, b\rangle| \leq ||a|| \cdot ||b||\,.$$

実 3 次元の場合も同様の計算が可能である. 実際, $a = {}^t[a_1, a_2, a_3], b = {}^t[b_1, b_2, b_3] \in \mathbb{R}^3$ の内積が

$$\langle a, b\rangle = a_1b_1 + a_2b_2 + a_3b_3$$

と定義されているならば,

$$\langle a, a\rangle\langle b, b\rangle - \langle a, b\rangle^2 = (a_1^2 + a_2^2 + a_3^2)(b_1^2 + b_2^2 + b_3^2) - (a_1b_1 + a_2b_2 + a_3b_3)^2$$

$$
\begin{aligned}
&= (\quad a_1^2b_1^2 + a_1^2b_2^2 + a_1^2b_3^2 \\
&\quad + a_2^2b_1^2 + a_2^2b_2^2 + a_2^2b_3^2 \\
&\quad + a_3^2b_1^2 + a_3^2b_2^2 + a_3^2b_3^2) \\
&- (\quad a_1b_1a_1b_1 + a_1b_1a_2b_2 + a_1b_1a_3b_3 \\
&\quad + a_2b_2a_1b_1 + a_2b_2a_2b_2 + a_2b_2a_3b_3 \\
&\quad + a_3b_3a_1b_1 + a_3b_2a_2b_2 + a_3b_3a_3b_3) \\
&= (a_1^2b_2^2 - 2a_1b_1a_2b_2 + a_2^2b_1^2) \\
&+ (a_1^2b_3^2 - 2a_1b_1a_3b_3 + a_3^2b_1^2) \\
&+ (a_2^2b_3^2 - 2a_2b_2a_3b_3 + a_3^2b_2^2) \\
&= (a_1b_2 - a_2b_1)^2 + (a_1b_3 - a_3b_1)^2 + (a_2b_3 - a_3b_2)^2 \geq 0.
\end{aligned}
$$

計算のポイントは3つ目の等号である. 2つ目の等号の後の式の前者の括弧の中と後者の括弧の中の「対角成分」は互いにキャンセルし, 前者と後者の括弧の中の $i < j$ に対する「(i, j) 成分」と「(j, i) 成分」をまとめて並べ直せば3つ目の等号が成立することがわかる.

ここまでたどり着けば実 n 次元の場合も同様の計算が可能であることが容易に想像できるはずである. なぜならば上に説明した3つ目の等号の導き方は次元によらない方法だからである[10].

実際, $a = {}^t[a_1, \ldots, a_n], b = {}^t[b_1, \ldots, b_n] \in \mathbb{R}^2$ の内積が

$$\langle a, b\rangle = \sum_{i=1}^{n} a_ib_i = a_1b_1 + \cdots + a_nb_n$$

と定義されているならば,

$$
\begin{aligned}
&\langle a, a\rangle\langle b, b\rangle - \langle a, b\rangle^2 \\
&= (a_1^2 + a_2^2 + \cdots + a_n^2)(b_1^2 + b_2^2 + \cdots + b_n^2) - (a_1b_1 + a_2b_2 + \cdots + a_nb_n)^2 \\
&= (\quad a_1^2b_1^2 + a_1^2b_2^2 + a_1^2b_3^2 + \cdots + a_1^2b_n^2 \\
&\quad + a_2^2b_1^2 + a_2^2b_2^2 + a_2^2b_3^2 + \cdots + a_2^2b_n^2 \\
&\quad + a_3^2b_1^2 + a_3^2b_2^2 + a_3^2b_3^2 + \cdots + a_3^2b_n^2 \\
&\quad + \cdots\cdots \\
&\quad + a_n^2b_1^2 + a_n^2b_2^2 + a_n^2b_3^2 + \cdots + a_n^2b_n^2) \\
&- (\quad a_1b_1a_1b_1 + a_1b_1a_2b_2 + a_1b_1a_3b_3 + \cdots + a_1b_1a_nb_n \\
&\quad + a_2b_2a_1b_1 + a_2b_2a_2b_2 + a_2b_2a_3b_3 + \cdots + a_2b_2a_nb_n \\
&\quad + a_3b_3a_1b_1 + a_3b_2a_2b_2 + a_3b_3a_3b_3 + \cdots + a_3b_3a_nb_n \\
&\quad + \cdots\cdots \\
&\quad + a_nb_na_1b_1 + a_nb_na_2b_2 + a_nb_na_3b_3 + \cdots + a_nb_na_nb_n) \\
&= (a_1^2b_2^2 - 2a_1b_1a_2b_2 + a_2^2b_1^2) + (a_1^2b_3^2 - 2a_1b_1a_3b_3 + a_3^2b_1^2) + \cdots + (a_1^2b_n^2 - 2a_1b_1a_nb_n + a_n^2b_1^2) \\
&+ (a_2^2b_3^2 - 2a_2b_2a_3b_3 + a_3^2b_2^2) + \cdots + (a_2^2b_n^2 - 2a_2b_2a_nb_n + a_n^2b_2^2) \\
&+ \cdots\cdots \\
&+ (a_{n-1}^2b_n^2 - 2a_{n-1}b_{n-1}a_nb_n + a_n^2b_{n-1}^2) \\
&= (a_1b_2 - a_2b_1)^2 + (a_1b_3 - a_3b_1)^2 + \cdots + (a_1b_n - b_na_1)^2
\end{aligned}
$$

[10] n が一般の場合の結果を得るために n が小さな場合の議論をよく観察して「それがうまく行く仕組み」を見抜くという考え方は非常に重要である.

$$
\begin{aligned}
&+ (a_2b_3 - a_3b_2)^2 + \cdots + (a_2b_n - b_na_2)^2 \\
&+ \cdots\cdots \\
&+ (a_{n-1}b_n - b_na_{n-1})^2 \\
&\geq 0.
\end{aligned}
$$

繰り返しになるが計算のポイントは 3 つ目の等号である. 2 つ目の等号の後の式の前者の括弧の中と後者の括弧の中の「対角成分」は互いにキャンセルし, 前者と後者の括弧の中の $i < j$ に対する「(i, j) 成分」と「(j, i) 成分」をまとめて並べ直せば 3 つ目の等号が成立することがわかる.

上の計算は $\cdots$ という記号を多用して視覚的直下に訴える方法を取ったが $\cdots$ を $\sum$ で置き換えて以下のように計算することもできる:

$$
\begin{aligned}
\langle a, a\rangle\langle b, b\rangle - \langle a, b\rangle^2 &= \sum_i a_i^2 \sum_j b_j^2 - \sum_i a_ib_i \sum_j a_jb_j \\
&= \sum_{i,j} a_i^2b_j^2 - \sum_{i,j} a_ib_ia_jb_j \\
&= \sum_i a_i^2b_i^2 + \sum_{i<j}(a_i^2b_j^2 + a_j^2b_i^2) - \sum_i (a_ib_i)^2 - \sum_{i<j} 2a_ib_ia_jb_j \\
&= \sum_{i<j}(a_i^2b_j^2 - 2a_ib_ia_jb_j + a_j^2b_i^2) \\
&= \sum_{i<j}(a_ib_j - a_jb_i)^2 \geq 0.
\end{aligned}
$$

もう, うんざりしているかもしれないが, 計算のポイントは 3 つ目の等号である. 3 つ目の等号では (i, j) に関する和を (i, i) に関する和と $i < j$ に対する (i, j) と (j, i) に関する和に分解することによって得られる. そして (i, i) に関する和の部分がキャンセルして第 4 の等号が成立する.

同様の計算は区間 $[a, b]$ 上の実数値連続函数 f, g の内積が

$$
\langle f, g\rangle = \int_a^b f(x)g(x)\,dx
$$

と定義されている場合にも可能である. 実際 $S = [a, b]^2$, $T = \{\,(x, y) \in S \mid x < y\,\}$ と置くと[11],

$$
\begin{aligned}
\langle f, f\rangle\langle g, g\rangle - \langle f, g\rangle^2 &= \int_a^b f(x)^2\,dx \int_a^b g(y)^2 dy - \int_a^b f(x)g(x)\,dx \int_a^b f(y)g(y)\,dy \\
&= \iint_S f(x)^2g(y)^2\,dx\,dy - \iint_S f(x)g(x)f(y)g(y)\,dx\,dy \\
&= \iint_T \bigl(f(x)^2g(y)^2 + f(y)^2g(x)^2\bigr)\,dx\,dy - \iint_T 2f(x)g(x)f(y)g(y)\,dx\,dy \\
&= \iint_T \bigl(f(x)^2g(y)^2 - 2f(x)g(x)f(y)g(y) + f(y)^2g(x)^2\bigr)\,dx\,dy \\
&= \iint_T \bigl(f(x)g(y) - f(y)g(x)\bigr)^2\,dx\,dy \geq 0.
\end{aligned}
$$

もう説明の必要がないと思うが, 計算のポイントは 3 つ目の等号である. 3 つ目の等号は正方形 $S = [a, b]^2$ 上での積分を上三角 $T = \{x < y\}$ と下三角 $\{x > y\}$ の上での積分に

[11] S は square (正方形) の頭文字であり, T は triangle (三角形) の頭文字である.

分解し, 後者の積分変数の x, y を引っくり返して上三角 T 上の積分にまとめ直すことによって得られる. 対角線 $x = y$ 上の積分を無視して良いのは対角線の面積が 0 であるからその上の積分が常に 0 になるからだと考えてもよいし, $\sum$ を用いた計算の場合と同様にキャンセルして消えると考えても構わない.

それでは a, b が複素ベクトルだったり, f, g が複素数値函数の場合はどのように考えれば良いのだろうか? 様々な考え方があるが, もっとも素朴な考え方は複素数 z と 2 つの実数の組 (x, y) が $z = x + iy$ によって一対一に対応していることを用いて, 実ベクトルや実数値函数に関して得られた結果が複素ベクトルや複素数値函数の場合にどのように翻訳されるかを考えてみることである.

まず, 複素 1 次元の場合について考えよう. 複素数 1 つと実数 2 つの組は一対一に対応しているので 1 つの複素数は実 2 次元のベクトルだとみなすことができる. 実 2 次元の場合の内積を複素数を用いて表現することを考えよう. それができれば実 $2n$ 次元の場合の結果を複素 n 次元の場合に翻訳できる.

$a, b \in \mathbb{C}$ が $a = a' + ia''$, $b = b' + ib''$ $(a', a'', b', b'' \in \mathbb{R})$ と表わされているとすると

$$\overline{a}b = (a'b' + a''b'') + i(a'b'' - a''b')$$

であるから

$$\operatorname{Re}\overline{a}b = a'b' + a''b''.$$

右辺は実 2 次元ベクトル ${}^t[a', a'']$ と ${}^t[b', b'']$ の内積に一致している[12]. そして $|a|$, $|b|$ はそれぞれ実 2 次元ベクトル ${}^t[a', a'']$ と ${}^t[b', b'']$ のノルムに等しいこともわかる. よって, 実 2 次元の場合の Cauchy-Schwarz の不等式は次のように翻訳される:

$$|\operatorname{Re}\overline{a}b| \leq |a| \cdot |b|.$$

この不等式は複素数についてよく理解していれば自明であるが, 実ベクトルの Cauchy-Schwarz の不等式を複素ベクトルの場合に翻訳するときの出発点になるだけではなく, 本質的な議論はこれで尽きているのである.

複素 n 次元ベクトル $a = {}^t[a_1, \ldots, a_n] \in \mathbb{C}^n$ が与えられているとき, 各成分 a_k を $a_k = a'_k + ia''_k$ $(a'_k, a''_k \in \mathbb{R})$ と表わしておき, 実 $2n$ 次元ベクトル $\mathbf{a} \in \mathbb{R}^{2n}$ を $\mathbf{a} = {}^t[a'_1, a''_1, \ldots, a'_n, a''_n]$ と定める. $b \in \mathbb{C}^n$ に対する $\mathbf{b} \in \mathbb{R}^{2n}$ も同様とする. 複素 n 次元ベクトル a, b の内積と実 $2n$ 次元ベクトル $\mathbf{a}$, $\mathbf{b}$ の内積が次のように定められているとする:

$$\langle a, b\rangle = \sum_{k=1}^{n} \overline{a_k} b_k \in \mathbb{C}, \qquad \langle \mathbf{a}, \mathbf{b}\rangle = \sum_{k=1}^{n} (a'_k b'_k + a''_k b''_k) \in \mathbb{R}.$$

---

[12] それでは虚部 $\operatorname{Im}\overline{a}b = a'b'' - a''b'$ は ${}^t[a', a'']$ と ${}^t[b', b'']$ の外積 (もしくはベクトル積) になっている. より正確に説明すると以下の通りである.

ベクトル解析において 2 つの実 3 次元ベクトル $\mathbf{a} = {}^t[a_1, a_2, a_3]$, $\mathbf{b} = {}^t[b_1, b_2, b_3]$ に対して**外積 (outer product)** もしくは**ベクトル積 (vector product)** が次のように定義される:

$$\mathbf{a} \times \mathbf{b} = {}^t[a_2b_3 - a_3b_2,\ a_3b_1 - a_1b_3,\ a_1b_2 - a_2b_1].$$

よって $\mathbf{a} = {}^t[a', a'', 0]$, $\mathbf{b} = {}^t[b', b'', 0]$ ならば $\mathbf{a} \times \mathbf{b} = {}^t[0, 0, a'b'' - a''b']$ の第 3 成分は $\operatorname{Im}\overline{a}b$ に一致する.

$\mathbf{a} \times \mathbf{b}$ は $\mathbf{a}$ と $\mathbf{b}$ に垂直でその長さが $\mathbf{a}$, $\mathbf{b}$ を 2 辺とする平行四辺形の面積に等しいベクトルになる. そのようなベクトルは 2 つ存在するが $\mathbf{a} \times \mathbf{b}$ は $(\mathbf{a}, \mathbf{b}, \mathbf{a} \times \mathbf{b})$ が右手系をなすように選ばれている.

特に $a'b'' - a''b'$ はベクトル ${}^t[a', a'']$ と ${}^t[b', b'']$ を 2 辺とする平行四辺形の面積に等しい. (そのことを証明してみよ.)

複素数を使えば実 2 次元ベクトルの世界を 1 つの数で扱うことができる. 実は同様に Hamilton の四元数を用いれば実 3 次元ベクトルの世界を 1 つの数で扱うことができる. 研究してみよ.

このとき上の方で説明した $n=1$ の場合の結果より,

$$\mathrm{Re}\langle a,b\rangle = \sum_{k=1}^{n} \mathrm{Re}\,\overline{a_k} b_k = \sum_{k=1}^{n} (a'_k b'_k + a''_k b''_k) = \langle \mathbf{a}, \mathbf{b}\rangle.$$

そして複素 n 次元ベクトルのノルム $||a||$, $||b||$ はそれぞれ実 $2n$ 次元ベクトルのノルム $||\mathbf{a}||$, $||\mathbf{b}||$ のノルムに等しいこともわかる. よって実 $2n$ 次元ベクトルに関する Cauchy-Schwarz の不等式は次のように翻訳される:

$$|\,\mathrm{Re}\langle a,b\rangle| \le ||a|| \cdot ||b||\,.$$

この結果から複素ベクトルの Cauchy-Schwarz の不等式

$$|\langle a,b\rangle| \le ||a|| \cdot ||b||$$

が容易に導かれる. 実際 $\langle a,b\rangle$ を $\langle a,b\rangle = re^{i\theta}$ $(r \ge 0, \theta \in \mathbb{R})$ と極表示すると,

$$|\langle a,b\rangle| = r = e^{-i\theta}\langle a,b\rangle = \langle a, e^{-i\theta} b\rangle = \mathrm{Re}\langle a, e^{-i\theta} b\rangle \le ||a|| \cdot \left|\left| e^{-i\theta} b \right|\right| = ||a|| \cdot ||b||\,.$$

ここまでたどり着けば複素ベクトルの場合の Cauchy-Schwarz の不等式も怖くないはずである.

しかし, これで満足してはいけない. なぜならば我々は 2 つの実ベクトルの成分の積の和によって内積を定義するところから出発したからである. 必ずしも内積がそのように定義されるとは限らない. 出発点でベクトルの成分を使っているせいで必要最小限どれだけの条件があれば Cauchy-Schwarz の不等式が成立するかもはっきりしていない.

この問題への 1 つの回答の仕方は公理的な考え方をすることである. 内積が満たすべき必要最小限の条件は何か, その条件だけを用いて Cauchy-Schawarz の不等式を証明できないか, その直観的意味は何であるか, などなどに関する答は多くの線形代数の教科書に書いてある.

この演習でもその考え方に沿って内積の基本性質 [**162**] および Cauchy-Schwarz の不等式を証明する問題 [**166**] のヒントに最終的な結果がまとめられている. 虫食い状態になった問題 [**166**] の解答例を以下に書いておこう.

Cauchy-Schwarz の不等式: V は複素ベクトル空間であり, $\langle\ ,\ \rangle$ は V における内積であるとする. このとき任意の $a, b \in V$ に対して, $|\langle a,b\rangle| \le ||a|| \cdot ||b||$ が成立し, 等号が成立するための必要十分条件は a, b の一方がもう一方の複素数倍になることである.

証明: $a \neq 0$ と仮定して良い. $c = b - za$ が a と直交するように $z \in \mathbb{C}$ を定めよう. $0 = \langle a,c\rangle = \boxed{\text{ア}} - z\boxed{\text{イ}}$ より $z = \boxed{\text{ア}}/\boxed{\text{イ}}$ とすれば c は a と直交する. このとき,

$$0 \le \langle c,c\rangle = \langle b - za, c\rangle = \boxed{\text{ウ}} = \boxed{\text{エ}} - z\boxed{\text{オ}} = ||b||^2 - \frac{|\langle a,b\rangle|^2}{||a||^2}.$$

ここで, 2 つ目の等号で a と c が直交することを用いた. 最初の不等号で等号が成立するための必要十分条件は $c = 0$ すなわち $b = za$ である. これで Cauchy-Schwarz の不等式が証明された. □

虫に食われた部分を埋めて, この証明が実際に内積の基本性質 (公理) のみを用いて遂行可能であることをチェックせよ.

虫に食われていない証明: $a \neq 0$ と仮定して良い. $c = b - za$ が a と直交するように $z \in \mathbb{C}$ を定めよう. $0 = \langle a, c\rangle = \langle a, b\rangle - z\langle a, b\rangle$ より $z = \langle a, b\rangle / \langle a, b\rangle$ とすれば c は a と直交する. このとき,

$$0 \leq \langle c, c\rangle = \langle b - za, c\rangle = \langle b, c\rangle = \langle b, b\rangle - z\langle b, a\rangle = ||b||^2 - \frac{|\langle a, b\rangle|^2}{||a||^2}.$$

ここで, 2 つ目の等号で a と c が直交することを用いた. 最初の不等号で等号が成立するための必要十分条件は $c = 0$ すなわち $b = za$ である. これで Cauchy-Schwarz の不等式が証明された. □

二次函数の判別式を用いて Cauchy-Schwarz の不等式を証明することもできる.

まず, V は実ベクトル空間であり, $\langle\ ,\ \rangle$ は V における内積であるとし, $a, b \in V$, $a \neq 0$ と仮定する. このとき $t \in \mathbb{R}$ の実数値函数 $f(t)$ を

$$f(t) = \langle b - ta, b - ta\rangle = ||a||^2 t^2 - 2\langle a, b\rangle t + ||b||^2$$

と定めると, $f(t) \geq 0$ である. よって $f(t)$ の判別式 D は 0 以下でなければいけない:

$$0 \geq \frac{D}{4} = \langle a, b\rangle^2 - ||a||^2 ||b||^2.$$

これで $|\langle a, b\rangle| \leq ||a|| \cdot ||b||$ が証明された.

次に, V は実ベクトル空間であり, $\langle\ ,\ \rangle$ は V における内積であるとし, $a, b \in V$, $a \neq 0$ と仮定する. このとき $z \in \mathbb{C}$ の複素数値函数 $f(z)$ を

$$f(z) = \langle b - za, b - za\rangle = ||a||^2 |z|^2 - 2\,\mathrm{Re}(\overline{z}\langle a, b\rangle) + ||b||^2$$

と定めると, $f(z) \geq 0$ である. しかし $f(z)$ は実二次函数ではないので判別式による判定法は使えない.

そこで $z = t \in \mathbb{R}$ と置くと,

$$f(z) = ||a||^2 t^2 - 2(\mathrm{Re}\langle a, b\rangle)t + ||b||^2.$$

$f(z) \geq 0$ なので右辺の判別式 D は 0 以下である:

$$0 \geq \frac{D}{4} = |\,\mathrm{Re}\langle a, b\rangle|^2 - ||a||^2 ||b||^2.$$

よって $|\,\mathrm{Re}\langle a, b\rangle| \leq ||a|| \cdot ||b||$ である. この不等式から Cauchy-Schwarz の不等式が容易に導かれるのであった.

さらに工夫して $\langle a, b\rangle$ を $\langle a, b\rangle = re^{i\theta}$ $(r \geq 0, \theta \in \mathbb{R})$ と極表示し, $z = te^{i\theta}$ $(t \in \mathbb{R})$ と置くと, $\overline{z}\langle a, b\rangle = rt = |\langle a, b\rangle|t$ なので,

$$f(z) = ||a||^2 t^2 - 2|\langle a, b\rangle|t + ||b||^2.$$

$f(z) \geq 0$ なので右辺の判別式 D は 0 以下である:

$$0 \geq \frac{D}{4} = |\langle a, b\rangle|^2 - ||a||^2 ||b||^2.$$

これで $|\langle a, b\rangle| \leq ||a|| \cdot ||b||$ が直接に証明された.

17　量子調和振動子と Hermite の多項式

この節は固有空間分解に関する演習である.

Hermite の多項式は**量子調和振動子 (quantum harmonic oscillator)** の固有値問題を解くときに表われる多項式のことである. 量子調和振動子の固有値問題とは次の常微分微分作用素の二乗可積分な固有函数を全て求めよという問題のことである:

$$H = \frac{1}{2m}(-i\hbar\partial)^2 + \frac{k}{2}x^2 = -\frac{\hbar^2}{2m}\partial^2 + \frac{k}{2}x^2.$$

ここで $\partial = d/dx$ であり, $m, k, \hbar > 0$ である[13]. 一般の場合は $y = \sqrt{2km}x/\hbar$ と変数変換すれば上の H は

$$H = k\left(-\frac{1}{2}\frac{d^2}{dy^2} + \frac{1}{2}y^2\right)$$

となる. よって $m = k = \hbar = 1$ の場合の固有値問題が解ければ一般の場合も解ける. そこで以下では簡単のため $m = k = \hbar = 1$ の場合のみを扱う.

[179] (急減少 C^∞ 函数の空間, 10 点) $\mathbb{R}$ 上の複素数値函数 f が**急減少 C^∞ 函数 (rapidly decreasing C^∞-function)** であるとは f が C^∞ (任意有限回微分可能) でかつ任意の $m, n = 0, 1, 2, \ldots$ に対して

$$\lim_{x\to\pm\infty} x^m f^{(n)}(x) = 0$$

が成立することである. $\mathbb{R}$ 上の急減少 C^∞ 函数全体のなす無限次元複素ベクトル空間を $\mathcal{S}(\mathbb{R})$ と表わす. このとき以下が成立する:

1. $\mathcal{S}(\mathbb{R})$ には内積を次のように入れることができる[14]:

$$\langle f, g\rangle = \int_{-\infty}^{\infty} \overline{f(x)}g(x)\,dx \qquad \big(f, g \in \mathcal{S}(\mathbb{R})\big).$$

   (ヒント: 任意の $f, g \in \mathcal{S}(\mathbb{R})$ に対して $|x|$ を十分大きくすれば $\left|\overline{f(x)}g(x)\right| \leq |x|^{-2}$ となる.)

2. 線形写像 $\partial : \mathcal{S}(\mathbb{R}) \to \mathcal{S}(\mathbb{R})$ を $(\partial f)(x) = f'(x)$ と定めることができる.

3. 任意の多項式 $a \in \mathbb{C}[x]$ に対して, 線形写像 $a : \mathcal{S}(\mathbb{R}) \to \mathcal{S}(\mathbb{R})$ を $(af)(x) = a(x)f(x)$ と定めることができる.

4. 多項式 $a_0, \ldots, a_N \in \mathbb{C}[x]$ に対して, 線形写像 $P = \sum_{n=0}^N a_n\partial^n : \mathcal{S}(\mathbb{R}) \to \mathcal{S}(\mathbb{R})$ を次のように定めることができる:

$$Pf = \sum_{n=0}^{N} a_n f^{(n)} \qquad (f \in \mathcal{S}(\mathbb{R})).$$

[13] バネ定数 k のバネの先に質量 m の質点がくっついておりバネの伸び縮みによって振動している状況を考える. バネの伸び (縮んだ場合はマイナスの値を取る) を x と書き, 質点の運動量を $p = m\dot{x}$ と書くと, 質点の運動エネルギーは $p^2/(2m)$ となり, 質点の位置エネルギーは $kx^2/2$ となる. よって全エネルギーは $H(p, x) = p^2/(2m) + kx^2/2$ となる. この $H(p, x)$ は古典調和振動子の Hamiltonian と呼ばれている. そこに $p = -i\hbar\partial$ を代入したのが常微分作用素の H である. H は量子調和振動子の Hamiltonian と呼ばれており, その固有値は観測したときに見出される全エネルギーという物理的意味を持っている. $\hbar = h/(2\pi)$ は **Planck 定数 (Planck constant)** と呼ばれる物理定数である. $h = 6.6260755 \times 10^{-34}$ Js かつ $\hbar = 1.05457266 \times 10^{-34}$ Js である. $1\,\mathrm{J} = 1\,\mathrm{kg\,m^2/s^2}$.

[14] 内積の公理を満たしていることを示せ.

このような P は**多項式係数の常微分作用素 (ordinary differential operator with polynomial coefficients)** と呼ばれている. □

[180] (量子調和振動子, 15 点) $\mathbb{R}$ 上の急減少 C^∞ 函数全体の空間を $\mathcal{S}(\mathbb{R})$ と表わし[15], $fe^{-x^2/2}$ ($f \in \mathbb{C}[x]$) の形の函数全体の空間を $\mathbb{C}[x]e^{-x^2/2}$ と表わす. 以下を示せ:

1. $\mathbb{C}[x]e^{-x^2/2}$ は $\mathcal{S}(\mathbb{R})$ の部分空間である.
2. $\mathbb{C}[x]e^{-x^2/2}$ は多項式係数の任意の常微分作用素の作用で閉じている.
3. 多項式係数の常微分作用素 H, a, a^* を次のように定める:
$$H = -\frac{1}{2}\partial^2 + \frac{1}{2}x^2, \quad a = \frac{i}{\sqrt{2}}(\partial + x), \quad a^* = \frac{i}{\sqrt{2}}(\partial - x).$$
これらは次を満たしている[16]:
$$\begin{aligned} &[a, a^*] = 1, && H = a^*a + \frac{1}{2}, \\ &[H, a] = -a, && [H, a^*] = a^*, \\ &\langle f, ag\rangle = \langle a^*f, g\rangle, && \langle f, Hg\rangle = \langle Hf, g\rangle. \end{aligned}$$
(ヒント: $[\partial, x] = 1$, $[AB, C] = [A, C]B + A[B, C]$ を用いて計算せよ. 部分積分によって $\langle f, \partial g\rangle = -\langle \partial f, g\rangle$ を示せ.)
4. $\phi_n = (a^*)^n e^{-x^2/2} \in \mathbb{C}[x]e^{-x^2/2}$ $(n = 0, 1, 2, \ldots)$ と置く. このとき,
$$H\phi_n = \left(n + \frac{1}{2}\right)\phi_n \qquad (n = 0, 1, 2, \ldots).$$
(ヒント: $[H, a^*] = a^*$ より $Ha^* = a^*(H+1)$ であるから $H(a^*)^n = (a^*)^n(H+n)$ であり, $ae^{-x^2/2} = 0$ より $He^{-x^2/2} = \frac{1}{2}e^{-x^2/2}$ である. よって $H\phi_n = (a^*)^n(H+n)e^{-x^2/2} = \left(n + \frac{1}{2}\right)(a^*)^n e^{-x^2/2} = \left(n + \frac{1}{2}\right)\phi_n$.)
5. $\phi_0, \phi_1, \phi_2, \ldots$ は $\mathbb{C}[x]e^{-x^2/2}$ の基底である.
(ヒント: ϕ_n を $\phi_n = f_n e^{-x^2/2}$ ($f_n \in \mathbb{C}[x]$) と表わすと, f_n は n 次の多項式になる.) □
6. $m \neq n$ のとき $\langle \phi_m, \phi_n\rangle = 0$.
(ヒント: $\left(n + \frac{1}{2}\right)\langle \phi_m, \phi_n\rangle = \langle \phi_m, H\phi_n\rangle = \langle H\phi_m, \phi_n\rangle = \left(m + \frac{1}{2}\right)\langle \phi_m, \phi_n\rangle$.)
7. $a\phi_n = n\phi_{n-1}$.
(ヒント: $ae^{-x^2/2} = 0$ であり, $[a, a^*] = 1$ より $[a, (a^*)^n] = n(a^*)^{n-1}$ である[17]. よって $a\phi_n = a(a^*)e^{-x^2/2} = [a, (a^*)^n]e^{-x^2/2} = n(a^*)^{n-1}e^{-x^2/2} = n\phi_{n-1}$.)

[15] 急減少 C^∞ 函数の定義は問題 **[179]** にある.
[16] $[A, B] = A \circ A - B \circ A = AB - BA$ である.
[17] 一般に次が成立している:
$$[A, B_1 \cdots B_n] = \sum_{i=1}^{n} B_1 \cdots B_{i-1}[A, B_i]B_{i+1} \cdots B_n.$$
これは次の公式 (Leibnitz rule) に似ている:
$$\frac{d}{dx}(f_1 \cdots f_n) = \sum_{i=1}^{n} f_1 \cdots f_{i-1}\frac{df_i}{dx}f_{i+1} \cdots f_n.$$

8. $||\phi_n||^2 = n!\sqrt{\pi}$.
   (ヒント: $a\phi_n = n\phi_{n-1}$ より $a^n\phi_n = n!e^{-x^2/2}$ である. よって $||\phi_n||^2 = \langle\phi_n, \phi_n\rangle = \langle(a^*)^n e^{-x^2/2}, \phi_n\rangle = \langle e^{-x^2/2}, a^n\phi_n\rangle = \langle e^{-x^2/2}, n!e^{-x^2/2}\rangle = n!\int_{-\infty}^{\infty} e^{-x^2}\,dx$.)

9. $e_n = \phi_n/\,||\phi_n||$ と置くと, $e_0, e_1, e_2, \ldots$ は $\mathbb{C}[x]e^{-x^2/2}$ の正規直交基底をなす[18]. □

[181] (Leibnitz の公式, 10 点) 必要なだけ微分可能な函数 f, g に対して,

$$(fg)^{(\nu)} = \sum_{k=0}^{\nu} \binom{\nu}{k} f^{(k)} g^{(\nu-k)} \qquad (\nu = 0, 1, 2, \ldots).$$

ここで $f^{(k)}$ は f の k 階の導函数である. □

ヒント 1: ν に関する帰納法. 二項係数

$$\binom{\nu}{k} = \frac{\nu(\nu-1)\cdots(\nu-k+1)}{k!}$$

は次の漸化式を満たしている **(Pascal の三角形)**:

$$\binom{\nu}{k} + \binom{\nu}{k+1} = \binom{\nu+1}{k+1}. \quad \square$$

ヒント 2: 以下のように二項定理を用いて帰納法に頼らずに直接証明することもできる:

$$(fg)^{(\nu)}(x) = \left(\frac{\partial}{\partial x} + \frac{\partial}{\partial y}\right)^{\nu} f(x)g(y)\Big|_{y=x} = \sum_{k=0}^{\nu} \binom{\nu}{k} \left(\frac{\partial}{\partial x}\right)^{k} \left(\frac{\partial}{\partial y}\right)^{\nu-k} f(x)g(y)\Big|_{y=x}$$
$$= \sum_{k=0}^{\nu} \binom{\nu}{k} f^{(k)}(x) g^{(\nu-k)}(y)\big|_{y=x} = \sum_{k=0}^{\nu} \binom{\nu}{k} f^{(k)}(x) g^{(\nu-k)}(x). \quad \square$$

[182] (Hermite の多項式, 20 点) 問題 **[164]** の状況を考える[19]. すなわち $V = \mathbb{C}[x]$ でかつ V には次のように内積 $(\ ,\ )$ が定められていると仮定する:

$$(f, g) = \int_{-\infty}^{\infty} \overline{f(x)} g(x)\, e^{-x^2} dx \qquad \big(f, g \in V = \mathbb{C}[x]\big).$$

内積の記号を問題 **[164]** とは変えたのは問題 **[180]** の結果と比べるためにである. **Hermite の多項式 (Hermite's polynomials)** $H_n(x)$ が次のように定義される:

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2} \qquad (n = 0, 1, 2, \ldots).$$

問題 **[180]** の $\phi_n \in \mathbb{C}[x]e^{-x^2/2}$ を $\phi_n = f_n e^{-x^2/2}$ ($f_n \in \mathbb{C}[x]$) と表わしておく. 問題 **[180]** の結果を用いて以下を示せ:

1. $H_n(x)$ は最高次の係数が 2^n の整数係数 n 次多項式であり, n が偶数か奇数かに応じて $H_n(x)$ は偶函数または奇函数になる.
   (ヒント: $-\partial(2^n x^n e^{-x^2}) = (2^{n+1}x^{n+1} - 2^n n x^{n-1})e^{-x^2}$.)

[18] $e_0, e_1, e_2, \ldots$ が $\mathbb{C}[x]e^{-x^2/2}$ の正規直交基底であるとは $e_0, e_1, e_2, \ldots$ が $\mathbb{C}[x]e^{-x^2/2}$ の基底でかつ $\langle e_m, e_n\rangle = \delta_{mn}$ を満たしていることである. $\mathbb{C}[x]e^{-x^2/2}$ は $\mathcal{S}(\mathbb{R})$ でも $L_2(\mathbb{R})$ でも稠密 (dense) なので $e_0, e_1, e_2, \ldots$ は $L_2(\mathbb{R})$ の**完全 (完備) 正規直交系 (complete orthonormal system, CONS)** をなす.

[19] 問題 **[176]** も参照せよ.

2. $H_n(x) = (\sqrt{2}i)^n f_n(x)$.
(ヒント: $H_n(x)e^{-x^2/2} = (\sqrt{2}i)^n \phi_n(x)$ を示せば良い. $e^{x^2/2} \circ \partial \circ e^{-x^2/2} = \partial - x = -\sqrt{2}ia^*$ であるから $H_n e^{-x^2/2} = e^{x^2/2}(-\partial)^n(e^{-x^2/2}e^{-x^2/2}) = (-e^{x^2/2} \circ \partial \circ e^{-x^2/2})^n e^{-x^2/2} = (\sqrt{2}ia^*)^n e^{-x^2/2} = (\sqrt{2}i)^n \phi_n$.)

3. $(H_m, H_n) = 2^n n!\sqrt{\pi}\delta_{m,n}$.
(ヒント: $(f, g) = \langle fe^{-x^2/2}, ge^{-x^2/2}\rangle$ より問題 **[180]** の結果とすぐ上の結果を用いればすぐにわかる.)

4. H_n は次の微分方程式を満たしている:

$$(\partial^2 - 2x\partial + 2n)H_n = H_n'' - 2xH_n' + 2nH_n = 0 \qquad (n = 0, 1, 2, \ldots).$$

(ヒント: $H_n e^{-x^2} = (-\partial)^n e^{-x^2}$ の両辺に $-\partial$ を作用させることによって $-H_n' + 2xH_n = H_{n+1}$ であることがわかる. よって $(\partial - 2x)H_n = -H_{n+1}$ である. 一方 $-\partial e^{-x^2} = 2xe^{-x^2}$ の両辺に $(-\partial)^n$ を作用させることによって $H_{n+1} = 2xH_n - 2nH_{n-1}$ であることもわかる[20]. よって $\partial H_n = 2nH_{n-1}$ である. よって $(\partial^2 - 2x\partial)H_n = (\partial - 2x)\partial H_n = 2n(\partial - 2x)H_{n-2} = -2nH_n$. もちろん, 問題 **[180]** の $H_n(x)e^{-x^2/2}$ は H の固有函数であるという結果を変形することによっても目標の結果が得られる.) □

[183] (Hermite の多項式の母函数, 20 点) 上の問題の続き:

1. $e^{-t^2+2tx} = \displaystyle\sum_{n=0}^{\infty} H_n(x)\frac{t^n}{n!}$.
(ヒント: $e^{-t^2+2tx} = e^{x^2}e^{-(t-x)^2}$ を t に関する巾級数に展開せよ[21]. ただし, そのとき $\left(\frac{\partial}{\partial t}\right)^n e^{-(t-x)^2} = \left(-\frac{\partial}{\partial x}\right)^n e^{-(t-x)^2}$ を使う.)

2. $\int_{-\infty}^{\infty} e^{-s^2+2sx}e^{-t^2+2tx}e^{-x^2}\,dx = \sqrt{\pi}e^{2st}$.
(ヒント: $-s^2 + 2sx - t^2 + 2tx - x^2 = -(x - s - t)^2 + 2st$.)

3. $(H_m, H_n) = 2^n n!\sqrt{\pi}\delta_{m,n} \quad (n = 0, 1, 2, \ldots)$.
(ヒント: すぐ上の公式の両辺を s, t の巾級数に展開せよ.)

4. $\left(\frac{\partial^2}{\partial x^2} - 2x\frac{\partial}{\partial x} + 2t\frac{\partial}{\partial t}\right)e^{-t^2+2tx} = 0$.
(ヒント: $t\frac{\partial}{\partial t}e^{x^2-(t-x)^2} = -2t(t-x)e^{x^2-(t-x)^2} = (-2t^2 + 2tx)e^{x^2-(t-x)^2}$ を x だけを含む微分作用素の作用で表わすことを考える. そのために $\frac{\partial}{\partial x}e^{-t^2+2tx} = 2te^{-t^2+2tx}$, $\frac{\partial^2}{\partial x^2}e^{-t^2+2tx} = 4t^2e^{-t^2+2tx}$ と計算してみれば $t\frac{\partial}{\partial t}$ と $-\frac{1}{2}\frac{\partial^2}{\partial x^2} + x\frac{\partial}{\partial x}$ を $e^{-t^2+2tx} = e^{x^2-(t-x)^2}$ に作用させた結果が等しいことがわかる.)

5. $H_n'' - 2xH_n' + 2nH_n = 0 \quad (n = 0, 1, 2, \ldots)$.
(ヒント: すぐ上の公式の左辺を t の巾級数に展開して各係数を 0 と置いた式が目的の公式である.) □

解説: このように母函数を使えば Hermite の多項式の性質をコンパクトな計算で導くことができる. □

[20] Leibnitz の公式 **[181]** を使う.
[21] t の解析函数 $f(t)$ に対して $f(t) = \sum_{n=0}^{\infty} \frac{1}{n!}f^{(n)}(0)t^n$ であることを用いて良い.

18 正規行列

18.1 正規行列, Hermite 行列, 反 Hermite 行列, ユニタリー行列

複素 n 次正方行列 A について,

- A は**正規行列 (normal matrix)** $\iff A^*A = AA^*$;
- A は **Hermite 行列 (Hermitian matrix)** $\iff A^* = A$;
- A は**反 Hermite 行列 (anti-Hermitian matrix, skew-Hermitian matrix)** $\iff A^* = -A$;
- A は**ユニタリー行列 (unitary matrix)** $\iff A^*A = AA^* = E$.

実 n 次正方行列 A について,

- A は**実正規行列** $\iff {}^tAA = A\,{}^tA$;
- A は**実対称行列 (real symmetrix matrix)** $\iff {}^tA = A$;
- A は**実交代行列 (real alternating matrix, real anti-symmetric matrix, real skew-symmetric matrix)** $\iff {}^tA = -A$;
- A は**直交行列 (orthogonal matrix)** $\iff {}^tAA = A\,{}^tA = E$.

これらのすべての行列は正規行列の特別な場合である.

[184] (12 点) 複素 n 次正方行列 A について,

1. A は正規行列 $\iff \langle Ax, Ay\rangle = \langle A^*x, A^*y\rangle \quad (x, y \in \mathbb{C}^n)$;
2. A は Hermite 行列 $\iff \langle Ax, y\rangle = \langle x, Ay\rangle \quad (x, y \in \mathbb{C}^n)$;
3. A は反 Hermite 行列 $\iff \langle Ax, y\rangle = -\langle x, Ay\rangle \quad (x, y \in \mathbb{C}^n)$;
4. $\sqrt{-1}A$ は反 Hermite 行列 $\iff$ A は Hermite 行列;
5. A はユニタリー行列 $\iff \langle Ax, Ay\rangle = \langle x, y\rangle \quad (x, y \in \mathbb{C}^n)$;
6. A はユニタリー行列 $\iff ||Ax|| = ||x|| \quad (x \in \mathbb{C}^n)$. □

ヒント: 最後の結論を導くには **[171]** を使えば良い. □

[185] (12 点) 上と類似の問題を実 n 次正方行列について定式化し, それを証明せよ. □

[186] (5 点) A が反 Hermite 行列ならば e^A はユニタリー行列である. □

[187] (Pauli のスピン行列, 5 点) 行列 σ_1, σ_2, σ_3 を次のように定める:

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

これらを **Pauli のスピン行列 (Pauli's spin matrix)** と呼ばれている. Pauli のスピン行列は Hermite 行列である. 実数 $t \in \mathbb{R}$ に対して $e^{it\sigma_k}$ $(k = 1, 2, 3)$ を計算し, ユニタリー行列になることを確かめよ. □

[188] (5 点) A が実交代行列ならば e^A は直交行列である. □

[189] (5 点) 実交代行列の例を 1 つ (それを A と書く) を挙げ, 実数 $t \in \mathbb{R}$ の函数 e^{tA} を計算し, 直交行列になることを確かめよ. □

18.2 正規行列の対角化 (Toeplitz の定理)

さてこの節の第一の目標は, 「複素 n 次正方行列が正規行列であるための必要十分条件はユニタリー行列で対角化可能であることである」という結果 (Toeplitz の定理) を証明することである. (実際にはその概略を示し, 細部を演習問題として解いてもらうことになる.)

しかし, 「ユニタリー行列で対角化可能」の意味を説明しておかないとこの結果がどうして素晴しいかを理解できなくなってしまう. そこでまず「行列の対角化」と「ユニタリー行列」について説明しておこう.

以下しばらくのあいだ単に行列と言えば複素 n 次正方行列を意味するものとする.

2 つの行列 A と B が**相似 (similar)** であるとは, ある正則行列 P が存在して $P^{-1}AP = B$ が成立することである.

行列 $A = [a_{ij}]$ の成分 a_{ij} は $\mathbb{C}^n$ の標準的な基底 $e_1, \ldots, e_n$ に A を作用させれば現われる:

$$Ae_j = a_{1j}e_1 + \cdots + a_{nj}e_n = e_1a_{1j} + \cdots + e_na_{nj}.$$

しかし, $\mathbb{C}^n$ には標準的でない基底が無限に存在する. 行列 A が定める一次変換の様子を理解するためには標準的な基底が必ずしも便利だとは限らない. そこで, $\mathbb{C}^n$ の任意の基底 $p_1, \ldots, p_n$ を取ると, Ap_i は $p_1, \ldots, p_n$ の一次結合で一意的に表わされる:

$$Ap_j = b_{1j}p_1 + \cdots + b_{nj}p_n = p_1b_{1j} + \cdots + p_nb_{nj} \qquad (b_{ij} \in \mathbb{C}).$$

この式は行列を使って次のようにまとめることができる:

$$A[p_1 \ \cdots \ p_n] = [p_1 \ \cdots \ p_n] \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix}.$$

よって, 行列 P, B を $P = [p_1 \ \cdots \ p_n]$, $B = [b_{ij}]$ と定めると, P は正則行列になり,

$$AP = PB, \quad \text{すなわち } P^{-1}AP = B.$$

よって, 行列 A は行列 B と相似である. 以上の議論はすべて逆転させることができる. もしも行列 A, B が相似であり, $P^{-1}AP = B$ という関係にあるとき, P の中の n 本の列ベクトルのなす $\mathbb{C}^n$ の基底 $p_1, \ldots, p_n$ に関して A の定める一次変換を表示して得られる行列が B になる.

つまり, 行列 A と相似な行列を考えることと A の定める一次変換を標準的とは限らない任意の基底を用いて表示し直すことは同じことである.

もしも, 行列 A と相似な対角行列 $D = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ が存在するとき, A は**対角化可能 (diagonalizable)** もしくは **半単純 (semisimple)** であると言う. そのとき, D は A の対角化と呼ばれる.

さて, 行列 A が $P^{-1}AP = D = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ と対角化可能であるとする. このとき, P の中の n 本の列ベクトルを $p_1, \ldots, p_n$ とすると,

$$A[p_1 \ \cdots \ p_n] = [p_1 \ \cdots \ p_n] \begin{bmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{bmatrix}.$$

これはさらに次のように書き直される:

$$Ap_j = \alpha_j p_j \qquad (j = 1, \ldots, n).$$

すなわち, α_j は A の固有値であり, p_j はそれに付随する固有ベクトルである. 対角化可能な行列 A の対角化は A の固有ベクトルだけで構成される $\mathbb{C}^n$ の基底を求めることと同値である.

さて, $\mathbb{C}^n$ の標準的な基底は標準的な内積に関して正規直交基底をなすのであった. 上の議論では新たな基底 $p_1, \ldots, p_n$ として正規直交基底とは限らない任意の基底を考えた. しかし, もしも可能ならば $p_1, \ldots, p_n$ を正規直交基底に取れれば便利である. 問題 [**173**] の結果より, $p_1, \ldots, p_n$ が正規直交基底であることと $P = [p_1 \ \cdots \ p_n]$ がユニタリー行列であることは同値である. よって, 上の議論で新たな基底を正規直交基底に制限することは, 正則行列 P としてユニタリー行列のみを考えることと同値である.

行列 A がユニタリー行列 P で対角化可能であるとは $P^{-1}AP$ が対角行列になることである.

[**190**] **(5 点)** A が正規行列であり, P がユニタリー行列であれば, $P^{-1}AP$ も正規行列である. 同様の結果が Hermite 行列, 反 Hermite 行列, ユニタリー行列についても成立する. □

[**191**] **(5 点)** A が実正規行列であり, Q が実直交行列であれば, $Q^{-1}AQ$ も実正規行列である. 同様の結果が実対称行列, 実交代行列, 実直交行列についても成立する. □

[**192**] **(5 点)** 行列 A がユニタリー行列で対角化可能であれば A は正規行列である. すなわち, あるユニタリー行列 P で $P^{-1}AP$ が対角行列になるものが存在するならば A は正規行列である. □

ヒント: 対角行列は正規行列である. □

上の問題 [**192**] の結果の逆を Toeplitz の定理と呼ぶ. この節の第一の目標は Toeplitz の定理を示すことである.

[**193**] **(任意の行列の三角化可能性, 10 点)** 任意の複素 n 次正方行列 A に対して, あるユニタリー行列 P で $P^{-1}AP$ が上三角行列になるものが存在する. □

ヒント: n に関する数学的帰納法. A の固有値 α とそれに付随する固有ベクトル v が存在する. v は単位ベクトルに取れ, v を含む正規直交基底 $p_1 = v, p_2, \ldots, p_n$ が取れる. このとき, $P = [p_1 \ \cdots \ p_n]$ と置くと, $P^{-1}AP$ は次の形になる:

$$P^{-1}AP = \begin{bmatrix} \alpha & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \cdots & b_{nn} \end{bmatrix}.$$

行列 $B = [b_{ij}]_{2 \le i,j \le n}$ に帰納法の仮定を用いよ. □

[194] (Toeplitz の定理, 10 点) 任意の正規行列 A に対してユニタリー行列 P で $P^{-1}AP$ が対角行列になるものが存在する. すなわち, $\mathbb{C}^n$ の正規直交基底 $p_1, \ldots, p_n$ で

$$Ap_j = \alpha_j p_j, \qquad \alpha_j \in \mathbb{C}$$

を満たすものが存在する. □

ヒント: **[193]** より, 正規な上三角行列が対角行列であることを示せば十分である. A を正規な上三角行列であるとし, $A^*A = AA^*$ の両辺の対角成分を比較してみよ. □

18.3 実正規行列の標準形

[195] (半単純実行列の標準形, 10 点) A は実 n 次正方行列であり, 複素正則行列を用いて対角化可能であるとする. このとき, 実正則行列 Q で $Q^{-1}AQ$ が次の形になるものが存在する:

$$Q^{-1}AQ = \begin{bmatrix} \alpha_1 & & & & & & & \\ & \ddots & & & & & & \\ & & \alpha_r & & & & & \\ & & & a_1 & b_1 & & & \\ & & & -b_1 & a_1 & & & \\ & & & & & \ddots & & \\ & & & & & & a_s & b_s \\ & & & & & & -b_s & a_s \end{bmatrix}.$$

ここで, $r + 2s = n$ かつ $\alpha_j, a_k, b_k \in \mathbb{R}$ であり, $b_k \neq 0$. このとき, α_j の全体は A の特性多項式の実数根の全体に一致し, $a_k \pm b_k i$ の全体は A の特性多項式の虚数根全体に一致する. □

ヒント: 実数の固有値に付随する固有ベクトルは実ベクトルに取れる. 虚数の固有値に付随する固有ベクトルは次のように処理する. $a, b \in \mathbb{R}$, $\alpha = a + bi$, $Ap = \alpha p$ のとき, A が実行列ならば $A\bar{p} = \bar{\alpha}\bar{p}$ であるから, $x = \mathrm{Re}\, p = (p + \bar{p})/2$, $y = \mathrm{Im}\, p = (p - \bar{p})/(2i)$ と置くと, $Ax = ax - by$, $Ay = bx + ay$. □

[196] (実正規行列に対する Toeplitz の定理, 10 点) 任意の実正規行列 A に対して直交行列 Q で $Q^{-1}AQ$ が次の形になるものが存在する:

$$Q^{-1}AQ = \begin{bmatrix} \alpha_1 & & & & & & & \\ & \ddots & & & & & & \\ & & \alpha_r & & & & & \\ & & & a_1 & b_1 & & & \\ & & & -b_1 & a_1 & & & \\ & & & & & \ddots & & \\ & & & & & & a_s & b_s \\ & & & & & & -b_s & a_s \end{bmatrix}.$$

ここで, $r + 2s = n$ かつ $\alpha_j, a_k, b_k \in \mathbb{R}$ であり, $b_k \neq 0$. このとき, α_j $a_k \pm b_k i$ の全体は A の特性多項式の根の全体に一致している. □

ヒント: 佐武 [St] の 170–171 頁. □

[197] (実対称行列の対角化, 10 点) 実対称行列 A に対してある直交行列 Q で $Q^{-1}AQ$ が実対角行列になるものが存在する. □

[198] (実交代行列の標準形, 10 点) 実交代行列 A に対してある直交行列 Q で $Q^{-1}AQ$ が次の形になるものが存在する:

$$Q^{-1}AQ = \begin{bmatrix} 0 & & & & & & & \\ & \ddots & & & & & & \\ & & 0 & & & & & \\ & & & 0 & b_1 & & & \\ & & & -b_1 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & b_s \\ & & & & & & -b_s & 0 \end{bmatrix}.$$

ここで, $b_k \in \mathbb{R}$ かつ $b_k \neq 0$. □

[199] (直交行列の標準形, 10 点) 直交行列 A に対してある直交行列 Q で $Q^{-1}AQ$ が次の形になるものが存在する:

$$Q^{-1}AQ = \begin{bmatrix} E_{r_1} & & & & & & & \\ & -E_{r_2} & & & & & & \\ & & \cos\theta_1 & \sin\theta_1 & & & & \\ & & -\sin\theta_1 & \cos\theta_1 & & & & \\ & & & & \ddots & & & \\ & & & & & \cos\theta_s & \sin\theta_s & \\ & & & & & -\sin\theta_s & \cos\theta_s & \end{bmatrix}.$$

ここで, $r_1 + r_2 + 2s = n$ かつ $\theta_k \in \mathbb{R}$ であり, E_r は r 次の単位行列である. □

以上の結果は非常に有用である. なぜならば多くの意味のある行列は正規行列になっているからである. 正規行列はユニタリー行列で対角化可能である. 実正規行列は直交行列によって標準形に変換できる.

19 実対称行列

この節は第 18 節の問題 [**197**] の続きである. 実対称行列に関する基本的な結果とその応用について説明する.

19.1 実対称行列, 実交代行列, 直交行列の定義

正方行列 A が**対称行列 (symmetric matrix)** であるとは ${}^tA = A$ が成立することであり[22], A が**交代行列 (alternating matrix, skew-symmetrix matrix)** であるとは ${}^tA = -A$ が成立することである. さらに, 実正方行列 A が**直交行列 (orthogonal matrix)** であるとは ${}^tAA = A{}^tA = E$ が成立することである.

[200] P は実 n 次行列であるとし, その列ベクトルの全体を $p_1, \ldots, p_n$ と書く. このとき, P が直交行列であるための必要十分条件は $p_1, \ldots, p_n$ が $\mathbb{R}^n$ の正規直交基底になることである. □

[201] A が n 次実対称行列であり, P が n 次実正則行列であるとき, ${}^tPAP$ も実対称行列になる. 特に P が直交行列であれば $P^{-1}AP$ も実対称行列になる. 同様の結果が実交代行列に関しても成立する. □

[202] 任意の n 次正方行列は対称行列と交代行列の和に一意的に分解可能である. □

ヒント: f は実軸上の任意の実数値函数であるとする. このとき, $g(x) = (f(x)+f(-x))/2$, $h(x) = (f(x) - f(-x))/2$ と置くと, $f = g + h$ でかつ g, h はそれぞれ偶函数, 奇函数になる. 任意の f は偶函数 g と奇函数 h の和に一意的に分解される. たとえば, $f(x) = e^x$ のとき, $g(x) = \cosh x$, $h(x) = \sinh x$. □

[203] n 次実対称行列全体の集合を $\mathrm{Sym}_n(\mathbb{R})$ と書き, n 次実交代行列全体の集合を $\mathrm{Alt}_n(\mathbb{R})$ と書く. このとき, $\mathrm{Sym}_n(\mathbb{R})$, $\mathrm{Alt}_n(\mathbb{R})$ は実ベクトル空間をなし, $\dim_{\mathbb{R}} \mathrm{Sym}_n(\mathbb{R}) = n(n+1)/2$, $\dim_{\mathbb{R}} \mathrm{Alt}_n(\mathbb{R}) = n(n-1)/2$ が成立する. □

[204] A, B が n 次対称行列であるとき, AB も対称行列になるための必要十分条件は A と B が可換[23]であることである. □

19.2 実対称行列の対角化可能性

[205] A が 2×2 の実対称行列であるとき, その特性多項式 $p_A(\lambda) = \det(\lambda E - A)$ が実根を持つことを判別式が非負になることをチェックすることによって証明せよ. □

[206] 実対称行列の固有値はすべて実数である[24]. □

ヒント: A は n 次の実対称行列であるとし, α は A の固有値であるとし, v はそれに付随する固有ベクトルであるとする. すなわち, $Av = \alpha v$, $\alpha \in \mathbb{C}$, $v \in \mathbb{C}^n$, $v \neq 0$. このとき, A が実対称行列であることより $\langle Av, v\rangle = \langle v, Av\rangle$. この等式の左辺と右辺を☆☆略☆☆と計算すると $\overline{\alpha} = \alpha$ であることがわかる. □

すでに問題 **[197]** で示されている「実対称行列の直交行列による対角化可能性」の証明の方針をここで再度紹介することにしよう. 正規行列まで一般化した議論がわかり難いと感じる人はまず最初に実対称行列の場合を扱ってみるのが良い. (もしくは Hermite 行列でも良い.)

---

[22] このプリントでは行列の転置を ${}^tA$ と表わしている. しかし, 多数派は ${}^tA$ の方であるようだ. 右上に転置の記号を書く場合には A^T と大文字の T を使うことが多い. この演習の転置行列の記号法は多数派にしたがっていないので注意して欲しい.

[23] $AB = BA$ であるということ.

[24] 固有値と固有ベクトルの組は複素数と複素ベクトルの範囲で探す.

[207] A は n 次実対称行列であるとし, $\alpha \in \mathbb{R}$ はその固有値であり, $p \in \mathbb{R}^n$ はそれに付随する固有ベクトルであるとする. このとき, p の直交補空間 $W = \{\, q \in \mathbb{R}^n \mid \langle p, q\rangle = 0 \,\}$ は A の作用で閉じている. すなわち $AW \subset W$ が成立している. □

ヒント: $\langle p, q\rangle = 0$ のとき $\langle p, Aq\rangle = ☆☆ = ☆☆ = ☆☆ = 0$. □

[208] **(実対称行列の対角化可能性)** 問題 **[207]** を用いた n に関する数学的帰納法によって, 以下を証明せよ:

(1) 任意の n 次実対称行列 A に対して, ある直交行列 P で $P^{-1}AP$ が実対角行列になるものが存在する.

(2) 任意の n 次実対称行列 A に対して, $\mathbb{R}^n$ のある正規直交基底 $p_1, \ldots, p_n$ と実数 $\alpha_1, \ldots, \alpha_n$ で $Ap_i = \alpha_i p_i$ $(i = 1, \ldots, n)$ を満たすものが存在する. □

ヒント: 問題 **[207]** の状況を考え, $q_1 = p$ と置き, W の正規直交基底 $q_2, \ldots, q_n$ を任意に取ると, $q_1, \ldots, q_n$ は $\mathbb{R}^n$ の正規直交基底になり, $Aq_1 = \alpha q_1$ であり, $Aq_2, \ldots, Aq_n$ は $q_2, \ldots, a_n$ の実一次結合になる. よって, $Q = [q_1 \ \cdots \ q_n]$ は直交行列になり, ある $n-1$ 次の実正方行列 B が存在して, $Q^{-1}AQ$ は次の形になる:

$$Q^{-1}AQ = \begin{bmatrix} \alpha & 0 \\ 0 & B \end{bmatrix}$$

$Q^{-1}AQ = {}^tQAQ$ も対称行列になるので B も対称行列になる. よって B に帰納法の仮定を適用できる. □

上と同様の結果は複素対称行列に対しては成立しない. (Hermite 行列に対してなら成立する.)

[209] ある複素対称行列 A でどのような正則行列 P を取っても $P^{-1}AP$ が対角行列にならないようなものが存在することを示せ. □

ヒント: 次の問題 **[210]** を使えば 2×2 の複素行列 A でそのような例を作ることは簡単である. A の成分をいつものように a, b, c, d と書き, $A \neq 0$, ${}^tA = A$, $A^2 = 0$ を満たす複素数 a, b, c, d を探してみよ. □

例: $A = \begin{bmatrix} i & 1 \\ 1 & -i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ i & 1 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ i & 1 \end{bmatrix}$ は複素対称行列でかつ $A^2 = 0$. □

[210] 半単純[25]かつ巾零[26]な n 次正方行列は零行列に限る. □

参考: 実は任意の正方行列は互いに可換な半単純行列と巾零行列の和に一意的に分解される (Jordan 分解). 上の問題の結果はその特殊な場合である. 行列の Jordan 分解およびその精密化である Jordan 標準形の理論に関しては後で説明する.

[25]正方行列 A が**半単純 (semisimple)** であるとはある正則行列 P で $P^{-1}AP$ が対角行列になるものが存在することである. ただし, A が実行列であっても P として複素行列も考えることに注意せよ. (K が任意の体であり, A が K の元を成分として持つ n 次正方行列であるとき, A が半単純であるとは K の代数閉包 $\bar{K}$ の元を成分として持つ n 次正則行列 P で $P^{-1}AP$ が対角行列になるものが存在することである.)

[26]正方行列 A が**巾零 (nilpotent)** であるとはある自然数 k で $A^k = 0$ となるものが存在することである.

19.3 実対称行列の対角化と固有値問題

実対称行列の対角化可能性 [**208**] の第一の解釈は実対称行列を実一次変換とみなすことによって得られる. 第二の解釈は実対称行列を実二次形式とみなすことによって得られる. この節の残りの部分では第一の解釈について解説し, 第二の解釈は次の節で扱うことにする.

A は n 次の実正方行列であるとする. A の実縦ベクトルへの積は $\mathbb{R}^n$ の一次変換[27]を定める. 逆にその一次変換を $\mathbb{R}^n$ の標準的な正規直交基底 $e_1, \ldots, e_n$ に作用させれば A の (i,j) 成分 a_{ij} が得られる:

$$Ae_j = \sum_{i=1}^{n} e_i a_{ij} = \sum_{i=1}^{n} a_{ij} e_i \quad (j = 1, \ldots, n).$$

しかし, $\mathbb{R}^n$ の基底の取り方は標準的な正規直交基底意外にも無限に存在する. 「目的に応じて基底の取り方を変える」という考え方は線形代数において最も基本的である. 行列 A の定める一次変換の性質を調べるためにはそのために最も便利な基底を選んでおくべきである.

A は n 次の実対称行列であるとし, A が定める $\mathbb{R}^n$ の一次変換について考える. 実対称行列の対角化可能性 [**208**] より, $\mathbb{R}^n$ のある正規直交 $p_1, \ldots, p_n$ と実数 $\alpha_1, \ldots, \alpha_n$ で

$$Ap_j = \alpha_j p_j \quad (j = 1, \ldots, n)$$

を満たすものが存在する. すなわち, 基準になる正規直交基底をうまく取り直せば, 実対称対称行列が定める一次変換は正規直交基底に含まれるベクトルを実数倍する変換に過ぎないことがわかる.

[**211**] 2 次の実対称行列 A と $p_1, p_2 \in \mathbb{R}^2$ を次のように定める:

$$A = \frac{1}{2}\begin{bmatrix} 5 & 1 \\ 1 & 5 \end{bmatrix}, \quad p_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad p_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 \\ 1 \end{bmatrix}.$$

このとき, p_1, p_2 は $\mathbb{R}^2$ の正規直交基底であり, A が定める $\mathbb{R}^2$ の一次変換は p_1 を 2 倍し, p_2 を 3 倍する. すなわち, 標準的な x 軸, y 軸を 45 度傾けたものを新たな直交軸とすると, 行列 A が定める一次変換は新たな直交軸のそれぞれを 2 倍, 3 倍に拡大する一次変換であることがわかる. (実際に図を描いてこのことをわかり易く説明せよ.) □

[**212**] 次の実対称行列を対角化せよ:

$$(1) \quad A_3 = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix}, \qquad (2) \quad A_3^{(1)} = \begin{bmatrix} 2 & -1 & 0 & -1 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & 0 \\ -1 & 0 & -1 & 2 \end{bmatrix}, \quad \square$$

参考: 上の $n = 3$ の場合だけではなく一般の n についても上と同様に行列 A_n, $A_n^{(1)}$ が定義される. ただし, $A_1^{(1)}$ の場合だけは例外的に非対角成分を -2 とする. それらの行列を

[27] ベクトル空間 V からそれ自身への線形写像を V の**一次変換 (linear transformation)** と呼ぶ.

A 型の Cartan 行列と呼ぶ. 実は A 型以外にも $B,\dots,F$ 型の Cartan 行列も定義され, それらは基本的な対称性を記述するための最小限のデータになっている.

略解: 直交行列 P, Q を次のように定める:

$$P=\begin{bmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \qquad Q=\begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{\sqrt{2}} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{\sqrt{2}} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{2} \end{bmatrix}$$

このとき, $P^{-1}A_3P=\mathrm{diag}(2,2+\sqrt{2},2-\sqrt{2})$, $Q^{-1}A_3^{(1)}Q=\mathrm{diag}(0,2,2,4)$. □

[213] 次の実対称行列 A_i の対角化 D_i と直交行列 P_i で $P_i^{-1}AP_i=D_i$ となるもの求めよ:

$$A_1=\begin{bmatrix} 2 & -2 & -1 \\ -2 & 2 & 1 \\ -1 & 1 & 5 \end{bmatrix}, \quad A_2=\begin{bmatrix} -3 & -6 & 6 \\ -6 & 1 & 3 \\ 6 & 3 & 1 \end{bmatrix}.$$

可能ならば P_i を整数だけを成分に持つ行列と対角行列の積で表わせ. □

略解: $D_1=\mathrm{diag}(0,3,6)$, $D_2=\mathrm{diag}(6,-11,4)$,

$$P_1=\begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ 0 & 1 & 2 \end{bmatrix}\begin{bmatrix} \sqrt{2} & 0 & 0 \\ 0 & \sqrt{3} & 0 \\ 0 & 0 & \sqrt{6} \end{bmatrix}^{-1},$$
$$P_2=\begin{bmatrix} 4 & -3 & 0 \\ -3 & -2 & 1 \\ 3 & 2 & 1 \end{bmatrix}\begin{bmatrix} \sqrt{34} & 0 & 0 \\ 0 & \sqrt{17} & 0 \\ 0 & 0 & \sqrt{2} \end{bmatrix}^{-1}. \quad \square$$

[214] 次の実対称行列 A_i の対角化 D_i と直交行列 P_i で $P_i^{-1}AP_i=D_i$ となるもの求めよ:

$$A_3=\begin{bmatrix} -1 & -6 & -6 \\ -6 & -1 & 6 \\ -6 & 6 & 6 \end{bmatrix}, \quad A_4=\begin{bmatrix} 5 & 2 & -4 \\ 2 & 5 & -4 \\ -4 & -4 & 3 \end{bmatrix}.$$

可能ならば P_i を整数だけを成分に持つ行列と対角行列の積で表わせ. □

略解: $D_3=\mathrm{diag}(-3,-7,14)$, $D_4=\mathrm{diag}(3,11,-1)$,

$$P_3=\begin{bmatrix} -3 & 1 & -2 \\ 3 & 1 & 2 \\ -4 & 0 & 3 \end{bmatrix}\begin{bmatrix} \sqrt{34} & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & \sqrt{17} \end{bmatrix}^{-1},$$
$$P_4=\begin{bmatrix} -1 & -1 & 1 \\ 1 & -1 & 1 \\ 0 & 1 & 2 \end{bmatrix}\begin{bmatrix} \sqrt{2} & 0 & 0 \\ 0 & \sqrt{3} & 0 \\ 0 & 0 & \sqrt{6} \end{bmatrix}^{-1}. \quad \square$$

[215] 次の実対称行列 A_i の対角化 D_i と直交行列 P_i で $P_i^{-1}AP_i = D_i$ となるもの求めよ:

$$A_5 = \begin{bmatrix} -2 & 2 & -1 \\ 2 & -2 & -1 \\ -1 & -1 & 1 \end{bmatrix}, \quad A_6 = \begin{bmatrix} -2 & -3 & -3 \\ -3 & 3 & -2 \\ -3 & -2 & 3 \end{bmatrix}.$$

可能ならば P_i を整数だけを成分に持つ行列と対角行列の積で表わせ. □

略解: $D_5 = \mathrm{diag}(-4, 2, -1)$, $D_6 = \mathrm{diag}(4, 5, -5)$,

$$P_5 = \begin{bmatrix} -1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & -2 & 1 \end{bmatrix} \begin{bmatrix} \sqrt{2} & 0 & 0 \\ 0 & \sqrt{6} & 0 \\ 0 & 0 & \sqrt{3} \end{bmatrix}^{-1},$$

$$P_6 = \begin{bmatrix} -1 & 0 & 2 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \sqrt{3} & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & \sqrt{6} \end{bmatrix}^{-1}. \quad \square$$

[216] 次の実対称行列 A_i の対角化 D_i と直交行列 P_i で $P_i^{-1}AP_i = D_i$ となるもの求めよ:

$$A_7 = \begin{bmatrix} -3 & 0 & -1 & 2 \\ 0 & 1 & 3 & 0 \\ -1 & 3 & 0 & 2 \\ 2 & 0 & 2 & 0 \end{bmatrix}, \quad A_8 = \begin{bmatrix} 5 & 2 & 4 & -1 \\ 2 & 0 & 2 & 2 \\ 4 & 2 & -1 & 2 \\ -1 & 2 & 2 & 1 \end{bmatrix}.$$

可能ならば P_i を整数だけを成分に持つ行列と対角行列の積で表わせ. □

略解: $D_7 = \mathrm{diag}(-5, -2, 1, 4)$, $D_8 = \mathrm{diag}(3, -4, 8, -2)$,

$$P_7 = \begin{bmatrix} -3 & -1 & -1 & 0 \\ 1 & -1 & 1 & 2 \\ -2 & 1 & 0 & 2 \\ 2 & 0 & -2 & 1 \end{bmatrix} \begin{bmatrix} 3\sqrt{2} & 0 & 0 & 0 \\ 0 & \sqrt{3} & 0 & 0 \\ 0 & 0 & \sqrt{6} & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}^{-1},$$

$$P_8 = \begin{bmatrix} -2 & 1 & 7 & 1 \\ 2 & 0 & 3 & -6 \\ 1 & -2 & 4 & 2 \\ 4 & 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & \sqrt{6} & 0 & 0 \\ 0 & 0 & 5\sqrt{3} & 0 \\ 0 & 0 & 0 & 5\sqrt{2} \end{bmatrix}^{-1}. \quad \square$$

[217] 次の実対称行列 A_i の対角化 D_i と直交行列 P_i で $P_i^{-1}AP_i = D_i$ となるもの求めよ:

$$A_9 = \begin{bmatrix} 3 & 2 & 2 & 2 \\ 2 & 2 & -2 & 5 \\ 2 & -2 & 3 & -2 \\ 2 & 5 & -2 & 2 \end{bmatrix}, \quad A_{10} = \begin{bmatrix} 5 & -1 & 2 & -1 \\ -1 & 4 & -1 & 0 \\ 2 & -1 & 5 & -1 \\ -1 & 0 & -1 & 4 \end{bmatrix}. \quad \square$$

可能ならば P_i を整数だけを成分に持つ行列と対角行列の積で表わせ. □

略解: $D_9 = \mathrm{diag}(-3, 9, 5, -1)$, $D_{10} = \mathrm{diag}(8, 3, 3, 4)$,

$$P_9 = \begin{bmatrix} 0 & -1 & 1 & -2 \\ 1 & -2 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ -1 & -2 & 0 & 1 \end{bmatrix} \begin{bmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & \sqrt{10} & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 \\ 0 & 0 & 0 & \sqrt{10} \end{bmatrix}^{-1},$$

$$P_{10} = \begin{bmatrix} -2 & 1 & -2 & 0 \\ 1 & 1 & 1 & 1 \\ -2 & 0 & 3 & 0 \\ 1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} \sqrt{10} & 0 & 0 & 0 \\ 0 & \sqrt{3} & 0 & 0 \\ 0 & 0 & \sqrt{15} & 0 \\ 0 & 0 & 0 & \sqrt{2} \end{bmatrix}^{-1}. \quad \square$$

[218] 問題 **[212]** で定義した Cartan 行列 $A_3^{(1)}$ の (i, j) 成分を a_{ij} と書き, 慣習にしたがって Cartan 行列の添字の 4 を 0 に置換するために $a_{0j} = a_{4j}$, $a_{i0} = a_{i4}$ と置く. a_{ij} $(i = 1, 2, 3)$ は Cartan 行列 A_3 の成分に一致している. z の多項式を成分に持つ行列 E_i, F_i, H_i $(i = 0, 1, 2, 3)$ を次のように定める:

$$E_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ E_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ E_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ E_0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ z & 0 & 0 & 0 \end{bmatrix},$$

$$F_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ F_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ F_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \ F_0 = \begin{bmatrix} 0 & 0 & 0 & z^{-1} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ H_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ H_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \ H_0 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

このとき, $i, j = 0, 1, 2, 3$ に対して以下が成立する:

1. $[H_i, E_j] = a_{ij} E_j, \quad [H_i, F_j] = -a_{ij} F_j$;
2. $[E_i, F_j] = \delta_{ij} H_i$;
3. $[E_i, [E_i, E_j]] = 0, \quad [F_i, [F_i, F_j]] = 0 \quad (i \neq j)$.

ここで $[X, Y] = XY - YX$ である. $\square$

参考: 上の問題の E_i, F_i, H_i $(i = 1, 2, 3)$ は Lie 代数 sl_3 の **Chevalley 生成元 (Chevalley generators)** と呼ばれており, E_i, F_i, H_i $(i = 0, 1, 2, 3)$ はアフィン Lie 代数 $\widehat{\mathrm{sl}}_3$ の **Chevalley 生成元 (Chevalley generators)** と呼ばれている. アフィン Lie 代数に関する教科書としては谷崎 [Tn] や脇本 [W] がおすすめである.

19.4 Hadamard の不等式

実対称行列もしくはより一般に Hermite 行列 A が**非負もしくは非負値 (non-negative)** であるとはそのすべての固有値が非負であることである. そのとき $A \geq 0$ と書く. すべての固有値が正であるとき A は**正もしくは正値 (positive)** であると言い, $A > 0$ と書く.

[219] A は実対称行列であるとする. このとき, A が非負値であるための必要十分条件はある実対称行列 B によって $A = B^2$ と表わせることである. □

ヒント: 十分性. A の固有値 α_i がすべて非負ならばその平方根 β_i を実数に取れる. $D = \mathrm{diag}(\beta_1, \ldots, \beta_n)$ と置く. 対称行列の直交行列による対角化可能性より, ある直交行列 P が存在して $A = PD^2\,{}^tP = PD\,{}^tPPD\,{}^tP$. □

[220] (Cholesky 分解) A が n 次正値実対称行列ならば対角成分が正の上三角行列 R で $A = {}^tRR$ を満たすものが一意に存在する. これを A の Cholesky 分解と呼ぶ. □

ヒント: 存在. 問題 **[219]** よりある実正方行列 B で $A = {}^tBB$ を満たすものが存在する[28]. A は正則行列なので B もそうである. よって B の中の列ベクトルたちに Schmidt の正規直交化法を適用することによって, 直交行列 Q と対角成分が正の上三角行列 R で $B = QR$ を満たすものが存在する (問題 **[175]**). このとき, $A = {}^tBB = {}^tRR$.

一意性. S も対角成分が正の上三角行列で $A = {}^tSS$ を満たしていると仮定する. このとき, ${}^tRR = {}^tSS$ なので $X = RS^{-1}$ と置くと $X = {}^t(X^{-1})$ である. X は対角成分が正の上三角行列であり, X^{-1} は対角成分が X のそれの逆数であるような上三角行列である. よって $X = E$ すなわち $R = S$ である. □

参考: A は正値実対称行列であり, その n 個の固有値は互いに異なると仮定する. そのとき, A_n $(n = 0, 1, 2, \ldots)$ を帰納的に $A_0 = A$, $A_n = {}^tR_nR_n$ (Cholesky 分解), $A_{n+1} = R\,{}^tR$ と定める. このとき, 列 A_n はある対角行列 D に収束し, D の対角成分は A の固有値が大きな順に並ぶ. この結果を用いれば固有値が互いに異なる正値実対称行列の固有値の近似値を数値計算することができる. この数値計算法とオープン戸田格子という古典可積分系の間には直接的な関係があることが知られている. 他にも行列の固有値の近似値を求める数値計算法には Cholesky 分解を使う方法の他に岩沢分解 ([**174**], [**175**]) を使う方法 (QR 法) などがある.

数値計算のアルゴリズムと可積分系の密接な関係に関しては中村 [N] を参照せよ. 行列の数値計算には GNU Octave[29] というフリーソフトウェアが便利である. 最近では科学技術計算に使える便利なフリーソフトウェアがたくさん存在する. □

[221] $A = [a_{ij}]$ が n 次非負値実対称行列ならば

$$|A| \leq \prod_{i=1}^{n} a_{ii}.$$

等号が成立するための必要十分条件は A が対角行列であることである. □

ヒント: A が正値と仮定して不等式を証明すれば十分である. なぜならば A が 0 を固有値として持つならば $A + \varepsilon E > 0$ $(\varepsilon > 0)$ に関する不等式の $\varepsilon \to 0$ の極限で A 自身に関する不等式が得られるからである. そこで $A > 0$ と仮定する. 問題 **[220]** より対角成分が正の上三角行列 R で $A = {}^tRR$ を満たすものが存在する. このとき $A = [a_{ij}]$ は $R = [r_{ij}]$ とすると, $a_{ii} = p_{1i}^2 + \cdots + p_{ii}^2 \geq p_{ii}^2$ である. よって,

$$\prod_{i=1}^{n} a_{ii} \geq \prod_{i=1}^{n} p_{ii}^2 = |P|^2 = |A|.$$

[28] B は実対称行列に取れるがここではその事実は必要ない.

[29] http://www.octave.org/

以上の議論によって不等号で等号が成立するための必要十分条件は R が対角行列であることである．そのための必要十分条件は R の一意性より A が対角行列であることである． □

[**222**] A は Hermite 行列であるとする．このとき, A が非負であるための必要十分条件はある Hermite 行列 B によって $A = B^2$ と表わせることである． □

ヒント: 問題 [**219**] とまったく同じやり方． □

解説: 実数について成立することの多くが対称行列や Hermite 行列でも成立する． □

[**223**] A が n 次正値 Hermite 行列ならば対角成分が正の複素上三角行列 R で $A = R^*R$ を満たすものが一意に存在する． □

ヒント: 一意性の証明は問題 [**220**] とまったく同様. 存在もほとんど同様で問題 [**174**] を使う． □

[**224**] $A = [a_{ij}]$ が n 次非負値 Hermite 行列ならば

$$|A| \leq \prod_{i=1}^{n} a_{ii}.$$

等号が成立するための必要十分条件は A が対角行列であることである． □

ヒント: 問題 [**221**] とまったく同様． □

[**225**] 任意の複素行列 A に対して $H = A^*A$ は非負値 Hermite 行列になる． □

ヒント: $H^* = A^*(A^*)^* = A^*A = H$. $Hu = \alpha u$ とすると, $\alpha\langle u, u\rangle = \langle u, Hu\rangle = \langle Au, Au\rangle \geq 0$. □

[**226**] **(Hadamard の不等式)** $A = [a_{ij}]$ は任意の n 次複素行列であるとし, A の中の n 本の列ベクトルを $a_1, \ldots, a_n$ と表わす．このとき,

$$|\det A| \leq \prod_{i=1}^{n} ||a_i|| \leq n^{n/2} \left[\max_{1\leq i,j\leq n} |a_{ij}|\right]^n.$$

ここで $|\det A|$ は行列 A の行列式の絶対値である． □

行列式の絶対値を上から評価しなければいけなくなったら, Hadamard の不等式というものがあったことを思い出そう.

ヒント: 問題 [**225**] より $H = A^*A$ と置くと $H = [h_{ij}]$ は非負値 Hermite 行列になる. よって不等式 [**224**] を H に適用できる. $h_{ii} = ||a_i||^2$ である．よって,

$$|\det A|^2 = \det H \leq \prod_{i=1}^{n} h_{ii} = \prod_{i=1}^{n} ||a_i||^2$$

よって $|\det A| \leq \prod_{i=1}^{n} ||a_i||$ である. $M = \max_{1\leq i,j\leq n} |a_{ij}|$ と置くと $||a_i||^2 \leq nM^2$ であるから, $\prod_{i=1}^{n} ||a_i|| \leq n^{n/2}M^n$ である． □

[227] A は任意の (m,n) 型実行列であるとすると以下が成立する:

(1) ${}^tAA$ は n 次の対称行列になり, その固有値はすべて非負の実数になる. そこで, ${}^tAA$ の 0 でない固有値の全体を $\gamma_1^2,\dots,\gamma_r^2$ $(\gamma_i\in\mathbb{R})$ と表わしておく.

(2) ある m 次の直交行列 P とある n 次の直交行列 Q が存在して,

$$ {}^tPAQ=\begin{bmatrix}\gamma_1 & & & & & & 0\\ & \ddots & & & & & \\ & & \gamma_r & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ 0 & & & & & 0 & \end{bmatrix}. \quad \square $$

ヒント: (1) ${}^tAAq=\beta q$ とすると, $0\le\langle Aq,Aq\rangle=\langle q,{}^tAAq\rangle=\beta\langle q,q\rangle$. (2) 対称行列の対角化可能性と (1) より, ある n 次の直交行列 Q が存在して,

$$ {}^t(AQ)AQ={}^tQ\,{}^tAAQ=\begin{bmatrix}\beta_1 & & 0\\ & \ddots & \\ 0 & & \beta_n\end{bmatrix}. $$

ここで $\beta_i=\gamma_i^2$ $(i=1,\dots,r)$, $\beta_i=0$ $(i=r+1,\dots,n)$. よって, AQ の $i=1,\dots,r$ 番目の列ベクトルを $b_i\in\mathbb{R}^m$ と書くと $\langle b_i,b_j\rangle=\gamma_i^2\delta_{ij}$ が成立しており, AQ の $i=r+1,\dots,n$ 番目の列ベクトルは 0 である. よって, $p_i=b_i/\gamma_i$ $(i=1,\dots,r)$ を拡張して $\mathbb{R}^m$ の正規直交基底 $p_1,\dots,p_m$ を構成でき, 直交行列 P を $P=[p_1\ \cdots\ p_m]$ と定めると ${}^tPAQ$ が上の形になる. $\square$

[228] A は任意の (m,n) 型複素行列であるとすると以下が成立する:

(1) A^*A は n 次の Hermite 行列になり, その固有値はすべて非負の実数になる. そこで, A^*A の 0 でない固有値の全体を $\gamma_1^2,\dots,\gamma_r^2$ $(\gamma_i\in\mathbb{R})$ と表わしておく.

(2) ある m 次のユニタリー行列 P とある n 次のユニタリー行列 Q が存在して,

$$ P^*AQ=\begin{bmatrix}\gamma_1 & & & & & & 0\\ & \ddots & & & & & \\ & & \gamma_r & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ 0 & & & & & 0 & \end{bmatrix}. \quad \square $$

ヒント: 問題 **[227]** とまったく同じやり方. $\square$

20 実二次形式

20.1 実二次形式の定義

実対称行列は実二次形式の一つの表現だとみなすことができる. **実二次形式 (real quadratic form)** とは有限個の文字 $x_1, \ldots, x_n$ の実数係数斉次 2 次式のことである. すなわち, 次の形の式を実二次形式と呼ぶ:

$$Q(x) = \sum_{i=1}^{n} a_{ii} x_i^2 + 2 \sum_{1 \le i < j \le n} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{R}.$$

実二次形式は自然に $\mathbb{R}^n$ 上の函数とみなすこともできる.

さらに, $i > j$ のとき $a_{ij} = a_{ji}$ とおき, 実対称行列 A を $A = [a_{ij}]$ と定め, x を縦ベクトル ${}^t[x_1 \ \cdots \ x_n]$ と解釈すると,

$$Q(x) = \sum_{i,j=1}^{n} a_{ij} x_i x_j = \sum_{i,j=1}^{n} x_i a_{ij} x_j = {}^t x A x = \langle x, Ax \rangle = \langle Ax, x \rangle$$

と書くことができる. これによって, 実対称行列 A と実二次形式 Q が一対一に対応している. 実対称行列 A に対応する二次形式を

$$Q_A(x) := A[x] := {}^t x A x$$

と書くことにする. ここで Q は quadratic の頭文字であり, $A[x]$ は Siegel の記号法である (佐武 [St] 158 頁).

実対称行列は実対称双一次形式の一つの表現だとみなすことができる. **実対称双一次形式 (real symmetric bilinear form)** とは写像 $B : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ で任意の $x, x_i, y, y_j \in \mathbb{R}^n$, $a_i, b_j \in \mathbb{R}$ に対して以下を満たすもののことである:

(a) $B(a_1 x_1 + a_2 x_2, y) = a_1 B(x_1, y) + a_2 B(x_2, y)$,
$B(x, b_1 y_1 + b_2 y_2) = b_1 B(x, y_1) + b_2 B(x, y_2)$ (双一次性);

(b) $B(y, x) = B(x, y)$ (対称性).

実対称双一次形式 B に対して対称行列 A を $a_{ij} = B(e_i, e_j)$, $A = [a_{ij}]$ と定めることができる. ここで e_i は $\mathbb{R}^n$ の標準的な基底である. このとき, $x, y \in \mathbb{R}^n$ の成分をそれぞれ x_i, y_j と書くと,

$$B(x, y) = \sum_{i,j=1}^{n} x_i y_j B(e_i, e_j) = \sum_{i,j=1}^{n} x_i a_{ij} y_j = {}^t x A y = \langle x, Ay \rangle = \langle Ax, y \rangle.$$

これによって実対称行列と実対称双一次形式が一対一に対応する.

実対称行列 A に対応する実双一次形式を B_A と書くことにすると,

$$Q_A(x) = B_A(x, x) = {}^t x A x.$$

以上をまとめると, これによって実二次形式と実対称双一次形式は実対称行列との対応を通して互いに一対一に対応していることがわかる.

実対称双一次形式 B に対応する実二次形式 Q は B の**極化形式 (polarization)** と呼ばれている.

[**229**] 実二次形式 Q は $\mathbb{R}^n$ 上の実数値函数であり, 次を満たしている:

(a) $Q(ax) = a^2 Q(x) \quad (a \in \mathbb{R},\, x \in \mathbb{R}^n)$;

(b) $B(x,y) = (Q(x+y) - Q(x) - Q(y))/2$ と置くと B は実対称双一次形式になる.

逆に Q がこの性質を持つ $\mathbb{R}^n$ 上の実数値函数であるとき, $a_{ij} = B(e_i, e_j)$, $A = [a_{ij}]$ と置くと $Q = Q_A$. □

解説: $B(x,y) = (Q(x+y) - Q(x) - Q(y))/2$ は $Q(x+y) = Q(x) + 2B(x,y) + Q(y)$ と書き直せる. この式は文字 x, y に関する公式 $(x+y)^2 = x^2 + 2xy + y^2$ の一般化になっている.

20.2 実二次形式の分類

可逆な線形変数変換で移り合う実二次形式は互いに同値であるという. すなわち, 実二次形式 Q_1 と Q_2 が互いに同値であるとは, ある n 次実正則行列 P が存在して,

$$Q_1(Px) = Q_2(x)$$

が成立することである. たとえば, $Q_1(x_1, x_2) = x_1^2 - x_2^2$ と $Q_2(x_1, x_2) = x_1^2 - 4x_1x_2 + 3x_2^2$ は同値である. なぜならば

$$Q_1(x_1 - 2x_2, x_2) = (x_1 - 2x_2)^2 - x_2^2 = x_1^2 - 4x_1x_2 + 3x_2^2 = Q_2(x_1, x_2).$$

線形な変数変換 $(x_1, x_2) \mapsto (x_1 - 2x_2, x_2)$ 可逆である.

[**230**] 実二次形式 Q_1 と Q_2 が同値であるとき $Q_1 \sim Q_2$ と書くと,

1. $Q_1 \sim Q_1$;
2. $Q_1 \sim Q_2 \implies Q_2 \sim Q_1$;
3. $Q_1 \sim Q_2,\, Q_2 \sim Q_3 \implies Q_1 \sim Q_3$. □

解説: この結果は実二次形式の同値性は同値関係の公理を満たしていることを意味している.

さて, 2 つの実二次形式が同値になるための必要十分条件は何だろうか. この問題に対する第一の解答が次の定理である.

定理 20.1 (Sylvester) 任意の実二次形式 Q に対してある $p, q \in \mathbb{Z}_{\geq 0}$ が存在して, Q は次の二次形式 $Q_{p,q}$ と同値になる:

$$Q_{p,q} = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2.$$

しかも, (p,q) は Q に対して一意的に定まり, 2 つの二次形式が同値になるための必要十分条件はそれぞれの (p,q) が一致することである. □

この定理の (p,q) を Q の**符号数 (signature)** と呼び, $Q_{p,q}$ を Q の標準形と呼ぶ. Q に対する符号数の一意性を **Sylvester の慣性法則 (Sylvester's law of inertia)** と呼ぶ.

注意: 文脈によっては $p-q$ を符号数 (signature) と呼ぶことも多いので注意せよ. 階数 $p+q$ とこの意味での符号数 $p-q$ の組は (p,q) と同じだけの情報量を持っている.

上の定理 20.1 を複数の演習問題に分けて証明しよう.

[231] n 次実対称行列 A, B に対応する実二次形式 Q_A, Q_B が互いに同値になるための必要十分条件はある n 次実正則行列 P で ${}^tPAP = B$ を満たすものが存在することである. □

ヒント: $Q_A(Px) = {}^t(Px)APx = {}^tx\,{}^tPAPx$. □

[232] (直交変換による実二次形式の標準形) A は n 次実対称行列であり, $\alpha_1,\dots,\alpha_n \in \mathbb{R}$ はその固有値の全体 (重複を含む) であるとする. このとき, ある n 次直交行列 T が存在して,

$$Q_A(Tx) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2.$$

$\alpha_1,\dots,\alpha_p > 0$, $\alpha_{p+1},\dots,\alpha_{p+q} < 0$, $\alpha_{p+q+1} = \cdots = \alpha_n = 0$ と仮定しても一般性が失われない. そのとき正則行列 P を

$$P = T \begin{bmatrix} \frac{1}{\sqrt{\alpha_1}} & & & & & & & & 0 \\ & \ddots & & & & & & & \\ & & \frac{1}{\sqrt{\alpha_p}} & & & & & & \\ & & & \frac{1}{\sqrt{-\alpha_{p+1}}} & & & & & \\ & & & & \ddots & & & & \\ & & & & & \frac{1}{\sqrt{-\alpha_{p+q}}} & & & \\ & & & & & & 1 & & \\ & & & & & & & \ddots & \\ 0 & & & & & & & & 1 \end{bmatrix}$$

と定めると

$$Q_A(Px) = Q_{p,q}(x) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2. \quad \square$$

ヒント: すぐ上の問題 **[231]** を用いて, 実対称行列の直交行列による対角化可能性 **[208]** を二次形式の言葉を用いて書き直しただけ. □

解説: 問題 **[232]** の結果より, 実二次形式 Q の符号数 (p,q) は Q に対応する実対称行列 A の正の固有値の個数と負の固有値の個数の組に等しいことがわかる. そこで実対称行列 A の符号数を対応する実二次形式の符号数 (p,q) であると定義しておく. □

[233] (Sylvester の慣性法則) 実二次形式 Q の符号数 (p,q) は Q から一意に定まる. □

ヒント: 二次形式 $Q_{p,q}$ を $\mathbb{R}^n$ 上の函数とみなし, n 次の正則行列 P が $Q_{p,q}(Px) = Q_{p',q'}(x)$ を満たしているとき, $p=p'$, $q=q'$ が成立していることを示せば良い.

$Q_{p,q}(x)$ に対応する実対称行列 $A_{p,q}$ の rank は $p+q$ であり, $Q_{p,q}(Px)$ に対応する実対称行列 ${}^tPAP$ の rank も $p+q$ なので $Q_{p,q}(Px) = Q_{p',q'}(x)$ より $p+q = p'+q'$ が導かれる. よって, $p < p'$ と仮定して矛盾を導けば良い.

$y = Px$ の第 i 成分を y_i と書き, x の成分 $x_1, \ldots, x_n$ に関する連立一次方程式

$$y_i = \sum_{j=1}^{n} p_{ij}x_j = 0 \quad (i = 1, \ldots, p), \qquad x_i = 0 \quad (i = p'+1, \ldots, n)$$

を考える. ここで p_{ij} は P の (i,j) 成分である. もしも $p < p'$ ならば方程式の個数 $p + (n - p')$ が n より小さくなるので, 非自明な解 $x_1, \ldots, x_n$ が存在する.

このとき, $y_{p+1}, \cdots, y_n$ について $y = Px \neq 0$ から導かれることと $Q_{p,q}(y) = Q_{p',q'}(x)$ から導かれることが互いに矛盾することを示せ. □

解: $x \neq 0$ で P は正則行列なので $y = Px \neq 0$ であり, 上の仮定より $y_1 = \cdots = y_p = 0$ なので $y_{p+1}, \cdots, y_n$ のどれかは 0 でない. ところが $Q_{p,q}(Px) = Q_{p',q'}(x)$ に非自明な解を代入すると

$$-y_{p+1}^2 - \cdots - y_{p+q}^2 = x_1^2 + \cdots + x_{p'}^2.$$

となるので, $y_{p+1}, \cdots, y_n$ がすべて 0 になってしまう. これは矛盾である. □

[234] $\mathbb{R}^n$ 上の 2 つの実二次形式が同値になるための必要十分条件はそれぞれの符号数が一致することである. □

ヒント: $Q_1(P_1x) = Q_{p,q}(x) = Q_2(P_2x)$ ならば $Q_1(P_1P_2^{-1}x) = Q_w(x)$. 逆に $Q_1(Px) = Q_2(x)$ でかつ $Q_1(T_1x) = Q_{p,q}(x)$, $Q_2(T_2x) = Q_{p',q'}(x)$ ならば $Q_{p,q}(T_2PT_1^{-1}x) = Q_{p'q'}(x)$ なので Sylvester の慣性法則を用いることができる. □

以上によって定理 20.1 の証明がすべて完了した.

20.3 n 次元実 Euclid 空間の直交座標系

[235] 2 次の実対称行列 A と 2 次行列 $P = [u\ v]$ を次のように定める:

$$A = \frac{1}{2}\begin{bmatrix} 11 & -3 \\ -3 & 19 \end{bmatrix}, \qquad P = [u\ v] = \frac{1}{\sqrt{10}}\begin{bmatrix} 3 & -1 \\ 1 & 3 \end{bmatrix}.$$

このとき, $P^{-1} = {}^tP$, $P^{-1}AP = \mathrm{diag}(5, 10)$ すなわち $Au = 5u$, $Av = 10v$ が成立する. xy 平面の新たな直交座標系 x', y' を

$$\begin{bmatrix} x \\ y \end{bmatrix} = P\begin{bmatrix} X \\ Y \end{bmatrix} = x'u + y'v$$

と定める. x' 軸と y' 軸を xy 平面に図示せよ. 行列 A の定める xy 平面からそれ自身への一次変換は $x'y'$ 座標ではどのように説明されるか? □

ヒント: x' 軸はベクトル u の方向になる. A が定める一次変換は x' 座標を☆倍して ☆座標を☆倍する一次変換である. □

さて, 以下は n 次元の一般論である.

n 次元実 Euclid 空間 $\mathbb{R}^n$ を考え, その点 x を実縦ベクトル ${}^t[x_1 \ \cdots \ x_n]$ と同一視しておく. 点 $x \in \mathbb{R}^n$ と $x_1, \ldots, x_n$ の関係は $\mathbb{R}^n$ の縦ベクトル空間としての標準的な正規直交基底 $e_1, \ldots, e_n$ を用いて,

$$x = x_1 e_1 + \cdots + x_n e_n$$

と書ける. 通常 Euclid 空間 $\mathbb{R}^n$ の座標はこの $x_1, \ldots, x_n$ を考える. しかし, Euclid 空間の中に浮かぶ物体 (直線, 平面, 球面, etc.) 形を調べるときには他の直交座標系を使うこともできるし, 実際, 目的に応じて便利な座標系を用いた方が良い.

標準的な正規直交基底 $e_1, \ldots, e_n$ と別の正規直交基底 $p_1, \ldots, p_n$ を任意に取り, 新たな直交座標系 $y_1, \ldots, y_n$ を

$$x = y_1 p_1 + \cdots + y_n p_n$$

によって定義することもできる. この式は, 直交行列 P を $P = [p_1 \ \cdots \ p_n]$ と定義することによって,

$$x = p_1 y_1 + \cdots + p_n y_n = [p_1 \ \cdots \ p_n] \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = Py.$$

ここで $y = {}^t[y_1 \ \cdots \ y_n]$ である. これを座標の直交変換と呼ぶことにする.

原点の位置を $a \in \mathbb{R}^n$ にずらして, 新たな直交座標系 $z_1, \ldots, z_n$ を

$$x = z_1 e_1 + \cdots + z_n e_n + a$$

によって定義することもできる. このとき $a = {}^t[a_1 \ \cdots \ a_n]$ とすると,

$$x_i = z_i + a_i \qquad (i = 1, \ldots, n).$$

座標 $z_1, \ldots, z_n$ がすべて 0 であるような $\mathbb{R}^n$ の点は a になる. これを座標の平行移動と呼ぶことにする.

座標の直交変換と平行移動を組み合わせて新たな直交座標系 $w_1, \ldots, w_n$ を

$$x = w_1 p_1 + \cdots + w_n p_n + a$$

によって定義することもできる. この式は

$$x = Pw + a = P(w + b).$$

と書ける. ここで $b = P^{-1}a = {}^tPa$ である.

以上では数式を用いて新たな直交座標系を作る方法を説明したが, 直観的には次のように考えれば良い. (3 次元 Euclid 空間の世界を思い浮かべながら読んで欲しい.)

当初 n 次元 Euclid 空間には標準的な直交座標系 $x_1, \ldots, x_n$ だけが定義されている. x_1 軸から x_n 軸は原点で互いに直交している.

上で定義した直交座標系 $y_1, \ldots, y_n$ において, 各 y_i 軸の方向は x_i 軸に等しいが, y_i 軸たちは原点ではなく点 a で交わっている.

上で定義した直交座標系 $z_1, \ldots, z_n$ において, z_i 軸たちは原点で直交しているが, それらの向きは x_i 軸たちとは全然異なっている.

上で定義した直交座標系 $w_1, \ldots, w_n$ において, w_i 軸たちは原点ではなく点 a で交わっており, それらの向きは x_i 軸たちとは全然異なっている.

第第 20.4 節では実二次函数および実二次超曲面を直交変換と平行移動によって変数変換して調べる.

ここでは, 最も簡単な一次函数の場合をまず調べておこう.

n 次元実 Euclid 空間 $\mathbb{R}^n$ 上の一次函数とは

$$f(x) = \sum_{i=1}^{n} a_i x_i + b$$

の形の函数のことである. ここで $a_i, b \in \mathbb{R}$ である. 縦ベクトル $a \in \mathbb{R}^n$ を $a = {}^t[a_1 \ \cdots \ a_n]$ と定めると,

$$f(x) = {}^t a x + b = \langle a, x \rangle + b$$

と書ける. もしも $a = 0$ ならば

$$f(x) = b \tag{1}$$

となる. $a \neq 0$ ならば単位ベクトル $p_1 = a/\,||a||$ を含む $\mathbb{R}^n$ の正規直交基底 $p_1, \ldots, p_n$ を取れる. 直交行列 P を $P = [p_1 \ \cdots \ p_n]$ と定める. このとき,

$${}^t a P = \big[\langle a, p_1 \rangle \ \langle a, p_2 \rangle \ \cdots \ \langle a, p_n \rangle\big] = [\alpha \ 0 \ \cdots \ 0].$$

ここで $\alpha = ||a|| > 0$ である. よって, x に Py を代入すると

$$g(y) := f(Py) = {}^t a P y + b = \alpha y_1 + b = \alpha(y_1 + c).$$

ここで $c = b/\alpha$ である. y_1 軸はちょうどベクトル a の報告を向いている. よって, a と x の内積は x の y_1 軸への射影の $\alpha = ||a||$ 倍になる. ($n = 3$ の場合に関して図を描いてみよ.) さらに, y に $z - ce_1$ を代入すると

$$h(z) := g(z - ce_1) = \alpha(z_1 - c + c) = \alpha z_1. \tag{2}$$

よって $a \neq 0$ のとき直交座標をうまく取り直せば, $\mathbb{R}^n$ 上の任意の一次函数は上の (2) の形に表わされることがわかった.

これはある意味当然である. なぜならば $a \neq 0$ の場合の一次函数のグラフは傾いた平面の形になる. その傾きの方向が単位ベクトル $p_1 = a/\,||a||$ で示され, その傾きの大きさは $||a||$ になる. よって, その一次函数が 0 になる点を原点に選び, 座標軸の 1 つが p_1 の方向を向いているような直交座標系を取ればその一次函数は (2) のように表示されるのである.

数学を楽に理解するコツは抽象的だが論理的に厳密な議論と直観的にわかり易いが厳密性が低い議論の両方を自由に行ったり来たりできるように努力することである.

20.4 実二次函数と実二次超曲面の分類

[236] xy 平面上の曲線 $6x^2 - 4xy + 9y^2 = 20$ を図示せよ. □

ヒント: 以下の手続きで曲線を描く.

1. 対称行列 $A = \begin{bmatrix} 6 & -2 \\ -2 & 9 \end{bmatrix}$ の固有値 α, β と対応する単位固有ベクトル u, v を求める.

2. $P = [u\ v]$ と置くと P は直交行列である.

3. ${}^tPAP = \mathrm{diag}(\alpha, \beta)$ となる.

4. 新たな座標系 (x', y') を $\begin{bmatrix} x \\ y \end{bmatrix} = P \begin{bmatrix} x' \\ y' \end{bmatrix} = x'u + y'v$ と定める. xy 平面に x' 軸と y' 軸を描き込む. x' 軸と y' 軸はそれぞれ u と v の方向を向いている.

5. 曲線の式は $\alpha x'^2 + \beta y'^2 = 20$ となる. この曲線を $x'y'$ 平面 $= xy$ 平面に描き込む.

ポイントは $ax^2 + 2bxy + cy^2$ の形の式を見掛けたら, 対称行列 $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ を対角化する直交行列 P を求めて, P を用いて座標変換して, 新たな座標で曲線の描くことである. □

略解: $P = [u\ v] = \dfrac{1}{\sqrt{5}} \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$, $\alpha = 5$, $\beta = 10$ となり, 曲線の式は $x'y'$ 座標では $\dfrac{x'^2}{4} + \dfrac{y'^2}{2} = 1$ の形になる. □

[237] 次の $(x, y) \in \mathbb{R}^2$ の二次函数 $z = f(x, y)$ のグラフの概型を描け:

$$z = f(x, y) = \alpha x^2 + \beta y^2 + \gamma.$$

ただし, (α, β) の符号を $(+,+)$, $(+,-)$, $(-,-)$, $(+,0)$, $(-,0)$, $(0,0)$ の 6 通りに分類してグラフの曲面を描いてみよ. それぞれのグラフと xy 平面 $z = 0$ の交わりはどのような形になるか? □

[238] 直交座標 x, y, z を持つ $\mathbb{R}^3$ における次の二次曲面の概型を描け:

1. $x^2 + y^2 + z^2 = 1$,
2. $x^2 + y^2 - z^2 = 1$,
3. $x^2 + y^2 - z^2 = -1$. □

[239] 直交座標 x, y, z を持つ $\mathbb{R}^3$ における次の二次曲面の概型を描け:

$$\alpha x^2 + \beta y^2 + \gamma z^2 = \delta.$$

ただし, $\alpha\beta\gamma\delta \neq 0$ と仮定する. $(\alpha, \beta, \gamma, \delta)$ の符号を $(+,+,+,+)$, $(+,+,-,+)$, $(+,+,-,-)$ の 3 通りに分類してそれぞれの場合に曲面の概型を描いてみよ. どうしてこの 3 通りだけを考えれば十分なのか説明せよ. 後者の 2 つの場合と $\delta = 0$ の場合の曲面を 1 つの図で描いてみよ. □

ヒント: 長谷川 [長谷川] 248 頁の 15.5 節図 2. □

この節の目標は一般次元の場合に実二次超曲面を分類することである.

2 次元平面上の非退化な実二次曲線は**楕円 (ellipse)** と**双曲線 (hyperbola)** の 2 通りに分類される. 退化した場合として**放物線 (parabola)** が得られる.

3 次元空間内の非退化な実二次曲面は問題 [**239**] でグラフを描いた**楕円面 (ellipsoid)**, **一葉双曲面 (hyperboloid of one sheet)**, **二葉双曲面 (hyperboloid of two sheets)** の 3 通りに分類されてしまう.

これらの事実を n 次元に一般化したい.

n 次元実 Euclid 空間 $\mathbb{R}^n$ 上の**二次函数 (quadratic function)** とは

$$f(x) := \sum_{i,j=1}^{n} a_{ij}x_ix_j + 2\sum_{i=1}^{n} b_ix_i + c$$

の形の函数のことである. ここで $a_{ij}, b_i, c \in$ でかつ $a_{ij} = a_{ji}$. 実二次函数 $f(x)$ が定める $\mathbb{R}^n$ における**二次超曲面 (quadric hypersurface, hypersurface of the second order)** とは方程式 $f(x) = 0$ が定める $\mathbb{R}^n$ の部分集合のことである.

実二次函数 $f(x)$ は実対称行列 $A = [a_{ij}]$ と実縦ベクトル $b = {}^t[b_1 \ \cdots \ b_n]$ を用いて,

$$f(x) = {}^txAx + 2\,{}^tbx + c = \langle x, Ax\rangle + \langle b, x\rangle + c$$

と表わすことができる. 最初の項の ${}^txAx = \langle x, Ax\rangle$ は実対称行列 A が定める実二次形式 $Q_A(x)$ に等しい. よって, A の固有値の全体を $\alpha_1, \ldots, \alpha_n$ とすると, 問題 [**232**] の前半の結果より, ある直交行列 T が存在して

$$Q_A(Ty) = {}^ty\,{}^tTATy = \alpha_1y_1^2 + \cdots + \alpha_ny_n^2$$

となる. そして, ${}^tbTy = {}^t({}^tTb)y$ であるから, $b' = {}^t[b'_1 \ \cdots \ b'_n] = {}^tTb = T^{-1}b$ と置けば,

$$g(y) := f(Ty) = \sum_{i}^{n} \alpha_iy_i^2 + 2\sum_{i=1}^{n} b'_iy_i + c. \tag{0}$$

これは n 次元実 Euclid 空間 $\mathbb{R}^n$ の直交座標系を直交変換することによって, 二次函数の二次の項をすべて $\alpha_iy_i^2$ の形にできることを意味している.

$|A| \neq 0$ (これは $\alpha_i \neq 0$ $(i = 1, \ldots, n)$ と同値) のとき, 二次函数 $f(x)$ と二次超曲面 $f(x) = 0$ は**非退化 (non-degenerate)** であるという. それ以外の場合には**退化している (degenerate)** という.

次のステップは変数 y_i を平行移動して表示をさらに簡単にすることである. これからやる計算は中学三年生または高校一年生のときに習う次の平方完成の繰り返しに過ぎない. $a \neq 0$ とすると,

$$ay^2 + 2by + c = a\left(y + \frac{b}{a}\right)^2 - \frac{b^2}{a} + c.$$

ここで $y = z - b/a$, $\gamma = -b^2/a + c$ と置くと,

$$ay^2 + 2by + c = az^2 + \gamma.$$

座標 y_i の座標 z_i への平行移動も同じように行なわれる. このような計算についてはすでに皆よく理解しているはずなので上の (0) 式の段階で大学で教えるべき議論の本質的な部分は終了していると考えられる.

さて, 平方完成の計算を実行するために次のように仮定する:

$$\alpha_i > 0 \quad (i = 1, \ldots, p),$$

$$\begin{aligned}
&\alpha_i < 0 \quad (i = p+1, \dots, p+q),\\
&\alpha_i = 0 \quad (i = p+q+1, \dots, n),\\
&b'_i \neq 0 \quad (i = p+q+1, \dots, p+q+s),\\
&b'_i = 0 \quad (i = p+q+s+1, \dots, n).
\end{aligned}$$

このとき,

$$\begin{aligned}
g(y) &= \sum_{i=1}^{p+q}(\alpha_i y_i^2 + 2b'_i x_i) + \sum_{i=p+q+1}^{p+q+s} 2b'_i y_i + c\\
&= \sum_{i=1}^{p+q} \alpha_i \left[\left(y_i + \frac{b'_i}{\alpha_i} \right)^2 - \frac{{b'_i}^2}{\alpha_i} \right] + \sum_{i=p+q+1}^{p+q+s} 2b'_i y_i + c\\
&= \sum_{i=1}^{p+q} \alpha_i \left(y_i + \frac{b'_i}{\alpha_i} \right)^2 + \sum_{i=p+q+1}^{p+q+s} 2b'_i y_i + \gamma.
\end{aligned}$$

ここで,

$$\gamma = -\sum_{i=1}^{p+q} \frac{{b'_i}^2}{\alpha_i} + c.$$

$s = 0$ の場合: 座標 y_i を座標 z_i に次のように平行移動する:

$$y_i = \begin{cases} z_i - b'_i/\alpha_i & (i = 1, \dots, p+q),\\ z_i & (i = p+q+1, \dots, n). \end{cases}$$

このとき, $g(y)$ を座標系 $z_1, \dots, z_n$ で見たものを $h(z)$ と書くと,

$$h(z) = \alpha_1 z_1^2 + \cdots + \alpha_{p+q} z_{p+q}^2 + \gamma. \tag{1}$$

($s \leq n-p-q$ なので, もしも A が非退化 ($|A| \neq 0$) ならば $p+q = n$ なので $s = 0$ となることに注意せよ.)

$s > 0$ の場合: 前節の終わりの結果より, $y_{p+q+1}, \dots, y_{p+q+s}$ を直交変換して平行移動すると,

$$\sum_{i=p+q+1}^{p+q+s} 2b'_i y_i + \gamma = \beta z_{p+q+1}$$

が成立するような直交座標 $z_{p+q+1}, \dots, z_{p+q+s}$ が取れる. ここで,

$$\beta := 2\left({b'_{p+q+1}}^2 + \cdots + {b'_{p+q+s}}^2 \right)^{1/2} > 0.$$

残りの新座標を次のように定める:

$$y_i = \begin{cases} z_i - b'_i/\alpha_i & (i = 1, \dots, p+q),\\ z_i & (i = p+q+s+1, \dots, n). \end{cases}$$

これで新たな直交座標系 $z_1, \dots, z_n$ が定まった. このとき, $g(y)$ を座標系 $z_1, \dots, z_n$ で見たものを $h(z)$ と書くと,

$$h(z) = \alpha_1 z_1^2 + \cdots + \alpha_{p+q} z_{p+q}^2 + \beta z_{p+q+1}. \tag{2}$$

以上によって次の定理が証明された.

定理 20.2 実二次函数 $f(x)$ は $x_1, \dots, x_n$ とは別の直交座標系 $z_1, \dots, z_n$ を適切に取ればその座標系において次の (1) または (2) のように表わされる:

$$h(z) = \alpha_1 z_1^2 + \cdots + \alpha_{p+q} z_{p+q}^2 + \gamma, \tag{1}$$
$$h(z) = \alpha_1 z_1^2 + \cdots + \alpha_{p+q} z_{p+q}^2 + \beta z_{p+q+1}. \tag{2}$$

ここで $\alpha_i > 0$ $(i = 1, \dots, p)$, $\alpha_i < 0$ $(i = p+1, \dots, p+q)$, $\gamma \in \mathbb{R}$, $\beta > 0$ である. □

系 20.3 (実二次超曲面の主軸変換) n 次元実 Euclid 空間における任意の実二次超曲面は適当に直交座標系 $z_1, \dots, z_n$ を選べば次の (1) または (2) と表示される:

$$\alpha_1 z_1^2 + \cdots + \alpha_{p+q} z_{p+q}^2 + \gamma = 0, \tag{1}$$
$$\alpha_1 z_1^2 + \cdots + \alpha_{p+q} z_{p+q}^2 + \beta z_{p+q+1} = 0. \tag{2}$$

ここで $\alpha_i > 0$ $(i = 1, \dots, p)$, $\alpha_i < 0$ $(i = p+1, \dots, p+q)$, $\gamma \in \mathbb{R}$, $\beta > 0$ である. このとき, z_1 軸から z_{p+q} 軸までをこの実二次超曲面の**主軸 (principal axis)** と呼ぶ. □

定理 20.2 によれば, 実二次函数 $f(x)$ に対してある直交行列 P とあるベクトル $s \in \mathbb{R}^n$ をうまく取って $f(P(x+s))$ を次の形にできる:

$$f(P(x+s)) = \alpha_1 x_1^2 + \cdots + \alpha_{p+q} x_{p+q}^2 + \gamma, \tag{1}$$
$$f(P(x+s)) = \alpha_1 x_1^2 + \cdots + \alpha_{p+q} x_{p+q}^2 + \beta x_{p+q+1}. \tag{2}$$

ここで $\alpha_i > 0$ $(i = 1, \dots, p)$, $\alpha_i < 0$ $(i = p+1, \dots, p+q)$, $\gamma \in \mathbb{R}$, $\beta > 0$ である. 系 20.3 では

$$\{\, x_i P e_i + P v \mid x_i \in \mathbb{R} \,\} \qquad (i = 1, \dots, p+q)$$

を二次超曲面 $f(x) = 0$ の主軸と呼ぶことにしたのであった. 二次曲面 $f(P(x+s)) = 0$ を二次超曲面を $f(x) = 0$ の主軸変換と呼ぶ.

[240] 主軸変換を求めることによって, $\mathbb{R}^3$ における次の実二次曲面がどのような曲面であるかを調べ, その概形の図を描け:

$$f(v) = 5x^2 + 3y^2 + 3z^2 - 4xy + 4xz + 10yz - 24x + 48y + 12 = 0.$$

ここで $v = {}^t[x, y, z]$ である. □

ヒント: $f(v)$ は次のように表わされる:

$$f(v) = {}^t v A v + 2\,{}^t b v + c.$$

ここで

$$A = \begin{bmatrix} 5 & -2 & 2 \\ -2 & 3 & 5 \\ 2 & 5 & 3 \end{bmatrix}, \quad b = \begin{bmatrix} -12 \\ 24 \\ 0 \end{bmatrix}, \quad c = 12.$$

まず, 直交行列 P で ${}^t PAP$ が対角行列 $D = \mathrm{diag}(\alpha, \beta, \gamma)$ になるものを求める. そのとき $b' = {}^t[b'_1, b'_2, b'_3] = {}^t Pb$ と置くと,

$$f(Pv) = {}^t v D v + 2\,{}^t b P v + c = \alpha x^2 + \beta y^2 + \gamma z^2 + 2b'_1 x + 2b'_2 y + 2b'_3 z + c.$$

この問題では $\alpha, \beta, \gamma \neq 0$ となるので, これはさらに次のように変形される:

$$f(Pv) = \alpha\left(x + \frac{b'_1}{\alpha}\right)^2 + \beta\left(y + \frac{b'_2}{\beta}\right)^2 + \gamma\left(z + \frac{b'_3}{\gamma}\right)^2 + c'.$$

ここで

$$c' = c - \frac{(b'_1)^2}{\alpha} - \frac{(b'_2)^2}{\beta} - \frac{(b'_3)^2}{\gamma}.$$

よって $s = -{}^t[b'_1/\alpha, b'_2/\beta, b'_3/\gamma]$ と置けば

$$f(P(v+s)) = \alpha x^2 + \beta y^2 + \gamma z^2 + c'.$$

ここまで計算できれば二次曲面 $f(P(v+s)) = 0$ のグラフを描くことができる. ただし, $f(P(v+s)) = 0$ のグラフを描くときの x, y, z 軸は $P(v+s)$ と変換する前の座標における主軸の位置に描かなければいけない. □

略解: $D = \mathrm{diag}(6, 8, -3)$ と置き, 直交行列 P を

$$P = \begin{bmatrix} -4 & 0 & 1 \\ 1 & 1 & 2 \\ -1 & 1 & -2 \end{bmatrix} \begin{bmatrix} 3\sqrt{2} & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & 3 \end{bmatrix}^{-1}$$

と定めると, ${}^tPAP = D$ である. このとき,

$$f(Pv) = 6x^2 + 8y^2 - 3z^2 + 24\sqrt{2}x + 24\sqrt{2}y + 24z + 12.$$

よって $s = -{}^t[2\sqrt{2}, 3\sqrt{2}/2, -4]$ と置くと,

$$f(P(v+s)) = 6x^2 + 8y^2 - 3z^2 - 24, \qquad Ps = {}^t[4, -7/2, 1/2].$$

さらに $f(P(v+s)) = 0$ は次と同値である:

$$\left(\frac{x}{2}\right)^2 + \left(\frac{y}{\sqrt{3}}\right)^2 - \left(\frac{z}{2\sqrt{2}}\right)^2 = 1. \quad \square$$

[241] 主軸変換を求めることによって, $\mathbb{R}^3$ における次の実二次曲面がどのような曲面であるかを調べ, その概形の図を描け:

$$\begin{aligned} f(v) = {} & 6x^2 + y^2 + 6z^2 + 2xy + 8xz - 2yz \\ & + (-8 - 5\sqrt{6})x + (2 + 10\sqrt{6})y + (-12 + 5\sqrt{6})z - 26 = 0. \end{aligned}$$

ここで $v = {}^t[x, y, z]$ である. □

ヒント: 問題 **[240]** と同様に計算すると $\gamma = 0$ となってしまい,

$$f(Pv) = \alpha x^2 + \beta y^2 + 2b'_1 x + 2b'_2 y + 2b'_3 z + c$$

の形になる. この問題の場合は $b'_3 > 0$ となる. $s' := -{}^t[b'_1/\alpha, b'_2/\beta, 0]$ と置くと $f(P(v+s'))$ は次の形になる:

$$f(P(v+s')) = \alpha x^2 + \beta y^2 + 2b'_3 z + c'.$$

よって $s = -{}^t[b'_1/\alpha, b'_2/\beta, c'/(2b'_3)]$ と置くと,

$$f(P(v+s)) = \alpha x^2 + \beta y^2 + 2b'_3 z. \quad \square$$

略解: $D = \mathrm{diag}(10, 3, 0)$ と置き, 対称行列 A と直交行列 P を

$$A = \begin{bmatrix} 6 & 1 & 4 \\ 1 & 1 & -1 \\ 4 & -1 & 6 \end{bmatrix}, \quad P = \begin{bmatrix} 1 & -1 & -1 \\ 0 & -1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \sqrt{2} & 0 & 0 \\ 0 & \sqrt{3} & 0 \\ 0 & 0 & \sqrt{6} \end{bmatrix}^{-1}$$

と定めると, ${}^tPAP = D$ が成立するので,

$$f(Pv) = 10x^2 + 3y^2 - 10\sqrt{2}x - 2\sqrt{3}y + 30z - 26.$$

$s' = -{}^t[1/\sqrt{2}, 1/\sqrt{3}, 0]$ と置くと,

$$f(P(v+s')) = 10x^2 + 3y^2 + 30z - 32.$$

よって, $s = s' + {}^t[0, 0, 16/15]$ と置くと,

$$f(P(v+s)) = 10x^2 + 3y^2 + 30z, \qquad Ps = \frac{\sqrt{6}}{90}\,{}^t[-1, 2, 1].$$

$f(P(v+s)) = 0$ と次は同値である:

$$z = -\left(\frac{x}{\sqrt{3}}\right)^2 - \left(\frac{y}{\sqrt{10}}\right)^2. \quad \square$$

20.5 射影空間の中の二次超曲面

[242] n 次元実 Euclid 空間上の実二次函数を次の形で表わすこともできる:

$$f(x') = [{}^tx', 1] \begin{bmatrix} A' & b \\ {}^tb & c \end{bmatrix} \begin{bmatrix} x' \\ 1 \end{bmatrix} \qquad (x' \in \mathbb{R}^n).$$

ここで A' は n 次実対称行列であり, $b \in \mathbb{R}^n$, $c \in \mathbb{R}$ である. $\square$

上の問題中の行列 $A = \begin{bmatrix} A' & b \\ {}^tb & c \end{bmatrix}$ は任意の $n+1$ 次実対称行列に成り得る. よって n 次元実 Euclid 空間上の実二次函数と $n+1$ 次の実対称行列は一対一に対応している. 上の問題のように二次函数を表示すれば $\begin{bmatrix} x' \\ 1 \end{bmatrix}$ の形の $n+1$ 次元ベクトルを考えるだけではなく, 任意の $n+1$ 次元ベクトル $x = \begin{bmatrix} x' \\ x_{n+1} \end{bmatrix} \in \mathbb{R}^{n+1}$ を考える方が理論的により自然であることが見えてくる. この観察は非常に重要である.

一般の場合に射影空間を定義するために K は任意の体であるとする. $K^{n+1} \setminus \{0\}$ の同値関係 $\sim$ 次のように定める:

$$x \sim y \iff \text{ある } c \in K^\times \text{ で } cx = y \text{ となるものが存在する.}$$

ここで $x, y \in K^{n+1} \smallsetminus \{0\}$ である. ベクトル x, y の成分を $x = {}^t[x_1, \ldots, x_{n+1}]$, $y = {}^t[y_1, \ldots, y_{n+1}]$ と書く. $x \sim y$ が成立するとき, x_i たちの比と y_i たちの比が等しいと言い, 次のように書くことにする:

$$x_1 : \cdots : x_{n+1} = y_1 : \cdots : y_{n+1} \iff x \sim y.$$

このやり方で「比」の概念を定義すれば x_i や y_i のどれかが 0 になっても通用する「比」の概念が得られることに注意せよ.

$K^{n+1} \smallsetminus \{0\}$ を同値関係 $\sim$ で割ってできる商空間を n **次元射影空間 (n-dimensional projective space)** と呼び, $\mathbb{P}^n(K)$ と表わす:

$$\mathbb{P}^n(K) := (K^{n+1} \smallsetminus \{0\})/\sim.$$

特に $\mathbb{P}^1(K)$ は射影直線と呼ばれ, $\mathbb{P}^2(K)$ は射影平面と呼ばれる.

ベクトル $x = {}^t[x_1, \ldots, x_{n+1}] \in K^{n+1} \smallsetminus \{0\}$ に対応する射影空間の点 $[x] \in \mathbb{P}^n(K)$ を

$$[x] = [x_1 : \cdots : x_{n+1}]$$

と比の記号を用いて表わす. 任意の $x, y \in K^{n+1} \smallsetminus \{0\}$ に対して,

$$[x] = [y] \iff x \sim y \iff x_1 : \cdots : x_{n+1} = y_1 : \cdots : y_{n+1}$$

であるから, 射影空間の点を比の記号を用いて表わすことは自然である.

[243] (射影直線の胞体分割) 直線 K と射影直線 $\mathbb{P}^1(K)$ の部分集合 $X_1 := \{\, [x_1 : 1] \mid x_1 \in K \,\}$ は対応 $x_1 \leftrightarrow [x_1 : 1]$ によって同一視できる[30]. $\mathbb{P}_1(K)$ の一点からなる部分集合 X_0 を $X_0 = \{[1 : 0]\}$ と定める. このとき $\mathbb{P}^1(K)$ は直線 X_1 と一点 X_0 の交わりのない和に分解される:

$$\mathbb{P}^1(K) = X_1 \sqcup X_0. \quad \square$$

解説: 直観的には, 射影直線のほとんどの部分は直線 K で構成されており, 無限遠にさらにもう一点存在するという風に考える. 実際, $x_1 \neq 0$ ならば $[x_1 : 1] = [1 : x_1^{-1}]$ なので形式的に $x_1 \to \infty$ とすれば $[x_1 : 1] \to [1 : 0]$ となる. $\square$

[244] (射影平面の胞体分割) 射影平面 $\mathbb{P}^2(K)$ の部分集合 X_2, X_1, X_0 を次のように定める:

$$X_2 = \{\, [x_1 : x_2 : 1] \mid x_1, x_2 \in K \,\}, \quad X_1 = \{\, [x_1 : 1 : 0] \mid x_1 \in K \,\}, \quad X_0 = \{[1 : 0 : 0]\}.$$

写像 $K^2 \to X_2$, ${}^t[x_1, x_2] \mapsto [x_1 : x_2 : 1]$ と $K \to X_1$, $x_1 \mapsto [x_1 : 1 : 0]$ は全単射である. 射影平面 $\mathbb{P}^2(K)$ は平面 X_2 と直線 X_1 と一点 X_0 の交わりのない和に分解される:

$$\mathbb{P}^2(K) = X_2 \sqcup X_1 \sqcup X_0. \quad \square$$

解説: $X_1 \sqcup X_0$ と射影直線 $\mathbb{P}^2(K)$ は自然に同一視できる. 直観的には, 射影平面のほとんどの部分は平面 K^2 で構成されており, 無限遠に射影直線 (地平線) が存在すると考える. 実際, $c \neq 0$ ならば $[x_1 : x_2 : 1] = [c^{-1}x_1 : x^{-1}x_2 : c^{-1}]$ なので $x_1 = cy_1$, $x_2 = cy_2$ と置き, 形式的に $c \to \infty$ とすれば $[x_1 : x_2 : 1] \to [y_1 : y_2 : 0]$ となる. $\square$

[30] 写像 $K \to X_1$, $x_1 \mapsto [x_1 : 1]$ が全単射であることを示せ.

[245] (射影空間の胞体分割) 射影空間 $\mathbb{P}^n(K)$ の部分集合 $X_n, X_{n-1}, \ldots, X_1, X_0$ を次のように定める:

$$\begin{aligned}
X_n &= \{\, [x_1 : \cdots : x_{n-1} : x_n : 1] \mid x_1, \cdots, x_{n-1}, x_n \in K \,\}, \\
X_{n-1} &= \{\, [x_1 : \cdots : x_{n-1} : 1 : 0] \mid x_1, \cdots, x_{n-1} \in K \,\}, \\
&\cdots\cdots\cdots \\
X_1 &= \{\, [x_1 : 1 : 0 : \cdots : 0] \mid x_1 \in K \,\}, \\
X_0 &= \{[1 : 0 : 0 : \cdots : 0]\}.
\end{aligned}$$

次の写像は全単射である:

$$K^m \to X_m, \quad {}^t[x_1, \cdots, x_m] \mapsto [x_1 : \cdots : x_m : 1 : 0 : \cdots : 0].$$

射影空間 $\mathbb{P}^n(K)$ は $X_n, X_{n-1}, \ldots, X_1, X_0$ の交わりのない和に分解される:

$$\mathbb{P}^2(K) = X_n \sqcup X_{n-1} \sqcup \cdots \sqcup X_1 \sqcup X_0. \quad \square$$

解説: $X_{n-1} \sqcup \cdots \sqcup X_0$ と $n-1$ 次元射影空間 $\mathbb{P}^{n-1}(K)$ は自然に同一視される. 直観的には, 射影平面のほとんどの部分は n 次元アフィン空間 K^n で構成されており, 無限遠に $n-1$ 次元射影空間が存在すると考える. $c \neq 0$ ならば $[x_1 : \cdots : x_n : 1] = [c^{-1}x_1 : \cdots : x^{-1}x_n : c^{-1}]$ なので $x_i = cy_i$ と置き, 形式的に $c \to \infty$ とすれば $[x_1 : \cdots : x_n : 1] \to [y_1 : \cdots : y_n : 0]$ となる. $\square$

[246] (射影変換とアフィン変換) $T \in GL_{n+1}(K)$ と $x, y \in K^{n+1} \smallsetminus \{0\}$ に対して, $[x] = [y]$ ならば $[Tx] = [Ty]$ が成立する. よって $T \in GL_{n+1}(K)$ の $[x] \in \mathbb{P}^n(K)$ への作用を $T \cdot [x] := [Tx]$ と定めることができる. これを射影空間 $\mathbb{P}^n(K)$ の**射影変換 (projective transformation)** と呼ぶ.

$P \in GL_n(K)$ と $v \in K^n$ が定める K^n の変換 $x' \mapsto Px' + v$ を K^n の**アフィン変換 (affine transformation)** と呼ぶ. すなわち可逆な線形変換 $x' \mapsto Px'$ と平行移動 $x' \mapsto x' + v$ を組み合わせてできる変換をアフィン変換と呼ぶ.

$x' = {}^t[x_1, \ldots, x_n] \in K^n$ に対して $\mathbb{P}^n(K)$ の点 $[x' : 1]$ を $[x' : 1] := [x_1 : \cdots : x_n : 1]$ と定めると, 問題 **[245]** の結果によって $\mathbb{P}^n(K)$ の部分集合 X_n と K^n は次のように同一視される:

$$K^n \cong X_n = \{\, [x' : 1] \mid x' \in K^n \,\}, \quad x' \leftrightarrow [x' : 1].$$

この同一視のもとで $P \in GL_n(K)$ と $v \in K^n$ に対応する K^n のアフィン変換は次の $T \in GL_{n+1}(K)$ で表現される:

$$T = \begin{bmatrix} P & v \\ 0 & 1 \end{bmatrix}. \quad \square$$

ヒント 1: 次の公式が成立する:

$$\begin{bmatrix} P & v \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x' \\ 1 \end{bmatrix} = \begin{bmatrix} Px' + v \\ 1 \end{bmatrix}. \quad \square$$

ヒント 2: $T = [t_{ij}]_{i,j=1}^{n+1} \in GL_{n+1}(K)$ と $x = {}^t[x_1, \ldots, x_{n+1}] \in K^{n+1}$ に対して, もしも $\sum_{j=1}^{n+1} t_{n+1,j}x_j \neq 0$ ならば

$$\begin{aligned} T[x_1 : \cdots : x_n : x_{n+1}] &= \left[\sum_{j=1}^{n+1} t_{1j}x_j : \cdots : \sum_{j=1}^{n+1} t_{nj}x_j : \sum_{j=1}^{n+1} t_{n+1,j}x_j \right] \\ &= \left[\frac{\sum_{j=1}^{n+1} t_{1j}x_j}{\sum_{j=1}^{n+1} t_{n+1,j}x_j} : \cdots : \frac{\sum_{j=1}^{n+1} t_{nj}x_j}{\sum_{j=1}^{n+1} t_{n+1,j}x_j} : 1 \right]. \end{aligned}$$

この一般的な公式で $t_{ij} = p_{ij}$ $(i, j = 1, \ldots, n)$, $t_{i,n+1} = v_i$ $(i = 1, \ldots, n)$, $t_{n+1,j} = 0$ $(j = 1, \ldots, n)$, $t_{n+1,n+1} = 1$, $x_{n+1} = 1$ と置くと $\sum_{j=1}^{n+1} t_{n+1,j}x_j = 1 \neq 0$ であるから,

$$T[x_1 : \cdots : x_n : 1] = \left[\sum_{j=1}^{n} p_{1j}x_j + v_1 : \cdots : \sum_{j=1}^{n} p_{nj}x_j + v_n : 1 \right]. \quad \square$$

さてここで問題 [**242**] の結果に戻ろう. 問題 [**242**] の結果によれば $\mathbb{R}^n$ 上の実二次函数 $f(x')$ は $n+1$ 次の実対称行列 A によって次のように表わされる:

$$f(x') = {}^t xAx = [{}^t x', 1] \begin{bmatrix} A' & b \\ {}^t b & c \end{bmatrix} \begin{bmatrix} x' \\ 1 \end{bmatrix} \qquad (x = {}^t[x', 1] \in \mathbb{R}^{n+1},\ x' \in \mathbb{R}^n).$$

問題 [**246**] の結果より, n 次の直交行列 P と n 次元ベクトル $v \in \mathbb{R}^n$ に対応するアフィン変換は

$$T = \begin{bmatrix} P & v \\ 0 & 1 \end{bmatrix} \in GL_{n+1}(\mathbb{R})$$

に対応する射影変換と同一視できる. 実二次函数の標準形 (定理 20.2) もしくは実二次超曲面の主軸変換 (系 20.3) に関する結果は「上の特別な形の射影変換 T による $A \mapsto {}^t TAT$ という変換で $n+1$ 次の実対称行列 A の形をできるだけ簡単にせよ」という問題に解答を与えていると考えられる.

それでは射影変換 T に制限を付けずに実二次超曲面の分類を考えるとどうなるであろうか. 注意しなければいけないことは一般の射影変換は $\mathbb{R}^n$ と同一視されている $X_n \subset \mathbb{P}^n(\mathbb{R})$ を保つとは限らないことである. 有限の位置にあった点が射影変換で無限遠に移ることがありえる.

しかし, そこまで変換の自由度を広げるメリットは大きい. なぜならばそうすることによって射影空間内の二次超曲面の分類が二次形式の分類に帰着してしまうことになるからである.

0 でない $n+1$ 次の実対称行列 A に対して $\mathbb{R}^{n+1}$ 上の二次函数 f を次のように定める:

$$f(x) = {}^t xAx \qquad (x \in \mathbb{R}^{n+1}).$$

このとき $x, y \in \mathbb{R}^{n+1} \setminus \{0\}$ に対して, $[x] = [y]$ ならばある $c \in \mathbb{R}^\times$ が存在して $cx = y$ となるので $f(y) = f(cx) = c^2 f(x)$ となり, $f(x) = 0$ と $f(y) = 0$ は同値になる. f の定める実射影空間 $\mathbb{P}^n(\mathbb{R})$ における**二次超曲面** V を次のように定義する:

$$V := \{\, [x] \in \mathbb{P}^n(\mathbb{R}) \mid f(x) = 0 \,\}.$$

射影変換で互いに移り合う二次超曲面は互いに同値であると言うことにする. 同値な実二次射影曲面の中からできるだけ簡単な表示を持つものを見付けるのが問題である.

[247] (実射影空間における実二次超曲面の分類) n 次元実射影空間 $\mathbb{P}^n(\mathbb{R})$ における実二次超曲面 V は射影変換によって次の表示を持つ実二次超曲面に移る:

$$x_1^2 + \cdots + x_p^2 = x_{p+1}^1 + \cdots + x_{p+q}^2.$$

しかも (p, q) は p と q の交換の違いを除いて V から一意に定まる. □

ヒント: これは定理 20.1 の言い換えに過ぎない. □

[248] (実射影平面上の実二次曲線の分類) 実射影平面 $\mathbb{P}^2(\mathbb{R})$ 上の実二次曲線 V は次の 3 通りのどれかに同値である:

$$x_1^2 + x_2^2 + x_3^2 = 0, \tag{1}$$
$$x_1^2 + x_2^2 = x_3^2, \tag{2}$$
$$x_1^2 + x_2^2 = 0, \tag{3}$$
$$x_1^2 = x_2^2, \tag{4}$$
$$x_1^2 = 0. \tag{5}$$

それぞれの方程式が定める実射影平面の部分集合は以下のようになる:

- (1) が定める実射影平面の部分集合は空集合になる.
- (2) の曲線は実平面 $\mathbb{R}^2$ と同一視される $X_2 = \{\, [x : y : 1] \mid x, y \in \mathbb{R} \,\}$ に含まれ, $x^2 + y^2 = 1$ と表わされる.
- (3) が定める実射影平面の部分集合は $[0 : 0 : 1]$ の一点になる.
- (4) は $x_1 \pm x_2$ のそれぞれを x_1, x_2 と置く変数変換によって $x_1 x_2 = 0$ に変換される. その方程式が定める実射影平面の部分集合は二つの射影直線 $\{[0 : x_2 : x_3]\}$ (y 軸) と $\{[x_1 : 0 : x_3]\}$ (x 軸) の和集合になる.
- (5) の定める実射影平面の部分集合は射影直線 $\{[0 : x_2 : x_3]\}$ (y 軸) になる. ($x_1^2 = 0$ は重根を持つので二重の射影直線であると考えられる.) □

解説: 射影ではないただの実平面上の非退化な二次曲線は楕円, 放物線, 双曲線と 3 通りに分類された. 上の問題の結果より, 正則な 3 次実対称行列の定める空集合でない実射影平面上の実二次曲線は円周 $x^2 + y^2 = 1$ と同値であることがわかる. ただの平面から射影平面に移り, さらにアフィン変換を射影変換に拡張すればこのように非退化な実二次曲線は本質的に一種類しか存在しないという簡明な結果が得られるのである. □

[249] (実射影空間内の実二次曲面の分類) 問題 **[248]** と同様にして実射影空間内の実二次曲面を分類せよ. □

ヒント: 実射影平面内の実二次曲線の場合よりも 3 通り増えて 8 通りに分類される. □

参考: さて, 上においては実数体上の二次超曲面を扱って来た. 複素数体のような代数閉体上の二次超曲面の分類はさらに易しくなる. 一般の体の場合も二次超曲面の分類は二次形式の分類に帰着する. このように二次超曲面については非常によくわかっていると考えて良い.

それではその次に扱うべき対象は何であろうか? それは射影平面上の三次曲線であろう. そこで出会う数学的対象が**楕円曲線 (elliptic curve)** である. 楕円曲線とは

$$y^2 = x^3 + ax + b$$

の形の方程式で定義される平面三次曲線のことである. 実は適切な設定のもとで射影平面上の三次曲線はどれもこの形の曲線に同値であることを証明できる. 上の方程式を平面三次曲線の **Weierstrass の標準形**もしくは **Weierstrass 方程式**と呼ぶ. 複素楕円曲線は位相的にトーラスの形をしている. 楕円曲線に関しては多くの入門書が発行されている. たとえばシルヴァーマン&テイト [ST] やキャッセルズ [C] を見よ. 複素楕円曲線と表裏一体の楕円函数論に関しては竹内 [Tkc] や梅村 [U] を見よ. □

20.6 定符号性と半定符号性

$\mathbb{R}^n$ 上の実二次形式 Q が**正値半定符号 (positive semidefinite)** であるとは任意の $x \in \mathbb{R}^n$ に対して $Q(x) \geq 0$ が成立することである. そのとき $Q \geq 0$ と書く. Q が**正値定符号 (positive semidefinite)** であるとは正値半定符号でかつ $Q(x) = 0$ が成立するための必要十分条件が $x = 0$ であることである. そのとき, $Q > 0$ と書く. さらに, 不等号の向きを逆にすることによって, **負値半定符号 (negative semidefinite)** であることと**負値定符号 (negativedefinite)** であることを定義する[31]. Q に対応する実対称行列 A にも同じ形容詞を適用する. たとえば $A \geq 0$ であるための必要十分条件は A の固有値がすべて 0 以上であることである.

[250] Q は $\mathbb{R}^n$ 上の実二次形式であり, (p, q) はその符号数であるとする. このとき,

1. Q が positive semidefinite $\iff$ $q = 0$.
2. Q が negative semidefinite $\iff$ $p = 0$.
3. Q が positive definite $\iff$ $(p, q) = (n, 0)$.
4. Q が negative definite $\iff$ $(p, q) = (0, n)$. □

[251] A は実対称行列とし, P は実正則行列とし, 実対称行列 B を $B = {}^tPAP$ と定める. このとき, A と B の固有値の集合は一般には異なるが, 正の固有値の個数と負の固有値の個数は互いに等しくなることを説明せよ. □

ヒント: 正の固有値の個数と負の固有値の個数が互いに等しくなることは Sylvester の慣性法則と同値. 固有値の集合が異なる場合があることは P として単位行列でない対角行列を取ればわかる. □

[252] A, B は n 次実対称行列であるとし, $a \in \mathbb{R}$ とする. このとき, 実二次形式の和とスカラー倍が

$$(Q_A + Q_B)(x) = Q_A(x) + Q_B(x) = Q_{A+B}(x), \qquad (aQ_A)(x) = a(Q_A(x)) = Q_{aA}(x)$$

と定義される. n 次実対称行列全体の集合 $\mathrm{Sym}_n(\mathbb{R})$ は $n(n+1)/2$ 次元の実ベクトル空間をなし, $\mathbb{R}^n$ 上の実二次形式全体の集合はそれに同型な実ベクトル空間をなす. □

[31]「正値半定符号」や「正値定符号」のような言い方はあまり聞き慣れないので演習の時間には「ポジティヴ・セマイデフィニト」「ポジティヴ・デフィニト」と言う場合が多いと思われる.

[253] A, B は n 次実対称行列であるとし, $a \in \mathbb{R}$ とする.

1. $A \geq 0, B \geq 0 \implies A + B \geq 0.$
2. $A > 0, B \geq 0 \implies A + B > 0.$
3. $A \geq 0, a \geq 0 \implies aA \geq 0.$
4. $A > 0, a > 0 \implies aA > 0.$ □

20.7 小行列式に関する準備

与えられた n 次実対称行列 A もしくはそれに対応する実二次形式 Q_A の符号数 (p, q) を調べる方法を演習問題の形でまとめておく. 目標は問題 **[269]** の結果の証明の概略を与えることである. そのためには小行列式に関する幾つかの結果が必要になる.

この節のアイデアは単純である. 行列式の余因子展開のような公式を行列を用いて書き直せば行列の等式が色々得られるが, そられの等式の両辺の行列式を取れば余因子に関する公式が色々得られる. これだけである. (問題 **[257]** のヒントを参照せよ.)

一般的な定義をするために A は任意の n 次正方行列であるとする. 以下, $\{1, \ldots, n\}$ の k 個の元を持つ部分集合 $I = \{i_1 < \cdots < i_k\}$ に対して,

$$|I| = k, \qquad \ell(I) = (i_1 - 1) + \cdots + (i_k - k)$$

と置き, I の補集合を I^c と書くことにする. たとえば $n = 5$, $I = \{1, 4, 5\}$ のとき $|I| = 3$, $\ell(I) = 4$, $I^c = \{2, 3\}$.

[254] $I = \{i_1 < \cdots < i_k\}$ の補集合を $I^c = \{j_1 < \cdots < j_{n-k}\}$ と表わすと,

$$\operatorname{sgn} \begin{pmatrix} 1 \cdots k & k+1 \cdots & n \\ i_1 \cdots i_k & j_1 & \cdots j_{n-k} \end{pmatrix} = (-1)^{\ell(I)}.$$

ここで左辺は $(1, \cdots, n)$ を $(i_1, \ldots, i_k, j_1, \ldots, j_{n-k})$ に移す置換の signature である. □

$\{1, \ldots, n\}$ の k 個の元を持つ部分集合 $I = \{i_1 < \cdots < i_k\}$, $J = \{j_1 < \cdots < j_k\}$ に対して, 行列 A に対して行列 A_{IJ} を

$$A_{IJ} = \begin{bmatrix} a_{i_1 j_1} & \cdots & a_{i_1 j_k} \\ \vdots & & \vdots \\ a_{i_k j_1} & \cdots & a_{i_k j_k} \end{bmatrix}$$

と定義し, これの行列式を (I, J) **小行列式 (minor)** と呼び,

$$a_{IJ} = |A_{IJ}| = \begin{vmatrix} a_{i_1 j_1} & \cdots & a_{i_1 j_k} \\ \vdots & & \vdots \\ a_{i_k j_1} & \cdots & a_{i_k j_k} \end{vmatrix}$$

と表わす. $I = J$ のとき $a_{II} = |A_{II}|$ を r 次の**主小行列式 (principal minor)** と呼び a_I と表わす. A_{II} も A_I と書くことにする.

さらに, 行列 A の (I,J) **余因子 (cofactor)** $\tilde{a}_{IJ}$ を次のように定める:

$$\tilde{a}_{IJ} = (-1)^{\ell(I)+\ell(J)} a_{I^cJ^c} = (-1)^{\ell(I)+\ell(J)} |A_{I^cJ^c}|.$$

$I=\{i\}$, $J=\{j\}$ のとき, $a_{IJ}=a_{ij}$ であり, $\tilde{a}_{ij} := \tilde{a}_{IJ}$ はすでに習ったはずの (i,j) 余因子に一致している.

各 k に対して, k 次の小行列式 $a_{IJ}=|A_{IJ}|$ ($|I|=|J|=k$) の全体で構成された正方行列を $A^{(k)}$ と表わし, k 次の余因子 $\tilde{a}_{IJ}=(-1)^{\ell(I)+\ell(J)}|A_{I^cJ^c}|$ ($|I|=|J|=k$) の全体で構成された正方行列を $\Delta_k(A)$ と表わすことにする:

$$A^{(k)} = \big[a_{IJ}\big]_{|I|=|J|=k} = \big[|A_{IJ}|\big]_{|I|=|J|=k},$$
$$\Delta_k(A) = \big[\tilde{a}_{IJ}\big]_{|I|=|J|=k} = \big[(-1)^{\ell(I)+\ell(J)}|A_{I^cJ^c}|\big]_{|I|=|J|=k}.$$

$A^{(k)}$, $\Delta_k(A)$ は共に $\binom{n}{k}$ 次の正方行列になる. たとえば $A^{(1)}=A$, $\Delta_1(A)=[\tilde{a}_{ij}]_{i,j=1}^n$ である. 簡単のため $\Delta(A)=\Delta_1(A)$ と置く.

[255] (Laplace 展開) I, K は $\{1,\dots,n\}$ の部分集合であり, $|I|=|K|=k$ を満たしていると仮定する. このとき,

$$\sum_{|J|=k} a_{IJ}\tilde{a}_{KJ} = \sum_{|J|=k} \tilde{a}_{JI}a_{JK} = |A|\delta_{IK}.$$

ここで和は $|J|=k$ を満たす $\{1,\dots,n\}$ の部分集合 J の全体を走る. その和は $\binom{n}{k}$ 個の項の和になる. 右辺の δ_{IK} は Kronecker's delta であり $I=K$ のときにのみ 1 になり, それ以外の場合には 0 になる. この結果を行列で書き直すと,

$$A^{(k)}\ {}^t\Delta_k(A) = {}^t\Delta_k(A)\ A^{(k)} = |A|E.$$

ここで E は $\binom{n}{k}$ 次の単位行列である. □

ヒント: 行列式の定義に戻れば証明できる. すでに習ったはずの $k=1$ の場合の Laplace 展開を繰り返し用いて証明することもできる. (高木 [Tkg1] 第 8 章第 52 節の 250–255 頁に詳しい説明がある.) 外積代数を用いた証明の方針が佐武 [St] 第 V 章第 4 節 225 頁の問 6 (略解が 313 頁にある) にある. (横沼 [Ykn] 92–96 頁に詳しい説明がある.) □

$k>1$ の一般の Laplace 展開はこの節では使用しない. $k=1$ の場合の結果を忘れている人は復習して欲しい. 次の問題の Jacobi の公式は後で使用される[32].

[256] 次の等式が成立することを直接確かめよ:

$$\begin{vmatrix} a_{11} & \cdots & a_{14} \\ \vdots & & \vdots \\ a_{41} & \cdots & a_{44} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}\begin{vmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{vmatrix} - \begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix}\begin{vmatrix} a_{23} & a_{24} \\ a_{43} & a_{44} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} \\ a_{41} & a_{42} \end{vmatrix}\begin{vmatrix} a_{23} & a_{24} \\ a_{33} & a_{34} \end{vmatrix}$$
$$+ \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}\begin{vmatrix} a_{13} & a_{14} \\ a_{43} & a_{44} \end{vmatrix} - \begin{vmatrix} a_{21} & a_{22} \\ a_{41} & a_{42} \end{vmatrix}\begin{vmatrix} a_{13} & a_{14} \\ a_{33} & a_{34} \end{vmatrix} + \begin{vmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{vmatrix}\begin{vmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{vmatrix}. \quad \square$$

[32] Jacobi の公式の解説は佐武 [St] 第 II 章第 5 節例 2 (66-67 頁) にある. 高木 [Tkg1] 定理 9.5 (295 頁) の証明に登場する最初の式は Jacobi の公式の特別な場合である.

ヒント: $n=4$, $k=2$ の場合の Laplace 展開だが直接計算で確かめなければいけない. 左辺の行列式の第 1 列と第 2 列について余因子展開してそれが右辺に等しくなることを確かめよ. □

[257] (Jacobi の公式) 余因子と主小行列式に関して次が成立する:

$$\begin{vmatrix} \tilde{a}_{k+1,k+1} & \cdots & \tilde{a}_{n,k+1} \\ \vdots & & \vdots \\ \tilde{a}_{k+1,n} & \cdots & \tilde{a}_{n,n} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kk} \end{vmatrix} |A|$$

ここで $\tilde{a}_{ij}$ は A の (i,j) 余因子である. 特に $k=n-2$ のとき,

$$\tilde{a}_{n-1,n-1}\tilde{a}_{n,n} - \tilde{a}_{n,n-1}\tilde{a}_{n-1,n} = \begin{vmatrix} a_{11} & \cdots & a_{1,n-2} \\ \vdots & & \vdots \\ a_{n-2,1} & \cdots & a_{n-2,n-2} \end{vmatrix} |A|^{n-k-1}. \quad \square$$

注意: $k=0$ のとき右辺に表われる空な行列式は 1 に等しいと約束しておく.

ヒント: $\sum_{\nu=1}^{n} a_{i\nu}\tilde{a}_{j\nu} = |A|\delta_{ij}$ より,

$$A \begin{bmatrix} 1 & & 0 & \tilde{a}_{k+1,1} & \cdots & \tilde{a}_{n,1} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & \tilde{a}_{k+1,k} & \cdots & \tilde{a}_{n,k} \\ 0 & \cdots & 0 & \tilde{a}_{k+1,k+1} & \cdots & \tilde{a}_{n,k+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \tilde{a}_{k+1,n} & \cdots & \tilde{a}_{n,n} \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,k} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{k,1} & \cdots & a_{k,k} & 0 & \cdots & 0 \\ a_{k+1,1} & \cdots & a_{k+1,k} & |A| & & 0 \\ \vdots & & \vdots & & \ddots & \\ a_{n,1} & \cdots & a_{n,k} & 0 & & |A| \end{bmatrix}$$

この等式の両辺の行列式を取る. □

[258] 上の問題 **[257]** の結果は Laplace 展開 **[255]** の最も簡単な場合 $(k=1)$ の場合の結果から導かれた. 一般の Laplace 展開を用いて問題 **[257]** の結果を一般化せよ. □

20.8 主小行列式を用いた符号数の計算の仕方

[259] A は n 次実対称行列であるとし, I は $\{1,\ldots,n\}$ の空でない任意の部分集合であるとする. このとき,

1. $A>0 \implies a_I = |A_I| > 0$.
2. $A \geq 0 \implies a_I = |A_I| \geq 0$.

ここで $a_I = |A_I|$ は I に対応する主小行列式である. □

ヒント: $x_i = 0$ $(i \notin I)$ を満たす x に対する $Q_A(x)$ の符号について考えてみよ. すると, $A_I = A_{II}$ がすべて positive (semi-)definite であることがわかる. □

[260] A は n 次実対称行列であるとし, $I_k = \{1,\ldots,k\}$ と置く. このとき,

$$A>0 \iff a_{I_k} = |A_{I_k}| > 0 \quad (1 \leq k \leq n).$$

ここで $a_{I_k} = |A_{I_k}|$ は I_k に対応する主小行列式である. □

ヒント: $\Longrightarrow$ の向きは問題 [**259**] の特別な場合である. 逆は n に関する数学的帰納法で証明する. $n=1$ のとき逆が成立することは明らか. $n-1$ まで逆が成立していると仮定する. そのとき A の左上にある $n-1$ 次正方行列 $A_{\{1,\dots,n-1\}}$ を B と書くと, $B>0$ が成立している. 特に B は正則行列になるので, A は次のように表わされる[33]:

$$A=\begin{bmatrix} B & a \\ {}^t a & a_{nn} \end{bmatrix} = \begin{bmatrix} E_{n-1} & 0 \\ {}^t aB^{-1} & 1 \end{bmatrix} \begin{bmatrix} B & 0 \\ 0 & a_{nn}-{}^t aB^{-1}a \end{bmatrix} \begin{bmatrix} E_{n-1} & B^{-1}a \\ 0 & 1 \end{bmatrix}.$$

この等式の行列式を取ると $|A|=|B|(a_{nn}-{}^t aB^{-1}a)$. $|A|=|A_{I_n}|>0$, $|B|>0$ より $a_{nn}-{}^t aB^{-1}a>0$. よって $\begin{bmatrix} B & 0 \\ 0 & a_{nn}-{}^t aB^{-1}a \end{bmatrix}>0$ であるが, この行列に対応する二次形式と A に対応する二次形式は同値なので $A>0$. □

[**261**] 問題 [**260**] の設定のもとで

$$A\geq 0 \implies a_{I_k}=|A_{I_k}|\geq 0 \quad (1\leq k\leq n).$$

は成立するが, 逆は成立しない. □

ヒント: $A=\mathrm{diag}(0,-1)$ は逆の反例になっている. 左上部分に 0 が詰まった実対称行列はすべて反例になる. □

[**262**] A は n 次対称行列であるとし, $r=\mathrm{rank}\,A$ と置く. このとき, A の r 次の主小行列式で 0 でないものが存在する. さらに A が実行列ならばそれらの主小行列式はすべて同じ符号を持つ. □

ヒント: この結果は高木 [Tkg1] 第 9 章第 61 節の定理 9.4 (293 頁) にある. □

略解: $r=\mathrm{rank}\,A$ ならばある $I=\{i_1,\dots,i_r\}$ と $J=\{j_1,\dots,j_r\}$ で I, J に対応する r 次の小行列式 $|A_{IJ}|=\det[a_{i_\mu i_\nu}]_{\mu,\nu=1}^r$ が 0 にならないものが存在する[34]. A の中の n 本の列ベクトルの全体を $a_1,\dots,a_n$ と書く. $a_1,\dots,a_n$ の張る r 次元のベクトル空間を V と書く. このとき, $a_{j_1},\dots,a_{j_r}$ は V の基底になり, A が対称なので $a_{i_1},\dots,a_{i_r}$ も V の基底になる. よって, r 次の正則行列 C で $[a_{i_1}\ \dots\ a_{i_r}]C=[a_{j_1}\ \dots\ a_{j_r}]$ をみたすものが存在する. この等式の両辺の行列の第 $i_1,\dots,i_r$ 行の部分を抜き出すと $A_{II}C=A_{IJ}$ となる. この両辺の行列式を取ると $|A_{II}||C(I,J)|=|A_{IJ}|$ であり, $|A_{IJ}|\neq 0$ なので $|A_{II}|\neq 0$ である. これで前半の証明が終わった.

後半を証明するために, $|A_{II}|\neq 0$, $|A_{JJ}|\neq 0$ と仮定する. このとき, 上と同様にして, r 次の正則行列 C で $[a_{i_1}\ \dots\ a_{i_r}]C=[a_{j_1}\ \dots\ a_{j_r}]$ をみたすものが存在することがわかる. この等式の両辺の行列の第 $i_1,\dots,i_r$ 行の部分を抜き出すと $A_{II}C=A_{IJ}$ となり, 第 $j_1,\dots,j_r$ 行の部分を抜き出すと $A_{JI}C=A_{JJ}$ となる. A は対称なので $|A_{JI}|=|A_{IJ}|$ となるから $|A_{II}||C|^2=|A_{JJ}|$ である. よって $|A_{II}|$ と $|A_{JJ}|$ の符号は等しい. □

[**263**] 問題 [**262**] によれば, A が n 次対称行列であり, $r=\mathrm{rank}\,A$ ならば A の r 次の主小行列式で 0 でないものが存在するのであった. しかし, $r-1$ 次の主小行列式はすべて 0 になってしまう場合があることを示せ. □

[33] 二次形式に関する議論でこのテクニックは頻繁に利用される.

[34] すでに習ったと思うが, 復習したい人は佐武 [St] 第 III 章定理 2 (90 頁) と 106 頁の説明を参照せよ.

ヒント: 右上から左下への対角線上の成分のみが 0 でない対称行列を考えてみよ. □

[264] A は n 次対称行列とし, $r = \operatorname{rank} A$, $I = \{i_1 < \cdots < i_r\}$, $|A_I| \neq 0$ であると仮定する. n 次対称行列 A' を

$$A' = \begin{bmatrix} A_I & 0 \\ 0 & 0 \end{bmatrix}$$

と定めると, Q_A と $Q_{A'}$ は同値になる. □

解説: この問題の結果と上の問題 **[262]** の結果を合わせれば rank が r の二次形式の性質は $n = r$ の場合の二次形式の性質を調べる問題に帰着できることがわかる.

ヒント: $I = \{1, \ldots, r\}$ と仮定して一般性は失われない. このとき, A_I^{-1} が存在することより,

$$A = \begin{bmatrix} A_I & B \\ {}^tB & C \end{bmatrix} = \begin{bmatrix} E_r & 0 \\ {}^tBA_I^{-1} & E_{n-r} \end{bmatrix} \begin{bmatrix} A_I & 0 \\ 0 & C - {}^tBA_I^{-1}B \end{bmatrix} \begin{bmatrix} E_r & A_I^{-1}B \\ 0 & E_{n-r} \end{bmatrix}$$

もしも $X := C - {}^tBA_I^{-1}B \neq 0$ ならば $\operatorname{rank} A = \operatorname{rank} A_I + \operatorname{rank} X > r$ となってしまうので矛盾する. よって $X = 0$ である. □

[265] A は n 次実対称行列であり, $|A_{IJ}|$ は A の $n-1$ 次の principal ではない[35]任意の小行列式であり, $|A_{KK}|$ は A_{IJ} の小行列式になっているような A の唯一の $n-2$ 次主小行列式であるとする ($K = I \cap J$). このとき, $|A_{II}| = 0$ ならば $|A_{KK}||A| \leq 0$ である. □

ヒント: Jacobi の公式 **[257]** の $k = n-2$ の場合より, 任意の n 次正方行列 A に対して,

$$|A_{II}||A_{JJ}| - |A_{IJ}||A_{JI}| = |A_{KK}||A|. \qquad (*)$$

A が実対称なので $|A_{JI}| = |A_{IJ}|$ であり, $|A_{II}| = 0$ ならば $|A_{KK}||A| = -|A_{IJ}|^2 \leq 0$. □

[266] n 次対称行列 A の $n-1$ 次と $n-2$ 次の主小行列式がすべて 0 ならば任意の $n-1$ 次小行列式も 0 になる. よって, $|A| \neq 0$ ならば A の $n-1$ 次と $n-2$ 次の主小行列式の中には 0 でないものが存在する. □

ヒント: Jacobi の公式 **[257]** の $k = n-2$ の場合を書き直すことによって得られた上の公式 $(*)$ を使う. A が対称行列ならば $|A_{JI}| = |A_{IJ}|$ であるから, A の $n-1$ 次と $n-2$ 次の主小行列式がすべて 0 ならば $|A_{II}| = |A_{JJ}| = |A_{KK}| = 0$ なので $(*)$ より $|A_{JI}| = |A_{IJ}| = 0$. □

[267] A は n 次対称行列であるとし, $r = \operatorname{rank} A$ と置く. このとき, $\{1, \ldots, n\}$ の部分集合の列

$$I_r \supset I_{r-1} \supset \cdots \supset I_1 \supset I_0 = \emptyset, \qquad |I_\nu| = \nu$$

で以下の条件を満たすものが存在する:

(a) $|A_{I_r}| \neq 0$

[35] $I \neq J$ であるということ

(b) 対応する主小行列式の列

$$0 \neq |A_{I_r}|,\ |A_{I_{r-1}}|,\ \cdots,\ |A_{I_1}|,\ |A_{I_0}| = 1$$

の中の隣り合う $|A_{I_{\nu+1}}|$ と $|A_{I_\nu}|$ は同時に 0 にならない.

(c) $|A_{I_\nu}| = 0$ ならば $A_{I_{\nu+1}}$ の ν 次の主小行列式はすべて 0 である.

さらに A が実行列で $|A_{I_\nu}| = 0$ ならばその両隣の $|A_{I_{\nu-1}}|$ と $|A_{I_{\nu+1}}|$ は反対の符号を持つ. □

ヒント: この結果は高木 [Tkg1] 第 9 章第 61 節の定理 9.5 (295 頁) にある. 問題 [**265**] の結果より, 前半が証明されれば実行列の場合に関する後半も証明される. 前半の証明. 問題 [**262**] の結果より, ある $I_r \subset \{1, \ldots, n\}$ で $|I_r| = r$ かつ $|A_{I_r}| \neq 0$ をみたすものが存在する. 列 $I_r \supset \cdots \supset I_k$ で $|I_\nu| = \nu$ $(k = k, k+1, \ldots, r)$ かつ $|A_{I_k}| \neq 0$ をみたすものが選ばれたと仮定する. ($k = r$ のときこの仮定はすでに成立している.) 問題 [**266**] の結果を対称行列 A_{I_k} に適用すれば, A_{I_k} の $k-1$ 次と $k-2$ 次の主小行列式の中に 0 でないものが存在する. A_{I_k} の $k-1$ 次の主小行列式の中に 0 でないものが存在する場合にはその主小行列式が $|A_{I_{k-1}}|$ に等しくなるように I_{k-1} を選ぶ. もしも A_{I_k} の $k-1$ 次主小行列式のすべてが 0 ならば 0 でならない $k-2$ 次小行列式の 1 つに $|A_{I_{k-2}}|$ が等しくなるように I_{k-2} を選び, $I_k \supset I_{k-1} \supset I_{k-2}$ かつ $|I_{k-1} = k-1$ をみたすような I_{k-1} を任意に取る. このような手続きで順次選ばれた $I_r \supset \cdots \supset I_1$ は前半の主張の条件をみたしている. □

[**268**] 問題 [**267**] の主小行列式の列を次の対称行列に対して 1 つずつ構成せよ:

$$(1)\quad A = \begin{bmatrix} a & & & & 0 \\ & 0 & & & \\ & & b & & \\ & & & 0 & \\ 0 & & & & c \end{bmatrix}, \qquad (2) B = \begin{bmatrix} 0 & & & & a \\ & & & b & \\ & & c & & \\ & b & & & \\ a & & & & 0 \end{bmatrix}$$

ここで, $a, b, c \in \mathbb{R}$, $abc \neq 0$. □

略解: A については

$$|A_{I_3}| = |\operatorname{diag}(a, b, c)| = abc, \quad |A_{I_2}| = |\operatorname{diag}(a, b)| = bc, \quad |A_{I_1}| = |\operatorname{diag}(a)| = a.$$

B については

$$|A_{I_5}| = |B| = a^2 b^2 c, \quad |A_{I_4}| = 0, \quad |A_{I_3}| = -b^2 c \quad |A_{I_2}| = 0, \quad |A_{I_1}| = c. \quad \square$$

次の結果は主小行列の情報から実二次形式の符号を決定する方法を与えている. (佐武 [St] 164 頁では結論だけが紹介されており, 高木 [Tkg1] 301–303 頁では詳しく解説されている.)

[**269**] A は n 次実対称行列とし, 対応する実二次形式 Q_A の符号数は (p, q) であるとする. 問題 [**267**] の主小行列式の列を取る $(r = p + q)$:

$$0 \neq |A_{I_r}|,\ |A_{I_{r-1}}|,\ \cdots,\ |A_{I_1}|,\ |A_{I_0}| = 1.$$

この列における符号変化の個数が q に等しい. □

ヒント: $I_\nu = \{1, \ldots, \nu\}$ と仮定しても一般性が失われない. 以下, 簡単のため $A_\nu = A_{I_\nu}$ と置く. 問題 **[264]** より $n = r$ の場合に帰着する. それを n に関する数学的帰納法で証明する. □

略解: $|A_{n-1}| \neq 0$ の場合. A_{n-1}^{-1} が存在するので,

$$A_n = A = \begin{bmatrix} A_{n-1} & a \\ {}^t a & a_{nn} \end{bmatrix} = \begin{bmatrix} E_{n-1} & 0 \\ {}^t a A_{n-1}^{-1} & 1 \end{bmatrix} \begin{bmatrix} A_{n-1} & 0 \\ 0 & \alpha \end{bmatrix} \begin{bmatrix} E_{n-1} & A_{n-1}^{-1} a \\ 0 & 1 \end{bmatrix}.$$

ここで $\alpha = a_{nn} - {}^t a A_{n-1}^{-1} a$. 行列式を取れば $\alpha = |A_n|/|A_{n-1}|$ であり, A_{n-1} の符号数を (p', q') とすると, $\alpha > 0$ のとき (n 次から $n-1$ 次で主小行列の符号が変化しないとき) $q = q'$ となり, $\alpha < 0$ のとき (n 次から $n-1$ 次で主小行列の符号が変化するとき) $q = q' + 1$ となる.

$|A_{n-1}| = 0$ の場合. この場合は $|A_{n-2}| \neq 0$ なので,

$$A_n = A = \begin{bmatrix} A_{n-2} & B \\ {}^t B & C \end{bmatrix} = \begin{bmatrix} E_{n-2} & 0 \\ {}^t B A_{n-2}^{-1} & E_2 \end{bmatrix} \begin{bmatrix} A_{n-2} & 0 \\ 0 & D \end{bmatrix} \begin{bmatrix} E_{n-2} & A_{n-1}^{-1} B \\ 0 & E_2 \end{bmatrix}.$$

ここで $D = C - {}^t B A_{n-2}^{-1} B$. 行列式を取ることによって, $|D| = |A_n|/|A_{n-2}|$ であることがわかる. $|A_n|$ と $|A_{n-2}|$ の符号は異なるので $|D| < 0$ である. よって, D 符号数は $(1, -1)$ である. したがって, A_{n-2} の符号数を (p', q') とすると $q = q' + 1$ となる. □

20.9 逆の二次形式

以下の問題における逆の二次形式の定義は高木 [Tkg1] 第 9 章第 64 節 305–306 頁の問題 1 にしたがった. (佐武 [St] 第 IV 章第 4 節 164 頁の問 4 とその解答 (304 頁) にも同様の説明がある.)

[270] (逆の二次形式) $A = [a_{ij}]$ は n 次実対称行列であるとする. 実二次形式 Q_A の**逆の二次形式 (reciprocal quadratic form)** R_A を次のように定める:

$$R_A(x) = -\begin{vmatrix} a_{11} & \cdots & a_{1n} & x_1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & x_n \\ x_1 & \cdots & x_n & 0 \end{vmatrix} = -\begin{vmatrix} 0 & x_1 & \cdots & x_n \\ x_1 & a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ x_n & a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

A の (i, i) 余因子を $\tilde{a}_{ij}$ と書き, 対称行列 $\Delta(A)$ を $\Delta(A) = \left[\tilde{a}_{ij}\right]$ と定める. このとき $R_A = Q_{\Delta(A)}$. □

[271] A は n 次実対称行列であり, その符号数は (p, q) であるとする. R_A は Q_A の逆の二次形式であるとする. このとき, 以下が成立する:

1. $|A| > 0$ ならば R_A の符号数は (p, q) である.
2. $|A| < 0$ ならば R_A の符号数は (q, p) である. □

ヒント: $|A| \neq 0$ ならば $\Delta(A) = {}^t\Delta(A) = |A|A^{-1}$ なので, 問題 [**270**] より $R_A = |A|Q_{A^{-1}}$. □

参考: 問題 [**260**] のヒントの方法を使えば $R_A = |A|Q_{A^{-1}}$ を問題 [**270**] を使わずに直接証明することもできる. 実際, A が正則行列ならば

$$\begin{bmatrix} A & x \\ {}^t x & 0 \end{bmatrix} = \begin{bmatrix} E & 0 \\ {}^t x A^{-1} & 1 \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & -{}^t x A^{-1} x \end{bmatrix} \begin{bmatrix} E & A^{-1}x \\ 0 & 1 \end{bmatrix}.$$

なのでこの両辺の行列式を取って -1 倍すれば良い.

[**272**] A は n 次実対称行列であり, R_A は Q_A の逆の二次形式であるとする. このとき, n 次正則行列 P に対して $R_A\big({}^t(P^{-1})x\big) = |P|^{-2}R_{{}^tPAP}(x)$. □

ヒント: 次の等式を証明して両辺の行列式を取る:

$$\begin{bmatrix} A & {}^t(P^{-1})x \\ {}^t x P^{-1} & 0 \end{bmatrix} = \begin{bmatrix} {}^t(P^{-1}) & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} {}^tPAP & x \\ {}^t x & 0 \end{bmatrix} \begin{bmatrix} P^{-1} & 0 \\ 0 & 1 \end{bmatrix}. \quad \square$$

[**273**] A は n 次実対称行列であり, その符号数は (p, q) であるとする. R_A は Q_A の逆の二次形式であるとする. このとき, 以下が成立する:

1. $\operatorname{rank} A = n - 1$ かつ q が偶数ならば R_A の符号数は $(1, 0)$.
2. $\operatorname{rank} A = n - 1$ かつ q が奇数ならば R_A の符号数は $(0, 1)$.
3. $\operatorname{rank} A < n - 1$ ならば $R_A = 0$. □

ヒント: ある n 次直交行列 P が存在して ${}^tPAP = \operatorname{diag}(\alpha_1, \ldots, \alpha_n)$ となる. i 番目を除いた残りの α_j たちの積を a_i と書くことにする. このとき, 問題 [**272**] と [**270**] と P が直交行列であるから $|P|^2 = 1$ であることを用いると,

$$R_A\big({}^t(P^{-1})x\big) = |P|^{-2}R_{{}^tPAP}(x) = a_1x_1^2 + \cdots + a_nx_n^2.$$

よって, もしも $\alpha_n = 0$ ならば $R_A\big({}^t(P^{-1})x\big) = a_nx_n^2$ となる. $\operatorname{rank} A = n - k$ ならばちょうど k 個の α_i が 0 になる. □

21 直交行列

21.1 直交群と特殊直交群の定義

n 次直交行列とは n 次実正則行列 A で $A^{-1} = {}^tA$ を満たしているもののことである. 次の問題の結果は今後自由に使われる.

[**274**] A の中の列ベクトルの全体を $a_1, \ldots, a_n \in \mathbb{R}^n$ と表わす ($A = [a_1\ \cdots\ a_n]$). $\mathbb{R}^n$ の標準的な正規直交基底を $e_1, \ldots, e_n$ とすると $a_j = Ae_j$ である. 以下の条件は互いに同値である:

(a) A は直交行列である.

(b) ${}^tA$ は直交行列である.

(c) $a_1, \ldots, a_n$ は $\mathbb{R}^n$ の正規直交基底である.

(d) A の定める一次変換は $\mathbb{R}^n$ の任意の正規直交基底を正規直交基底に移す.

(e) 任意の $x, y \in \mathbb{R}^n$ に対して $\langle Ax, Ay\rangle = \langle x, y\rangle$.

(f) 任意の $x \in \mathbb{R}^n$ に対して $||Ax|| = ||x||$. □

直交行列の定める一次変換を直交変換と呼ぶ.

直交変換は正規直交基底を正規直交基底に移すような一次変換である. 直交変換はベクトルの長さ (ノルム) を保つような一次変換である. 直観的にそのような一次変換にはどのようなものがあるだろうか? 次のような一次変換は直交変換になるはずである:

- 正規直交基底を連続的に回転した結果を与える一次変換,
- ある (超) 平面に関する**鏡映 (reflection)**.

たとえば xy 平面における y 軸の向きを反転する一次変換は x 軸に関する鏡映 (変換) である. xyz 空間における z 軸の向きを反転する一次変換は xy 平面に関する鏡映変換である. xy 平面に鏡があるときその鏡を見ている人はあたかも鏡の中に自分自身が存在するように見えているはずである (ただし z 軸の向きは逆になっている). そのような様子を数学的に表現したのが鏡映変換である. (正確な定義は第 21.6 節で行なう.)

実は連続的な回転と鏡映の積で直交変換の全体は尽きている. この事実を証明することはこの節全体の目標の 1 つである.

n 次直交行列全体のなす集合を $O(n)$ と書き, 行列式が 1 であるような n 次直交行列全体のなす集合を $SO(n)$ と書くことにする:

$$O(n) = \{\, A \in M_n(\mathbb{R}) \mid {}^tAA = A\,{}^tA = E \,\}, \quad SO(n) = \{\, A \in O(n) \mid \det A = 1 \,\}.$$

集合 G と写像 $\cdot : G \times G \to G$, $(a, b) \mapsto ab$ と元 $e \in G$ と写像 $(\ )^{-1} : G \to G$, $a \mapsto a^{-1}$ の四つ組 $\big(G, \cdot, e, (\ )^{-1}\big)$ が**群 (group)** であるとは以下が成立していることである:

- **結合法則** $(ab)c = a(bc) \quad (a, b, c \in G)$;
- **単位元** $ea = ae = a \quad (a \in G)$;
- **逆元** $a^{-1}a = aa^{-1} = e \quad (a \in G)$.

しかし実際には, 群の演算 ab, 単位元 e, 逆元 a^{-1} の定め方は詳しく説明せずに, 「G は群である」と言う場合が多い. そのような説明を見た読者は群の演算, 単位元, 逆元の定め方を明確に定義した上で上の 3 つの条件が成立していることをチェックしなければいけない.

[275] $O(n)$ と $SO(n)$ は行列の積に関して群をなす. □

ヒント: 群の演算は行列の積で定める. ただしそのとき, $A, B \in O(n)$ ならば $AB \in O(n)$ であることと $A, B \in SO(n)$ ならば $AB \in SO(n)$ であることを証明しなければいけない. 単位元は単位行列 E と定める. ただしそのとき, $E \in SO(n) \subset O(n)$ を証明しなければいけない. 逆元は逆行列によって定める. ただしそのとき, $A \in O(n)$ ならば A^{-1} が存在して $A^{-1} \in O(n)$ であることと $A \in SO(n)$ ならば A^{-1} が存在して $A^{-1} \in SO(n)$ であることを証明しなければいけない. 群の 3 つの公理が成立していることは, 行列の積が結合法則を満たしていることなどからほとんど明らかである. □

$O(n)$ を n 次の**直交群 (orthogonal group)** と呼び, $SO(n)$ を n 次の**特殊直交群 (special orthogonal group)** と呼ぶ. 直観的には $SO(n)$ は n 次元 Euclid 空間に作用する連続的な回転の全体のなす群であり, $O(n)$ はさらに鏡映も含んでいる. この事実の厳密な証明は後の方の問題を解けば得られる.

[276] $\det O(n) = \{\pm 1\}$ かつ $\det SO(n) = \{1\}$ である[36]. さらに $\det S = -1$ を満たす任意の $S \in O(n)$ を取るとき,

$$O(n) = SO(n) \cup SO(n)S = SO(n) \cup S\,SO(n).$$

ここで和集合は交わりのない和集合 (disjoint union) である[37]. すなわち, $O(n)$ の元は $SO(n)$ の元であるか $SO(n)$ の元に S をかけたもの (左からかけても右からかけてもよい) のどちらか片方になる. □

ヒント: $A \in O(n)$ のとき ${}^tAA = E$ なのでその両辺の行列式を取ると $(\det A)^2 = 1$ である. よって $\det A = \pm 1$. $E, \mathrm{diag}(1, \ldots, 1, -1) \in O(n)$ であり, それぞれの行列式を取ると $1, -1$ になる. $S \in O(n)$, $\det S = -1$ と仮定する. $A \in O(n)$ が $\det A = -1$ を満たしているとき $B = S^{-1}A$, $C = AS^{-1}$ と置くと $\det B = \det C = 1$. □

以上の問題の結果より, $O(n)$ の任意の元は $SO(n)$ の元と行列式が -1 の直交行列の積 (積の順序はどちらでも良い) で表わせることがわかった. しかも行列式が -1 の直交行列の簡単な例として $\mathrm{diag}(1, \ldots, 1, -1)$ が取れる. よって $SO(n)$ がどういう集合であるかがよくわかれば $O(n)$ がどういう集合であるかもよくわかるということになる.

21.2 2 次直交行列の世界

まず $n = 2$ の場合に直交行列の世界がどういう様子をしているかを調べてみよう. この場合はすべての結果を直接的な計算によって容易に得ることができる.

[277] $SO(2)$ と $O(2)$ は以下のように表示できることを示せ:

$$SO(2) = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \,\middle|\, \theta \in \mathbb{R} \right\},$$

$$O(2) = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \,\middle|\, \theta \in \mathbb{R} \right\} \cup \left\{ \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \,\middle|\, \theta \in \mathbb{R} \right\}.$$

[36] 行列の集合 $\mathcal{G}$ に対して $\det \mathcal{G} := \{ \det A \mid A \in \mathcal{G} \}$. 一般に写像 $f : X \to Y$ に対して $f(X) = \{ f(x) \mid x \in X \}$.

[37] $SO(2) \cap SO(2)S = SO(n) \cap S\,SO(n) = \emptyset$ であるということ.

後者の結果を次のように書くこともできる:

$$O(2) = SO(2) \cup SO(2) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

この和は交わりのない和 (disjoint union) であることを直接証明せよ. □

ヒント: どうやっても何とかなる. たとえば 2 次実行列 A の成分を a, b, c, d と置いて ${}^tAA = E$ という条件を適当に整理するという直接的な方法で証明することもできる. 問題 **[274]** より $O(2)$ の元は $\mathbb{R}^2$ の正規直交基底全体の集合と同一視できることを使っても良い. $\mathbb{R}^2$ の正規直交基底は xy 平面上の単位ベクトル p とそれに直交する単位ベクトル q の組である. p は $p = {}^t[\cos\theta \ \sin\theta]$ と表わせる. この p に直交する単位ベクトルは $q = \pm {}^t[-\sin\theta \ \cos\theta]$ の 2 つである. 図を描いてみよ. □

[278] $\theta \in \mathbb{R}$ に対して行列 $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ が定める xy 平面の一次変換は時計の反対回りに角度 θ の回転になっていることを図を描いて説明せよ. さらに行列 $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ が定める xy 平面の一次変換は y 軸の向きを反転する鏡映であることを図を描いて説明せよ. □

解説: 実は一般の n 次元の場合も本質的にこの 2 つの変換ですべての直交変換を表示することができる. □

[279] 単位ベクトル $p = {}^t[\cos\phi \ \sin\phi]$ $(\theta \in \mathbb{R})$ に垂直な (原点を通る) 直線に関する鏡映変換 S_p を

$$S_p(x) = x - 2\langle p, x\rangle p \qquad (x \in \mathbb{R}^2)$$

と定める. このとき S_p の行列表示は次のようになる:

$$S_p = \begin{bmatrix} -\cos 2\phi & -\sin 2\phi \\ -\sin 2\phi & \cos 2\phi \end{bmatrix} = \begin{bmatrix} \cos 2\phi & -\sin 2\phi \\ \sin 2\phi & \cos 2\phi \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

よって p に関する鏡映変換 S_p は x 軸の向きを反転する鏡映変換をしてから左回りに角度 2ϕ だけ回転する直交変換に等しい. □

ヒント: $S_p(x) = x - p\,{}^tpx = (E - p\,{}^tp)x$ より $S_p = E - p\,{}^tp$ である. あとは三角函数の倍角の公式を使って整理すれば良い. 図を描いて結論が直観的にも明らかであることを確かめてみよ. □

[280] **(二面体群)** $n \in \mathbb{Z}_{\geq 3}$ とする. xy 平面上の n 個の点

$$P_k = \left(\cos\frac{2\pi k}{n}, \ \sin\frac{2\pi k}{n}\right) \qquad (k = 0, 1, \ldots, n-1)$$

を次々に線分で結んでできる図形を正 n 角形と呼ぶ. 正 n 角形をそれ自身の上に移す直交変換全体の集合 D_n は次のように表示される:

$$D_n = \{E, R, R^2, \ldots, R^{n-1}, A, RA, R^2A, \ldots, R^{n-1}A\}.$$

ここで,

$$R = \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

D_n は群をなし, **二面体群 (dihedral group)** と呼ばれている. □

ヒント: P_0 を P_k に移す直交変換は 2 通りある. □

[281] 問題 **[280]** の二面体群 D_n を考える. $A, B \in D_n$ を次のように定める:

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & -\cos\frac{2\pi}{n} \end{bmatrix},$$

このとき以下が成立する:

1. A は P_1 を P_{n-1} に移すような鏡映であり, B は P_0 を P_{n-1} に移すような鏡映である.
2. $D_n = \{\, (AB)^k,\, (AB)^k A \mid k = 0, 1, \ldots, n-1 \,\}$.
3. $A^2 = B^2 = E$ かつ $(AB)^n = E$. □

ヒント: $AB = R$. わかり難い場合は $n = 5, 6$ の場合に図を描いてみよ. □

参考: A, B は二面体群 D_n の生成元であり, $A^2 = B^2 = E$, $(AB)^n = E$ は二面体群 D_n の基本関係式である. すなわち, 二面体群 D_n の元は A, B だけを用いて表わすことができ, $A^2 = B^2 = E$, $(AB)^n = E$ だけから二面体群 D_n の元たちが満たしている全ての関係式を導くことができる.

n 次対称群 S_n も二面体群の場合と類似の基本関係式を持つ生成元を持つ. 生成元: $s_i = (i, i+1)$ $(i = 1, \ldots, n-1)$. 基本関係式: $s_i^2 = 1$, $(s_i s_{i+1})^3 = 1$, $(s_i s_j)^2 = 1$ $(|i-j| \geq 2)$. 実は S_n の生成元 s_i も鏡映によって表現可能である. 問題 **[309]** を見よ. □

21.3 3 次直交行列の世界

$\theta \in \mathbb{R}$ に対して行列式が 1 の 3 次直交行列 $R(\theta), S(\theta), T(\theta) \in SO(3)$ を次のように定める:

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix},\ S(\theta) = \begin{bmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{bmatrix},\ T(\theta) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}.$$

$R(\theta)$, $S(\theta)$, $T(\theta)$ はそれぞれ xy, zx, yz 平面の角度 θ の回転を表現している.

[282] $SO(3)$ が以下のように表示されることを示せ:

$$SO(3) = \{\, R(\theta)S(\phi)T(\psi) \mid 0 \leq \theta < 2\pi,\ -\pi/2 \leq \phi \leq \pi/2,\ 0 \leq \psi < 2\pi \,\}. \quad \square$$

ヒント: e_1, e_2, e_3 を回転することによって $\mathbb{R}^3$ の正規直交基底を構成することを考える. まず xy 平面を角度 $0 \leq \theta < 2\pi$ 回転させて (e_1, e_2, e_3) を次の正規直交基底 (e_1', e_2', e_3') に移す:

$$(e_1', e_2', e_3') = (\cos\theta\, e_1 + \sin\theta\, e_2,\ -\sin\theta\, e_1 + \cos\theta\, e_2,\ e_3).$$

この回転によって x, y, z 軸は x', y', z' 軸に移るとする. 次に $z'x'$ 平面を角度 $-\pi/2 \leq \phi \leq \pi/2$ 回転させて (e_1', e_2', e_3') を次の正規直交基底 (e_1'', e_2'', e_3'') に移す:

$$(e_1'', e_2'', e_3'') = (\cos\phi\, e_1' - \sin\phi\, e_3',\ e_2',\ \sin\phi\, e_1' + \cos\phi\, e_2').$$

この回転によって x', y', z' 軸は x'', y'', z'' 軸に移るとする. 以上の操作によって e_1'' を任意の単位ベクトルに移せる. 最後に $y''z''$ 平面を角度 $0 \leq \psi < 2\pi$ 回転させて (e_1'', e_2'', e_3'') を次の正規直交基底 (p_1, p_2, p_3) に移す:

$$(p_1, p_2, p_3) = (e_1'',\ \cos\psi\, e_2'' + \sin\psi\, e_3'',\ -\sin\psi\, e_2'' + \cos\psi\, e_3'').$$

$p_1 = e_1''$ と直交するベクトル全体は e_2'', e_3'' で張られる平面に一致しているので, p_2 を p_1 に垂直な任意の単位ベクトルに移すことができる. p_1, p_2 に直交する単位ベクトルは $\pm p_3$ のどちらかに等しい. 以上によって任意の 3 次直交行列は $P = [p_1\ p_2\ p_3]$ または $P' = [p_1\ p_2\ -p_3]$ の形をしていることがわかった. 上の操作を行列で書くと,

$$[e_1'\ e_2'\ e_3'] = [e_1\ e_2\ e_3]R(\theta), \quad [e_1''\ e_2''\ e_3''] = [e_1'\ e_2'\ e_3']S(\phi), \quad [p_1\ p_2\ p_3] = [e_1''\ e_2''\ e_3'']T(\psi).$$

よって $P = R(\theta)S(\phi)T(\psi)$ である. これより $\det P = 1$ であり, $\det P' = -1$ であることがわかる. したがって任意の $SO(3)$ の元はこの P の形で表わされる. 以上の議論を図を描いて説明せよ. □

[283] (Euler 角) $SO(3)$ が以下のように表示されることを示せ:

$$SO(3) = \{\, R(\varphi)S(\theta)R(\psi) \mid 0 \leq \varphi < 2\pi,\ 0 \leq \theta \leq \pi,\ 0 \leq \psi < 2\pi \,\}.$$

φ, θ, ψ を **Euler 角 (Euler's angle)** と呼ぶ[38]. □

ヒント: e_1, e_2, e_3 を回転することによって $\mathbb{R}^3$ の正規直交基底を構成することを考える. まず xy 平面を角度 $0 \leq \varphi < 2\pi$ 回転させて (e_1, e_2, e_3) を次の正規直交基底 (e_1', e_2', e_3') に移す:

$$(e_1', e_2', e_3') = (\cos\varphi\, e_1 + \sin\varphi\, e_2,\ -\sin\varphi\, e_1 + \cos\varphi\, e_2,\ e_3).$$

この回転によって x, y, z 軸は x', y', z' 軸に移るとする. 次に $z'x'$ 平面を角度 $0 \leq \theta \leq \pi$ 回転させて (e_1', e_2', e_3') を次の正規直交基底 (e_1'', e_2'', e_3'') に移す:

$$(e_1'', e_2'', e_3'') = (\cos\theta\, e_1' - \sin\theta\, e_3',\ e_2',\ \sin\theta\, e_1' + \cos\theta\, e_2').$$

この回転によって x', y', z' 軸は x'', y'', z'' 軸に移るとする. 以上の操作によって e_3'' を任意の単位ベクトルに移せる. 最後に $x''y''$ 平面を角度 $0 \leq \psi < 2\pi$ 回転させて (e_1'', e_2'', e_3'') を次の正規直交基底 (p_1, p_2, p_3) に移す:

$$(p_1, p_2, p_3) = (\cos\psi\, e_1'' + \sin\psi\, e_2'',\ -\sin\psi\, e_1'' + \cos\psi\, e_2'',\ e_3'').$$

$p_3 = e_3''$ と直交するベクトル全体は e_1'', e_2'' で張られる平面に一致しているので, p_2 を p_3 に垂直な任意の単位ベクトルに移すことができる. p_2, p_3 に直交する単位ベクトルは $\pm p_1$ のどちらかに等しい. 以上によって任意の 3 次直交行列は $P = [p_1\ p_2\ p_3]$ または $P' = [-p_1\ p_2\ p_3]$ の形をしていることがわかった. 上の操作を行列で書くと,

$$[e_1'\ e_2'\ e_3'] = [e_1\ e_2\ e_3]R(\varphi), \quad [e_1''\ e_2''\ e_3''] = [e_1'\ e_2'\ e_3']S(\theta), \quad [p_1\ p_2\ p_3] = [e_1''\ e_2''\ e_3'']R(\psi).$$

よって $P = R(\varphi)S(\theta)R(\psi)$ である. これより $\det P = 1$ であり, $\det P' = -1$ であることがわかる. したがって任意の $SO(3)$ の元はこの P の形で表わされる. 以上の議論を図を描いて説明せよ. □

[38] Euler 角は剛体の運動を記述するときによく使われる.

[284] $g(\varphi,\theta,\psi)=R(\varphi)S(\theta)R(\psi)$ と置くと $g(\varphi,\theta,\psi)^{-1}=g(\pi-\psi,\theta,\pi-\varphi)$. □

ヒント: 山内・杉浦 [YmS] 第 II 章第 2 節問 3(50 頁) の解答 (191 頁). $A=R(\pi)=\mathrm{diag}(-1,-1,1)$ と置くと $A^2=E$, $AS(-\theta)A=S(\theta)$ である. よって,

$$g(\varphi,\theta,\psi)^{-1}=R(-\psi)S(-\theta)R(-\varphi)=\text{☆☆☆}=R(-\psi+\pi)S(\theta)R(\pi-\varphi).\quad\square$$

問題 **[282]** もしくは Euler 角 **[283]** の結果によって $SO(3)$ の任意の 2 点が $SO(3)$ 内の連続的な曲線で結べることがわかる. ((θ,ϕ,ψ) もしくは Euler 角を連続的に動かせばよい.) この事実を「$SO(3)$ は弧状連結 (arcwise connected) である」という.

これに対して $O(3)$ は弧状連結ではない. なぜならば $E, S=\mathrm{diag}(1,1,-1)\in O(3)$ の 2 点を結ぶ $O(3)$ 内の連続的な曲線が存在するならば, $\det E=1$, $\det S=-1$ なので中間値の定理よりその連続的な曲線上のどこかで行列式が 0 になってしまうからである[39].

問題 **[276]** の結果より $O(3)$ は 2 つの弧状連結成分 $SO(3)$ と $SO(3)\,\mathrm{diag}(1,1,-1)$ に分かれていることがわかる[40].

ベクトルの並べ方が異なる基底は異なるとみなすことにすれば $\mathbb{R}^3$ の正規直交基底 (p_1,p_2,p_3) の全体は $P=[p_1\ p_2\ p_3]$ の行列式が ±1 のどちらになるかによって分類される. 上で説明した実は, P の行列式が同じになる正規直交基底どうしは連続的な変形によって移り合い, P の行列式が互いに異なる 2 つの正規直交基底は連続的な変形によって決して移り合わないことを意味している.

通常 P の行列式が 1 になるような正規直交基底は**右手系**と呼ばれ, -1 になるような正規直交基底は**左手系**と呼ばれている. 上の議論によって, 右手系と左手系は連続的な変形によって互いに移り合わない. 通常図を描く場合には右手の人指し指, 中指, 親指の指す方向のそれぞれを x, y, z 軸の方向とみなす.

21.4 Hamilton の四元数の世界

3 次元実 Euclid 空間の連続的回転の世界 $SO(3)$ を完全に理解するためには**四元数 (quaternion)** の世界を導入しなければいけない[41]. 2 次元平面の回転が複素数を用いれば $e^{i\theta}$ の形で表現できたことと同じように 3 次元空間の回転を四元数を用いて表現することができる.

Hamiltn の四元数体 $\mathbb{H}$ を以下のように定義する. まず $\mathbb{R}$ 上のベクトル空間として $\mathbb{H}$ を $1,i,j,k$ を基底に持つ $\mathbb{R}$ 上のベクトル空間と定義する:

$$\mathbb{H}=\mathbb{R}1\oplus\mathbb{R}i\oplus\mathbb{R}j\oplus\mathbb{R}k.$$

すなわち $\mathbb{H}$ の任意の元 u は

$$u=a1+bi+cj+dk,\qquad a,b,c,d\in\mathbb{R}$$

[39] 同様の議論で $GL_n(\mathbb{R})$ も弧状連結でないことを示せる.

[40] $GL_n(\mathbb{R})$ も行列式の正負による分類によって 2 つの弧状連結成分に分かれていることを示せる. ヒント: 岩沢分解によって $O(n)$ の場合に帰着する. $O(n)$ の場合の結果は第 21.5 節で扱う.

[41] 一般の $SO(n)$ の場合は **Clifford 代数 (Clifford algebra)** を導入する必要がある. 物理的に Clifford 代数は Fermion の代数である.

の形で一意に表わされる. $\mathbb{R}$ 上の双線形写像 $\mathbb{H}\times\mathbb{H}\to\mathbb{H}$, $(u,v)\mapsto uv$ を次の条件によって定める:

$$11=1,\quad 1i=i1=i,\quad 1j=j1=j,\quad 1k=k1=k,$$
$$ii=jj=kk=-1,\quad ij=-ji=k,\quad jk=-kj=i,\quad ki=-ik=j.$$

$a\in\mathbb{R}$ と $a1\in\mathbb{H}$ を同一視し, $a+bi\in\mathbb{C}$ $(a,b\in\mathbb{R})$ と $a1+bi\in\mathbb{H}$ を同一視する.

[285] 四元数体 $\mathbb{H}$ の任意の元は $z+jw$ $(z,w\in\mathbb{C})$ と一意的に表わされ, $zj=j\overline{z}$ $(z\in\mathbb{C})$ が成立している. □

[286] $u\in\mathbb{H}$ が $u^2=-1$ を満たすための必要十分条件は u が $u=bi+cj+dk$ $(b,c,d\in\mathbb{R},$ $b^2+c^2+d^2=1)$ と表わされることである. そのとき $\{\,x+yu\mid x,y\in\mathbb{R}\,\}$ は複素数体のコピーとみなせる. □

解説: $\mathbb{C}$ の $\mathbb{H}$ への埋め込み方の全体の集合は2次元球面 $S^2=\{\,(b,c,d)\in\mathbb{R}^3\mid b^2+c^2+d^2=1\,\}$ と同一視できる.

四元数 $u=a+bi+cj+dk\in\mathbb{H}$ $(a,b,c,d\in\mathbb{R})$ に対して, その共役元 u^* を

$$u^*=a-bi-cj-dk$$

と定め, u の実部 $\mathrm{Re}\,u$ を次のように定める:

$$\mathrm{Re}\,u=a.$$

$\mathbb{H}$ に $\mathbb{R}$ 上の内積 $\langle\ ,\ \rangle$ を次のように定める:

$$\langle u,v\rangle:=\mathrm{Re}(u^*v)=aa'+bb'+cc'+dd'.$$

ここで $u=a+bi+cj+dk$, $v=a'+b'i+c'j+d'k$ $(a,b,c,d,a',b',c',d'\in\mathbb{R})$. この内積に関する u のノルム (絶対値) を $|u|$ と書く:

$$|u|=\langle u,u\rangle^{1/2}=(a^2+b^2+c^2+d^2)^{1/2}$$

[287] 以下を示せ:

1. $1,i,j,k$ は $\mathbb{H}$ の $\mathbb{R}$ 上の正規直交基底である.
2. 任意の $u,v\in\mathbb{H}$ に対して $(uv)^*=v^*u^*$.
3. 任意の $u,v\in\mathbb{H}$ に対して $\mathrm{Re}(uv)=\mathrm{Re}(vu)$.
4. 任意の $u\in\mathbb{H}$ に対して $u^*u=uu^*=|u|^2$.
5. 任意の $u,v\in\mathbb{H}$ に対して $|uv|=|u||v|$.
6. **(結合法則)** 任意の $u,v,w\in\mathbb{H}$ に対して $(uv)w=u(vw)$.
7. **(非零元の逆元)** 0 でない任意の $u\in\mathbb{H}$ に対してある $v\in\mathbb{H}$ で $vu=uv=1$ を満たすものが一意に存在する. □

ヒント: 結合法則の証明は u, v, w が $1, i, j, k$ の場合に帰着する. 逆元の一意性: $vu = 1$, $uw = 1$ のとき $v = v1 = v(uw) = (vu)w = 1w = w$. 逆元の存在: $v = u^*/|u|^2$ と置けば良い. □

[288] 四元数を用いて次の公式を証明せよ:

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3)^2\\ &+ (x_1y_3 - x_3y_1 - x_4y_2 + x_2y_4)^2 + (x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2)^2. \quad \square\end{aligned}$$

ヒント: $u = x_1 + x_2i + x_3j + x_4k$, $v = y_1 + y_2i + y_3j + y_4k$ のとき,

$$|u|^2|v|^2 = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

であり, $z_1, z_2, z_3, z_4 \in \mathbb{R}$ を $u^*v = z_1 + z_2i + z_3j + z_4k$ と定めると,

$$|u^*v|^2 = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

そして問題 **[287]** の結果より $|u|^2|v|^2 = |u^*v|^2$ である. □

参考: この公式は「任意の正の整数は 4 つの整数の平方の和になる」という Lagrange の定理を証明するときに用いられる. $1 = 1^2 + 0^2 + 0^2 + 0^2$, $2 = 1^2 + 1^2 + 0^2 + 0^2$ と上の公式より Lagrange の定理の証明は「任意の奇素数は 4 つの整数の平方の和になる」ことを示すことに帰着する. Lagrange の証明についてはたとえばヒンチン [Kh] 第 3 章第 5 節 (132–135 頁) を見よ. □

[289] (四元数体の複素行列表現) 行列 I, J, K を次のように定める:

$$I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad K = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

$u \in \mathbb{H}$ に対して $\phi(u) \in M_2(\mathbb{C})$ を次のように定める:

$$\phi(u) := aE + bI + J(cE + dI) = \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix}.$$

ここで, $u = z + jw \in \mathbb{H}$, $z = a + bi$, $w = c + di \in \mathbb{C}$, $a, b, c, d \in \mathbb{R}$ である. ($\phi(1) = E$, $\phi(i) = i$, $\phi(j) = J$, $\phi(k) = K$ であることに注意せよ.) このとき,

1. $\phi(au) = a\phi(u) \quad (a \in \mathbb{R}, u \in \mathbb{H})$;
2. $\phi(u + v) = \phi(u) + \phi(v) \quad (u, v \in \mathbb{H})$;
3. $\phi(uv) = \phi(u)\phi(v) \quad (u, v \in \mathbb{H})$;
4. $\phi(1) = E \quad (u, v \in \mathbb{H})$;
5. $\phi(u^*) = \phi(u)^* \quad (u \in \mathbb{H})$;
6. $\operatorname{Re} u = \frac{1}{2} \operatorname{tr} \phi(u) \quad (u \in \mathbb{H})$;

7. $\langle u, v\rangle = \frac{1}{2}\operatorname{tr}\bigl(\phi(u)^*\phi(v)\bigr) \quad (u, v \in \mathbb{H})$;

8. $|u|^2 = \det\phi(u) \quad (u \in \mathbb{H})$.

以上のの結果より, $1 \leftrightarrow E$, $i \leftrightarrow I$, $j \leftrightarrow J$, $k \leftrightarrow K$ という同一視によって, 四元数体 $\mathbb{H}$ と上の形の 2 次複素正方行列の全体の集合は同一視できることがわかった. □

ヒント: $\phi(uv) = \phi(u)\phi(v)$ の証明は u, v が i, j, k の場合に帰着する. まず $I^2 = J^2 = -E$, $IJ = -JI = K$ を示せ. それらより $K^2 = -E$, $JK = -KJ = I$, $KI = -IK = J$ が導かれる. □

注意: [**187**] で定義した Pauli のスピン行列は四元数の行列表現と関係している. I, J, K は符号と並び方の違い除いて Pauli のスピン行列の i 倍に一致している. □

四元数 $u \in \mathbb{H}$ で $|u| = 1$ を満たすもの全体の集合を $U(1, \mathbb{H})$ と表わす[42]:

$$U(1, \mathbb{H}) := \{\, u \in \mathbb{H} \mid |u| = 1 \,\} = \{\, u \in \mathbb{H} \mid u^*u = uu^* = 1 \,\}.$$

2 次複素正則行列 A で $A^{-1} = A^*$ かつ $\det A = 1$ を満たすもの全体の集合を $SU(2)$ と表わす:

$$SU(2) := \{\, A \in M_2(\mathbb{C}) \mid A^*A = AA^* = E,\ \det A = 1 \,\}.$$

[**290**] $U(1, \mathbb{H})$ は四元数の積に関して群をなし, $SU(2)$ は行列の積に関して群をなすことを示せ. $SU(2)$ は 2 次の**特殊ユニタリー群 (special unitary group)** と呼ばれている. 問題 [**289**] の同一視を通して, $SU(2)$ と集合 $U(1, \mathbb{H})$ を同一視できることを示せ. すなわち,

$$\begin{aligned} SU(2) &= \left\{ \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} \,\middle|\, z, w \in \mathbb{C},\ |z|^2 + |w|^2 = 1 \right\} \\ &= \left\{ \begin{bmatrix} a+bi & -c+di \\ c+di & a-bi \end{bmatrix} \,\middle|\, a, b, c, d \in \mathbb{R},\ a^2+b^2+c^2+d^2 = 1 \right\} \end{aligned}$$

であることを示せ. □

ヒント: 2×2 行列の話なので真面目に計算するだけ. □

解説: $S^3 = \{\, (a, b, c, d) \in \mathbb{R}^4 \mid a^2 + b^2 + c^2 + d^2 = 1 \,\}$ は 3 次元球面と呼ばれている. 4 次元 Euclid 空間に表面が 3 次元に球面が浮かんでいる様子を想像しなければいけない. 3 次元

[42] この記号法は $U(1) = \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$ の四元数の場合への拡張である. より一般には

$$U(n) = \{\, A \in M_n(\mathbb{C}) \mid A^*A = AA^* = E \,\}, \quad U(n, \mathbb{H}) = \{\, A \in M_n(\mathbb{H}) \mid A^*A = AA^* = E \,\}.$$

実は $U(n, \mathbb{H})$ は**ユニタリー・シンプレクティック群 (unitary symplectic group)** $Sp(n) = U(2n) \cap Sp_n(\mathbb{C})$ に同型である. 複素シンプレクティック群 $Sp_n(\mathbb{C})$ は次のように定義される:

$$Sp_n(\mathbb{C}) = \{\, A \in M_{2n}(\mathbb{C}) \mid {}^tAJ_nA = J_n \,\}.$$

ここで J_n は対角線に問題 [**289**] で定義した J を n 個並べてできる $2n$ 次の正方行列である. 特に $Sp_1(\mathbb{C}) = SL_2(\mathbb{C}) = \{\, A \in M_2(\mathbb{C}) \mid \det A = 1 \,\}$ なので $Sp(1) = SU(2)$ である. $U(n, \mathbb{H})$ から $Sp(n)$ への同型写像は $A \in U(n, \mathbb{H})$ に対して A の各成分の四元数を問題 [**289**] の ϕ によって 2 次複素正方行列に置換することによって得られる $2n$ 次複素正方行列 $\phi(A)$ を対応させることによって得られる. 問題 [**290**] はこの結果の特別な場合である.

Euclid 空間に浮かぶ表面が 2 次元の通常の球面 S^2 は 2 次元球面と呼ばれている. 上の問題の結果は $SU(2)$ が位相的に 3 次元球面 S^3 と同相であることを意味している[43]. 前節で $SO(3)$ は Euler 角などによって 3 次元の空間であることは大体わかっている. $SO(3)$ がどういう形をしているかは $SU(2)$ と $SO(3)$ を関係付けることによって調べることができる. それを実行するのが目標である. □

まとめ: $SU(2) = U(1,\mathbb{H}) = S^3$ という同一視が可能である.

四元数体の元の指数函数が自然に定義される:

$$e^u = \sum_{n=0}^{\infty} \frac{u^n}{n!} \qquad (u \in \mathbb{H}).$$

複素数の場合と同様に $\theta \in \mathbb{R}$ に対して次の公式が成立している:

$$e^{i\theta} = \cos\theta + i\sin\theta, \quad e^{j\theta} = \cos\theta + j\sin\theta, \quad e^{k\theta} = \cos\theta + k\sin\theta.$$

[291] $U(1,\mathbb{H})$ は次のように表わされる:

$$U(1,\mathbb{H}) = \left\{ e^{k\varphi}e^{j\theta}e^{k\psi} \;\middle|\; \varphi,\theta,\psi \in \mathbb{R} \right\}. \quad \square$$

注意: Euler 角 **[283]** との類似性に注意せよ. □

ヒント: $kj = -jk$ より

$$\begin{aligned} e^{k\varphi}e^{j\theta}e^{k\psi} &= \cos\theta e^{k(\varphi+\psi)} + \sin\theta j e^{k(\varphi-\psi)} \\ &= \cos\theta\cos(\varphi+\psi) + k\cos\theta\sin(\varphi+\psi) \\ &\quad + j\sin\theta\cos(\varphi-\psi) + i\sin\theta\sin(\varphi-\psi). \quad \square \end{aligned}$$

$\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ の正規直交基底 (i,j,k) と $\mathbb{R}^3$ の標準的な正規直交基底 (e_1,e_2,e_3) を同一視することによって, $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \mathbb{R}^3$ と同一視する.

[292] 任意の $g \in U(1,\mathbb{H})$ に対して $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \mathbb{R}^3$ の直交変換 $\rho(g)$ を

$$\rho(g)x := gxg^{-1} \qquad (x \in \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \mathbb{R}^3)$$

と定めることができ, 次が成立している:

$$\rho(gh) = \rho(g)\rho(h) \quad (g,h \in U(1,\mathbb{H})), \qquad \rho(1) = \mathrm{id}_{\mathbb{R}^3}.$$

ここで $\mathrm{id}_{\mathbb{R}^3}$ は $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \mathbb{R}^3$ の恒等写像である[44]. $g = e^{i\theta}, e^{j\theta}, e^{k\theta}$ $(\theta \in \mathbb{R})$ に対して, 基底 $(i,j,k) = (e_1,e_2,e_3)$ に関する $\rho(g)$ の行列表示は次のようになる:

$$\rho(e^{i\theta}) = T(2\theta), \quad \rho(e^{j\theta}) = S(2\theta), \quad \rho(e^{k\theta}) = R(2\theta).$$

ここで $R(\theta), S(\theta), T(\theta)$ は第 21.3 節の最初に定義した回転行列である. よって, $\varphi,\theta,\psi \in \mathbb{R}$ に対して

$$\rho(e^{k\varphi})\rho(e^{j\theta})\rho(e^{k\psi}) = R(2\varphi)S(2\theta)R(2\psi).$$

したがって, 問題 **[291]** と問題 **[283]** より, ρ は $U(1,\mathbb{H})$ から $SO(3)$ への全射であることがわかる. □

---

[43] 同相という言葉を知らなくても気にする必要はない. 直観的には 2 つの空間のあいだに連続的に一対一対応を構成できるとき, 2 つの空間は互いに**同相 (homeomorphic)** であると言う.

[44] 集合 X の**恒等写像 (identity map)** id_X とは $\mathrm{id}_X(x) = x$ $(x \in X)$ で定義される写像のことである. 恒等写像は何も動かさない.

ヒント: $g \in U(1,\mathbb{H})$ に対して $g^* = g^{-1}$ なので

$$\langle \rho(g)x, \rho(g)y\rangle = \mathrm{Re}\big((gxg^*)^* gyg^*\big) = \mathrm{Re}\big(gx^*g^*gyg^*\big) = \mathrm{Re}(x^*y) = \langle x, y\rangle.$$

$ik = -ki$ であるから,

$$\rho(e^{k\theta})i = e^{k\theta}ie^{-k\theta} = e^{2k\theta}i = i\cos 2\theta + j\sin 2\theta. \quad \square$$

上の問題を見ると, 四元数の世界における角度 θ の回転に対応する 3 次元空間の回転は倍の角度 2θ の回転になっている. このことから想像されるように $\rho : U(1,\mathbb{H}) \to SO(3)$ は 2 : 1 写像になっている. すなわち $SO(3)$ の 1 点は $U(1,\mathbb{H})$ の 2 点と対応している. 次の問題を見よ.

[293] 問題 **[292]** の $\rho : U(1,\mathbb{H}) \to SO(3)$ を考える. このとき $g, h \in U(1,\mathbb{H})$ に対して $\rho(g) = \rho(h)$ が成立するための必要十分条件は $g = \pm h$ が成立することである. $\square$

ヒント: 十分性はほとんど明らか. 必要性は以下のように証明する. $x = gh^{-1}$ と置くことによって $\rho(x) = \mathrm{id}$ ならば $x = \pm 1$ であることを示せば良いことがわかる. $\rho(x) = \mathrm{id}$ ならば特に $xix^{-1} = i$ かつ $xjx^{-1} = j$ である. $xix^{-1} = i$ より $x \in \mathbb{C}$ かつ $|x| = 1$ であることがわかり, さらに $xjx^{-1} = j$ より $x = \pm 1$ であることがわかる. $\square$

解説: 3 次元球面上の原点を中心として点対称の位置にある 2 点をすべて同一視してできる空間を 3 次元実射影空間と呼び, $\mathbb{P}^3(\mathbb{R})$ と書くことにする:

$$\mathbb{P}^3(\mathbb{R}) = S^3/\!\sim, \qquad x \sim \pm x.$$

$U(1,\mathbb{H}) = SU(2)$ は自然に 3 次元球面 S^3 と同一視できるのであった. $\pm g \in U(1,\mathbb{H})$ に対応する 3 次元球面上の 2 つの点は原点を中心として点対称の位置にある. よって上の問題は 3 次元実射影空間 $\mathbb{P}^3(\mathbb{R})$ と $SO(3)$ が同一視できることを意味している[45] $\square$

まとめ: $SO(3) = \mathbb{P}^3(\mathbb{R})$ と同一視できる.

すでに大活躍した $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ を $\mathrm{u}(1,\mathbb{H})$ と書くことにする:

$$\mathrm{u}(1,\mathbb{H}) = \mathbb{R}i + \mathbb{R}j + \mathbb{R}k.$$

$\mathrm{u}(1,\mathbb{H})$ は $\mathbb{R}^3$ と同一視されるだけではなく, そこに有用な構造 (Lie 群 $U(1,\mathbb{H})$ の Lie 代数の構造) を入れることができる.

[294] 以下を示せ:

1. 任意の $u, v \in \mathrm{u}(1,\mathbb{H})$ に対して $[u, v] \in \mathrm{u}(1,\mathbb{H})$ である[46].

[45] この辺の説明はわかり難いかもしれないので, 直接質問してくれれば図を描いてより詳しく説明する. 重要なのは $SU(2) = U(1,\mathbb{H})$ や $SO(3)$ のような回転全体の空間の「形」が完全にわかってしまうことである. $\mathbb{P}^3(\mathbb{R})$ がどういう世界なのかよく理解できない人は 2 次元球面から実射影平面を構成することが直観的にどういうことなのかについて考えてみよ.

[46] $[u, v] = uv - vu$ (交換子) である. $\mathrm{u}(1,\mathbb{H})$ が交換子について閉じているということはそれが Lie 代数であることを意味している.

2. 任意の $u \in \mathrm{u}(1,\mathbb{H})$ に対して $e^u \in U(1,\mathbb{H})$ である[47]. □

ヒント: $[i,j]=2k$, $[j,k]=2i$, $[k,i]=2j$ である. $u \in \mathrm{u}(1,\mathbb{H})$ のとき $u^* = -u$ なので $(e^u)^* = e^{-u} = (e^u)^{-1}$. □

上の問題に対応する複素行列における結果は次のようになる.

[295] 実ベクトル空間 $\mathrm{su}(2)$ を次のように定義する:

$$\mathrm{su}(2) = \{\, A \in M_2(\mathbb{C}) \mid A^* = -A,\ \mathrm{tr}\, A = 0 \,\}.$$

このとき以下が成立する:

1. $\mathrm{su}(2) = \mathbb{R}I + \mathbb{R}J + \mathbb{R}K$.
2. 任意の $A, B \in \mathrm{su}(2)$ に対して $[A,B] \in \mathrm{su}(2)$ である[48].
3. 任意の $A \in \mathrm{su}(2)$ に対して $e^A \in SU(2)$. □

ヒント: 任意の正方行列 A, B に対して $\mathrm{tr}[A,B]=0$ である. $A^*=-A$, $B^*=-B$ のとき $[A,B]^* = [B^*,A^*] = [B,A] = -[A,B]$ となる. $A^*=-A$ のとき $(e^A)^* = e^{-A} = (e^A)^{-1}$ となる. $\mathrm{tr}\, A = 0$ ならば $\det e^A = 1$ となることの証明には次の問題の結果を使う.

[296] A が n 次複素正方行列ならば $\det e^A = e^{\mathrm{tr}\, A}$. □

ヒント 1: 問題 **[193]** より, ある複素正則行列 P が存在して $P^{-1}AP$ は上三角行列になり, $P^{-1}AP$ の対角成分には A の固有値 $\alpha_1, \ldots, \alpha_n$ が並ぶ. このとき, $e^{P^{-1}AP}$ の対角成分には $e^{\alpha_1}, \ldots, e^{\alpha_n}$ が並ぶ. よって $\det e^A = \det e^{P^{-1}AP} = e^{\alpha_1+\cdots+\alpha_n} = e^{\mathrm{tr}\, P^{-1}AP} = e^{\mathrm{tr}\, A}$. □

ヒント 2: $f(t) = \det e^{At}$ と置くと $f(0)=1$ であり, 次の問題の結果より

$$\frac{f'(t)}{f(t)} = \mathrm{tr}\left(e^{-At}\frac{d}{dt}e^{At}\right) = \mathrm{tr}(e^{-At}e^{At}A) = \mathrm{tr}\, A.$$

よって $f(t) = e^{t\,\mathrm{tr}\, A}$ である. $t=1$ と置けば示すべき結論が得られる. □

[297] $\det X$ を $X = [x_{ij}]_{i,j=1}^n$ の成分 x_{ij} の多項式であるとみなす. このとき,

$$\frac{d\det X}{\det X} = \mathrm{tr}(X^{-1}\, dX). \quad \square$$

ヒント: 行列式 $\det X$ と X の (i,j) 余因子 $\tilde{x}_{ij}$ の定義より,

$$\frac{\partial \det X}{\partial x_{ij}} = \tilde{x}_{ij}.$$

よって, $\Delta(X) = [\tilde{x}_{ij}]$, $dX = [dx_{ij}]$ と置くと,

$$d\det X = \sum_{i,j=1}^n \tilde{x}_{ij}\, dx_{ij} = \mathrm{tr}({}^t\Delta(X)\, dX) = \det X \cdot \mathrm{tr}(X^{-1}\, dX).$$

より詳しい解説が佐武 [St] 第 II 章第 3 節 (84–85 頁) にある. □

$SU(2)$ と $SO(3)$ の関係の入門的な詳しい解説が山内・杉浦 [YmS] の第 II 章第 2 節 41–50 頁にあるので興味のある方は参照されたり. 横田 [Ykt] の 30 頁の例 53, 例 54 も参照せよ.

[47] $U(1,\mathbb{H})$ の実多様体としての次元は 3 に等しく, $\mathrm{u}(1,\mathbb{H})$ の実ベクトル空間としての次元も 3 に等しいので, 「$u \in \mathrm{u}(1,\mathbb{H})$ ならば $e^u \in U(1,\mathbb{H})$」は $\mathrm{u}(1,\mathbb{H})$ が $U(1,\mathbb{H})$ の Lie 代数であることを意味している.

[48] $[A,B] = AB - BA$ (交換子) である.

21.5 n 次直交行列の世界

n 次の正方行列で (i,j) 成分のみが 1 で他の成分がすべて 0 であるようなものを E_{ij} と書き, (i,j) **行列単位 (matrix unit)** と呼ぶ.

$\theta \in \mathbb{R}$ と $i \neq j$ に対して n 次の直交行列 $R_{ij}(\theta)$ を次のように定める:

$$R_{ij}(\theta) = (E_{ii} + E_{jj})\cos\theta + (E_{ji} - E_{ij})\sin\theta + \sum_{k\neq i,j} E_{kk}.$$

たとえば $n = 3$ のとき第 21.3 節の記号にしたがえば $R_{12}(\theta) = R(\theta)$, $R_{31}(\theta) = S(\theta)$, $R_{23}(\theta) = T(\theta)$ である.

[298] $R_{ji}(\theta) = R_{ij}(-\theta) = R_{ij}(\theta)^{-1}$. □

[299] $SO(n)$ は次のように表わされる:

$$SO(n) = \Big\{ \prod_{i<j} R_{ij}(\theta_{ij}) \;\Big|\; \theta_{ij} \in \mathbb{R}\ (i<j) \Big\}.$$

ここで $r_{ij} = R_{ij}(\theta_{ij})$ たちの積の順序は辞書式に左から $r_{12}r_{13}\cdots r_{1n}r_{23}\cdots r_{2n}\cdots r_{n-1,n}$ と並んでいると仮定する. □

ヒント: 問題 **[282]** のヒントを n 次元に拡張すれば良い. 厳密には n に関する帰納法で証明すれば良い. □

[300] $A \in O(n)$ であるとし, A の固有値 -1 の重複度を q と書くことにする. (もしも A が -1 を固有値に持たなければ $q = 0$.) このとき, $A \in SO(n)$ であるための必要十分条件は q が奇数であることである. □

ヒント: 第 18 節の問題 **[199]** の結果を使う. そのとき $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{bmatrix}$ に注意せよ. □

[301] $SO(n)$ は弧状連結である[49]. □

ヒント 1: 問題 **[299]** の結果を使う. $SO(n)$ の任意の元 A を $R_{ij}(\theta_{ij})$ たちの積で表示しておく. $R_{ij}(t\theta_{ij})$ たちの積は t に関して連続であり $t = 0$ のとき単位行列になり $t = 1$ のとき A になる. □

ヒント 2: 第 18 節の問題 **[199]** の結果を使う. 問題 **[300]** のヒントも参照せよ. □

第 18 節の問題 **[199]** の結果に解説を追加しておきたい. そのためにその内容を全文再掲しておこう. 問題 **[199]** の結果:

直交行列 A に対してある直交行列 Q で $Q^{-1}AQ$ が次の形になるものが存在する:

$$Q^{-1}AQ = \begin{bmatrix} E_{r_1} & & & & & & & \\ & -E_{r_2} & & & & & & \\ & & \cos\theta_1 & \sin\theta_1 & & & & \\ & & -\sin\theta_1 & \cos\theta_1 & & & & \\ & & & & \ddots & & & \\ & & & & & \cos\theta_s & \sin\theta_s & \\ & & & & & -\sin\theta_s & \cos\theta_s & \end{bmatrix}.$$

ここで, $r_1 + r_2 + 2s = n$ かつ $\theta_k \in \mathbb{R}$ であり, E_r は r 次の単位行列である. □

[49] $SO(n)$ の単位元 E と任意の元 A を結ぶ $SO(n)$ 内の連続的な曲線が存在することを示せ.

この結果は次のような幾何学的意味を持っている. いつものように直交行列 Q の中の列ベクトルを $q_1, \ldots, q_n$ と書いておく. 正規直交基底 $q_1, \ldots, q_n$ が定める $\mathbb{R}^n$ の直交座標系を $y_1, \ldots, y_n$ と書くことにする. 座標系 y_i で見れば直交変換 A は次のように見える:

- A の作用は $y_1, \ldots, y_{r_1}$ を何も変えない.
- A の作用は $y_{r_1+1}, \ldots, y_{r_1+r_2}$ を -1 倍する.
- A の作用は $y_{r_1+r_2+2k-1} y_{r_1+r_2+2k}$ 平面を右回りに角度 θ_k だけ回転する $(k = 1, \ldots, s)$.

問題 [**199**] の結果は任意の直交変換に対してこのような便利な直交座標系を選ぶことができることを意味している. 線形代数の基本は便利な基底を選んでその基底を用いて線形写像を調べることである.

[**302**] 任意の $A \in SO(3)$ はある軸の回りをある角度だけ回転させる直交変換を表現している. □

解説: この問題の結果はまさに $SO(3)$ の元は回転を表現していることを意味している. □

ヒント: 問題 [**199**] の結果より, 任意の $A \in SO(3)$ に対してある直交行列 Q と実数 θ で

$$Q^{-1}AQ = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}$$

を満たすものが存在することがわかる. □

[**303**] $O(n)$ は弧状連結でない[50]. 同様に $GL_n(\mathbb{R})$ も弧状連結でない. □

ヒント: $E, S = \mathrm{diag}(-1, 1, \ldots, 1) \in O(n)$ である. もしも連続写像 $C : [0,1] \to O(n)$ で $C(0) = E$, $C(1) = S$ を満たすものが存在したとすれば, $\det C(0) = 1$ でかつ $\det C(1) = -1$ なので, 中間値の定理より, ある $t \in [0,1]$ が存在して $\det C(t) = 0$ となる. しかし, $C(t)$ は正則行列なのでそうはならない. よって矛盾. □

21.6 鏡映変換

任意に 0 でないベクトル $a \in \mathbb{R}^n$ を取る. a に垂直な超平面 H_a が次のように定義される:

$$H_a = \{\, x \in \mathbb{R}^n \mid \langle a, x \rangle = 0 \,\}.$$

超平面 H_a に関する**鏡映 (reflection)** $S_a : \mathbb{R}^n \to \mathbb{R}^n$ が次のように定義される[51]:

$$S_a(x) = x - \langle a^\vee, x \rangle a, \qquad a^\vee := \frac{2a}{||a||^2} = \frac{2a}{\langle a, a \rangle}.$$

[**304**] この S_a が実際に「鏡映」と呼ぶべき変換になっていることを図を描いて直観的に説明せよ. □

[50] E と $\mathrm{diag}(-1, 1, \ldots, 1)$ を $O(n)$ 内の連続的な曲線で結ぶことができないことを示せ.

[51] $a^\vee$ という記号法は **ルート系 (root system)** の理論における標準的な記号法である. ルート系に関しては谷崎 [Tn] などの Lie 代数の教科書を参照せよ.

ヒント: 単位ベクトル p を $p = a/||a||$ と定めると

$$S_a(x) = S_p(x) = x - 2\langle p, x\rangle p \qquad (x \in \mathbb{R}^n).$$

$\langle p, x\rangle$ はベクトル x の直線 $\{\, tp \mid t \in \mathbb{R} \,\}$ への射影の長さの ± 1 倍に一致している. □

[305] 鏡映 S_a は線形変換であり, 任意の $x, y \in \mathbb{R}^n$ に対して $\langle S_a(x), S_a(y)\rangle = \langle x, y\rangle$. すなわち鏡映変換 S_a は直交変換である. □

ヒント: 上の $S_a(x) = S_p(x) = x - 2\langle p, x\rangle p$ という表示を利用せよ. □

[306] 単位ベクトル p を $p = {}^t[p_1 \ \cdots \ p_n] := a/||a||$ と定める. このとき, 鏡映変換 S_a の行列表示は次のようになることを示せ:

$$S_a = E - 2p\,{}^tp = \begin{bmatrix} 1-2p_1p_1 & -2p_1p_2 & -2p_1p_3 & \cdots & -2p_1p_n \\ -2p_2p_1 & 1-2p_2p_2 & -2p_2p_3 & \cdots & -2p_2p_n \\ -2p_3p_1 & -2p_3p_2 & 1-2p_3p_3 & \cdots & -2p_3p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -2p_np_1 & -2p_np_2 & -2p_np_3 & \cdots & 1-2p_np_n \end{bmatrix}.$$

これが直交行列であることを直接的計算で確かめてみよ. □

ヒント: 行列表示がこうなることを示すためには $(E - 2p\,{}^tp)x = x - 2\langle p, x\rangle p$ を示せば良いが, ほとんど明らかである. (もしくは, S_p の行列表示が上の行列になっていることは $S_p(e_j)$ が上の行列の第 j 列ベクトルに一致していることを確かめても良い.) 直交行列であることは ${}^t(E - 2p\,{}^tp)(E - 2p\,{}^tp) = E$ を示せば良いが, $1 = ||p||^2 = {}^tpp$ であるから簡単である. 次の問題も参照せよ. □

[307] n 次実対称行列 A が $A^2 = A$ を満たしているならば $E - 2A$ は直交行列である. □

参考: $A^2 = A$ を満たしている行列の固有値は 1 または 0 である. よって, $A^2 = A$ を満たしている n 次実対称行列 A に対して, ある直交行列 P が存在して $P^{-1}AP = \mathrm{diag}(1, \ldots, 1, 0, \ldots, 0)$ となる. 1 の個数を k とし, P の第 j 列ベクトルを p_j と書くことにすると, A は $p_1, \ldots, p_k$ で張られる部分ベクトル空間への直交射影の行列表現になっていることがわかる. このとき $P^{-1}(E - 2A)P = \mathrm{diag}(-1, \ldots, -1, 1, \ldots, 1)$ であり, $\det(E - 2A) = (-1)^k$ (k は A の固有値 1 の重複度) が成立する. (この事実を用いて上の問題の結果を証明できるが, そんなことをしなくても直接的に証明可能であるのでそうして欲しい.) □

[308] 0 でない任意のベクトル $a \in \mathbb{R}^n$ に対して, ある直交行列 P が存在して

$$P^{-1}S_aP = \begin{bmatrix} E_{n-1} & 0 \\ 0 & -1 \end{bmatrix}.$$

特に $\det S_a = -1$ である. □

ヒント: $p_n = a/||a||$ を含む $\mathbb{R}^n$ の正規直交基底 $p_1, \ldots, p_n$ を任意に取ると, $S_a(p_i) = p_i$ $(i = 1, \ldots, n-1)$, $S_a(p_n) = -p_n$ となる. そのとき $P = [p_1 \ \cdots \ p_n]$ と置くと $S_aP = P\,\mathrm{diag}(1, \ldots, 1, -1)$. □

[309] $\alpha_i = e_i - e_{i+1} \in \mathbb{R}^n$ $(i = 1, \ldots, n-1)$ と置く. このとき $\alpha_i^\vee = 2\alpha/\langle a, a\rangle = \alpha_i$ であり,

$$[a_{ij}]_{i,j=1}^{n-1} := [\langle \alpha_i^\vee, \alpha_j \rangle]_{i,j=1}^{n-1} = \begin{bmatrix} 2 & -1 & & & 0 \\ -1 & 2 & -1 & & \\ & -1 & 2 & \ddots & \\ & & \ddots & \ddots & -1 \\ 0 & & & -1 & 2 \end{bmatrix}.$$

この行列を A_{n-1} 型の Cartan 行列と呼ぶ. $S_i = S_{\alpha_i}$ $(i = 1, \ldots, n-1)$ と置く. このとき,

$$S_i(\alpha_j) = \alpha_j - \alpha_i a_{ij} \qquad (i, j = 1, \ldots, n-1).$$

よって $\alpha_1, \ldots, \alpha_{n-1}$ で張られる格子[52] は S_i の作用で閉じている. さらに次も成立している:

$$\begin{aligned} &S_i^2 = E \qquad (i = 1, \ldots, n-1), \\ &S_i S_{i+1} S_i = S_{i+1} S_i S_{i+1} \qquad (i = 1, \ldots, n-2), \\ &S_i S_j = S_j S_i \qquad (|i-j| \geq 2). \quad \square \end{aligned}$$

ヒント: ベクトル x の第 i 成分を x_i と書くと, S_i の x への作用は x_i 成分と x_{i+1} 成分の交換になっている. よって i と $i+1$ を交換する互換を $s_i = (i, i+1)$ と書けば, 鏡映 S_i たちは s_i たちと同じ関係式を満たしている. $\square$

解説: 実は上の問題の結果は置換群を鏡映によって忠実に表現できることを意味している. しかも $\det S_i = -1$ なので, 置換群の元 $\sigma = s_{i_1} \cdots s_{i_l}$ に対して対応する置換行列を $S_\sigma = S_{i_1} \cdots S_{i_l}$ と定めると $\det S_\sigma = \operatorname{sgn} \sigma$ が成立している. すなわち置換群の元の signature は対応する置換行列の行列式に一致している. $\square$

参考: 隣り合わせの数の交換の繰り返しで数の並びを自由に変えることができるので, n 次の置換群 S_n は $s_i = (i, i+1)$ $(i = 1, \ldots, n-1)$ から生成される[53]. 実はこの事実は阿弥陀籤 (あみだくじ) によって任意の置換を作り出せることと同値である. あみだくじによる抽選は, 縦線を上から下に進み, 横線があればその先の隣りの縦線に移るという操作によって行なわれる. あみだくじの中の i 番目の縦線と $i+1$ 番目の縦線のあいだの横線はまさに s_i の役目を果たしているのである. あみだくじが定める置換の signature はあみだくじの横線の個数が偶数ならば 1 で奇数ならば -1 である.

実は目で見易くするためには横線部分をバッテンに描き直した方が良い. さらにバッテンを線が上下に交差しているように描き直せば**組紐 (braid)** の世界が出現する. (この意味がよくわからない人は質問してくれれば詳しく説明する.) 左上から右下への線と右上から左下への線の交差の上下はどれも同じ (たとえば前者が常に上で後者が常に下) であるとして, $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ に対応する図を描いてみよ. 左辺と右辺はひもを連続的にずらすことによって互いに移り合うことがわかる. この関係式は組紐において最も重要かつ基本的な関係式である.

---

[52] $\alpha_1, \ldots, \alpha_{n-1}$ で張られる**格子 (lattice)** とは

$$\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_{n-1} = \{\, k_1\alpha_1 + \cdots + k_{n-1}\alpha_{n-1} \mid k_1, \ldots, k_{n-1} \in \mathbb{Z} \,\}$$

という集合のことである. この集合は和と差で閉じている. この格子は A_{n-1} 方の root 格子と呼ばれている. (各 α_i は単純 root と呼ばれている.)

[53] S_n の任意の元は有限個の s_i たちの積で表わされる.

この意味で $s_is_{i+1}s_i = s_{i+1}s_is_{i+1}$ という関係式を**組紐関係式 (braid relation)** と呼ぶことがある. この関係式は数理物理学における解ける模型 (可解模型) と書く関係しているので, 画期的な仕事をした 2 人の物理学者の名を取って **Yang-Baxter 関係式**と呼ぶこともある.

「くみひも」や「あみだくじ」のような日常生活に登場するものは実は数学的にも基本的でかつ重要な対象なのである. □

22 体上の 1 変数多項式環における Euclid の互除法

実は Jordan 標準形の理論は本質的に体上の 1 変数多項式環の理論である. すでに Cayley-Hamilton の定理[54] の有用さから行列の理論では多項式が重要な役目を果たしていることがなんとなく想像できるだろう.

22.1 体について

この辺で少し気分を変えて, K は任意の**体 (field)** であるとし, K 係数の多項式や K 上のベクトル空間について考えることにする[55].

ここでは体の定義について詳しく説明しない. 体の定義を知らない人は K は実数体 $\mathbb{R}$ または $\mathbb{C}$ であると考えて良い. たとえば K^n と書いてあれば $\mathbb{R}^n$ または $\mathbb{C}^n$ であると解釈して良い. そうしたい人は以下を読まずに先に進んで良い[56].

しかし, 基礎的な体の例として $\mathbb{R}$ や $\mathbb{C}$ 以外にどのようなものがあるかについて少しだけ説明しておく. 新たな抽象概念を学ぶときには, その概念に合致する基礎的かつ重要な例には具体的にどのようなものがあるかを調べておく必要がある[57].

有理数体 $\mathbb{Q}$ も基礎的でかつ重要な体である. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ のような体では 1 つ以上の 1 の和 $1+\cdots+1$ が 0 になることはない. そのような体は**標数 0 (of characteristic 0)** であるという. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は標数 0 の体である.

体 K が**正標数 (of positive characteristic)** であるとは K の中の 1 つ以上の 1 の和 $1+\cdots+1$ のどれかが 0 になることである. 0 になる $1+\cdots+1$ の最小の長さをその体の**標数 (characteristic)** と呼ぶ. 正標数の体の標数は素数 $2, 3, 5, 7, 11, \ldots$ のどれかになることが知られている.

各素数 p に対して集合

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$$

に足し算と掛け算の p で割った余りによって定義することによって自然に体の構造を入れることができる. たとえば, 4 を 3 で割った余りは 1 なので, $\mathbb{F}_3 = \{0, 1, 2\}$ において

[54] Hamilton-Cayley の定理と呼んでいる文献も多い.

[55] K の元を成分に持つ (m, n) 型行列全体の集合を $M_{m,n}(K)$ と書くことにする. 特に n 次正方行列全体の集合を $M_n(K) = M_{n,n}(K)$ と表わす. さらに正則行列 $A \in M_n(K)$ 全体の集合を $GL_n(K)$ と表わす. n 個の K の元が縦に並べた縦ベクトル全体の集合を K^n と書くことにする. $K^n = M_{n,1}(K)$ とみなせる. よって $A \in M_n(K)$ と $v \in K^n$ の積 $Av \in K^n$ が定義され, A は K 上のベクトル空間 K^n の一次変換を定める. すべて $K = \mathbb{R}, \mathbb{C}$ の場合と同様であると考えて良い.

[56] もちろん筆者は読んで欲しいと思いながら書いている.

[57] 代数学が何を研究する分野であるかを知るためにはシャファレヴィッチ [Sh] がおすすめである.

$2+2=2\cdot 2=1$ である. $\mathbb{F}_p$ の標数は p になる (p 個の 1 の和を p で割った余りは 0). $\mathbb{F}_p$ のように有限個の元で構成される体を**有限体 (finite field)** と呼ぶ. 有限体も重要な基礎な体である.

実数全体の集合 $\mathbb{R}$ は有理数全体の集合 $\mathbb{Q}$ を絶対値に関して完備化することによって構成される. 実は通常の絶対値ではなく, 各素数 p に対して p を因子としてたくさん含んでいればいるほど 0 に近付くような絶対値 (付値と呼ばれる) に関して $\mathbb{Q}$ を完備化することによって, p 進体 $\mathbb{Q}_p$ を構成することができる. 集合として $\mathbb{Q}_p$ は次のように表示できる:

$$\mathbb{Q}_p = \{\, a_n p^n + a_{n+1}p^{n+1} + a_{n+2}p^{n+2} + \cdots \mid n \in \mathbb{Z},\ a_i = 0, 1, \ldots, p-1 \,\}.$$

実数体 $\mathbb{R}$ には無限個の仲間 $\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7, \mathbb{Q}_{11}, \ldots$ が存在する. 実は 20 世紀の数学の発展によってこれらは非常に仲が良いことが知られている.

$\mathbb{C}$ は $\mathbb{R}$ に $i=\sqrt{-1}$ を付け加えることによって構成される. これと同じ構成を $\mathbb{Q}$ に対して適用すると Gauss 体 $\mathbb{Q}(i)$ が得られる. 他にも $\mathbb{Q}(\sqrt{2})$ のような体を考えることもできる.

体 K が**代数閉体 (algebraically closed field)** であるとは K 係数の任意の代数方程式 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ ($n \geq 1$, $a_i \in K$) の根が K の中に存在することである.

代数学の基本定理の主張は「複素数体 $\mathbb{C}$ は代数閉体である」である. この演習ではこの結果を自由に用いて良い.

有理数係数のある代数方程式 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ ($n \geq 1$, $a_i \in \mathbb{Q}$) の根になっているような複素数を**代数的数 (algebraic number)** と呼び, そうでない複素数を**超越数 (transcendental nuber)** と呼ぶ. たとえば $\sqrt{2}$ は無理数だが代数的数であり, $e = 2.718281828\cdots$ や $\pi = 3.141592653\cdots$ は超越数である.

代数的数全体の集合 $\overline{\mathbb{Q}}$ は代数閉体になることを示せる[58]. $\overline{\mathbb{Q}}$ を $\mathbb{Q}$ の**代数閉包 (algebraic closure)** と呼ぶ.

実は任意の体 K に対してその代数閉包 $\overline{K}$ が存在する. すなわち K を含むある代数閉体 $\overline{K}$ が存在して, その任意の元は K 係数のある代数方程式の根になっている. この結果は後で体の理論を習ったときに証明される. この演習ではこの結果を証明抜きで自由に使って良い.

たとえば有限体 $\mathbb{F}_p$ の代数閉包 $\overline{\mathbb{F}}_p$ は $\mathbb{F}_p$ に 1 の巾根をすべて付け加えることによって構成可能である. 任意の $e = 1, 2, 3, \ldots$ に対して $\overline{\mathbb{F}}_p$ は部分体で元の個数が $q = p^e$ 個であるものが唯一存在する. それを $\mathbb{F}_q$ と書き, 位数 q の有限体と呼ぶ.

大体において以上に登場したような体が基礎的であり, 他の体はそれらから出発して様々な手続きによって構成される.

まとめ: よく登場する基礎的な体には, 実数体 $\mathbb{R}$, 複素数体 $\mathbb{C}$ の他に有理数体 $\mathbb{Q}$, p 進体 $\mathbb{Q}_p$, 有理数体の代数閉包 $\overline{\mathbb{Q}}$, 有限体 $\mathbb{F}_q$, 有限体の代数閉包 $\overline{\mathbb{F}}_p$ などが存在する.

[310] 任意の $\alpha \in \mathbb{C}$ に対して $\mathbb{Q}$ と α を含む $\mathbb{C}$ の最小の部分体を $\mathbb{Q}(\alpha)$ と書くことにする. m は平方数でない整数であるとし, $\alpha = \sqrt{m}$ と置く. このとき $\mathbb{Q}(\alpha)$ は 1 と α を基底に持つ $\mathbb{Q}$ 上のベクトル空間になっている. そして, α の積はそのベクトル空間に $\mathbb{Q}$ 上の一次変換を定める. 基底 $(1, \alpha)$ に関するその一次変換の行列表示は $\begin{bmatrix} 0 & m \\ 1 & 0 \end{bmatrix}$ になる. □

[58] この結果は後で体の理論を習ったときに証明されることになる.

ヒント: $\mathbb{Q}(\alpha)$ は $\mathbb{Q}$ と α を含み四則演算で閉じている. 特に $\mathbb{Q}+\mathbb{Q}\alpha \subset \mathbb{Q}(\alpha)$ である. ところが $\mathbb{Q}+\mathbb{Q}\alpha$ も四則演算で閉じているので体をなす. よって $\mathbb{Q}(\alpha)$ の最小性より $\mathbb{Q}+\mathbb{Q}\alpha = \mathbb{Q}(\alpha)$ である. α は有理数でないので 1 と α は $\mathbb{Q}$ 上一次独立である. $\alpha\cdot 1 = 0\cdot 1 + 1\cdot\alpha$ でかつ $\alpha\cdot\alpha = m\cdot 1 + 0\cdot\alpha$. □

有限体上の理論では「点の個数を数える」問題が重要である[59].

[311] $GL_n(\mathbb{F}_q) = \{\, A \in M_n(\mathbb{F}_q) \mid \det A \neq 0 \,\}$ の元の個数は幾つか? □

ヒント: $GL_n(\mathbb{F}_q)$ は $\mathbb{F}_q^n$ の基底 $(v_1,\dots,v_n)$ 全体の集合と同一視できる. v_1 として $\mathbb{F}_q^n$ の任意の 0 でない任意のベクトルを取れるので, v_1 の取り方は q^n-1 通りある. v_1 が与えられたとき, v_2 として v_1 で張られる 1 次元の部分空間に含まれない任意のベクトルが取れるので, v_2 の取り方は q^n-q 通りある. v_1, v_2 が与えられたとき, v_3 として v_1, v_2 で張られる 2 次元の部分空間に含まれない任意のベクトルが取れるので, v_3 の取り方は q^n-q^2 通りある. ····· □

解: $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{n^2}\prod_{i=1}^{n}(1-q^{-i})$. □

22.2 Euclid の互除法

この節では K は任意の体であるとする. 「任意の体」という言葉を使うのが怖い人は $K=\mathbb{R}$ または $\mathbb{C}$ であると考えて良い.

$f = f(\lambda)$ が K **を係数に持つ** λ **に関する多項式 (polynomial in** λ **with coefficients in** K**)** であるとは f が次のような式であることである[60]:

$$f(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0, \quad a_i \in K.$$

この f が $a_n \neq 0$ を満たしているとき, f の**次数 (degree)** は n であると言い, $\deg f = n$ と置く. ただし $f=0$ の場合は例外的に $\deg f = -\infty$ と定める. K を係数に持つ多項式は K **上の多項式 (polynomial over** K**)** と呼ばれる場合もある.

K を係数の持つ λ に関する多項式全体の集合は $K[\lambda]$ と表わされる. $K[\lambda]$ の 2 つの元には自然に和と差と積が定義される[61]. $K[\lambda]$ に和と差と積の構造を入れたものは K **上の** λ **に関する多項式環 (polynomial ring in** λ **over** K**)** と呼ばれている.

多項式環 $K[\lambda]$ の最重要な性質は割り算によって商と余りを計算できることである[62].

[312] 任意の $f, g \in K[\lambda]$ に対して $g \neq 0$ ならばある $q, r \in K[\lambda]$ で次を満たすものが一意に存在する:

$$f = qg + r, \qquad \deg r < \deg g.$$

[59] 岩波数学辞典などで「Weil 予想」について調べてみよ. 驚くべきことに有限体上の幾何において「点の個数を数える」ことは実数を用いた通常の幾何における「トポロジーを調べる」ことに対応している. 驚くべきことに有限体上の幾何のような離散的な世界においてもトポロジーの直観が適用可能なのである.

[60] 少々ラフな説明の仕方だがこれで意味はわかるだろう.

[61] これもラフな説明だが大学入学前の数学の勉強ですでにどういう意味なのか知っているはずである.

[62] そのような割り算が可能な環は Euclid 整域 (Euclidean domain) と呼ばれている. 有理整数環 $\mathbb{Z}$ も Euclid 整域である. Euclid 整域は単項イデアル整域 (principal ideal domain) の典型的な例になっている. これらの事実は環論の初歩として後で習うことになる. しかし, 環論の初歩において大学入学以前に習った整数や多項式の世界が極めて基本的かつ重要な役割を果たすことである. 後で体の Galois 理論について習うときにも 1 変数多項式環に関する基本的な結果が基本的かつ重要な役割を果たす.

q を f **を** g **で割った商 (quotient of** f **divided by** g**)** と呼び, r を f **を** g **で割った余り (remainder of** f **divided by** g**)** と呼ぶ. □

$h \in K[\lambda]$ が $f_1, \ldots, f_n \in K[\lambda]$ の**最大公約元 (greatest common divisor, g.c.d.)** であるとは h が $f_1, \ldots, f_n$ の公約元でかつ h が $f_1, \ldots, f_n$ の任意の公約元で割り切れることである.

[313] $f_1, \ldots, f_n \in K[\lambda]$ の最大公約元が存在するならば 0 でない K の元による定数倍を除いて一意に定まる. □

ヒント 1: $g, h \in K[\lambda]$ はともに 0 でない $f_1, \ldots, f_n \in K[\lambda]$ の最大公約元であると仮定する. もしも $\deg g < \deg h$ ならば g が h で割り切れることがないので矛盾する. よって $\deg g = \deg h$ である. h は g で割り切れるのである $a \in K$ $(a \neq 0)$ が存在して $h = ag$ となる. □

ヒント 2: 0 でない $K[\lambda]$ の元で逆数が $K[\lambda]$ の中に含まれるものは 0 でない K の元に限るという事実を使う. f_i がすべて 0 ならば 0 が最大公約元になる. f_i の中に 0 でないものが存在すると仮定する. そのとき 0 は f_i たちの公約元にならない. $g, h \in K[\lambda]$ はともに $f_1, \ldots, f_n \in K[\lambda]$ の最大公約元であると仮定する. $g \neq 0$, $h \neq 0$ である. ある $a, b \in K[\lambda]$ が存在して $h = ag$, $g = bh$ である. よって $h = ag = abh$ であるから $ab = 1$ である. したがって $a, b \in K$ かつ $a \neq 0$, $b \neq 0$ である. □

解説: ヒント 1 は多項式の次数の概念を用いているが簡単でわかり易い. ヒント 2 は一般の環 (より正確には整域) に適用できる議論である. □

割り算ができる環では最大公約元を **Euclid の互除法 (Euclidean algorithm)** で求めることができる.

[314] (Euclid の互除法) $f, g \in K[\lambda]$, $g \neq 0$ に対して, f_k $(k = 0, 1, 2, \ldots)$ を以下の手続きによって定めることができる:

- $f_0 = f$, $f_1 = g$ と定める.
- もしも $f_k \neq 0$ ならば $q_k, f_{k+1} \in K[\lambda]$ を次の条件によって定める:

$$f_{k-1} = q_k f_k + f_{k+1}, \qquad \deg f_{k+1} < \deg f_k.$$

- もしも $f_{k+1} = 0$ すなわち $f_{k-1} = q_k f_k$ ならば手続きを終了する.

$\deg f_k$ は単調に減少するのでこの手続きは必ず有限ステップで終了する. $f_{k-1} = q_k f_k$ のとき f_k は f, g の最大公約元になっている. □

ヒント: 上の手続きの結果以下のような計算の列が得られる:

$$\begin{aligned}
&f_0 = f, \\
&f_1 = g \neq 0, \\
&f_0 = q_1 f_1 + f_2, && \deg f_2 < \deg f_1, \\
&f_1 = q_2 f_2 + f_3, && \deg f_3 < \deg f_2, \\
&\quad \cdots\cdots && \quad \cdots\cdots
\end{aligned}$$

$$f_{k-2} = q_{k-1}f_{k-1} + f_k, \qquad \deg f_k < \deg f_{k-1},$$
$$f_{k-1} = q_k f_k.$$

これを下から逆順に眺め直すと f_k は $f_{k-1}, f_{k-2}, \ldots, f_1, f_0$ すべての約元[63] になっていることがわかる．もしも $h \in K[\lambda]$ が f_0, f_1 の公約元ならば各ステップの等式を $f_j = f_{j-2} - q_{k-1}f_{k-1}$ と書き直して上から順に見て行けば h は $f_0, f_1, \ldots, f_{k-1}, f_k$ すべての約元になっていることもわかる．□

[315] $K = \mathbb{R}$ のとき $f(\lambda) = \lambda^4 + \lambda^3 + 2\lambda^2 + \lambda + 1$, $g(\lambda) = \lambda^3 - 1$ の最大公約元を Euclid の互除法と素因子分解の両方の方法で求めてそれらが定数倍を除いて一致していることを確かめよ．□

略解: $f(\lambda) = (\lambda^2+1)(\lambda^2+t+1)$, $g(\lambda) = (\lambda-1)(\lambda^2+\lambda+1)$ であるから, f, g の最大元は $h(\lambda) = \lambda^2+\lambda+1$ である．一方, $f_0 = f$, $f_1 = g$, $f_2(\lambda) = 2\lambda^2+2\lambda+2$ であり, $f_1(\lambda) = (\frac{1}{2}\lambda - \frac{1}{2})f_2(\lambda)$ であるから, f_2 は f_0, f_1 の最大公約元である．$f_2 = 2h$ である．□

[316] $f, g \in \mathbb{Q}[x]$ を $f(x) = x^4 - 2x^2 + 1$, $g(x) = x^3 - 1$ と定める．素因子分解と Euclid の互除法 **[314]** の 2 つの方法で f と g の最大公約多項式を求め, 0 でない有理数倍を除いて一致していることを確かめよ．□

略解: $f(x) = (x-1)^2(x+1)^2$, $g(x) = (x-1)(x^2+x+1)$ であるから, f と g の最大公約多項式は $x-1$ である．Euclid の互除法で計算すると $f_2(x) = -2x^2+x+1$, $f_3(x) = \frac{3}{4}x - \frac{3}{4}$, $f_4(x) = 0$ となり, 最大公約多項式は $f_3(x) = \frac{3}{4}(x-1)$ であることがわかる．□

[317] $f, g \in \mathbb{Q}[x]$ を $f(x) = (x+2)^2(x^2+x-1)(x^2+1)$, $g(x) = (x-2)(x^2-2)(x^2+1)$ と定める．このとき f と g の最大公約多項式が x^2+1 である．Euclid の互除法 **[314]** で f と g の最大公約多項式を計算すると, 出て来る数字がどんどん大きくなってしまい, 手計算がかなり大変になることを確かめよ．コンピューターを用いて計算しても構わない．その場合はコンピューターをどのように使ったかについても説明すること．□

ヒント: 計算結果は次のようになる．虫食いを埋めよ:

$$f_0(x) = f(x) = x^6 + 5x^5 + \boxed{ア}x^4 + 5x^3 + 3x^2 - 4,$$
$$f_1(x) = g(x) = x^5 - \boxed{イ}x^4 - x^3 + 2x^2 - 2x + 4,$$
$$f_2(x) = 23x^4 + 10x^3 - \boxed{ウ}x^2 + 10x - 32, \qquad q_1(x) = x + 7,$$
$$f_3(x) = \frac{238}{\boxed{エ}}x^3 + \frac{324}{\boxed{エ}}x^2 + \frac{\boxed{カ}}{529}x + \frac{\boxed{キ}}{529}, \qquad q_2(x) = \frac{1}{23}x - \frac{56}{529},$$
$$f_4(x) = -\frac{42320}{14161}x^2 - \frac{42320}{14161}, \qquad q_3(x) = \frac{23}{119}x - \frac{2536}{14161},$$
$$f_5(x) = 0, \qquad q_4(x) = -\frac{1685159}{11193640}x - \frac{1147041}{5596820}. \quad \square$$

[63]「約数」「約元」は英語では共に “divisor” である．

略解: $f_0 = f$, $f_1 = g$ と置き, f_{k-1} を f_k で割った余りを f_{k+1} とし, 商を q_k とする計算の結果は次のようになる:

$$
\begin{aligned}
&f_0(x) = f(x) = x^6 + 5x^5 + 8x^4 + 5x^3 + 3x^2 - 4,\\
&f_1(x) = g(x) = x^5 - 2x^4 - x^3 + 2x^2 - 2x + 4,\\
&f_2(x) = 23x^4 + 10x^3 - 9x^2 + 10x - 32, \qquad q_1(x) = x + 7,\\
&f_3(x) = \frac{238}{529}x^3 + \frac{324}{529}x^2 + \frac{238}{529}x + \frac{324}{529}, \qquad q_2(x) = \frac{1}{23}x - \frac{56}{529},\\
&f_4(x) = -\frac{42320}{14161}x^2 - \frac{42320}{14161}, \qquad q_3(x) = \frac{23}{119}x - \frac{2536}{14161},\\
&f_5(x) = 0, \qquad q_4(x) = -\frac{1685159}{11193640}x - \frac{1147041}{5596820}.
\end{aligned}
$$

f_4 が f, g の最大公約多項式である. □

[318] 2 つの整数 $m, n \in \mathbb{Z}$ の最大公約数も Euclid の互除法で計算できることを示せ. □

[319] 2 つの多項式 $f, g \in K[\lambda]$ の最大公約元を $d \in K[\lambda]$ とすると, ある多項式 $a, b \in K[\lambda]$ で $d = af + bg$ を満たすものが存在する. □

ヒント 1: Euclid の互除法を使う. Euclid の互除法のステップを上から順番に見て行き, $d = f_k = af_0 + bf_1 = af + bg$ という式が得られることを示す. □

ヒント 2: まず, $I = K[\lambda]f + K[\lambda]g = \{\, af + bg \mid a, b \in K[\lambda] \,\}$ と置き[64], I に含まれる 0 でない多項式の中で次数が最小のものを h とすると $I = K[\lambda]h = \{\, ch \mid c \in K[\lambda] \,\}$ であることを示す. これより h が f, g の最大公約元であることが導かれる. 任意に $p \in I$ を取り p を h で割った余り r を考えると, $r \in I$ かつ $\deg r < \deg h$ なので h の次数の最小性より $r = 0$ である. すなわち I の任意の元は h で割り切れる. よって $I = K[\lambda]h$ であり, 特に f, g は h で割り切れる. 一方 $h \in I$ より $h = af + bh$ $(a, b \in K[\lambda])$ と書けるので, h は f, g の任意の公約元で割り切れる. よって h は f, g の最大公約元である. □

解説: 上の 2 つのヒントはどちらも重要である. ヒント 1 の方法はアルゴリズムを与えているが, ヒント 2 の方法はそうではない. しかし, ヒント 2 の方法はアルゴリズムを直接扱う複雑さがないので一般的な議論に適している. □

[320] 2 つの多項式 $f, g \in K[\lambda]$ が互いに素[65] であるならば, 任意の $b \in K[\lambda]$ に対してある $a \in K[\lambda]$ で $\deg a < \deg g$ かつ $af \equiv b \mod g$ を満たすものが一意に存在する[66]. □

ヒント: 問題 **[319]** の結果より, ある $p, q \in K[\lambda]$ で $1 = pf + qg$ を満たすものが存在する. よって $b = bpf + bqg \equiv bpf \mod g$ である. よって a を bq を g で割った余りとすれば存在が示される. 一意性は以下のようにして示される. ある $p \in K[\lambda]$ で $pf \equiv 1 \mod g$ を満たすものが存在する. よって $a, c \in K[\lambda]$ が $af \equiv cf \equiv b \mod g$ を満たしているならば p をかけて $a \equiv c$ (g) である. よって a, c の次数がともに g の次数より小さいならば $a = c$ である. □

---

[64] I を f, g から生成される $K[\lambda]$ のイデアル (ideal) と呼び (f, g) のように表わす. このヒントの議論は実質的に $K[\lambda]$ が単 項イデアル整域であることの証明と単項イデアル整域において $(f, g) = (h)$, $h = \gcd(f, g)$ であることの証明を含んでいる.

[65] 最大公約元が 1 であるということ.

[66] $f \equiv g \mod h$ は f を h で割った余りと g を h で割った余りが等しいという意味である.

[321] 2 つの整数 $m, n \in \mathbb{Z}$ の最大公約数を $d \in \mathbb{Z}$ とすると, ある整数 $a, b \in \mathbb{Z}$ で $d = am + bn$ を満たすものが存在する.

ヒント: 問題 **[319]** とほとんど同じ. □

[322] 2 つの整数 $m, n \in \mathbb{Z}_{>0}$ が互いに素[67] であるならば, 任意の整数 $b \in \mathbb{Z}$ に対してある $a \in \mathbb{Z}$ で $0 \leq a < n$ かつ $am \equiv b \mod n$ を満たすものが一意に存在する. □

ヒント: 問題 **[321]** の結果を使う. 問題 **[320]** とほとんど同じ. □

次の問題の結果はよく使われる.

[323] $f_1, \ldots, f_n \in K[\lambda]$ の最大公約元を $d \in K[\lambda]$ とすると, ある $a_1, \ldots, a_n \in K[\lambda]$ で $d = a_1 f_1 + \cdots + a_n f_n$ を満たすものが存在する. □

ヒント 1: n に関する帰納法. $n = 1$ の場合は明らか. $f_1, \ldots, f_{n-1}$ の最大公約元 g と f_n の最大公約元 h は $f_1, \ldots, f_{n-1}, f_n$ の最大公約元である. 実際, h は $f_1, \ldots, f_{n-1}, f_n$ の公約元であり, $f_1, \ldots, f_{n-1}, f_n$ の任意の公約元で h は割り切れる. 帰納法の仮定より g は $g = b_1 f_1 + \cdots + b_{n-1} f_{n-1}$ $(b_i \in K[\lambda])$ と表わされる. 問題 **[319]** より h は $h = c_1 g + c_2 f_n$ $(c_i \in K[\lambda])$ と表わされる. よって, $a_i = c_1 b_i$ $(i = 1, \ldots, n-1)$, $a_n = c_2$ と置けば $h = a_1 f_1 + \cdots + a_n f_n$ が成立する. □

ヒント 2: まず, $I = \sum_{i=1}^{n} K[\lambda] f_i$ と置き, I に含まれる 0 でない多項式の中で次数が最小のものを h とすると $I = K[\lambda]h$ が成立することを示す. このとき h は f_i たちの最大公約元であることが示される. 問題 **[319]** のヒント 2 とまったく同様の議論を繰り返せ. □

[324] $m_1, \ldots, m_N \in \mathbb{Z}$ の最大公約数を $d \in \mathbb{Z}$ とすると, ある $a_1, \ldots, a_N \in K[\lambda]$ で $d = a_1 m_1 + \cdots + a_N m_N$ を満たすものが存在する. □

22.3 Lagrange の補間公式

[325] $f, g \in K[\lambda]$ はともに次数が $n-1$ 以下であるとする. このとき互いに異なる n 個の $\alpha_1, \ldots, \alpha_n \in K$ について $f(\alpha_i) = g(\alpha_i)$ $(i = 1, \ldots, n)$ が成立しているならば $f = g$ である. □

ヒント 1: $h = a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_{n-1}\lambda^{n-1} = f - g$ と置いて $h = 0$ を示せば良い. $h(\alpha_i) = 0$ $(i = 1, \ldots, n)$ は剰余定理より, h が $\lambda - \alpha_i$ $(i = 1, \ldots, n)$ のすべてで割り切れることと同値である. よって h は $(\lambda - \alpha_1) \cdots (\lambda - \alpha_n)$ で割り切れる. そのとき h の次数は $n-1$ 以下だと仮定したので $h = 0$ である. □

[67] 最大公約数が 1 であるということ.

ヒント 2: $h(\alpha_i)=0$ $(i=1,\dots,n)$ は次と同値である:

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} = 0.$$

左辺の n 次正方行列の行列式は Vandermonde の公式

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1\le i<j\le n} (\alpha_j-\alpha_i).$$

より 0 ではない. よって $a_0=a_1=a_2=\cdots=a_n=0$ すなわち $h=0$ となる. □

[326] $p_1,\dots,p_r$ は互いに異なる N 個の素数であるとし, $N=p_1\cdots p_r$ と置く. $m,n\in\mathbb{Z}$ はともに 0 以上 N 未満の整数であるとする. このとき $m\equiv n \mod p_i$ $(i=1,\dots,r)$ ならば $m=n$ である. □

[327] $\alpha_1,\dots,\alpha_n\in K$ は互いに異なると仮定し, $f\in K[\lambda]$ を

$$f(\lambda)=(\lambda-\alpha_1)\cdots(\lambda-\alpha_n)$$

と定める. このとき, $f(\lambda)/(\lambda-\alpha_i)\in K[\lambda]$ $(i=1,\dots,n)$ は定数以外に共通の因子を持たないので, 1 はそれらの最大公約元である. 次の公式が成立している:

$$\sum_{i=1}^{n} \frac{1}{f'(\alpha_i)}\frac{f(\lambda)}{\lambda-\alpha_i}=1 \qquad \left(\text{すなわち}\quad \frac{1}{f(\lambda)}=\sum_{i=1}^{n}\frac{1}{f'(\alpha_i)}\frac{1}{\lambda-\alpha_i}\right).$$

たとえば, 互いに異なる $\alpha,\beta,\gamma\in K$ に対して,

$$\frac{(\lambda-\beta)(\lambda-\gamma)}{(\alpha-\beta)(\alpha-\gamma)}+\frac{(\lambda-\alpha)(\lambda-\gamma)}{(\beta-\alpha)(\beta-\gamma)}+\frac{(\lambda-\alpha)(\lambda-\beta)}{(\gamma-\alpha)(\gamma-\beta)}=1,$$

$$\frac{1}{(\lambda-\alpha)(\lambda-\beta)(\lambda-\gamma)}$$
$$=\frac{1}{(\alpha-\beta)(\alpha-\gamma)}\frac{1}{\lambda-\alpha}+\frac{1}{(\beta-\alpha)(\beta-\gamma)}\frac{1}{\lambda-\beta}+\frac{1}{(\gamma-\alpha)(\gamma-\beta)}\frac{1}{\lambda-\gamma}.$$ □

ヒント: $\phi_i(\lambda)=f(\lambda)/[f'(\alpha_i)(\lambda-\alpha_i)]\in K[\lambda]$ と置くと, $\phi_i(\alpha_i)=1$ かつ $j\neq i$ のとき $\phi_i(\alpha_j)=0$. あとは $p(\alpha_i)=1$ $(i=1,\dots,n)$ を満たす次数が $n-1$ 以下の多項式が 1 に限ることを示すために問題 **[325]** を使う. □

[328] (Lagrange の補間公式) $\alpha_1,\dots,\alpha_n\in K$ は互いに異なると仮定し, $f\in K[\lambda]$ を

$$f(\lambda)=(\lambda-\alpha_1)\cdots(\lambda-\alpha_n)$$

と定める. このとき, 任意の $b_1, \ldots, b_n \in K$ に対して多項式

$$p(\lambda) = \sum_{i=1}^{n} \frac{b_i}{f'(\alpha_i)} \frac{f(\lambda)}{\lambda - \alpha_i}$$

は $p(\alpha_i) = b_i$ $(i = 1, \ldots, n)$ を満たしている次数が $n-1$ 以下の唯一の多項式である. この結果は **Lagrange の補間公式 (Lagrange's interpolation formula)** と呼ばれている. たとえば, 互いに異なる $\alpha, \beta, \gamma \in K$ と任意の $a, b, c \in K$ に対して,

$$p(\lambda) = a\frac{(\lambda-\beta)(\lambda-\gamma)}{(\alpha-\beta)(\alpha-\gamma)} + b\frac{(\lambda-\alpha)(\lambda-\gamma)}{(\beta-\alpha)(\beta-\gamma)} + c\frac{(\lambda-\alpha)(\lambda-\beta)}{(\gamma-\alpha)(\gamma-\beta)}$$

は $p(\alpha) = a$, $p(\beta) = b$, $p(\gamma) = c$ を満たす次数が 3 以下の唯一の多項式である. □

ヒント: 唯一性の証明には問題 **[325]** の結果を使う. 問題 **[327]** のヒントを見よ. □

[329] 体 K の標数は 0 であると仮定する[68]. $\alpha \in K$ と $n \in \mathbb{Z}_{>0}$ を任意に取る. このとき, 多項式 $f \in K[\lambda]$ が

$$f^{(\nu)}(\alpha) = 0 \quad (\nu = 0, 1, \ldots, n-1)$$

を満たすための必要十分条件は f が $(\lambda - \alpha)^n$ で割り切れることである. □

ヒント: 十分性は $(\lambda-\alpha)^n g(\lambda)$ を微分してみればすぐにわかる[69]. 必要性は n に関する帰納法で以下のようにして示される. $n = 1$ の場合は剰余定理より成立する. $n > 1$ で $n-1$ まで成立しているならば $f(\lambda) = (\lambda-\alpha)^{n-1} g(\lambda)$ $(g \in K[\lambda])$ と書ける. その両辺を $n-1$ 回微分して λ に α を代入すると $0 = f^{(n-1)}(\alpha) = (n-1)!g(\alpha)$ となる. K の標数は 0 なので K の中で $(n-1)! \neq 0$ なので $g(\alpha) = 0$ が成立する. そのとき剰余定理より g は $\lambda - \alpha$ で割り切れる. □

[330] K の標数が正であるとき, ある $f \in K[\lambda]$ で $f \neq 0$ かつ $f' = 0$ となるものが存在する. □

ヒント: $f(\lambda) = g(\lambda)^p$. さらに詳しい解説を読みたければ体論について解説してある任意の代数学の教科書における分離多項式の解説を参照せよ. □

[331] 体 K の標数は 0 であると仮定する[70]. 互いに異なる $\alpha_1, \ldots, \alpha_s \in K$ と $n_1, \ldots, n_s \in \mathbb{Z}_{>0}$ を任意に取り, $n = n_1 + \cdots + n_s$ と置く. このとき, 任意の $b_{i,\nu} \in K$ $(i = 1, \ldots, s,$ $\nu = 0, 1, \ldots, n_i - 1)$ に対して, ある多項式 $p \in K[\lambda]$ で次数が $n-1$ 以下でかつ

$$p^{(\nu)}(\alpha_i) = b_{i,\nu} \qquad (i = 1, \ldots, s,\ \nu = 0, 1, \ldots, n_i - 1)$$

を満たすものが唯一存在する. ここで $p^{(\nu)}$ は p の ν 階の導函数である. □

---

[68] 「標数 0 の体」という言葉を知らない人は $K = \mathbb{C}$ と仮定して良い.
[69] $k > 0$ のとき f が $(\lambda-\alpha)^k$ で割り切れるならば f' は $(\lambda-\alpha)^{k-1}$ で割り切れる.
[70] 「標数 0 の体」という言葉を知らない人は $K = \mathbb{C}$ と仮定して良い.

ヒント 1: $f(\lambda)=(\lambda-\alpha_1)^{n_1}\cdots(\lambda-\alpha_s)^{n_s}$ と置く. 唯一性は「すべての $b_{i,\nu}$ が 0 ならば条件を満たす p が 0 になる」ことに帰着する. すべての $b_{i,\nu}$ が 0 ならば問題 **[329]** の結果より, p は $(\lambda-\alpha_i)^{n_i}$ $(i=1,\ldots,s)$ のすべてで割り切れる. よって p は f で割り切れる. p の次数は $n-1$ 以下であると仮定したので $p=0$ でなければいけない. 存在は以下のように示される. K は標数 0 なので $b_i\in K[\lambda]$ を次のように定めることができる:

$$b_i(\lambda)=b_{i,0}+b_{i,1}(\lambda-\alpha_i)+\frac{1}{2!}b_{i,2}(\lambda-\alpha_i)^2+\cdots+\frac{1}{(n_i-1)!}b_{i,n_i-1}(\lambda-\alpha_i)^{n_i-1}.$$

この b_i は $b_i^{(\nu)}(\alpha_i)=b_{i,\nu}$ を満たしている. よって p の満たすべき等式は

$$p(\lambda)\equiv b_i(\lambda)\mod(\lambda-\alpha_i)^{n_i}\qquad(i=1,\ldots,s)$$

と同値である[71]. $f_i(\lambda)=f(\lambda)/(\lambda-\alpha_i)^{n_i}$ と置く. f_i と $(\lambda-\alpha_i)^{n_i}$ は互いに素なので問題 **[320]** の結果より, ある $a_i\in K[\lambda]$ が存在して $a_if_i\equiv b_i \mod(\lambda-\alpha_i)^{n_i}$ となる. このとき, $p=a_1f_1+\cdots+a_sf_s$ は上の満たすべき条件を満たしている. p の次数が n 以上ならば f で割った余りを改めて p とすれば良い. □

ヒント 2: $a_if_i\equiv b_i \mod(\lambda-\alpha_i)^{n_i}$ を満たす多項式 a_i の具体形を以下のように計算することができる. $\lambda=\alpha_i$ で正則な λ の有理式 $b_i(\lambda)/f_i(\lambda)$ の $\lambda-\alpha_i$ に関する巾級数展開を次のように書いておく:

$$\frac{b_i(\lambda)}{f_i(\lambda)}=a_{i,0}+a_{i,1}(\lambda-\alpha_i)+\cdots+a_{i,\nu}(\lambda-\alpha_i)^{\nu}+\cdots.$$

ここで,

$$a_{i,\nu}=\frac{1}{\nu!}\left[\frac{d^\nu}{d\lambda^\nu}\frac{b_i(\lambda)}{f_i(\lambda)}\right]_{\lambda=\alpha_i}\qquad(\nu=0,1,2,\ldots).$$

多項式 $a_i(\lambda)$ を上の展開における最初の n_i 項の和と定める:

$$a_i(\lambda)=a_{i,0}+a_{i,1}(\lambda-\alpha_i)+\cdots+a_{i,n_i-1}(\lambda-\alpha_i)^{n_i-1}\qquad(i=1,\ldots,s).$$

この $a_i(\lambda)$ は $a_i(\lambda)f_i(\lambda)\equiv b_i(\lambda) \mod(\lambda-\alpha_i)^{n_i}$ を満たしている. しかもこのとき $p=a_1f_1+\cdots+a_sf_s$ の次数は $n=n_1+\cdots+n_s$ 未満である. □

解説: ヒント 2 の方法を使えば $a_{i,\nu}$ たちが α_i と $b_{i,\nu}$ たちの $\mathbb{Q}$ 上の有理式で表わせることもわかる ($b_{i,\nu}$ については線形). 特に n_i がすべて 1 の場合の具体的な公式が Lagrange の補間公式 **[328]** である. ヒント 2 の方法によって得られる結果は Lagrange の補間公式の一般化になっており, **Lagrange-Sylvester の補間公式**と呼ばれている. □

定理 22.1 (Lagrange-Sylvester の補間公式) K は標数 0 の体であるとする. 互いに異なる $\alpha_1,\ldots,\alpha_s\in K$ と $n_1,\ldots,n_s\in\mathbb{Z}_{>0}$ を任意に取り, $f\in K[\lambda]$ を

$$f(\lambda)=(\lambda-\alpha_1)^{n_1}\cdots(\lambda-\alpha_s)^{n_s}$$

と定め, $n=\deg f=n_1+\cdots+n_s$ と置く. 各 $i=1,\ldots,s$ に対して次数が n_i 未満の多項式 $b_i\in K[\lambda]$ を任意に取る. このとき, 次数が n 未満の多項式 $p\in K[\lambda]$ で

$$p^{(\nu)}(\alpha_i)=b_i^{(\nu)}(\alpha_i)\qquad(i=1,\ldots,s,\ \nu=0,1,\ldots,n_i-1)$$

[71] $b_{i,\nu}$ たちから $b_i(\lambda)$ を構成するためだけに K の標数が 0 であるという仮定を使った. 最初から $b_i(\lambda)$ を与えて問題を定式化し直せば標数 0 という仮定は必要でなくなる. 正標数の世界では $n!$ で自由に割ることができなくなるので微分を用いた議論が色々うまく行かなくなる.

を満たすものが唯一存在する. しかも p は次の表示を持つ:

$$p(\lambda) = \sum_{i=1}^{s} \sum_{\nu=0}^{n_i-1} \frac{1}{\nu!} \left[\frac{d^\nu}{d\lambda^\nu} \frac{b_i(\lambda)}{f_i(\lambda)} \right]_{\lambda=\alpha_i} \frac{f(\lambda)}{(\lambda-\alpha_i)^{n_i-\nu}}. \quad \square$$

[332] $N \in \mathbb{Z}_{>0}$ とし, その素因数分解を $N = p_1^{n_1} \cdots p_s^{n_s}$ と表わす. ここで p_i は互いに異なす素数であり, $n_i \in \mathbb{Z}_{>0}$ である. このとき, 任意の $b_{i,\nu} \in \{0, 1, \ldots, p_i - 1\}$ $(i = 1, \ldots, s,$ $\nu = 0, 1, \ldots, n_i - 1)$ に対して, ある $m \in \mathbb{Z}$ で 0 以上 N 未満でかつ

$$m \equiv b_{i,0} + b_{i,1} p_i + b_{i,2} p_i^2 + \cdots + b_{i,n_i-1} p_i^{n_i-1} \mod p_i^{n_i}$$

を満たすものが唯一存在する. $\square$

ヒント: $b_i = b_{i,0} + b_{i,1} p_i + b_{i,2} p_i^2 + \cdots + b_{i,n_i-1} p_i^{n_i-1}$ と置くと b_i は 0 以上 $p_i^{n_i}$ 未満である[72]. $N_i = N/p_i^{n_i}$ と置くと N_i たちの最大公約数は 1 なので問題 **[324]** の結果より, 任意の整数 m は $m = a_1 N_1 + \cdots + a_s N_s$ $(a_i \in \mathbb{Z})$ と表わされる[73]. m が $m \equiv a_i N_i \equiv b_i \mod p_i^{n_i}$ $(i = 1, \ldots, s)$ を満たしていれば m を N で割った余り (0 以上 N 未満の整数に取る) も同じ条件を満たしている. よって m がその条件を満たすように a_i たちを取れることを示せば良い. しかし, N_i と $p_i^{n_i}$ は互いに素なので問題 **[322]** の結果より $a_i N_i \equiv b_i \mod p_i^{n_i}$ を満たす $a_i \in \{0, 1, \ldots, p_i^{n_i} - 1\}$ が一意に存在する. $\square$

[333] 互いに異なる $\alpha, \gamma \in K$ に対して $\lambda - \gamma$ と $(\lambda - \alpha)^2$ は互いに共通因子を持たないので, 1 はそれらの最大公約元である. 次が成立する:

$$\frac{\lambda-\gamma}{\alpha-\gamma} - \frac{(\lambda-\alpha)(\lambda-\gamma)}{(\alpha-\gamma)^2} + \frac{(\lambda-\alpha)^2}{(\gamma-\alpha)^2} = 1,$$

$$\frac{1}{(\lambda-\alpha)^2(\lambda-\gamma)} = \frac{1}{\alpha-\gamma}\frac{1}{(\lambda-\alpha)^2} - \frac{1}{(\alpha-\gamma)^2}\frac{1}{\lambda-\alpha} + \frac{1}{(\gamma-\alpha)^2}\frac{1}{\lambda-\gamma}.$$

この公式が問題 **[327]** の終わりの 2 つの公式から $\beta \to \alpha$ の極限で得られることを示せ[74]. $\square$

22.4 1 変数有理函数の部分分数展開

体 K 上の λ に関する有理函数 (rational function in λ over K) とは K 上の λ に関する多項式の分数式 (有理式) のことである. それら全体の集合を $K(\lambda)$ と表わす:

$$K(\lambda) = \{\, g/f \mid f, g \in K,\ f \neq 0 \,\}.$$

$K(\lambda)$ は体をなすので体 K 上の λ に関する有理函数体と呼ばれている[75].

---

[72] 実は $b_{i,\nu}$ を持ち出したのは問題 **[331]** との類似を見易くするためにそうしただけであり, 本質的な意味はない. b_i さえあれば十分である.

[73] 問題 **[324]** の結果より, ある $c_i \in \mathbb{Z}$ が存在して $1 = c_1 N_1 + \cdots + c_s N_s$ となる. これの両辺に m をかければ良い.

[74] この場合の極限は純代数的に扱うこともできるが, $K = \mathbb{R}, \mathbb{C}$ と考えて問題を解いても良い.

[75] 有理函数は有理数に似ており, $\sqrt{\lambda^2+1}$ のような無理函数 (代数函数の一種) は $\sqrt{2}$ のような無理数 (代数的数の一種) に似ており, $\log \lambda$ のような超越函数は π のような超越数に似ている. このように函数の世界と数の世界のあいだには類似関係がある. このような見方は非常に基本的でありかつ重要である. なぜならばこのような見方をすれば函数の世界と数の世界のどちらか片方で開発された方法や直観がもう一方にも適用できるかもしれないという考え方ができるようになるからである.

[334] $K(\lambda)$ の部分集合 $\{1, \lambda, \lambda^2, \dots\}$ と $\left\{ \frac{1}{\lambda-\alpha}, \frac{1}{(\lambda-\alpha)^2}, \frac{1}{(\lambda-\alpha)^3}, \dots \right\}$ $(\alpha \in K)$ たちの和集合は K 上一次独立である. □

ヒント: λ^i $(i = 0, 1, 2, \dots)$, $(\lambda-\alpha)^{-j}$ $(\alpha \in K, j = 1, 2, 3, \dots)$ たちの K 上での一次結合 f が 0 ならば一次結合の係数も 0 であることを示せば良い. もしも一次結合の中に 0 でない $a_j(\lambda-\alpha)^{-j}$ のような項が含まれているならばそのような最大の j を取って, $(\lambda-\alpha)^j f(\lambda)$ の λ に α を代入すれば $a_j = 0$ となって矛盾する. よって $f = 0$ は λ^i $(i = 0, 1, 2, \dots)$ の一次結合でなければいけない. しかしその一次結合の中に 0 でない係数が存在すれば 0 でない多項式ができてしまうので矛盾する. よって一次結合の係数はすべて 0 でなければいけない. □

[335] (有理函数の部分分数展開) 次数が $n \geq 0$ のモニックな[76]多項式 $f \in K[\lambda]$ と $m \geq n$ に対して, K 上の m 次元ベクトル空間 V を次のように定める:

$$V = \{\, g/f \in K(\lambda) \mid g \in K[\lambda],\ \deg g < m \,\}.$$

f は次のように一次式の積に分解されると仮定する[77]:

$$f(\lambda) = (\lambda - \alpha_1)^{n_1} \cdots (\lambda - \alpha_s)^{n_s}.$$

ここで α_i は f の相異なる根であり, $n = n_1 + \cdots + n_s$ である. このとき V は次の集合 B を基底に持つ:

$$B = \{1, \lambda, \dots, \lambda^{m-n-1}\} \cup \bigcup_{i=1}^{s} \left\{ \frac{1}{\lambda-\alpha_i}, \frac{1}{(\lambda-\alpha_i)^2}, \cdots, \frac{1}{(\lambda-\alpha_i)^{n_i}}. \right\}$$

したがって任意の有理式 $h \in K(\lambda)$ は次の形で一意的に表わされる:

$$h(\lambda) = q(\lambda) + \sum_{i=1}^{s} \left[\frac{a_{i,1}}{\lambda-\alpha_i} + \frac{a_{i,2}}{(\lambda-\alpha_i)^2} + \cdots + \frac{a_{i,n_i}}{(\lambda-\alpha_i)^{n_i}} \right].$$

ここで $q \in K[\lambda]$ でかつ $a_{i,\nu} \in K$ であり, $\alpha_1, \dots, \alpha_s \in K$ は互いに異なる. さらに q は h の分子を h の分母で割った余りになる. □

ヒント: B は V の部分集合である. B の元の個数は m に等しい. 問題 **[334]** より B の張る K 上のベクトル空間の次元は V の次元の m に等しい. これらの事実から B が V の基底になることがわかる. □

[336] (有理数の部分分数展開) 任意の有理数 $h \in \mathbb{Q}$ は次の形で一意的に表わされる:

$$h = q + \sum_{i=1}^{s} \left[\frac{a_{i,1}}{p_i} + \frac{a_{i,2}}{p_i^2} + \cdots + \frac{a_{i,n_i}}{p_i^{n_i}} \right].$$

ここで $q \in \mathbb{Z}$ でかつ $a_{i,\nu} \in \{0, 1, \dots, p_i - 1\}$ であり, $p_1, \dots, p_s \in K$ は互いに異なる素数である. □

[76] 最高次の係数が 1 であるという意味.
[77] $K = \mathbb{C}$ もしくはより一般に K が代数閉体であればこの仮定が成立している.

ヒント: 有理数 h は $h = g/f$, $g \in \mathbb{Z}$, $f = p_1^{n_1} \cdots p_s^{n_s}$ と表わすことができる. $f_i = f/p_i^{n_i}$ と置くと, f_i と $p_i^{n_i}$ は互いに素であるから, 問題 [**322**] の結果より $a_i f_i \equiv g \mod p_i^{n_i}$ を満たす $a_i \in \{0, 1, \ldots, p_i^{n_i} - 1\}$ が一意に存在する. 0 以上 $p_i^{n_i}$ 未満の整数 a_i は

$$a_i = a_{i,1} p_i^{n_i - 1} + a_{i,2} p_i^{n_i - 2} + \cdots + a_{i,n_i - 1} p_i + a_{i,n_i}, \quad a_{i,\nu} \in \{0, 1, \ldots, p_i - 1\}$$

と一意に表示できる[78]. $c = a_1 f_1 + \cdots + a_s f_s$ と置くと $c \equiv g \mod f$ である. よって $g = qf + c$ $(q \in \mathbb{Z})$ と書ける. この両辺を f で割れば部分分数展開表示の存在が示される. 部分分数展開表示の一意性については自分で考えてみよ. □

[**337**] 有理函数の部分分数展開 [**335**] を用いて Lagrange の補間公式 [**328**] を証明せよ. □

ヒント: Lagrange の補間公式の設定は問題 [**335**] の $s = n$, $n_1 = \cdots = n_s = 1$, $m = n$ の場合の設定に等しい. よって次数が $n - 1$ 次以下の任意の $p \in K[\lambda]$ に対して p/f は次の形で一意的に表わされる:

$$\frac{p(\lambda)}{f(\lambda)} = \frac{a_1}{\lambda - \alpha_1} + \cdots + \frac{a_n}{\lambda - \alpha_n}, \qquad a_i \in K.$$

両辺に $f(\lambda)$ をかけて $\lambda = \alpha_i$ と置けば

$$p(\alpha_i) = a_i f_i(\alpha_i) = a_i f'(\alpha_i).$$

ここで $f_i(\lambda) = f(\lambda)/(\lambda - \alpha_i)$ である. よって $a_i = p(\alpha_i)/f'(\alpha_i)$ となる. □

[**338**] K が代数閉体であるとき[79], 有理函数の部分分数展開 [**335**] を用いて, よく使われる問題 [**323**] の結果を証明せよ. □

ヒント: K は代数閉体であると仮定したので各 f_i は一次式の積に分解される. f_i たちを最大公約元 d で同時に割っておくことにすれば $d = 1$ の場合だけを考えれば良いことがわかる. f_i たちの最小公倍元 f に対して, $1/f$ を部分分数展開して, その両辺に f をかければ 1 を f_i たちの多項式倍の和で表わす式が得られる. □

以上によって, K が代数閉体のとき, よく使われる問題 [**323**] の結果について少なくとも 3 通りの証明が存在することがわかった:

- Euclid の互除法を使う方法 (問題 [**323**] のヒント 1),
- 単項イデアルの考え方を使う方法 (問題 [**323**] のヒント 2),
- 部分分数展開を使う方法 (K が代数閉体の場合, 上の問題のヒント).

[78] これを a_i の p_i 進展開と呼ぶ. a_i を p_i で割った余りが a_{i,n_i} になり, その商をさらに p_i で割った余りが a_{i,n_i-1} になる. 以下同様に $a_{i,\nu}$ を求めて行けば p_i 進展開表示の存在が示される.

[79] 「代数閉体」という言葉が怖い人は $K = \mathbb{C}$ と仮定してよい.

23 一般固有空間分解と Jordan 標準形

この節では佐武 [St] の方針にしたがって Jordan 標準形の存在の証明の解説を演習問題の羅列によって行なうことにする[80]. その方針は以下の通りである:

1. まず正方行列の Jordan 分解 (互いに可換な半単純行列と巾零行列の和への分解) の存在を証明する.
2. それと同時に一般固有分解が証明される. よって Jordan 標準形を求める問題は巾零行列の標準形を求める問題に帰着される.
3. 巾零行列の標準形の存在を証明する.
4. Jordan 標準形の一意性を証明する.

問題 [**158**] の計算問題が解けるようになることを第一の目標にせよ. 計算ができるようになったら Jordan 標準形の存在と一意性の証明の理解に挑戦せよ.

[**339**] **(問題 [158] への補足)** 問題 [**158**] の A_i の最小多項式 $\varphi_i(\lambda)$ を求めよ. 最小多項式の定義については第 23.4 節を参照せよ. □

ヒント: 固有値がすべて整数になるように問題を作ってある. がんばって計算しましょう. □

略解: 以下のように J_i, P_i を定めると $P_i^{-1}A_iP_i = J_i$ である:

$$J_1 = \begin{bmatrix} -2 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad J_2 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad J_3 = \begin{bmatrix} -2 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$P_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ -2 & -1 & 0 & 1 \\ -2 & -1 & -3 & 0 \\ 1 & 0 & -1 & 1 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 3 & 0 & 4 & 2 \\ 6 & -1 & 4 & 4 \\ 0 & 2 & 9 & 0 \\ 2 & -1 & -2 & 1 \end{bmatrix}, \quad P_3 = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & 3 & 1 & 1 \\ -1 & 0 & 0 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix},$$

$$J_4 = \begin{bmatrix} -2 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad J_5 = \begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad J_6 = \begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},$$

[80] Jordan 標準形の存在の証明には少なくとも 3 通りの方法がある.

1 つ目は行列の Jordan 分解 (互いに可換な半単純行列と巾零行列の和への分解) と巾零行列の標準形の存在を直接証明するという方法である. この 1 つ目の方法は佐武 [St] 第 IV 章や杉浦 [Sg] 第 1 章などで解説されている.

2 つ目は行列の有理標準形を経由する方法である. 有理標準形とは問題 [**375**] で定義されているコンパニオン行列 $C_1, \ldots, C_t$ を対角線に並べた形に行列でもとの行列と相似でかつ $p_{C_1} \mid \cdots \mid p_{C_t}$ を満たすもののことである. もとの行列から四則演算のみを用いて有理標準形は計算される. この 2 つ目の方法は韓・伊理 [KI] の第 3.2 節で解説されている.

3 つ目は単因子論を使う方法である. 単因子論は本質的に 1 変数多項式環上の有限生成加群の構造論に同値なので, この方法は環と加群の理論の応用であるとみなせる. この 3 つ目の方法の解説は堀田 [H2] の第 3 章と第 4 章が良い. 堀田 [H1] も参照せよ.

3 つのどれも数学的に重要である. しかし本質的に 2 つ目の方法と 3 つ目の方法は同類だとみなすことができる.

$$P_4 = \begin{bmatrix} -1 & 0 & -2 & -1 \\ 2 & 1 & 5 & 2 \\ 0 & 2 & 3 & 0 \\ 2 & -1 & 1 & 1 \end{bmatrix}, \quad P_5 = \begin{bmatrix} 4 & 3 & 2 & 1 \\ 3 & 3 & 2 & 1 \\ 2 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \qquad P_6 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ -2 & -1 & 1 & 1 \\ -2 & -1 & -3 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

A_i の最小多項式を $\varphi_i(\lambda)$ と書くと,

$$\varphi_1(\lambda) = (\lambda+2)^3(\lambda-2), \quad \varphi_2(\lambda) = (\lambda+1)(\lambda-1), \quad \varphi_3(\lambda) = (\lambda+2)^2(\lambda-1),$$
$$\varphi_4(\lambda) = (\lambda+2)^2(\lambda-1)^2, \quad \varphi_5(\lambda) = (\lambda+1)^2, \qquad \varphi_6(\lambda) = (\lambda+1)^2,$$

A_5 と A_6 の最小多項式は等しいのに Jordan 標準形は異なることに注意せよ. そのようなことは 3 次行列では起こり得ない. 3 次以下の行列では最小多項式だけで Jordan 標準形がわかってしまう. □

計算問題の作り方: 上のような問題を作るのときには, まず正則行列 P を色々作る. Jordan 標準形 J を任意に用意して $A = PJP^{-1}$ を計算して「A の Jordan 標準形を求めよ」とすれば計算問題のいっちょあがりである. 問題は逆行列の計算が易しい P を系統的に生成することである. 逆行列の分母には $\det P$ が登場する. だから A を整数だけで構成された行列にしたければ分母の $\det P$ が 1 であることが望ましい. その場合は逆行列の計算も易しくなる.

行列式が 1 の n 次正方行列全体の集合 $SL_n(K)$ は群をなし, その任意の元は $E + aE_{ij}$ $(a \in K, i \neq j)$ の形の行列を有限個かけ合わせたもので表わせる. (E_{ij} は (i,j) 成分だけが 1 で他の成分が 0 であるような正方行列であり, 行列単位と呼ばれている.) 成分を整数に制限した $SL_n(\mathbb{Z})$ の場合もその任意の元は $E + nE_{ij}$ $(n \in K, i \neq j)$ の形の行列を有限個かけ合わせたもので表わせる. この事実を使えば整数を成分に持つ行列式が 1 の行列を系統的に生成できる. 実は $SL_n(\mathbb{Z})$ の任意の元は $E \pm E_{i,i+1}$, $E \pm E_{i+1,i}$ の有限個の積で表示できる. □

23.1 巾零行列と半単純行列

K は任意の代数閉体であると仮定し, K の元を成分に持つ行列について考える. K の元を数と呼ぶことがある. 「任意の代数閉体」という言葉を使うのが怖い人は $K = \mathbb{C}$ であると考えてよい.

正方行列 $A \in M_n(K)$ に対して[81] A 巾零であることと半単純であることを次のように定める:

- A が**巾零 (nilpotent)** $\iff$ ある正の整数 k が存在して $A^k = 0$.
- A が**半単純 (semisimple)** $\iff$ A は対角化可能.

ここで A が**対角化可能 (diagonalizable)** であるとはある正則行列 P で $P^{-1}AP$ が対角行列になるものが存在することである. 対角成分が $(\alpha_1, \ldots, \alpha_n)$ であるような対角行列を $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ と表わすことにする.

2 つの正方行列 $A, B \in M_n(K)$ が可換, 同時対角化可能, 同時三角化可能であることを以下のように定義する:

- A と B が可換 $\iff$ $AB = BA$.

[81] $M_n(K)$ は体 K の元を成分に持つ n 次正方行列全体の集合である.

- A と B は同時対角化可能 $\iff$ ある正則行列 P で $P^{-1}AP$ と $P^{-1}BP$ がともに対角行列になるようなものが存在する.
- A と B は同時三角化可能 $\iff$ ある正則行列 P で $P^{-1}AP$ と $P^{-1}BP$ がともに上三角行列になるようなものが存在する.

[340] $P \in GL_n(K)$ のとき[82]以下が成立する:

1. $A \in M_n(K)$ が巾零ならば PAP^{-1} も巾零である.
2. $A \in M_n(K)$ が半単純ならば PAP^{-1} も半単純である. □

[341] 以下を示せ:

1. 上三角行列が巾零であるための必要十分条件は対角成分がすべて 0 になることである.
2. 対角行列は半単純である.
3. 上三角行列でも下三角行列でもない 2 次複素巾零行列が存在する.
4. 対角行列でない 2 次複素半単純行列が存在する.
5. 巾零でも半単純でも上三角でもない 2 次複素正方行列が存在する. □

[342] $A \in M_n(K)$ が巾零でかつ半単純ならば $A = 0$ である. □

ヒント: 巾零ならば固有値は 0 だけである. よって A を対角化すると 0 になる. そのような A は 0 だけである. □

[343] $m+n$ 次正方行列 A を m 次正方行列 B と n 次正方行列 C と (m,n) 型行列 D を用いて $A = \begin{bmatrix} B & D \\ 0 & C \end{bmatrix}$ と定めると, A が巾零であることと B と C の両方が巾零であることは同値である. □

ヒント: A^n は $\begin{bmatrix} B^n & * \\ 0 & C^n \end{bmatrix}$ の形になり, $\begin{bmatrix} 0 & * \\ 0 & 0 \end{bmatrix}$ の形の行列は巾零になる. □

[344] $m+n$ 次正方行列 A を m 次正方行列 B と n 次正方行列 C を用いて $A = \begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix}$ と定めると, A が半単純であることと B と C の両方が半単純であることは同値である. □

ヒント: B と C が半単純ならば m 次正方行列 Q と n 次正方行列 R が存在して $Q^{-1}BQ$ と $R^{-1}CR$ はともに対角行列になるので, Q と R を対角線に並べてできる行列を P とすれば P は A を対角化する. 逆を示すために A は半単純であると仮定し, $m+n$ 次正方行列 P で対角化されていると仮定する. そのとき P の中の列ベクトルを $p_1, \ldots, p_{m+n}$ は A の固有ベクトルになる. 各 p_i を $p_i = \begin{bmatrix} u_i \\ v_i \end{bmatrix}$ $(u_i \in K^m, v_i \in K^n)$ と表わすと u_i は B の

[82] $GL_n(K)$ は K の元を成分に持つ n 次正則行列全体の集合である.

固有ベクトルになり, v_i は C の固有ベクトルになる. 適当に $u_{i_1}, \dots, u_{i_m}$ を選ぶとそれらは K^m の基底をなし, 適当に $v_{j_1}, \dots, v_{j_n}$ を選ぶとそれらは K^n の基底をなす[83]. このとき $Q = [u_{i_1} \ \cdots \ u_{i_m}]$, $R = [v_{j_1} \ \cdots \ v_{j_n}]$ と置けば, Q は B を対角化し, R は C を対角化する. □

[345] $\alpha_1, \dots, \alpha_s \in K$ は互いに異なり, $n = n_1 + \cdots + n_s$, $n_i > 0$ であるとする. n 次対角行列 A を

$$A = \begin{bmatrix} \alpha_1 E_{n_1} & & & 0 \\ & \alpha_2 E_{n_2} & & \\ & & \ddots & \\ 0 & & & \alpha_s E_{n_s} \end{bmatrix}$$

と定める. このとき, n 次正方行列 B が A と可換であるための必要十分条件は B が次の形をしていることである:

$$B = \begin{bmatrix} B_1 & & & 0 \\ & B_2 & & \\ & & \ddots & \\ 0 & & & B_s \end{bmatrix}.$$

ここで B_i は n_i 次正方行列である. □

ヒント: 任意の n 次正方行列 B は (n_i, n_j) 型正方行列 B_{ij} を用いて

$$B = \begin{bmatrix} B_{11} & B_{12} & \cdots & B_{1n} \\ B_{21} & B_{22} & \cdots & B_{2n} \\ \vdots & \vdots & & \vdots \\ B_{n1} & B_{n2} & \cdots & B_{nn} \end{bmatrix}$$

と表わされる. AB と BA を計算して比較してみよ. □

$\alpha \in K$ に対して n 次正方行列 $J_n(\alpha)$ を次のように定める:

$$J_n(\alpha) = \alpha E_n + J_n(0) = \begin{bmatrix} \alpha & 1 & & & 0 \\ & \alpha & 1 & & \\ & & \alpha & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \alpha \end{bmatrix}, \qquad J_n(0) = \begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & 0 \end{bmatrix}.$$

[346] $A \in M_n(K)$ が $J_n(\alpha)$ と可換であるための必要十分条件は A が次の形をしていることである.

$$A = \sum_{k=0}^{n-1} a_k J_n(0)^k = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ & a_0 & a_1 & \ddots & \vdots \\ & & a_0 & \ddots & a_2 \\ & & & \ddots & a_1 \\ 0 & & & & a_0 \end{bmatrix}, \qquad a_i \in K. \quad \square$$

[83] K^{m+n} の任意のベクトルは p_i たちの一次結合になっているので, K^m, K^n の任意のベクトルはそれぞれ u_i たち, v_j たちの一次結合になっている. よって u_i たちから K^m の基底を選び, v_j たちから K^n の基底を選ぶことができる.

ヒント: αE_n は任意の n 次正方行列と可換なので $J_n(0)$ と可換な行列がどのような行列であるかを調べれば良い. □

参考: $J_n(\alpha)$ と可換な行列全体のなす空間の次元は n である. 対角成分に互いに異なる n 個の数が並んでいる任意の n 次対角行列 A に対して, A と可換な行列全体と対角行列全体は一致するので, A と可換な行列全体のなす空間の次元は n になる. 実は「任意に n 次正方行列 A を与えたとき, A と可換な行列全体のなす空間の次元は n 以上になる」ことを証明できる. □

[**347**] $A, B \in M_n(K)$ が可換でかつともに巾零ならば $A+B$ も巾零になる. □

ヒント: A と B が可換ならば $(A+B)^k$ の展開に二項定理を適用できる. □

[**348**] **(同時対角化)** $A, B \in M_n(K)$ が可換でかつともに半単純ならば A と B は同時対角化可能であり, $A+B$ も半単純になる. □

ヒント: A と B が同時対角化可能ならば $A+B$ も対角化可能であることはすぐにわかる. A, B が可換でかつともに半単純ならば同時対角化可能であることは問題 [**344**] と問題 [**345**] を用いて証明される. A は半単純なのである正則行列 P で $P^{-1}AP$ が問題 [**345**] の A の形の対角行列になるものが存在する. そのとき $P^{-1}AP$ と可換な $P^{-1}BP$ は問題 [**345**] の B の形をしている. 問題 [**344**] より, $P^{-1}BP$ の対角線に並ぶ各ブロック B_i も半単純になるのである正則行列 Q_i で対角化される. Q_i たちを対角線に並べてできる行列を Q とする. このとき PQ は A と B を同時対角化する. □

[**349**] 次の行列 A, B を同時対角化せよ:

$$A = \begin{bmatrix} -4 & 15 & -9 \\ -1 & 4 & -3 \\ -1 & 5 & -4 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & -15 & 9 \\ 1 & -7 & 3 \\ 1 & -5 & 1 \end{bmatrix}. \quad \square$$

ヒント: まずどちらか片方をある正則行列 Q で対角化する. すると $Q^{-1}AQ$, $Q^{-1}BQ$ の少なくとも片方は対角行列になっている. 運が良ければ両方同時に対角化されているが, 運が悪い場合には片方の対角線に $(2,2)$ 型のブロックが表われる. それを対角化すれば問題 [**348**] のヒントの方法で同時対角化が終了する. □

略解: 行列 P を次のように定める:

$$P := \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 3 & 1 & 1 \end{bmatrix}, \quad P^{-1} = \begin{bmatrix} 0 & -1 & 1 \\ -1 & 8 & -5 \\ 1 & -5 & 3 \end{bmatrix}.$$

このとき $P^{-1}AP = \mathrm{diag}(-1,-1,-2)$, $P^{-1}BP = \mathrm{diag}(-2,-2,-1)$. □

[**350**] **(同時三角化)** $A, B \in M_n(K)$ が可換ならば A と B は同時三角化可能である. □

ヒント: n に関する帰納法. K は代数閉体だと仮定したので, 特性多項式 $p_A(\lambda) = |\lambda E - A|$ の根 α が K の中に存在する. α に対応する A の固有空間の基底を $v_1, \ldots, v_k$ とし, それを K^n 全体の基底 $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ に拡張する. α に対応する A の固有空間のベクトル v に対して $ABv = BAv = \alpha Bv$ なので Bv も α に対応する A の固有空間に含まれ

る. すなわち B の作用で α に対応する A の固有空間は保たれる. よって $Bq_1, \ldots, Bq_k$ は $q_1, \ldots, q_k$ の一次結合になる. したがって, $V = [v_1 \ \cdots \ v_n]$ と置くと,

$$V^{-1}AV = \begin{bmatrix} \alpha E_k & * \\ 0 & A'' \end{bmatrix}, \quad V^{-1}BV = \begin{bmatrix} B' & * \\ 0 & B'' \end{bmatrix}.$$

ここで B' は k 次の正方行列であり, A'', B'' は $n-k$ 次の正方行列である. しかも, A と B が可換であることより A'' と B'' も可換であることが導かれる. よって帰納法の仮定より, ある k 次正則行列 Q と $n-k$ 次正則行列 R が存在して $Q^{-1}B'Q$, $R^{-1}A''R$, $R^{-1}B''R$ はすべて上三角行列になる. このとき, P を

$$P = V \begin{bmatrix} Q & * \\ 0 & R \end{bmatrix}$$

と定めれば P によって A と B は同時に上三角化される. □

Jordan 標準形の理論にできるだけ早く進みたい人はここから第 23.5 節にジャンプして構わない.

23.2 抽象ベクトル空間について

K は任意の体とする. 「任意の体」という言葉が怖い人は $K = \mathbb{R}$ または $\mathbb{C}$ と考えて良い.

今までこの演習では主として縦ベクトルのベクトル空間とそれに作用するの行列を扱って来た. 次の subsection では一般の抽象ベクトル空間とそれに作用する一次変換を扱う[84]. この subsection は次の subsection への助走である[85].

一般に V が体 K 上の**ベクトル空間 (vector space over K)** もしくは**線形空間 (linear space)** であるとは V は集合であり, 加法 $+ : V \times V \to V$ と零元 $0 \in V$ と加法に関する逆元 $- : V \to V$ と K の元による V の元のスカラー倍 $\cdot : K \times V \to V$ が定めらえていて, 以下のベクトル空間の公理が満たされていることである[86]:

1. V は加法に関して可換群をなす. すなわち $u, v, w \in V$ に対して,
   (a) $(u + v) + w = u + (v + w)$;
   (b) $0 + u = u + 0 = u$;
   (c) $(-u) + u = u + (-u) = 0$;
   (d) $u + v = v + u$.

[84] 代数的な一般論を展開するときには数字が並んでいる縦ベクトルや行列を扱うよりも抽象ベクトル空間や一次変換を扱う方が都合が良い.

[85] したがって説明は完璧ではない.

[86] 一般に K が体ではなく**環 (ring)** の場合は同じ公理系を満たす V は K 上の**加群 (module over K)** もしくは K **加群 (K-module)** と呼ばれる. 加群の方がベクトル空間よりも一般的な述語である. 体 K 上の加群は体 K 上のベクトル空間に等しい. なお一般の環に K という記号を割り振ることは少ない. 英語の ring の頭文字を取って R と書いたり, フランス語の anneau の頭文字を取って A と書くことが多い. 体に F や K という記号が割り振られることが多いのは, 英語で体を field と呼び, ドイツ語では Körper と呼ぶからである.

2. スカラー倍 $\cdot : K \times V \to V$ は結合的かつ**双加法的 (bi-additive)** であり, 1 の積は恒等写像になる. すなわち $a, b \in K$, $u, v \in V$ に対して,

   (a) $(ab)u = a(bu)$;

   (b) $a(u+v) = au + bv$;

   (c) $(a+b)u = au + bu$;

   (d) $1u = u$.

U と V が体 K 上のベクトル空間であるとき, 写像 $f : U \to V$ が**線形写像もしくは一次写像 (linear mapping)** であるとは $a \in K$, $u, u' \in U$ に対して以下の条件を満たしていることである[87]:

1. 加法性　$f(u+u') = f(u) + f(u')$;

2. スカラー倍との可換性　$f(au) = af(u)$.

V からそれ自身への線形写像は V の**線形変換もしくは一次変換 (linear transformation)** と呼ばれる. 線形写像 f の逆写像 f^{-1} が存在するならば f^{-1} も線形写像になる. 逆写像を持つような線形写像を**線形同型写像 (linear isomorphism)** と呼ぶ. 単に**同型写像 (isomorphism)** と呼ぶことも多い.

K 上のベクトル空間 V の部分集合 $\{v_i\}_{i\in I}$ が V の基底であるとは任意の $v \in V$ が $v = \sum_{i\in I} a_i v_i$ ($a_i \in K$, 有限個を除いて $a_i = 0$) と一意に表わされることである[88]. 体上のベクトル空間の理論の出発点になる定理は「任意の体 K 上の任意のベクトル空間 V は基底 $\{v_i\}_{i\in I}$ を持ち, I の濃度は基底の取り方によらず V のみによって一意に決まる」という結果である. V の基底の濃度が有限であるとき V は**有限次元 (finite dimensional)** であると言い, 基底の取り方によらずに決まる基底の元の個数を V の次元と呼び, $\dim V$ もしくは $\dim_K V$ と表わす. 基底の濃度が無限であるとき V は**無限次元 (infinite dimensional)** であると言う. しかし無限次元のベクトル空間の場合は位相を入れて基底の概念を一般化しておかないと不便な場合の方が多い.

以上のように抽象的な定義だけを説明しても何をやりたいのかよくわからないだろう. そこで以下では典型的な例について説明する.

例 23.1 (行列) K^n は体 K 上の n 次元ベクトル空間である. 我々は K^n を縦ベクトルの空間とみなしてきたのであった. 行列の空間 $M_n(K)$ も K 上のベクトル空間であり, その次元は n^2 である. 任意の正方行列 $A \in M_n(K)$ は縦ベクトルとの積によって K^n の一次変換を定めるのであった. しかも, K^n の一次変換は正方行列と一対一に対応しているのであった.

---

[87] 線形写像の定義は幾何的には次のように説明される. 加法性 $f(u+u') = f(u) + f(u')$ は U の中の 4 点 $0, u, u+u' u', 0$ を順次線分で結んでできる平行四辺形が f によって V の中の 4 点 $0, f(u), f(u)+f(u'), f(u'), 0$ を順次線分で結んでできる平行四辺形に移されることを意味している. スカラー倍との可換性 $f(au) = af(u)$ は U の中の直線 $\{au\}_{a\in K}$ が f によって $\{af(u)\}_{a\in K}$ に自然に移されることを意味している. 線形写像は真っ直なものや平らなものを真っ直なものと平らなものに移す. 色々図を描いて線形写像がどのような写像なのかを直観的に理解するように努力せよ.

[88] この定理が成立する環は体だけである. 体以外の環上の加群では基底が取れるとは限らないので状況がずっと複雑になる. 体上のベクトル空間の理論がそれほど難しくないのは基底が取れるからである.

例 23.2 (微分作用素) 実直線上の任意有限回微分可能な複素数値函数全体の集合 $C^\infty(\mathbb{R})$ は自然に $\mathbb{C}$ 上の無限次元ベクトル空間をなす. $f \in C^\infty(\mathbb{R})$ に対してその導函数 $f' \in C^\infty(\mathbb{R})$ を対応させる写像を ∂ と書くことにする. このとき ∂ は $C^\infty(\mathbb{R})$ の一次変換である. 任意有限回微分可能な函数 $a \in C^\infty(\mathbb{R})$ が任意に与えられたとき $f \in C^\infty(\mathbb{R})$ に函数 a と f の積 $af \in C^\infty(\mathbb{R})$ を対応させる写像を乗じられる函数と同じ記号で a と書くことにする. このとき a は $C^\infty(\mathbb{R})$ の一次変換である. ∂ や a のように函数の空間に作用する一次変換は**作用素もしくは演算子 (operator)** と呼ばれることが多い. 次の形の作用素は**常微分作用素 (ordinary differential operator)** と呼ばれている:

$$L = a_N\partial^N + a_{N-1}\partial^{N-1} + \cdots + a_2\partial^2 + a_1\partial + a_0, \qquad a_i \in C^\infty(\mathbb{R}).$$

変数の個数を増やして **偏微分作用素 (partial differential operator)** も同様に定義される. 微分作用素の積 (写像の合成) を $\circ$ と書くことにすると[89],

$$(\partial \circ a - a \circ \partial)f = \partial(af) - a(\partial f) = a'f + af' - af' = a'f,$$
$$\therefore\ \partial \circ a - a \circ \partial = a'$$

となり, ∂ と函数倍 a は作用素として一般に非可換になる[90]. 可換になるのは a が定数である場合だけである. 2 つの行列が一般に非可換になるのと同じように 2 つの微分作用素も一般に非可換になる. 微分作用素は線形写像の重要な例である. □

例 23.3 (積分作用素) 閉区間 $[0,1]$ 上の連続な複素数値函数全体の集合 $C([0,1])$ は自然に $\mathbb{C}$ 上の無限次元ベクトル空間をなす. 閉区間の直積 $[0,1]\times[0,1]$ 常の複素数値連続函数 $K(x,y)$ を任意に取り, 写像 $T_K : C([0,1]) \to C([0,1])$ を次のように定める:

$$(T_K f)(x) = \int_0^1 K(x,y)f(y)\,dy \qquad (f \in C([0,1])).$$

このとき T_K は $C([0,1])$ の一次変換である. T_K は**核函数 (kernel function)** $K(x,y)$ に対応する**積分作用素 (integral operator)** と呼ばれる. 積分作用素も線形写像の重要な例である. n 次正方行列 $K = [k_{ij}]$ と縦ベクトル $f = {}^t[f_1\ \cdots\ f_n]$ の積 Kf の第 i 成分を $(Tf)_i$ と書くと, 行列の積の定義より

$$(Kf)_i = \sum_{i=1}^n k_{ij}f_j \qquad (f = {}^t[f_1\ \cdots\ f_n] \in K^n).$$

この式と上の積分作用素の定義を比較すれば積分作用素は行列の積の定義における有限和を積分に置き換えることによって定義されていることがわかる.

実際には存在しないが, もしも

$$f(x) = \int_0^1 \delta(y-x)f(y)\,dx$$

[89]面倒なので $\circ$ を書かない場合の方が多い.

[90]特別に可換になる場合には数学的に非常に面白いことが起こっている場合が多い. 互いに可換な微分作用素を構成するという問題は重要である. 互いに可換な常微分作用素の組に関しては代数曲面の理論との関係付けることによってかなりよくわかっている. 偏微分作用素の場合に関しては量子可積分系との関係から見て, まだたくさんの面白そうな問題が残っている.

を満たす函数 $\delta(y-x)$ が存在すればそれを核函数に持つ積分作用素は恒等写像になる. $\delta(y-x)$ は函数としては存在しないが, 測度 (measure) もしくくは超函数 (distribution) としては存在する[91]. □

無限次元のベクトル空間の典型的な例は適当な条件を満たす函数全体の空間である. 我々は $V=K^n$ のような有限次元ベクトル空間における直観の多くをある種の函数全体のなす無限次元ベクトル空間にも適用できる. 有限次元のベクトル空間に関する理解は無限次元の場合にも役に立つ. 特に微分作用素や積分作用素に行列に関して学んだ考え方や直観を適用することは生産的である[92].

V が体 K 上のベクトル空間であるとき, V の部分集合 W が加法とスカラー倍で閉じていれば W も自然に体 K 上のベクトル空間とみなせる. そのとき W は V の**ベクトル部分空間 (vector subspace)** もしくは**線形部分空間 (linear subspace)** と呼ばれる. 単に**部分空間 (subspace)** と呼ばれることも多い.

例 23.4 実直線上の複素数値函数全体の集合を V と書くと V は自然に $\mathbb{C}$ 上の無限次元ベクトル空間をなす. 実直線上の複素数値連続函数全体の集合 $W=C(\mathbb{R})$ は V の線形部分空間であり, 実直線上の複素数値連続微分可能函数全体の集合 $U=C^1(\mathbb{R})$ は $W=C(\mathbb{R})$ の線形部分空間である[93]. □

---

[91] $\delta(y-x)$ は実際には (写像の意味での) 函数ではないのに (Dirac の) **デルタ函数 (delta function)** と呼ばれている. 直観的に $\delta(y-x)$ は $y=x$ に無限に近い領域の外で 0 になり, $y=x$ に無限に近い領域では無限大の値を取り, y に関して積分すると 1 になるような "函数" である. Dirac のデルタ函数は Kronecker のデルタの連続版である. Kronecker デルタを成分に持つような行列が単位行列になるのと同じように, Dirac のデルタ函数を核函数に持つ積分作用素は恒等写像になる.

超函数 (distribution) は問題 [**179**] で定義されている急減少 C^∞ 函数の空間 $\mathcal{S}(\mathbb{R})$ に適切な位相を入れたものの**位相的双対空間 (topological dual space)** の元として定義される. 函数空間の位相的双対空間の概念を用いれば函数の概念を手軽にかつ大幅に拡張できる.

函数概念の一般化の仕方にはこの双対空間を用いる Schwartz の方法の他に実領域を複素領域に膨らませることによって複素正則函数の実領域における代数的境界値として超函数 **(hyperfunction)** を定義する佐藤幹夫の方法がある. 実軸は複素上半平面と複素下半平面に挟まれている. 複素上半平面上の正則函数 $F_+(z)$ と複素下半平面上の正則函数 $F_-(z)$ を任意に与えたとき, $f(x)=F_+(x+0i)-F_-(x-0i)$ によって実軸上の佐藤の超函数が定義される. たとえば Dirac のデルタ函数は次のように定義される:

$$\delta(x)=-\frac{1}{2\pi i}\left(\frac{1}{x+0i}-\frac{1}{x-0i}\right).$$

これが $\int_{-\infty}^{\infty}\delta(x)f(x)\,dx=f(0)$ を満たしていることは Cauchy の積分公式を形式的に適用すれば確かめられる. すなわち複素函数論における Cauchy の積分公式を佐藤超函数の視点から眺めなおすと Dirac のデルタ函数が満たすべき公式に見えてしまうのである. 1 変数複素函数論を十分に習得すると 1 変数の佐藤超函数論を大きな困難抜きに理解できるようになる. 多変数の場合には多変数複素函数論が必要になるのでずっと難しい.

なお, 核函数として超函数も許すことにすると微分作用素も積分作用素の形で表わすことができる. たとえば函数 $a(x)$ をかける作用素と x で微分する作用素は

$$\int_{-\infty}^{\infty}\delta(y-x)a(y)f(y)\,dy=a(x)f(x),\qquad -\int_{-\infty}^{\infty}\delta'(y-x)f(y)\,dy=f'(x).$$

と表現される. 後者の公式は形式的に部分積分すれば得られる. これらの公式は超函数論によって厳密な数学として正当化可能である.

[92] もちろん無限次元の場合には有限次元の場合にはない難しさがある. しかしそもそもその困難が無限次元特有の問題であることを認識するためには有限次元の場合に関する知識が不可欠である.

[93] $\mathbb{R}$ 上の複素数値函数は $\mathbb{R}$ の各点ごとに複素数が対応しているので連続無限個の複素数の組だとみなすことができる. しかし実際にはすべての函数をまとめて考えると意味のある議論はできないので, 連続性や微分可能性を仮定したりするので単に無限個の数字が並んでいるだけとはみなせなくなる.

[351] 以上に登場した例のどれか 1 つを詳細に解説してみよ. □

[352] V は複素ベクトル空間であり, H と A は V の一次変換であり, ある $\alpha \in \mathbb{C}$ について $[H, A] = \alpha A$ を満たしているとする[94]. このとき $v \in V$ が H の固有値 β に属する固有ベクトルでかつ $Av \neq 0$ ならば Av は H の固有値 $\alpha + \beta$ に属する固有ベクトルになる. □

ヒント: $[H, A] = \alpha A$ は $HA = A(\alpha + H)$ と書き直される. よって $Hv = \beta v$ ならば $HAv = A(\alpha + H)v = (\alpha + \beta)Av$. □

参考: 固有ベクトル (もしくは函数空間に作用する作用素の固有函数) を具体的に求めるために上の問題の方法は非常によく使われる. その典型例は量子調和振動子 **[180]** の場合である. □

U, V は体 K 上のベクトル空間であるとし, $f : U \to V$ は線形写像であるとする. このとき f の**核 (kernel)** $\operatorname{Ker} f$ と**像 (image)** $\operatorname{Im} f$ が次のように定義される[95]:

$$\operatorname{Ker} f = f^{-1}(0) = \{\, u \in U \mid f(u) = 0 \,\}, \qquad \operatorname{Im} f = f(U) = \{\, f(u) \mid u \in U \,\}.$$

$\operatorname{Ker} f, \operatorname{Im} f$ はそれぞれ U, V の部分空間をなす[96].

[353] 上の設定のもとでさらに U が有限次元ならば

$$\dim U - \dim \operatorname{Ker} f = \dim \operatorname{Im} f. \quad \square$$

結論の直観的な説明[97]: $n = \dim U$ と置く. 線形写像 f は n 次元ベクトル空間 U を k 次元分の方向を潰して V の中に移すとする. そのとき f による U の像の次元は k 次元潰れた分だけ下がって $n - k$ になる. これが上の問題の結論の直観的意味である. 上の問題の結論を書き直した

$$\dim U - \dim \operatorname{Im} f = \dim \operatorname{Ker} f.$$

という式の直観的意味は次のように説明される. 線形写像 f は n 次元ベクトル空間 U を V の中の l 次元の部分空間うつすとする. n 次元が l 次元に移されるためには $n - l$ 次元分の方向をつぶしてうつさなければいけない. たとえば直方体を長方形にうつすためにはある 1 つの方向について潰さなければいけない. 直方体を線分にうつすためには 2 つの方向について潰さなければいけない. その潰す方向の本数が f の核 $\operatorname{Ker} f$ の次元なのである.

ヒント 1: $k = \dim \operatorname{Ker} f$ と置く. $\operatorname{Ker} f$ の基底 $u_1, \ldots, u_k$ を取り, それに $u_{k+1}, \ldots, u_n$ を付け加えて U 全体の基底を構成できる. そのとき $v_i = f(u_{k+i})$ と置くと $v_1, \ldots, v_{n-k}$ は $\operatorname{Im} f$ の基底をなす. □

ヒント 2: 準同型定理 $U/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$ より $\dim \operatorname{Im} f = \dim(U/\operatorname{Ker} f) = \dim U - \dim \operatorname{Ker} f$. □

---

[94] $[H, A] = HA - AH$ である.

[95] 実はさらに**余核 (cokernel)** $\operatorname{Coker} f$ と**余像 (coimage)** $\operatorname{Coim} f$ が次のように定義される:

$$\operatorname{Coker} f = V/\operatorname{Im} f, \qquad \operatorname{Coim} f = U/\operatorname{Ker} f.$$

準同型定理とは「自然な同型 $\operatorname{Coim} f \xrightarrow{\sim} \operatorname{Im} f$ が存在する」という結果のことである.

[96] $\operatorname{Ker} f$ を求める問題は $f(u) = 0$ の形の一次方程式を解くことに対応しており, $\operatorname{Im} f$ を求める問題は u に関する一次方程式 $f(u) = v$ が解を持つような v の全体を求めることに対応している. これらの二種類の一次方程式の理論は線形写像の核と像の理論に集約されることになる.

[97] 論理的な説明と直観的な説明の両方が重要である. 論理と直観は数学をやる上でどちらも不可欠である.

[354] V_i は体 K 上の有限次元ベクトル空間であるとし, 次の線形写像の列を考える:

$$V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{s-1}} V_s \xrightarrow{f_s} V_{s+1}.$$

この列を f_1 から f_i まで合成してできる V_1 から V_k への線形写像を $f_i \circ \cdots \circ f_1$ ($i = 0$ のときは id_{V_1}) と書くことにする. このとき

$$\sum_{i=1}^{s} \dim(\mathrm{Ker}\, f_i \cap \mathrm{Im}(f_{i-1} \circ \cdots \circ f_1)) = \dim \mathrm{Ker}(f_s \circ \cdots \circ f_1).$$

よって,

$$\sum_{i=1}^{s} \dim \mathrm{Ker}\, f_i \geq \dim \mathrm{Ker}(f_s \circ \cdots \circ f_1). \quad \square$$

結論の直観的な説明: 線形写像 $f_1, \ldots, f_s$ によって n 次元ベクトル空間 V_1 を順次潰してより小さな次元のベクトル空間にうつすことを考える. 最終的に潰れる次元 $\dim \mathrm{Ker}(f_s \circ \cdots \circ f_1)$ は各ステップで潰れる次元 $\dim(\mathrm{Ker}\, f_i \cap \mathrm{Im}(f_{i-1} \circ \cdots \circ f_1))$ の総和になる. $\mathrm{Im}(f_{i-1} \circ \cdots \circ f_1)$ は $f_{i-1} \circ \cdots \circ f_1$ でつぶした結果の像であり, $\mathrm{Ker}\, f_i$ は f_i が V_i 全体をどれだけ潰すかを意味している. f_i は $\mathrm{Im}(f_{i-1} \circ \cdots \circ f_1)$ を $\mathrm{Ker}\, f_i \cap \mathrm{Im}(f_{i-1} \circ \cdots \circ f_1)$ の分だけ潰す.

ヒント: $g_i = f_i \circ \cdots \circ f_1$ ($g_0 = \mathrm{id}_{V_1}$) と置く. 問題 **[353]** の結論を $\dim U - \dim \mathrm{Im}\, f = \dim \mathrm{Ker}\, f$ と変形して, f_i の $\mathrm{Im}\, g_{i-1}$ への制限 $f_i|_{\mathrm{Im}\, g_{i-1}} : \mathrm{Im}\, g_{i-1} \to V_{i+1}$ に適用すると

$$\dim \mathrm{Im}\, g_{i-1} - \dim \mathrm{Im}\, g_{i-1} = \dim(\mathrm{Ker}\, f_i \cap \mathrm{Im}\, g_{i-1})$$

となることがわかる. この等式を $i = 1, \ldots, s$ について足し上げると, $\mathrm{Im}\, g_0 = \dim V_1$, $g_s = f_s \circ \cdots \circ f_1$ なので

$$\sum_{i=1}^{s} \dim(\mathrm{Ker}\, f_i \cap \mathrm{Im}\, g_{i-1}) = \dim V_1 - \dim \mathrm{Im}(f_s \circ \cdots \circ f_1) = \dim \mathrm{Ker}(f_s \circ \cdots \circ f_1).$$

$\dim \mathrm{Ker}\, f_i \geq \dim(\mathrm{Ker}\, f_i \cap \mathrm{Im}\, g_{i-1})$ なのでただちに次が導かれる:

$$\sum_{i=1}^{s} \dim \mathrm{Ker}\, f_i \geq \dim V_1 - \dim \mathrm{Im}(f_s \circ \cdots \circ f_1). \quad \square$$

注意: $A \in M_{m,n}(K)$ のとき A が定める線形写像 $A : K^n \to K^m$ について次が成立している:

$$\mathrm{rank}\, A = \dim \mathrm{Im}\, A, \qquad n - \mathrm{rank}\, A = \dim \mathrm{Ker}\, A.$$

この演習の一部に登場した $n - \mathrm{rank}\, A$ という式は $\dim \mathrm{Ker}\, A$ を意味している. $\square$

23.3 固有空間分解

K は任意の体とする. 「任意の体」という言葉が怖い人は $K = \mathbb{R}$ または $\mathbb{C}$ と考えて良い.

K 上のベクトル空間 V がその部分空間 $V_1, \ldots, V_s$ の直和であるとは任意の $v \in V$ が

$$v = v_1 + \cdots + v_s, \qquad v_i \in V_i$$

と一意的に表わされることである[98]. このとき次のように書く:

$$V = \bigoplus_{i=1}^{s} V_i = V_1 \oplus \cdots \oplus V_s = V_1 \dotplus \cdots \dotplus V_s.$$

K 上のベクトル空間 V と V の一次変換 $A : V \to V$ と $\alpha \in K$ に対して, V の部分空間 $V_\alpha = V(A;\alpha)$ を次のように定義する:

$$V_\alpha = V(A;\alpha) = \{\, v \in V \mid Av = \alpha v \,\}.$$

V が A の固有空間の直和に分解するとは

$$V = \bigoplus_{\alpha \in K} V_\alpha = \bigoplus_{\alpha \in K} V(A;\alpha)$$

が成立すること, すなわち任意の $v \in V$ が

$$v = \sum_{\alpha \in K} v_\alpha, \quad (v_\alpha \in V_\alpha \text{ であり, 有限個の } \alpha \in K \text{ を除き } v_\alpha = 0)$$

と一意に表わされることである. $V_\alpha = V(A;\alpha) \neq 0$ のとき $V(A;\alpha)$ は A の**固有空間** と呼ばれ, $V(A;\alpha)$ に含まれる 0 でないベクトルを A の**固有値** α に対応する**固有ベクトル** と呼ぶ.

[355] K 上の 2 変数多項式全体の空間 $V = K[x,y]$ は $A = x\partial/\partial x + y\partial/\partial y$ の固有空間の直和に分解する. □

ヒント: $x^m y^n$ $(m,n \in \mathbb{Z}_{\geq 0})$ は $V = K[x,y]$ の基底である. □

注意: K の標数が 0 ならば $x\partial/\partial x + y\partial/\partial y$ の固有値全体の集合は $\mathbb{Z}_{\geq 0}$ になり, 固有空間はすべて有限次元になる. K の標数が $p > 0$ ならば $x\partial/\partial x + y\partial/\partial y$ の固有値全体の集合は $\mathbb{F}_p = \{0,1,2,\ldots,p-1\}$ になり, 同時固有空間はすべて無限次元になる. □

[356] $\mathbb{R}$ 上の任意有限回微分可能な複素数値函数全体のなす複素ベクトル空間を $C^\infty(\mathbb{R})$ と表わし, その部分空間 $C^\infty(S^1)$ を次のように定義する:

$$C^\infty(S^1) = \{\, f \in C^\infty(\mathbb{R}) \mid f(x+2\pi) = f(x) \ (x \in \mathbb{R}) \,\}.$$

$C^\infty(S^1)$ には内積 $\langle\ ,\ \rangle$ を次のように定めることができる[99]:

$$\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} \overline{f(x)} g(x)\, dx \qquad \big(f, g, \in C^\infty(S^1)\big)$$

$\partial = d/dx$ と $\Delta = -\partial^2$ は $C^\infty(S^1)$ からそれ自身への複素線形写像であり,

$$\langle f, \Delta g \rangle = \langle \Delta f, g \rangle = \langle \partial f, \partial g \rangle, \qquad \langle f, \Delta f \rangle = ||\partial f||^2 \geq 0$$

を満たしている (Δ の半正値 Hermite 性). $C^\infty(S^1)$ に作用する作用素 Δ の固有値と固有函数をすべて求めよ. □

[98] V_i たちの中に $\{0\}$ が混じっていてもこの定義は意味を持っている. $V_i = \{0\}$ ならば V_i のベクトルとして 0 以外に選びようがないのでそのような V_i を除いて考えても直和全体には影響しないが, $V_i = \{0\}$ の場合も含めておく方が良い.

[99] 内積の公理を満たしていることをチェックせよ.

ヒント: $f, g \in C^\infty(S^1)$ に対して部分積分の公式 $\int_0^{2\pi} f(x)g'(x)\,dx = -\int_0^{2\pi} f'(x)g(x)\,dx$ が成立していることを使えば Δ の半正値 Hermite 性を示せる. Δ の半正値 Hermite 性より Δ の固有値は 0 以上の実数になる. 固有値の集合は函数 u に関する微分方程式 $-u'' = \lambda u$ が $C^\infty(S^1)$ の中に解を持つような $\lambda \geq 0$ の全体に一致し, 固有函数はそのときの 0 でない解に一致する[100]. まず微分方程式 $-u'' = \lambda u$ を解き, その解が周期 2π を持つ場合を抽出せよ. □

略解: 固有値全体の集合は $\{n^2\}_{n\in\mathbb{Z}} = \{0, 1, 4, 9, \ldots\}$ である. 固有値 0 に属する固有函数は 1 の定数倍であり, $n \neq 0$ のとき固有値 n^2 に属する固有函数は $e^{\pm nix}$ の一次結合になる. □

[357] V は K 上のベクトル空間であるとし, A は V の一次変換であるとする. $\alpha_1, \ldots, \alpha_s \in K$ は A の相異なる固有値であり[101], α_i に対応する固有空間を V_i と書くことにする. このとき, $v_i \in V_i$ かつ $v_1 + \cdots + v_s = 0$ ならば $v_1 = \cdots = v_s = 0$ である. 特に $\dim V_1 + \cdots + \dim V_s \leq \dim V$ である. □

ヒント: $v_1 + \cdots + v_s = 0$ の両辺に $E, A, A^2, \ldots, A^{s-1}$ を作用させた結果を行列で書くと,

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_s \\ \vdots & \vdots & & \vdots \\ \alpha_1^{s-1} & \alpha_2^{s-1} & \cdots & \alpha_s^{s-1} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_s \end{bmatrix} = 0$$

左辺の正方行列の行列式は Vandermonde の公式より 0 でない. よって $v_1 = \cdots = v_s = 0$ である. このことから V_i の基底の $i = 1, \ldots, s$ に関する和集合は一次独立になることが示される. よって $\dim V_1 + \cdots + \dim V_s \leq \dim V$ である. □

[358] $A \in M_n(K)$ を $V = K^n$ の一次変換とみなすとき, A が対角化可能であることと V が A の固有空間の直和に分解することは同値である. □

ヒント: A が対角化可能であるならばある正則行列 P で $P^{-1}AP$ が対角行列になるものが存在する. そのとき P の中の列ベクトル $p_1, \ldots, p_n$ は A の固有ベクトルだけで構成された K^n の基底になっている. 固有値 α_i に属する固有ベクトルになっている p_j の全体を $p_{i,1}, \ldots, p_{i,n_i}$ と書き, これらで張られる K^n の部分空間を V_i と書くことにする. このとき $V_1 \oplus \cdots \oplus V_s = V = K^n$ であり, $V_i = V(A; \alpha_i)$ である[102]. よって $V(A; \alpha_1) \oplus \cdots \oplus V(A; \alpha_s) = V$ である. 逆にこの条件が成立しているならば $V(A; \alpha_i)$ の基底たちの $i = 1, \ldots, s$ に関する和集合を $p_1, \ldots, p_n$ と書き, $P = [p_1 \ \cdots \ p_n]$ と置くと, $P^{-1}AP$ は対角行列になる. □

解説: 行列の性質を行列の成分の操作だけによって理解しようとするのは苦しい. 行列の性質を行列の成分にさわらずにとらえておくと理論の展開が易しくなる場合が多い. 行列の半単純性を対角化可能性ではなく, 固有空間分解可能性によってとらえておくと便利な場合が多い. □

---

[100] 微分方程式論をまだ未習の場合には次の事実を認めて使って良い: $-u'' = p^2 u$ ($p \in \mathbb{C}$) の $C^\infty(\mathbb{R})$ における解全体の集合は 2 次元のベクトル空間をなす. $p \neq 0$ のとき解空間の基底として e^{ipx} と e^{-ipx} が取れ, $p = 0$ のとき解空間の基底として $1, x$ が取れる.

[101] 相異なる固有値の**全体**でなくてもよい.

[102] $V_i \subset V(A; \alpha_i)$ であることはすぐにわかる. $v \in K^n$ を $v = v_1 + \cdots + v_s$, $v_i \in V_i$ と表わしておくと, $Av = \alpha_i v$ となるための必要十分条件は $j \neq i$ に対して $v_j = 0$ となることであることがわかる.

[359] K 上のベクトル空間 V はその一次変換 A の固有空間の直和に分解していると仮定する:

$$V = \bigoplus_{\alpha\in K} V_\alpha, \qquad V_\alpha = V(A;\alpha) = \{\, v \in V \mid Av = \alpha v \,\}.$$

すなわち任意の $v \in V$ は

$$v = \sum_{\alpha\in K} v_\alpha, \quad (v_\alpha \in V_\alpha \text{ であり, 有限個の } \alpha \in K \text{ を除き } v_\alpha = 0)$$

と一意に表わされると仮定する. $v \in V$ に対して $v_\alpha \in V_\alpha$ を対応させる V からそれ自身への写像を P_α と書き, それを V から V_α への**射影 (projection)** と呼ぶ. 任意の $v \in V$ に対して $P_\alpha v \neq 0$ となる $\alpha \in K$ は高々有限個しか存在しない. さらに次が成立している:

$$V_\alpha = \operatorname{Im} P_\alpha, \qquad P_\alpha P_\beta = \delta_{\alpha,\beta} P_\alpha, \qquad \sum_{\alpha\in K} P_\alpha = \mathrm{id}_V, \qquad A = \sum_{\alpha\in K} \alpha P_\alpha.$$

ここで $\sum_{\alpha\in K} P_\alpha$ や $\sum_{\alpha\in K} \alpha P_\alpha$ は一般には無限和になってしまうが, $P_\alpha v$ は高々有限個の α の除いて 0 になると仮定してあるので線形写像として well-defined であることに注意せよ. □

ヒント: 定義を用いて計算するだけで良い. たとえば $\mathrm{id}_V v = v = \sum v_\alpha = \sum P_\alpha v$ より $\sum P_\alpha = \mathrm{id}_V$ である. □

[360] V は体 K 上の任意のベクトル空間であり, 各 $\alpha \in K$ に対して線形写像 $P_\alpha : V \to V$ が与えられており, 任意の $v \in V$ に対して $P_\alpha v \neq 0$ となる $\alpha \in K$ は高々有限個しか存在せず,

$$P_\alpha P_\beta = \delta_{\alpha,\beta} P_\alpha, \qquad \sum_{\alpha\in K} P_\alpha = \mathrm{id}_V$$

が成立していると仮定する. このとき, V の一次変換 A を

$$A = \sum_{\alpha\in K} \alpha P_\alpha$$

と定めると, V は A の固有空間 $\operatorname{Im} P_\alpha$ の直和に分解される. □

ヒント: $\sum P_\alpha = \mathrm{id}_V$ より $v = \sum P_\alpha v$ であるから, 任意の $v \in V$ は $v = \sum v_\alpha$ ($v_\alpha \in \operatorname{Im} P_\alpha$ は有限個を除いて 0) と表わされる. $P_\alpha P_\beta = \delta_{\alpha,\beta} P_\alpha$ より, $\sum v_\beta = 0$ ($v_\beta \in \operatorname{Im} P_\beta$ は有限個を除いて 0) のとき, $0 = P_\alpha \sum v_\beta = v_\alpha$ である. これより表示の一意性が出るので $V = \bigoplus \operatorname{Im} P_\alpha$ である. $V(A;\alpha) = \operatorname{Im} P_\alpha$ となることもすぐにわかる. □

解説: 以上の 2 つ問題によって K 上のベクトル空間 V がその一次変換 A の固有空間の直和に分解されるための必要十分条件はある線形写像 $P_\alpha : V \to V$ ($\alpha \in K$) で任意の $v \in V$ に対して $P_\alpha v \neq 0$ となる $\alpha \in K$ は高々有限個しか存在せず,

$$P_\alpha P_\beta = \delta_{\alpha,\beta} P_\alpha, \qquad \sum_{\alpha\in K} P_\alpha = \mathrm{id}_V$$

を満たしているものが存在し, これらによって A が

$$A = \sum_{\alpha\in K} \alpha P_\alpha$$

と表示できることであることがわかった. このとき $V(A;\alpha) = \operatorname{Im} P_\alpha$ となる. □

V は K 上の任意のベクトル空間であるとし, A, B は V の一次変換であるとする. V の部分空間 $V_{\alpha,\beta} = V(A,B;\alpha,\beta)$ を次のように定める:

$$V_{\alpha,\beta} = V(A,B;\alpha,\beta) = \{\, v \in V \mid Av = \alpha v,\ Bv = \beta v \,\}.$$

$V_{\alpha,\beta} = V(A,B;\alpha,\beta) \neq 0$ のとき $V_{\alpha,\beta} = V(A,B;\alpha,\beta)$ は (A,B) の**同時固有空間** と呼ばれ, $V_{\alpha,\beta} = V(A,B;\alpha,\beta)$ に含まれる 0 でないベクトルを (A,B) の**同時固有値**[103] (α,β) を持つ**同時固有ベクトル**と呼ぶ.

V が A,B の同時固有空間の直和に分解するとは

$$V = \bigoplus_{\alpha,\beta\in K} V_{\alpha,\beta} = \bigoplus_{\alpha,\beta\in K} V(A,B;\alpha,\beta)$$

が成立すること, すなわち任意の $v \in V$ が

$$v = \sum_{\alpha,\beta\in K} v_{\alpha,\beta} \quad (v_{\alpha\,\beta} \in V_{\alpha,\beta} \text{ であり, 有限個の } (\alpha,\beta) \in K^2 \text{ を除き } v_{\alpha,\beta} = 0)$$

と一意に表わされることである.

[361] K 上の 2 変数多項式全体の空間 $V = K[x,y]$ は $A = x\partial/\partial x$ と $B = y\partial/\partial y$ の同時固有空間の直和に分解する. □

ヒント: $x^m y^n$ $(m,n \in \mathbb{Z}_{\geq 0})$ は $V = K[x,y]$ の基底である. □

注意: K の標数が 0 ならば $x\partial/\partial x$ と $y\partial/\partial y$ の同時固有値全体の集合は $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ になり, 同時固有空間はすべて 1 次元になる. K の標数が $p > 0$ ならば $x\partial/\partial x$ と $y\partial/\partial y$ の同時固有値全体の集合は $\mathbb{F}_p \times \mathbb{F}_p$ になり, 同時固有空間はすべて無限次元になる. □

[362] $A,B \in M_n(K)$ を $V = K^n$ の一次変換とみなすとき, A,B が同時対角化可能であることと V が A,B の同時固有空間の直和に分解することは同値である. □

ヒント: 問題 **[358]** と同様の議論で良い. □

[363] (同時固有空間分解) A,B は K 上のベクトル空間 V の互いに可換な一次変換であり, V が A, B それぞれの固有空間の直和に分解するならば, V は A,B の同時固有空間の直和に分解する. □

解説: $V = K^n$ ならば同時対角化可能性と同時固有空間分解可能性が同値であること **[362]** を使えば問題 **[348]** の結果からこの問題の結論が直ちに導かれる. しかし, それでは無限次元の V の場合の証明にはならない. 行列の成分を操作する「対角化」の概念を用いずに, 「固有空間分解」のような行列の成分に一切触らずに定義できる概念だけで証明を閉じておくことも重要である. □

ヒント: 仮定より $V = \bigoplus_{\alpha\in K} V(A;\alpha) = \bigoplus_{\beta\in K} V(B;\beta)$ でかつ $AB = BA$ である. 定義より $V(A,B;\alpha,\beta) = V(A;\alpha) \cap V(B;\beta)$ である.

---

[103] 「同時固有値」という用語はあまり標準的ではない. その代わりによく使われるのが「ウェイト (weight)」という用語である. $V_{\alpha,\beta}$ に含まれるベクトルをウェイト (α,β) を持つベクトルと呼び, $V_{\alpha,\beta}$ をウェイト (α,β) のウェイト空間と呼ぶことにする場合が多い.

任意の $v \in V$ が有限個の $v_{\alpha,\beta} \in V(\alpha,\beta)$ の有限和で一意に表わされることを示さなければいけない.

まず表示の一意性を証明しよう. $v_{\alpha,\beta}, w_{\alpha,\beta} \in V(\alpha,\beta)$ は有限個を除いて 0 であり, $v = \sum_{\alpha,\beta} v_{\alpha,\beta} = \sum_{\alpha,\beta} w_{\alpha,\beta}$ を満たしていると仮定する. このとき $u_{\alpha,\beta} = v_{\alpha,\beta} - w_{\alpha,\beta} \in V(\alpha_i,\beta)$ は $\sum_{\alpha,\beta} u_{\alpha,\beta} = 0$ を満たしている. 表示の一意性を示すためには $u_{\alpha,\beta} = 0$ を示せば良い. $u_\alpha := \sum_\beta u_{\alpha,\beta}$ と置くと $u_\alpha \in V(A;\alpha)$ かつ $\sum_\alpha u_\alpha = 0$ であるから $V = \bigoplus_{\alpha\in K} V(A;\alpha)$ より $u_\alpha = 0$ である. さらに $u_{\alpha,\beta} \in V(B;\beta)$ と $V = \bigoplus_{\beta\in K} V(B;\beta)$ より $u_{\alpha,\beta} = 0$ が導かれる. (ここまでは A と B の可換性を使っていない.)

次に表示の存在を証明しよう. $V = \bigoplus_{\alpha\in K} V(A;\alpha)$ より任意の $v \in V$ は $v = \sum_\alpha v_\alpha$ ($v_\alpha \in V(A;\alpha)$ は有限個を除いて 0) と表わせる. $V = \bigoplus_{\beta\in K} V(B;\beta)$ より各 v_α は $v_\alpha = \sum_\beta v_{\alpha,\beta}$ ($v_{\alpha,\beta} \in V(B;\beta)$ は有限個を除いて 0) と表わせる. このとき

$$\sum_\beta A v_{\alpha,\beta} = A v_\alpha = \alpha v_\alpha = \sum_\alpha \alpha v_{\alpha,\beta}, \qquad \alpha v_{\alpha,\beta} \in V(B;\beta)$$

であり, A, B の可換性より

$$BAv_{\alpha,\beta} = ABv_{\alpha,\beta} = A\beta v_{\alpha,\beta} = \beta A v_{\alpha,\beta}$$

より $Av_{\alpha,\beta} \in V(B;\beta)$ である. $V = \bigoplus_{\beta\in K} V(B;\beta)$ より $Av_{\alpha,\beta} = \alpha v_{\alpha,\beta}$ すなわち $v_{\alpha,\beta} \in V(A;\alpha)$ である. 以上によって $v_{\alpha,\beta} \in V(A;\alpha) \cap V(B;\beta) = V(A,B;\alpha,\beta)$ であることがわかった. □

[364] 複素ベクトル空間 V の半単純一次変換について以下が成立する:

1. A はすべての固有値が非負の実数であるような V の半単純一次変換であり, $k = 1,2,3,\ldots$ であるとする. このとき A の固有値 α に対応する固有空間 $V(A,\alpha)$ と A^k の固有値 α^k に対応する固有空間 $V(A^k,\alpha^k)$ は等しい. よって V の A に関する固有空間分解と A^k に関する固有空間分解は一致する.

2. A, B はともにすべての固有値が非負の実数であるような V の半単純一次変換であるとし, $k = 1,2,3,\ldots$ であるとする. このとき $A^k = B^k$ ならば $A = B$ である[104].

3. A はすべての固有値が非負の実数であるような V の半単純一次変換であるとし, $k = 1,2,3,\ldots$ であるとする. このとき V の一次変換 B と A が可換であることと B と A^k と可換であることは同値である. □

ヒント: 1. $V(A,\alpha) \subset V(A^k,\alpha^k)$ は常に成立する. A はすべての固有値が非負の実数であるような半単純一次変換なので $V = \bigoplus_{\alpha\geq 0} V(A,\alpha)$ である. $\alpha,\beta \geq 0$ のとき $\alpha \neq \beta$ ならば $\alpha^k \neq \beta^k$ なので $V(A^k,\alpha^k) \cap V(A^k,\beta^k) = \{0\}$ である. これより $\alpha \geq 0$ に対して $V(A,\alpha) = V(A^k,\alpha^k)$ であることがわかる.

2. 上の結果より A と A^k に関する固有空間分解は等しく, B と B^k に関する固有空間分解は等しい. $A^k = B^k$ より A と B の固有値の集合は等しく, A と B に関する固有空間分解が等しいことがわかる. よって $A = B$ である.

3. 半単純一次変換 A と任意の一次変換 B が可換であるための必要十分条件は A の固有空間を B が保つことである. 仮定より A と A^k に関する固有空間分解は等しいので B と A が可換であることと B と A^k が可換であることは同値である. □

[104] この結果は「2 つの非負の実数 a, b が $a^k = b^k$ を満たしているならば $a = b$ である」という事実の行列の場合への拡張になっている.

[365] (極分解) A は n 次の複素正方行列であるとする. このとき固有値のすべてが非負の実数であるような Hermite 行列 H とユニタリー行列 U で $A = HU$ を満たすものが存在する. これを A の**極分解 (polar decomposition)** と呼ぶ. H は常に一意的であり, もしも A が可逆ならば U も一意的である. そして A が正規行列であることと H と U が可換であることは同値である. □

解説: この問題は「任意の複素数 z は $z = re^{i\theta}$ ($r \in \mathbb{R}_{\geq 0}$, $\theta \in \mathbb{R}$ と表わされ, r は常に一意的であり, $z \neq 0$ ならば $e^{i\theta}$ も一意的である」という結果の行列への拡張である. □

ヒント: 問題 **[228]** の結果より, あるユニタリー行列 P, Q で $D = P^*AQ$ が対角成分が非負の実数であるような対角行列になるものが存在する. よって $H = PDP^*$, $U = PQ^*$ と置けば $A = HU$ かつ H は固有値がすべて非負の Hermite 行列であり, U はユニタリー行列である. これで極分解の存在が示された. $A = H_1U_1 = H_2U_2$ を A の 2 つの極分解とすると $AA^* = H_1^2 = H_2^2$ が成立する. よって問題 **[364]** の結果より $H_1 = H_2$ となる. これで H の一意性が示された. もしも A が可逆ならば $H_1 = H_2$ も可逆になる. そのとき $U_1 = H_1^{-1}H_2U_2 = U_2$ である. これで可逆な A に対する U の一意性も示された. H と U が可換であれば $A^*A = U^{-1}H^2U = U^{-1}UH^2 = H^2 = AA^*$ なので A は正規行列になる. 逆に A が正規行列であれば $U^{-1}H^2U = A^*A = AA^* = H^2$ であるから H^2 と U は可換である. よって問題 **[364]** の結果より H と U は可換になる. □

23.4 最小多項式

K は任意の代数閉体であると仮定し, K の元を成分に持つ行列について考える. K の元を数と呼ぶことがある. 「任意の代数閉体」という言葉を使うのが怖い人は $K = \mathbb{C}$ であると考えてよい.

$A \in M_n(K)$ に対して, 多項式の集合 I_A を次のように定める[105]:

$$I_A = \{\, f \in K[\lambda] \mid f(A) = 0 \,\}.$$

このとき I_A は和と任意の多項式倍で閉じている.

[366] $I_A \neq 0$. □

ヒント 1: Cayley-Hamilton の定理. □
ヒント 2: 任意の $f \in K[\lambda]$ に対して $f(A) = 0$ ならば $f = 0$ と仮定して矛盾を導こう. もしもそうならば $E, A, A^2, A^3, \ldots$ は一次独立になる. よって n^2 次元の $M_n(K)$ が $E, A, A^2, A^3, \ldots$ で張られる無限次元の部分空間を含むことになって矛盾する. □

[367] (最小多項式の定義) I_A に含まれる 0 でない多項式の中で次数が最小でかつモニック[106]なものが一意に存在する. その多項式を A の**最小多項式 (minimal polynomial)** と呼び, $\varphi_A(\lambda)$ と書くことにする. □

ヒント: 存在は上の問題より. $f, g \in I_A$ はともに条件を満たしているとする. このとき f を g で割った商を q と書き, 余りを r と書く. もしも $q \neq 1$ ならば f または g がモニックでなくなるので $q = 1$ である. もしも $r \neq 0$ ならば $r(A) = 0$ より f, g の次数の最小性に矛盾するので $r = 0$ である. よって $f = g$ である. □

[105] I はイデアル (ideal) の頭文字を取った. 標準的な記法ではない. ここだけの記法である.
[106] 最高次の係数が 1 であるという意味.

[368] A の最小多項式を φ_A と書くと $I_A = K[\lambda]\varphi_A$ である. すなわち A を代入して 0 になる任意の多項式は最小多項式の多項式倍で表わされる. 特に A の特性多項式は A の最小多項式で割り切れる. □

ヒント: $g \in I_A$ を最小多項式 φ_A で割った余りを r とすると, $r(A) = 0$ となるので φ_A の次数の最小性より $r = 0$ でなければいけない. よって g は φ_A で割り切れる. A の特性多項式 p_A は Cayley-Hamilton の定理より I_A の元なので最小多項式で割り切れる. □

[369] $A \in M_n(K)$ と $P \in GL_n(K)$ に対して A と PAP^{-1} の最小多項式は等しい. □

ヒント: $f \in K[\lambda]$ に対して $f(PAP^{-1}) = Pf(A)P^{-1}$ であるから $f(A) = 0 \iff f(PAP^{-1}) = 0$. □

[370] m 次正方行列 B と n 次正方行列 C を用いて $m+n$ 次正方行列 A を $A = \begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix}$ と定める. このとき A の最小多項式 φ_A は B の最小多項式 φ_B と C の最小多項式 φ_C の最小公倍多項式になる. □

ヒント: 最小公倍多項式の定義より, φ_A が φ_B, φ_C で割り切れることと, $f \in K[\lambda]$ が φ_B, φ_C で割り切れるならば f は φ_A でも割り切れることを示せば良い. $0 = \varphi_A(A) = \begin{bmatrix} \varphi_A(B) & 0 \\ 0 & \varphi_A(C) \end{bmatrix}$ より $\varphi_A(B) = 0$ かつ $\varphi_A(C) = 0$. よって φ_A は φ_B, φ_C で割り切れる. f が φ_B, φ_C で割り切れるならば $f(B) = 0$, $f(C) = 0$ となるので $f(A) = 0$ となる. よって f は φ_A で割り切れる. □

[371] $A \in M_n(K)$ のとき, A の最小多項式 φ_A の n 乗は A の特性多項式 p_A で割り切れる. □

注意: この問題の結果を **[368]** の p_A が φ_A で割り切れるという結果を合わせると, p_A と φ_A の根が重複度を除き一致していることもわかる. □

ヒント: 行列係数の多項式に関する剰余定理 **[69]** を $\varphi_A(\lambda)E$ に適用すると, ある行列係数多項式 $G(\lambda)$ が存在して $\varphi_A(\lambda)E = (\lambda E - A)G(\lambda)$ となる. この等式の両辺の行列式を取ると $\varphi_A(\lambda)^n = p_A(\lambda)\det G(\lambda)$. □

[372] $\alpha, \beta, \gamma \in K$ は互いに異なると仮定し, $x, y, z \in K$ に対して行列 A, B, C, D を次のように定める:

$$A = \begin{bmatrix} \alpha & x & z \\ 0 & \beta & y \\ 0 & 0 & \gamma \end{bmatrix}, \quad B = \begin{bmatrix} \alpha & x & z \\ 0 & \alpha & y \\ 0 & 0 & \gamma \end{bmatrix}, \quad C = \begin{bmatrix} \alpha & x & z \\ 0 & \alpha & y \\ 0 & 0 & \alpha \end{bmatrix}, \quad D = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -z & -y & -x \end{bmatrix}.$$

このとき以下が成立する:

1. A の最小多項式は常に $(\lambda - \alpha)(\lambda - \beta)(\lambda - \gamma)$ になる.
2. B の最小多項式は $(\lambda - \alpha)(\lambda - \gamma)$ または $(\lambda - \alpha)^2(\lambda - \gamma)$ になる. そして前者になるための必要十分条件は $x = 0$ である.

3. C の最小多項式は $\lambda-\alpha$ または $(\lambda-\alpha)^2$ または $(\lambda-\alpha)^3$ のどれかになる. そして $(\lambda-\alpha)^2$ になるための必要十分条件[107]は $xy=0$ である.

4. D の最小多項式は常に $\lambda^3+x\lambda^2+y\lambda+z$ になる.
(ヒント: D の特性多項式は $p_D(\lambda)=\lambda^3+x\lambda^2+y\lambda+z$ である. K は代数閉体だと仮定してあるので, 特性多項式は $p_D(\lambda)=(\lambda-a)(\lambda-b)(\lambda-c)$ $(a,b,c\in K)$ と一次式の積に分解する. $(D-aE)(D-bE)$ の一番右上の成分は 1 になる.) □

[373] $\alpha_1,\dots,\alpha_s\in K$ は互いに異なり, $n=n_1+\cdots+n_s$, $n_i>0$ であるとする. n 次対角行列 A を

$$A=\begin{bmatrix}\alpha_1E_{n_1} & & & 0\\ & \alpha_2E_{n_2} & & \\ & & \ddots & \\ 0 & & & \alpha_sE_{n_s}\end{bmatrix}$$

と定める. このとき A の最小多項式は $\varphi(\lambda)=(\lambda-\alpha_1)\cdots(\lambda-\alpha_s)$ である. □

ヒント: $\varphi(A)=0$ であることがすぐにわかる. $\varphi(A)$ を割り切る次数が s 未満の任意の多項式を f とすると $f(A)\neq 0$ となることもすぐに確かめられる. □

[374] 次の n 次正方行列の最小多項式を求めよ:

$$J_n(\alpha)=\alpha E_n+J_m(0)=\begin{bmatrix}\alpha & 1 & & & 0\\ & \alpha & 1 & & \\ & & \alpha & \ddots & \\ & & & \ddots & 1\\ 0 & & & & \alpha\end{bmatrix}.$$ □

ヒント: $A=J_n(\alpha)$ の特性多項式は $p_A(\lambda)=(\lambda-\alpha)^n$ となる. 実☆☆れ☆そ☆まま☆小☆項☆☆☆る. □

[375] **(コンパニオン行列)** 次の形の n 次正方行列のを **コンパニオン行列 (同伴行列, companion matrix)** と呼ぶ:

$$C(a_0,\dots,a_{n-1})=\begin{bmatrix}0 & 1 & & & 0\\ & 0 & \ddots & & \\ & & \ddots & 1 & \\ 0 & & & 0 & 1\\ -a_{n-1} & -a_{n-2} & \cdots & -a_1 & -a_0\end{bmatrix}.$$

コンパニオン行列 $C(a_0,\dots,a_{n-1})$ の特性多項式は

$$p_{C(a_0,\dots,a_{n-1})}(\lambda)=\lambda^n+a_0\lambda^{n-1}+a_1\lambda^{n-2}+\cdots+a_{n-2}\lambda+a_{n-1}$$

となり, 最小多項式は特性多項式に等しい. □

[107]他の場合は簡単である.

ヒント: 行列式 $|\lambda E - C(a_0,\dots,a_{n-1})|$ を第 1 列について余因子展開することによって帰納的に特性多項式を計算できる:

$$\begin{vmatrix} \lambda & -1 & & & 0 \\ & \lambda & \ddots & & \\ & & \ddots & -1 & \\ & & & \lambda & -1 \\ 0 & & & & \\ a_{n-1} & a_{n-2} & \cdots & a_1 & \lambda - a_0 \end{vmatrix} = \lambda \begin{vmatrix} \lambda & -1 & & 0 \\ & \ddots & \ddots & \\ 0 & & \lambda & -1 \\ a_{n-2} & \cdots & a_1 & \lambda - a_0 \end{vmatrix} + (-1)^n a_n \begin{vmatrix} -1 & & & 0 \\ \lambda & -1 & & \\ & \ddots & \ddots & \\ 0 & & \lambda & -1 \end{vmatrix}.$$

よって $p_n(\lambda) = p_{C(a_0,\dots,a_{n-1})}(\lambda)$ と置くと $p_n(\lambda) = \lambda p_{n-1}(\lambda) + a_{n-1}$ である. 最小多項式については次の問題を見よ. □

[**376**] 次の形の n 次正方行列の最小多項式は特性多項式に等しくなる:

$$A = \begin{bmatrix} * & 1 & & 0 \\ \vdots & \ddots & \ddots & \\ \vdots & & \ddots & 1 \\ * & \cdots & \cdots & * \end{bmatrix}. \quad \square$$

ヒント: A の形の行列を $n-1$ 個かけると一番右上の $(1,n)$ 成分は 1 になる. より一般に A の形の行列を k 個かけると次の形になる:

$$\begin{bmatrix} b_{11} & \cdots & b_{1,k} & 1 & & 0 \\ * & \ddots & & \ddots & \ddots & \\ \vdots & \ddots & \ddots & & \ddots & 1 \\ \vdots & & \ddots & \ddots & & b_{n-k+1,n} \\ \vdots & & & \ddots & \ddots & \vdots \\ * & \cdots & \cdots & \cdots & * & b_{nn} \end{bmatrix}.$$

よって A の特性多項式の根を $\alpha_1,\dots,\alpha_n$ と書くと $k < n$ のとき $(A-\alpha_1 E)\cdots(A-\alpha_k E) \neq 0$ である. □

[**377**] 問題 [**376**] の行列 A に対して, 対角成分が 1 の下三角行列 U と $a_1,\dots,a_n \in K$ で $U^{-1}AU = C(a_0,\dots,a_{n-1})$ を満たすものが一意に存在する. ここで $C(a_0,\dots,a_{n-1})$ は問題 [**375**] で定義したコンパニオン行列である. □

ヒント 1: A, U の成分に記号を割り振り, U と a_i に関する方程式 $AU = UC(a_0,\dots,a_{n-1})$ が一意に解けることを確かめれば良い. たとえば $n = 3$ のとき,

$$\begin{bmatrix} a_{11} & 1 & 0 \\ a_{21} & a_{22} & 1 \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ u_{21} & 1 & 0 \\ u_{31} & u_{32} & 1 \end{bmatrix} = \begin{bmatrix} a_{11}+u_{21} & 1 & 0 \\ a_{21}+a_{22}u_{21}+u_{31} & a_{22}+u_{32} & 1 \\ a_{31}+a_{32}u_{21}+a_{33}u_{31} & a_{32}+a_{33}u_{32} & a_{33} \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ u_{21} & 1 & 0 \\ u_{31} & u_{32} & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a_2 & -a_1 & -a_0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & u_{21} & 1 \\ -a_3 & u_{31}-a_2 & u_{32}-a_1 \end{bmatrix}.$$

よって u_{ij} と a_0, a_1, a_2 に関する方程式 $AU = UC(a_0, a_1, a_2)$ は $u_{21} = -a_{11}$, $u_{31} = -a_{21} - a_{22}u_{21}$, $a_2 = -a_{31} - a_{32}u_{21} - a_{33}u_{31}$, $u_{32} = u_{21} - a_{22}$, $a_1 = u_{31} - a_{32} - a_{33}u_{32}$, $a_0 = u_{32} - a_{33}$ と一意に解ける. □

ヒント 2: 対角成分の 1 つ右上の成分だけが 1 で他の成分が 0 であるような n 次正方行列を Λ と表わす. 各 $k = 0, 1, 2, \ldots$ に対して $(k+1, 1), (k+2, 2), \ldots, (n, n-k)$ 以外の成分がすべて 0 であるような下三角行列全体の空間を V_k と書くことにする. $k \geq n$ の場合は $V_n = 0$ と約束しておく. このとき問題の行列 A は $A = \Lambda + A_0 + \cdots + A_{n-1}$, $A_k \in V_k$ と一意に表わされ, 対角成分がすべて 1 であるような下三角行列 U は $U = E + U_1 + \cdots + U_{n-1}$, $U_k \in V_k$ と一意に表わされる. (i, j) 行列単位を E_{ij} と書き[108], $C_k = -a_k E_{n,n-k}$ と置くと $C_k \in V_k$ であり, コンパニオン行列 $C = C(a_0, \ldots, a_{n-1})$ は $C = \Lambda + C_0 + \cdots + C_{n-1}$ と表わされる. このとき $AU = UC$ は U_k, C_k に関する次の連立方程式と同値である:

$$
\begin{aligned}
&[\Lambda, U_1] - C_0 = -A_0,\\
&[\Lambda, U_2] - C_1 = -A_0U_1 - A_1 + U_1C_0,\\
&[\Lambda, U_3] - C_2 = -A_0U_2 - A_1U_1 - A_2 + U_1C_1 + U_2C_0,\\
&\qquad\cdots\cdots\\
&[\Lambda, U_{n-1}] - C_{n-2} = -A_0U_{n-2} - \cdots - A_{n-3}U_1 - A_{n-2} + U_1C_{n-3} + \cdots + U_{n-3}C_0,\\
&[\Lambda, U_n] - C_{n-1} = -A_0U_{n-1} - \cdots - A_{n-2}U_1 - A_{n-1} + U_1C_{n-2} + \cdots + U_{n-2}C_0.
\end{aligned}
$$

ここで $U_n = 0$ である. 任意の $Z_k \in V_k$ は $[\Lambda, X_{k+1}] + Y_k$ $(X_{k+1} \in V_{k+1}, Y_k \in KE_{n,n-k})$ と一意に表わされることを示せる. よって上の連立方程式は上から順に一意に解ける. □

[378] (最小多項式による半単純性の判定法) $A \in M_n(K)$ が半単純であるための必要十分条件は A の最小多項式が重根を持たないことである. 特に A の特性多項式が重根を持たなければ A は半単純である. □

ヒント: 問題 **[369]**, **[373]** より半単純なら最小多項式が重根を持たないことがわかる. 最小多項式 $\varphi_A(\lambda)$ が重根を持たないと仮定する. すなわち $\varphi_A(\lambda) = (\lambda - \alpha_1) \cdots (\lambda - \alpha_s)$ と一次式の積に分解され α_i は互いに異なると仮定する. このとき

$$\varphi_A(A) = (A - \alpha_1 E) \cdots (A - \alpha_s E) = 0$$

であるから, 問題 **[354]** の結果より

$$\sum_{i=1}^{s} \dim \mathrm{Ker}(A - \alpha_i E) \geq \dim \mathrm{Ker}\, \varphi(A) = n.$$

A の固有値 α_i に対応する固有空間は $\mathrm{Ker}(A - \alpha_i E)$ に等しい. 問題 **[357]** の結果より逆向きの不等式が成立しているので等号が成立する. よって A の固有ベクトルだけで構成された K^n の基底 $p_1, \ldots, p_n$ が存在する. このとき $P = [p_1 \ \ldots \ p_n]$ は A を対角化する. □

[379] (最小多項式の有理的計算法) $A \in M_n(K)$ とし, A の最小多項式を $\varphi_A(\lambda)$ と書き, 特性多項式を $p_A(\lambda) = \det(\lambda E - A)$ と書くことにする. $\lambda E - A$ のすべての (i, j) 余因子のモニックな最大公約多項式を $d(\lambda)$ と書くと $\varphi_A(\lambda) = p_A(\lambda)/d(\lambda)$ である. □

[108] (i, j) 成分だけが 1 で他の成分がすべて 0 である正方行列を (i, j) 行列単位と呼び, E_{ij} と書く.

解説: 行列式の定義より特性多項式と余因子は四則演算だけで計算でき, 最大公約多項式も Euclid の互除法より四則演算で計算できるので, 正方行列の最小多項式は四則演算だけで計算できることがわかる. よって代数閉体 K の任意の部分体 L に対して $A \in M_n(L)$ の最小多項式は L 係数の多項式として四則演算だけで計算できる. □

ヒント: $\lambda E - A$ の (i,j) 余因子を $f_{ij}(\lambda)$ と書き, $F(\lambda) = [f_{ij}(\lambda)]$ と置く. $d(\lambda)$ は $f_{ij}(\lambda)$ たちの最大公約多項式であるから, ある行列係数多項式 $G(\lambda)$ でその成分の最大公約多項式が 1 で $F(\lambda) = d(\lambda)G(\lambda)$ を満たすものが存在する. 余因子展開の公式より,

$$d(\lambda)\,{}^tG(\lambda)(\lambda E - A) = {}^tF(\lambda)(\lambda E - A) = p_A(\lambda)E.$$

よって特性多項式 $p_A(\lambda)$ は $d(\lambda)$ で割り切れる. $f = p_A/d \in K[\lambda]$ と置くと ${}^tG(\lambda)(\lambda E - A) = f(\lambda)E$ である. このとき行列係数多項式の剰余定理 [**69**] より $f(A) = 0$ となる. よって $f(\lambda)$ は最小多項式 $\varphi_A(\lambda)$ で割り切れる. $g = f/\varphi_A \in K[\lambda]$ と置く. $\varphi_A(\lambda)E$ に行列係数多項式の剰余定理 [**69**] を適用するとある行列係数多項式 $H(\lambda)$ で $\varphi_A(\lambda)E = H(\lambda)(\lambda E - A)$ を満たすものが存在する. この等式の両辺に $g = f/\varphi_A$ をかけて左辺に ${}^tG(\lambda)(\lambda E - A) = f(\lambda)E$ を適用すると ${}^tG(\lambda)(\lambda E - A) = g(\lambda)H(\lambda)(\lambda E - A)$ となる. この等式の両辺に右から ${}^tF(\lambda)$ をかけて $p_A(\lambda)$ で割ると ${}^tG(\lambda) = g(\lambda)H(\lambda)$ となる. ところが $G(\lambda)$ の成分たちの最大公約多項式は 1 なので g は定数でなければいけない. ところが $g = f/\varphi_A = p_A/(\varphi_A d)$ より g の最高次の係数は 1 でなければいけない. したがって $g = 1$ である. これで $f = \varphi_A$ が示された. □

23.5 Jordan 分解と一般固有空間分解

行列の Jordan 標準形の話に戻ろう.

K は任意の代数閉体であると仮定し, K の元を成分に持つ行列について考える. K の元を数と呼ぶことがある. 「任意の代数閉体」という言葉を使うのが怖い人は $K = \mathbb{C}$ であると考えてよい.

定理 23.5 (Jordan 分解) 任意の行列 $A \in M_n(K)$ に対して半単純行列 $S \in M_n(K)$ と巾零行列 $N \in M_n(K)$ の組で $A = S + N$ かつ $SN = NS$ を満たすものが一意に存在する. しかも各 A ごとにある多項式 $g \in K[\lambda]$ で $S = g(A)$, $N = A - g(A)$ を満たすものが存在する. 上のような $A = S + N$ を行列 A の **Jordan 分解 (Jordan decomposition)** と呼ぶ. (あとで説明する乗法的 Jordan 分解との区別を強調したい場合は**加法的 Jordan 分解 (additive Jordan decomposition)** と呼ぶ.) S, N はそれぞれ A の**半単純部分 (semisimple part)**, **巾零部分 (nilpotent part)** と呼ばれている. □

Jordan 分解の証明では第 22 節で特に詳しく説明した問題 [**323**] の結果が決定的に重要な役目を果たす. その結果をここに再掲しておこう:

> $f_1, \ldots, f_n \in K[\lambda]$ の最大公約元を $d \in K[\lambda]$ とすると, ある $a_1, \ldots, a_n \in K[\lambda]$ で $d = a_1 f_1 + \cdots + a_n f_n$ を満たすものが存在する. □

[**380**] **(Jordan 分解の存在)** $A \in M_n(K)$ の Jordan 分解が存在して, A の半単純部分と巾零部分が A の多項式で表わされることを以下の方針で証明せよ:

1. ある 0 でないモニックな多項式 $f \in K[\lambda]$ で $f(A) = 0$ となるものが存在する. (ヒント: Cayley-Hamilton の定理もしくは最小多項式の存在.)

2. K は代数閉体だと仮定してあったので f は一次式の積に分解する:

$$f(\lambda) = (\lambda - \alpha_1)^{m_1} \cdots (\lambda - \alpha_s)^{m_s}.$$

ここで $\alpha_1, \ldots, \alpha_s \in K$ は互いに異なり, m_i は正の整数である. $f_i(\lambda) = f(\lambda)/(\lambda - \alpha_i)^{m_i}$ と置くと $f_1, \ldots, f_s$ の最大公約多項式は 1 になる. よって問題 **[323]** の結果より, ある $a_1, \ldots, a_s \in K[\lambda]$ が存在して $a_1 f_1 + \cdots + a_s f_s = 1$ となる.

3. $p_i = a_i f_i$ と置き, $P_i = p_i(A)$ と置くと

$$P_i P_j = \delta_{ij} P_i, \qquad P_1 + \cdots + P_s = E.$$

(ヒント: $p_1 + \cdots + p_s = 1$ なので $P_1 + \cdots + P_s = E$ である. $i \neq j$ のとき $f_i f_j$ は f で割り切れるので $f_i(A) f_j(A) = 0$. よって $P_i P_j = 0$ $(i \neq j)$. $P_i = E P_i = (P_1 + \cdots + P_s) P_i = P_i^2$.)

4. K^n の部分空間 V_i を $V_i = \operatorname{Im} P_i = \{ P_i x \mid x \in K^n \}$ と定めると, 任意の $v \in K^n$ は $v = v_1 + \cdots + v_s$, $v_i \in V_i$ と一意に表わされる. (ヒント: 表示の存在は $P_1 + \cdots + P_s = E$ より. 表示の一意性は $P_i P_j = \delta_{ij} P_i$ より.)

5. $S = \alpha_1 P_1 + \cdots + \alpha_s P_s$, $N = A - S$ と置くと S, N は A の多項式になるので, $SN = NS$ である.

6. S は半単純である. (ヒント: V_i たちの基底の和集合を $u_1, \ldots, u_n$ と書くと $U = [u_1 \ \cdots \ u_n]$ は S を対角化する.)

7. N は巾零である. (ヒント: $v_i \in V_i$ に対して $N v_i = (A - \alpha_i E) v_i$ である. $P_i = p_i(A)$ と A は可換なので $N v_i \in V_i$ である. $(\lambda - \alpha_i)^{m_i} p_i(\lambda) = a_i(\lambda) f(\lambda)$ なので $N^{m_i} v_i = (A - \alpha_i E)^{m_i} v_i = a_i(A) f(A) v_i = 0$. 一般の $v \in V$ は $v = v_1 + \cdots + v_s$, $v_i \in V_i$ と表わされるので $m = \max\{m_1, \ldots, m_s\}$ と置くと $N^m v = 0$.) □

[381] (Jordan 分解の一意性) Jordan 分解の一意性を証明せよ. □

ヒント: 問題 **[380]** より A の Jordan 分解 $A = S + N$ で S, N が A の多項式になるものが存在する. もう 1 つの Jordan 分解 $A = S' + N'$ が与えられたとき $S' = S$, $N' = N$ となることを示せば良い. $A = S + N = S' + N'$ より $S - S' = N' - N$ である. Jordan 分解の定義から S' と N' は互いに可換であるので A とも可換である. S, N は A の多項式なので S', N' は S, N とも可換である. よって, 問題 **[348]** より $S - S'$ も半単純になり, 問題 **[347]** より $N' - N$ も巾零になる. したがって, 問題 **[342]** より $S - S' = N' - N = 0$ である. □

[382] $A, B \in M_n(K)$ であるとし A の Jordan 分解を $A = S + N$ (S は半単純, N は巾零) と書いておく. このとき A と B が可換であるための必要十分条件は B が S および N と可換になることである. □

ヒント: $A = S + N$ より B が S および N と可換ならば A とも可換である. S と N は A の多項式で書けるので, B が A と可換ならば S および N とも可換である. □

[383] (一般固有空間分解) K^n は A の一般固有空間

$$W_A(\alpha_i) = \{\, v \in K^n \mid (A-\alpha_i E)^k v = 0 \ (\exists k \geq 0) \,\} \qquad (i = 1, \ldots, s)$$

の直和に分解される．ここで $\alpha_1, \ldots, \alpha_s$ は A の相異なる固有値の全体である．すなわち任意の $v \in V$ は $v = v_1 + \cdots + v_s$, $v_i \in W_A(\alpha_i)$ の形で一意に表わされる． □

ヒント: 問題 **[380]** の記号のもとで $V_i = W_A(\alpha_i)$ が成立することを示せば良い[109]．$V_i \subset W_A(\alpha_i)$ は $(\lambda-\alpha_i)^{m_i} p_i(\lambda) = a_i(\lambda) f(\lambda)$ より $(A-\alpha_i E)^{m_i} V_i = a_i(A) f(A) V = 0$ となることより出る．$V_i \supset W_A(\alpha_i)$ の方は次のように示される．$(A-\alpha_i E)^k v = 0$ と仮定する．もしも p_i が $\lambda - \alpha_i$ で割り切れるならば $p_1 + \cdots + p_s = 1$ も $\lambda - \alpha_i$ で割り切れるので矛盾する．よって $p_i(\lambda)$ は $(\lambda-\alpha_i)^k$ と共通因子を持たない．したがってある多項式 $a, b \in K[\lambda]$ が存在して $a(\lambda)p_i(\lambda) + b(\lambda)(\lambda-\alpha_i)^k = 1$ となる．これの λ に A を代入して v に作用させると $P_i a(A) v = v$ となる．よって $v \in P_i K^n = V_i$ である.) □

[384] (Jordan 標準形の一歩手前) 正方行列 $A \in M_n(K)$ の Jordan 分解を $A = S + N$ (S は半単純, N は巾零) と書くことにする．このとき, ある正則行列 $P \in GL_n(K)$ が存在して $P^{-1}AP$, $P^{-1}SP$, $P^{-1}NP$ は以下のような形になる:

$$P^{-1}AP = \begin{bmatrix}
\alpha_1 & * & \cdots & * & & & & & 0 \\
 & \alpha_1 & \ddots & \vdots & & & & & \\
 & & \ddots & * & & & & & \\
0 & & & \alpha_1 & & & & & \\
 & & & & \ddots & & & & \\
 & & & & & \ddots & & & \\
 & & & & & & \alpha_s & * & \cdots & * \\
 & & & & & & & \alpha_s & \ddots & \vdots \\
 & & & & & & & & \ddots & * \\
0 & & & & & & 0 & & & \alpha_s
\end{bmatrix},$$

$$P^{-1}SP = \begin{bmatrix}
\alpha_1 & & & & & & & & & 0 \\
 & \alpha_1 & & & & & & & & \\
 & & \ddots & & & & & & & \\
 & & & \alpha_1 & & & & & & \\
 & & & & \ddots & & & & & \\
 & & & & & \ddots & & & & \\
 & & & & & & \alpha_s & & & \\
 & & & & & & & \alpha_s & & \\
 & & & & & & & & \ddots & \\
0 & & & & & & & & & \alpha_s
\end{bmatrix},$$

[109] 問題 **[380]** の f は A の固有値以外の根を持たないものが取れる．たとえば A の特性多項式や最小多項式が取れる．よって α_i は A の固有値であると考えて良い．

$$P^{-1}NP = \begin{bmatrix} 0 & * & \cdots & * & & & & & & 0 \\ & 0 & \ddots & \vdots & & & & & & \\ & & \ddots & * & & & & & & \\ 0 & & & 0 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 0 & * & \cdots & * \\ & & & & & & & 0 & \ddots & \vdots \\ & & & & & & & & \ddots & * \\ 0 & & & & & & 0 & & & 0 \end{bmatrix}.$$

ここで, $\alpha_1, \ldots, \alpha_s$ は A の相異なる固有値の全体であり, α_i の重複度を n_i と書くと, $P^{-1}AP$ と $P^{-1}SP$ の対角線には各 α_i が n_i 個ずつ並んでおり, $P^{-1}AP$ と $P^{-1}NP$ の対角線には n_i 次の上三角行列が並んでいる.

特に A と S の特性多項式, トレース, 行列式は等しい. □

ヒント: S は半単純なのである正則行列 Q が存在して $Q^{-1}SQ$ は上の形になる. このとき $Q^{-1}NQ$ は $Q^{-1}SQ$ と可換なので問題 **[345]** の結果より次の形になる:

$$Q^{-1}NQ = \begin{bmatrix} N_1 & & 0 \\ & \ddots & \\ 0 & & N_s \end{bmatrix}.$$

ここで N_i は n_i 次の正方行列である. N は巾零なので問題 **[343]** の結果より N_i たちも巾零になる. 問題 **[193]** もしくは (その一般化である問題 **[350]**) より各 N_i に対してある n_i 次正則行列 R_i が存在して $R_i^{-1}N_iR_i$ は上三角行列になる. N_i は巾零なので $R_i^{-1}N_iR_i$ の対角成分はすべて 0 でなければいけない. $R_1, \ldots, R_s$ を対角線に並べてできる正則行列を R と書き, $P = QR$ と置く. このとき R は $Q^{-1}SQ$ と可換なので $P^{-1}SP = R^{-1}Q^{-1}SQR = Q^{-1}SQ$ であり, $P^{-1}NP = R^{-1}Q^{-1}NQR$ は対角線に $R_i^{-1}N_iR_i$ が並んでいる行列になる. よって $P^{-1}SP$ と $P^{-1}NP$ は上に示された形になっている. そのとき $P^{-1}AP = P^{-1}SP + P^{-1}NP$ も上に示された形になっている. このとき, $p_A(\lambda) = p_{P^{-1}AP}(\lambda) = p_{P^{-1}SP}(\lambda) = p_S(\lambda)$ である. トレースと行列式についても同様である[110]. □

解説: 上のヒントは Jordan 分解可能性さえ認めてしまえば, Jordan 標準形の一歩手前の結果を容易に導けることも示している. ただし, Jordan 分解の他に次のような結果も必要になるのだが: 「対角行列と可換な行列がどのような形になるか」**[345]**, 「対角線に正方ブロックが並んだ行列が巾零でならば各ブロックも巾零である」**[343]**, 「任意の正方行列は相似変換で上三角行列に変換できる」**[193]**. これらの結果は直接的な計算や行列のサイズに関する帰納法で容易に証明可能である.

Jordan 標準形の理論は「途中で使われた結果は後の方で示された結果を認めれば容易に示されてしまう」という性質を持っている. だから結論を暗記するためには後の方で証

[110] トレースが特性多項式の λ^{n-1} の係数の -1 倍に等しく, 行列式が特性多項式の定数項の $(-1)^n$ 倍に等しいという結果を使っても良いし, トレースは重複を含めた固有値の和に等しく, 行列式は重複を含めた固有値の積に等しいという結果を使っても良い.

明されるより強い結果を覚えるようにして, その強い結果を認めれば途中で使われた中間的な結果が容易に導かれることをチェックしておけば良い[111]. □

[**385**] $A \in M_n(K)$ の半単純部分を S と書く. A と S の最小多項式が等しくならない場合があることを示せ. □

ヒント: 例を 1 つ以上示せば良い. 対角部分が αE であるような上三角行列でそのような例を探してみよ. (そのとき $S = 0$ となる.) 問題 [**372**] も参考にせよ. □

正方行列 $A \in M_n(K)$ が**巾単 (unipotent)** であるとは $A - E$ が巾零 (nilpotent) になることである. すなわち A が $A = E + N$ (N は巾零) と表わされるとき A は巾単であるという.

[**386**] 巾単行列は正則行列である. □

ヒント: 等比級数の和の公式 $1/(1+x) = 1 - x + x^2 - x^3 + \cdots$ を $A = E + N$, $N^r = 0$ に適用せよ. $B = E - N + N^2 - N^3 + \cdots + (-1)^r N^r$ (有限和) と置くと $AB = BA = E$ となる. □

解説: 行列や作用素の等比級数は **Neumann 級数 (Neumann series)** と呼ばれている. もしも Neumann 級数 $\sum_{k=0}^{\infty}(-N)^k$ が収束すればそれは $E + N$ の逆行列になっている. N が巾零ならば Neumann 級数は有限和になる. □

定理 23.6 (乗法的 Jordan 分解) 任意の正則行列 $A \in GL_n(K)$ に対して半単純正則行列 $S \in GL_n(K)$ と巾単行列 $U \in GL_n(K)$ の組で $A = SU$ かつ $SU = US$ を満たすものが一意に存在する. これを正則行列 A の**乗法的 Jordan 分解 (multiplicative Jordan decomposition)** もしくは **Chevalley 分解 (Chevalley decomposition)** と呼ぶ. このとき S, U はそれぞれ A の**半単純部分 (semisimple part)**, **巾単部分 (unipotent part)** と呼ばれている. 乗法的 Jordan 分解における半単純部分と加法的 Jordan 分解における半単純部分は等しいので, それらを区別する必要はない. □

[**387**] 以下の方針で乗法的 Jordan 分解の存在と一意性を証明せよ.

1. A の Jordan 分解を $A = S + N$ (S は半単純, N は巾零) と書く. Jordan 標準形の一歩手前 [**384**] の結果より $0 \neq \det A = \det S$ である. よって S も正則行列である.

2. $U = S^{-1}A = E + S^{-1}N$ と置く. S と N は可換なので S^{-1} と N は可換になり, $S^{-1}N$ は巾零になる. よって U は巾単行列である.

3. S と $S^{-1}N$ は可換なので U と S も可換である. これで乗法的 Jordan 分解の存在が示された.

4. 逆に $A = SU$ (S は半単純, U は巾単) が乗法的 Jordan 分解であるとき, $N = A - S = S(U - E)$ と置くと $A = S + N$ は加法的 Jordan 分解である. よって乗法的 Jordan 分解の一意性は加法的 Jordan 分解の一意性に帰着する.
(ヒント: $A = SU = S'U'$ (S, S' は半単純, U, U' は巾単) は 2 種類の乗法的 Jordan 分解であるとし, $N = A - S$, $N' = A - S'$ と置く. このとき $A = S + N = S' + N'$ は 2 種類の加法的 Jordan 分解である. 加法的 Jordan 分解の一意性より $S = S'$, $N = N'$ である. このとき $U = S^{-1}A = S'^{-1}A = U'$ である.) □

[111] たとえば Jordan 標準形の一歩手前の結果を認めて Cayley-Hamilton の定理を証明してみよ.

23.6 巾零行列の標準形と Jordan 標準形

K は任意の代数閉体であると仮定し, K の元を成分に持つ行列について考える. K の元を数と呼ぶことがある. 「任意の代数閉体」という言葉を使うのが怖い人は $K = \mathbb{C}$ であると考えてよい.

任意に正方行列 $A \in M_n(K)$ を取り, A の相異なる固有値の全体を $\alpha_1, \ldots, \alpha_s$ と書き, 各 α_i の重複度を n_i と書くことにする.

Jordan 標準形の一歩手前 [**384**] の結果によれば, ある正則行列 $P \in GL_n(K)$ が存在して $P^{-1}AP$ が対角線には n_i 次の上三角行列のブロックが並んだ形になり, 各々のブロックの対角線には α_i が n_i 個並んでいる. しかし, $*$ で表示されている非対角線部分の形をどれだけ単純化できるかという問題はまだ残っている. 以下ではその問題を解くことにしよう.

その問題を解くためは $P^{-1}AP$ の対角線に並んだ各ブロックごとに解けば良いので, 最初から A が次の形をしていると仮定して構わない:

$$A = \alpha E + N, \qquad N = \begin{bmatrix} 0 & a_{12} & \cdots & a_{1n} \\ & 0 & \ddots & \vdots \\ & & \ddots & a_{n-1,n} \\ 0 & & & 0 \end{bmatrix}.$$

問題は巾零行列 N の形をある正則行列 P による相似変換 $P^{-1}NP$ によってできるだけ単純化することである. αE の部分は任意の P と可換なので無視して構わない.

答を説明するために m 次正方行列 $J_m(\alpha)$ を次のように定義する:

$$J_m(\alpha) := \begin{bmatrix} \alpha & 1 & & 0 \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{bmatrix} = \alpha E_m + J_m(0), \qquad J_m(0) = \begin{bmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}.$$

$J_m(\alpha)$ の形の行列を **Jordan ブロック行列 (Jordan block matrix)** と呼び, $J_m(0)$ の形の行列を **巾零 Jordan ブロック行列 (nilpotent Jordan block matrix)** と呼ぶことにする. 特に $J_1(\alpha)$ は 1 次の正方行列なので数の α と同一視できる.

さて, 問題の答は以下の通り.

定理 23.7 (巾零行列の標準形) 任意の巾零行列 $N \in M_n(K)$ に対してある正則行列 $P \in GL_n(K)$ をうまく選んで, $P^{-1}NP$ が対角線に巾零 Jordan ブロック $J_{m_1}(0), \ldots, J_{m_t}(0)$ が並んだ形の行列になるようにできる:

$$P^{-1}NP = \begin{bmatrix} J_{m_1}(0) & & 0 \\ & \ddots & \\ 0 & & J_{m_t}(0) \end{bmatrix} = \begin{bmatrix} 0 & 1 & \cdots & 0 & & & & & & & 0 \\ & 0 & \ddots & \vdots & & & & & & & \\ & & \ddots & 1 & & & & & & & \\ 0 & & & 0 & & & & & & & \\ & & & & \ddots & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & 0 & 1 & \cdots & 0 & \\ & & & & & & & 0 & \ddots & \vdots & \\ & & & & & & & & \ddots & 1 & \\ 0 & & & & & & 0 & & & 0 & \end{bmatrix}.$$

しかも $(m_1,\dots,m_t)$ はその並べ方の順序を除いて P の取り方によらずに N のみから一意に定まる. この形の $P^{-1}NP$ を巾零行列 N の Jordan 標準形と呼び, 各 $J_{m_i}(0)$ を N の Jordan 細胞と呼ぶ. □

我々が目標としている最終定理は次の Jordan 標準形の存在と一意性である.

定理 23.8 (Jordan 標準形) 任意の正方行列 $A \in M_n(K)$ に対してある正則行列 $P \in GL_n(K)$ で $P^{-1}AP$ が対角線に Jordan ブロック $J_{m_1}(\alpha_1),\dots,J_{m_t}(\alpha_t)$ が並んだ形の行列になるようにできる:

$$P^{-1}AP = \begin{bmatrix} J_{m_1}(\alpha_1) & & 0 \\ & \ddots & \\ 0 & & J_{m_t}(\alpha_t) \end{bmatrix} = \begin{bmatrix} \alpha_1 & 1 & & 0 & & & & & 0 \\ & \alpha_1 & \ddots & & & & & & \\ & & \ddots & 1 & & & & & \\ 0 & & & \alpha_1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & \ddots & & & \\ & & & & & & \alpha_t & 1 & 0 \\ & & & & & & & \alpha_t & \ddots \\ & & & & & & & & \ddots & 1 \\ 0 & & & & & & 0 & & & \alpha_t \end{bmatrix}.$$

しかも $(m_1,\alpha_1;\dots;m_t,\alpha_t)$ はその並べ方の順序を除いて P の取り方によらず, A だけから一意に定まる. 上の $P^{-1}AP$ を行列 A の **Jordan 標準形 (Jordan normal form, Jordan canonical form)** と呼び, 各 $J_{m_i}(\alpha_i)$ を A の **Jordan 細胞 (Jordan cell)** と呼ぶ. □

以下における我々の目標は以上の結果を証明することである.

[**388**] Jordan 標準形の一歩手前 [**384**] の結果と巾零行列の標準形の存在 (定理 23.7 の一部) を仮定して, 正方行列の Jordan 標準形の存在 (定理 23.8 の一部) を証明せよ. □

ヒント: Jordan 標準形の一歩手前 [**384**] の結果より, 任意の正方行列 $A \in M_n(K)$ に対してある正則行列 $Q \in GL_n(K)$ が存在して $Q^{-1}AQ$ は次の形になる:

$$Q^{-1}AQ = \begin{bmatrix} \alpha_1 E_{n_1} & & 0 \\ & \ddots & \\ 0 & & \alpha_s E_{n_s} \end{bmatrix} + \begin{bmatrix} N_1 & & 0 \\ & \ddots & \\ 0 & & N_s \end{bmatrix}.$$

ここで $\alpha_1,\dots,\alpha_s$ は A の相異なる固有値の全体であり, n_i は α_i の重複度であり, N_i は n_i 次の巾零行列である. 巾零行列の標準形の存在より, 各 N_i に対してある正則行列 $R_i \in GL_{n_i}(K)$ が存在して $R_i^{-1}N_iR_i$ が次の形になる:

$$R_i^{-1}N_iR_i = \begin{bmatrix} J_{m_{i1}}(0) & & 0 \\ & \ddots & \\ 0 & & J_{m_{i,t(i)}}(0) \end{bmatrix}.$$

R_i を順に対角線に並べてできる行列を R と書き, $P = QR$ と置く. $\alpha_{ij} = \alpha_i$ $(i = 1,\dots,s,\ j = 1,\dots,t(i))$ と置き, (m_{ij},α_{ij}) 全体の番号を付け直して, (m_k,α_k) $(k = 1,\dots,t)$ と書く. このとき $P^{-1}AP$ はちょうど定理 23.8 の Jordan 標準形の形になっている. □

巾零行列 $N \in M_n(K)$ に対して $V = K^n$ の部分空間 V_j を次のように定める:

$$V_j = \operatorname{Ker} N^j = \{\, v \in V = K^n \mid N^j v = 0 \,\} \qquad (j = 0, 1, 2, \ldots).$$

これ以後 $N^{\nu-1} \neq 0$, $N^\nu = 0$ であると仮定する. このとき, j が大きくなるほど N^j の作用で 0 になるベクトルは増えるので

$$0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_{\nu-1} \subset V_\nu = V = K^n.$$

そして $NV_j \subset V_{j-1}$ が成立している. この様子と相性の良い $V = K^n$ の基底を取ることが目標である. (その基底で N を表示すると巾零行列の標準形の形になっている.)

この段落は一般論であり, この段落に限っては V と書いても K^n であるとは限らない. 一般に K 上のベクトル空間 U とその部分空間 V に対して U の部分空間 W が V の**補空間 (complement)** であるとは U が V と W の直和分解されること (すなわち $U = V \oplus W$) である[112]. V の基底を $\{v_i\}_{i\in I}$ とするとそれに一次独立な U のベクトルの集合 $\{w_j\}_{j\in J}$ を追加して U の基底を構成することができる[113]. そのとき W を $\{w_j\}_{j\in J}$ で張られる U の部分空間[114]とすると W は V の補空間である. 以下では U の任意の部分空間 V の U における補空間 W が存在することを自由に用いる.

さて我々の議論の基礎になるのは次の結果である.

[389] 上の方の記号のもとで $j = 2, \ldots, \nu$ に対して, V_j における V_{j-1} の補空間 X_j を任意に取る. このとき N の X_j への制限は単射である. さらに $NX_j \subset V_{j-1}$, $NX_j \cap V_{j-2} = 0$ が成立しているので V_{j-1} における V_{j-2} の補空間で NX_j を含むものが存在する. □

ヒント: $v \in X_j$, $Nv = 0$ ならば $N^{j-1}v = 0$ すなわち $v \in V_{j-1}$ となり $v \in X_j \cap V_{j-1} = 0$ となる. よって N の X_j への制限は単射である. $X_j \subset V_j$ なので $NX_j \subset NV_j \subset V_{j-1}$ である. $v \in X_j$ が $Nv \in V_{j-2}$ を満たしているならば $N^{j-1}v = 0$ すなわち $v \in V_{j-1}$ となるので $v \in X_j \cap V_{j-1} = 0$ なので $Nv = N0 = 0$ である. これで $NX_j \cap V_{j-2} = 0$ も示された. よって NX_j の基底と V_{j-2} の基底の和集合を拡張して V_{j-1} の基底を構成できる. 拡張した分と NX_j の基底の和集合で張られる V_{j-1} の部分空間は V_{j-1} における V_{j-2} の補空間になる. □

上の問題 **[389]** の状況で X_j の基底を $x_1, \ldots, x_p$ と書き, V_{j-1} における V_{j-2} の補空間で NX_j を含むものの基底を $Nx_1, \ldots, Nx_p, y_1, \ldots, y_q$ と取り, V_{j-2} の基底を $N^2x_1, \ldots, N^2x_p$, $Ny_1, \ldots, Ny_q, z_1, \ldots, z_r$ と取ると, 以下のように V_j, V_{j-1}, V_{j-2} の基底が取れたことになる:

$$V_j \left\{ \begin{array}{l} \qquad\qquad x_1, \ldots, x_p \\ V_{j-1} \left\{ \begin{array}{l} \qquad Nx_1, \ldots, Nx_p, \quad y_1, \ldots, y_q \\ V_{j-2} \{\ N^2x_1, \ldots, N^2x_p,\ Ny_1, \ldots, Ny_q,\ z_1, \ldots, z_r \end{array} \right. \end{array} \right.$$

---

[112] 任意の $u \in U$ が $u = v + w$ $(v \in V, w \in W)$ と一意的に表わされるとき U は V と W に直和分解されるといい, $U = V \oplus W$ と書く. V と W が U の部分空間であるとき $U = V \oplus W$ であるための必要十分条件は $U = V + W$ かつ $V \cap W = 0$ が成立することである.

[113] U が無限次元の場合は選択公理と同値な Zorn の補題が必要になる. Jordan 標準形の理論では有限次元の場合だけを扱うので Zorn の補題を用いた証明を知らなくても何も問題がない.

[114] $\sum_{j\in J} b_j w_j$ ($b_j \in K$ は有限個を除いて 0) の形の U のベクトル全体の集合は U の部分空間をなす. それを $\{w_j\}_{j\in J}$ で張られる U の部分空間と呼ぶ.

この様子を V 全体に拡張しよう. そのために $j=\nu,\nu-1,\nu-2,\dots,1$ と上から順に V_j の部分空間 $U_j\subset W_j$ を以下のように定める.

まず, V_ν における $V_{\nu-1}$ の補空間 U_ν を任意に取り, V_ν の部分空間 W_ν を次のように定義する:

$$W_\nu = U_\nu + NU_\nu + \cdots + N^{\nu-1}U_\nu.$$

次に, $V_{\nu-1}$ における $NU_\nu + V_{\nu-2}$ の補空間 $U_{\nu-1}$ を任意に取り, $V_{\nu-1}$ の部分空間 $W_{\nu-1}$ を次のように定義する:

$$W_{\nu-1} = U_{\nu-1} + NU_{\nu-1} + \cdots + N^{\nu-2}U_{\nu-1}.$$

その次に, $V_{\nu-2}$ における $N^2U_\nu + NU_{\nu-1} + V_{\nu-3}$ の補空間 $U_{\nu-1}$ を任意に取り, $V_{\nu-2}$ の部分空間 $U_{\nu-2}$ を次のように定義する:

$$W_{\nu-2} = U_{\nu-2} + NU_{\nu-2} + \cdots + N^{\nu-3}U_{\nu-1}.$$

帰納的に V_j の部分空間 $U_j\subset W_j$ が $j=\nu,\nu-1,\dots,k+1$ まで構成されたと仮定する. もしも $k+1=1$ ならばそれで部分空間の構成を終了する. もしも $k+1\geq 2$ ならば V_k における $N^{\nu-k}U_\nu + N^{\nu-k-1}U_{\nu-1} + \cdots + NU_{k+1} + V_{k-1}$ の補空間 U_k を任意に取り, V_k の部分空間 W_k を次のように定義する:

$$W_k = U_k + NU_k + \cdots + N^{k-1}U_k.$$

[**390**] 以上の構成のもとで以下が成立している:

1. $V = W_1\oplus W_2\oplus\cdots\oplus W_\nu$.
2. $W_k = U_k\oplus NU_k\oplus\cdots\oplus N^{k-1}U_k$.
3. N は次の同型写像の列を与える: $U_k \xrightarrow{\sim} NU_k \xrightarrow{\sim}\cdots\xrightarrow{\sim} N^{k-1}U_k$. □

解説: この問題の結論は V が以下の表にあるベクトル空間の直和に分解され, 各 k に対して $U_k, NU_k,\dots,N^{k-1}U_k$ はすべて N による対応によって同型になるということである:

$$\begin{array}{ccccccc}
U_\nu & & & & & & \\
NU_\nu & U_{\nu-1} & & & & & \\
N^2U_\nu & NU_{\nu-1} & U_{\nu-2} & & & & \\
\vdots & \vdots & \vdots & \ddots & & & \\
N^{\nu-3}U_\nu & N^{\nu-4}U_{\nu-1} & N^{\nu-5}U_{\nu-2} & \cdots & U_3 & & \\
N^{\nu-2}U_\nu & N^{\nu-3}U_{\nu-1} & N^{\nu-4}U_{\nu-2} & \cdots & NU_3 & U_2 & \\
N^{\nu-1}U_\nu & N^{\nu-2}U_{\nu-1} & N^{\nu-3}U_{\nu-2} & \cdots & N^2U_3 & NU_2 & U_1
\end{array} \qquad (*)$$

そして右から k 番目の縦の列の直和が W_k に等しく, 下から k 段目までの直和が V_k になる.

ヒント: 問題 [**389**] の結果を用いて上の図 $(*)$ の上の方から順番に示したい結果が成立していることを証明する. U_ν の構成の仕方より

$$V = K^n = V_\nu = U_\nu\oplus V_{\nu-1}.$$

問題 [**389**] より U_ν は $NU_\nu \subset V_{\nu-1}$ に同型に移される. $U_{\nu-1}$ の構成の仕方より

$$V_{\nu-1} = NU_\nu \oplus U_{\nu-1} \oplus V_{\nu-2}.$$

問題 [**389**] より $NU_\nu \oplus U_{\nu-1}$ は $N^2U_\nu \oplus NU_{\nu-1} \subset V_{\nu-2}$ に同型にうつされる[115]. $U_{\nu-2}$ の構成より

$$V_{\nu-2} = N^2U_\nu \oplus NU_{\nu-1} \oplus U_{\nu-2} \oplus V_{\nu-2}.$$

以上の議論を帰納的に繰り返せば良い. □

各 U_k の基底 $u_{k1}, \ldots, u_{k,t_k}$ 任意に取り, それらを次のような順番に並べる:

$$\begin{aligned}
&u_{11};\ \ldots;\ u_{1t_1};\\
&Nu_{21}, u_{21};\ \cdots;\ Nu_{2t_2}, u_{2t_2};\\
&N^2u_{31}, Nu_{31}, u_{31};\ \cdots;\ N^2u_{3t_3}, Nu_{3t_3}, u_{3t_3};\\
&\qquad\qquad \cdots\cdots\cdots\\
&N^{\nu-1}u_{\nu1}, \ldots, N^2u_{\nu1}, Nu_{\nu1}, u_{\nu1};\ \cdots;\ N^{\nu-1}u_{\nu t_\nu}, \ldots, N^2u_{\nu t_\nu}, Nu_{\nu t_\nu}, u_{\nu t_\nu}.
\end{aligned} \tag{$**$}$$

問題 [**390**] よりこれらは V の基底をなす. これらの全体を $p_1, \ldots, p_n$ と書き $P = [p_1\ \cdots\ p_n]$ と置く.

[**391**] 以上の構成のもとで $P^{-1}NP$ は定理 23.7 の意味で標準形になっている. □

ヒント: $(**)$ の $(u_{11}; \cdots; N^{\nu-1}u_{\nu t_\nu}, \ldots, Nu_{\nu t_\nu}, u_{\nu t_\nu})$ の部分列 $(N^{k-1}u_{ki}, \ldots, Nu_{ki}, u_{ki})$ で張られる $V = K^n$ の部分空間は $N^k u_{ki} = 0$ なので N の作用で閉じている. N を $N^{k-1}u_{ki}, \ldots, Nu_{ki}, u_{ki}$ に作用させると,

$$N[N^{k-1}u_{ki}\ \ldots\ Nu_{ki}\ u_{ki}] = [N^{k-1}u_{ki}\ \ldots\ Nu_{ki}\ u_{ki}] \begin{bmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}.$$

よって $P^{-1}NP$ はこの式の右辺に表われた巾零 Jordan ブロックを対角線に並べた形になる. □

以上によって巾零行列の存在 (定理 23.7 の一部) が証明された. よって問題 [**388**] によって Jordan 標準形の存在 (定理 23.8 の一部) も証明されたことになる. あとは Jordan 標準形の一意性だけが問題になる.

[**392**] 巾零行列 $N \in M_n(K)$ の j 次の[116] Jordan 細胞の個数は

$$(\dim \mathrm{Ker}\, N^j - \dim \mathrm{Ker}\, N^{j-1}) - (\dim \mathrm{Ker}\, N^{j+1} - \dim \mathrm{Ker}\, N^j)$$

に等しい. 特に巾零 Jordan 細胞の全体 $(J_{m_1}(0), \ldots, J_{m_t}(0))$ はその並べ方を除いて巾零行列 N だけから一意に定まる. □

[115] 同型写像は直和を保つ.
[116] 「サイズが j の」という意味.

ヒント: $N' = P^{-1}NP$ が標準形になっていると仮定し, N' に対して図 $(*)$ の状況を構成し, U_j の代わりに U'_j と表わす. N' は標準形になっているので基底 $(**)$ は $V = K^n$ の標準的な基底を並べ直すことによって構成できる. その作業を実行すれば N' の中のサイズ j の Jordan 細胞の個数は $\dim U'_j$ に等しいことがわかる. N, U_j を $N', U'j$ で置き換えた図 $(*)$ において下から j 段目までの部分空間の直和は $\operatorname{Ker} N'^j$ に等しい. よって下から j 段目だけの部分空間の直和の次元は $\dim \operatorname{Ker} N'^j - \dim \operatorname{Ker} N'^{j-1}$ に等しい. したがって U'_j の次元は「下から j 段目だけの部分空間の直和の次元」から「下から $j+1$ 段目だけの部分空間の直和の次元」を引いた数に等しい. 以上によって N' の中のサイズ j の Jordan 細胞の個数は

$$\dim U'_j = (\dim \operatorname{Ker} N'^j - \dim \operatorname{Ker} N'^{j-1}) - (\dim \operatorname{Ker} N'^{j+1} - \dim \operatorname{Ker} N'^j)$$

に等しい. $N'^j = P^{-1}N^jP$ なので $\dim \operatorname{Ker} N'^j = \dim \operatorname{Ker} N^j$ なので示したい結果が得られる. □

これで定理 23.7 (巾零行列の標準形の存在と一意性) が証明された.

[393] 正方行列 $A \in M_n(K)$ の固有値 α に属する j 次の Jordan 細胞の個数は $B = A - \alpha E$ に対する

$$(\dim \operatorname{Ker} B^j - \dim \operatorname{Ker} B^{j-1}) - (\dim \operatorname{Ker} B^{j+1} - \dim \operatorname{Ker} B^j)$$

に等しい. 特に Jordan 細胞の全体 $(J_{m_1}(\alpha_1), \ldots, J_{m_t}(\alpha_t))$ はその並べ方を除いて正方行列 A だけから一意に定まる. □

ヒント: $A' = P^{-1}AP$ が Jordan 標準形になっていると仮定し, $B' = A' - \alpha E$ の中の巾零 Jordan ブロック全体を対角線に並べてできる行列を N' と書く. このとき $\dim \operatorname{Ker} B'^j = \dim \operatorname{Ker}(N')^j$ であり, N' の中のサイズ j の巾零 Jordan 細胞の個数と A' の中の固有値 α に属する j 次の Jordan 細胞の個数に等しい. よって, 問題 **[392]** の結果より, A' の中の固有値 α に属する j 次の Jordan 細胞の個数は

$$(\dim \operatorname{Ker} B'^j - \dim \operatorname{Ker} B'^{j-1}) - (\dim \operatorname{Ker} B'^{j+1} - \dim \operatorname{Ker} B'^j)$$

に等しい. $B'^j = P^{-1}B^jP$ なので示したい結果が得られる. □

これで定理 23.8 (正方行列の Jordan 標準形の存在と一意性) も証明された.

[394] 次の n 次複素正方行列 A の Jordan 標準形 J と $P^{-1}AP = J$ を満たす正則行列 P の例と最小多項式 $\varphi(\lambda)$ を求めよ:

$$A = \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ a^n & & & 0 \end{bmatrix} \qquad (a \in \mathbb{C}). \quad \square$$

ヒント: $a = 0$ のときは A 自身が Jordan 標準形になっているので, $a \neq 0$ の場合だけが問題になる. $a \neq 0$ と仮定する. A の特性多項式は $p_A(\lambda) = \lambda^n - a^n$ なので A は互いに異なる n 個の固有値 $ae^{2\pi ik/n}$ $(k = 0, 1, \ldots, n-1)$ を持つ. よって A は☆単☆であり, その Jordan 標準形 J は相異なる固有値を☆角成☆に並べた対☆☆列になる. 最小多項式は☆☆多☆式に等しい. 固有値 $\alpha_k = ae^{2\pi ik/n}$ に属す固有ベクトルとして $p_k = {}^t[1 \ \alpha_k \ \alpha_k^2 \ \cdots \ \alpha_k^{n-1}]$ が取れる. これを並べてできる行列を P とすれば $P^{-1}AP = J$ となる. □

[395] p は任意の素数であるとし, K は標数 p の代数閉体であるとする[117]. 次のように定められた p 次正方行列 $A \in M_p(K)$ の Jordan 標準形を求めよ:

$$A = \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ a^p & & & 0 \end{bmatrix} \qquad (a \in K). \quad \square$$

ヒント: $a = 0$ のときは A 自身が Jordan 標準形になっているので, $a \neq 0$ の場合だけが問題になる. $a \neq 0$ と仮定する. 一般に標数 p の世界では $(a-b)^p = a^p - b^p$ である. よって A の特性多項式は $p_A(\lambda) = \lambda^p - a^p = (\lambda - a)^p$ になる. $(A - aE)^{p-1}$ の一番右上の成分は 1 になるので $(A - aE)^{p-1} \neq 0$ である (問題 **[376]** のヒントを見よ). よって A の最小多項式は特性多項式に一致することがわかる[118]. したがって A の Jordan 標準形は $J_p(a)$ になる. $\square$

参考: 標数 p の世界では $(\lambda - a)(\lambda^{p-1} + a\lambda^{p-2} + a^2\lambda^{p-3} + \cdots + a^{p-2}\lambda + a^{p-1}) = \lambda^p - a^p = (\lambda - a)^p$ であるから, $(\lambda - a)^{p-1} = \lambda^{p-1} + a\lambda^{p-2} + a^2\lambda^{p-3} + \cdots + a^{p-2}\lambda + a^{p-1}$ である. この公式を用いて $(A - aE)^{p-1}$ を計算してみよ. すると, K^p の標準的基底を $e_1, \ldots, e_p$ と書くとき, $(A - aE)^{p-1}e_p = {}^t[1\ a\ a^2\ \cdots\ a^{p-1}] \neq 0$ となることがわかる. よって

$$(A - aE)^{p-1}e_p, \cdots, (A - aE)^2 e_p, (A - aE)e_p, e_p$$

は K^p の基底をなし, その基底に関する A の表現は A の Jordan 標準形になる. $\square$

[396] p は任意の素数であるとし, K は標数 0 の体であるとする. このとき任意の $a, b \in K$ に対して $(a+b)^p = a^p + b^p$ かつ $(-a)^p = -a^p$ である[119]. $\square$

ヒント: 二項定理より

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-2}a^2b^{p-2} + \binom{p}{p-1}ab^{p-1} + b^p.$$

しかし, $\binom{p}{1}, \ldots, \binom{p}{p-1}$ は p で割り切れるので K の中で 0 になる. よって $(a+b)^p = a^p + b^p$ である. 特に $b = -a$ と置くと $0 = (a + (-a))^p = a^p + (-a)^p$ である. よって $(-a)^p = -a^p$ である[120]. $\square$

[397] 正方行列 $A \in M_n(K)$ の特性多項式を $p_A(\lambda)$ と表わす. K は代数閉体だと仮定したので特性多項式は次のように一次式の積に分解される:

$$p_A(\lambda) = (\lambda - \alpha_1)^{n_1} \cdots (\lambda - \alpha_s)^{n_s}.$$

ここで $\alpha_1, \ldots, \alpha_s$ たちは $p_A(\lambda)$ の相異なる根の全体である. このとき以下の二条件は互いに同値である:

---

[117] 最小の標数 p の代数閉体は p 個の元を持つ有限体 $\mathbb{F}_p$ に 1 の巾根をすべて付け加えてできる $\mathbb{F}_p$ の代数閉包 $\overline{\mathbb{F}}_p$ である.

[118] 実は問題 **[375]** の特殊な場合.

[119] $(ab)^p = a^p b^p$ であることは明らかなので $a \mapsto a^p$ は K から K 自身への体の準同型写像になっている. これは **Frobenius 準同型 (Frobenius homomorphism)** と呼ばれている.

[120] 次のように考えても良い. $p = 2$ のとき K の中で $2 = 0$ より $a + a = 0$ なので $-a = a$ である. よって $p = 2$ のとき $(-a)^p = (-a)^2 = a^2 = -a^2$ である. p が奇素数のとき $(-a)^p = -a^p$ である.

(a) A の最小多項式は特性多項式 $p_A(\lambda)$ に一致する.

(b) A の Jordan 標準形 J は次の形になる:

$$J = \begin{bmatrix} J_{n_1}(\alpha_1) & & 0 \\ & \ddots & \\ 0 & & J_{n_s}(\alpha_s) \end{bmatrix}.$$

すなわち A の各固有値 α_i に属する Jordan 細胞は唯一つになる. □

ヒント: A の固有値 α_i に属する Jordan 細胞のすべてを対角線に並べてできる n_i 次正方行列を J_i と書くことにする. A の Jordan 標準形 J は J_i を対角線に並べた行列になる. A の最小多項式は J の最小多項式に等しいので, (a) が成立するための必要十分条件は $(J_i - \alpha_i)^{n_i - 1} \neq 0$ が成立することである. それが成立するための必要十分条件は $J_i = J_{n_i}(\alpha_i)$ すなわち (b) が成立することである. もしも J_i の中に Jordan 細胞が複数含まれているとすればある $m < n_i$ で $(J_i - \alpha_i)^m = 0$ となってしまうことが簡単に確かめられる. $J_m(0)^{m-1} \neq 0$, $J_m(0)^m = 0$ に注意せよ. □

24 行列方程式 $AX - XB = C$

すでに行列の対角化や Jordan 標準形の重要な応用先として A^n や e^{At} を計算する問題があることをすでに説明した. この節では別の応用先について説明しよう.

K は任意の代数閉体であると仮定し, K の元を成分に持つ行列について考える. K の元を数と呼ぶことがある. 「任意の代数閉体」という言葉を使うのが怖い人は $K = \mathbb{C}$ であると考えてよい.

この節では $A = [a_{ij}]$ は m 次正方行列であるとし, $B = [b_{ij}]$ は n 次正方行列であるとし, $C = [c_{ij}]$ は (m, n) 型行列であるとする. すなわち $A \in M_m(K)$, $B \in M_n(K)$, $C \in M_{m,n}(K)$ であるとする. この節では $X = [x_{ij}] \in M_{m,n}(K)$ に関する

$$AX - XB = 0$$

という方程式と

$$AX - XB = C$$

という方程式について考える. これらの方程式は応用上たびたび現われる.

さらに写像 $\phi : M_{m,n}(K) \to M_{m,n}(K)$ を

$$\phi(X) = AX - XB \qquad (X \in M_{m,n}(K))$$

と定める. このとき ϕ は線形写像である. 実際, $X, Y \in M_{m,n}(K)$, $a, b \in K$ に対して,

$$\begin{aligned} \phi(aX + bY) &= A(aX + bY) - (aX + bY)B = aAX + bBY - aXB - bYB \\ &= a(AX - XB) + b(AY - YB) = a\phi(X) + b\phi(Y). \end{aligned}$$

[398] 線形写像 ϕ の核 (kernel) と像 (image) の定義を説明し, 以下の事実を説明せよ:

1. 方程式 $AX - XB = 0$ の解全体の集合は $M_{m,n}(K)$ の線形部分空間 $\operatorname{Ker}\phi$ に一致する.

2. 方程式 $AX-XB=C$ の解が存在するような $C\in M_{m,n}(K)$ 全体の集合は $M_{m,n}(K)$ の線形部分空間 $\mathrm{Im}\,\phi$ に一致する.

3. X_1 は方程式 $AX-XB=C$ の任意の解であるとする. このとき方程式 $AX-XB=C$ の解全体の集合は X_1 と方程式 $AX-XB=0$ の解の和全体の集合と一致する. □

Jordan 標準形の理論より, ある正則行列 $P\in GL_m(K)$ と $Q\in GL_n(K)$ が存在して $J_A=P^{-1}AP$ と $J_B=Q^{-1}BK$ はそれぞれ A と B の Jordan 標準形になる. このとき, $Y=PXQ^{-1}$, $D=P^{-1}CQ$ と置けば方程式 $AX-XB=C$ は方程式 $J_AY-YJ_B=D$ と同値になる. 方程式 $AX-XB=C$ の定性的な性質を調べるためには最初から A, B が Jordan 標準形であると仮定してよい. そこで A, B は Jordan 標準形であると仮定する:

$$A=\begin{bmatrix} J_{m_1}(\alpha_1) & & 0 \\ & \ddots & \\ 0 & & J_{m_s}(\alpha_s) \end{bmatrix},\qquad B=\begin{bmatrix} J_{n_1}(\beta_1) & & 0 \\ & \ddots & \\ 0 & & J_{n_t}(\beta_t) \end{bmatrix}.$$

X, C を (m_μ,n_ν) 型行列 $X_{\mu\nu}$, $C_{\mu\nu}$ に分割して

$$X=\begin{bmatrix} X_{11} & \cdots & X_{1t} \\ \vdots & & \vdots \\ X_{s1} & \cdots & X_{st} \end{bmatrix},\qquad C=\begin{bmatrix} C_{11} & \cdots & C_{1t} \\ \vdots & & \vdots \\ C_{s1} & \cdots & C_{st} \end{bmatrix}$$

と表わしておく. このとき方程式 $AX-XB=C$ は次の連立方程式と同値である:

$$J_{m_\mu}(\alpha_\mu)X_{\mu\nu}J_{n_\nu}(\beta_\nu)=C_{\mu\nu}\qquad(\mu=1,\dots,s,\ \nu=1,\dots,t).$$

これより方程式 $AX-XB=C$ の定性的性質を調べる問題は A, B が Jordan ブロック行列である場合に帰着する.

[399] $\alpha\neq\beta$, $A=J_m(\alpha)$, $B=J_n(\beta)$ であるとき以下が成立する:

1. 方程式 $AX-XB=0$ の解は $X=0$ 以外に存在しない.

2. 任意の $C\in M_{m,n}(K)$ に対して $AX-XB=C$ の解が唯一存在する. □

ヒント 1: AX と BX を具体的に書き下すと,

$$AX=J_m(\alpha)X=\begin{bmatrix} \alpha x_{11}+x_{21} & \alpha x_{12}+x_{22} & \cdots & \alpha x_{1n}+x_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha x_{m-1,1}+x_{m1} & \alpha x_{m-1,2}+x_{m2} & \cdots & \alpha x_{m-1,n}+x_{m-1,n} \\ \alpha x_{m1}+0 & \alpha x_{m2}+0 & \cdots & \alpha x_{m,n}+0 \end{bmatrix},$$

$$XB=XJ_n(\beta)=\begin{bmatrix} \beta x_{11}+0 & \beta x_{12}+x_{11} & \cdots & \beta x_{1n}+x_{1,n-1} \\ \vdots & \vdots & & \vdots \\ \beta x_{m-1,1}+0 & \beta x_{m-1,2}+x_{m-1,1} & \cdots & \beta x_{m-1,n}+x_{m-1,n-1} \\ \beta x_{m1}+0 & \beta x_{m2}+x_{m1} & \cdots & \beta x_{m,n}+x_{m,n-1} \end{bmatrix}.$$

まず AX と XB の一番左下の $(m,1)$ 成分を比較する. $\alpha\neq\beta$ と仮定したので $x_{m1}=0$ であることがわかる. 次に第 1 列を下から順に比較して行くと X の第 1 列がすべて 0 であ

ることがわかる. 同様に第 m 行を左から右に順に比較して行くと X の第 m 行がすべて 0 であることがわかる. 第 2 列と第 $m-1$ 行以降も左下から上もしくは右に順次成分を比較して行けば全部 0 であることが確かめられる. よって $AX - XB = 0$ の解は $X = 0$ だけである. 同様の順序で $AX - XB = C$ の両辺の成分を比較すると, 任意の C に対して方程式 $AX - XB = C$ の解 X が一意に存在することが確かめられる. □

ヒント 2: $AX - XB = 0$ の解が $X = 0$ だけであることと問題 [**398**] の結果から, 任意の C に対して $AX - XB = C$ の解が一意に存在することを示せる. 問題 [**398**] の 3 より解の一意性が出る. $\dim \mathrm{Im}\,\phi = \dim M_{m,n}(K) - \dim \mathrm{Ker}\,\phi = \dim M_{m,n}(K)$ より ϕ は全射である. よって問題 [**398**] の 3 より解の存在が出る. □

[**400**] $A = J_m(\alpha)$, $B = J_n(\alpha)$ であるとき以下が成立する:

1. $m \leq n$ のとき方程式 $AX - XB = 0$ の任意の解は次の形で一意に表わされる:

$$X = \begin{bmatrix} 0 & \cdots & 0 & x_1 & x_2 & x_3 & \cdots & x_m \\ & 0 & \cdots & 0 & x_1 & x_2 & \ddots & \vdots \\ & & 0 & \cdots & 0 & x_1 & \ddots & x_3 \\ & & & \ddots & & \ddots & \ddots & x_2 \\ 0 & & & & 0 & \cdots & 0 & x_1 \end{bmatrix}.$$

2. $m \geq n$ のとき方程式 $AX - XB = 0$ の任意の解は次の形で一意に表わされる:

$$X = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ 0 & x_1 & x_2 & \ddots & \vdots \\ \vdots & 0 & x_1 & \ddots & x_3 \\ 0 & \vdots & 0 & \ddots & x_2 \\ & 0 & \vdots & \ddots & x_1 \\ & & 0 & & 0 \\ & & & \ddots & \vdots \\ 0 & & & & 0 \end{bmatrix}.$$

3. 特に方程式 $AX - XB = 0$ の解空間 $\mathrm{Ker}\,\phi$ の次元は $\min\{m, n\}$ になる. □

ヒント: $J_m(\alpha)X - XJ_n(\alpha) = J_m(0)X - XJ_n(0)$ なので $\alpha = 0$ の場合に帰着する. あとはその各成分を具体的に書き表わし, じっと眺めれば問題の結果が成立していることがわかる. 感じがつかめなければ $(m, n) = (3, 5), (4, 5), (5, 3), (5, 4)$ などの場合に $J_m(0)X - XJ_n(0)$ の全成分を書き下してみよ. □

[**401**] $A = J_m(\alpha)$, $B = J_n(\alpha)$ であるとき以下が成立する:

1. $m \leq n$ のとき方程式 $AX - XB = C$ の解が存在するための必要十分条件は C が次満たしていることである.

$$c_{m1} = 0,$$
$$c_{m-1,1} + c_{m2} = 0,$$

$$\cdots\cdots$$
$$c_{21} + \cdots + c_{m,m-1} = 0,$$
$$c_{11} + c_{22} + \cdots + c_{mm} = 0.$$

この条件は C の中の左上から右下に向けて斜めの成分を足し上げたものが左下から m 段目まで 0 になるという条件である.

2. $m \geq n$ のとき方程式 $AX - XB = C$ の解が存在するための必要十分条件は C が次満たしていることである.

$$c_{m1} = 0,$$
$$c_{m-1,1} + c_{m2} = 0,$$
$$\cdots\cdots$$
$$c_{m-n+2,1} + \cdots + c_{m,n-1} = 0,$$
$$c_{m-n+1,1} + c_{m-n+2,2} + \cdots + c_{mn} = 0.$$

この条件は C の中の左上から右下に向けて斜めの成分を足し上げたものが左下から n 段目まで 0 になるという条件である.

3. 特に方程式 $AX - XB = C$ が解を持つ C 全体の空間 $\mathrm{Im}\,\phi$ の次元は $mn - \min\{m, n\}$ になる. □

ヒント: $J_m(\alpha)X - XJ_n(\alpha) = J_m(0)X - XJ_n(0)$ なので $\alpha = 0$ の場合に帰着する. あとはその各成分を具体的に書き表わし, じっと眺めれば問題の結果が成立していることがわかる. 感じがつかめなければ $(m, n) = (3, 5), (4, 5), (5, 3), (5, 4)$ などの場合に $J_m(0)X - XJ_n(0)$ の全成分を書き下してみよ. □

[402] $A \in M_m(K)$ の固有値全体の集合と $B \in M_n(K)$ の固有値全体の集合の交わりが空ならば以下が成立する:

1. 方程式 $AX - XB = 0$ の解は $X = 0$ だけである.
2. 任意の $C \in M_{m,n}(K)$ に対して方程式 $AX - XB = C$ の解が一意に存在する. □

ヒント: 問題 **[399]** に帰着する. □

解説: この問題の結果は $\det A \neq 0$ ならば任意の C に対して方程式 $AX = C$ の解が一意に存在するという結果を含んでいる. $AX = C$ は $B = 0$ の場合の $AX - XB = C$ という方程式である. $B = 0$ の固有値全体の集合は $\{0\}$ である. よって A の固有値全体の集合と B の固有値全体の集合の交わりが空であるという条件は A のすべての固有値が 0 でないという条件と同値である. その条件は $\det A \neq 0$ と同値である. □

[403] $m = n$ かつ $A = B$ の場合について考える. $A \in M_n(K)$ に対して以下の条件は互いに同値である:

(a) A の最小多項式は特性多項式に一致する.

(b) A の各固有値に属す Jordan 細胞は唯一つである.

(c) $X \in M_n(K)$ に関する方程式 $[A, X] = 0$ の解全体の空間の次元が n になる[121].

一般に方程式 $[A, X] = 0$ の解全体の空間の次元は n 以上になる. □

ヒント: (a) と (b) の同値性は問題 **[397]** である. よって (b) と (c) の同値性と $[A, X] = 0$ の解全体の空間の次元が n 以上であることを示すことだけが問題になる. 最初から A は Jordan 標準形であると仮定して良いので, 解くべき問題は問題 **[399]**, **[400]** に帰着する. たとえば A, X が

$$A = \begin{bmatrix} J_p(\alpha) & 0 \\ 0 & J_q(\beta) \end{bmatrix}, \qquad X = \begin{bmatrix} P & Q \\ R & S \end{bmatrix}$$

という形をしている場合に限定すれば以下のように証明される. ただしここで $0 < p \leq q$, $p + q = n$, $P \in M_p(K)$, $Q \in M_{p,q}(K)$, $R \in M_{q,p}(K)$, $S \in M_q(K)$ であるとする. このとき $[A, X] = 0$ は次と同値である:

$$J_p(\alpha)P - PJ_p(\alpha) = 0, \quad J_p(\alpha)Q - QJ_q(\beta) = 0,$$
$$J_q(\beta)R - RJ_p(\alpha) = 0, \quad J_q(\beta)S - SJ_q(\beta) = 0.$$

$\alpha \neq \beta$ ならば問題 **[399]** の結果より $Q = 0$, $R = 0$ であり, 問題 **[400]** の結果より P に関する方程式の解空間は p 次元であり, S に関する方程式の解空間は q 次元になるので, $[A, X] = 0$ の解空間の次元は $p + q = n$ になる. $\alpha = \beta$ ならば問題 **[400]** の結果より P, Q, R, S に関する方程式の解空間の次元はそれぞれ p, p, p, q になるので, $[A, X] = 0$ の解空間の次元は $3p + q > n$ となる. □

[404] $m = n$ かつ $A = B$ の場合について考える. $A \in M_n(K)$ が半単純でかつ固有値が重複を持たないと仮定する. このとき以下が成立する:

1. 任意の $X \in M_n(K)$ に対して, $[A, X] = 0$ が成立することと A と X が同時対角化可能であることは同値である.

2. 任意の $C \in M_n(K)$ に対して, $X \in M_n(K)$ に関する方程式 $[A, X] = C$ の解が存在するための必要十分条件は, ある正則行列 $P \in GL_n(K)$ で $P^{-1}AP$ が対角行列でかつ $P^{-1}CP$ の対角成分がすべて 0 になるものが存在することである. □

ヒント: A は半単純 (対角化可能) であると仮定しているのでこの問題はすでに Jordan 標準形の応用問題ではない. 仮定よりある $P \in GL_n(K)$ で $P^{-1}AP = A' = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ (α_i は互いに異なる) となるものが存在する. $X' = P^{-1}XP$, $C' = P^{-1}CP$ と置けば $[A, X] = C$ と $[A', X'] = C'$ は同値である. $[A', X']$ の成分を具体的に書き下し, α_i たちが互いに異なることに注意すれば問題の結果が容易に示される. □

25 単因子の計算と Jordan 標準形

この節では単因子に基いた Jordan 標準形の計算の仕方を解説する. 単因子論とそれに基いた Jordan 標準形の理論の完全な展開は第 27 節で行ない, この節は計算法だけを天下り的に解説するだけですませる. どうしてこの節で解説する方法で Jordan 標準形が正しく求まるかに関しては第 27 節を見よ.

[121] $[A, X] = AX - XA$ である.

なお, 他のほとんどの場所では体 K 上の多項式環として文字 λ から生成されるものを主に用いているがこの節では文字 x から生成されるものを用いる[122].

25.1 一変数多項式環上の行列の単因子の計算

A は体 K 上の一変数多項式環 $K[x]$ 上の (m,n) 型行列であるとする. A に以下の基本操作を有限回ほどこすことを行列の基本変形と呼ぶ:

- A のある行の多項式倍を別の行に加える.
- A のある行に K の 0 でない元をかける.
- A の 2 つの行を交換する.
- A のある列の多項式倍を別の列に加える.
- A のある列に K の 0 でない元をかける.
- A の 2 つの列を交換する.

A は行列の基本変形によって次の形に変形できる:

$$\begin{bmatrix} g_1 & & & 0 \\ & g_2 & & \\ & & g_3 & \\ 0 & & & \ddots \end{bmatrix}, \qquad g_i \text{ はモニックまたは } 0 \text{ で } g_1 \mid g_2 \mid g_3 \mid \cdots.$$

ここで $f \mid g$ は「f が g を割り切る」という意味である. 0 は任意の f で割り切れることに注意せよ $(0 = 0 \cdot f)$. しかも $(g_1, g_2, \ldots)$ は A に対して一意的である. $(g_1, g_2, \ldots)$ を A の**単因子 (elementary divisor)** と呼ぶ.

例 25.1 単因子の計算の仕組みの一端を理解するために $\mathbb{Q}[x]$ 上の次の行列の単因子を求めてみよう:

$$A := \begin{bmatrix} x+1 & 0 \\ 0 & x \end{bmatrix}.$$

$x+1$ は x を割り切らないので $(x, x+1)$ は A の単因子ではない. しかし, 次のように基本変形して A の単因子が $(1, x(x+1))$ であることがわかる:

$$\begin{bmatrix} x+1 & 0 \\ 0 & x \end{bmatrix} \to \begin{bmatrix} x+1 & x \\ 0 & x \end{bmatrix} \to \begin{bmatrix} x+1 & -1 \\ 0 & x \end{bmatrix}$$
$$\to \begin{bmatrix} 1 & x+1 \\ -x & 0 \end{bmatrix} \to \begin{bmatrix} 1 & x+1 \\ 0 & x(x+1) \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & x(x+1) \end{bmatrix}.$$

各矢印の操作はそれぞれ順に以下の通りである: 第 2 行を第 1 行に加える, 第 1 列を第 2 列から引く, 第 1 列と第 2 列を交換してから第 1 列を -1 倍する, 第 1 行の x 倍を第 2 行に足す, 第 1 列の $x+1$ 倍を第 2 列から引く. □

[122] その理由は式を大量にコンピューターに入力するときには λ よりも x の方が易しいからである. λ と出力するためには `\lambda` と入力しなければいけない.

例 25.2 単因子の計算の例をもう一つ示しておこう. これを見れば一般の場合にどのように計算すればよいかがわかるはずである. 例として $\mathbb{Q}[x]$ 上の次の行列の単因子を求めてみよう:

$$A := \begin{bmatrix} 4\,x^2+8\,x+4 & x^2+4\,x+3 & x^3+3\,x^2-2\,x-5 \\ -8\,x^3-8\,x^2+6\,x+6 & -2\,x^3-6\,x^2+x+5 & -2\,x^4-4\,x^3+9\,x^2+6\,x-8 \\ -6\,x^2-6\,x & -2\,x^2-3\,x-1 & -2\,x^3-x^2+4\,x+1 \end{bmatrix}.$$

第 1 列と第 2 列を交換して, 第 1 行の $2x-2$ 倍を第 2 行に足して, 第 1 行と第 2 行を交換して, 第 1 行を -1 倍した結果を A_1 とする:

$$A_1 = \begin{bmatrix} x+1 & 2\,x+2 & x^2-2 \\ x^2+4\,x+3 & 4\,x^2+8\,x+4 & x^3+3\,x^2-2\,x-5 \\ -2\,x^2-3\,x-1 & -6\,x^2-6\,x & -2\,x^3-x^2+4\,x+1 \end{bmatrix}.$$

第 1 行の $x+3$ 倍を第 2 行から引き去り, 第 1 行と第 2 行を交換し, 第 1 列と第 3 列を交換した結果を A_2 とする:

$$A_2 = \begin{bmatrix} 1 & 2\,x^2-2 & 0 \\ x^2-2 & 2\,x+2 & x+1 \\ -2\,x^3-x^2+4\,x+1 & -6\,x^2-6\,x & -2\,x^2-3\,x-1 \end{bmatrix}.$$

第 1 行の倍数を第 2 行以降から引き去り, 第 1 列の倍数を第 2 列以降から引き去り, 第 1 列と第 1 行の第 $(1,1)$ 成分以外をすべて 0 にした結果を A_3 とする:

$$A_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2\,x^4+6\,x^2+2\,x-2 & x+1 \\ 0 & 4\,x^5+2\,x^4-12\,x^3-10\,x^2+2\,x+2 & -2\,x^2-3\,x-1 \end{bmatrix}.$$

第 2 列と第 3 列を交換して, 第 2 行の倍数を第 3 行から引き去り, 第 2 列の倍数を第 3 列から引き去り, 第 2 列と第 2 行の第 $(2,2)$ 成分以外をすべて 0 にした結果を A_4 とすると第 $(3,3)$ 成分も 0 になる:

$$A_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

したがって A の単因子は $(1, x+1, 0)$ である. □

[405] $\mathbb{Q}[x]$ 上の次の行列の単因子を求めよ:

$$\begin{bmatrix} 2\,x^4-8\,x^3+9\,x^2-4\,x+1 & -2\,x^3+4\,x^2-2\,x & 4\,x^4-8\,x^3+4\,x^2+x-1 \\ 2\,x^4-7\,x^3+5\,x^2+x-1 & -2\,x^3+3\,x^2-1 & 4\,x^4-6\,x^3+3\,x-1 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $(x-1, (x-1)^2)$. □

[406] $\mathbb{Q}[x]$ 上の次の行列の単因子を求めよ:

$$\begin{bmatrix} x^5-x^4-x+1 & x^5+2\,x^4-x-2 & x^5+x^4-x-1 \\ x^6-3\,x^5+x^4+x^3+4\,x & x^6-4\,x^4-x^3-2\,x^2-x+3 & x^6-x^5-2\,x^4-x^2+x+2 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $((x^2+1)(x+1),(x^2+1)(x+1)(x-1))$. □

[407] $\mathbb{Q}[x]$ 上の次の行列の単因子を求めよ:

$$\begin{bmatrix} -2\,x^2+3\,x+3 & 0 & -2\,x-1 \\ 8\,x^4-6\,x^3-32\,x^2+7\,x+19 & 4\,x^3-3\,x+1 & 8\,x^4+8\,x^3+4\,x^2-6\,x-7 \\ 4\,x^3-x^2-13\,x-8 & 2\,x^2+2\,x & 4\,x^3+8\,x^2+7\,x+3 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $(1,x+1,x+1)$. □

[408] $\mathbb{Q}[x]$ 上の次の行列の単因子を求めよ:

$$\begin{bmatrix} -2\,x^3-2\,x^2+3\,x+2 & x^2+x-2 & -x+1 & x^2+x-1 & x-2 \\ -2\,x^4+2\,x^2 & x^3-x & x^2-1 & x^3-x & -2\,x^4+4\,x^2-2 \\ 3\,x^2-x-2 & -2\,x+2 & -2\,x^2+2\,x & -x+1 & 2\,x^4-3\,x^2-3\,x+4 \\ 4\,x^4+4\,x^3-5\,x-3 & -2\,x^3-2\,x^2+4 & -2\,x^2+2\,x & -2\,x^3-2\,x^2+2 & 4\,x^4-8\,x^2-3\,x+7 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $(1,x+1,(x+1)(x-1),0)$. □

25.2 単因子に基いた Jordan 標準形の計算

K は代数閉体であるとする[123]. K 上の正方行列 A の**有理標準形 (rational normal form, rational canonical form, Frobebius 標準形, Frobenius normal form, Frobenius canonical form)** と **Jordan 標準形 (Jordan normal form, Jordan canonical form)** を単因子に基いた以下の手続きで求めることができる:

1. **特性行列 (characteristic matrix)** $xE-A$ の単因子を求める.
2. 単因子の中から 1 を除いたものを $f_1,\dots,f_s$ とする.
3. このとき A の有理標準形は $f_1,\dots,f_s$ に対応するコンパニオン行列を対角線に並べてできる正方行列になる. ただし多項式

   $$f(x)=x^n+a_0x^{n-1}+a_1x^{n-2}+\cdots+a_{n-2}x+a_{n-1}\in K[x]$$

   に対応する**コンパニオン行列 (同伴行列, companion matrix)** C_f は次のように定義される:

   $$C_f=\begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & \ddots & & \\ & & \ddots & 1 & \\ 0 & & & 0 & 1 \\ -a_{n-1} & -a_{n-2} & \cdots & -a_1 & -a_0 \end{bmatrix}.$$

[123] 代数閉体という言葉が怖ければ $K=\mathbb{C}$ だと仮定して良い.

4. すべての f_i を一次式の積に分解する:

$$f_i(x) = (x - \alpha_{i,1})^{n_{i,1}} \cdots (x - \alpha_{i,r_i})^{n_{i,r_i}}.$$

ここで $\alpha_{i,1}, \ldots, \alpha_{i,r_i} \in K$ は互いに異なり, $n_{i,1}, \ldots, n_{i,r_i}$ は正の整数である.

5. このとき A の **Jordan 細胞 (Jordan cell)** の全体は

$$J_{n_{i,j}}(\alpha_{i,j}) \qquad (i = 1, \ldots, s,\ j = 1, \ldots, r_i).$$

になり, A の Jordan 標準形はこれらの Jordan 細胞を対角線に並べてできる正方行列になる. ただし $J_n(\alpha)$ は次の形の n 次正方行列である:

$$J_n(\alpha) = \begin{bmatrix} \alpha & 1 & & & 0 \\ & \alpha & 1 & & \\ & & \alpha & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \alpha \end{bmatrix}. \quad \square$$

[409] 体 K 上の一変数多項式

$$f(x) = x^n + a_0 x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-2} x + a_{n-1} x \in K[x]$$

に対応するコンパニオン行列 C_f の特性行列 $xE - C_f$ の単因子が $(1, \ldots, 1, f)$ になることを直接確かめよ. $\square$

ヒント: たとえば $f(x) = x^4 + ax^3 + bx^2 + cx + d$ の特性行列 $xE - C_f$ は以下のように基本変形できる:

$$\begin{bmatrix} x & -1 & 0 & 0 \\ 0 & x & -1 & 0 \\ 0 & 0 & x & -1 \\ d & c & b & a+x \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 & x \\ x & -1 & 0 & 0 \\ 0 & x & -1 & 0 \\ c & b & a+x & d \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 & 0 \\ x & -1 & 0 & 0 \\ 0 & x & -1 & 0 \\ c & b & a+x & d+cx \end{bmatrix}$$

$$\to \begin{bmatrix} -1 & 0 & 0 & 0 \\ x & -1 & 0 & 0 \\ 0 & x & -1 & x^3 \\ c & b & a+x & d+cx+bx^2 \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 & 0 \\ x & -1 & 0 & 0 \\ 0 & x & -1 & 0 \\ c & b & a+x & d+cx+bx^2+ax^3+x^4 \end{bmatrix}$$

$$\to \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & f(x) \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & f(x) \end{bmatrix}.$$

ここでそれぞれの矢印は順に次のような行列の基本変形である: 第 1 列が第 4 列にくるように列を巡回置換する, 第 1 列の x 倍を第 4 列に加える, 第 2 列の x^2 倍を第 4 列に加える, 第 3 列の x^3 倍を第 4 列に加える, 行の基本変形によって対角成分以外を 0 にする, 第 1 行から第 3 行に -1 をかけて対角成分の -1 を 1 にする. これで C_f の特性行列の単因子が $(1, 1, 1, f(x))$ になることがわかった. $\square$

例 25.3 単因子に計算に基いた Jordan 標準形の計算の例を一つ示そう. これを見れば一般の場合にもどのように計算すればよいかがわかるはずである. 例として $\mathbb{Q}$ 上の次の行列の Jordan 標準形を求めてみよう:

$$A := \begin{bmatrix} -4 & -7 & 6 & -11 & -6 \\ 2 & 1 & -1 & 2 & -1 \\ 4 & 4 & -2 & 4 & -1 \\ 2 & 5 & -4 & 7 & 5 \\ 0 & -4 & 5 & -8 & -8 \end{bmatrix}.$$

この行列の特性行列 $xE - A$ を A_0 と書くことにする:

$$A_0 = xE - A = \begin{bmatrix} x-4 & -7 & 6 & -11 & -6 \\ 2 & x+1 & -1 & 2 & -1 \\ 4 & 4 & x-2 & 4 & -1 \\ 2 & 5 & -4 & x+7 & 5 \\ 0 & -4 & 5 & -8 & x-8 \end{bmatrix}.$$

これに行列の基本変形をほどこして単因子を求めよう. A_0 の第 2 行に -1 をかけて, 第 2 行と第 1 行を交換し, 第 5 列を第 1 列と交換した結果を A_1 とする:

$$A_1 = \begin{bmatrix} 1 & -x-1 & 1 & -2 & -2 \\ -6 & -7 & 6 & -11 & x-4 \\ -1 & 4 & x-2 & 4 & 4 \\ 5 & 5 & -4 & x+7 & 2 \\ x-8 & -4 & 5 & -8 & 0 \end{bmatrix}.$$

第 1 行の倍数を残りの行から引き去り, 第 1 列の倍数を残りの列から引き去ることによって, 第 1 行と第 1 列の第 $(1,1)$ 成分以外をすべて 0 にした結果を A_2 とする:

$$A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -6\,x-13 & 12 & -23 & x-16 \\ 0 & -x+3 & x-1 & 2 & 2 \\ 0 & 5\,x+10 & -9 & x+17 & 12 \\ 0 & x^2-7\,x-12 & -x+13 & 2\,x-24 & 2\,x-16 \end{bmatrix}.$$

第 5 列に $1/2$ をかけて, 第 5 列と第 2 列を交換し, 第 3 行と第 2 列を交換した結果を A_3 とする:

$$A_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & x-1 & 2 & -x+3 \\ 0 & \frac{1}{2}\,x-8 & 12 & -23 & -6\,x-13 \\ 0 & 6 & -9 & x+17 & 5\,x+10 \\ 0 & x-8 & -x+13 & 2\,x-24 & x^2-7\,x-12 \end{bmatrix}.$$

第 2 行の倍数を第 3 行以降から引き去り, 第 2 列の倍数を第 3 列以降から引き去ること

によって, 第 2 行と第 2 列の第 $(2,2)$ 成分以外をすべて 0 にした結果を A_4 とする:

$$A_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{2}x^2+\frac{17}{2}x+4 & -x-7 & \frac{1}{2}x^2-\frac{31}{2}x+11 \\ 0 & 0 & -6x-3 & x+5 & 11x-8 \\ 0 & 0 & -x^2+8x+5 & -8 & 2x^2-18x+12 \end{bmatrix}.$$

第 5 行に $-1/8$ をかけて第 5 行と第 3 行を交換し, 第 4 列と第 3 行を交換した結果を A_5 とする:

$$A_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & \frac{1}{8}x^2-x-\frac{5}{8} & -\frac{1}{4}x^2+\frac{9}{4}x-\frac{3}{2} \\ 0 & 0 & x+5 & -6x-3 & 11x-8 \\ 0 & 0 & -x-7 & -\frac{1}{2}x^2+\frac{17}{2}x+4 & \frac{1}{2}x^2-\frac{31}{2}x+11 \end{bmatrix}.$$

第 3 行の倍数を第 4 行以降から引き去り, 第 3 列の倍数を第 4 列以降から引き去ることによって, 第 3 行と第 3 列の第 $(3,3)$ 成分以外をすべて 0 にした結果を A_6 とする:

$$A_6 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{8}x^3+\frac{3}{8}x^2-\frac{3}{8}x+\frac{1}{8} & \frac{1}{4}x^3-x^2+\frac{5}{4}x-\frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{8}x^3-\frac{5}{8}x^2+\frac{7}{8}x-\frac{3}{8} & -\frac{1}{4}x^3+x^2-\frac{5}{4}x+\frac{1}{2} \end{bmatrix}.$$

第 4 行を第 5 行に加えて, 第 5 行と第 4 行を交換した結果を A_7 とする:

$$A_7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{4}x^2+\frac{1}{2}x-\frac{1}{4} & -\frac{1}{2}x^2+x-\frac{1}{2} \\ 0 & 0 & 0 & -\frac{1}{8}x^3+\frac{3}{8}x^2-\frac{3}{8}x+\frac{1}{8} & -\frac{1}{4}x^2+\frac{1}{2}x-\frac{1}{4} \end{bmatrix}.$$

第 4 列の 2 倍を第 5 列から引き去り, 第 4 行の $x/2-1/2$ 倍を第 5 行から引き去り, 第 4 行を -4 倍し, 第 5 行を 4 倍した結果を A_8 とする:

$$A_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & x^2-2x+1 & 0 \\ 0 & 0 & 0 & 0 & x^3-4x^2+5x-2 \end{bmatrix}.$$

成分を因数分解すると第 $(4,4)$ 成分が第 $(5,5)$ 成分を割り切ることがわかる:

$$A_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & 0 & 0 & (x-2)(x-1)^2 \end{bmatrix}.$$

よって特性行列 $xE-A$ の単因子は次に等しい:

$$(1,1,1,x^2-2x+1,x^3-4x^2+5x-2)=(1,1,1,(x-1)^2,(x-2)(x-1)^2).$$

これより, A の Jordan 細胞は $J_1(2)$, $J_2(1)$, $J_s(1)$ の 3 つになり, A の有理標準形 (Frobenius 標準形) F と Jordan 標準形 J がそれぞれ次の形になることがわかった:

$$F=\left[\begin{array}{ccc|cc} 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & \\ 2 & -5 & 4 & & \\ \hline & & & 0 & 1 \\ 0 & & & -1 & 2 \end{array}\right],\quad J=\left[\begin{array}{c|cc|cc} 2 & & & & 0 \\ \hline & 1 & 1 & & \\ & 0 & 1 & & \\ \hline & & & 1 & 1 \\ 0 & & & 0 & 1 \end{array}\right]. \quad \square$$

[410] $\mathbb{C}$ 上の次の行列の特性行列の単因子と Jordan 標準形を求めよ:

$$A_1=\begin{bmatrix} -4 & -6 & 3 & 6 \\ -4 & -3 & 2 & 4 \\ 10 & 4 & -7 & -10 \\ -12 & -10 & 8 & 14 \end{bmatrix},\quad A_2=\begin{bmatrix} 11 & 4 & -8 & -8 \\ 10 & 5 & -8 & -8 \\ 6 & 2 & -5 & -4 \\ 14 & 6 & -10 & -11 \end{bmatrix}$$

計算の過程の概略も説明せよ. $\square$

略解: $xE-A_1$ の単因子は $(1,1,1,(x+2)(x+1)(x-1)(x-2))$ であるから, A_1 の Jordan 細胞は $(J_1(-2),J_1(-1),J_1(1),J_1(2))=(-2,-1,1,2)$ である. $xE-A_2$ の単因子は $(1,1,(x-1)(x+1),(x-1)(x+1))$ であるから, A_2 の Jordan 細胞は $(-1,-1,1,1)$ である. $\square$

[411] $\mathbb{C}$ 上の次の行列の特性行列の単因子と Jordan 標準形を求めよ:

$$A_3=\begin{bmatrix} -10 & 13 & -3 & -4 \\ -9 & 9 & -3 & -1 \\ 9 & -19 & 2 & 10 \\ -9 & 7 & -3 & 1 \end{bmatrix},\quad A_4=\begin{bmatrix} 6 & 7 & 14 & 7 \\ 8 & 7 & 16 & 8 \\ -6 & -6 & -13 & -6 \\ -3 & -3 & -6 & -4 \end{bmatrix}.$$

計算の過程の概略も説明せよ. $\square$

略解: $xE-A_3$ の単因子は $(1,1,x+1,(x+1)(x-2)^2)$ であるから, A_3 の Jordan 細胞は $(-1,-1,J_2(2))$ である. $xE-A_4$ の単因子は $(1,x+1,x+1,(x+1)^2)$ であるから, A_4 の Jordan 細胞は $(-1,-1,J_2(-1))$ である. $\square$

[412] $\mathbb{C}$ 上の次の行列の特性行列の単因子と Jordan 標準形を求めよ:

$$A_5=\begin{bmatrix} 5 & -2 & -3 & 0 \\ -4 & -2 & 2 & -3 \\ 12 & -3 & -7 & 1 \\ 4 & 1 & -2 & 2 \end{bmatrix},\quad A_6=\begin{bmatrix} 4 & -10 & -4 & -5 \\ 3 & -8 & -6 & -5 \\ 1 & -6 & 0 & -3 \\ -6 & 20 & 12 & 12 \end{bmatrix}.$$

計算の過程の概略も説明せよ. $\square$

略解: $xE-A_5$ の単因子は $(1,1,1,(x-1)(x+1)^3)$ であるから, A_5 の Jordan 細胞は $(1,J_3(-1))$ である. $xE-A_6$ の単因子は $(1,1,x-2,(x-2)^3)$ であるから, A_6 の Jordan 細胞は $(2,J_3(2))$ である. □

[**413**] $\mathbb{C}$ 上の次の行列の特性行列の単因子と Jordan 標準形を求めよ:

$$A_7=\begin{bmatrix} 1 & 5 & 1 & 2\\ 0 & 5 & 1 & 1\\ -2 & -8 & -2 & -1\\ -1 & -1 & -1 & 2 \end{bmatrix},\quad A_8=\begin{bmatrix} 9 & -12 & 6 & 10\\ 15 & -19 & 5 & 19\\ 5 & -6 & -1 & 8\\ 5 & -6 & 0 & 7 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $xE-A_7$ の単因子は $(1,1,1,(x-1)^2(x-2)^2)$ であるから, A_7 の Jordan 細胞は $(J_2(1),J_2(2))$ である. $xE-A_8$ の単因子は $(1,1,(x+1)^2,(x+1)^2)$ であるから, A_8 の Jordan 細胞は $(J_2(-1),J_2(-1))$ である. □

[**414**] $\mathbb{C}$ 上の次の行列の特性行列の単因子と Jordan 標準形を求めよ:

$$A_9=\begin{bmatrix} -5 & -1 & 2 & 1\\ 17 & 3 & -12 & -2\\ 1 & 0 & -3 & 1\\ 10 & 3 & -7 & -3 \end{bmatrix},\quad A_{10}=\begin{bmatrix} 6 & 6 & -11 & -9\\ -2 & -1 & 5 & 4\\ 2 & 3 & -5 & -6\\ -2 & -3 & 7 & 8 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $xE-A_9$ の単因子は $(1,1,1,(x+2)^4)$ であるから, A_9 の Jordan 細胞は $J_4(-2)$ だけである. $xE-A_{10}$ の単因子は $(1,1,(x-2)^2,(x-2)^2)$ であるから, A_{10} の Jordan 細胞は $(J_2(2),J_2(2))$ である. □

[**415**] $\mathbb{C}$ 上の次の行列の特性行列の単因子と Jordan 標準形を求めよ:

$$B_1=\begin{bmatrix} -2 & 6 & -1 & 1 & 8\\ 2 & 2 & -1 & 1 & -1\\ -4 & 6 & 1 & 1 & 8\\ 0 & -2 & 1 & 1 & -2\\ -4 & 4 & 0 & 0 & 8 \end{bmatrix},\quad B_2=\begin{bmatrix} -14 & 0 & -4 & 5 & -7\\ 1 & 1 & -1 & 0 & 1\\ 8 & 0 & 2 & -3 & 4\\ -4 & -4 & 3 & 0 & -4\\ 19 & -4 & 9 & -8 & 8 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $xE-B_1$ の単因子は $(1,1,x-2,(x-2)^2,(x-2)^2)$ であるから, B_1 の Jordan 細胞は $(2,J_2(2),J_2(2))$ である. $xE-B_2$ の単因子は $(1,1,1,(x+1)^2,(x-1)(x+1)^2)$ であるから, B_2 の Jordan 細胞は $(1,J_2(-1),J_2(-1))$ である. □

[**416**] $\mathbb{C}$ 上の次の行列の特性行列の単因子と Jordan 標準形を求めよ:

$$B_3=\begin{bmatrix} -6 & 6 & -3 & -8 & 0\\ 0 & 2 & 7 & -1 & -4\\ 0 & -1 & -2 & 1 & 1\\ 2 & 0 & 6 & 1 & -3\\ -5 & 5 & -4 & -7 & 0 \end{bmatrix},\quad B_4=\begin{bmatrix} 5 & 3 & 0 & 3 & -5\\ -6 & -3 & 3 & -2 & 5\\ 4 & 3 & 1 & 3 & -5\\ -10 & -7 & 3 & -4 & 10\\ -6 & -4 & 3 & -2 & 6 \end{bmatrix}.$$

計算の過程の概略も説明せよ. □

略解: $xE-B_3$ の単因子は $(1,1,1,(x+1)^2,(x+1)^3)$ であるから, B_3 の Jordan 細胞は $(J_2(-1),J_3(-1))$ である. $xE-B_4$ の単因子は $(1,1,x-1,x-1,(x-1)^3)$ であるから, B_4 の Jordan 細胞は $(1,1,J_3(1))$ である. □

26 コンパニオン行列の Jordan 標準形

この節では第 27 節で体 K 上のベクトル空間の理論から一変数多項式環 $K[\lambda]$ 上の加群の理論に進む前に後者がどのように役に立つかに関して感じをつかむためにコンパニオン行列の Jordan 標準形について解説する.

K は任意の代数閉体であると仮定し, K の元を成分に持つ行列について考える. K の元を数と呼ぶことがある. 「任意の代数閉体」という言葉を使うのが怖い人は $K=\mathbb{C}$ であると考えてよい.

26.1 $(\lambda-\alpha)^n$ に対応するコンパニオン行列の Jordan 標準形

[417] $\mathbb{Z}$ 係数の s 変数多項式環 $R=\mathbb{Z}[x_1,\ldots,x_s]$ を考え, $n_i\in\mathbb{Z}_{>0}$, $n_1+\cdots+n_s=n$ とし, R 係数の多項式 $p(\lambda)\in R[\lambda]$ を次のように定める:

$$p(\lambda)=(\lambda-x_1)^{n_1}\cdots(\lambda-x_s)^{n_s}.$$

これを λ について展開して $a_i\in R$ を次のように定める:

$$p(\lambda)=\lambda^n+a_0\lambda^{n-1}+a_1\lambda^{n-1}+\cdots+a_{n-2}\lambda+a_{n-1}.$$

このとき $\frac{1}{k!}p^{(k)}(\lambda)\in R[\lambda]$ $(k\in\mathbb{Z}_{\geq 0})$ であり, $\frac{1}{k!}p^{(k)}(x_i)=0$ $(k=0,1,\ldots,n_i-1)$ が成立している. すなわち

$$\binom{n}{k}x_i^{n-k}+\binom{n-1}{k}a_0x_i^{n-k-1}+\cdots+\binom{k+1}{k}a_{n-k-2}x_i+\binom{k}{k}a_{n-k-1}=0$$
$$(k=0,1,\ldots,n_i-1).$$

さらに, この公式中の $x_1,\ldots,x_s$ のそれぞれに任意の体 K の任意の元 $\alpha_1,\ldots,\alpha_s$ を代入することができ[124], 代入後の公式も成立している. □

ヒント: $\frac{1}{k!}\left(\frac{\partial}{\partial\lambda}\right)^k\lambda^l=\binom{l}{k}\lambda^{l-k}$ より $\frac{1}{k!}\left(\frac{\partial}{\partial\lambda}\right)^k$ の作用は $R[\lambda]$ の元を $R[\lambda]$ の元に移す. $\frac{1}{k!}p^{(k)}(x_i)=0$ $(k=0,1,\ldots,n_i-1)$ を書き直せば問題の結論が得られる. 整数係数の多項式の中の変数には任意の体の元を代入できるので最後の結論も得られる. □

注意: $K=\mathbb{C}$ (もしくは K の標数は 0) とみなしている人にとって上の問題は重要ではない. もしも K の標数が正で $k!$ が標数で割り切れるならば K の中で $k!=0$ になる. 正標数の世界では任意の $k!$ で割る操作を考えることができない. しかし, 上の問題のように整数係数の多項式の世界を経由すれば $k!$ で割った後の公式が正当化される場合がある. 整数係数多項式の世界で成立している公式は変数に任意の体の元[125]を代入した結果も成立している. □

[124] $a_0,a_1,\ldots,a_{n-1}$ たちの中にも $x_1,\ldots,x_s$ が含まれていることに注意せよ
[125] 任意の可換環の元でもよい.

[418] 任意に $\alpha \in K$ を取り, $a_0, \dots, a_{n-1} \in K$ を次のように定める:

$$(\lambda - \alpha)^n = \lambda^n + a_0\lambda^{n-1} + \cdots + a_{n-2}\lambda + a_{n-1}.$$

行列 $C, P \in M_n(K)$ を次のように定める[126]:

$$C = C(a_0, \dots, a_{n-1}) = \begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & \ddots & & \\ & & \ddots & 1 & \\ 0 & & & 0 & 1 \\ -a_{n-1} & -a_{n-2} & \cdots & -a_1 & -a_0 \end{bmatrix},$$

$$P = \left[\binom{i-1}{j-1}\alpha^{i-j}\right]_{i,j=1}^{n} = \begin{bmatrix} 1 & & & & & 0 \\ \alpha & 1 & & & & \\ \alpha^2 & 2\alpha & 1 & & & \\ \alpha^3 & 3\alpha^2 & 3\alpha & 1 & & \\ \vdots & \vdots & \vdots & & \ddots & \\ \alpha^{n-1} & (n-1)\alpha^{n-2} & \binom{n-1}{2}\alpha^{n-3} & \binom{n-1}{3}\alpha^{n-4} & \cdots & 1 \end{bmatrix}.$$

このとき P による相似変換は C を Jordan 標準形に変換する:

$$P^{-1}CP = J_n(\alpha). \quad \square$$

ヒント 1: $p(\lambda) = (\lambda - \alpha)^n = \lambda^n + a_0\lambda^{n-1} + \cdots + a_{n-1}$ と置くと, 問題 **[417]** の結果より,

$$\binom{n}{k}\alpha^{n-k} = -\binom{k}{k}a_{n-k-1} - \binom{k+1}{k}a_{n-k-2}\alpha - \cdots - \binom{n-1}{k}a_0\alpha^{n-k-1}$$
$$(k = 0, 1, \dots, n-1).$$

この公式と二項係数の漸化式 (Pascal の三角形) を用いて $CP = PJ_n(\alpha)$ の両辺が一致することを直接確かめることができる.

たとえば $n = 4$ のとき

$$CP = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -a_3 & -a_2 & -a_1 & -a_0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \alpha^2 & 2\alpha & 1 & 0 \\ \alpha^3 & 3\alpha^2 & 3\alpha & 1 \end{bmatrix}$$
$$= \begin{bmatrix} \alpha & 1 & 0 & 0 \\ \alpha^2 & 2\alpha & 1 & 0 \\ \alpha^3 & 3\alpha^2 & 3\alpha & 1 \\ -a_3 - a_2\alpha - a_1\alpha^2 - a_0\alpha^3 & -a_2 - 2a_1\alpha - 3a_0\alpha^2 & -a_1 - 3a_0\alpha & -a_0 \end{bmatrix},$$

$$PJ_n(\alpha) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \alpha^2 & 2\alpha & 1 & 0 \\ \alpha^3 & 3\alpha^2 & 3\alpha & 1 \end{bmatrix}\begin{bmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{bmatrix} = \begin{bmatrix} \alpha & 1 & 0 & 0 \\ \alpha^2 & 2\alpha & 1 & 0 \\ \alpha^3 & 3\alpha^2 & 3\alpha & 1 \\ \alpha^4 & 4\alpha^3 & 6\alpha^2 & 4\alpha \end{bmatrix}.$$

[126] P の定義において二項係数の定義は $\binom{n}{k} = n(n-1)(n-2)\cdots(n-k+1)/k!$ なので $k = n+1, n+2, \dots$ のとき $\binom{n}{k} = n(n-1)\cdots(n-n)\cdots(n-k+1)/k! = 0$ となることに注意せよ.

これに以下を適用すれば $CP = PJ_n(\alpha)$ であることがわかる:

$$\begin{aligned}
0 &= p(\alpha) = \alpha^4 + a_0\alpha^3 + a_1\alpha^2 + a_2\alpha + a_3,\\
0 &= p'(\alpha) = 4\alpha^3 + 3a_0\alpha^2 + 2a_1\alpha + a_2,\\
0 &= \frac{1}{2}p''(\alpha) = 6\alpha^2 + 3a_0\alpha + a_1,\\
0 &= \frac{1}{3!}p^{(3)}(\alpha) = 4\alpha + a_0. \quad \square
\end{aligned}$$

ヒント 2: 文字 t が $(t-\alpha)^n = 0$ を満たしていると仮定すると[127]

$$t^n = -a_0t^{n-1} - a_1t^{n-2} - \cdots - a_{n-1}$$

なので以下が成立する:

$$\begin{aligned}
&t[1, t, \ldots, t^{n-2}, t^{n-1}]\\
&= [t, t^2, \ldots, t^{n-1}, -a_0t^{n-1} - a_1t^{n-2} - \cdots - a_{n-1}]\\
&= [1, t, \ldots, t^{n-2}, t^{n-1}]\,{}^tC,
\end{aligned}$$

$$\begin{aligned}
&t[1, t-\alpha, \ldots, (t-\alpha)^{n-2}, (t-\alpha)^{n-1}]\\
&= [t, t(t-\alpha), \ldots, t(t-\alpha)^{n-2}, t(t-\alpha)^{n-1}]\\
&= [\alpha + (t-\alpha), \alpha(t-\alpha) + (t-\alpha)^2, \ldots, \alpha(t-\alpha)^{n-2} + (t-\alpha)^{n-1}, \alpha(t-\alpha)^{n-1}]\\
&= [1, t-\alpha, \ldots, (t-\alpha)^{n-2}, (t-\alpha)^{n-1}]\,{}^tJ_n(\alpha).
\end{aligned}$$

そして, 二項定理より,

$$\begin{aligned}
[1, t, \ldots, t^{n-2}, t^{n-1}] &= [1, \alpha + (t-\alpha), \ldots, (\alpha + (t-\alpha))^{n-2}, (\alpha + (t-\alpha))^{n-1}]\\
&= [1, t-\alpha, \ldots, (t-\alpha)^{n-2}, (t-\alpha)^{n-1}]\,{}^tP.
\end{aligned}$$

以上を用いて $t[1, t, \ldots, t^{n-2}, t^{n-1}]$ を二通りに計算すると,

$$\begin{aligned}
t[1, t, \ldots, t^{n-2}, t^{n-1}] &= [1, t, \ldots, t^{n-2}, t^{n-1}]\,{}^tC\\
&= [1, t-\alpha, \ldots, (t-\alpha)^{n-2}, (t-\alpha)^{n-1}]\,{}^tP\,{}^tC,\\
t[1, t, \ldots, t^{n-2}, t^{n-1}] &= t[1, t-\alpha, \ldots, (t-\alpha)^{n-2}, (t-\alpha)^{n-1}]\,{}^tP\\
&= [1, t-\alpha, \ldots, (t-\alpha)^{n-2}, (t-\alpha)^{n-1}]\,{}^tJ_n(\alpha)\,{}^tP.
\end{aligned}$$

よって ${}^tP\,{}^tC = {}^tJ_n(\alpha)\,{}^tP$ すなわち $CP = PJ_n(\alpha)$ である. $\square$

[127] このように仮定して良いかどうかに疑問を持った人は多項式環 $K[\lambda]$ のイデアル

$$\big((\lambda-\alpha)^n\big) = K[\lambda](\lambda-\alpha)^n = \{\, g(\lambda)(\lambda-\alpha)^n \mid g \in K[\lambda] \,\}$$

で割ってできる剰余環 (residue ring, 商環, quotient ring) $R = K[\lambda]/\big((\lambda-\alpha)^n\big)$ について学ばなければいけない.

代数学において M/N は「M の中の N の元をすべて 0 とみなしてできる空間」を意味している. したがって R は多項式環 $K[\lambda]$ の中で $\big((\lambda-\alpha)^n\big)$ の元をすべて 0 とみなしてできる空間である. よって λ に対応する R の元を t と書けば $(t-\alpha)^n = 0$ が成立している.

R は K 上の n 次元ベクトル空間をなし, その基底として $1, t, \ldots, t^{n-1}$ と $1, t-\alpha, \ldots, (t-\alpha)^{n-1}$ が取れる. この基底に関して t の積が定める一次変換を行列表示するとそれぞれ ${}^tC$, ${}^tJ_n(\alpha)$ になり, それら二つの基底のあいだの変換行列は ${}^tP$ になっている. これが以下の計算の数学的意味である.

26.2 一般のコンパニオン行列の Jordan 標準形

[419] (コンパニオン行列の Jordan 標準形 1) 問題 **[375]** で定義されたコンパニオン行列 $C = C(a_0, \ldots, a_{n-1})$ $(a_i \in K)$ について考える:

$$C = C(a_0, \ldots, a_{n-1}) = \begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & \ddots & & \\ & & \ddots & 1 & \\ 0 & & & 0 & 1 \\ -a_{n-1} & -a_{n-2} & \cdots & -a_1 & -a_0 \end{bmatrix}.$$

K は代数閉体だと仮定したので[128], C の特性多項式

$$p_C(\lambda) = \lambda^n + a_0\lambda^{n-1} + a_1\lambda^{n-2} + \cdots + a_{n-2}\lambda + a_{n-1} \qquad (*)$$

は次のように一次式の積に分解される:

$$p_C(\lambda) = (\lambda - \alpha_1)^{n_1} \cdots (\lambda - \alpha_s)^{n_s}.$$

ここで $\alpha_1, \ldots, \alpha_s$ たちは $p_C(\lambda)$ の相異なる根の全体であり, $n_1 + \cdots + n_s = n$ である. このとき C の Jordan 標準形 J は次の形になる:

$$J = \begin{bmatrix} J_{n_1}(\alpha_1) & & 0 \\ & \ddots & \\ 0 & & J_{n_s}(\alpha_s) \end{bmatrix}.$$

すなわち C の各固有値 α_i に属する Jordan 細胞は唯一つになる. □

ヒント: 問題 **[375]** の結論は, コンパニオン行列 $C = C(a_0, \ldots, a_{n-1})$ の特性多項式が $(*)$ の形になることと最小多項式が特性多項式に等しくなることであった. 後者の結論と問題 **[397]** の結果を合わせればこの問題の結論がただちに得られる. □

上のヒントの方法では問題 **[418]** の場合と違って $P^{-1}CP = J$ となる正則行列 P の具体形がわからない. しかも, そこで使用されている問題 **[397]** のヒントでは Jordan 標準形の存在を仮定してしまっていたので, Jordan 標準形の存在の別証明にも使えない.

しかし, 問題 **[418]** の結果を一般化することによって $p_C(\lambda)$ の根の情報から P を直接的にかつ具体的に構成することができる. 問題 **[421]** を見よ.

[420] (Vandermonde の公式の一般化) $\mathbb{Z}$ 係数の s 変数多項式環 $R = \mathbb{Z}[x_1, \ldots, x_s]$ を考え, $n_i \in \mathbb{Z}_{>0}$, $n_1 + \cdots + n_s = n$ とする. R の元を成分に持つ (n, n_i) 型行列 $P_i \in M_{n,n_i}(K)$ を次のように定義する:

$$P_i = \left[\binom{\mu - 1}{\nu - 1} x_i^{\mu-\nu} \right]_{1 \le \mu \le n,\ 1 \le \nu \le n_i}.$$

[128] 代数閉体という言葉が怖ければ $K = \mathbb{C}$ だと考えて良い.

具体的に書き下すと[129],

$$P_i = \begin{bmatrix} \binom{0}{0} & & & & & 0 \\ \binom{1}{0}x_i & \binom{1}{1} & & & & \\ \binom{2}{0}x_i^2 & \binom{2}{1}x_i & \binom{2}{2} & & & \\ \binom{3}{0}x_i^3 & \binom{3}{1}x_i^2 & \binom{3}{2}x_i & \binom{3}{3} & & \\ \vdots & \vdots & \vdots & & \ddots & \\ \binom{n_i-1}{0}x_i^{n_i-1} & \binom{n_i-1}{1}x_i^{n_i-2} & \binom{n_i-1}{2}x_i^{n_i-3} & \binom{n_i-1}{3}x_i^{n_i-4} & \cdots & \binom{n_i-1}{n_i-1} \\ \binom{n_i}{0}x_i^{n_i} & \binom{n_i}{1}x_i^{n_i-1} & \binom{n_i}{2}x_i^{n_i-2} & \binom{n_i}{3}x_i^{n_i-3} & \cdots & \binom{n_i}{n_i-1}x_i \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \binom{n-1}{0}x_i^{n-1} & \binom{n-1}{1}x_i^{n-2} & \binom{n-1}{2}x_i^{n-3} & \binom{n-1}{3}x_i^{n-4} & \cdots & \binom{n-1}{n_i-1}x_i^{n-n_i} \end{bmatrix}.$$

P は $P_1, \ldots, P_s$ を横に並べてできる n 次正方行列であるとする:

$$P = [P_1 \ \cdots \ P_s].$$

このとき次が成立している:

$$\det P = \prod_{1 \le i < j \le s} (x_j - x_i)^{n_i n_j}.$$

この公式の $n = s$, $n_1 = \cdots = n_s = 1$ の場合は Vandermonde の公式なので, この結果は Vandermonde の公式の一般化になっている.

この公式より, 任意の体 K とその相異なる元 $\alpha_1, \ldots, \alpha_s$ に対して, P の中の $x_1, \ldots, x_s$ のそれぞれに $\alpha_1, \ldots, \alpha_s$ を代入してできる K の元を成分に持つ正方行列は可逆であることがわかる. □

ヒント: $n_1 \ge \cdots \ge n_s$ であると仮定して良い. さらに $n_{t-1} > n_t \ge 1 = n_{t+1} = \cdots = n_s$ と仮定する. $m = n_1 + \cdots + n_t$ に関する帰納法で公式を証明する. $m = 0$ すなわち $n = s$, $n_1 = \cdots = n_s = 1$ のとき, 示すべき公式は Vandermonde の公式に一致するので成立している. m まで公式が成立していると仮定する.

$\det P$ の中の第 $m - n_t + 1$ 列から第 $m + 1$ 列は次のような様子をしている:

$$\det P = \begin{vmatrix} * & \binom{0}{0} & & & 0 & 1 & * \\ * & \binom{1}{0}x_t & \binom{1}{1} & & & x_{t+1} & * \\ \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots \\ * & \binom{n_t-1}{0}x_t^{n_t-1} & \binom{n_t-1}{1}x_t^{n_t-2} & \cdots & \binom{n_t-1}{n_t-1} & x_{t+1}^{n_t-1} & * \\ * & \binom{n_t}{0}x_t^{n_t} & \binom{n_t}{1}x_t^{n_t-1} & \cdots & \binom{n_t}{n_t-1}x_t & x_{t+1}^{n_t} & * \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ * & \binom{n-1}{0}x_t^{n-1} & \binom{n-1}{1}x_t^{n-2} & \cdots & \binom{n-1}{n_t-1}x_t^{n-n_t} & x_{t+1}^{n-1} & * \end{vmatrix}.$$

よって, $\det P$ に $\frac{1}{n_t!}\left(\frac{\partial}{\partial x_{t+1}}\right)^{n_t}$ を作用させて, $(x_{t+1}, x_{t+2}, \ldots, x_s)$ に $(x_t, x_{t+1}, \ldots, x_{s-1})$ を代入した結果は n_t を 1 つ増やした場合の公式の左辺に一致する. したがって, 公式の右辺に $\frac{1}{n_t!}\left(\frac{\partial}{\partial x_{t+1}}\right)^{n_t}$ を作用させて $(x_{t+1}, x_{t+2}, \ldots, x_s)$ に $(x_t, x_{t+1}, \ldots, x_{s-1})$ を代入した結果が公式の右辺で n_t を 1 つ増やして s を 1 つ減らした結果に一致することを示せば良い.

[129]印刷上では P_i が横長に見えてしまうかもしれないが, 実際には P_i は縦長の (n, n_i) 型の行列である.

公式の右辺に含まれる x_{t+1} を含む因子は $n_{t+1} = \cdots = n_s = 1$ であるから

$$(x_{t+1} - x_1)^{n_1} \dots (x_{t+1} - x_{t-1})^{n_{t-1}} (x_{t+1} - x_t)^{n_t} (x_{t+2} - x_{t+1}) \cdots (x_s - x_{t+1}).$$

公式の右辺に $\frac{1}{n_t!} \left(\frac{\partial}{\partial x_{t+1}} \right)^{n_t}$ を作用させて x_{t+1} に x_t を代入した結果は公式の右辺の x_{t+1} を含む因子を次に置き換えた結果に等しい:

$$(x_t - x_1)^{n_1} \dots (x_t - x_{t-1})^{n_{t-1}} (x_{t+2} - x_t) \cdots (x_s - x_t).$$

よって, その結果は公式の右辺の x_{t+1} を含む因子を消去し, 右辺の x_t を含み x_{t-1} を含まない因子

$$(x_t - x_1)^{n_1 n_t} \dots (x_t - x_{t-1})^{n_{t-1} n_t} (x_{t+2} - x_t)^{n_t} \cdots (x_s - x_t)^{n_t}$$

を次で置換した結果に一致する:

$$(x_t - x_1)^{n_1 (n_t+1)} \dots (x_t - x_{t-1})^{n_{t-1} (n_t+1)} (x_{t+2} - x_t)^{n_t+1} \cdots (x_s - x_t)^{n_t+1}.$$

よって, さらに $(x_{t+2}, \dots, x_s)$ に $(x_{t+1}, \dots, x_{s-1})$ を代入した結果は次に等しい:

$$\prod_{1 \le i < j \le s-1} (x_j - x_i)^{m_i m_j}.$$

ここで

$$m_i = \begin{cases} n_i & (i = 1, \dots, t-1), \\ n_t + 1 & (i = t), \\ n_{i+1} & (i = t+1, \dots, s-1). \end{cases}$$

この結果は公式の右辺で n_t を 1 つ増やして s を 1 つ減らした結果に一致している. □

解説: $y_1, \dots, y_n$ に関する Vandermonde の行列式を考える:

$$\Delta = \prod_{1 \le i < j \le n} (y_j - y_i) = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ y_1 & y_2 & y_3 & \cdots & y_n \\ y_1^2 & y_2^2 & y_3^2 & \cdots & y_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ y_1^{n-1} & y_2^{n-1} & y_3^{n-1} & \cdots & y_n^{n-1} \end{vmatrix}.$$

変数 $y_{n_1 + \cdots + n_{i-1} + \nu + 1}$ $(\nu = 0, \dots, n_i - 1)$ を $x_{i,\nu}$ と表わし, y_i たちに関する偏微分作用素 L を次のように定める:

$$L = \prod_{i=1}^{s} \prod_{\nu=0}^{n_i - 1} \frac{1}{\nu!} \left(\frac{\partial}{\partial x_{i,\nu}} \right)^{\nu}.$$

このとき, $\det P$ は $L\Delta$ の中の $x_{i,\nu}$ $(\nu = 0, \dots, n_i - 1)$ に x_i を代入したものに等しい. 上のヒントは実質的にこの事実を用いている.

例として $n = 5$, $s = 2$, $n_1 = 3$, $n_2 = 2$ の場合を考えよう. このとき

$$L\Delta = \frac{\partial}{\partial y_2} \frac{1}{2!} \frac{\partial^2}{\partial y_3^2} \frac{\partial}{\partial y_5} \Delta = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ y_1 & 1 & 0 & y_4 & 1 \\ y_1^2 & 2y_2 & 1 & y_4^2 & 2y_5 \\ y_1^3 & 3y_2^2 & 2y_3 & y_4^3 & 3y_5^2 \\ y_1^4 & 4y_2^3 & 4y_3^2 & y_4^4 & 4y_5^3 \end{vmatrix}.$$

よって $L\Delta$ の中の y_1, y_2, y_3 に x_1 を代入し y_4, y_5 に x_2 を代入したものは $\det P$ に等しい. 一方,

$$\Delta = \prod_{1\le i<j\le 5}(y_j - y_i) = (y_2 - y_1)\prod_{3\le j\le 5}[(y_j - y_1)(y_j - y_2)]\prod_{3\le i<j\le 5}(y_j - y_i),$$

$$\begin{aligned}\Gamma_1 &:= \frac{\partial}{\partial y_2}\Delta\bigg|_{y_2=y_1} = \prod_{3\le j\le 5}(y_j - y_1)^2\prod_{3\le i<j\le 5}(y_j - y_i)\\ &= (y_3 - y_1)^2\prod_{4\le j\le 5}(y_j - y_1)^2\prod_{4\le j\le 5}(y_j - y_3)\cdot(y_5 - y_4),\end{aligned}$$

$$\Gamma_2 := \frac{1}{2!}\frac{\partial^2}{\partial y_3^2}\bigg|_{y_3=y_1} = (y_5 - y_4)\prod_{4\le j\le 5}(y_j - y_1)^3,$$

$$\Gamma_3 := \frac{\partial}{\partial y_5}\Gamma_2\bigg|_{y_5=y_4} = (y_4 - y_1)^6.$$

Γ_3 は $L\Delta$ で $y_1 = y_2 = y_3$, $y_4 = y_5$ と置いた結果に等しい. よって $\det P = (x_2 - x_1)^6 = (x_2 - x_1)^{n_1 n_2}$ である. □

[421] (コンパニオン行列の Jordan 標準形 2) 問題 **[419]** の状況を仮定する. (n, n_i) 型行列 $P_i \in M_{n,n_i}(K)$ を次のように定義する:

$$P_i = \left[\binom{\mu-1}{\nu-1}\alpha_i^{\mu-\nu}\right]_{1\le\mu\le n,\ 1\le\nu\le n_i}.$$

具体的に書き下すと[130],

$$P_i = \begin{bmatrix}
\binom{0}{0} & & & & & 0\\
\binom{1}{0}\alpha_i & \binom{1}{1} & & & & \\
\binom{2}{0}\alpha_i^2 & \binom{2}{1}\alpha_i & \binom{2}{2} & & & \\
\binom{3}{0}\alpha_i^3 & \binom{3}{1}\alpha_i^2 & \binom{3}{2}\alpha_i & \binom{3}{3} & & \\
\vdots & \vdots & \vdots & & \ddots & \\
\binom{n_i-1}{0}\alpha_i^{n_i-1} & \binom{n_i-1}{1}\alpha_i^{n_i-2} & \binom{n_i-1}{2}\alpha_i^{n_i-3} & \binom{n_i-1}{3}\alpha_i^{n_i-4} & \cdots & \binom{n_i-1}{n_i-1}\\
\binom{n_i}{0}\alpha_i^{n_i} & \binom{n_i}{1}\alpha_i^{n_i-1} & \binom{n_i}{2}\alpha_i^{n_i-2} & \binom{n_i}{3}\alpha_i^{n_i-3} & \cdots & \binom{n_i}{n_i-1}\alpha_i\\
\vdots & \vdots & \vdots & \vdots & & \vdots\\
\binom{n-1}{0}\alpha_i^{n-1} & \binom{n-1}{1}\alpha_i^{n-2} & \binom{n-1}{2}\alpha_i^{n-3} & \binom{n-1}{3}\alpha_i^{n-4} & \cdots & \binom{n-1}{n_i-1}\alpha_i^{n-n_i}
\end{bmatrix}.$$

このとき $P_1, \ldots, P_s$ を横に並べてできる n 次正方行列を P とすると, P は逆行列を持ち $P^{-1}CP$ は Jordan 標準形になる. すなわち $P = [P_1\ \cdots\ P_s]$ と置くと $P \in GL_n(K)$ かつ $P^{-1}CP = J$ が成立する. □

ヒント 1: 問題 **[418]** のヒント 1 の一般化.

P が逆行列を持つことは Vandermonde の公式の一般化 **[420]** よりわかる.

$P_i J_{n_i}(\alpha_i)$ の第 ν 列は P_i の第 $\nu-1$ 列と第 ν 列の α 倍の和に等しい. よって, $P_i J_{n_i}(\alpha_i)$ の (μ, ν) 成分は $\binom{\mu-1}{\nu-2}\alpha^{\mu-\nu+1} + \binom{\mu-1}{\nu-1}\alpha^{\mu-\nu+1} = \binom{\mu}{\nu-1}\alpha^{\mu-\nu+1}$ に等しい.

[130]印刷上では P_i が横長に見えてしまうかもしれないが, 実際には P_i は縦長の (n, n_i) 型の行列である.

CP_i の第 1 行から第 $n-1$ 行はそれぞれ P_i の第 2 行から第 n 行に等しいので, $\mu = 1, \dots, n-1$ に対して CP_i の (μ, ν) 成分は $\binom{\mu}{\nu-1}\alpha^{\mu-\nu+1}$ に等しい. よって CP_i と $P_i J_{n_i}(\alpha_i)$ の第 1 行から第 $n-1$ 行は互いに等しい.

問題 [**417**] の結果で $x_i = \alpha_i$, $k = \nu - 1$ と置けば,

$$\binom{n}{\nu-1}\alpha_i^{n-\nu+1} = -a_{n-\nu}\binom{\nu-1}{\nu-1} - a_{n-\nu-1}\binom{\nu}{\nu-1}\alpha_i - \cdots - a_0\binom{n-1}{\nu-1}\alpha_i^{n-\nu} \qquad (\nu = 1, \dots, n_i).$$

CP_i の第 (n, ν) 成分はこの式の右辺に等しい. よって CP_i と $P_i J_{n_i}(\alpha_i)$ の第 n 行は互いに等しい.

これで $CP_i = P_i J_{n_i}(\alpha_i)$ が示された. よって

$$\begin{aligned} CP &= [CP_1 \ \cdots \ CP_s] = [P_1 J_{n_1}(\alpha_1) \ \cdots \ P_s J_{n_s}(\alpha_s)] \\ &= [P_1 \ \cdots \ P_s] \begin{bmatrix} J_{n_1}(\alpha_1) & & 0 \\ & \ddots & \\ 0 & & J_{n_s}(\alpha_s) \end{bmatrix} = PJ. \end{aligned}$$

これで $CP = PJ$ が証明された. □

上のヒント 1 の方法は直接的であるが, その考え方では天下り的に導入された複雑な行列 P の正体も不明なままだし, P の可逆性を証明するためには $\det P$ を計算しなければいけなかった. 次のヒント 2 の方法を用いれば行列 P の正体が明らかになり, P の可逆性も自然に証明される. 二項定理より,

$$\lambda^\mu = ((\lambda - \alpha_i) + \alpha_i)^\mu = \sum_{\nu=0}^{\mu} \binom{\mu}{\nu} \alpha_i^{\mu-\nu} (\lambda - \alpha_i)^\nu.$$

$(\lambda - \alpha_i)^\nu$ の係数は P_i の $(\mu+1, \nu+1)$ 成分に等しい. これが行列 P の正体である. より詳しい説明については以下のヒント 2 を見よ.

ただし初歩的な可換環論の知識を用いている. 複雑に見える数式の正体を明らかにするためには理論が必要になる. 初歩的な可換環論に関しては第 27 節で解説する.

我々は体の世界を離れて可換環の世界に本格的に旅立つことが必要な段階に到達した. 体 K の次に出会う可換環は体上の一変数多項式環 $K[\lambda]$ である.

ヒント 2: 問題 [**418**] のヒント 2 の一般化. 次の自然な $K[\lambda]$ 加群の同型が成立している[131]:

$$K[\lambda]/(p(\lambda)) \xrightarrow{\sim} \prod_{i=1}^{s} K[\lambda]/\big((\lambda - \alpha_i)^{n_i}\big), \quad f(\lambda) \bmod p(\lambda) \mapsto \big(f(\lambda) \bmod (\lambda - \alpha_i)^{n_i}\big)_{i=1}^{s}.$$

$t \in R$ と $t_i \in R_i$ を $t = \lambda \bmod p(\lambda)$, $t_i = \lambda \bmod (\lambda - \alpha_i)^{n_i}$ と定める. それらは $p(t) = 0$, $(t_i - \alpha_i)^{n_i} = 0$ を満たしている.

[131] 問題 [**469**] のヒントで証明の方針を示す. この同型は中国式剰余定理 (Chinese remainder theorem) の特殊な場合である.

$1, t, \ldots, t^{n-1}$ は同型の左辺の K 基底である. $1, t_i - \alpha_i, \ldots, (t_i - \alpha_i)^{n_i - 1}$ は同型の右辺における R_i の基底になっている. $(t_i - \alpha_i)^\nu \in R_i$ に対応する R の元を $e_{i,\nu}$ と書くことにする. このとき $e_{i,\nu}$ $(i = 1, \ldots, s,\ \nu = 0, 1, \ldots, n_i - 1)$ は R の別の K 基底をなす.

同型の両辺への λ 倍の作用と上の同型写像は可換である. 両辺への λ 倍の作用は両辺への K 上の一次変換を定める. λ は左辺には t 倍で作用し, 右辺の各 R_i には t_i 倍で作用する. よって以下が成立することがわかる.

$p(t) = 0$ より, λ の R への作用の基底 $1, t, \ldots, t^{n-1}$ に関する行列表示はコンパニオン行列の転置 ${}^tC$ になる:

$$\lambda[1, t, \ldots, t^{n-1}] = [1, t, \ldots, t^{n-1}]\,{}^tC.$$

$(t_i - \alpha_i)^{n_i} = 0$ より, λ の R_i への作用の基底 $1, t_i - \alpha_i, \ldots, (t_i - \alpha_i)^{n_i - 1}$ に関する行列表示はは Jordan ブロック行列の転置 ${}^tJ_{n_i}(\alpha_i)$ になる:

$$\lambda[1, t_i - \alpha_i, \ldots, (t_i - \alpha_i)^{n_i - 1}] = [1, t_i - \alpha_i, \ldots, (t_i - \alpha_i)^{n_i - 1}]\,{}^tJ_{n_i}(\alpha_i).$$

この結果を上の同型を通して R の基底 $e_{i,\nu}$ に関する結果に翻訳すると, λ の R への作用の基底 $e_{i,\nu}$ に関する行列表示が Jordan ブロック行列の転置を対角線に並べた形の行列 ${}^tJ$ になることがわかる:

$$\lambda[e_{i,\nu}] = [e_{i,\nu}]\,{}^tJ.$$

ここで $[e_{i,\nu}] = [e_{1,0}, \ldots, e_{1,n_1-1}, \ldots\ldots, e_{s,0}, \ldots, e_{s,n_s-1}]$ である.

したがって, もしも R の 2 つの基底 t^μ と $e_{i,\nu}$ のあいだの変換行列が ${}^tP$ であることがわかれば, P が可逆であることと ${}^tP\,{}^tC = {}^tJ\,{}^tP$ すなわち $CP = PJ$ が成立することがわかる.

t^μ に対応する R_i の元は t_i^μ に等しい. 二項定理より,

$$t_i^\mu = ((t_i - \alpha_i) + \alpha_i)^\mu = \sum_{\nu=0}^{n_i-1} \binom{\mu}{\nu} \alpha_i^{\mu-\nu} (t_i - \alpha_i)^\nu.$$

係数に P_i の $(\mu + 1, \nu + 1)$ 成分が現われていることに注意すれば次が成立することがわかる:

$$[1, t, \ldots, t^{n-1}] = [e_{i,\nu}]\,{}^tP.$$

${}^tP$ は 2 つの基底のあいだの変換行列なので可逆である. したがって P も可逆である.

以上の結果を使って $\lambda[1, t, \ldots, t^{n-1}]$ を 2 通りに計算すると,

$$\lambda[1, t, \ldots, t^{n-1}] = [1, t, \ldots, t^{n-1}]\,{}^tC = [e_{i,\nu}]\,{}^tP\,{}^tC,$$
$$\lambda[1, t, \ldots, t^{n-1}] = \lambda[e_{i,\nu}]\,{}^tP = [e_{i,\nu}]\,{}^tJ\,{}^tP.$$

よって ${}^tP\,{}^tC = {}^tJ\,{}^tP$ すなわち $CP = PJ$ が成立する. □

27 体上の 1 変数多項式環上の加群

K は任意の体であるとする. 「任意の体」という用語に慣れていない人は $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ であると考えて良い. (さらに K が代数閉体だと仮定する場合には $K = \mathbb{C}$ であると考えて良い.)

すっきりした説明をするためにはどうしても可換環とその上の加群の一般論が必要になるので必要最小限の一般論を混じえながら, 体上の一変数多項式環とその上の加群の理論について解説する.

27.1 可換環とイデアルと単項イデアル整域

R が**可換環 (commutative ring)** であるとは[132], R が集合であり, 加法 $+ : R \times R \to R$ と $0 \in R$ と加法の逆元 $- : R \to R$ と乗法 $\cdot : R \times R \to R$ と $1 \in R$ が与えられていて, 以下が成立していることである:

1. R は加法に関して可換群をなす. すなわち $a, b, c \in M$ に対して,
   (a) $(a + b) + c = a + (b + c)$;
   (b) $0 + a = a + 0 = a$;
   (c) $(-a) + a = a + (-a) = 0$;
   (d) $a + b = b + a$.
2. 乗法 $\cdot : R \times R \to R$ は**結合的 (associative)** かつ**双加法的 (bi-additive)** であり, $1 \in R$ は乗法に関する単位元になる. すなわち $a, b, c \in R$ に対して,
   (a) $(ab)c = a(bc)$;
   (b) $a(b + c) = ab + ac$;
   (c) $(a + b)c = ac + bc$;
   (d) $1a = a1 = a$.
3. R の乗法は**可換 (commutative)** である. すなわち $a, b \in R$ に対して
   (e) $ab = ba$.

さらに次の条件が成立しているならば R は**体 (field)** であるという[133]:

4. 任意の $a \in R \setminus \{0\}$ に対してある $b \in R \setminus \{0\}$ が存在して $ba = ab = 1$.

このような b は a に対して一意的に定まる. 実際 $ba = 1$, $ab' = 1$ ならば $b' = 1b' = (ba)b' = b(ab') = b1 = b$. 要するに 0 でない $a \in R$ に対してその逆元 $a^{-1} = 1/a$ が常に R 自身の中に存在するような可換環を体と呼ぶのである. たとえば $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である.

可換環 R が**整域 (integral domain)** であるとは, 任意の $a, b \in R$ に対して $ab = 0$ ならば $a = 0$ または $b = 0$ が成立することである.

[422] 体は整域である. □

[423] 体 K 上の一変数多項式環 $K[\lambda]$ は整域である. □

[424] $\mathbb{Z}$ は整域である. □

[425] R が整域ならば R 上の n 変数多項式環 $R[x_1, \ldots, x_n]$ も整域である. □

可換環論について習いたての時期には整域の元としては整数や多項式のようなものを想像しておけばよい.

---

[132] 面倒な場合には単に環 (ring) と呼ぶ場合もある.
[133] **可換体 (commutative field)** と呼ぶ場合もある. 非可換な体は**斜体 (skew field)** と呼ばれる.

[**426**] K を体とし, R は K の元を成分に持つ n 次の対角行列全体の集合であるとすると, R は自然に可換環をなす. $n \geq 2$ ならば R は整域でない. □

ヒント: $n \geq 2$ のとき, $a = \mathrm{diag}(1, 0, 0, \ldots, 0)$, $b = \mathrm{diag}(0, 1, 0, \ldots, 0)$ と置くと $ab = 0$ である. よって $n \geq 2$ のとき R は整域でない. □

可換環 R の部分集合 I が R の**イデアル (ideal)** であるとは次の 2 つの条件が成立していることである:

1. 任意の $f, g \in I$ に対して $f + g \in I$;
2. 任意の $a \in R$ と $f \in I$ に対して $af \in I$.

後者の条件を $RI \subset I$ と略記することがある[134]. $1 \in R$ なので実際には $RI = I$ が成立している.

R の部分集合 I に対して, I がイデアルであることは I の元たちの任意の R 係数有限一次結合が I に含まれることと同値である.

[**427**] I が R のイデアルのとき $1 \in I$ と $I = R$ は同値である. □

R のイデアル I, J に対して, I の元と J の元の和全体の集合を $I + J$ と書き, I の元と J の元の積の有限和全体の集合を IJ と書くことにする.

[**428**] I, J, J' が可換環 R のイデアルであるとき, $I + J$ と $I \cap J$ と IJ も R のイデアルであり, 以下が成立している:

1. $IJ \subset I \cap J \subset I \subset I + J$.
2. $I(J + J') = IJ + IJ', \quad RI = I, \quad I + R = R$.
3. $I \subset J$ ならば $I \cap J = I$, $I + J = J$. □

[**429**] $f_1, \ldots, f_n \in R$ に対して R の部分集合 I を次のように定める:

$$I = Rf_1 + \cdots + Rf_n = \{\, a_1 f_1 + \cdots + a_n f_n \mid a_1, \ldots, a_n \in R \}.$$

このとき I は $f_1, \ldots, f_n$ を含む最小のイデアルである. これを $f_1, \ldots, f_n$ **から生成されるイデアル (ideal generated by** $f_1, \ldots, f_n$**)** と呼び $(f_1, \ldots, f_n)$ と表わす. □

ヒント: I は $f_1, \ldots, f_n$ の R 係数一次結合全体の集合なので $f_1, \ldots, f_n$ を含むイデアルは I を含んでいなければいけない. □

整域 R が**単項イデアル整域 (principal ideal domain)** もしくは **PID** であるとは, R の任意のイデアル I に対してある $a \in R$ で $I = (a) = Ra$ を満たすものが存在することである.

[**430**] **(体のイデアルによる特徴付け)** R は可換環であるとする. このとき R が体であるための必要十分条件は R のイデアルが 0 と R 以外に存在しないことである. 体のイデアルの全体は $(0), (1)$ なので体は単項イデアル整域である. □

[134] より正確に言えば R の元と I の元の積の有限和全体の集合を RI と定義しておく.

ヒント: R が体であるとき I が R の 0 でないイデアルならば 0 でない $a \in I$ が存在する. よって $1 = a^{-1}a \in I$ であるから $I = R$ となる. R が体でないならば逆元を持たない 0 でない $a \in R$ が存在する. このとき, $I = Ra$ は R の 0 でないイデアルであり, $1 \notin I$ であるから $I \neq R$ である. □

解説: 第 27.2 節で解説するように可換環 R のイデアルの定義は R 自身の R 部分加群の定義と一致し, 体 K 上の加群の定義は体 K 上のベクトル空間の定義と一致している. 上の問題の結論の意味は「体上の 1 次元ベクトル空間の部分空間の次元は 1 以下になる」ということである. 単項イデアル整域の定義はこの事実の一般化になっている. 厳密な言い方ではないが「$M = Ru$ のように表わされる R 加群 M の "次元は 1 以下" である」と仮にいうことにすれば, 整域 R が単項イデアル整域であるとは R 自身の任意の R 部分加群の "次元が 1 以下" になることである. もちろん一般の整域では "次元" の大きさに関するこのような直観は通用しない (問題 [**438**], [**439**]). "次元" の大きさに関する直観が通用する単項イデアル整域上の加群の世界は体上のベクトル空間の世界の次に簡単になる. それとは対照的に一般の整域や可換環上の加群の世界はおそろしく複雑である. □

[**431**] **(体上の 1 変数多項式環は PID)** 体 K 上の一変数多項式環 $K[\lambda]$ の 0 でない任意のイデアル I に対して, モニックな多項式 $f \in I$ で $I = K[\lambda]f = (f)$ を満たすものが一意に存在する. よってモニックな多項式 $f \in K[\lambda]$ と $K[\lambda]$ の 0 でないイデアルは一対一に対応している. 特に $K[\lambda]$ は単項イデアル整域である. □

ヒント: $I \neq \{0\}$ なので I に含まれる 0 でない多項式の中に次数が最小の多項式 $f \in I$ が存在する. 必要ならば最高次の係数で割ることによって f はモニックなものに取れる. 任意に $g \in I$ を取り, g を f で割った余りを r とする. $r \in I$ でかつ r の次数は f より小さいので f の次数の最小性より $r = 0$ である. よって $g \in (f)$ である. これで $I = (f)$ であることがわかった. モニックな多項式 $f, g \in I$ が $I = (f) = (g)$ を満たしているとする. このときある $a, b \in K[\lambda]$ が存在して $g = af$, $f = bg$ が成立する. このとき, $g = af = abg$ なので $ab = 1$ よって $a, b \in K \setminus \{0\}$ である. しかし f も g もモニックなので $a = b = 1$ である. これで $f = g$ であることがわかった. □

[**432**] **($\mathbb{Z}$ は PID)** $\mathbb{Z}$ の任意のイデアル I に対して, 非負の整数 $m \in I$ で $I = m\mathbb{Z} = (m)$ を満たすものが一意に存在する. よって 0 以上の整数 $m \in \mathbb{Z}_{\geq 0}$ と $\mathbb{Z}$ のイデアルは一対一に対応している. 特に $\mathbb{Z}$ は PID である. □

ヒント: 問題 [**431**] とまったく同様. □

解説: 上の問題の結果を用いてよく使われる問題 [**324**] の結果を再証明しておこう. 上の問題の結果より, $\mathbb{Z}$ は単項イデアル整域なので, 任意の $m_1, \ldots, m_N \in \mathbb{Z}$ に対して, ある $h \in \mathbb{Z}$ で $(m_1, \ldots, m_N) = (h)$ を満たすものが存在する. このとき $m_i \in h\mathbb{Z}$ なので m_i はどれも h で割り切れ, $h \in m_1\mathbb{Z} + \cdots + m_N\mathbb{Z}$ なので h は $m_1, \ldots, m_N$ の任意の公約数で割り切れる. よって h は $m_1, \ldots, m_N$ の最大公約数である. □

問題 [**431**], [**432**] より「割り算」できる整域は単項イデアル整域になることがわかる.

「割り算」ができる整域を正確に定義したものは **Euclid 整域 (Euclidean domain)** と呼ばれている. 整域 R が Euclid 整域であるとは, $\{0, 1, 2, \ldots\}$ と同型な全順序集合 $\mathcal{V}$ と写像 $\sigma : R \to \mathcal{V}$ が与えられていて[135], 以下の条件が成立していることである:

[135] $\mathcal{V}$ は任意の整列集合に取っても良い.

(a) 任意の $a \in R$ に対して $a = 0$ であることと $\sigma(a)$ が $\mathcal{V}$ の最小限であることは同値である.

(b) 任意の $a, b \in R$ に対して, $a \neq 0$ ならばある $q, r \in R$ で $b = aq + r$ かつ $\sigma(r) < \sigma(a)$ を満たすものが存在する[136].

このとき σ を**サイズ函数 (size function)** と呼ぶことにする.

たとえば, $R = \mathbb{Z}$ は $\mathcal{V} = \{0, 1, 2, \ldots\}$, $\sigma(a) = |a|$ によって Euclid 整域であり, R が体 K 上の 1 変数多項式環 $K[\lambda]$ は $\mathcal{V} = \{-\infty, 0, 1, 2, \ldots\}$, $\sigma(a) = \deg a$ によって Euclid 整域である. 便宜的に $\deg 0 = -\infty$ と定義しておいたのであった.

[433] ($\mathbb{Z}[i]$ は Euclid 整域) $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$ は自然に可換環をなす. $\mathbb{Z}[i]$ の元を **Gauss 整数**と呼び, $\mathbb{Z}[i]$ を **Gauss の整数環** と呼ぶ. サイズ函数 $\sigma : \mathbb{Z}[i] \to \{0, 1, 2, \ldots\}$ を $m + ni \in \mathbb{Z}[i]$ $(m, n \in \mathbb{Z})$ に対して $\sigma(m + ni) = |m + ni|^2 = m^2 + n^2$ と定めれば, $\mathbb{Z}[i]$ は Euclid 整域である. □

ヒント: まず $\mathbb{Z}[i]$ を複素平面上に図示せよ. $a, b \in \mathbb{Z}[i]$, $a \neq 0$ であるとする. このとき b/a に最も近い $\mathbb{Z}[i]$ の元を q とすると, $\mathbb{Z}[i]$ の形より $|b/a - q| \leq \sqrt{2}/2 < 1$ であることがわかる. $|b - aq| < |a|$ であるから, $r = b - aq \in \mathbb{Z}[i]$ と置くと $\sigma(r) = |r|^2 = |b - aq|^2 < |a|^2 = \sigma(a)$ である. □

[434] 1 の原始 3 乗根を $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2$ と書くことにする. $\mathbb{Z}[\omega] = \{m + n\omega \mid m, n \in \mathbb{Z}\}$ は自然に可換環をなす. サイズ函数 $\sigma : \mathbb{Z}[\omega] \to \{0, 1, 2, \ldots\}$ を $m + n\omega \in \mathbb{Z}[i]$ $(m, n \in \mathbb{Z})$ に対して $\sigma(m + n\omega) = |m + n\omega|^2 = m^2 - mn + n^2$ と定めれば, $\mathbb{Z}[\omega]$ は Euclid 整域である. □

ヒント: まず $\mathbb{Z}[\omega]$ を複素平面上に図示せよ. $a, b \in \mathbb{Z}[\omega]$, $a \neq 0$ であるとする. b/a に最も近い $\mathbb{Z}[\omega]$ の元を q とすると, $\mathbb{Z}[\omega]$ の形より $|b/a - q| < 1$ であることがわかる. そのとき $|b - aq| < |a|$ であるから, $r = b - aq \in \mathbb{Z}[\omega]$ と置くと $\sigma(r) = |r|^2 = |b - aq|^2 < |a|^2 = \sigma(a)$ である. □

[435] (Euclid 整域は PID) Euclid 整域は PID である. □

ヒント: 問題 **[431]** とまったく同様. □

[436] 体 K 上の多項式 $f_1, \ldots, f_n \in K[\lambda]$ に対して

$$(f_1, \ldots, f_n) = (g), \qquad (f_1) \cap \cdots \cap (f_n) = (h)$$

を満たす $g, h \in K[\lambda]$ が存在し, g は $f_1, \ldots, f_n$ の最大公約元になり, h は $f_1, \ldots, f_n$ の最小公倍元になる. □

ヒント: そのような g と h の存在は問題 **[431]** の結果から得られる. $g \in (f_1, \ldots, f_n) = K[\lambda]f_1 + \cdots + K[\lambda]f_n$ なので g は $f_1, \ldots, f_n$ の任意の公約元で割り切れる. $f_i \in K[\lambda]g$ なのでどの f_i も g で割り切れる. よって g は $f_1, \ldots, f_n$ の最大公約元である. $(f_1) \cap \cdots \cap (f_n) = K[\lambda]f_1 \cap \cdots \cap K[\lambda]f_n$ は f_i たちの公倍元全体の集合なので $(f_1) \cap \cdots \cap (f_n) = (h)$ ならば h は f_i たちの公倍元であり, f_i たちの任意の公倍元は h で割り切れる. よって h は $f_1, \ldots, f_n$ の最小公倍元である. □

[136] 商 q と余り r は一意的に定まらなくてもよい.

[437] 任意の整数 $a_1, \ldots, a_n \in \mathbb{Z}$ に対して

$$(a_1, \ldots, a_n) = (b), \qquad (a_1) \cap \cdots \cap (a_n) = (c)$$

を満たす $b, c \in \mathbb{Z}$ が存在し, b は $a_1, \ldots, a_n$ の最大公約数になり, c は $a_1, \ldots, a_n$ の最小公倍元になる. □

ヒント: 問題 **[436]** とまったく同様. □

[438] 体 K 上の 2 変数多項式環 $K[x, y]$ のイデアル $I = (x, y)$ に対して, どのような $h \in I$ を取っても $I \neq (h)$ となる. よって $K[x, y]$ は単項イデアル整域ではない. □

ヒント: 任意の $f \in K[x, y]$ に対して, $f \in I = (x, y)$ が成立するための必要十分条件は f の定数項が 0 であることである. よって $I \neq 0, K[x, y]$ である. ある $h \in I$ で $I = (h)$ を満たすものが存在すると仮定して矛盾を導く. ある $a, b \in K[x, y]$ が存在して $x = ah$, $y = bh$ となる. $h \in K$ ならば $(h) = 0, K[x, y]$ となるので $h \notin K$ である. すなわち h は次数が 1 以上の多項式である. よって $x = ah$ の両辺の多項式としての次数を考えると $a \in K \setminus \{0\}$ でなければいけないことがわかる. よって $h = a^{-1}x$ なので $y = bh = a^{-1}bx$ となって矛盾する. □

参考: 上の問題より, $n \geq 2$ のとき体上の n 変数多項式環は PID にならないこともわかる. そのせいで多変数多項式環のイデアルの世界はおそろしく複雑になる. それとは対照的に一変数多項式環のイデアルの世界は易しい. 幾何的には体上の n 変数多項式環のイデアルは n 次元アフィン空間内の代数的な図形と対応している[137]. 次元が 1 ならば直線上の図形なのでせいぜい有限個の点が並ぶ程度であり易しい. しかし, 次元が 2 以上になると図形として曲線や曲面などが存在可能なのでおそろしく複雑になる. 多変数多項式環のイデアルの世界がおそろしく複雑な理由は幾何的にはこのように理解できる. □

[439] 体 $\mathbb{Z}$ 上の 1 変数多項式環 $\mathbb{Z}[x]$ のイデアル $I = (7, x)$ に対して, どのような $h \in I$ を取っても $I \neq (h)$ となる. よって $\mathbb{Z}[x]$ は単項イデアル整域ではない. □

ヒント: $f \in \mathbb{Z}[x]$ に対して, $f \in I = (7, x)$ が成立するための必要十分条件は f の定数項が 7 で割り切れることである. よって $I \neq 0, \mathbb{Z}[x]$ である. ある $h \in I$ で $I = (h)$ を満たすものが存在すると仮定して矛盾を導く. ある $a, b \in \mathbb{Z}[x]$ が存在して $7 = ah$, $x = bh$ となる. $h = 0, \pm 1$ ならば $(h) = 0, \mathbb{Z}[x]$ となるので $h \neq 0, \pm 1$ である. x に関する $7 = ah$ の両辺の次数を考えると $a, h \in \mathbb{Z}$ であり, $a = \pm 1$, $h = \pm 7$ であることがわかる. よって $x = bh = \pm 7b$ となって矛盾する. □

27.2 可換環上の加群

集合 M が環 R 上の**加群 (module over R)** もしくは R **加群 (R-module)** であるとは加法 $+ : M \times M \to M$, ゼロ元 $0 \in M$ と加法に関する逆元 $- : M \to M$ と R の元の

[137] Hilbert の基定理より $R = K[x_1, \ldots, x_n]$ の任意のイデアル I はある $f_1, \ldots, f_N \in I$ によって $I = (f_1, \ldots, f_N)$ と表わされる. 1 このイデアルは $x_1, \ldots, x_n$ に関する連立方程式 $f_1 = \cdots = f_n = 0$ に対応していると考えられる. たとえば $R = \mathbb{R}[x, y, z]$ のとき $I = (x^2 + y^2 - 1, z)$ は xy 平面上の単位円の方程式に対応している.

M の元への作用 $\cdot : R \times M \to M$ が定義されていて, 以下の R 加群の公理が成立していることである[138]:

1. M は加法に関して可換群をなす. すなわち任意の $u, v, w \in M$ に対して,
   (a) $(u+v)+w = u+(v+w)$;
   (b) $0+u = u+0 = u$;
   (c) $(-u)+u = u+(-u) = 0$;
   (d) $u+v = v+u$.
2. スカラー倍 $\cdot : R \times M \to M$ は結合的かつ**双加法的 (bi-additive)** であり, $1 \in R$ の作用は恒等写像になる. すなわち任意の $a, b \in R$, $u, v \in M$ に対して,
   (a) $(ab)u = a(bu)$;
   (b) $a(u+v) = au+av$;
   (c) $(a+b)u = au+bu$;
   (d) $1u = u$.

R が体ならばこの公理は体上のベクトル空間の公理に等しい.

[440] たとえば R 自身は自然に R 加群とみなせる. 数ベクトル空間の場合と同様に n 個の R の元の組全体の集合 R^n も自然に R 加群をなす. この事実を正確に説明せよ. □

M が R 加群であるとき, M の部分集合 N が M の R **部分加群 (R-submodule)** であるとは次の 2 つの条件が成立していることである:

1. 任意の $u, v \in N$ に対して $u+v \in N$;
2. 任意の $a \in R$ と $u \in N$ に対して $au \in N$.

後者の条件を $RN \subset N$ と略記することがある[139]. $1 \in R$ なので実際には $RN = N$ が成立している.

イデアルは部分加群の特別な場合である.

[441] 可換環 R のイデアルの定義と R 自身の R 部分加群の定義が一致していることを確かめよ. □

---

[138] 実は以下の定義において R は非可換環であっても良い. その場合には非可換環 R 上の**左 R 加群 (left R-module)** の定義になる. 可換環上の加群については左加群と右加群を区別する必要はないが, 非可換環上の加群については左加群と右加群を区別する必要がある.

たとえば, 複素 n 次正方行列全体の集合 $M_n(\mathbb{C}) = M_{n,n}(\mathbb{C})$ は $n \geq 2$ ならば自然に非可換環をなす. 複素 n 次元縦ベクトルには左から複素 n 次正方行列をかけることができるので, 複素 n 次元縦ベクトル全体の空間 $M_{n,1}(\mathbb{C})$ は自然に $M_n(\mathbb{C})$ 上の左加群とみなされる. 同様に複素 n 次元横ベクトルには右から複素 n 次正方行列をかけることができるので, 複素 n 次元横ベクトル全体の空間 $M_{1,n}(\mathbb{C})$ は自然に $M_n(\mathbb{C})$ 上の右加群とみなされる. この場合には縦ベクトルと横ベクトルの違いが左加群と右加群の違いに対応している.

[139] より正確に言えば, R の元と N の元の積の有限和全体の集合を RN と定義しておく.

[442] L が R 加群であり, M, N が L の R 部分加群であるとき, M との元と N の元の和全体の集合 $M+N$ と $M\cap N$ は共に L の R 部分加群になる. さらに I が R のイデアルであるとき I の元と M の元の積の有限和全体の集合 IM は M の R 部分加群である. □

M, N が R 加群であるとき, 写像 $\phi : M \to N$ が R 上の**準同型写像 (homomorphism over R)** もしくは R **準同型 (R-homomorphism)** であるとは次の 2 つの条件が成立していることである:

1. 任意の $u, v \in M$ に対して $\phi(u+v) = \phi(u) + \phi(v)$.
2. 任意の $a \in R$ と $u \in M$ に対して $\phi(au) = a\phi(u)$.

R が体ならば R 準同型の定義は体上の線形写像の定義に一致する.

[443] 可換環 R の元を成分に持つ (m,n) 型行列全体の集合を $M_{m,n}(R)$ と表わし, n 次正方行列全体の集合を $M_n(R)$ と表わす. ベクトル空間の場合と同様に R^n と縦ベクトルの空間 $M_{n,1}(R)$ を同一視しておく. このとき行列 $A \in M_{m,n}(R)$ に対して写像 $\phi : R^n \to R^m$ を $\phi(u) = Au \in M_{m,1}(R)$ $(u \in R^n = M_{n,1}(R))$ と定めると ϕ は R 準同型である. □

[444] 任意の R 準同型 $\phi : R^n \to R^m$ は (m,n) 型行列 $A \in M_{m,n}(R)$ で一意的に表現できる. □

ヒント: ベクトル空間の場合と同様である. 第 i 成分だけが 1 で他の成分が 0 であるような R^n の元を e_i と書くことにする. 文脈によって区別が付く場合は R^m の e_i も同じ記号 e_i で表わすことにする. R 準同型 $\phi : R^n \to R^m$ を与える行列 $A \in M_{m,n}(R)$ は次の式によって得られる:

$$[\phi(e_1), \ldots, \phi(e_n)] = [e_1, \ldots, e_m]A = A.$$

このとき $x = {}^t[x_1, \ldots, x_n] \in R^n$ に対して

$$\begin{aligned}\phi(x) &= \phi(x_1e_1 + \cdots + x_ne_n) = x_1\phi(e_1) + \cdots + x_n\phi(e_n)\\ &= \phi(e_1)x_1 + \cdots + \phi(e_n)x_n = [\phi(e_1), \ldots, \phi(e_n)]x = Ax.\end{aligned}$$

これで ϕ の行列表現が存在することがわかった. $A, B \in M_{m,n}$ が $\phi(x) = Ax = Bx$ $(x \in R^n)$ を満たしているならば $(A$ の第 i 列$) = Ae_i = Be_i = (B$ の第 i 列$)$ となるので $A = B$ である. これで行列表現の一意性もわかった. □

解説: 注意 R が体でないならば R^n と同型でない有限生成 R 加群が存在する. たとえば $R = \mathbb{Z}$ のとき $M = \mathbb{Z}/24\mathbb{Z}$ は有限群なので絶対に $\mathbb{Z}^n$ と同型にならない. □

[445] **(同型写像)** R 加群のあいだの R 準同型 $\phi : M \to N$ が逆写像 ϕ^{-1} を持つとき, ϕ^{-1} も R 準同型になる. このとき ϕ は R **同型 (R-isomorphism)** であるという. R 加群 M, N のあいだに R 同型が存在するとき, M と N は R **上同型 (isomorphic over R)** であるという. □

[446] **(核と像)** R 加群のあいだの R 準同型 $\phi : M \to N$ に対して, その**核 (kernel)** $\operatorname{Ker}\phi$ と**像 (image)** $\operatorname{Im}\phi$ が次のように定義される:

$$\operatorname{Ker}\phi = \phi^{-1}(0) = \{\, u \in M \mid \phi(u) = 0 \,\}, \qquad \operatorname{Im}\phi = \phi(M) = \{\, \phi(u) \mid u \in M \,\}.$$

このとき, $\operatorname{Ker}\phi$ は M の R 部分加群であり, $\operatorname{Im}\phi$ は N の R 部分加群である. □

[**447**] R 加群のあいだの準同型写像 $\phi : M \to N$ に対して以下が成立する:

1. M の R 部分加群 M' に対して $\phi(M')$ は N の R 部分加群である.
2. N の R 部分加群 N' に対して $\phi^{-1}(N')$ は M の R 部分加群である.
3. M の R 部分加群 M' に対して $\phi^{-1}(\phi(M')) = M' + \operatorname{Ker}\phi$.
4. N の R 部分加群 N' に対して $\phi(\phi^{-1}(N')) = N' \cap \operatorname{Im}\phi$.
5. ϕ が全射ならば, $\operatorname{Ker}\phi$ を含む M の R 部分加群 M' と N の R 部分加群 N' が対応 $M' \mapsto N' = \phi(M')$ およびその逆対応 $N' \mapsto M' = \phi^{-1}N'$ によって一対一に対応する. □

ヒント: 1, 2, 3, 4 から 5 が出る. □

[**448**] **(直積加群)** 可換環 R 上の加群の族 $\{M_i\}_{i\in I}$ の直積集合 $\prod_{i\in I} M_i$ には自然に R 群の構造が入る. そして各 $i \in I$ に対して写像 $\pi_i : \prod_{j\in I} M_j \to M_i$ を $\pi_i((v_j)_{j\in I}) = v_i$ と定めると, π_i は全射 R 準同型である. 以上を確かめよ. R 加群としての $\prod_{i\in I} M_i$ を $\{M_i\}_{i\in I}$ の**直積加群 (direct product module)** と呼ぶ. □

ヒント: $M = \prod_{i\in I} M_i$ の加法は各成分ごとに定め, $a \in R$ と $(v_i)_{i\in I} \in M$ に対して $a(v_i)_{i\in I} = (av_i)_{i\in I}$ と定める. □

[**449**] **(直和加群 1)** 可換環 R 上の加群の直積 $\prod_{i\in I} M_i$ の R 部分加群 $\bigoplus_{i\in I} M_i$ を次のように定めることができる:

$$\bigoplus_{i\in I} M_i = \Big\{ (v_i)_{i\in I} \in \prod_{i\in I} M_i \;\Big|\; \text{有限個を除いて } v_i = 0 \Big\}.$$

特に I が有限集合ならば $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$ である. 写像 $\iota_i : M_i \to \bigoplus_{j\in I} M_j$ を $\iota_i(v_i) = (v_{i,j})_{j\in I}$ と定める. ここで $v_{i,i} = v_i$ でかつ $j \neq i$ のとき $v_{i,j} = 0 \in M_j$ である. このとき ι_i は単射 R 準同型である. 以上を確かめよ. 通常 M_i と $\iota_i(M_i) \subset \bigoplus_{i\in I} M_i$ は ι_i を通して同一視され, $\bigoplus_{i\in I} M_i$ は $\{M_i\}_{i\in I}$ の**直和加群 (direct sum module)** と呼ばれる. □

$I = \{1, \ldots, n\}$ のとき直積加群と直和加群を次のように書くことも多い:

$$\prod_{i\in I} M_i = M_1 \times \cdots \times M_n, \qquad \bigoplus_{i\in I} M_i = M_1 \oplus \cdots \oplus M_n.$$

たとえば

$$R^n = \overbrace{R \times \cdots \times R}^{n \text{ times}} = \overbrace{R \oplus \cdots \oplus R}^{n \text{ times}}.$$

[**450**] **(直和加群 2)** 可換環 R 上の加群 M の部分加群の族 $\{M_i\}_{i\in I}$ が与えられたとき, R 準同型 $\phi : \bigoplus_{i\in I} M_i \to M$ を $\phi((v_i)_{i\in I}) = \sum_{i\in I} v_i$ と定めることができる. 右辺の和は直和加群の定義より有限和なので well-defined である. このとき以下の条件は互いに同値である:

(a) $\phi : \bigoplus_{i\in I} M_i \to M$, $(v_i)_{i\in I} \mapsto \sum_{i\in I} v_i$ は R 同型である.

(b) 任意の $v \in M$ が $v = \sum_{i\in I} v_i$ $(v_i \in M_i$ であり, 有限個を除いて $v_i = 0)$ と一意に表わされる.

この条件が成立するとき ϕ を通して $\bigoplus_{i\in I} M_i$ と M を同一視して, M は部分加群 M_i たちの直和であるということが多い. □

27.3 商加群と加群の準同型定理

以下 R は可換環であるとする.

R 加群 M とその R 部分加群 N に対して, M を N で割ってできる**商加群 (quotient module)** M/N が以下のように定義される. まず各 $u \in M$ に対して $u \bmod N$ を次のように定める:

$$u \bmod N := u + N = \{\, u + v \mid v \in N \,\}.$$

さらに M/N を次のように定める:

$$M/N := \{\, u \bmod N \mid u \in M \,\}.$$

M/N には以下の条件によって R 加群の構造を入れることができる:

1. $u, v \in M$ に対して $(u \bmod N) + (v \bmod N) = (u + v) \bmod N$.
2. $a \in R$ と $u \in M$ に対して $a(u \bmod N) = (au) \bmod N$.

ただし, この定義が well-defined でかつ実際に R 加群の構造を M/N に定めることをチェックしなければいけない.

[451] 実際にそのことを以下の方針でチェックせよ.

1. $u, v \in M$ に対して $u \bmod N = v \bmod N$ と $u - v \in N$ は同値である.
2. $u, u', v, v' \in M$ は $u \bmod N = u' \bmod N$, $v \bmod N = v' \bmod N$ を満たしていると仮定する. このとき $(u + v) - (u' + v') = (u - u') + (v - v') \in N$ である. よって $(u + v) \bmod N = (u' + v') \bmod N$ である. これで $(u \bmod N) + (v \bmod N)$ が u, v の取り方によらずにうまく定義されることがわかった.
3. $u, u' \in M$ は $u \bmod N = u' \bmod N$ を満たしていると仮定する. このとき $a \in R$ に対して $au - au' = a(u - u') \in N$ である. よって $(au) \bmod N = (au') \bmod N$ である. これで $a(u \bmod N)$ が u の取り方によらずにうまく定義されることがわかった.
4. M が $+$ について可換群をなすことから, M/N が $+$ について可換群をなすことを導ける.
5. M が R 加群であることから M/N も R 加群であることを導ける.
6. 自然な写像 $\pi : M \to M/N$, $u \mapsto u \bmod N$ は全射 R 準同型である.
7. $\mathrm{Ker}\, \pi = N$ である. □

体 K 上のベクトル空間の商加群は**商ベクトル空間 (quotient vector space)** と呼ばれる.

商加群を理解するときに $u \bmod N = u + N$ を M の部分集合であることにこだわり続けてはいけない. $u \bmod N = u + N$ をあたかも「一点」であるかのように考えなければいけない.

u を通る N に「平行」な M の部分空間 $u + N$ の上の点をすべて同一の点だとみなしてできる加群が M/N である. 直観的に M/N は M を N 方向に潰してできる加群である.

代数学において記号法 M/N は M の中の N を 0 に潰してできる空間という意味で使われる.

[452] $\mathbb{R}^3$ の部分空間 Z を $Z = \{\, (0, 0, z) \mid z \in \mathbb{R} \,\}$ と定める. このとき, $\mathbb{R}^3/Z$ は $\mathbb{R}$ 上の 2 次元のベクトル空間になる. □

ヒント: $e_1 \bmod Z$, $e_2 \bmod Z$ が $\mathbb{R}^3/Z$ の基底をなすことを示せ. □

解説: $\mathbb{R}^3/Z$ は直観的に 3 次元空間 $\mathbb{R}^3$ を z 軸方向に潰してできる 2 次元空間だとみなせる. すなわち $\mathbb{R}^3$ の中の z 軸に平行な直線を「一点」に潰してできる 2 次元空間が $\mathbb{R}^3/Z$ である. □

[453] $\mathbb{Z}$ 加群 $\mathbb{Z}$ を部分加群 $3\mathbb{Z}$ で割ってできる $\mathbb{Z}$ 加群 $\mathbb{Z}/3\mathbb{Z}$ の元の個数は 3 である. □

ヒント: $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z},\, 1 + 3\mathbb{Z},\, 2 + 3\mathbb{Z}\}$ である. □

解説: $\mathbb{Z}/3\mathbb{Z}$ は 3 の倍数をすべて 0 と同一視してできる加群である. $\mathbb{Z}/3\mathbb{Z}$ において 3 の倍数はすべて 0 と同一視されているので差が 3 の倍数であるような 2 つの数はすべて同一視される. 結果的に $\mathbb{Z}/3\mathbb{Z}$ は 3 で割った余りの値で整数全体を分類してできる空間になる. □

R 加群のあいだの R 準同型 $\phi : M \to N$ に対して, その**余核 (cokernel)** $\operatorname{Coker}\phi$ と**余像 (coimage)** $\operatorname{Coim}\phi$ が次のように定義される:

$$\operatorname{Coker}\phi = N/\operatorname{Im}\phi, \qquad \operatorname{Coim}\phi = M/\operatorname{Ker}\phi.$$

[454] R 加群のあいだの R 準同型 $\phi : M \to N$ に対して以下が成立する:

1. ϕ が単射 $\iff \operatorname{Ker}\phi = 0$.
2. ϕ が全射 $\iff \operatorname{Coker}\phi = 0$.
3. ϕ が同型 $\iff \operatorname{Ker}\phi = 0$ かつ $\operatorname{Coker}\phi = 0$. □

次の**準同型定理 (homomorphism theorem)** は準同型写像に関する最も基本的な結果であり, 空気のごとく自由に使われる.

[455] (加群の準同型定理) R 加群のあいだの R 準同型 $\phi : M \to N$ は次の R 同型を誘導 (induce) する:

$$\tilde{\phi} : \operatorname{Coim}\phi \xrightarrow{\sim} \operatorname{Im}\phi, \quad u \bmod \operatorname{Ker}\phi \mapsto \phi(u).$$

$\operatorname{Im}\phi = \phi(M)$ と $\operatorname{Coim}\phi = M/\operatorname{Ker}\phi$ を代入すればこの同型は次のように表わされる:

$$\tilde{\phi} : M/\operatorname{Ker}\phi \xrightarrow{\sim} \phi(M), \quad u \bmod \operatorname{Ker}\phi \mapsto \phi(u). \quad \square$$

ヒント: 記号の簡単のため $N = \mathrm{Ker}\,\phi$ と置く. $u, u' \in M$ が $u \bmod N = u' \bmod N$ を満たしているとき, $u - u' \in N$ なので $\phi(u) - \phi(u') = \phi(u - u') = 0$ である. よって $\tilde{\phi}$ は well-defined である. $u, v \in M$ と $a \in R$ に対して,

$$\begin{aligned}&\tilde{\phi}((u \bmod N) + (v \bmod N)) = \tilde{\phi}((u + v) \bmod N)\\ &= \phi(u + v) = \phi(u) + \phi(v) = \tilde{\phi}(u \bmod N) + \tilde{\phi}(v \bmod N),\\ &\tilde{\phi}(a(u \bmod N)) = \tilde{\phi}((au) \bmod N) = \phi(au) = a\phi(u) = a\tilde{\phi}(u \bmod N).\end{aligned}$$

これで $\tilde{\phi}$ が R 準同型であることがわかった. 任意の $\phi(u) \in \phi(M)$ に対して $\tilde{\phi}(u \bmod N) = \phi(u)$ であるから $\tilde{\phi}$ は全射である. 任意の $u \in M$ に対して $0 = \tilde{\phi}(u \bmod N) = \phi(u)$ ならば $u \in N$ であり, よって M/N の中で $u \bmod N = 0$ である. これで $\tilde{\phi}$ が単射であることもわかった. 全単射準同型は同型写像である. □

[456] 体 K 上の一変数 n 次多項式 $f \in K[\lambda]$ を任意に取る. このとき f で生成されるイデアル $(f) = K[\lambda]f$ は $K[\lambda]$ 自身の $K[\lambda]$ 部分加群である. よって $K[\lambda]$ 自身の商加群 $K[\lambda]/(f)$ が定義される. $K \subset K[\lambda]$ なので自然に $K[\lambda]$ 加群は K 上のベクトル空間とみなされる. $K[\lambda]/(f)$ は K 上の n 次元のベクトル空間である. □

ヒント: 次数が n 未満の多項式全体のなす $K[\lambda]$ の K 部分ベクトル空間を V と書く. $\dim_K V = n$ である. 自然な写像 $\pi : K[\lambda] \to K[\lambda]/(f)$, $a \mapsto a \bmod f$ の V 上への制限 $\phi = \pi|_V$ が K 同型であることを示す[140]. $a \in K$, $g \in K[\lambda]$ に対して $\phi(ag) = (ag) \bmod f = a(g \bmod f) = a\phi(g)$ なので ϕ は K 線形写像である. $g \bmod f \in K[\lambda]/(f)$ が 0 であるための必要十分条件は g が f で割り切れることである. $g \in V$ のとき $\deg g < n$ なので $\phi(g) = g \bmod f = 0$ ならば $g = 0$ である. よって $\phi : M \to K[\lambda]/(f)$ は単射である. 任意の $g \in K[\lambda]$ に対して g を f で割った余りを $r \in V$ と書くと, $g - r \in (f)$ なので $\phi(r) = r \bmod f = g \bmod f$ である. よって $\phi : M \to K[\lambda]/(f)$ は全射である. これで ϕ が K 同型であることがわかった. □

解説: 上の問題とそのヒントは $K[\lambda]/(f)$ は「f で割った余り」全体のなす $K[\lambda]$ 加群とみなせることを示している. 直観的に $K[\lambda]/(f)$ は一変数多項式環 $K[\lambda]$ の中で f およびその多項式倍を 0 とみなすことによってできる加群である. □

[457] 任意に正の整数 $n \in \mathbb{Z}$ を取る. このとき n で生成されるイデアル $(n) = n\mathbb{Z}$ は $\mathbb{Z}$ 自身の $\mathbb{Z}$ 部分加群である. よって $\mathbb{Z}$ 自身の商加群 $\mathbb{Z}/n\mathbb{Z}$ が定義される. このとき $\mathbb{Z}/n\mathbb{Z}$ の元の個数は n である. □

ヒント: 集合 N を $N = \{0, 1, 2, \ldots, n-1\}$ と定める. 自然な写像 $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto a \bmod n$ の N 上への制限 $\phi = \pi|_N$ が全単射であることを示す[141]. $a \bmod n \in \mathbb{Z}/n\mathbb{Z}$ が 0 であるための必要十分条件は a が n で割り切れることである. $a \in N$ のとき $0 \le a < n$ なので $\phi(a) = a \bmod m = 0$ ならば $a = 0$ である. よって $\phi : N \to \mathbb{Z}/n\mathbb{Z}$ は単射である. 任意の $a \in \mathbb{Z}$ に対して a を n で割った余りを $r \in N$ と書くと, $a - r \in n\mathbb{Z}$ なので $\phi(r) = r \bmod n = a \bmod n$ である. よって $\phi : N \to \mathbb{Z}/n\mathbb{Z}$ は全射である. これで ϕ が全単射であることがわかった. □

[140] $K[\lambda]/(f)$ の元を $g \bmod (f)$ の代わりに $g \bmod f$ と書くことにする. $g \bmod f$ を「g モッド f」と読んだり, 「g modulo f」と読んだりする. 直観的に $g \bmod f$ は g を f で割った余りのことである.

[141] $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ の元を $a \bmod (n)$ や $a \bmod n\mathbb{Z}$ の代わりに $a \bmod n$ と書くことにする. 直観的に $a \bmod n$ は a を n で割った余りのことである.

解説: 上の問題とそのヒントは $\mathbb{Z}/n\mathbb{Z}$ は「n で割った余り」全体のなす加群とみなせることを示している. 直観的に $\mathbb{Z}/n\mathbb{Z}$ は有理整数環 $\mathbb{Z}$ の中で n およびその倍数を 0 とみなすことによってできる加群である. □

以下の**同型定理たち (isomorphism theorems)** は非常に有用である.

[458] R 加群のあいだの全射 R 準同型 $\phi : M \to N$ と N の R 部分加群 N' に対して, $\phi^{-1}(N')$ は M の R 部分加群であり, 次の R 同型が存在する:

$$M/\phi^{-1}(N') \xrightarrow{\sim} N/N', \quad u \bmod \phi^{-1}(N') \mapsto \phi(u) \bmod N'. \quad \square$$

ヒント: N から N/N' への自然な全射 R 準同型 $v \mapsto v \bmod N'$ を $N \twoheadrightarrow N'$ と書くことにする. R 準同型の列 $M \xrightarrow{\phi} N \twoheadrightarrow N/N'$ の合成が全射でかつその核が $\phi^{-1}(N')$ であることを示し, 準同型定理を適用せよ. □

[459] **(第二同型定理)** R 加群 L の 2 つの R 部分加群 M, N に対して次の R 同型が存在する:

$$M/(M \cap N) \xrightarrow{\sim} (M+N)/N, \quad u \bmod M \cap N \mapsto u \bmod N. \quad \square$$

参考: 準同型定理を**第一同型定理 (first isomorphism theorem)** と呼ぶことがある. □

ヒント: 集合 A が集合 X の部分集合であるとき A の X への**包含写像 (inclusion mapping)** を $A \hookrightarrow X$ と書くことにする. R 準同型の列 $M \hookrightarrow M+N \twoheadrightarrow (M+N)/N$ の合成が全射でかつその核が $M \cap N$ であることを示し, 準同型定理を適用せよ. □

[460] **(第三同型定理)** R 加群 L とその R 部分加群 $N \subset M \subset L$ に対して, M/N は L/N の R 部分加群になり, 次の R 同型が存在する:

$$L/M \xrightarrow{\sim} (L/N)/(M/N), \quad u \bmod M \mapsto (u \bmod N) \bmod M/N.$$

ヒント: R 準同型の列 $L \twoheadrightarrow L/N \twoheadrightarrow (L/N)/(M/N)$ の合成が全射でかつその核が M であることを示し, 準同型定理を適用せよ. □

次の結果もよく使われる.

[461] $\{M_i\}_{i\in I}$ は R 加群の族であり, 各 $i \in I$ に対して N_i は M_i の R 部分加群であるとする. このとき $\bigoplus_{i\in I} N_i$ は自然に $\bigoplus_{i\in I} M_i$ の R 部分加群とみなせ, 次の自然な R 同型が存在する:

$$\bigoplus_{i\in I} M_i \Big/ \bigoplus_{i\in I} N_i \xrightarrow{\sim} \bigoplus_{i\in I} M_i/N_i, \quad (v_i)_{i\in I} \bmod \bigoplus_{i\in I} N_i \mapsto (v_i \bmod N_i)_{i\in I}.$$

つまり直和を構成する操作と商加群を構成する操作は可換である[142]. □

ヒント: R 準同型 $\phi : \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} M_i/N_i$ を $\phi((v_i)_{i\in I}) = (v_i \bmod N_i)_{i\in I}$ と定めることができる. これに準同型定理を適用せよ □

[142]直和は他の多くの操作と可換になる. ここでは曖昧に「操作」という言葉を使っているが, **圏 (category)** と**函手 (functor)** の言葉を使えばより正確に「操作」の概念を扱うことができる. **加法圏 (additive category)** のあいだの**加法函手 (additive functor)** は常に有限直和と可換になる. 加群の準同型定理に類似の結果が成立している加法圏は **Abel 圏 (Abelian category)** と呼ばれており, **ホモロジー代数 (homological algebra)** のような道具の基礎になっている.

27.4 剰余環と環の準同型定理

可換環のあいだの写像 $\phi : A \to B$ が**環準同型 (ring homomorphism)** であるとは以下の条件を満たしていることである:

1. 任意の $a, b \in A$ に対して $\phi(a+b) = \phi(a) + \phi(b)$ かつ $\phi(ab) = \phi(a)\phi(b)$.
2. $\phi(1) = 1$.

[462] (剰余環) A は任意の可換環であり, I はそのイデアルであるとする. このとき A 自身の商加群 A/I には次によって自然に可換環の構造が入る:

$$(a \bmod I) \cdot (b \bmod I) := (ab) \bmod I \qquad (a, b \in A).$$

A/I を A の**剰余環 (residue ring)** もしくは**商環 (quotient ring)** と呼ばれる. 自然な写像 $\pi : A \to A/I$, $a \mapsto a \bmod I$ は環準同型である. □

ヒント: $a, a', b, b' \in A$ が $a \bmod I = a' \bmod I$, $b \bmod I = b' \bmod I$ を満たしているとき, $a - a', b - b' \in I$ であるから, $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a') \in I$ である. よって A/I における積は well-defined である. A/I が可換環をなすことが A が可換環であることより容易に導かれる. □

[463] (環の同型写像) 可換環のあいだの環準同型 $\phi : A \to B$ が逆写像 ϕ^{-1} を持つとき, ϕ^{-1} も環準同型である. このとき ϕ は**環の同型写像 (ring isomorphism)** であるという. 可換環 A と B が**環として同型 (isomorphic as rings)** であるとは A と B のあいだの環の同型写像が存在することである. □

可換環 A の部分集合 B が和と差と積に関して閉じており 1 を含むならば B は自然に可換環をなす. そのとき B は A **の部分環 (subring of A)** であるという.

可換環のあいだの環準同型 $\phi : A \to B$ に対してもその核と像が加群のあいだの準同型写像の場合と同様に定義される:

$$\operatorname{Ker}\phi = \{\, a \in A \mid \phi(a) = 0 \,\}, \qquad \operatorname{Im}\phi = \phi(A) = \{\, \phi(a) \mid a \in A \,\}.$$

[464] $\phi : A \to B$ は可換環のあいだの環準同型であるとすると以下が成立する:

1. A' が A の部分環であれば $\phi(A')$ は B の部分環である.
2. B' が B の部分環であれば $\phi^{-1}(B')$ は A の部分環である.
3. I が A のイデアルであれば $\phi(I)$ は $\phi(A')$ のイデアルである. しかし $\phi(I)$ は B のイデアルであるとは限らない.
4. J が B のイデアルであれば $\phi^{-1}(J)$ は A のイデアルである.
5. I が A のイデアルであれば $\phi^{-1}(\phi(I)) = I + \operatorname{Ker}\phi$.
6. J が B のイデアルであれば $\phi(\phi^{-1}(J)) = J \cap \operatorname{Im}\phi$.
7. もしも ϕ が全射ならば, $\operatorname{Ker}\phi$ を含む A のイデアル I と B のイデアル J は対応 $I \mapsto J = \phi(I)$ と逆対応 $J \mapsto I = \phi^{-1}(J)$ によって一対一に対応する.

ヒント: 3 の後半は次のような例がある. $A = \mathbb{Z}$, $B = \mathbb{Z}[x]$ であるとし, ϕ は $\mathbb{Z} \subset \mathbb{Z}[x]$ の包含写像であるとする. このとき任意の $m \in \mathbb{Z}_{\neq 0}$ に対して, $I = m\mathbb{Z}$ は $A = \mathbb{Z}$ のイデアルであるが $\phi(I) = m\mathbb{Z} \subset \mathbb{Z}[x]$ は $B = \mathbb{Z}[x]$ のイデアルではない. □

[465] (環の準同型定理) 可換環のあいだの環準同型 $\phi : A \to B$ に対して $\operatorname{Ker}\phi$ は A のイデアルになり, $\operatorname{Im}\phi$ は B の部分環をなす. しかも次の自然な環の同型写像が存在する:

$$\tilde{\phi} : A/\operatorname{Ker}\phi \xrightarrow{\sim} \operatorname{Im}\phi, \quad a \bmod \operatorname{Ker}\phi \mapsto \phi(a). \quad \square$$

ヒント: 加群の準同型定理とほとんど同じ. □

[466] 可換環のあいだの全射環準同型 $\phi : A \to B$ と B のイデアル J にに対して, $\phi^{-1}(J)$ は A のイデアルであり, 次の環同型が存在する:

$$A/\phi^{-1}(J) \xrightarrow{\sim} B/J, \quad a \bmod \phi^{-1}(J) \mapsto \phi(a) \bmod J. \quad \square$$

ヒント: $A \to B \twoheadrightarrow B/J$ の合成に準同型定理を適用せよ. □

[467] (第二同型定理) 可換環 A とそのイデアル I と部分環 B に対して, $B \cap I$ は B のイデアルになり, 次の環同型が存在する:

$$B/(B \cap I) \xrightarrow{\sim} (B + I)/I, \quad a \bmod B \cap I \mapsto a \bmod I. \quad \square$$

ヒント: $B \hookrightarrow B + I \twoheadrightarrow (B + I)/I$ の合成に準同型定理を適用せよ. □

[468] (第三同型定理) 可換環 A とそのイデアル $J \subset I \subset A$ に対して, I/J は A/J のイデアルになり, 次の環同型が存在する:

$$A/I \xrightarrow{\sim} (A/J)/(I/J), \quad a \bmod I \mapsto (a \bmod J) \bmod I/J.$$

ヒント: $A \twoheadrightarrow A/J \twoheadrightarrow (A/J)/(I/J)$ の合成に準同型定理を適用せよ. □

可換環 $R_1, \ldots, R_s$ の直積 $R = \prod_{i=1}^{s} R_i = R_1 \times \cdots \times R_s$ には自然に可換環の構造が入る. R の加法と乗法は各成分ごとに定め, R の 1 は $1 = (1, \ldots, 1)$ と定める.

[469] 体 K 上の一変数多項式環 $K[\lambda]$ を考え, 互いに異なる $\alpha_1, \ldots, \alpha_s \in K$ を任意に取り, $n_i \in \mathbb{Z}_{>0}$ とし, $p(\lambda) \in K[\lambda]$ を次のように定める:

$$p(\lambda) = (\lambda - \alpha_1)^{n_1} \cdots (\lambda - \alpha_s)^{n_s}.$$

このとき次の環同型存在する:

$$K[\lambda]/(p(\lambda)) \xrightarrow{\sim} \prod_{i=1}^{s} K[\lambda]/\big((\lambda - \alpha_i)^{n_i}\big), \quad f(\lambda) \bmod p(\lambda) \mapsto \big(f(\lambda) \bmod (\lambda - \alpha_i)^{n_i}\big)_{i=1}^{s}.$$

しかもこれは $K[\lambda]$ 加群の同型写像でもある. □

ヒント: 記号の簡単のため $A = K[\lambda]$, $I = (p(\lambda))$, $I_i = \big((\lambda-\alpha_i)^{n_i}\big)$ と置く. 写像 $\phi : A \to \prod_{i=1}^s A/I_i$ を $\phi(a) = (a \bmod I_i)_{i=1}^s$ と定める. ϕ は環準同型かつ A 準同型である. よって準同型定理より ϕ が全射でかつ $\operatorname{Ker}\phi = I$ であることを示せば示したい結果がすべて得られる.

$p_i(\lambda) = p(\lambda)/(\lambda-\alpha_i)^{n_i} \in A$ と置くと, $p_1, \dots, p_s$ は共通因子を持たないので問題 **[323]** の結果より, ある $a_1, \dots, a_s \in A$ で $a_1p_1 + \cdots + a_sp_s = 1$ を満たすものが存在する. よって $a_ip_i \equiv \delta_{ij} \mod I_j$ である. したがって任意の $(f_i \bmod I_i)_{i=1}^s \in \prod_{i=1}^s A/I_i$ に対して, $f = f_1a_1p_1 + \cdots + f_sa_sp_s \in A$ と置くと, $f \equiv f_ia_ip_i \equiv f_i \mod I_i$ である. すなわち $\phi(f) = (f_i \mod I_i)_{i=1}^s$ である. これで ϕ が全射であることがわかった.

$f \in A$ に対して $\phi(f) = (f \bmod I_i)_{i=1}^s = 0$ となるための必要十分条件は f がすべての $(\lambda-\alpha_1)^{n_1}, \dots, (\lambda-\alpha_s)^{n_s}$ で割り切れることである. この条件は f が $p(\lambda)$ で割り切れることと同値である. よって $\operatorname{Ker}\phi = (p(\lambda)) = I$ である. □

解説: 上の問題の結果は問題 **[331]** の結果や Lagrange-Sylvester の補間公式 (定理 22.1) を本質的に含んでいる. 上の問題の結果は問題 **[421]** のヒント 2 の出発点になっている. 上の問題を使えばコンパニオン行列の Jordan 標準形の存在を証明でき, しかも Jordan 標準形と相似変換行列の具体形も求まる. □

[470] (f 進展開) 体 K 係数の n 次多項式 $f \in K[\lambda]$ と正の整数 e が任意に与えられたとき, $K[\lambda]/(f^e)$ の任意の元は次の形で一意に表わされる:

$$g \bmod f^e = (a_0 + a_1f + a_2f^2 + \cdots + a_{e-1}f^{e-1}) \bmod f^e$$
$$(g, a_i \in K[\lambda],\ \deg g < n^e,\ \deg a_i < n). \quad \square$$

ヒント: 問題 **[456]** の結果とヒントを f^e に適用することによって $K[\lambda]/(f^e)$ の元と次数が n^e 未満の多項式は一対一に対応していることがわかる. よって次数が n^e 未満の多項式 $g \in K[\lambda]$ が

$$g = a_0 + a_1f + a_2f^2 + \cdots + a_{e-1}f^{e-1} \qquad (a_i \in K[\lambda],\ \deg a_i < n) \qquad (*)$$

と一意に表わされることを示せば良い. g が与えられたとき以下の手続きで次数が n 未満の $a_0, a_1, a_2, \dots \in K[\lambda]$ が得られる:

1. g を f で割った余りを a_0 とし, 商を g_1 とする.
2. もしも $g_k = 0$ ならば手続きを終了し, $a_k, a_{k+1}, \dots$ はすべて 0 であるとする.
3. もしも $g_k \neq 0$ ならば g_k を f で割った余りを a_k とし, 商を g_{k+1} として, 1 つ前のステップに戻る.

g_k の次数はこの手続きの各ステップで n 以上下がるので, $\deg g < n^e$ ならばこの手続きは遅くとも a_{e-1} を求めた段階で終了する. そのとき $(*)$ が成立しているので表示の存在が証明される. 逆に $(*)$ が成立しているならば各 a_i は上の手続きで求めたものと一致することも容易に確かめられるので, 表示の一意性も確かめられる. □

解説: $f(\lambda) = \lambda - \alpha$ のとき上の問題の展開は

$$g \equiv a_0 + a_1(\lambda-\alpha) + a_2(\lambda-\alpha)^2 + \cdots + a_{e-1}(\lambda-\alpha)^{e-1} \mod (\lambda-\alpha)^e \quad (a_i \in K)$$

と $\lambda-\alpha$ に関する巾級数展開 (Taylor 展開) を $e-1$ 次で切ったものになる. だから可換環 $K[\lambda]/\big((\lambda-\alpha)^e\big)$ は $\lambda-\alpha$ に関する巾級数展開を $e-1$ 次で切ることによって得られた世界になっている. 代数の世界では Taylor 展開の概念はこのように定式化される. □

[471] 2 以上の整数 $n \in \mathbb{Z}_{\geq 2}$ を任意に取り, $n = p_1^{e_1} \cdots p_s^{e_r}$ は n の素因数分解であるとする[143]. すなわち $p_1, \ldots, p_s$ は互いに異なる素数であり, $e_i \in \mathbb{Z}_{>0}$ であるとする. このとき次の環同型が存在する:

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z}), \quad a \bmod n \mapsto (a \bmod p_1^{e_1}, \ldots, a \bmod p_s^{e_r}). \quad \square$$

ヒント: 問題 **[469]** とまったく同様. $\square$

解説: 上の問題の結果は問題 **[332]** の結果と本質的に同値である. 次の問題を見よ. $\square$

[472] **(n 進展開)** 正の整数 n, e が任意に与えられたとき, $\mathbb{Z}/n^e\mathbb{Z}$ の任意の元は次の形で一意に表わされる:

$$m \bmod n^e = (a_0 + a_0 n + a_2 n^2 + \cdots a_{e-1} n^{e-1}) \bmod n^e$$
$$(m, a_i \in \mathbb{Z},\ 0 \leq m < n^e,\ 0 \leq a_i < n). \quad \square$$

ヒント: 問題 **[457]** の結果とヒントを使えば問題 **[470]** とまったく同様である. $\square$

参考: $n = 10$ の場合は通常の十進法の話になる. 面白いのは負の整数を n 進展開した場合である. たとえば -1 を 2 進展開すると,

$$-1 \equiv 2^e - 1 = 1 + 2 + 2^2 + \cdots + 2^{e-1} \mod 2^e.$$

ここで形式的に $e \to \infty$ とすると[144],

$$-1 = 1 + 2 + 2^2 + 2^3 + 2^4 + \cdots$$

が成立する. これは等比級数の和の公式 $1 + a + a^2 + \cdots = 1/(1-a)$ の $a = 2$ の場合である. このような議論を数学的に厳密に正当化すると p 進数の理論が得られる. $\mathbb{Z}_2$ もしくは $\mathbb{Q}_2$ の中で $1 + 2 + 2^2 + \cdots$ は実際に収束して -1 に等しくなる[145]. $\square$

可換環 R のイデアル I, J が $I + J = R$ を満たしているとき, I と J は**互いに素 (coprime)** であるという.

問題 **[469]**, **[471]** の結果は**中国式剰余定理 (Chinese remainder theorem)** の特殊な場合である.

[473] **(中国式剰余定理)** R は任意の可換環であるとし, $I_1, \ldots, I_n$ は R のイデアルであり, その中のどの 2 つも互いに素であると仮定する. すなわち $I_i + I_j = R$ $(i \neq j)$ が成立していると仮定する. このとき以下が成立する:

(1) $J_i = I_1 \cdots I_{i-1} I_{i+1} \cdots I_n$ と置くと[146] $J_1 + \cdots + J_n = R$ が成立する.

---

[143] p_i の p は prime (素数) の頭文字であり, e_i の e は exponent (指数) の頭文字である.

[144] -1 を素数 2 に対応する "点" で "Taylor 展開" するという風に考えよ. 素数 p と $\lambda - \alpha$ は非常に似ている. $\lambda - \alpha$ に関する巾級数展開は Taylor 展開と呼ばれている. それと同様の展開を素数に対しても考えることができるのである.

[145] 各素数 p に対して定まる $\mathbb{Z}_p$, $\mathbb{Q}_p$ はそれぞれ p **進整数環 (p-adic integer ring)**, p **進数体 (p-adic number field)** と呼ばれており, 集合として以下のように表わされる:

$$\mathbb{Z}_p = \{\, a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots \mid a_i = 0, 1, \ldots, p-1 \,\},$$
$$\mathbb{Q}_p = \{\, a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \cdots \mid n \in \mathbb{Z},\ a_i = 0, 1, \ldots, p-1 \,\}.$$

$\mathbb{Z}_p$ は $\mathbb{Z}/p^e\mathbb{Z}$ の $e \to \infty$ での**射影極限 (projective limit)** として構成され, $\mathbb{Q}_p$ は $\mathbb{Z}_p$ の分数体に等しい.

[146] $n = 1$ のとき $J_1 = R$ であると約束しておく.

(2) $I_1I_2\cdots I_n = I_1\cap\cdots\cap I_n$ である.

(3) 記号の簡単のため $I = I_1I_2\cdots I_n = I_1\cap\cdots\cap I_n$ と置く. 次の環同型が存在する:

$$R/I \xrightarrow{\sim} \prod_{i=1}^{n} R/I_i, \quad f \bmod I \mapsto \bigl(f \bmod I_i\bigr)_{i=1}^{n}.$$

これは R 加群の同型写像でもある. □

注意: 上の問題の (1) は「$a_1,\dots,a_n \in K[\lambda]$ のどの 2 つも互いに素であるならば, $b_i = a_1\cdots a_{i-1}a_{i+1}\cdots a_n$ と置くと $b_1,\dots,b_n$ の最大公約元は 1 になる」という結果の一般化になっている. さらに (2) は「$a_1,\dots,a_n \in K[\lambda]$ のどの 2 つも互いに素であるならば, $a_1,\dots,a_n$ の最小公倍元は $a_1\cdots a_n$ に等しい」という結果の一般化になっている. 問題 [**436**] を見よ.

ヒント 1: (1) n に関する帰納法で証明する. $n=1$ の場合は定義より $J_1 = R$ なので成立している. $n\geq 1$ のとき, 帰納法の仮定より $J_i' = I_1\cdots I_{i-1}I_{i+1}\cdots I_{n-1}$ $(i=1,\dots,n-1)$ と置くと, $J_1'+\cdots+J_{n-1}' = R$ が成立する. $i=1,\dots,n-1$ に対して $I_n+I_i = R$ なので, ある $a_i\in I_n$ と $b_i\in I_i$ で $a_i+b_i=1$ を満たすものが存在する. このとき $\prod_{i=1}^{n-1}(a_i+b_i)=1$ であり, この等式の左辺を展開すると $b_1\cdots b_{n-1}\in I_1\cdots I_{n-1}$ 以外の項がすべて I_n に含まれることがわかる. これで $I_n + I_1\cdots I_{n-1} = R$ が示された. したがって

$$\begin{aligned} R &= (J_1'+\cdots+J_{n-1}')(I_n + I_1\cdots I_{n-1}) \\ &= J_1'I_n+\cdots+J_{n-1}'I_n + I_1\cdots I_{n-1} = J_1+\cdots+J_n. \end{aligned}$$

(2) $I_1\cdots I_n\subset I_1\cap\cdots\cap I_n$ は常に成立するので逆の包含関係を示せば良い. (1) よりある $g_i\in J_i$ で $g_1+\cdots+g_n=1$ を満たすものが存在する. 任意の $f\in I_1\cap\cdots\cap I_n$ に対して $fg_i\in I_1\cdots I_n$ なので $f = fg_1+\cdots+fg_n\in I_1\cdots I_n$ である.

(3) 写像 $\phi: R\to\prod_{i=1}^n R/I_i$ を $\phi(f) = \bigl(f\bmod I_i\bigr)_{i=1}^n$ と定めると ϕ は環準同型かつ R 準同型である. したがって, 環の準同型定理と R 加群の準同型定理より, $\operatorname{Ker}\phi = I_1\cap\cdots\cap I_n$ および ϕ の全射性を示せば良い. $\phi(f)=0$ と $f\in I_i$ $(i=1,\dots,n)$ は同値であり, これはさらに $f\in I_1\cap\cdots\cap I_n$ と同値である. よって $\operatorname{Ker}\phi = I_1\cap\cdots\cap I_n$ である. (1) よりある $g_i\in J_i$ で $g_1+\cdots+g_n=1$ を満たすものが存在する. 任意の $f_1,\dots,f_n\in R$ に対して, $f = f_1g_1+\cdots+f_ng_n$ と置くと $f\equiv f_i \mod I_i$ である. すなわち $\phi(f) = \bigl(f_i\bmod I_i\bigr)_{i=1}^n$ である. これで ϕ の全射性が示された. □

ヒント 2: (1) を次のように証明することもできる. $i<j$ のとき $I_i+I_j = R$ であるから, ある $a_i^{ij}\in I_i$, $a_j^{ij}\in I_j$ で $a_i^{ij}+a_j^{ij}=1$ を満たすものが存在する. このとき $\prod_{1\leq i<j\leq n}(a_i^{ij}+a_j^{ij})=1$ である. 左辺を展開すると次の形にまとめられることがわかる:

$$g_1+\cdots+g_n=1, \qquad g_i\in J_i.$$

$I_1\cdots I_n$ に含まれる項は $I_1\cdots I_n\subset J_i$ なので g_i のどれにくりこんでも良い. □

解説: 上の問題で $R=K[\lambda]$, $I_i = \bigl((\lambda-\alpha_i)^{n_i}\bigr)$ とすれば問題 [**469**] の結果が導かれる. そのとき, $(p(\lambda)) = I_1\cdots I_n = I$ であり, 問題 [**469**] のヒントにおける a_ip_i は上の問題のヒントにおける g_i の役目を果たしており, $(p_i(\lambda)) = J_i$ が成立している. □

27.5 単元と素元と既約元

R は可換環であるとする.

$a \in R$ が**可逆元 (invertible element)** もしくは**単元 (単数, unit)** であるとは, ある $a' \in R$ で $a'a = aa' = 1$ を満たすものが存在することである. そのとき a' を a の逆元と呼び, a^{-1} と表わす. a の逆元は存在するとすれば唯一である.

可換環 R の中の可逆元全体の集合を $R^\times$ と表わし, R の**単元群 (単数群, unit group)** と呼ぶことにする.

[474] 以下を証明せよ:

1. 可換環 R に対して $R^\times$ は Abel 群をなす.
2. $\mathbb{Z}^\times = \{\pm 1\}$.
3. 体 K 上の 1 変数多項式環 $K[\lambda]$ の単数群は $K^\times = \{a \in K \mid a \neq 0\}$ に等しい. □

[475] K は体であるとし, 0 でない $f \in K[\lambda]$ を任意に取るとき,

$$\big(K[\lambda]/(f)\big)^\times = \{\, g \bmod f \mid g \in K[\lambda],\ f \text{ と } g \text{ は互いに素} \,\}. \quad \square$$

ヒント: 問題 **[431]** の結果および解説より, f と g の最大公約元を d とすると $(f, g) = (d)$ であるから, 任意の $g \in K[\lambda]$ に対して, $g \bmod f \in K[\lambda]/(f)$ が可逆であるための必要十分条件が $(f, g) = (1)$ であることを示せば良い. $(f, g) = (1)$ であることと, ある $a, b \in K[\lambda]$ で $af + bg = 1$ を満たすものが存在することは同値であり, さらにこの条件はある $b \in K[\lambda]$ で $bg \equiv 1 \mod f$ を満たすものが存在することと同値である. よって $(f, g) = (1)$ であることと $g \bmod f$ が可逆であることは同値である. □

[476] K は体であるとし, $\alpha \in K$, $n \in \mathbb{Z}_{>0}$ であるとする. このとき,

$$\Big(K[\lambda]\big/\big((\lambda - \alpha)^n\big)\Big)^\times = \{\, f \bmod (\lambda - \alpha)^n \mid f \in K[\lambda],\ f(\alpha) \neq 0 \,\}. \quad \square$$

ヒント: 任意の $f \in K[\lambda]$ に対して剰余定理より $f(\alpha) \neq 0$ と f が $\lambda - \alpha$ で割り切れないことは同値である. よって問題 **[475]** の結果を使えば示したい結果が導かれる. □

解説: $f(\alpha) \neq 0$ のとき $f \bmod (\lambda - \alpha)^n$ の逆元の具体的な形は等比級数の和の公式 $1 + a + a^2 + \cdots = (1 - a)^{-1}$ を用いて以下のように計算できる. $a_0 = f(\alpha) \in K^\times$ と置くと, f は $f(\lambda) = a_0\big(1 - (\lambda - \alpha)g(\lambda)\big)$ $(g \in K[\lambda])$ と表わされる. よって形式的に

$$f(\lambda)^{-1} = a_0^{-1}\big(1 + (\lambda - \alpha)g(\lambda) + (\lambda - \alpha)^2 g(\lambda)^2 + (\lambda - \alpha)^3 g(\lambda)^3 + \cdots\big).$$

括弧の中の級数を $n - 1$ 次の巾までで切ることによって得られる多項式を h とする:

$$h(\lambda) = a_0^{-1}\big(1 + (\lambda - \alpha)g(\lambda) + (\lambda - \alpha)^2 g(\lambda)^2 + \cdots + (\lambda - \alpha)^{n-1} g(\lambda)^{n-1}\big).$$

このとき $fh \equiv 1 \mod (\lambda - \alpha)^n$ が成立する:

$$\begin{aligned} f(\lambda)h(\lambda) &\equiv \big(1 - (\lambda - \alpha)g(\lambda)\big)\big(1 + (\lambda - \alpha)g(\lambda) + \cdots + (\lambda - \alpha)^{n-1} g(\lambda)^{n-1}\big) \\ &\equiv 1 + (\lambda - \alpha)g(\lambda) + \cdots + (\lambda - \alpha)^{n-1} g(\lambda)^{n-1} \\ &\quad - (\lambda - \alpha)g(\lambda) - \cdots - (\lambda - \alpha)^{n-1} g(\lambda)^{n-1} - (\lambda - \alpha)^n g(\lambda)^n \\ &\equiv 1. \end{aligned}$$

これはもちろん $\bmod (\lambda - \alpha)^n$ での計算である. □

[**477**] 0 でない整数 $n \in \mathbb{Z}$ を任意に取るとき,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\, m \bmod n \mid m \in \mathbb{Z},\ m \text{ と } n \text{ は互いに素} \,\}.$$

特に素数 p に対して $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ は体をなす. □

ヒント: 前半は問題 [**475**] とまったく同様. 前半より素数 p に対して $m \bmod p$ が可逆であることと m と p が互いに素であることは同値である. その条件は m が p で割り切れないことと同値であり, さらにその条件は $m \not\equiv 0 \mod p$ であることである. よって $\mathbb{Z}/p\mathbb{Z}$ の 0 でない元は可逆になり, $\mathbb{Z}/p\mathbb{Z}$ は体をなす. □

例: たとえば $p = 7$ のとき $2 \cdot 4 \equiv 3 \cdot 5 \equiv 6 \cdot 6 \equiv 1 \mod 7$ である. □

[**478**] **(Euler 函数)** 正の整数 $n \in \mathbb{Z}_{>0}$ に対して, $(\mathbb{Z}/n\mathbb{Z})^\times$ の元の個数を $\varphi(n)$ と書き, **Euler 函数**と呼ぶ. n の素因数分解を $n = p_1^{e_1} \cdots p_r^{e_r}$ と書くと,

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \quad \square$$

ヒント: 問題 [**471**] の結果より $\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{e_i})$ である. 問題 [**477**] の結果より素数 p に対して $(\mathbb{Z}/p^e\mathbb{Z})^\times$ の元の個数は 0 以上 p^e 未満の整数で p で割り切れないもの全体の個数に一致する. 割り切れるものの個数は p^{e-1} なので $\varphi(p^e) = p^e - p^{e-1}$ である. □

可換環 R のイデアル I が**素イデアル (prime ideal)** であるとは $I \neq R$ でかつ任意の $a, b \in R$ に対して $ab \in I$ ならば $a \in I$ または $b \in I$ となることである. この条件の対偶を考えれば, I が素イデアルであることと I の補集合が積に関して閉じていることが同値であることもわかる.

[**479**] **(それで割って整域になるのが素イデアル)** 可換環 R のイデアル $I \neq R$ に対して, I が素イデアルになるための必要十分条件は R/I が整域になることである. □

ヒント: R/I が整域になるための必要十分条件は任意の $a, b \in R$ に対して $(ab) \bmod I = (a \bmod I)(b \bmod I) = 0$ ならば $a \bmod I = 0$ または $b \bmod I = 0$ が成立することである. $a \bmod I = 0$ と $a \in I$ は同値なので, これは任意の $a, b \in R$ に対して $ab \in I$ ならば $a \in I$ または $b \in I$ となることと同値である. □

可換環 R のイデアル I が**極大イデアル (maximal ideal)** であるとは $I \neq R$ でかつ I を含むイデアルが I と R 以外に存在しないことである.

[**480**] **(それで割って体になるのが極大イデアル)** 可換環 R のイデアル $I \neq R$ に対して, I が極大イデアルになるための必要十分条件は R/I が体になることである. □

ヒント: 問題 [**430**] の結果より R/I が体になるための必要十分条件は R/I のイデアルが 0 と R だけになることである. 問題 [**464**] の最後の結果より, その条件は R の I を含むイデアルが I と R だけになることと同値である. □

問題 [**479**], [**480**] による素イデアルと極大イデアルの特徴付けは定義そのものと同じくらい自由に使用される.

[**481**] **(極大ならば素)** 可換環 R の極大イデアルは素イデアルである. □

ヒント: 体は整域であるから, 問題 [**479**], [**480**] の結果を使えばただちに得られる. □

[**482**] 素イデアルだが極大イデアルでない例を一つ挙げよ. □

ヒント: $R=\mathbb{Z}[x]$, $I=\mathbb{Z}[x]x$ と置くと $R/I\cong\mathbb{Z}$. □

[**483**] $\phi : A \to B$ は可換環のあいだの環準同型であるとする. このとき B の素イデアル P に対して $\phi^{-1}(P)$ は A の素イデアルになる. しかし B の極大イデアル $\mathfrak{m}$ に対して $\phi^{-1}(\mathfrak{m})$ は A の極大イデアルになるとは限らない. □

ヒント: 素イデアルの定義より $P\neq B$ である. そのとき $1\notin P$ なので $1\notin\phi^{-1}(P)$ である. よって $\phi^{-1}(P)\neq A$ である. $a,b\in A$ が $ab\in\phi^{-1}(P)$, $a\notin\phi^{-1}(P)$ を満たしているならば, $\phi(a)\phi(b)=\phi(ab)\in P$, $\phi(a)\notin P$ であるから $\phi(b)\in P$ すなわち $b\in\phi^{-1}(P)$ である. これで $\phi^{-1}(P)$ が A の素イデアルであることがわかった.

ϕ は $\mathbb{Z}[x]$ の $\mathbb{Q}[x]$ への包含写像であるとする. $\mathfrak{m}=\mathbb{Q}[x]x$ と置くと $\mathbb{Q}[x]/\mathfrak{m}\cong\mathbb{Q}$ であるから $\mathfrak{m}$ は $\mathbb{Q}[x]$ の極大イデアルである. しかし, $\phi^{-1}(\mathfrak{m})=\mathbb{Z}[x]x$ であり, $\mathbb{Z}[x]/\mathbb{Z}[x]x\cong\mathbb{Z}$ であるから, $\phi^{-1}(\mathfrak{m})$ は $\mathbb{Z}[x]$ の素イデアルであるが極大イデアルではない. □

参考: 任意の可換環 A と**アフィン概型 (affine scheme)** と呼ばれるある種の多様体 (図形) は一対一に対応している.

たとえば体 K 上の 1 変数多項式環 $K[x]$ に対応する多様体は K 上定義された直線であり, 2 変数多項式環 $K[x,y]$ に対応する多様体は K 上定義された平面である. $a,b\in K$ に対して $R=K[x,y]/(y^2-x^3-ax-b)$ に対応する多様体は方程式 $y^2=x^3+ax+b$ で定義された曲線 (K 上定義された楕円曲線) である.

A に対応するアフィン概型は $\operatorname{Spec}A$ と表わされる. 集合として $\operatorname{Spec}A$ は A の素イデアル全体の集合である. たとえば $\operatorname{Spec}\mathbb{Z}=\{(0),(2),(3),(5),(7),(11),\ldots\}$ であるから, $\mathbb{Z}$ に対応する多様体は集合として素数全体の集合に一点 $*=(0)$ を付け加えたものであるとみなせる.

上の問題 [**483**] より, 素イデアル全体の集合が環準同型による引き戻しで閉じているという良い性質を持つことがわかる. どうして素イデアル全体の集合が多様体 (図形) とみなせるかに関してはリード [R] を参照せよ.

可換環論は多様体の局所理論であるという認識抜きで可換環論を勉強すると, 代数的感覚に特別に秀でた人以外は抽象的過ぎて何をやっているかわからなくなってしまう. □

整域 R の元 a が**素元 (prime element)** であるとは $a\neq 0$ でかつ $(a)=Ra$ が R の素イデアルになることであると定める. 素元 a は単元ではない. もしもそうならば $(a)=R$ となり, 素イデアルの定義に反する.

可換環 R の元 a, b に対して, $a\sim b$ であるとはある $u\in R^\times$ で $a=ub$ となるものが存在することであると定める.

整域 R の元 a が**既約元 (irreducible element)** であるとは, a が単元ではなく, 任意の $b,c\in R$ に対して $a=bc$ ならば $b\in R^\times$ または $c\in R^\times$ になることであると定める. 上の記号を用いれば, この条件は $a=bc$ ならば $a\sim b$ または $a\sim c$ となるという条件と同値である. 既約元は 0 にはならない. なぜならば $0=0\cdot 0$ かつ $0\notin R^\times$ であるからである.

体上の多項式環 $K[\lambda]$ の既約元を既約多項式と呼び, $\mathbb{Z}$ の既約元を素数と呼ぶ.

[484] R は整域であるとし, $a, b \in R$ であるとする. このとき $a \sim b$ と $(a) = (b)$ は同値である. □

ヒント: $a \sim b$ と仮定する. ある $u \in R^\times$ で $a = ub$ となるものが存在する. このとき $r \in R$ に対して, $ra \in (a)$ ならば $ra = rub \in (b)$ であり, $rb \in (b)$ ならば $rb = ru^{-1}a \in (a)$ である. よって $(a) = (b)$ である. 逆に $(a) = (b)$ と仮定する. このときある $r, s \in R$ で $a = rb$, $b = sa$ となるものが存在する. このとき $a = rb = rsa$ なので R が整域であることを使うと $1 = rs$ である. よって $r, s \in R^\times$ である. これで $a \sim b$ であることが示された. □

[485] (素元ならば既約元) R は整域であるとする. このとき R の素元は R の既約元である. □

ヒント: a は素元であると仮定し, $b, c \in R$ は $a = bc$ を満たしている仮定する. このとき $bc \in (a)$ なので $c \notin (f)$ と仮定すると $b \in (f)$ である. よってある $d \in R$ が存在して $b = ad$ である. よって $a = adc$ である. R は整域なので $dc = 1$ である. これで $c \in R^\times$ であることがわかった. □

[486] R が単項イデアル整域であるとき, 0 でない $a \in R$ に対して以下の条件は互いに同値である:

(1) (a) は R の極大イデアルである.

(2) (a) は R の素イデアルである.

(3) a は R の素元である.

(4) a は R の既約元である. □

ヒント: 問題 **[481]** の結果より (1) ならば (2) である. 素元の定義より (2) と (3) は同値である. 問題 **[485]** の結果より (3) ならば (4) である. (4) から (1) を導こう. a は既約元であると仮定し, I は R に等しくない (a) を含むイデアルであるとする. R は単項イデアル整域なので, ある $b \in R$ が存在して $I = (b)$ となる. $a \in I = (b)$ よりある $c \in R$ が存在して $bc = a \in (a)$ となる. $(b) = I \neq R$ より $b \notin R^\times$ であり, a は既約元なので $c \in R^\times$ となる. よって $(a) = (bc) = (b) = I$ である. これで (a) が極大イデアルであることがわかった. □

上の問題の結果は体 K 上の一変数多項式環 $K[\lambda]$ や有理整数環 $\mathbb{Z}$ のような単項イデアル整域において空気のごとく自由に使われる.

[487] 0 でない多項式 $f \in K[\lambda]$ に対して, f が既約多項式であることと $K[\lambda]/(f)$ が体になることは同値である. □

ヒント: $K[\lambda]$ は単項イデアル整域であるから問題 **[486]** からただちに得られる. □

参考: この問題の結果は体 K から K を含む別の体を構成するための最も基本的な方法である. 代数学で体の Galois 理論を習うときに用いられる非常に基本的な結果である. □

[488] $\mathbb{R}[\lambda]$ において $\lambda^2 + 1$ は既約多項式である. よって $\mathbb{R}[\lambda]/(\lambda^2 + 1)$ は体になる. この体は複素数体に同型である. □

ヒント: $\mathbb{R}[\lambda]$ の中で λ^2+1 を 0 とみなせば λ は虚数単位 i と同一視できる. □

整域 R が**素元分解整域 (factorial domain)** であるとは次の条件を満たしていることであると定める:

(a) R の 0 でない任意の元は有限個の素元の積で表わされる[147].

整域 R が**一意分解整域 (unique factorization domain, UFD)** であるとは次の 2 つの条件を満たしていることであると定める:

(b) R の 0 でない任意の元は有限個の既約元の積で表わされ, しかもその表示は積の順序と単元倍の違いを除いて一意的である.

(c) R の既約元は R の素元である.

定理 27.1 整域 R が素元分解整域であることと一意分解整域であることは同値である. □

演習問題の羅列によってこの定理を証明しよう.

[489] (素元分解整域における既約元は素元) R が素元分解整域ならば R の既約元は R の素元である. □

ヒント: R は素元分解整域であるとし, $x \in R$ は R の 0 でも単元でも素元でもないと仮定する. このとき x は $x = p_1 \cdots p_r$ (p_i は R の素元でかつ $r \geq 2$) と表わされる. よって x は R の既約元ではない. □

[490] (整域における素元分解の一意性) 整域 R において 0 でない元の素元分解 (有限個の素元の積による表示) は存在するとすれば, 積の順序と単元倍を除いて一意的である. □

ヒント: p_i, q_j は素元であり, $p_1 \cdots p_m = q_1 \cdots q_n$ が成立していると仮定する. このとき $q_1 \cdots q_n \in (p_1)$ であり, (p_1) は素イデアルなのでどれかの q_j は (p_1) に含まれる. 番号を入れ替えて $q_1 \in (p_1)$ としてよい. ある $a_1 \in R$ で $q_1 = a_1 p_1$ となるものが存在する. 素元は定義より単元ではないので $p_1 \notin R^\times$ である. 問題 **[485]** より素元は既約元なので $a \in R^\times$ である. $q_1 = a_1 p_1$ を $p_1 \cdots p_m = q_1 \cdots q_n$ に代入し, R が整域であることを使うと, $p_2 \cdots p_m = a_1 q_2 \cdots q_n$ であることがわかった. 以下同様の論法で番号を入れ替えれば, 結局ある $a_i \in R^\times$ で $q_i = a_i p_i$ $(i = 1, \ldots, m)$ を満たすものが存在して, $1 = a_1 \cdots a_m q_{m+1} \cdots q_n$ となることがわかる. 素元は単元ではないので $m = n$ でなければいけない. □

[491] 問題 **[485]**, **[489]**, **[490]** の結果を用いて定理 27.1 を証明せよ. □

ヒント: R は素元分解整域であると仮定する. 問題 **[485]**, **[490]** の結果より, (b) が導かれる. 問題 **[489]** の結果より, (c) が導かれる. よって素元分解整域ならば一意分解整域である. 逆に R が一意分解整域であると仮定すれば (a) が成立するので, R は素元分解整域である. □

以下では素元分解整域と一意分解整域を区別せずに扱い, 主として一意分解整域という用語を用いる.

[147] 0 個の元の積は単元になると約束しておく.

[**492**] 体 K 上の一変数多項式環 $K[\lambda]$ は一意分解整域である. □

ヒント: $K[\lambda]$ は単項イデアル整域なので素元と既約多項式は一致している. 任意の 0 でない多項式 $f \in K[\lambda]$ が既約多項式の積に分解することを示せば良い. $\deg f$ に関する帰納法で証明する. $\deg f = 1$ のとき f は既約多項式である. $\deg f \geq 2$ とする. f が既約ならばこれ以上示すべきことは何もない. f が既約でないならば次数が 1 以上の多項式 $g, h \in K[\lambda]$ が存在して $f = gh$ となる. このとき $\deg f = \deg g + \deg h$ なので $\deg g, \deg h < \deg f$ である. よって帰納法の仮定より g, h は既約多項式の積に分解される. そのとき $f = gh$ も既約多項式の積に分解している. □

参考: 一般に R が一意分解整域ならば R 上の n 変数多項式環 $R[x_1, \ldots, x_n]$ も一意分解整域になる (Gauss の定理). □

[**493**] $\mathbb{Z}$ は一意分解整域である. □

ヒント: $\mathbb{Z}$ は単項イデアル整域なので素元と既約元すなわち素数は一致している. 0 でない整数 a が素数の積に分解されることを示せば良い. $|a|$ に関する帰納法で証明する. $|a| = 1$ のとき a は単元なので 0 個の素数の積に分解されている. $|a| \geq 2$ とする. a が素数ならばこれ以上示すことは何もない. a が素数でないならば絶対値が 2 以上の整数 b, c が存在して $a = bc$ となる. b, c の絶対値は a より小さいので帰納法の仮定より b, c は素数の積に分解される. そのとき $a = bc$ も素数の積に分解されている. □

参考: 実は任意の単項イデアル整域が一意分解整域であることを証明できる. しかし, そのためには「可換環 R の任意のイデアル I に対して $R \neq I$ ならば I を含む R の極大イデアルが存在する」という結果を用いなければいけない. その証明には Zorn の補題が必要である. 直観的には I が極大でないならばそれにどんどん元を付け加えて行けばいつかは極大イデアルになるはずである. しかし実際には無限に元を付け加えなければいけないかもしれない. そういう場合には「Zorn の補題を使って解決」というのが数学の常套手段になっている. 興味のある方はたとえば堀田 [H1] の 45 頁の定理 9.1(iii) と 47 頁の定理 9.2 を参照して欲しい. □

[**494**] 体 K 上の一変数多項式環 $K[t]$ の t^2, t^3 から生成される部分環を $R = K[t^2, t^3]$ と表わす. R は一意分解整域ではない. □

ヒント: $R = K[t^2, t^3]$ は基底 $1, t^2, t^3, t^4, \ldots$ を持つ. 特に $t \notin R$ である. $R^\times = K^\times$ である. よって t^2 と t^3 は R の既約元であり, $t^2 \not\sim t^3$ である. したがって, $t^6 = (t^2)^3 = (t^3)^2$ は t^6 の 2 つの既約元分解であり, 積の順序の置換や単数倍によって互いに移り合わない. これで R が一意分解整域でないことがわかった. □

参考: $x = t^2$, $y = t^3$ は曲線 $y^2 = x^3$ のパラメーター表示になっている. 曲線 $y^2 = x^3$ のグラフを描くと点 $(x, y) = (0, 0)$ でとがっている. 曲線 $y^2 = x^3$ における $(x, y) = (0, 0)$ のような特異点を**カスプ (cusp)** と呼ぶ[148]. $K[x, y]/(y^2 - x^3) = K[t^2, t^3]$ はカスプを持つ曲線 $y^2 = x^3$ の上の多項式函数のなす環である. それに t を加えて $K[t]$ という特異点のない直線上の函数環を構成する操作は特異点解消 (resolution of singularities) の最も簡単な場合である. 広中平祐 (1931–) は標数が 0 の場合には任意の次元において特異点が常に解消可能であることを証明し, 1970 年に Fields 賞 (Fields medal prize) を受賞している. 広中の特異点解消定理は様々な分野に応用を持つ大定理である. □

[148] cusp は「とがった先端」という意味の名詞である.

[495] ($\mathbb{Z}[\sqrt{-5}]$ は一意分解整域ではない) $\mathbb{Z}$ と $\alpha \in \mathbb{C}$ に対して $\mathbb{Z}$ と α を含む $\mathbb{C}$ の最小の部分環を $\mathbb{Z}[\alpha]$ と書く. このとき以下が成立することを示せ:

1. $\mathbb{Z}[\sqrt{-5}] = \{\, m + n\sqrt{-5} \mid m, n \in \mathbb{Z} \,\}$.
2. $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$.
3. 2, 3, $1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ の既約元である.
4. $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ より $\mathbb{Z}[\sqrt{-5}]$ は一意分解整域ではないことがわかる.
5. 複素平面上に $\mathbb{Z}[\sqrt{-5}]$ とそのイデアル (2), (3), $A = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$, $B = (3, 1 + \sqrt{-5})$, $C = (3, 1 - \sqrt{-5})$ がどのような集合であるかをわかり易く図示せよ.
6. $1 \pm \sqrt{-5}$ は $\bmod 2$ でも $\bmod 3$ でも 0 ではないが, $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ は $\bmod 2$ でも $\bmod 3$ でも 0 になる. このことより 2, 3 は $\mathbb{Z}[\sqrt{-5}]$ の素元でないことがわかる.
7. A, B, C は $\mathbb{Z}[\sqrt{-5}]$ の素イデアルである.
8. $(2) = A^2$, $(3) = BC$ であるから, $(6) = A^2BC$ である. □

ヒント: 1. $\mathbb{Z}[\alpha]$ は $\mathbb{Z}$ と $\sqrt{-5}$ を含み加法と乗法で閉じているので $\mathbb{Z}[\alpha]$ は右辺を含まなければいけない. その右辺は $\mathbb{C}$ の部分環をなすので等号が成立する.

2. $\mathbb{Z}[\sqrt{-5}]$ の絶対値が 1 未満の元は 0 に限る. よって $\mathbb{Z}[\sqrt{-5}]$ の元が単元であるためにはその絶対値が 1 であることが必要である. 複素平面上に $\mathbb{Z}[\sqrt{-5}]$ の図を描いてみれば明らかなようにそのような元は ± 1 しかない. よって $\mathbb{Z}[\sqrt{-5}] = \{\pm 1\}$ である.

3. $\mathbb{Z}[\sqrt{-5}]$ の $0, \pm 1$ 以外の元の絶対値は 2 以上である. よって $\mathbb{Z}[\sqrt{-5}]$ の 0 でも単元でもない 2 個以上の元の積の絶対値は 4 以上になる. このことから 2, 3, $1 \pm \sqrt{-5}$ が $\mathbb{Z}[\sqrt{-5}]$ の既約元であることがわかる.

4. $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ は 6 の既約元の積への二種類の分解であり, $1 \pm \sqrt{-5} \not\sim 2, 3$ である. よって $\mathbb{Z}[\sqrt{-5}]$ は一意分解整域ではない.

5. $A = \mathbb{Z}2 + \mathbb{Z}(1 + \sqrt{-5}) = \mathbb{Z}2 + \mathbb{Z}(1 - \sqrt{-5})$, $B = \mathbb{Z}3 + \mathbb{Z}(1 + \sqrt{-5})$, $C = \mathbb{Z}3 + \mathbb{Z}(1 - \sqrt{-5}) = \mathbb{Z}3 + \mathbb{Z}(1 + 2\sqrt{-5})$.

7. $\mathbb{Z}[\sqrt{-5}]/A \cong \mathbb{F}_2$, $\mathbb{Z}[\sqrt{-5}]/B \cong \mathbb{Z}[\sqrt{-5}]/C \cong \mathbb{F}_3$.

8. $2 = -2 \cdot 2 + (1 + \sqrt{-5})(1 - \sqrt{-5}) \in A^2$ であるから $(2) \subset A^2$ である. 逆に $(1 + \sqrt{-5})^2 = -4 + 2\sqrt{-5} \in (2)$ であるから $A^2 \subset (2)$ であることもわかる. よって $(2) = A^2$ である. 同様にして $(3) = BC$ も確かめられる. □

参考: 上の問題の結果は E. Kummner (1810–1893) による理想数 (ideal number) としてのイデアルのアイデアを説明するためによく使われる. たとえば高木 [Tkg2] 第 5 章第 41 節 273–274 頁を見よ. $\mathbb{Z}[\sqrt{-5}]$ では数の既約元の積への分解の一意性も成立していないし, 数の素元の積への分解も存在するとは限らない. しかし, イデアルの素イデアルの積への一意分解可能性は成立している. 数の世界では成立していない素因数分解の一意存在がイデアル (理想数) の世界では成立しているのである. この事実を抽象化することによって **Dedekind 整域 (Dedekind domain)** の理論が構築され, 代数的整数論の基礎になっている. □

27.6 行列の基本変形

R は可換環であるとする.

[496] $A \in M_n(R)$ の逆行列が $M_n(R)$ の中に存在するための必要十分条件は $\det A \in R^\times$ が成立することである. □

ヒント: ある $B \in M_n(R)$ で $AB = BA = E$ となるものが存在するならば $\det A \det B = 1$ なので $\det A \in R^\times$ である. A の (i,j) 余因子を (i,j) 成分に持つ行列を Δ と書くと ${}^t\Delta A = A\,{}^t\Delta = (\det A)E$ なので, $\det A \in R^\times$ ならば $(\det A)^{-1}\,{}^t\Delta$ は A の逆行列である. □

群 $GL_n(R)$, $SL_n(R)$ を次のように定義する:

$$GL_n(R) = \{\, A \in M_n(R) \mid \det A \in R^\times \,\}, \quad SL_n(R) = \{\, A \in M_n(R) \mid \det A = 1 \,\}.$$

たとえば $GL_n(\mathbb{Z})$ は整数を成分に持つ n 次正方行列で行列式が ± 1 になるもの全体の集合である. $SL_n(R)$ は $GL_n(R)$ の部分群をなす.

[497] $A = [a_{ij}] \in GL_n(R)$ ならば $(a_{1j}, \ldots, a_{nj}) = (1) = R \quad (j = 1, \ldots, n)$. □

ヒント: A の (i,j) 余因子を $\tilde{a}_{ij}$ と書くと $\sum_i \tilde{a}_{ij} a_{ij} = |A| \in R^\times$. □

(i,j) 成分だけが 1 で他の成分が 0 であるような n 次正方行列を E_{ij} と書き, n 次の単位行列を E と書くことにする. n を陽に示したい場合は $E_{n;ij}$, E_n と書くことにする.

任意の $a \in R$ と $b \in R^\times$ に対して**基本行列 (elementary matrices)** $U_{ij}(a) \in SL_n(R)$, $D_i(b) \in GL_n(R)$ を次のように定める[149]:

$$U_{ij}(a) = E + aE_{ij} \qquad (i \neq j),$$
$$D_i(b) = E_{11} + \cdots + E_{i-1,i-1} + bE_{ii} + E_{i+1,i+1} + \cdots + E_{nn}.$$

$U_{ij}(a)$ の方は任意の $a \in R$ に対して定義されているが, $i \neq j$ の場合だけに定義されている. $D_i(b)$ の方は単数 $b \in R^\times$ のみに対して定義されている. n を陽に示したい場合には $U_{n;ij}(a)$, $D_{n;i}(b)$ と書くことにする.

U_{ij} は対角成分がすべて 1 の三角行列なので $\det U_{ij}(a) = 1$ である. $D_i(b)$ は対角行列であり, i 番目の対角成分だけが b で他の対角成分が 1 であるような行列なので $\det D_i(b) = b \in R^\times$ である.

[498] $n = 3$ の場合に 6 種類の $U_{ij}(a)$ と 3 種類の $D_i(b)$ を書き下してみよ. そして, $n = 3$ の場合に $U_{ij}(a)^{-1} = U_{ij}(-a)$ および $D_i(b)^{-1} = D_i(b^{-1})$ を証明せよ. □

[499] 一般の n で $U_{ij}(a)^{-1} = U_{ij}(-a)$, $D_i(b)^{-1} = D_i(b^{-1})$ が成立している. □

[500] $i \neq j$ のとき $e^{aE_{ij}} = U_{ij}(a)$ である. □

上の 2 問のヒント: $E_{ij}E_{kl} = \delta_{jk}E_{il}$ である. 特に $i \neq j$ のとき $E_{ij}E_{ij} = 0$. □

[149] $U_{ij}(a)$ の U は unipotent matrix (巾単行列) の頭文字であり, $D_i(b)$ の D は diagonal matrix (対角行列) の頭文字である.

[501] $i \neq 0$, $b \in R^\times$ のとき $D_i(b)U_{ij}(a) = U_{ij}(ba)D_i(b)$, $U_{ij}(a)D_j(b) = D_j(b)U_{ij}(a)$ であり, $k \neq i, j$ ならば $D_k(b)U_{ij}(a) = U_{ij}D_k(b)$ である. □

ヒント: $D_i(b)U_{ij}(a) = U_{ij}(ba)D_i(b)$ は i, j に関係した部分だけを抜き出せば次のように証明される:

$$\begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} b & ba \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & ba \\ 0 & 1 \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix}. \quad \square$$

$n = 3$, $(i, j, k) = (1, 2, 3)$, $x = {}^t[x_i, x_j, x_k]$, $y = [y_i, y_j, y_k]$ に対して,

$$U_{ij}(a)x = \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_i \\ x_j \\ x_k \end{bmatrix} = \begin{bmatrix} x_i + ax_j \\ x_j \\ x_k \end{bmatrix},$$

$$D_i(b)x = \begin{bmatrix} b & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_i \\ x_j \\ x_k \end{bmatrix} = \begin{bmatrix} bx_i \\ x_j \\ x_k \end{bmatrix},$$

$$yU_{ij}(a) = \begin{bmatrix} y_i & y_j & y_k \end{bmatrix} \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} y_i & ay_i + y_j & y_k \end{bmatrix},$$

$$yD_i(b) = \begin{bmatrix} y_i & y_j & y_k \end{bmatrix} \begin{bmatrix} b & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} by_i & y_j & y_k \end{bmatrix}.$$

これより, 以下が成立することがわかる:

- $U_{m;ij}(a)$ を (m, n) 型行列 A に左からかける操作は A の第 i 行に第 j 行の a 倍を加えるという操作に等しい.
- $D_{m;i}(b)$ を (m, n) 型行列 A に左からかける操作は A の第 i 行を b 倍するという操作に等しい.
- $U_{n;ij}(a)$ を (m, n) 型行列 A に右からかける操作は A の第 i 列の a 倍を第 j 列に加えるという操作に等しい.
- $D_{n;i}(b)$ を (m, n) 型行列 A に右からかける操作は A の第 i 列を b 倍するという操作に等しい.

これらの操作を行列の**基本操作 (elementary operation)** と呼び, 基本操作を任意有限回繰り返すことによって得られる行列の変形を行列の**基本変形 (elementary transformation)** と呼ぶことにする[150].

[502] 行列の基本変形は行の任意置換と列の任意置換を含んでいる. □

[150]堀田 [H1], [H2] では基本操作を**基本変形 (fundamental transformation)** と呼び, 基本変形を**初等変形 (elementary transformation)** と呼んでいる.

ヒント: $D_j(-1)U_{ij}(1)U_{ji}(-1)U_{ij}(1)$ の左からのかけ算は第 i 行と第 j 行を交換することが以下のように確かめられる:

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}x_i\\ x_j\end{bmatrix}=\begin{bmatrix}x_i+x_j\\ x_j\end{bmatrix},\quad \begin{bmatrix}1 & 0\\ -1 & 1\end{bmatrix}\begin{bmatrix}x_i+x_j\\ x_j\end{bmatrix}=\begin{bmatrix}x_i+x_j\\ -x_i\end{bmatrix},$$
$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}x_i+x_j\\ -x_i\end{bmatrix}=\begin{bmatrix}x_j\\ -x_i\end{bmatrix},\quad \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}x_j\\ -x_i\end{bmatrix}=\begin{bmatrix}x_j\\ x_i\end{bmatrix}.$$

これより $P_{ij}=D_j(-1)U_{ij}(1)U_{ji}(-1)U_{ij}(1)$ が

$$P_{ij}=E_{ij}+E_{ji}+\sum_{k\neq i,j}E_{kk}$$

という形であることが確かめられるので, P_{ij} の右からのかけ算が第 i 列と第 j 行を交換することもわかる[151]. □

注意: 上の P_{ij} をも基本行列とみなし, 行列の基本操作に行の置換と列の置換を始めから含めておく流儀もある. 上の問題によってどちらでも同じことなので本質的な違いはない. ただし, 上で定義した行列の基本操作は体上の一変数多項式環 $K[\lambda]$ や有理整数環 $\mathbb{Z}$ のような Euclid 整域の元を成分に持つ行列の基本操作である. 一般の単項イデアル整域を扱う場合には次の行列 $X_{ij}(a,b,c,d)$ の左と右からの積が定める操作も行列の基本操作の中に含めておかなければいけない[152]:

$$X_{ij}(a,b,c,d)=aE_{ii}+bE_{ij}+cE_{ji}+dE_{jj}+\sum_{k\neq i,j}E_{kk}\quad (ad-bc\in R^\times,\ i\neq j).$$

このとき $X_{ij}(1,a,0,1)=U_{ij}(a)$, $X_{ij}(b,0,0,1)=D_i(b)$, $X_{ij}(0,1,1,0)=P_{ij}$ ある. □

[503] (Euclid の互除法再論) R が体 K 上の一変数多項式環 $K[\lambda]$ であるとき, 行列の基本変形によって $K[\lambda]$ の元を成分に持つ縦ベクトルと横ベクトルに関して Euclid の互除法を実行できる. すなわち, $f_1,\dots,f_n\in K[\lambda]$ の最大公約元を g とすると, 有限個の基本行列の積で表示できる行列 $A,B\in GL_n(K[\lambda])$ で $A\,{}^t[f_1,\dots,f_n]={}^t[g,0,\dots,0]$, $[f_1,\dots,f_n]B=[g,0,\dots,0]$ を満たすものが存在する. □

ヒント: A の存在が証明されれば B は $B={}^tA$ として得られるので A の存在だけを証明すれば良い. ベクトル ${}^t[f_1,\cdots,f_n]$ に基本変形を以下のような手続きをほどこす:

1. $f_1=\cdots=f_n=0$ ならば手続きを終了する.
2. 成分の置換によって 0 でない成分の中で次数が最小のものを f_1 に持って来る.
3. $f_2,\dots,f_n$ から f_1 の多項式倍を引き去ることによって $f_2,\dots,f_n$ をそれぞれを f_1 で割った余りに変換できる.
4. もしも $f_2=\cdots=f_n=0$ ならばこの手続きを終了し, そうでないならばステップ 2 に戻る.

[151] P_{ij} の P は permutation (置換) の頭文字である. P_{ij} は transposition (互換) の操作に対応した行列なので T_{ij} と書くという考え方もあるが, 置換 $\sigma\in S_n$ に対応する置換行列を $P_\sigma=\sum_{i=1}^n E_{\sigma(i)i}$ と書いた場合に記号の統一が取れるようにするためには P にした方が良い.

[152] たとえば堀田 [H1] 67 頁を参照せよ. そこでは $X_{ij}(a,b,c,d)$ は $E_{ij}(\alpha,\beta,\gamma,\delta)$ と書かれている.

この手続きによって $f_2,\dots,f_n$ の次数の最大値は単調に減少するので有限回でこの手続きは終了し, 最終的に ${}^t[g,0,\dots,0]$ の形のベクトルが得られる. しかもどのステップでも $f_1,\dots,f_n$ の最大公約元が保たれることが確かめられるので[153], g は $f_1,\dots,f_n$ の最大公約元である[154]. □

[504] 体 K 上の一変数多項式環 $K[\lambda]$ に関して以下が成立する:

1. $GL_n(K[\lambda])$ の任意の元は有限個の基本行列の積で表わされる.

2. $SL_n(K[\lambda])$ の任意の元は $U_{ij}(a)$ の型の有限個の基本行列の積で表わされる. □

ヒント: 1. n に関する帰納法で $A\in GL_n(K[\lambda])$ が行列の基本変形で単位行列に変形できることを示せばよい. 問題 **[497]** の結果と問題 **[503]** の結果より, 行列の行に関する基本変形によって A の第 1 列に Euclid の互除法を適用して A を $\begin{bmatrix}1 & *\\ 0 & A'\end{bmatrix}$ の形に変形できる. ここで $A'\in GL_{n-1}(K[\lambda])$ は $n-1$ 次の正方行列である. さらに行列の列に関する基本変形によって, これを $\begin{bmatrix}1 & 0\\ 0 & A'\end{bmatrix}$ の形に変形できる. よって A' に帰納法の仮定を適用すれば任意の $A\in GL_n(K[\lambda])$ が行列の基本変形によって単位行列に変形できることがわかる.

2. 上の 1 の結果より, 任意の $A\in SL_n(K[\lambda])$ は基本行列の積で表わされる. 問題 **[501]** の結果より, 基本行列の積は $U_{ij}(a)$, $D_k(b)$ の順序を並び換えて

$$D_{k_1}(b_1)\cdots D_{k_r}(b_r)U_{i_1j_1}(a_1)\cdots U_{i_sj_s}(a_s),\qquad b_i\in K^\times$$

と表わされる. このとき $1=\det A=b_1\cdots b_r$ である. 問題 **[502]** のヒントの議論を参考にすれば, $i\neq j$, $b\in K[\lambda]^\times$ に対して $S_{ij}(b)=U_{ij}(b)U_{ji}(-b^{-1})U_{ij}(b)$ と置くと,

$$S_{ij}(b)=bE_{ij}-b^{-1}E_{ji}+\sum_{k\neq i,j}E_{kk}$$

であることがわかる[155]. よって $S_{ij}(-1)S_{ij}(b)=D_i(b^{-1})D_j(b)$ である[156]. したがって

$$\prod_{k_i\neq 1}[S_{k_i1}(-1)S_{k_i1}(b_i)]\cdot D_{k_1}(b_1)\cdots D_{k_r}(b_r)=D_1(b_1\cdots b_r)=D_1(1)=E.$$

よって $D_{k_1}(b_1)\cdots D_{k_r}(b_r)$ の部分も $U_{ij}(a)$ の形の基本行列の積で表わされることがわかった. □

---

[153] $f_i=q_if_1+r_i$ $(i=1,\dots,n)$ ならば $f_1,r_2,\dots,r_n$ の公約元は $f_1,f_2,\dots,f_n$ の公約元である. $r_i=f_i-p_1f_1$ $(i=1,\dots,n)$ なので逆に $f_1,f_2,\dots,f_n$ の公約元は $f_1,r_2,\dots,r_n$ の公約元である. よって $f_1,r_2,\dots,r_n$ と $f_1,f_2,\dots,f_n$ の公約元の集合は一致するので, 特に最大公約元も一致する.

[154] g と 0 の最大公約元は g であることが次のようにして示される. g と 0 は g で割り切れる ($g=1\cdot g$, $0=0\cdot g$). 0 はいつでも割り切れるので, 0 と g の公約元は g の約元に等しい. よって 0 と g の任意の公約元は g を割り切る.

[155] i,j に関係ある部分だけを抜き出すと,

$$S_{ij}(b)=\begin{bmatrix}1 & b\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ -b^{-1} & 1\end{bmatrix}\begin{bmatrix}1 & b\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & b\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & b\\ -b^{-1} & 0\end{bmatrix}=\begin{bmatrix}0 & b\\ -b^{-1} & 0\end{bmatrix}.$$

[156] i,j に関係する部分だけを抜き出すと,

$$S_{ij}(-1)S_{ij}(b)=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & b\\ -b^{-1} & 0\end{bmatrix}=\begin{bmatrix}b^{-1} & 0\\ 0 & b\end{bmatrix}.$$

[505] (Euclid の互除法再論) $R=\mathbb{Z}$ であるとき, 行列の基本変形によって整数を成分に持つ縦ベクトルと横ベクトルに関して Euclid の互除法を実行できる. すなわち, $a_1,\dots,a_n\in K[\lambda]$ の最大公約元を b とすると, 有限個の基本行列の積で表示できる行列 $A,B\in GL_n(\mathbb{Z})$ で $A\,{}^t[a_1,\dots,a_n]={}^t[b,0,\dots,0]$, $[a_1,\dots,a_n]B=[b,0,\dots,0]$ を満たすものが存在する. □

ヒント: 問題 **[503]** とまったく同様. □

[506] $\mathbb{Z}$ に関して以下が成立する:

1. $GL_n(\mathbb{Z})$ の任意の元は有限個の基本行列の積で表わされる.
2. $SL_n(\mathbb{Z})$ の任意の元は $U_{ij}(a)$ の型の有限個の基本行列の積で表わされる. □

ヒント: 問題 **[504]** とまったく同様.

解説: 問題 **[504]**, **[506]** の結果より, $R=K[\lambda],\mathbb{Z}$ の場合の (m,n) 型行列 A の基本変形は $P\in GL_m(R)$ と $Q\in GL_n(R)$ を左と右からかける操作 $A\mapsto PAQ$ に等しいことがわかる. □

例 27.2 $R=\mathbb{Q}[x]$ とする. $v\in R^3$ を $v={}^t[x^2-1,x^2+x-2,x^2+2x-3]$ と定める. $P\in GL_3(R)$ で $Pv={}^t[x-1,0,0]$ となるものを一つ求めよう. 基本変形による Euclid の互除法を v に適用すると,

$$\begin{bmatrix}x^2-1\\x^2+x-2\\x^2+2x-3\end{bmatrix}\to\begin{bmatrix}x^2-1\\x-1\\2x-2\end{bmatrix}\to\begin{bmatrix}0\\x-1\\0\end{bmatrix}\to\begin{bmatrix}x-1\\0\\0\end{bmatrix}.$$

1 番目の矢印は第 1 成分を第 2 および第 3 成分から引く操作であり, 2 番目の矢印は第 2 成分に $x+1$ をかけて第 1 成分から引き, 第 2 成分の 2 倍を第 3 成分から引く操作であり, 3 番目の矢印は第 1 成分と第 2 成分を交換する操作である. この基本変形に対応する行列 P は次のようになる:

$$P=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&-(x+1)&0\\0&1&0\\0&-2&1\end{bmatrix}\begin{bmatrix}1&0&0\\-1&1&0\\-1&0&1\end{bmatrix}=\begin{bmatrix}-1&1&0\\x+2&-(x+1)&0\\1&-2&1\end{bmatrix}.$$

このとき,

$$P^{-1}=\begin{bmatrix}x+1&1&0\\x+2&1&0\\x+3&1&1\end{bmatrix}.$$

P^{-1} の第 1 列がこの形にならなければいけないことは $v=P^{-1}\,{}^t[x-1,0,0]$ と $v={}^t[(x+1)(x-1),(x+2)(x-1),(x+3)(x-1)]$ よりわかる. 残りの 2 列をうまく選んで $\det P^{-1}=1$ となるようにできれば構成したい P が得られる. □

[507] $R=\mathbb{Q}[x]$ であるとし, $v\in R^3$ を

$$v={}^t[x^3+2x^2-x-2,x^3+4x^2+x-6,x^3+3x^2-x-3]$$

と定める. $P\in GL_3(R)$ で $Pv={}^t[x-1,0,0]$ となるものを一つ求め, P^{-1} を計算せよ. □

略解: たとえば P を次のように取れば良い:

$$P = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ -(x+3) & -(x+1) & 2(x+2) \\ -\frac{1}{2}x(x+3) & -\frac{1}{2}(x+1)(x+2) & (x+1)(x+2) \end{bmatrix},\ P^{-1} = \begin{bmatrix} (x+1)(x+2) & 0 & 1 \\ (x+2)(x+3) & 1 & 1 \\ (x+1)(x+3) & \frac{1}{2} & 1 \end{bmatrix}.$$

P^{-1} の第 1 列がこの形になることは v の成分を因数分解すれば確かめられる. $\det P^{-1} = 1$ であることも容易に確かめられる. □

[508] $R = \mathbb{Q}[x]$ であるとし, $v_1, v_2 \in R^4$ を

$$v_1 = \begin{bmatrix} x^4 + 2\,x^3 - 2\,x - 1 \\ x^3 - 3\,x - 2 \\ x^4 + 3\,x^3 + 4\,x^2 + 3\,x + 1 \\ x^3 - 2\,x^2 - 7\,x - 4 \end{bmatrix}, \quad v_2 = \begin{bmatrix} x^3 + 3\,x^2 + 2\,x \\ x^3 + 4\,x^2 + 5\,x + 2 \\ x^3 + 5\,x^2 + 8\,x + 4 \\ x^3 - 2\,x^2 - 7\,x - 4 \end{bmatrix}$$

と定める. $P_i \in GL_4(R)$ で $P_i v_i$ が ${}^t[*, 0, 0, 0]$ の形になるものを一つ求め, P_i^{-1} を計算せよ. □

略解: v_1, v_2 の成分は次のように因数分解される:

$$v_1 = \begin{bmatrix} (x+1)^3\,(x-1) \\ (x+1)^2\,(x-2) \\ (x+1)^2\,(x^2+x+1) \\ (x+1)^2\,(x-4) \end{bmatrix}, \quad v_2 = \begin{bmatrix} x\,(x+2)\,(x+1) \\ (x+1)^2\,(x+2) \\ (x+1)\,(x+2)^2 \\ (x+1)^2\,(x-4) \end{bmatrix}.$$

P_1, P_2 としてたとえば以下が取れる:

$$P_1 = \begin{bmatrix} \frac{1}{3} & -\frac{1}{3}\,x - \frac{2}{3} & 0 & 0 \\ x - 2 & -(x-1)\,(x+1) & 0 & 0 \\ -\frac{1}{3}\,x^2 - \frac{1}{3}\,x - \frac{1}{3} & \frac{1}{3}\,(x^2+x+1)\,(x+2) & 1 & 0 \\ -\frac{1}{3}\,x + \frac{4}{3} & \frac{1}{3}\,(x-4)\,(x+2) & 0 & 1 \end{bmatrix},$$

$$P_2 = \begin{bmatrix} \frac{1}{6}\,x - \frac{5}{6} & -\frac{1}{6}\,x + \frac{5}{6} & 0 & \frac{1}{6} \\ -x - 1 & x & 0 & 0 \\ x + 2 & -x - 2 & 1 & 0 \\ (x+1)\,(x-4) & -(x+1)\,(x-4) & 0 & x+2 \end{bmatrix}.$$

このとき

$$P_1 v_1 = \begin{bmatrix} (x+1)^2 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad P_2 v_2 = \begin{bmatrix} x+1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

でかつ

$$P_1^{-1} = \begin{bmatrix} (x-1)\,(x+1) & -\frac{1}{3}\,x - \frac{2}{3} & 0 & 0 \\ x - 2 & \frac{-1}{3} & 0 & 0 \\ x^2 + x + 1 & 0 & 1 & 0 \\ x - 4 & 0 & 0 & 1 \end{bmatrix},$$

$$P_2^{-1} = \begin{bmatrix} (x+2)\,x & -1 & 0 & -\frac{1}{6}x \\ (x+2)(x+1) & -1 & 0 & -\frac{1}{6}x - \frac{1}{6} \\ (x+2)^2 & 0 & 1 & -\frac{1}{6}x - \frac{1}{3} \\ (x+1)(x-4) & 0 & 0 & -\frac{1}{6}x + \frac{5}{6} \end{bmatrix}. \quad \square$$

[509] K は体であり, $R = K[x, y]$ であるとする. $v = {}^t[x, y] \in R^2 = M_{2,1}(R)$ とすると, どのような $P \in GL_2(R)$ を取っても Pv は $f(x, y)e_1 = {}^t[f(x, y), 0]$ $(f \in R)$ の形にならない. $\square$

ヒント: P の逆行列を $P^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $(a, b, c, d \in R)$ と書けば $Pv = \begin{bmatrix} f \\ 0 \end{bmatrix}$ となるとき, $\begin{bmatrix} x \\ y \end{bmatrix} = v = P^{-1}Pv = \begin{bmatrix} af \\ cf \end{bmatrix}$ である. f は x, y の共通因子なので $\alpha := f \in K^\times$ である. よって $a = \alpha^{-1}x$, $b = \alpha^{-1}y$ である. $P^{-1} \in GL_2(R)$ であるから $ad - bc \in R^\times = K^\times$ である. よって $ad-bc$ の中の x, y に 0 を代入すると 0 にならない. しかし $ad-bc = \alpha^{-1}(xd-yc)$ であるから x, y に 0 を代入すると 0 になる. よって矛盾する. $\square$

27.7 単因子と行列式因子

定理 27.3 (単因子) R は体 K 上の一変数多項式環 $K[\lambda]$ または $\mathbb{Z}$ であるとし[157], R の元を成分に持つ (m, n) 型行列 $A \in M_{m,n}(R)$ 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 $e_1, \ldots, e_s$ は単元倍を除いて一意に定まる. $e_1, \ldots, e_s$ を行列 A の**単因子 (elementary divisors)** と呼ぶ[158]. $\square$

以下において K は体であるとし, R が K 上の一変数多項式環 $K[\lambda]$ の場合と有理整数環 $\mathbb{Z}$ の場合を扱う.

[510] $R = K[\lambda]$ の場合に定理 27.3 の条件を満たす基本変形の存在を証明せよ. $\square$

[157] もちろん R は一般の Euclid 整域でも成立する. 基本変形を適切に拡張しておけば任意の単項イデアル整域でも成立する. たとえば堀田 [H1] の第 12 節を参照せよ.

[158] 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.

ヒント 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 R 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 でない次数が最小の元を 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 行の第 $(1,1)$ 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 の多項式倍を引き去ることによって e_1 よりも次数が低い 0 でない元を構成できるので, e_1 の次数の最小性に反する. したがって $a_{11} = e_1$ でそれ以外の第 1 列と第 1 行の成分は割り切れる. そのことから行列の基本変形によって, $a_{11} = e_1$ はそのままにそれ以外の第 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 の次数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: 上のヒント 1 の証明は単因子を計算するためのアルゴリズムを与えない. しかし下のヒント 2 はアルゴリズムを与える.

ヒント 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 でない次数が最小の成分を第 $(1,1)$ 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) $a_{21}, \ldots, a_{m1}$ のすべてが a_{11} で割り切れるならば第 1 行の多項式倍を第 $2, \ldots, m$ 行に加えて第 $(2,1), \ldots, (m,1)$ 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) $a_{21}, \ldots, a_{m1}$ 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 (問題 [**503**] のヒントを見よ):
   $$\begin{bmatrix} a & b \\ 0 & B \end{bmatrix}, \qquad 0 \neq a \in R, \quad b \in M_{1,n-1}(R), \quad B \in M_{m-1,n-1}(R).$$
   ここで a は A の第 1 列の最大公約元であり, $\deg a < \deg a_{11}$ 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) $a_{12}, \ldots, a_{1n}$ のすべてが a_{11} で割り切れるならば第 1 列の多項式倍を第 $2, \ldots, m$ 列に加えて第 $(1,2), \ldots, (1,n)$ 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) $a_{12}, \ldots, a_{1n}$ 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 (問題 [**503**] のヒント

を見よ):

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

ここで a は A の第 1 行の最大公約元であり, $\deg a < \deg a_{11}$ 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:

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

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 行の他の成分のすべてが割り切れないならば $\deg a_{11}$ の次数がより小さくなるからである. そして両方がすべて割り切れるならば A は (♯) の形に変形されてしまう.

4. この時点で A は (♯) 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 $\deg a_{11}$ がより小さくなるからである. □

[511] $R = \mathbb{Z}$ の場合に定理 27.3 の条件を満たす基本変形の存在を証明せよ. □

ヒント: 問題 **[510]** とまったく同様. □

$R = K[\lambda], \mathbb{Z}$ のとき, (m,n) 型行列 $A \in M_{m,n}(R)$ に対して A のすべての i 次小行列式[159]の最大公約元を $d_i(A)$ と書き, A の**行列式因子 (determinaltal divisor)** と呼ぶ[160].

[512] (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 (単元倍を除いて) 不変である. □

ヒント: A に基本操作をほどこした行列を B とする. 基本操作の逆もまた基本操作なので $d_i(A)$ と $d_i(B)$ が単元倍を除いて等しいことを示すためには, $d_i(B)$ が $d_i(A)$ で割り切れることを示せば良い. 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良い. $B = D_{m;k}(b)A$ と $B = AD_{n,k}(b)$ の場合は B の i 次の小行列式は A の i 次の小行列式に等しいか b 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. $B = U_{m;k,l}(a)A$ と $B = AU_{n;k,l}$ の場合は B の i 次の小行列式は A の i 次の小行列式の倍元の和の形になるので $d_i(A)$ で割り切れる. □

[159] (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.

[160] 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 [H1] では単因子は d_i と表わされ, 行列式因子を Δ_i と表わされているので混乱しないように注意せよ.

[513] (単因子と行列式因子の関係) $A \in M_{m,n}(R)$ の単因子を $e_1, \ldots, e_s$ と書き, 行列式因子を $d_1, \ldots, d_k$ と書くとき, 必要ならば単元倍を調整することによって次が成立する:

$$d_1 = e_1,\ d_2 = e_1e_2,\ \ldots,\ d_s = e_1e_2\cdots e_s, \qquad d_i = 0 \quad (i > s).$$

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

$$e_1 = d_1,\ e_2 = d_2/d_1,\ \ldots,\ e_s = d_s/d_{s-1}. \quad \square$$

注意: この問題を解けば定理 27.3 の証明が終了することになる. $\square$

ヒント: A を基本変形することによって次の形の行列が得られたとする:

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

問題 **[513]** の結果より, 単元倍を調節すれば $d_i(A) = d_i(B)$ である. しかし, $d_i(B)$ は容易に計算できる: $d_1(B) = e_1$, $d_2(B) = e_1e_2$, ..., $d_r(B) = e_1e_2\cdots e_s$, $d_i(B) = 0$ $(i > s)$. $\square$

27.8 有限生成加群

可換環 R 上の加群 M が R **上有限生成 (finitely generated over R)** であるとはある $u_1, \ldots, u_n \in R$ で

$$M = Ru_1 + \cdots + Ru_n$$

を満たすものが存在することである. このとき任意の $u \in M$ は

$$u = a_1u_1 + \cdots + a_nu_n, \qquad a_1, \ldots, a_n \in R$$

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しなければいけない.

[514] R が単項イデアル整域であるとき, M が R 上高々 n 個の元から生成される有限生成 R 加群であるならば, その任意の R 部分加群も R 上高々 n 個の元から生成される[161]. $\square$

ヒント: n に関する帰納法で証明する.

$n = 1$ のとき, $M = Ru_1$ であるとし, 全射 R 準同型 $\phi : R \to M$ を $\phi(a) = au_1$ と定める. N が M の R 部分加群ならば $\phi^{-1}(N)$ は R の R 部分加群すなわちイデアルである. R は単項イデアル整域なのである $v \in R$ で $\phi^{-1}(N) = Rv$ を満たすものが存在する. このとき $N = \phi(\phi^{-1}(N)) = \phi(Rv) = R\phi(v)$ である.

[161] これは, 単項イデアル整域上の有限生成加群に対して, ベクトル空間の場合に成立している「部分空間の次元は小さくなる」という結果に近い結果が成立していることを意味している.

$n \geq 2$ であるとし, $n-1$ まで問題の結論が成立していると仮定する. $M = Ru_1 + \cdots + Ru_n$ であるとし, N はその任意の R 部分加群であるとする. $n = 1$ の場合を Ru_1 の R 部分加群 $N \cap Ru_1$ に適用すると, ある $v_1 \in N \cap Ru_1$ で $N \cap Ru_1 = Rv_1$ を満たすものが存在する. $M' = M/Ru_1$ と置き, M から M' への自然な全射 R 準同型を π と書くことにする. このとき $M' = R\pi(u_2) + \cdots + R\pi(u_n)$ である. よって帰納法の仮定より, ある $v_2, \ldots, v_n \in N$ で $\pi(N) = R\pi(v_2) + \cdots + R\pi(v_n)$ を満たすものが存在する. よって任意の $v \in N$ に対してある $a_2, \ldots, a_n \in R$ で $\pi(v) = a_2\pi(v_2) + \cdots + a_n\pi(v_n)$ となるものが存在する. そのとき, $v - (a_2v_2 + \cdots + a_nv_n) \in \operatorname{Ker} \pi|_N = N \cap Ru_1$ である. よってある $a_1 \in R$ で $v - (a_2v_2 + \cdots + a_nv_n) = a_1v_1$ となるものが存在する. これで $N = Rv_1 + \cdots + Rv_n$ であることが証明された. □

[515] (有限生成自由加群) 可換環 R 上の加群 M に対して以下の条件は互いに同値である:

(a) M は R^n と R 加群として同型である.

(b) ある $u_1, \ldots, u_n \in M$ が存在して, 任意の $u \in M$ は

$$u = a_1u_1 + \cdots + a_nu_n, \qquad a_1, \ldots, a_n \in R$$

と一意に表わされる.

これらの同値な条件が成立しているとき, M は**階数 n の有限生成自由 R 加群 (finitely generated free R-module of rank n)** と呼ばれ, (b) の $u_1, \ldots, u_n$ は M の**自由 R 基底 (free R-basis)** と呼ばれる[162]. □

ヒント: R 同型 $\phi : R^n \xrightarrow{\sim} M$ が存在するとき, $\phi(e_1), \ldots, \phi(e_n)$ は M の自由 R 基底になる[163]. $u_1, \ldots, u_n$ が M の自由 R 基底であるとき, $\phi : R^n \to M$ を $\phi({}^t[a_1, \ldots, a_n]) = a_1u_1 + \cdots + a_nu_n$ と定めると ϕ は R 同型である. □

[516] (階数の一意性) 簡単のため R は $K[\lambda]$ または $\mathbb{Z}$ であるとする[164]. M は有限生成自由 R 加群であるとする. そのとき M の階数は自由 R 基底の取り方に寄らず一定である. □

ヒント: $R = K[\lambda]$ ならば $F = K(\lambda)$ (K 上の一変数有理函数体[165]) であるとし, $R = \mathbb{Z}$ ならば $F = \mathbb{Q}$ であるとする. このとき R は体 F の部分環である. $u_1, \ldots, u_m$ と $v_1, \ldots, v_n$ は M の自由 R 基底であるとする. u_i たちと v_j たちは互いに相手の R 係数の一次結合で一意的に表わされる. よって, 行列 $A \in M_{m,n}(R)$ と $B \in M_{n,m}(R)$ で

$$[u_1, \ldots, u_m]A = [v_1, \ldots, v_n], \qquad [v_1, \ldots, v_n]B = [u_1, \ldots, u_m]$$

[162] free という単語は「ない」という意味でもよく使われる. たとえば tax-free と言えば「無税の」という意味である. free module の意味での free は「非自明な一次関係がない」「非自明な一次関係に束縛されていないという意味で自由な」という意味である.

[163] e_i は第 i 成分だけが 1 で他は 0 の縦ベクトル. 単因子の記号と混乱しないように注意せよ.

[164] 実際には任意の可換環 R で成立する. もしも R が整域ならばヒントにおける体 F として R の商体 (分数体) を取れば良い. R が一般の可換環の場合には Zorn の補題を用いて存在が証明される極大イデアル $\mathfrak{m}$ で割った剰余体 $k = R/\mathfrak{m}$ を用いた議論で商体 F を用いた議論を置き換えれば良い. たとえば堀田 [H1] 62 頁の定理 11.2 を見よ.

[165] 多項式の分数全体のなす体を有理函数体と呼ぶ.

を満たすものが一意に存在する. このとき,

$$[u_1,\dots,u_m]AB=[u_1,\dots,u_m],\qquad [v_1,\dots,v_n]BA=[v_1,\dots,v_n]$$

なので $AB=E_m$ かつ $BA=E_n$ が成立する. $R\subset F$ なので A, B は体 F の元を成分に持つ行列とみなせる. よって体上の行列に関する理論より $m=n$ でなければいけないことがわかる. □

[517] (自由基底の取り換え) M は可換環 R 上の階数 n の有限生成自由加群であるとし, $u_1,\dots,u_n$ はその自由 R 基底であるとすると, $v_1,\dots,v_n\in M$ に対して行列 $A=[a_{ij}]\in M_n(R)$ で

$$v_i=a_{1i}u_1+\cdots+a_{ni}u_n\qquad (i=1,\dots,n)$$

を満たすものが一意に存在する. このとき, $v_1,\dots,v_n$ が M の自由 R 基底になるための必要十分条件は $A\in GL_n(R)$ となることである. □

ヒント: v_i たちを u_i たちの R 係数一次結合で表わす式は $[v_1,\dots,v_n]=[u_1,\dots,u_n]A$ と書き直せる. もしも v_i たちが M の自由 R 基底ならばある $B\in M_n(R)$ で $[u_1,\dots,u_n]=[v_1,\dots,v_n]B$ を満たすものが一意に存在する. このとき $[u_1,\dots,u_n]AB=[u_1,\dots,u_n]$ かつ $[v_1,\dots,v_n]BA=[v_1,\dots,v_n]$ なので $AB=BA=E_n$ である. よって $A\in GL_n(R)$ である. 逆に $A\in GL_n(R)$ であると仮定する. $[u_1,\dots,u_n]=[v_1,\dots,v_n]A$ と u_i たちを v_i たち R 係数一次結合で表わせるので, 任意の M の元は v_i たちの R 係数一次結合で表わせる. $a_1v_1+\cdots+a_nv_n=0$, $a_i\in R$ すなわち $[v_1,\dots,v_n]a=0$, $a={}^t[a_1,\dots,a_n]$ とすると, $[u_1,\dots,u_n]Aa=0$ であるから, $Aa=0$ である. よって $a=0$ である. このことより v_i たちの R 係数一次結合で M の元を表わす方法は一通りしか存在しないことがわかる. □

[518] R は単項イデアル整域であるとし, M は高々 n 個の元から生成される有限生成 R 加群であるとする. このとき, 全射 R 準同型 $\pi:R^n\to M$ と行列 $A\in M_n(R)$ で $\operatorname{Ker}\pi=\operatorname{Im}A$ となるものが存在し, R 同型 $M\cong R^n/\operatorname{Im}A$ が成立する. □

ヒント: 全射 R 準同型 $\pi:R^n\to M$ を $\pi({}^t[a_1,\dots,a_n])=a_1u_1+\cdots+a_nu_n$ と定めることができる. 問題 **[514]** の結果より, $\operatorname{Ker}\pi=Rv_1+\cdots+Rv_n$ と書ける. R 準同型 $\psi:R^n\to R^n$ を $\psi({}^t[b_1,\dots,b_n])=b_1v_1+\cdots+b_nv_n$ と定め, A は ψ を表現する行列であるとする[166]. このとき $\operatorname{Im}A=\operatorname{Im}\psi=Rv_1+\cdots+Rv_n=\operatorname{Ker}\pi$ が成立している. 同型 $M\cong R^n/\operatorname{Im}A$ は準同型定理より, ただちに得られる. □

参考: 準同型の列 $L\to M\to N$ が**完全 (exact)** であるとは $\operatorname{Im}(L\to M)=\operatorname{Ker}(M\to N)$ が成立していることである. たとえば, $\operatorname{Ker}(N\to 0)=N$ なので $M\to N\to 0$ が完全であることと $M\to N$ が全射 ($\operatorname{Im}(M\to N)=N$) であることは同値である. これとは双対的に $\operatorname{Im}(0\to M)=0$ なので $0\to M\to N$ が完全であることと $M\to N$ が単射 ($\operatorname{Ker}(M\to N)=0$) であることは同値である. より長い準同型の列を考える場合にはこの条件を考えることができる場所すべてについてこの条件が成立しているとき, その列は完全であるという. 上の問題の結論は次のように言い換えられる. 単項イデアル整域 R 上の高々 n 個の元から生成される有限生成加群 M に対して次のような完全列が存在する:

$$0\longleftarrow M\xleftarrow{\pi}R^n\xleftarrow{A}R^n.$$

[166] $A=[v_1,\dots,v_n]$ である. 問題 **[444]** を見よ.

$\pi : R^n \to R^n$ から $A : R^n \to R^n$ を作ったのと同様の手続きでこの完全列は無限に延長できる:

$$0 \longleftarrow M \xleftarrow{\pi} R^n \xleftarrow{A} R^n \longleftarrow R^n \longleftarrow \cdots .$$

実は $m \leq n$ を適切に選んで次のような完全列を構成することができる:

$$0 \longleftarrow M \xleftarrow{\pi} R^n \xleftarrow{A} R^m \longleftarrow 0.$$

この結果は一般の単項イデアル整域でも成立しているが, この演習では $R = K[\lambda]$, $\mathbb{Z}$ の場合だけを扱う.

定理 27.4 ($K[\lambda]$ と $\mathbb{Z}$ 上の有限生成加群の構造定理) $R = K[\lambda]$, $\mathbb{Z}$ であるとし, M は R 上の有限生成自由加群であるとする. このとき, $r \in \mathbb{Z}_{\geq 0}$ と

$$f_1 \mid f_2 \mid \cdots \mid f_s, \qquad f_1 \notin R^\times, \quad f_s \neq 0$$

を満たす $f_1, \ldots, f_s \in R$ で R 加群としての同型

$$M \cong R/Rf_1 \oplus \cdots \oplus R/Rf_s \oplus R^r$$

が成立するものが存在する. しかも r と $f_1, \ldots, f_s$ は単元倍を除いて M から一意に定まる[167]. そこで

$$(f_1, f_2, \ldots, f_s, \overbrace{0, \ldots, 0}^{r})$$

を M の**単因子型 (type of elementary divisors)** と呼ぶことにする. □

以上の定理の証明を演習問題とヒントの羅列によって解説する.

[519] (単因子型の存在) 定理 27.4 における単因子型の存在を証明せよ. □

ヒント: M が高々 n 個の元から生成される有限生成 R 加群であるならば, 問題 **[518]** の結果より, 全射 R 準同型 $\pi : R^n \to M$ と行列 $A \in M_{n,m}(R)$ で[168] $\operatorname{Ker}\pi = \operatorname{Im} A$ を満たすものが存在する. そのとき R 同型 $M \cong R^n/\operatorname{Im} A$ が存在する. 行列 A を R 準同型 $A : R^m \to R^n$ とみなし, R^m, R^n の自由基底の取り換えによって A をできるだけ簡単な形にすることを考える. 問題 **[517]** と定理 27.3 より A は次の形をしていると仮定して良い:

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

さらに $e_{t-s} \in R^\times$, $e_{t-s+1} \notin R^\times$ であるとし, $f_1 = e_{t-s+1}, \ldots, f_{s-1} = e_{t-1}, f_s = e_t$ と置く. このとき

$$\operatorname{Im} A = \overbrace{R \oplus \cdots \oplus R}^{t-s \text{ times}} \oplus Rf_1 \oplus \cdots \oplus Rf_s \oplus \overbrace{0 \oplus \cdots \oplus 0}^{n-t \text{ times}}.$$

[167] この結果は R が任意の単項イデアル整域の場合にも成立するが, この演習では $R = K[\lambda]$, $\mathbb{Z}$ の場合のみを扱う.

[168] $m = n$ に取れるがここでは必要ない.

よって, $r = n - t$ と置けば問題 [**461**] の結果より

$$\begin{aligned} M &\cong R^n/\operatorname{Im} A = (\overbrace{R \oplus \cdots \oplus R}^{n \text{ times}})/\operatorname{Im} A \\ &\cong \overbrace{R/R \oplus \cdots \oplus R/R}^{t-s \text{ times}} \oplus R/Rf_1 \oplus \cdots \oplus R/Rf_s \oplus \overbrace{R/0 \oplus \cdots \oplus R/0}^{r \text{ times}}. \\ &\cong R/Rf_1 \oplus \cdots \oplus R/Rf_s \oplus R^r. \quad \square \end{aligned}$$

[**520**] (**ねじれ部分**) 一般に可換環 R 上の加群 M の**ねじれ部分 (torsion part)** M_{tor} が次のように定義される:

$$M_{\mathrm{tor}} = \{\, v \in M \mid \text{ある } a \in R \text{ で } a \neq 0 \text{ かつ } av = 0 \text{ を満たすものが存在する} \,\}.$$

M_{tor} は M の R 部分加群であることを示せ. $M = M_{\mathrm{tor}}$ のとき M は**ねじれ加群 (torsion module)** であるといい, $M_{\mathrm{tor}} = 0$ のとき M は**ねじれを持たない (torsion-free)** という. R が整域ならば R 自身は R 上の加群としてねじれを持たず, 0 でない $f \in R$ に対する R/Rf はねじれ加群であることを示せ. さらに $\{M_i\}_{i \in I}$ が R 加群の族であるとき, 次が成立することを示せ:

$$\Big(\bigoplus_{i \in I} M_i\Big)_{\mathrm{tor}} = \bigoplus_{i \in I} (M_i)_{\mathrm{tor}}. \quad \square$$

ヒント: $M = \bigoplus_{i \in I} M_i$ と置き, $v = (v_i)_{i \in I} \in M$ であるとする. もしも $v \in M_{\mathrm{tor}}$ ならばある $a \in R$ で $a \neq 0$ かつ $av = 0$ を満たすものが存在する. そのとき $0 = av = (av_i)_{i \in I}$ であるから任意の $i \in I$ に対して $av_i = 0$ である. すなわち $v_i \in (M_i)_{\mathrm{tor}}$ である. よって $v = (v_i)_{i \in I} \in \bigoplus_{i \in I} (M_i)_{\mathrm{tor}}$ である. 逆に $v = (v_i)_{i \in I} \in \bigoplus_{i \in I} (M_i)_{\mathrm{tor}}$ であると仮定し, 0 でない v_i の全体を $v_{i_1}, \ldots, v_{i_n}$ とする. $v_{i_\nu} \in (M_{i_\nu})_{\mathrm{tor}}$ なのである $a_\nu \in R$ で $a_\nu \neq 0$ かつ $a_\nu v_{i_\nu} = 0$ を満たすものが存在する. このとき $a = a_1 \cdots a_n$ と置くと $av = 0$ である. よって $v \in M_{\mathrm{tor}}$ である. これで $\big(\bigoplus_{i \in I} M_i\big)_{\mathrm{tor}} = \bigoplus_{i \in I} (M_i)_{\mathrm{tor}}$ が示された. $\square$

[**521**] R は整域であるとし, $f_1, \ldots, f_s \in R$ はゼロでないとする. このとき R 加群としての同型

$$M \cong R/Rf_1 \oplus \cdots \oplus R/Rf_s \oplus R^r$$

が成立しているならば

$$M_{\mathrm{tor}} \cong R/Rf_1 \oplus \cdots \oplus R/Rf_s. \quad \square$$

ヒント: 問題 [**520**] の結果より $(R/Rf_i)_{\mathrm{tor}} = R/Rf_i$ かつ $R_{\mathrm{tor}} = 0$ であり, この問題の結論が成立することがわかる. $\square$

[**522**] (r **の一意性**) 定理 27.4 における r の一意性を証明せよ. $\square$

ヒント: 問題 [**521**] の結果より定理 27.4 の状況のもとで

$$M_{\mathrm{tor}} \cong R/Rf_1 \oplus \cdots \oplus R/Rf_s$$

である. よって $M/M_{\mathrm{tor}} \cong R^r$ である. したがって, 問題 [**516**] の結果より r が M より一意的に定まることがわかる. $\square$

したがって, 定理 27.4 の証明を完了するためにはねじれ加群 M_{tor} に対して $f_1, \ldots, f_s$ が単元倍を除いて一意に定まることを証明すれば良いことがわかった.

[523] R は整域であるとし, $f, g \in R$ はともに 0 ではなく, 互いに素 $(Rf + Rg = R)$ であると仮定する. $\nu \in \mathbb{Z}_{>0}$ を任意に取り, R 加群 M, N を $M = R/Rf^\nu$, $N = R/Rg^\nu$ と定める. このとき以下が成立する:

1. R 部分加群の減少列 $M \supset fM \supset f^2M \supset \cdots f^{\nu-1}M \supset f^\nu M = 0$ が得られ, R 加群としての同型 $f^\mu M \cong R/Rf^{\nu-\mu}$, $f^{\mu-1}M/f^\mu M \cong R/Rf$ $(\mu = 1, \ldots, \nu)$ が成立する.
2. $N = fN = f^2N = \cdots$ であるから, $f^{\mu-1}N/f^\mu N = 0$ $(\mu = 1, \ldots, \nu)$ である. □

ヒント: 1. $u = 1 \bmod f^\nu \in M$ と置くと, $M = Ru$ であり, $f^\mu M = Rf^\mu u$ であり, $a \in R$ に対して $au = 0$ と $a \in Rf^\nu$ は同値である. $f^\mu M \ni af^\mu u = af \cdot f^{\mu-1}u \in f^{\mu-1}M$ なので $f^\mu M \subset f^{\mu-1}M$ である. R 準同型 $R \to f^\mu M$, $a \mapsto af^\mu u$ に準同型定理を適用すれば $f^\mu M \cong R/Rf^{\nu-\mu}$ であることがわかる. R 準同型 $R \to f^{\mu-1}M/f^\mu M$, $a \mapsto af^{\mu-1}u \bmod f^\mu M$ に準同型定理を適用すれば $f^{\mu-1}M/f^\mu M \cong R/Rf$ であることがわかる.

2. $N \subset fN$ を示せば良い. N の元は $a \bmod g^\nu$ $(a \in R)$ の形をしている. 仮定よりある $b, c \in R$ で $bf + cg = 1$ となるものが存在する. そのとき $1 = (af + bg)^\nu = fh + c^\nu g^\nu$ $(h \in R)$ が成立し, したがって $a = fha + ac^\nu g^\nu$ $(a \in R)$ が成立する. よって $a \bmod g^\nu = fha \bmod g^\nu \in fN$ である. これで $N \subset fN$ が示された. □

[524] (ねじれ加群の構造定理) $R = K[\lambda]$, $\mathbb{Z}$ であるとし[169], M は R 上の有限生成ねじれ加群であると仮定する. このとき R の素元 $p_1, \ldots, p_n$ および $m_{i,\nu} \in \mathbb{Z}_{\leq 0}$ $(i = 1, \ldots, n, \nu = 1, 2, 3, \ldots)$ で以下の条件を満たすものが存在する:

(1) $i \neq j$ ならば $p_i \not\sim p_j$ である[170].

(2) 各 $i = 1, \ldots, n$ に対して $m_{i,1}, m_{i,2}, \ldots$ に含まれる 0 でない数の個数は有限であり, 少なくとも 1 つは 0 でない.

(3) 以下の R 同型が成立する:

$$M \cong \bigoplus_{i=1}^{n} \bigoplus_{\nu=1}^{\infty} (R/Rp_i^\nu)^{m_{i,\nu}}.$$

しかもこのような $p_1, \ldots, p_n$ は M から単元倍と並べ方の順序を違いを除いて一意的に定まり, $m_{i,\nu}$ も M から一意的に定まる. □

ヒント: 問題 **[519]**, **[521]** の結果より, 0 でも単元でもない R の元 $f_1 \mid \cdots \mid f_s$ が存在して R 同型 $M \cong R/Rf_1 \oplus \cdots \oplus R/Rf_s$ が得られる. R は一意分解整域なので $f_i \sim p_1^{\nu_{i,1}} \cdots p_n^{\nu_{i,n}}$ と本質的に一意に素元分解される. ここで p_i は R の素元であり, $i \neq j$ ならば $p_i \not\sim p_j$ であり, $\nu_{i,n} \in \mathbb{Z}_{\geq 0}$ である. そのとき中国式剰余定理 **[473]** によって同型

$$R/Rf_i \cong R/Rp_1^{\nu_{i,1}} \oplus \cdots \oplus R/Rp_n^{\nu_{i,n}}$$

が得られる. よって問題の同型が存在することがわかる.

p_i と $m_{i,\nu}$ の一意性を示そう. (3) の同型を仮定する. 問題 **[523]** の結果より,

$$p_i^{\mu-1}M/p_i^\mu M \cong \bigoplus_{\nu \geq \mu} (R/Rp_i)^{m_{i,\nu}} \qquad (\mu = 1, 2, 3, \ldots)$$

[169] 実際には R は任意の単項イデアル整域として良いが, この演習ではこの場合だけを扱う.
[170] $f \sim g$ であるとはある単元 $c \in R^\times$ で $cf = g$ を満たすものが存在することである.

が成立する. 問題 [**486**], [**480**] の結果より $K_i = R/Rp_i$ は体であり,

$$\dim_{K_i}(p_i^{\mu-1}M/p_i^{\mu}M) = m_{i,\mu} + m_{i,\mu+1} + m_{i,\mu+2} + \cdots \qquad (\text{有限和}).$$

よって

$$m_{i,\mu} = \dim_{K_i}(p_i^{\mu-1}M/p_i^{\mu}M) - \dim_{K_i}(p_i^{\mu}M/p_i^{\mu+1}M). \qquad (*)$$

R の素元 p で $p \not\sim p_i\ (= 1, \ldots, n)$ を満たすものを取ると, 問題 [**523**] の結果より, $M/pM = 0$ である. よって $p_1, \ldots, p_n$ は $M/pM \neq 0$ となる素元 p の集合である. 以上のことより, $p_1, \ldots, p_n$ が単数倍と順序を除いて M から一意に定まり, $m_{i,\mu}$ も M から一意に定まることがわかる. □

注意: 上のヒントにおける $(*)$ という結果と問題 [**392**], [**393**] の結果の類似に注意せよ. この類似性は偶然ではない. □

参考: $m_{i,\mu}$ の一意性は **Krull-Remak-Schmidt の定理**からも導かれる. ここでは詳しい説明は避けるが, Krull-Remak-Schmidt の定理とは「長さ有限の加群の直既約分解が同値なものを除いて一意に存在する」という結果である. 単項イデアル整域上の有限生成ねじれ加群 M は長さ有限であり, 問題 [**524**] (3) の M の分解は M の直既約分解である. 直既約分解の同値を除いた一意性から直既約成分の重複度 $m_{i,\mu}$ の一意性が導かれる. たとえば服部 [Ht] 113–114 頁では実際そのようにして単項イデアル整域上の有限生成ねじれ加群の単因子型の一意性を証明している. □

[**525**] 定理 27.4 における $f_1, \ldots, f_s$ の一意性を証明せよ. □

ヒント: 問題 [**524**] のヒントの議論を詳しく見直せば次が成立していることがわかる:

$$(\nu_{i,s}, \nu_{i,s-1}, \cdots, \nu_{i,1}) = (\overbrace{\nu_i, \ldots, \nu_i}^{m_{i,\nu_i}}, \overbrace{\nu_i - 1, \ldots, \nu_i - 1}^{m_{i,\nu_i-1}}, \ldots\ldots, \overbrace{1, \ldots, 1}^{m_{i,1}}, \overbrace{0, \ldots, 0}^{m_{i,0}}).$$

ここで ν_i は $m_{i,\nu} \neq 0$ となる最大の ν であり, $m_{i,0} = s - \sum_{\nu=1}^{\nu_i} m_{i,\nu}$ と置いた. よって f_i は問題 [**524**] の結果によって一意性が保証されている $m_{i,\nu}$ から逆に f_i が $f_i \sim p_1^{\nu_{i,1}} \cdots p_n^{\nu_{i,n}}$ によって M から単数倍を除いて一意に定まることがわかる. □

以上によって定理 27.4 の証明が完了した.

$R = K[\lambda]$ の場合の定理 27.4 と K が代数閉体の場合の問題 [**524**] は次の定理にまとめられる.

定理 27.5 (有限生成 $K[\lambda]$ 加群の構造定理) K は任意の体であり, M は有限生成 $K[\lambda]$ 加群であるとする. このとき, 非負の整数 $r \in \mathbb{Z}_{\geq 0}$ と 0 でない次数が 1 以上のモニックな多項式 $f_1, \ldots, f_s \in K[\lambda]$ で

$$f_1 \mid f_2 \mid \cdots \mid f_s$$

を満たし, $K[\lambda]$ 同型

$$M \cong K[\lambda]/(f_1) \oplus \cdots \oplus K[\lambda]/(f_s) \oplus K[\lambda]^r$$

が成立するようなものが一意に存在する. さらに K が代数閉体であるならば, 有限個を除いて 0 であるような非負の整数の族 $\{m_{\alpha,\nu}\}_{\alpha \in K,\, \nu \in \mathbb{Z}_{>0}}$ で $K[\lambda]$ 同型

$$M \cong K[\lambda]^r \oplus \bigoplus_{\alpha \in K} \bigoplus_{\nu=1}^{\infty} \Big(K[\lambda]/\big((\lambda - \alpha)^{\nu}\big) \Big)^{m_{\alpha,\nu}}$$

が成立するようなものが一意に存在する. □

$\mathbb{Z}$ 上の有限生成加群の場合に関して, 定理 27.4 と問題 [**524**] の結果は次のようにまとめられる.

定理 27.6 (有限生成 Abel 群の基本定理) M は有限生成 $\mathbb{Z}$ 加群であるとする[171]. 素数全体の集合を $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ と書くことにする. このとき, 非負の整数 $r \in \mathbb{Z}_{\geq 0}$ と 2 以上の整数 $f_1, \ldots, f_s \in \mathbb{Z}$ で

$$f_1 \mid f_2 \mid \cdots \mid f_s$$

を満たし, 同型

$$M \cong \mathbb{Z}/f_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/f_s\mathbb{Z} \oplus \mathbb{Z}^r$$

が成立するようなものが一意に存在する. さらに有限個を除いて 0 であるような非負の整数の族 $\{m_{p,\nu}\}_{p\in\mathcal{P},\, \nu\in\mathbb{Z}_{>0}}$ で同型

$$M \cong \mathbb{Z}^r \oplus \bigoplus_{p\in\mathcal{P}} \bigoplus_{\nu=1}^{\infty} (\mathbb{Z}/p^\nu\mathbb{Z})^{m_{p,\nu}}$$

が成立するようなものが一意に存在する. □

27.9 Jordan 標準形再論

代数閉体 K 上の一変数多項式環 $K[\lambda]$ 上の有限生成加群に関する定理 27.5 の後半は Jordan 標準形の理論を含んでいる.

[**526**] **(Jordan 標準形再論)** 代数閉体 K 上の一変数多項式環 $K[\lambda]$ 上の有限生成加群に関する定理 27.5 の後半を用いて, Jordan 標準形の存在と一意性 (定理 23.8) を証明せよ. □

ヒント: K は任意の代数閉体であるとし, $A \in M_n(K)$ は K 上の任意の正方行列であるとする. このとき $M = K^n$ には次のようにして自然に $K[\lambda]$ 加群の構造を定めることができる:

$$f(\lambda)v = f(A)v \qquad (f \in K[\lambda],\ v \in M = K^n).$$

Cayley-Hamilton の定理もしくは最小多項式の理論より, ある 0 でない多項式 $\varphi \in K[\lambda]$ が存在して $\varphi(A) = 0$ となる. よって M はねじれ加群である. したがって定理 27.5 の後半より, 有限個を除いて 0 であるような非負の整数の族 $\{m_{\alpha,\nu}\}_{\alpha\in K,\, \nu\in\mathbb{Z}_{>0}}$ で $K[\lambda]$ 同型

$$M \cong \bigoplus_{\alpha\in K} \bigoplus_{\nu=1}^{\infty} \Big(K[\lambda]/\big((\lambda-\alpha)^\nu\big) \Big)^{m_{\alpha,\nu}}$$

が成立するようなものが一意に存在する. $u_k \in K[\lambda]/\big((\lambda-\alpha)^\nu\big)$ を

$$u_k = (\lambda-\alpha)^k \bmod (\lambda-\alpha)^\nu \in K[\lambda]/\big((\lambda-\alpha)^\nu\big)$$

[171] 任意の Abel 群は自然に $\mathbb{Z}$ 加群とみなせるので, この仮定は M が有限生成 Abel 群であるという仮定に等しい.

定めると, $u_{\nu-1}, u_{\nu-2}, \ldots, u_1, u_0$ は $K[\lambda]\big/\big((\lambda-\alpha)^\nu\big)$ の K 基底をなす. その基底に関して λ すなわち A の $K[\lambda]\big/\big((\lambda-\alpha)^\nu\big)$ への作用を行列表示すると Jordan ブロック行列 $J_\nu(\alpha)$ が得られる:

$$\begin{aligned}[\lambda u_{\nu-1}, \lambda u_{\nu-2}, \ldots, \lambda u_0] &= [\alpha u_{\nu-1}, u_{\nu-1} + \alpha u_{\nu-2}, \ldots, u_1 + \alpha u_0] \\ &= [u_{\nu-1}, u_{\nu-2}, \ldots, u_0] J_\nu(\alpha).\end{aligned}$$

そのような基底を M 全体で考えれば λ すなわち A の M への作用の行列表示は Jordan 標準形の形をしている. Jordan 細胞の情報は M から一意に定まる $m_{i,\nu}$ と一致している. よって Jordan 標準形の一意性も出る. □

体 K の元 $a_0, \ldots, a_{n-1}$ に対してコンパニオン行列 (同伴行列, companion matrix) $C(a_0, \ldots, a_{n-1})$ を次のように定義したのであった:

$$C(a_0, \ldots, a_{n-1}) = \begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & \ddots & & \\ & & \ddots & 1 & \\ 0 & & & 0 & 1 \\ -a_{n-1} & -a_{n-2} & \cdots & -a_1 & -a_0 \end{bmatrix}.$$

問題 **[375]** の結論は, コンパニオン行列 $C(a_0, \ldots, a_{n-1})$ の特性多項式が

$$f(\lambda) = \lambda^n + a_0\lambda^{n-1} + a_1\lambda^{n-2} + \cdots + a_{n-2}\lambda + a_{n-1} \in K[\lambda]$$

に等しく, かつその最小多項式が特性多項式に等しくなることであった. 逆にモニックな多項式 f に対してコンパニオン行列 C_f を次のように定義する:

$$C_f = C(a_0, \ldots, a_{n-1}).$$

体 K 上の一変数多項式環 $K[\lambda]$ 上の有限生成加群に関する定理 27.5 の前半から次の定理が導かれる.

[527] (正方行列の有理標準形) K は代数閉体とは限らない任意の体であるとし, $A \in M_n(K)$ は K 上の任意の正方行列であるとする. このとき, 次数が 1 以上のモニックな多項式 $f_1, \ldots, f_s \in K[\lambda]$ で以下を満たすものが一意に存在する:

(1) $f_1 \mid f_2 \mid \cdots \mid f_s$.

(2) $n_i = \deg f_i$ と置くと $n_1 + \cdots + n_s = n$.

(3) ある $P \in GL_n(K)$ で次を満たすものが存在する:

$$P^{-1}AP = \begin{bmatrix} C_{f_1} & & 0 \\ & \ddots & \\ 0 & & C_{f_s} \end{bmatrix}. \qquad (*)$$

等式 $(*)$ の右辺を A の**有理標準形 (rational canonical form, rational normal form)** もしくは **Frobenius 標準形 (Frobenius canonical form, Frobenius normal form, Frobenius form)** と呼ぶ. □

ヒント: $M = K^n$ には次のようにして自然に $K[\lambda]$ 加群の構造を定めることができる:

$$f(\lambda)v = f(A)v \qquad (f \in K[\lambda],\ v \in M = K^n).$$

Cayley-Hamilton の定理もしくは最小多項式の理論より, ある 0 でない多項式 $\varphi \in K[\lambda]$ が存在して $\varphi(A) = 0$ となる. よって M はねじれ加群である. したがって体 K 上の一変数多項式環 $K[\lambda]$ 上の有限生成加群に関する定理 27.5 の前半より, 次数が 1 以上のモニックな多項式 $f_1, \ldots, f_s \in K[\lambda]$ で $f_1 \mid f_2 \mid \cdots \mid f_s$ を満たし, $K[\lambda]$ 同型

$$M \cong K[\lambda]/(f_1) \oplus \cdots \oplus K[\lambda]/(f_s)$$

が成立するものが一意に存在する. $n_i = \deg f_i$ と置いて, 両辺の K 上のベクトル空間としての次元を計算すれば $n = n_1 + \cdots + n_s$ であることがわかる. f_i を

$$f_i(\lambda) = \lambda^{n_i} + a_{i,0}\lambda^{n_i-1} + \cdots + a_{i,n_i-3}\lambda^2 + a_{i,n_i-2}\lambda + a_{i,n_i-1}, \qquad a_{i,k} \in K$$

と表わし, $K[\lambda]/(f_i)$ の基底 $v_{i,1}, \ldots, v_{i,n_i}$ を次のように定める:

$$\begin{aligned}
v_{i,1} &= (\lambda^{n_i-1} + a_{i,0}\lambda^{n_i-2} + \cdots + a_{i,n_i-3}\lambda + a_{i,n_i-2}) \bmod f_i,\\
v_{i,2} &= (\lambda^{n_i-2} + a_{i,0}\lambda^{n_i-3} + \cdots + a_{i,n_i-3}) \bmod f_i,\\
&\cdots\cdots\\
v_{i,n_i-1} &= (\lambda + a_0) \bmod f_i,\\
v_{i,n_i} &= 1 \bmod f_i.
\end{aligned}$$

この基底に関して λ すなわち A の $K[\lambda]/(f_i)$ への作用を行列表示すると C_{f_i} が得られる:

$$\begin{aligned}
[\lambda v_{i,1}, \lambda v_{i,2}, \ldots, \lambda v_{i,n_i}] &= [-a_{i,n_i-1}v_{i,n_i}, v_{i,1} - a_{i,n_i-2}v_{i,n_i}, \ldots, v_{i,n_i-1} - a_0 v_{i,n_i}]\\
&= [v_{i,1}, v_{i,2}, \ldots, v_{i,n_i}]C_{f_i}.
\end{aligned}$$

よって λ すなわち A の M への作用を基底 $v_{i,k}$ に関して行列表示すると A の有理標準形が得られる. □

注意: $K[\lambda]/(f_i)$ の基底として, より自然な $w_{i,k} = \lambda^k \bmod f_i$ $(k = 0, 1, \ldots, n_i - 1)$ を取ると, λ の作用の行列表示は ${}^tC_{f_i}$ になる:

$$\begin{aligned}
[\lambda w_{i,0}, \ldots, \lambda w_{i,n_i-2}, \lambda w_{i,n_i-1}] &= [w_{i,1}, \ldots, w_{i,n_i-1}, -a_{n_i-1}w_{i,0} - \cdots - a_0 w_{i,n_i-1}]\\
&= [w_{i,1}, \ldots, w_{i,n_i-2}, w_{i,n_i-1}]\,{}^tC_{f_i}.
\end{aligned}$$

問題 [**418**] のヒント 2 と問題 [**421**] のヒント 2 も参照せよ. □

[**528**] 問題 [**527**] の記号のもとで, A の最小多項式 φ_A は f_s に等しく, A の特性多項式 p_A は $f_1 \cdots f_s$ に等しい:

$$\varphi_A(\lambda) = f_s(\lambda), \qquad p_A(\lambda) = f_1(\lambda) \cdots f_s(\lambda). \quad \square$$

ヒント: 問題 [**375**] の結果より $C_i = C_{f_i}$ と置くと $\varphi_{C_i} = p_{C_i} = f_i$ である. 問題 [**529**] も見よ. □

[529] K は任意の体であるとする. 次のような形の正方行列 B の最小多項式は B_i たちの最小多項式の最小公倍多項式に等しい:

$$B = \begin{bmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_s \end{bmatrix}, \qquad B_i \in M_{n_i}(K). \quad \square$$

さて, それでは有理標準形や Jordan 標準形を具体的に計算するにはどうすれば良いのだろうか.

K は任意の体であるとし, $A \in M_n(K)$ は K 上の任意の正方行列であるとする. このとき $M = K^n$ には次のように $K[\lambda]$ 加群の構造を定めることができる:

$$f(\lambda)v = f(A)v \qquad (f \in K[\lambda],\ v \in M = K^n).$$

Cayley-Hamilton の定理もしくは最小多項式の理論より, ある 0 でない多項式 $\varphi \in K[\lambda]$ が存在して $\varphi(A) = 0$ となる. よって M はねじれ加群である.

K^n と $K[\lambda]^n$ の標準的な基底をどちらも同じ記号 $e_1, \ldots, e_n$ と表わし, 全射 $K[\lambda]$ 準同型 $\pi : K[\lambda]^n \to M$ を次のように定める:

$$\pi(a_1 e_1 + \cdots + a_n e_n) = a_1(A)e_1 + \cdots + a_n(A)e_n \qquad (a_i \in K[\lambda]).$$

問題は $\operatorname{Ker}\pi$ がどのような形をしているかである.

[530] (特性行列) 行列 $\lambda E - A \in M_n(K[\lambda])$ が定める $K[\lambda]$ 準同型を $\phi : K[\lambda]^n \to K[\lambda]^n$ と書く:

$$\phi(v) = (\lambda E - A)v \qquad (v \in K[\lambda]^n).$$

このとき $\operatorname{Im}\phi = \operatorname{Ker}\pi$ である. 体 K 上の正方行列 $A \in M_n(K)$ に対して多項式環 $K[\lambda]$ 上の行列 $\lambda E - A \in M_n(K[\lambda])$ を A の**特性行列 (characteristic matrix)** と呼ぶ[172]. $\square$

ヒント: まず $\operatorname{Im}\phi \subset \operatorname{Ker}\pi$ であることを示そう. そのためには $\pi \circ \phi = 0$ を示せば良い. よって $\pi(\phi(e_i)) = 0$ を示せば良い. 実際にそれを計算すると

$$\pi(\phi(e_i)) = \pi((\lambda E - A)e_i) = \pi(\lambda e_i - Ae_i) = Ae_i - Ae_i = 0.$$

次に $\dim_K(K[\lambda]^n/\operatorname{Im}\phi) = n$ を示そう. $\operatorname{Im}\phi$ は $\phi(e_i) = \lambda e_i - Ae_i$ を含む. よって e_i, $\lambda^k\phi(e_i)$ $(i = 1, \ldots, n,\ k = 0, 1, 2, \ldots)$ は $K[\lambda]^n$ の K 基底をなす. よって $e_i \bmod \operatorname{Im}\phi$ $(i = 1, \ldots, n)$ は $K[\lambda]^n/\operatorname{Im}\phi$ の K 基底をなす. $\operatorname{Im}\phi = \operatorname{Ker}\pi$ を示そう. もしも $\operatorname{Ker}\pi$ が $\operatorname{Im}\phi$ よりも真に大きければ $\dim_K(K[\lambda]^n/\operatorname{Ker}\pi) < n$ となる. しかし, 準同型定理より $M \cong R^n/\operatorname{Ker}\pi$ なので $\dim_K(R^n/\operatorname{Ker}\pi) = n$ であるから矛盾する. よって $\operatorname{Im}\phi = \operatorname{Ker}\pi$ である. $\square$

[172]特性行列 $\lambda E - A$ の行列式は特性多項式 $p_A(\lambda)$ になる. 特性多項式 $p_A(\lambda)$ は A の固有値と一般固有空間の次元の情報は含んでいるが Jordan 標準形の情報を完全には含んでいない. それに対して, すぐ後に説明するように特性行列 $\lambda E - A$ の単因子は Jordan 標準形の情報を完全に含んでいる.

[531] (特性行列の単因子と有理標準形) 特性行列 $\lambda E - A$ の単因子を $g_1 \mid g_2 \mid \cdots \mid g_n$ (g_i はモニックまたは 0) とする. このとき特性多項式に関して $p_A(\lambda) = \det(\lambda E - A) = g_1 g_2 \cdots g_n$ が成立する. 特に $g_n \neq 0$ である. さらに $g_1, \ldots, g_{n-s} = 1$, $\deg g_{n-s+1} \geq 1$ と仮定し, $f_1 = g_{n-s+1}$, $f_2 = g_{n-s+2}$, $\ldots$, $f_s = g_n$ と置く. すなわち $g_1, \ldots, g_n$ から 1 を除いて得られる列を $f_1, \ldots, f_s$ と書くことにする. そのときそれらは問題 **[527]** の $f_1, \ldots, f_s$ に等しい. すなわちそのとき A の有理標準形は次に等しい:

$$\begin{bmatrix} C_{f_1} & & 0 \\ & \ddots & \\ 0 & & C_{f_s} \end{bmatrix}. \quad \square$$

ヒント: ある $P, Q \in GL_n(K)$ が存在して

$$P(\lambda E - A)Q = \operatorname{diag}(g_1, g_2, \ldots, g_n), \qquad g_1 \mid g_2 \mid \cdots \mid g_n, \quad g_i \text{ はモニックまたは } 0.$$

このとき, $a := \det P \det Q \in K^\times$ と置くと, $p_A(\lambda) = \det(\lambda E - A) = a g_1 g_2 \cdots g_n$ である. よって最高次の係数を比較すると $g_1, \ldots, g_n$ はどれもモニックであり, $a = 1$ であることがわかる. このとき, 問題 **[530]** の結果より, 問題 **[519]** のヒントと同様にして, $K[\lambda]$ 同型

$$M \cong K[\lambda]/(f_1) \oplus \cdots \oplus K[\lambda]/(f_s)$$

が成立することがわかる. $\square$

参考: 上の記号のもとで $\operatorname{diag}(g_1, g_2, \ldots, g_n)$ を特性行列 $\lambda E - A$ の **Smith 標準形 (Smith normal form, Smith canonical form)** と呼ぶことがある. $\square$

[532] (特性行列の単因子と Jordan 標準形) さらに K は代数閉体であると仮定し, 問題 **[531]** の $f_1, \ldots, f_s$ は次のように一次式の積に分解されていると仮定する:

$$f_i(\lambda) = (\lambda - \alpha_{i,1})^{n_{i,1}} \cdots (\lambda - \alpha_{i,r_i})^{n_{i,r_i}} \qquad (i = 1, \ldots, s).$$

ここで $k \neq l$ のとき $\alpha_{i,k} \neq \alpha_{i,l}$ であり, $n_{i,k}$ は正の整数である. このとき A の Jordan 細胞の全体は $J_{n_{i,k}}(\alpha_{i,k})$ $(i = 1, \ldots, s,\ k = 1, \ldots, r_i)$ になる. $\square$

ヒント: 中国式剰余定理より,

$$K[\lambda]/(f_i) \cong K[\lambda]\big/\big((\lambda - \alpha_{i,1})^{n_{i,1}}\big) \oplus \cdots \oplus K[\lambda]\big/\big((\lambda - \alpha_{i,s_i})^{n_{i,s_i}}\big).$$

各 $K[\lambda]\big/\big((\lambda - \alpha_{i,k})^{n_{i,k}}\big)$ の基底を $(\lambda - \alpha_{i,k})^\nu$ $(\nu = n_{i,k} - 1, \ldots, 1, 0)$ に取り, その基底に関して λ すなわち A の作用を行列表示すれば A の Jordan 標準形が得られる. $\square$

以上によって, 体 K 上の正方行列 $A \in M_n(K)$ の有理標準形や Jordan 標準形を求めるためには特性行列 $\lambda E - A \in M_n(K[\lambda])$ の単因子を計算すればよいことがわかった.

単因子を計算するための手続きは問題 **[510]** のヒント 2 にある. Jordan 標準形を計算するためには $f_1 \mid \cdots \mid f_s$ である必要はないので, 単因子計算の手続きのステップ 5 で B のすべての成分が a で割り切れることをチェックせずに B に対してその手続きを再帰的に適用する作業に移行して構わない.

要約 27.7 (単因子に基いた行列の標準形の計算の仕方) 体 K 上の正方行列 $A \in M_n(K)$ の有理標準形と Jordan 標準形を以下のような手続きで求めることができる:

1. まず特性行列 $\lambda E - A$ の単因子 $g_1 \mid g_2 \mid \cdots \mid g_n$ (g_i はモニックな多項式) を計算する. 単因子を計算するための手続きは問題 **[510]** のヒント 2 にある.

2. 単因子の列 $g_1 \mid g_2 \mid \cdots \mid g_n$ から 1 を除いたものを $f_1 \mid f_s \mid \cdots \mid f_s$ と書けば, A の有理標準形 (Frobenius 標準形) は次に等しい:

$$\begin{bmatrix} C_{f_1} & & 0 \\ & \ddots & \\ 0 & & C_{f_s} \end{bmatrix}.$$

   これより A の最小多項式が f_s であることもわかる.

3. $f_1, \ldots, f_s$ が次のように一次式の積に分解されているとする:

$$f_i(\lambda) = (\lambda - \alpha_{i,1})^{n_{i,1}} \cdots (\lambda - \alpha_{i,r_i})^{n_{i,r_i}} \qquad (i = 1, \ldots, s).$$

   ここで $k \neq l$ のとき $\alpha_{i,k} \neq \alpha_{i,l}$ であり, $n_{i,k}$ は正の整数である. このとき A の Jordan 細胞の全体は

$$J_{n_{i,k}}(\alpha_{i,k}) \qquad (i = 1, \ldots, s,\ k = 1, \ldots, r_i)$$

   になる. この結論が成立するためには単因子が満たすべき条件 $g_1 \mid g_2 \mid \cdots \mid g_n$ が成立していなくても良く, 特性行列 $\lambda E - A$ が行列の基本変形によって対角化されているだけで十分である.

そして, この計算法の基礎は体 K 上の一変数多項式環 $K[\lambda]$ 上の有限生成加群の構造定理 (定理 27.5) である. □

参考文献

[U] 梅村浩, 楕円関数論—楕円曲線の解析学, 東京大学出版会, 2000

[KI] 韓太舜, 伊理正夫, ジョルダン標準形, UP 応用数学選書 8, 東京大学出版会, 1982

[C] キャッセルズ, J. W., 楕円曲線入門, 徳永浩雄訳, 岩波書店, 1996

[KO] 小林俊行, 大島利雄, Lie 群と Lie 環 1, 岩波講座現代数学の基礎 12, 岩波書店, 1999

[St] 佐武一郎, 線型代数学, 数学選書 1, 裳華房, 1974

[Sh] シャファレヴィッチ, I. R., 代数学とは何か, 蟹江幸博訳, シュプリンガー・フェアラーク東京, 2001

[ST] シルヴァーマン, J. H., テイト, J., 楕円曲線論入門, 足立恒雄, 木田雅成, 小松啓一, 田谷久雄訳, シュプリンガー・フェアラーク東京, 1995

[Sg] 杉浦光夫, Jordan 標準形と単因子論 I, II, 岩波講座基礎数学, 線型代数 iii, 1976

[Tkg1] 高木貞治, 代数学講義, 改定新版, 共立出版, 1965

[Tkg2] 高木貞治, 初等整数論講義, 第 2 版, 共立出版, 1971

[Tkc] 竹内端三, 楕圓函數論, 岩波全書, 岩波書店, 1936

[Ts] 田坂隆士, 2 次形式 I, II, 岩波講座基礎数学, 線型代数 iii, 1976

[Tn] 谷崎俊之, リー代数と量子群, 現代数学の潮流, 共立出版, 2002

[長谷川] 長谷川浩司, 線型代数, 日本評論社, 2004

[Ht] 服部昭, 現代代数学, 近代数学講座 1, 朝倉書店, 1968

[Kh] ヒンチン, A. Y., 数論の 3 つの真珠, 蟹江幸博訳, はじめよう数学 4, 日本評論社, 2000

[T] 寺沢寛一, 自然科学者のための数学概論, 増訂版, 岩波書店, 1954, 1983, 1986

[N] 中村佳正編, 可積分系の応用数理, 裳華房, 2000

[H1] 堀田良之, 代数入門——群と加群——, 数学シリーズ, 裳華房, 1987

[H2] 堀田良之, 加群十話——加群入門——, すうがくぶっくす 3, 朝倉書店, 1988

[YmS] 山内恭彦, 杉浦光夫, 連続群論入門, 新数学シリーズ 18, 培風館, 1960

[Ykt] 横田一郎, 群と位相, 基礎数学選書, 裳華房, 1971

[Ykn] 横沼健雄, テンソル代数と外積代数, 岩波講座基礎数学, 線型代数 iv, 1976

[R] リード, M., 可換環論入門, 伊藤由佳理訳, 岩波書店, 2000

[W] 脇本実, 無限次元 Lie 環, 岩波講座現代数学の展開 3, 岩波書店, 1999