代数学序論 B 演習

黒木 玄　(東北大学大学院理学研究科数学専攻)

2007 年 6 月 19 日

目 次

7 計算問題

正規行列と Sylvester の慣性法則の問題は講義で習っていなければやる必要はない. (しかし数学的常識として結果と計算例は知っておいた方が良い.)

Jordan 標準形の計算は試験対策のためできるだけやっておく方が良いだろう.

7.1 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 ([**227**]). これの逆が成立する ([**228**]).

定理 7.1 (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 7.2 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. □

[152] (5 点) 上の例の計算が正しいことを確かめよ. □

[153] (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:

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

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:

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

[1] ノルムが 1 の固有ベクトルのこと.

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:

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

[154] **(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. $\square$

[155] **(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 $(u, v) = 0$. $\square$

[156] **(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. $\square$

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

参考 7.3 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. $\square$

[2]虚数単位の実数倍を純虚数と呼ぶ.

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.

[157] (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 7.4 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. □

7.2 Sylvester の慣性法則

実対称行列 $A = [a_{ij}]$ から

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

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 $\alpha_1, \dots, \alpha_n$ 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:

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

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 $\alpha_1, \dots, \alpha_p > 0$, $\alpha_{p+1}, \dots, \alpha_{p+q} < 0$, $\alpha_{p+q+1} = \cdots = \alpha_n = 0$ と仮定できる. このとき

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

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 7.5 (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. □

[158] (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 $x, y, \dots$ 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 $(2,1)$. □

[159] (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. □

[160] (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. □

7.3 Jordan 標準形の計算

[161] (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 $P_i^{-1} A_i P_i = J_i$ 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 $P_i^{-1} A_i P_i = J_i$ である:

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

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

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

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

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. □

8 体上の 1 変数多項式環における Euclid の互除法の応用

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[3] 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.

8.1 Lagrange の補間公式

[162] $f, g \in K[\lambda]$ 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 $\alpha_1, \dots, \alpha_n \in K$ について $f(\alpha_i) = g(\alpha_i)$ $(i = 1, \dots, n)$ 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. $h(\alpha_i) = 0$ $(i = 1, \dots, n)$ は剰余定理より, h が $\lambda - \alpha_i$ $(i = 1, \dots, n)$ 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. □

ヒント 2: $h(\alpha_i) = 0$ $(i = 1, \dots, n)$ は次と同値である:

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} = 0.$$

[3] Hamilton-Cayley の定理と呼んでいる文献も多い.

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. □

[163] $p_1, \dots, p_r$ 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. □

[164] $\alpha_1, \dots, \alpha_n \in K$ 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,

$$\frac{(\lambda-\beta)(\lambda-\gamma)}{(\alpha-\beta)(\alpha-\gamma)} + \frac{(\lambda-\alpha)(\lambda-\gamma)}{(\beta-\alpha)(\beta-\gamma)} + \frac{(\lambda-\alpha)(\lambda-\beta)}{(\gamma-\alpha)(\gamma-\beta)} = 1,$$

$$\frac{1}{(\lambda-\alpha)(\lambda-\beta)(\lambda-\gamma)} = \frac{1}{(\alpha-\beta)(\alpha-\gamma)} \frac{1}{\lambda-\alpha} + \frac{1}{(\beta-\alpha)(\beta-\gamma)} \frac{1}{\lambda-\beta} + \frac{1}{(\gamma-\alpha)(\gamma-\beta)} \frac{1}{\lambda-\gamma}. \quad □$$

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 **[162]** を使う. □

[165] (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 $b_1, \dots, b_n \in K$ 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 $p(\alpha_i) = b_i$ $(i = 1, \dots, n)$ 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 [**162**] の結果を使う. 問題 [**164**] のヒントを見よ. □

[**166**] 体 K の標数は 0 であると仮定する[4]. $\alpha \in K$ と $n \in \mathbb{Z}_{>0}$ を任意に取る. このとき, 多項式 $f \in K[\lambda]$ が

$$f^{(\nu)}(\alpha) = 0 \quad (\nu = 0, 1, \dots, n-1)$$

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[5]. 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. □

[**167**] 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. □

[**168**] 2 つの多項式 $f, g \in K[\lambda]$ が互いに素[6] 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[7]. □

ヒント: 問題 [**31**] 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. □

[**169**] 体 K の標数は 0 であると仮定する[8]. 互いに異なる $\alpha_1, \dots, \alpha_s \in K$ と $n_1, \dots, n_s \in \mathbb{Z}_{>0}$ を任意に取り, $n = n_1 + \cdots + n_s$ と置く. このとき, 任意の $b_{i,\nu} \in K$ ($i = 1, \dots, s$, $\nu = 0, 1, \dots, n_i - 1$) に対して, ある多項式 $p \in K[\lambda]$ で次数が $n-1$ 以下でかつ

$$p^{(\nu)}(\alpha_i) = b_{i,\nu} \qquad (i = 1, \dots, s,\ \nu = 0, 1, \dots, n_i - 1)$$

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. □

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 [**166**] の結果より, p は $(\lambda - \alpha_i)^{n_i}$ $(i = 1, \dots, s)$ のすべてで割り切れる. よって p は f で割り切れる.

---

[4]「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.
[5] $k > 0$ 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.
[6] 最大公約元が 1 であるということ.
[7] $f \equiv g \mod h$ 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.
[8]「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.

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

$$p(\lambda) \equiv b_i(\lambda) \mod (\lambda-\alpha_i)^{n_i} \qquad (i=1,\dots,s)$$

と同値である[9]. $f_i(\lambda) = f(\lambda)/(\lambda-\alpha_i)^{n_i}$ と置く. f_i と $(\lambda-\alpha_i)^{n_i}$ は互いに素なので問題 **[168]** の結果より, ある $a_i \in K[\lambda]$ が存在して $a_i f_i \equiv b_i \mod (\lambda-\alpha_i)^{n_i}$ となる. このとき, $p = a_1 f_1 + \cdots + a_s f_s$ 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: $a_i f_i \equiv b_i \mod (\lambda-\alpha_i)^{n_i}$ 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,

$$a_{i,\nu} = \frac{1}{\nu!}\left[\frac{d^\nu}{d\lambda^\nu}\frac{b_i(\lambda)}{f_i(\lambda)}\right]_{\lambda=\alpha_i} \qquad (\nu=0,1,2,\dots).$$

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:

$$a_i(\lambda) = a_{i,0} + a_{i,1}(\lambda-\alpha_i) + \cdots + a_{i,n_i-1}(\lambda-\alpha_i)^{n_i-1} \qquad (i=1,\dots,s).$$

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 $p = a_1 f_1 + \cdots + a_s f_s$ 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 **[165]** 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 8.1 (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 $\alpha_1,\dots,\alpha_s \in K$ と $n_1,\dots,n_s \in \mathbb{Z}_{>0}$ 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 $i=1,\dots,s$ 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

$$p^{(\nu)}(\alpha_i) = b_i^{(\nu)}(\alpha_i) \qquad (i=1,\dots,s,\ \nu=0,1,\dots,n_i-1)$$

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:

$$p(\lambda) = \sum_{i=1}^{s}\sum_{\nu=0}^{n_i-1}\frac{1}{\nu!}\left[\frac{d^\nu}{d\lambda^\nu}\frac{b_i(\lambda)}{f_i(\lambda)}\right]_{\lambda=\alpha_i}\frac{f(\lambda)}{(\lambda-\alpha_i)^{n_i-\nu}}. \quad □$$

[9] $b_{i,\nu}$ 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.

[170] 2 つの整数 $m, n \in \mathbb{Z}_{>0}$ が互いに素[10] 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 $0 \le a < n$ 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 **[25]** の結果を使う. 問題 **[168]** とほとんど同じ. □

[171] $N \in \mathbb{Z}_{>0}$ 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. □

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[11]. $N_i = N/p_i^{n_i}$ と置くと N_i たちの最大公約数は 1 なので問題 **[26]** の結果より, 任意の整数 m は $m = a_1N_1 + \cdots + a_sN_s$ $(a_i \in \mathbb{Z})$ と表わされる[12]. m が $m \equiv a_iN_i \equiv b_i \mod p_i^{n_i}$ $(i = 1, \ldots, s)$ 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 **[170]** の結果より $a_iN_i \equiv b_i \mod p_i^{n_i}$ を満たす $a_i \in \{0, 1, \ldots, p_i^{n_i} - 1\}$ が一意に存在する. □

[172] 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 **[164]** 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[13]. □

8.2 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:

$$K(\lambda) = \{\, g/f \mid f, g \in K,\ f \ne 0 \,\}.$$

$K(\lambda)$ 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[14].

[10] 最大公約数が 1 であるということ.

[11] 実は $b_{i,\nu}$ を持ち出したのは問題 **[169]** 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.

[12] 問題 **[26]** の結果より, ある $c_i \in \mathbb{Z}$ が存在して $1 = c_1N_1 + \cdots + c_sN_s$ となる. これの両辺に m をかければ良い.

[13] 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.

[14] 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.

[173] $K(\lambda)$ 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. □

[174] **(有理函数の部分分数展開)** 次数が $n \geq 0$ のモニックな[15]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[16]:

$$f(\lambda) = (\lambda-\alpha_1)^{n_1} \cdots (\lambda-\alpha_s)^{n_s}.$$

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 **[173]** 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. □

[175] **(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. □

[15]最高次の係数が 1 であるという意味.
[16]$K = \mathbb{C}$ 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 [**170**] の結果より $a_i f_i \equiv g \mod p_i^{n_i}$ を満たす $a_i \in \{0, 1, \dots, p_i^{n_i} - 1\}$ が一意に存在する. 0 以上 $p_i^{n_i}$ 未満の整数 a_i は

$$a_i = a_{i,1} p_i^{n_i - 1} + a_{i,2} p_i^{n_i - 2} + \cdots + a_{i,n_i - 1} p_i + a_{i,n_i}, \quad a_{i,\nu} \in \{0, 1, \dots, p_i - 1\}$$

と一意に表示できる[17]. $c = a_1 f_1 + \cdots + a_s f_s$ 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. □

[**176**] 有理函数の部分分数展開 [**174**] を用いて Lagrange の補間公式 [**165**] を証明せよ. □

ヒント: Lagrange の補間公式の設定は問題 [**174**] 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. □

[**177**] K が代数閉体であるとき[18], 有理函数の部分分数展開 [**174**] を用いて, よく使われる問題 [**32**] 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 [**32**] 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 [**32**] のヒント 1),
- 単項イデアルの考え方を使う方法 (問題 [**32**] 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).

---

[17] 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.

[18]「代数閉体」という言葉が怖い人は $K = \mathbb{C}$ と仮定してよい.

9 一般固有空間分解と Jordan 標準形

この節では佐武 [佐武] 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[19]. 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 [**161**] 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.

[**178**] **(問題 [161] への補足)** 問題 [**161**] 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 9.4 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:

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

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

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

[19] 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 [佐武] 第 IV 章や杉浦 [杉浦] 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 [**217**] で定義されているコンパニオン行列 $C_1, \dots, C_t$ 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 [韓・伊理] 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 [堀田 2] の第 3 章と第 4 章が良い. 堀田 [堀田 1] 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,

$$\begin{aligned} &\varphi_1(\lambda) = (\lambda+2)^3(\lambda-2), && \varphi_2(\lambda) = (\lambda+1)(\lambda-1), && \varphi_3(\lambda) = (\lambda+2)^2(\lambda-1), \\ &\varphi_4(\lambda) = (\lambda+2)^2(\lambda-1)^2, && \varphi_5(\lambda) = (\lambda+1)^2, && \varphi_6(\lambda) = (\lambda+1)^2, \end{aligned}$$

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． □

9.1 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[20] 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 $(\alpha_1, \dots, \alpha_n)$ であるような対角行列を $\mathrm{diag}(\alpha_1, \dots, \alpha_n)$ 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 $\iff$ $AB = BA$.

[20] $M_n(K)$ 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.

[179] $P \in GL_n(K)$ のとき[21]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. □

[180] 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. □

[181] $A \in M_n(K)$ 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. □

[182] $m+n$ 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. □

[183] $m+n$ 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 $p_1, \dots, p_{m+n}$ 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

[21] $GL_n(K)$ 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[22]. 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. □

[184] $\alpha_1,\dots,\alpha_s\in K$ 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, 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:

$$J_n(\alpha)=\alpha E_n+J_n(0)=\begin{bmatrix}\alpha & 1 & & & 0\\ & \alpha & 1 & & \\ & & \alpha & \ddots & \\ & & & \ddots & 1\\ 0 & & & & \alpha\end{bmatrix},\qquad J_n(0)=\begin{bmatrix}0 & 1 & & & 0\\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1\\ 0 & & & & 0\end{bmatrix}.$$

[185] $A\in M_n(K)$ 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.

$$A=\sum_{k=0}^{n-1}a_kJ_n(0)^k=\begin{bmatrix}a_0 & a_1 & a_2 & \cdots & a_{n-1}\\ & a_0 & a_1 & \ddots & \vdots\\ & & a_0 & \ddots & a_2\\ & & & \ddots & a_1\\ 0 & & & & a_0\end{bmatrix},\qquad a_i\in K.\ \square$$

[22] 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. □

[186] $A, B \in M_n(K)$ 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. □

[187] (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 **[183]** と問題 **[184]** 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 **[184]** 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 **[184]** の B の形をしている. 問題 **[183]** 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. □

[188] 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 **[187]** 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 $P^{-1}AP = \operatorname{diag}(-1,-1,-2)$, $P^{-1}BP = \operatorname{diag}(-2,-2,-1)$. □

[189] (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 $v_1, \dots, v_k$ とし, それを K^n 全体の基底 $v_1, \dots, v_k, v_{k+1}, \dots, v_n$ 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 $Bq_1, \dots, Bq_k$ は $q_1, \dots, q_k$ 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 9.5 節にジャンプして構わない.

9.2 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[23]. この subsection は次の subsection への助走である[24].

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[25]:

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) $u+v = v+u$.

[23] 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.

[24] したがって説明は完璧ではない.

[25] 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[26]:

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[27]. 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 9.1 (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.

---

[26] 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.

[27] 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 9.2 (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[28],

$$\begin{aligned}&(\partial \circ a - a \circ \partial)f = \partial(af) - a(\partial f) = a'f + af' - af' = a'f,\\ &\therefore\ \partial \circ a - a \circ \partial = a'\end{aligned}$$

となり, ∂ と函数倍 a は作用素として一般に非可換になる[29]. 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 9.3 (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

$$f(x) = \int_0^1 \delta(y-x)f(y)\,dx$$

[28]面倒なので $\circ$ を書かない場合の方が多い.

[29]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[30]. $\square$

[190] (急減少 C^∞ 函数の空間) $\mathbb{R}$ 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 $m, n = 0, 1, 2, \dots$ 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[31]:

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

(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 $\left|\overline{f(x)}g(x)\right| \le |x|^{-2}$ 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.

---

[30] $\delta(y-x)$ 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 **[190]** 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.

[31] 内積の公理を満たしていることを示せ.

4. 多項式 $a_0, \dots, a_N \in \mathbb{C}[x]$ 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:

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

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. □

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[32].

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 9.4 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[33]. □

[191] 以上に登場した例のどれか 1 つを詳細に解説してみよ. □

[192] 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[34]. 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[35]:

$$\operatorname{Ker} f = f^{-1}(0) = \{\, u \in U \mid f(u) = 0 \,\}, \qquad \operatorname{Im} f = f(U) = \{\, f(u) \mid u \in U \,\}.$$

---

[32] 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.

[33] $\mathbb{R}$ 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.

[34] $[H, A] = HA - AH$ である.

[35] 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.

$\operatorname{Ker} f$, $\operatorname{Im} f$ はそれぞれ U, V の部分空間をなす[36].

[193] 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[37]: $n = \dim U$ 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 $u_1, \dots, u_k$ を取り, それに $u_{k+1}, \dots, u_n$ 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 $v_1, \dots, v_{n-k}$ は $\operatorname{Im} f$ の基底をなす. $\square$

ヒント 2: 準同型定理 $U/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$ より $\dim \operatorname{Im} f = \dim(U/\operatorname{Ker} f) = \dim U - \dim \operatorname{Ker} f$. $\square$

[194] 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

$$\sum_{i=1}^{s} \dim(\operatorname{Ker} f_i \cap \operatorname{Im}(f_{i-1} \circ \cdots \circ f_1)) = \dim \operatorname{Ker}(f_s \circ \cdots \circ f_1).$$

よって,

$$\sum_{i=1}^{s} \dim \operatorname{Ker} f_i \geq \dim \operatorname{Ker}(f_s \circ \cdots \circ f_1). \quad \square$$

結論の直観的な説明: 線形写像 $f_1, \dots, f_s$ 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 $\dim \operatorname{Ker}(f_s \circ \cdots \circ f_1)$ は各ステップで潰れる次元 $\dim(\operatorname{Ker} f_i \cap \operatorname{Im}(f_{i-1} \circ \cdots \circ f_1))$ の総和になる. $\operatorname{Im}(f_{i-1} \circ \cdots \circ f_1)$ は $f_{i-1} \circ \cdots \circ f_1$ でつぶした結果の像であり, $\operatorname{Ker} f_i$ 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 $\operatorname{Im}(f_{i-1} \circ \cdots \circ f_1)$ を $\operatorname{Ker} f_i \cap \operatorname{Im}(f_{i-1} \circ \cdots \circ f_1)$ の分だけ潰す.

[36] $\operatorname{Ker} f$ 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.

[37] 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.

ヒント: $g_i = f_i \circ \cdots \circ f_1$ ($g_0 = \mathrm{id}_{V_1}$) と置く. 問題 **[193]** 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. $\square$

9.3 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[38]. 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

$$V = \bigoplus_{\alpha \in K} V_\alpha = \bigoplus_{\alpha \in K} V(A;\alpha)$$

[38] 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.

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.

[195] 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 $\mathbb{F}_p = \{0,1,2,\dots,p-1\}$ になり, 同時固有空間はすべて無限次元になる. □

[196] $\mathbb{R}$ 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[39]:

$$\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} \overline{f(x)} g(x)\, dx \qquad \bigl(f, g, \in C^\infty(S^1)\bigr)$$

$\partial = d/dx$ 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. □

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[40]. 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 $\{n^2\}_{n \in \mathbb{Z}} = \{0,1,4,9,\dots\}$ 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. □

[39] 内積の公理を満たしていることをチェックせよ.

[40] 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.

[197] 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. $\alpha_1,\dots,\alpha_s\in K$ は A の相異なる固有値であり[41], 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 $\dim V_1+\cdots+\dim V_s\le\dim V$ である. □

ヒント: $v_1+\cdots+v_s=0$ の両辺に $E,A,A^2,\dots,A^{s-1}$ 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 $i=1,\dots,s$ 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 $\dim V_1+\cdots+\dim V_s\le\dim V$ である. □

[198] $A\in M_n(K)$ 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 $p_1,\dots,p_n$ 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 $p_{i,1},\dots,p_{i,n_i}$ 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[42]. 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 $i=1,\dots,s$ に関する和集合を $p_1,\dots,p_n$ 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. □

[199] 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 $P_\alpha v\ne 0$ 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:

$$V_\alpha=\operatorname{Im}P_\alpha,\qquad P_\alpha P_\beta=\delta_{\alpha,\beta}P_\alpha,\qquad \sum_{\alpha\in K}P_\alpha=\mathrm{id}_V,\qquad A=\sum_{\alpha\in K}\alpha P_\alpha.$$

[41] 相異なる固有値の**全体**でなくてもよい.

[42] $V_i\subset V(A;\alpha_i)$ 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 $j\ne i$ に対して $v_j=0$ となることであることがわかる.

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. □

[200] 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 $\mathrm{Im}\, P_\alpha$ 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 $v = \sum v_\alpha$ ($v_\alpha \in \mathrm{Im}\, P_\alpha$ 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, $\sum v_\beta = 0$ ($v_\beta \in \mathrm{Im}\, P_\beta$ 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 $V = \bigoplus \mathrm{Im}\, P_\alpha$ である. $V(A;\alpha) = \mathrm{Im}\, P_\alpha$ 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 $V(A;\alpha) = \mathrm{Im}\, P_\alpha$ 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**[43] (α,β) を持つ**同時固有ベクトル**と呼ぶ.

[43]「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.

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.

[**201**] 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. □

[**202**] $A,B \in M_n(K)$ 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 [**198**] と同様の議論で良い. □

[**203**] **(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 [**202**] を使えば問題 [**187**] 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.

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

$$BAv_{\alpha,\beta} = ABv_{\alpha,\beta} = A\beta v_{\alpha,\beta} = \beta Av_{\alpha,\beta}$$

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. □

[204] 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[44].

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. □

[205] 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 $\gamma_1^2,\ldots,\gamma_r^2$ $(\gamma_i \in \mathbb{R})$ 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,

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

[44] 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.

ヒント: (1) ${}^t\!AAq = \beta q$ とすると, $0 \le \langle Aq, Aq\rangle = \langle q, {}^t\!AAq\rangle = \beta\langle q, q\rangle$. (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,

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

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. □

[206] 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 **[205]** とまったく同じやり方. □

[207] (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 $z = re^{i\theta}$ $(r \in \mathbb{R}_{\ge 0}, \theta \in \mathbb{R}$ と表わされ, r は常に一意的であり, $z \ne 0$ 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 **[206]** 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 **[204]** 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 **[204]** の結果より H と U は可換になる. □

9.4 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[45]:

$$I_A = \{\, f \in K[\lambda] \mid f(A) = 0 \,\}.$$

このとき I_A は和と任意の多項式倍で閉じている.

[208] $I_A \neq 0$. □

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 $E, A, A^2, A^3, \dots$ は一次独立になる. よって n^2 次元の $M_n(K)$ が $E, A, A^2, A^3, \dots$ 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. □

[209] **(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[46]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. □

[210] 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. □

[211] $A \in M_n(K)$ 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 $f(A)=0 \iff f(PAP^{-1})=0$. □

[212] 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. □

[45] 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.
[46] 最高次の係数が 1 であるという意味.

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. □

[**213**] $A \in M_n(K)$ 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 [**210**] 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 [**138**] 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 $\varphi_A(\lambda)^n = p_A(\lambda)\det G(\lambda)$. □

[**214**] $\alpha, \beta, \gamma \in K$ 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[47]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.) □

[**215**] $\alpha_1, \dots, \alpha_s \in K$ 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 A の最小多項式は $\varphi(\lambda) = (\lambda - \alpha_1) \cdots (\lambda - \alpha_s)$ である. □

[47] 他の場合は簡単である.

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. □

[**216**] 次の n 次正方行列の最小多項式を求めよ:

$$J_n(\alpha)=\alpha E_n+J_m(0)=\begin{bmatrix}\alpha & 1 & & & 0\\ & \alpha & 1 & & \\ & & \alpha & \ddots & \\ & & & \ddots & 1\\ 0 & & & & \alpha\end{bmatrix}.\quad □$$

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. □

[**217**] **(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. □

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:

$$\begin{vmatrix}\lambda & -1 & & & 0\\ & \lambda & \ddots & & \\ & & \ddots & -1 & \\ 0 & & & \lambda & -1\\ a_{n-1} & a_{n-2} & \cdots & a_1 & \lambda-a_0\end{vmatrix}=\lambda\begin{vmatrix}\lambda & -1 & & 0\\ & \ddots & \ddots & \\ 0 & & \lambda & -1\\ a_{n-2} & \cdots & a_1 & \lambda-a_0\end{vmatrix}+(-1)^n a_n\begin{vmatrix}-1 & & & 0\\ \lambda & -1 & & \\ & \ddots & \ddots & \\ 0 & & \lambda & -1\end{vmatrix}.$$

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. □

[**218**] 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:

$$A=\begin{bmatrix}* & 1 & & 0\\ \vdots & \ddots & \ddots & \\ \vdots & & \ddots & 1\\ * & \cdots & \cdots & *\end{bmatrix}.\quad □$$

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. □

[**219**] 問題 [**218**] 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 [**217**] 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 $k=0,1,2,\dots$ に対して $(k+1,1),(k+2,2),\dots,(n,n-k)$ 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[48], $C_k=-a_kE_{n,n-k}$ と置くと $C_k\in V_k$ であり, コンパニオン行列 $C=C(a_0,\dots,a_{n-1})$ 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:

$$\begin{aligned} &[\Lambda,U_1]-C_0=-A_0,\\ &[\Lambda,U_2]-C_1=-A_0U_1-A_1+U_1C_0,\\ &[\Lambda,U_3]-C_2=-A_0U_2-A_1U_1-A_2+U_1C_1+U_2C_0,\\ &\qquad\qquad\cdots\cdots \end{aligned}$$

[48] (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.

$$[\Lambda, U_{n-1}] - C_{n-2} = -A_0 U_{n-2} - \cdots - A_{n-3}U_1 - A_{n-2} + U_1 C_{n-3} + \cdots + U_{n-3}C_0,$$
$$[\Lambda, U_n] - C_{n-1} = -A_0 U_{n-1} - \cdots - A_{n-2}U_1 - A_{n-1} + U_1 C_{n-2} + \cdots + U_{n-2}C_0.$$

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． □

[**220**] **(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 [**211**], [**215**] 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 [**194**] の結果より

$$\sum_{i=1}^{s} \dim \operatorname{Ker}(A - \alpha_i E) \geq \dim \operatorname{Ker} \varphi(A) = n.$$

A の固有値 α_i に対応する固有空間は $\operatorname{Ker}(A - \alpha_i E)$ に等しい．問題 [**197**] 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． □

[**221**] **(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． □

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 [**138**] 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 [**138**] 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． □

9.5 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 9.5 (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 8 節で特に詳しく説明した問題 [**32**] 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:

> $f_1, \dots, f_n \in K[\lambda]$ の最大公約元を $d \in K[\lambda]$ とすると, ある $a_1, \dots, a_n \in K[\lambda]$ で $d = a_1 f_1 + \cdots + a_n f_n$ を満たすものが存在する. □

[**222**] **(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 $\alpha_1, \dots, \alpha_s \in K$ 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 $f_1, \dots, f_s$ の最大公約多項式は 1 になる. よって問題 [**32**] の結果より, ある $a_1, \dots, a_s \in K[\lambda]$ 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 $u_1, \dots, u_n$ 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 $Nv_i = (A - \alpha_i E)v_i$ である．$P_i = p_i(A)$ と A は可換なので $Nv_i \in V_i$ 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 $m = \max\{m_1, \dots, m_s\}$ と置くと $N^m v = 0$.) □

[**223**] **(Jordan 分解の一意性)** Jordan 分解の一意性を証明せよ． □

ヒント: 問題 [**222**] 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 [**187**] より $S - S'$ も半単純になり, 問題 [**186**] より $N' - N$ も巾零になる．したがって, 問題 [**181**] より $S - S' = N' - N = 0$ である． □

[**224**] $A, B \in M_n(K)$ 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． □

[**225**] **(一般固有空間分解)** K^n は A の一般固有空間

$$W_A(\alpha_i) = \{\, v \in K^n \mid (A - \alpha_i E)^k v = 0 \ (\exists k \geq 0) \,\} \qquad (i = 1, \dots, s)$$

の直和に分解される．ここで $\alpha_1, \dots, \alpha_s$ 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 [**222**] 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[49]．$V_i \subset W_A(\alpha_i)$ 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.) □

[**226**] **(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． □

[49] 問題 [**222**] 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．

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 $p_1 = v, p_2, \dots, p_n$ 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. □

[227] (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 **[227]** の結果の逆を Toeplitz の定理と呼ぶ.

[228] (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 $p_1, \dots, p_n$ 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: **[226]** 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. □

[229] (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:

$$P^{-1}AP = \begin{bmatrix} \alpha_1 & * & \cdots & * & & & & & 0 \\ & \alpha_1 & \ddots & \vdots & & & & & \\ & & \ddots & * & & & & & \\ 0 & & & \alpha_1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & \ddots & & & \\ & & & & & & \alpha_s & * & \cdots & * \\ & & & & & & & \alpha_s & \ddots & \vdots \\ & & & & & & & & \ddots & * \\ 0 & & & & & & 0 & & & \alpha_s \end{bmatrix},$$

$$P^{-1}SP = \begin{bmatrix} \alpha_1 & & & & & & & & & 0 \\ & \alpha_1 & & & & & & & & \\ & & \ddots & & & & & & & \\ & & & \alpha_1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & \alpha_s & & & \\ & & & & & & & \alpha_s & & \\ & & & & & & & & \ddots & \\ 0 & & & & & & & & & \alpha_s \end{bmatrix},$$

$$P^{-1}NP = \begin{bmatrix} 0 & * & \cdots & * & & & & & & 0 \\ & 0 & \ddots & \vdots & & & & & & \\ & & \ddots & * & & & & & & \\ 0 & & & 0 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 0 & * & \cdots & * \\ & & & & & & & 0 & \ddots & \vdots \\ & & & & & & & & \ddots & * \\ 0 & & & & & & 0 & & & 0 \end{bmatrix}.$$

ここで, $\alpha_1, \dots, \alpha_s$ 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 [**184**] 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 [**182**] の結果より N_i たちも巾零になる. 問題 [**226**] もしくは (その一般化である問題 [**189**]) 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. $R_1, \dots, R_s$ 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[50]. □

[50] 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.

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」[**184**], 「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」[**182**], 「任意の正方行列は相似変換で上三角行列に変換できる」[**226**]. 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[51]. □

[**230**] $A \in M_n(K)$ 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 [**214**] 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.

[**231**] 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. $B=E-N+N^2-N^3+\cdots+(-1)^rN^r$ (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 9.6 (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. □

[**232**] 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 [**229**] 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.

[51] 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.

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.) □

9.6 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 $\alpha_1, \dots, \alpha_s$ 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 [**229**] 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:

$$A = \alpha E + N, \qquad N = \begin{bmatrix} 0 & a_{12} & \cdots & a_{1n} \\ & 0 & \ddots & \vdots \\ & & \ddots & a_{n-1,n} \\ \text{\Large 0} & & & 0 \end{bmatrix}.$$

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:

$$J_m(\alpha) := \begin{bmatrix} \alpha & 1 & & \text{\Large 0} \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ \text{\Large 0} & & & \alpha \end{bmatrix} = \alpha E_m + J_m(0), \qquad J_m(0) = \begin{bmatrix} 0 & 1 & & \text{\Large 0} \\ & 0 & \ddots & \\ & & \ddots & 1 \\ \text{\Large 0} & & & 0 \end{bmatrix}.$$

$J_m(\alpha)$ 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 9.7 (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 $J_{m_1}(0), \dots, J_{m_t}(0)$ 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 9.8 (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.

[**233**] Jordan 標準形の一歩手前 [**229**] の結果と巾零行列の標準形の存在 (定理 9.7 の一部) を仮定して, 正方行列の Jordan 標準形の存在 (定理 9.8 の一部) を証明せよ. □

ヒント: Jordan 標準形の一歩手前 [**229**] 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 9.8 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:

$$V_j = \operatorname{Ker} N^j = \{\, v \in V = K^n \mid N^j v = 0 \,\} \qquad (j = 0, 1, 2, \dots).$$

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[52]. 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[53]. そのとき W を $\{w_j\}_{j\in J}$ で張られる U の部分空間[54]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.

[**234**] 上の方の記号のもとで $j = 2, \dots, \nu$ 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. □

[52]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.

[53]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.

[54]$\sum_{j\in J} b_j w_j$ ($b_j \in K$ 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.

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 [**234**] の状況で X_j の基底を $x_1, \dots, x_p$ 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 $Nx_1, \dots, Nx_p, y_1, \dots, y_q$ と取り, V_{j-2} の基底を $N^2x_1, \dots, N^2x_p$, $Ny_1, \dots, Ny_q, z_1, \dots, z_r$ 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:

$$V_j \left\{ \begin{array}{l} \qquad\qquad\qquad x_1, \dots, x_p \\ V_{j-1} \left\{ \begin{array}{l} \qquad\quad Nx_1, \dots, Nx_p, \quad y_1, \dots, y_q \\ V_{j-2} \left\{ N^2x_1, \dots, N^2x_p,\ Ny_1, \dots, Ny_q,\ z_1, \dots, z_r \right. \end{array} \right. \end{array} \right.$$

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:

$$W_k = U_k + NU_k + \cdots + N^{k-1}U_k.$$

[**235**] 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 [**234**] 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 [**234**] 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 [**234**] 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[55]. $U_{\nu-2}$ 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 $u_{k1}, \dots, u_{k,t_k}$ 任意に取り, それらを次のような順番に並べる:

$$\begin{array}{l}
u_{11};\ \dots;\ u_{1t_1}; \\
Nu_{21}, u_{21};\ \cdots;\ Nu_{2t_2}, u_{2t_2}; \\
N^2u_{31}, Nu_{31}, u_{31};\ \cdots;\ N^2u_{3t_3}, Nu_{3t_3}, u_{3t_3}; \\
\qquad\qquad\cdots\cdots\cdots \\
N^{\nu-1}u_{\nu1}, \dots, N^2u_{\nu1}, Nu_{\nu1}, u_{\nu1};\ \cdots;\ N^{\nu-1}u_{\nu t_\nu}, \dots, N^2u_{\nu t_\nu}, Nu_{\nu t_\nu}, u_{\nu t_\nu}.
\end{array} \qquad (**)$$

問題 [**235**] よりこれらは V の基底をなす. これらの全体を $p_1, \dots, p_n$ と書き $P = [p_1\ \cdots\ p_n]$ と置く.

[**236**] 以上の構成のもとで $P^{-1}NP$ は定理 9.7 の意味で標準形になっている. □

ヒント: $(**)$ の $(u_{11};\cdots;N^{\nu-1}u_{\nu t_\nu}, \dots, Nu_{\nu t_\nu}, u_{\nu t_\nu})$ の部分列 $(N^{k-1}u_{ki}, \dots, Nu_{ki}, u_{ki})$ 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 $N^{k-1}u_{ki}, \dots, Nu_{ki}, u_{ki}$ に作用させると,

$$N[N^{k-1}u_{ki}\ \dots\ Nu_{ki}\ u_{ki}] = [N^{k-1}u_{ki}\ \dots\ Nu_{ki}\ u_{ki}] \begin{bmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}.$$

[55] 同型写像は直和を保つ.

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 9.7 の一部) が証明された. よって問題 **[233]** によって Jordan 標準形の存在 (定理 9.8 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.

[237] 巾零行列 $N \in M_n(K)$ の j 次の[56] Jordan 細胞の個数は

$$(\dim \operatorname{Ker} N^j - \dim \operatorname{Ker} N^{j-1}) - (\dim \operatorname{Ker} N^{j+1} - \dim \operatorname{Ker} N^j)$$

に等しい. 特に巾零 Jordan 細胞の全体 $(J_{m_1}(0), \dots, J_{m_t}(0))$ 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. □

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 9.7 (巾零行列の標準形の存在と一意性) が証明された.

[238] 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 $(J_{m_1}(\alpha_1), \dots, J_{m_t}(\alpha_t))$ 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 **[237]** 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 9.8 (正方行列の Jordan 標準形の存在と一意性) も証明された.

[56]「サイズが j の」という意味.

[**239**] 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 $ae^{2\pi ik/n}$ $(k = 0, 1, \dots, n-1)$ 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. $\square$

[**240**] 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[57]. 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 [**218**] 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[58]. 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 $e_1, \dots, e_p$ 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. $\square$

[**241**] 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[59]. $\square$

---

[57] 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.

[58] 実は問題 [**217**] の特殊な場合.

[59] $(ab)^p = a^p b^p$ 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.

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, $\binom{p}{1}, \dots, \binom{p}{p-1}$ 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[60]. □

[242] 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 $\alpha_1, \dots, \alpha_s$ 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:

(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. □

10 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

$$AX - XB = 0$$

[60] 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.

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,

$$\begin{aligned}\phi(aX + bY) &= A(aX + bY) - (aX + bY)B = aAX + bBY - aXB - bYB \\ &= a(AX - XB) + b(AY - YB) = a\phi(X) + b\phi(Y).\end{aligned}$$

[243] 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 $\operatorname{Im}\phi$ 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.

[244] $\alpha \neq \beta$, $A = J_m(\alpha)$, $B = J_n(\beta)$ 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 **[243]** 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 **[243]** の 3 より解の一意性が出る. $\dim \operatorname{Im} \phi = \dim M_{m,n}(K) - \dim \operatorname{Ker} \phi = \dim M_{m,n}(K)$ より ϕ は全射である. よって問題 **[243]** の 3 より解の存在が出る. □

[245] $A = J_m(\alpha)$, $B = J_n(\alpha)$ 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 $\operatorname{Ker}\phi$ 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. □

[246] $A=J_m(\alpha)$, $B=J_n(\alpha)$ であるとき以下が成立する:

1. $m\le n$ 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.

$$\begin{aligned}&c_{m1}=0,\\&c_{m-1,1}+c_{m2}=0,\\&\qquad\cdots\cdots\\&c_{21}+\cdots+c_{m,m-1}=0,\\&c_{11}+c_{22}+\cdots+c_{mm}=0.\end{aligned}$$

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. $m\ge n$ 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.

$$\begin{aligned}&c_{m1}=0,\\&c_{m-1,1}+c_{m2}=0,\\&\qquad\cdots\cdots\\&c_{m-n+2,1}+\cdots+c_{m,n-1}=0,\\&c_{m-n+1,1}+c_{m-n+2,2}+\cdots+c_{mn}=0.\end{aligned}$$

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 $\operatorname{Im}\phi$ 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. □

[247] $A\in M_m(K)$ 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 [**244**] 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. □

[**248**] $m = n$ 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[61].

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 [**242**] 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 [**244**], [**245**] 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:

$$\begin{aligned} &J_p(\alpha)P - PJ_p(\alpha) = 0, \quad J_p(\alpha)Q - QJ_q(\beta) = 0, \\ &J_q(\beta)R - RJ_p(\alpha) = 0, \quad J_q(\beta)S - SJ_q(\beta) = 0. \end{aligned}$$

$\alpha \neq \beta$ ならば問題 [**244**] の結果より $Q = 0$, $R = 0$ であり, 問題 [**245**] 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 [**245**] 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. □

[**249**] $m = n$ 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. □

[61] $[A, X] = AX - XA$ 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. □

参考文献

[Dirac] ディラック, P. A. M.: 量子力学, 原書第 4 版, 朝永振一郎他共訳, 岩波書店, 1968

[Infeld] インフェルト, L.: ガロアの生涯—神々の愛でし人市井三郎訳, 日本評論社, 新版第 3 版, 1996

[韓・伊理] 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

[佐武] 佐武一郎: 線型代数学, 裳華房数学選書 1, 324 頁.

[杉浦] 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

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

[堀田 2] 堀田良之: 加群十話 — 代数学入門, 朝倉書店, すうがくぶっくす 3, 186 頁.

[横田] 横田一郎: 群と位相, 裳華房, 基礎数学選書 5

[山内・杉浦] 山内恭彦, 杉浦光雄: 連続群論入門, 培風館, 新数学シリーズ 18

[失業率] 労働力調査　長期時系列データ
`http://www.stat.go.jp/howto/case1/01.htm`
から「第 3 表 (3) 年齢階級 (5 歳階級), 男女別完全失業者数及び完全失業率」
`http://www.stat.go.jp/data/roudou/longtime/zuhyou/lt03-03.xls`
をダウンロード

[GDP] 平成 15 年度国民経済計算
`http://www.esri.cao.go.jp/jp/sna/h17-nenpou/17annual-report-j.html`
から「4. 主要系列表（3）経済活動別国内総生産　実質暦年」
`http://www.esri.cao.go.jp/jp/sna/h17-nenpou/80fcm3r_jp.xls`
をダウンロード