２００９年１１月１０日改訂

第9章

標準形の応用

9.1　行列の指数関数

e を自然対数の底とする．微分積分学で学んだように, 任意の実数 x に対してテイラー展開

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^k}{k!} + \cdots$$

が成り立つ．複素数 $z = x + yi$ についても級数

$$\sum_{k=0}^{\infty} \frac{z^k}{k!} = 1 + z + \frac{z^2}{2!} + \cdots + \frac{z^k}{k!} + \cdots$$

が収束して

$$e^x(\cos y + i \sin y) \tag{9.1}$$

に等しいことが示せる (問9.2)．このことを踏まえて (9.1) によって $e^z = e^{x+iy}$ を定義した (オイラーの公式) のであった．この節では, この定義を一般の複素正方行列に対して拡張する．

そのためには, “行列の列” に対して収束と発散の概念を定義しなければならない．A_k $(k = 1, 2, \ldots)$ を (m, n) 型行列とする．これらの全体を $\{A_k\}$ で表

して行列の列と考える．A_k を成分で表して $A_k = \left(a_{ij}^{(k)}\right)$ とおく．ある (m,n) 型行列 $A = (a_{ij})$ が存在して，

$$\lim_{k\to\infty} a_{ij}^{(k)} = a_{ij} \quad (1 \leqq i \leqq m,\ 1 \leqq j \leqq n)$$

が成り立つとき，$\{A_k\}$ は**収束**するといい，

$$\lim_{k\to\infty} A_k = A$$

で表す．このとき，A を $\{A_k\}$ の**極限**という．極限は存在すればだだ 1 つに定まる．$\{A_k\}$ が収束しないとき，$\{A_k\}$ は**発散**するという．

(m,n) 型行列 $A = (a_{ij})$ に対して

$$\|A\| = \max_{1\leqq i\leqq m,\ 1\leqq j\leqq n} |a_{ij}|$$

とおく．$\lim_{k\to\infty} A_k = A$ であるためには，$\lim_{k\to\infty} \|A_k - A\| = 0$ が成り立つことが必要十分である．

問 9.1. 次の行列 A に対して $\lim_{k\to\infty} A^k$ が存在するか否かを判定し，存在するならばそれを求めよ．ただし，A のジョルダン標準形を $J = P^{-1}AP$ とすると $J^k = P^{-1}A^kP$ であることに注意せよ．

1) $\begin{pmatrix} -1 & 1 & 3 \\ 0 & 1 & 6 \\ -1 & 1 & -1 \end{pmatrix}$　2) $\begin{pmatrix} \frac{1}{12} & \frac{1}{12} & -\frac{1}{12} \\ \frac{11}{12} & -\frac{1}{12} & \frac{1}{12} \\ \frac{1}{3} & \frac{1}{3} & \frac{2}{3} \end{pmatrix}$　3) $\begin{pmatrix} \frac{3}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$

命題 9.1.1. 1) $\|A\| \geqq 0$. 等号が成り立つのは $A = O$ のときに限る．

2) $\|cA\| = |c|\|A\|$　$(c \in \boldsymbol{C})$.

3) $\|A + B\| \leqq \|A\| + \|B\|$.

証明　3) のみ示す．$A = (a_{ij})$, $B = (b_{ij})$ とする．各 i, j に対して

$$|a_{ij} + b_{ij}| \leqq |a_{ij}| + |b_{ij}| \leqq \|A\| + \|B\|$$

が成り立つことによる．　□

命題 9.1.2. 1) A, B をそれぞれ (m,n) 型および (n,p) 型行列とすると, $\|AB\| \leqq n\|A\|\|B\|$ が成り立つ.
2) A を n 次正方行列とすると, 任意の自然数 k に対して, $\|A^k\| \leqq n^{k-1}\|A\|^k$ が成り立つ.

証明 1) AB の各 (i,j) 成分について

$$\left|\sum_{l=1}^{n} a_{il}b_{lj}\right| \leqq \sum_{l=1}^{n} |a_{il}| \cdot |b_{lj}| \leqq n\|A\|\|B\|$$

が成り立つことによる.
2) $k = 1$ の場合は自明. $k \geqq 2$ のときは 1) より $\|A^k\| = \|AA^{k-1}\| \leqq n\|A\|\|A^{k-1}\|$ が成り立つので, 数学的帰納法によって示される. □

同じ型の行列 A_k $(k = 1, 2, \ldots)$ に対して, $\sum_{k=1}^{\infty} A_k$ の形の式を行列の**無限級数**という. $S_n = \sum_{k=1}^{n} A_k$ とおき, $\lim_{n\to\infty} S_n = S$ が存在するとき, 無限級数 $\sum_{k=1}^{\infty} A_k$ は S に**収束**する, または**和**が S であるといい, $\sum_{k=1}^{\infty} A_k = S$ と表す. $\{S_n\}$ が発散するとき, $\sum_{k=1}^{\infty} A_k$ は**発散**するという.

n 次正方行列 A に対して級数

$$\sum_{k=0}^{\infty} \frac{A^k}{k!} = I + A + \frac{A^2}{2!} + \cdots + \frac{A^k}{k!} + \cdots \tag{9.2}$$

が収束することを証明しよう. $\dfrac{A^k}{k!}$ の (i,j) 成分を $a_{ij}^{(k)}$ とおくと, 命題 9.1.2 の 2) より

$$\left|a_{ij}^{(k)}\right| \leqq \frac{1}{k!}n^{k-1}\|A\|^k$$

が成り立つ. ここで級数

$$\sum_{k=0}^{\infty} \frac{1}{k!}n^{k-1}\|A\|^k = \frac{1}{n}\sum_{k=0}^{\infty} \frac{1}{k!}n^k\|A\|^k = \frac{1}{n}e^{n\|A\|}$$

は収束するので, $\sum_{k=1}^{\infty} a_{ij}^{(k)}$ も収束する[1]. 行列の級数の和 (9.2) を行列の**指数関数**と呼び, e^A あるいは $\exp A$ で表す.

命題 9.1.3. 1) $\exp O = I$.

2) P を正則行列とすると, $\exp(P^{-1}AP) = P^{-1}(\exp A)P$.

3) $\det(\exp A) = e^{\mathrm{tr}A}$, とくに $\exp A$ は正則である.

証明 1) は自明. 2) は $(P^{-1}AP)^k = P^{-1}A^kP$ による.

3) A は n 次とする. A の固有値を重複度をこめて $\lambda_1, \lambda_2, \ldots, \lambda_n$ とすると, フロベニウスの定理 (定理 6.3.9) の証明と同様にして, $\exp A$ の固有値は重複度をこめて $e^{\lambda_1}, e^{\lambda_2}, \ldots, e^{\lambda_n}$ であることが示せる. したがって命題 6.2.3 の 1) と 2) より, 次のことが成り立つ.

$$\det(\exp A) = e^{\lambda_1}e^{\lambda_2}\cdots e^{\lambda_n} = e^{\lambda_1+\lambda_2+\cdots+\lambda_n} = e^{\mathrm{tr}A}.$$

$e^{\mathrm{tr}A} \neq 0$ であるから, $\exp A$ は正則である. □

定理 9.1.4. $AB = BA$ ならば $\exp(A+B) = \exp A \exp B$.

証明 $S_k = \sum_{r=0}^{k} \frac{1}{r!}(A+B)^r$, $S_k' = \sum_{s=0}^{k} \frac{1}{s!}A^s$, $S_k'' = \sum_{t=0}^{k} \frac{1}{t!}B^t$ とおく. 仮定より $AB = BA$ であるから, 数の場合と同様に 2 項定理が成り立つ. すなわち

$$(A+B)^r = \sum_{s=0}^{r} \binom{r}{s} A^sB^{r-s} = r! \sum_{s+t=r} \frac{1}{s!t!}A^sB^t$$

である. ゆえに, 次の式が成り立つ.

$$\begin{aligned} S_{2k} - S_k'S_k'' &= \sum_{s+t\leqq 2k} \frac{1}{s!t!}A^sB^t - \left(\sum_{s=0}^{k}\frac{1}{s!}A^s\right)\left(\sum_{t=0}^{k}\frac{1}{t!}B^t\right) \\ &= \sum \frac{1}{s!t!}A^sB^t. \end{aligned}$$

ただし, 最後の和において (s,t) は

$$s+t \leqq 2k, \qquad \max\{s,t\} > k \tag{9.3}$$

[1] 各 k に対して $|a_k| \leqq |b_k|$ であって $\sum |b_k|$ が収束すれば, $\sum a_k$ も収束する. 微分積分学の教科書を参照せよ.

の範囲を動く. この範囲に (s,t) は $k(k+1)$ 個存在する. 命題 9.1.2 の 2) より

$$\frac{1}{s!t!}\|A^sB^t\| \leqq \frac{1}{s!t!}n^{s+t-1}\|A\|^s\|B\|^t$$

が成り立つ. ゆえに, $M=\max\{1,\|A\|,\|B\|\}$ とおくと, (9.3) の範囲の (s,t) に対して

$$\frac{1}{s!t!}\|A^sB^t\| \leqq \frac{1}{(k+1)!}(nM)^{2k}$$

が成り立つ. したがって

$$\|S_{2k}-S'_kS''_k\| \leqq k(k+1)\frac{(nM)^{2k}}{(k+1)!} = \frac{(nM)^{2k}}{(k-1)!}$$

を得る. ここに $\lim_{k\to\infty}\dfrac{(nM)^{2k}}{(k-1)!}=0$ であるから, $\lim_{k\to\infty}\|S_{2k}-S'_kS''_k\|=0$ である. また命題 9.1.1 の 3) より

$$\begin{aligned}&\|\exp(A+B)-\exp A\exp B\|\\ \leqq\ &\|\exp(A+B)-S_{2k}\|+\|S_{2k}-S'_kS''_k\|+\|S'_kS''_k-\exp A\exp B\|\end{aligned}$$

である. 定義より $\lim_{k\to\infty}S_{2k}=\exp(A+B)$ であり, $\lim_{k\to\infty}S'_k=\exp A$, $\lim_{k\to\infty}S''_k=\exp B$ より $\lim_{k\to\infty}S'_kS''_k=\exp A\exp B$ である. したがって, $\exp(A+B)=\exp A\exp B$ が成り立つ. □

任意の実数 t と正方行列 A に対して

$$\exp(tA)=\sum_{k=0}^{\infty}\frac{t^k}{k!}A^k = I+tA+\frac{t^2}{2!}A^2+\cdots+\frac{t^k}{k!}A^k+\cdots$$

が定義される. 定理より次が成り立つ.

系 9.1.5. 1) $\exp(-A)=(\exp A)^{-1}$.

2) $\exp(sA)\exp(tA)=\exp(s+t)A \quad (s,\,t\in\boldsymbol{R})$.

問 9.2. 複素数 $z=x+iy$ に対して

$$\sum_{n=0}^{\infty}\frac{z^n}{n!}=e^x(\cos y+i\sin y)$$

が成り立つことを示せ.

問 9.3. 次の行列 A に対して A^n と $\exp A$ を求めよ.

1) $\begin{pmatrix} 1 & 0 & 4 \\ 2 & 4 & -3 \\ -2 & -1 & 6 \end{pmatrix}$ 2) $\begin{pmatrix} 4 & 1 & -2 \\ 2 & 4 & -3 \\ 4 & 2 & -2 \end{pmatrix}$

成分 $a_{ij}(t)$ $(1 \leqq i \leqq m,\ 1 \leqq j \leqq n)$ が $t \in \boldsymbol{R}$ に関する関数である, (m,n) 型行列 $A(t) = (a_{ij}(t))$ を考える. 各成分 $a_{ij}(t)$ が微分可能のとき, $A(t)$ は**微分可能**であるという. このとき, $a'_{ij}(t)$ を成分とする行列 $(a'_{ij}(t))$ を $A(t)$ の**導関数**といい, $A'(t)$ または $\dfrac{d}{dt}A(t)$ で表す. もちろん

$$A'(a) = \lim_{t \to a} \frac{A(t) - A(a)}{t - a}$$

が成り立つ.

収束するベキ級数は微分可能で項別微分可能であるから[2)],

$$\begin{aligned} \frac{d}{dt}\exp(tA) &= \sum_{k=1}^{\infty} \frac{t^{k-1}}{(k-1)!}A^k = A + tA^2 + \cdots + \frac{t^{k-1}}{(k-1)!}A^k + \cdots \\ &= A\exp(tA) = \exp(tA)A \end{aligned} \tag{9.4}$$

が成り立つ.

問 9.4. $A(t)$, $B(t)$ は n 次正方行列で微分可能とする. 次を示せ.

1) $\dfrac{d}{dt}(A(t)B(t)) = \dfrac{d}{dt}A(t)\cdot B(t) + A(t)\cdot\dfrac{d}{dt}B(t)$.

2) $A(t)$ が正則ならば, $\dfrac{d}{dt}A(t)^{-1} = -A(t)^{-1}\cdot\dfrac{d}{dt}A(t)\cdot A(t)^{-1}$.

$\exp(tA)$ を求めよう. まず A がジョルダン細胞 $J(\lambda, m)$ の場合を考える. $J(0,m) = N$ とおくと, $J(\lambda,m) = \lambda I + N$ がなりたつ. すなわち,

$$J(\lambda,m) = \begin{pmatrix} \lambda & & & & \\ & \lambda & & & \\ & & \ddots & & \\ & & & \lambda & \\ & & & & \lambda \end{pmatrix} + \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix} = \lambda I + N.$$

[2)] 微分積分学の教科書を参照せよ.

N^k は $k < m$ のときは対角線の k 行上の斜線上の成分が 1 で他の成分が 0 の行列であり, $k \geqq m$ のときは $N^k = O$ であることを思いだそう. したがって,

$$J(\lambda, m)^n = \sum_{k=0}^{m-1} \binom{n}{k} \lambda^{n-k} N^k \tag{9.5}$$

である. ただし, $k > n$ のときは $\binom{n}{k} = 0$ とする. よって,

$$\begin{aligned}
\exp(tJ(\lambda, m)) &= \sum_{n=0}^{\infty} \frac{t^n}{n!} J(\lambda, m)^n \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{m-1} \frac{t^n}{k!(n-k)!} \lambda^{n-k} N^k \\
&= \sum_{k=0}^{m-1} \frac{t^k}{k!} \left(\sum_{n=0}^{\infty} \frac{t^n}{n!} \lambda^n \right) N^k \\
&= \sum_{k=0}^{m-1} \frac{t^k}{k!} e^{t\lambda} N^k.
\end{aligned}$$

すなわち,

$$\exp(tJ(\lambda, m)) = \begin{pmatrix}
e^{t\lambda} & te^{t\lambda} & \frac{t^2}{2!}e^{t\lambda} & \cdots & \frac{t^{m-1}}{(m-1)!}e^{t\lambda} \\
0 & e^{t\lambda} & te^{t\lambda} & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \frac{t^2}{2!}e^{t\lambda} \\
\vdots & & \ddots & \ddots & te^{t\lambda} \\
0 & \cdots & 0 & 0 & e^{t\lambda}
\end{pmatrix} \tag{9.6}$$

である.

一般のジョルダン行列 J に対しても同様にして $\exp(tJ)$ を計算できる. よって, $\exp(tA) = P(\exp t(J))P^{-1}$ (命題 9.1.3 の 2) による) を使って $\exp(tA)$ を計算出来る.

9.2 線形微分方程式

9.2.1 一般の 1 階連立線形微分方程式

実変数 t の n 個の複素数値関数 $x_1(t)$, $x_2(t)$, …, $x_n(t)$ を未知関数とする,

$$\begin{cases} \dfrac{d}{dt}x_1(t) = a_{11}(t)x_1(t) + a_{12}(t)x_2(t) + \cdots + a_{1n}(t)x_n(t) + b_1(t), \\ \dfrac{d}{dt}x_2(t) = a_{21}(t)x_1(t) + a_{22}(t)x_2(t) + \cdots + a_{2n}(t)x_n(t) + b_2(t), \\ \qquad\qquad \vdots \\ \dfrac{d}{dt}x_n(t) = a_{n1}(t)x_1(t) + a_{n2}(t)x_2(t) + \cdots + a_{nn}(t)x_n(t) + b_n(t) \end{cases}$$

という形の微分方程式を **1 階連立線形微分方程式**という. ただし, $a_{ij}(t)$ $(1 \leqq i,\ j \leqq n)$, $b_i(t)$ $(1 \leqq i \leqq n)$ は $\boldsymbol{R}$ 上で定義された複素数値連続関数とする.

$$A(t) = \begin{pmatrix} a_{11}(t) & a_{12}(t) & \cdots & a_{1n}(t) \\ a_{21}(t) & a_{22}(t) & \cdots & a_{2n}(t) \\ \vdots & \vdots & & \vdots \\ a_{n1}(t) & a_{n2}(t) & \cdots & a_{nn}(t) \end{pmatrix}, \quad \boldsymbol{b}(t) = \begin{pmatrix} b_1(t) \\ b_2(t) \\ \vdots \\ b_n(t) \end{pmatrix}, \quad \boldsymbol{x}(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_n(t) \end{pmatrix}$$

とおけば, 上の連立微分方程式は

$$\frac{d}{dt}\boldsymbol{x}(t) = A(t)\boldsymbol{x}(t) + \boldsymbol{b}(t) \tag{9.7}$$

と表せる. 微分方程式の理論の基礎となるのは, 解の存在と一意性を保証する次の定理である. 証明は微分方程式の教科書を参照せよ.

定理 9.2.1. 任意の $t_0 \in \boldsymbol{R}$ と c_1, c_2, …, $c_n \in \boldsymbol{C}$ に対して, **初期条件**

$$x_i(t_0) = c_i \quad (1 \leqq i \leqq n) \tag{9.8}$$

を満たす (9.7) の解 $\boldsymbol{x}(t)$ が存在する. また, $\boldsymbol{x}_1(t)$, $\boldsymbol{x}_2(t)$ をともに初期条件 (9.8) を満たす (9.7) の解とすると, $\boldsymbol{x}_1(t)$, $\boldsymbol{x}_2(t)$ は恒等的に相等しい.

(9.7) において $\boldsymbol{b}(t) = \boldsymbol{0}$ である場合

$$\frac{d}{dt}\boldsymbol{x}(t) = A(t)\boldsymbol{x}(t) \tag{9.9}$$

を**斉次方程式**という. $c \in \boldsymbol{C}$ とする. $\boldsymbol{x}_1(t)$, $\boldsymbol{x}_2(t)$ がともに (9.9) を満たすとき, $\boldsymbol{x}_1(t) + \boldsymbol{x}_2(t)$, $c\boldsymbol{x}_1(t)$ は再び (9.9) を満たす. これらを和およびスカラー倍として定義すると, 4 章冒頭の (4.1), (4.2), (4.5), (4.6), (4.7), (4.8) が成り立つ. また, t によらずに恒等的に $\mathbf{0}$ であるベクトル (これも同じ $\mathbf{0}$ で表す) は (4.3) を満たす. また, $-\boldsymbol{x}_1(t)$ は $\boldsymbol{x}_1(t)$ の逆ベクトルになって (4.4) が成り立つ. したがって, (9.9) を満たす $\boldsymbol{x}(t)$ の全体を V とおくと, V は抽象的ベクトル空間の意味で複素ベクトル空間である. $\boldsymbol{x}_0(t)$ を (9.7) の 1 つの解 (**特殊解**という) とすれば, 次が成り立つ.

定理 9.2.2. (9.7) の任意の解 (**一般解**という) は, $\boldsymbol{x}_0(t)$ に (9.9) の解を加えることによって得られる.

問 9.5. 定理 9.2.2 を証明せよ.

以下, (9.9) の解空間 V について考察する. $\boldsymbol{x}_1(t)$, $\boldsymbol{x}_2(t)$, ..., $\boldsymbol{x}_n(t)$ を (9.9) の解とする.

$$\boldsymbol{x}_j(t) = \begin{pmatrix} x_{1j}(t) \\ x_{2j}(t) \\ \vdots \\ x_{nj}(t) \end{pmatrix} \quad (1 \leqq j \leqq n)$$

と成分で表し, 行列式

$$|\, \boldsymbol{x}_1(t)\ \boldsymbol{x}_2(t)\ \cdots\ \boldsymbol{x}_n(t)\,| = \begin{vmatrix} x_{11}(t) & x_{12}(t) & \cdots & x_{1n}(t) \\ x_{21}(t) & x_{22}(t) & \cdots & x_{2n}(t) \\ \vdots & \vdots & & \vdots \\ x_{n1}(t) & x_{n2}(t) & \cdots & x_{nn}(t) \end{vmatrix}$$

を $W(t)$ とおく. $W(t)$ を $\boldsymbol{x}_1(t)$, $\boldsymbol{x}_2(t)$, ..., $\boldsymbol{x}_n(t)$ の**ロンスキー行列式**という.

定理 9.2.3. $A(t)$ のトレース $\sum_{i=1}^{n} a_{ii}(t)$ を $\operatorname{tr} A(t)$ で表せば,

$$W(t) = W(t_0) \exp\left(\int_{t_0}^{t} \operatorname{tr} A(t) dt \right)$$

が成り立つ. ただし, x が数の場合にも e^x を $\exp(x)$ で表す (とくに, x が複雑な式の場合).

証明　練習問題 3.12 と同様にして

$$\frac{d}{dt}W(t)=\sum_{i=1}^{n}\begin{vmatrix} x_{11}(t) & x_{12}(t) & \cdots & x_{1n}(t)\\ \vdots & \vdots & & \vdots\\ x'_{i1}(t) & x'_{i2}(t) & \cdots & x'_{in}(t)\\ \vdots & \vdots & & \vdots\\ x_{n1}(t) & x_{n2}(t) & \cdots & x_{nn}(t)\end{vmatrix} \tag{9.10}$$

が成り立つ. ただし, $x'_{ij}(t)$ は $\dfrac{d}{dt}x_{ij}(t)$ を表す. $\boldsymbol{x}_j(t)$ $(1 \leqq j \leqq n)$ は (9.9) の解であるから,

$$x'_{ij}(t)=\sum_{k=1}^{n}a_{ik}(t)x_{kj}(t) \quad (1 \leqq i,\ j \leqq n)$$

が成り立つ. したがって, (9.10) の右辺の第 1 項の第 1 行は

$$\begin{aligned}&(x'_{11}(t),x'_{12}(t),\ldots,x'_{1n}(t))\\ =&\left(\sum_{k=1}^{n}a_{1k}(t)x_{k1}(t),\sum_{k=1}^{n}a_{1k}(t)x_{k2}(t),\ldots,\sum_{k=1}^{n}a_{1k}(t)x_{kn}(t)\right)\\ =&a_{11}(t)(x_{11}(t),x_{12}(t),\ldots,x_{1n}(t))+a_{12}(t)(x_{21}(t),x_{22}(t),\ldots,x_{2n}(t))\\ &+\cdots+a_{1n}(t)(x_{n1}(t),x_{n2}(t),\ldots,x_{nn}(t))\end{aligned}$$

に等しい. したがって, (9.10) の右辺の第 1 項は

$$a_{11}(t)\begin{vmatrix} x_{11}(t) & x_{12}(t) & \cdots & x_{1n}(t)\\ x_{21}(t) & x_{22}(t) & \cdots & x_{2n}(t)\\ \vdots & \vdots & & \vdots\\ x_{n1}(t) & x_{n2}(t) & \cdots & x_{nn}(t)\end{vmatrix}+a_{12}(t)\begin{vmatrix} x_{21}(t) & x_{22}(t) & \cdots & x_{2n}(t)\\ x_{21}(t) & x_{22}(t) & \cdots & x_{2n}(t)\\ \vdots & \vdots & & \vdots\\ x_{n1}(t) & x_{n2}(t) & \cdots & x_{nn}(t)\end{vmatrix}$$

$$+\cdots+a_{1n}(t)\begin{vmatrix} x_{n1}(t) & x_{n2}(t) & \cdots & x_{nn}(t)\\ x_{21}(t) & x_{22}(t) & \cdots & x_{2n}(t)\\ \vdots & \vdots & & \vdots\\ x_{n1}(t) & x_{n2}(t) & \cdots & x_{nn}(t)\end{vmatrix}$$

に等しい. ところが, この式の第 2 項から後は (同じ行が 2 つ現れるので) 0 である. よって, 最初の項だけ残って, (9.10) の右辺の第 1 項は

$$a_{11}(t)W(t)$$

に等しいことが分かる.

同様にして (9.10) の右辺の第 i 項は $a_{ii}(t)W(t)$ に等しいので $(1 \leqq i \leqq n)$,

$$\frac{d}{dt}W(t) = \sum_{i=1}^{n} a_{ii}(t) \cdot W(t) = \operatorname{tr} A(t) \cdot W(t) \tag{9.11}$$

が成り立つ. ここで,

$$f(t) = W(t_0) \exp\left(\int_{t_0}^{t} \operatorname{tr} A(t)dt\right)$$

とおくと, $f(t)$ は $W(t)$ と同じ微分方程式 (9.11) と初期条件 $f(t_0) = W(t_0)$ を満たすので, 解の一意性により $W(t) = f(t)$ が成り立つ. □

系 9.2.4. ある $t_0 \in \boldsymbol{R}$ に対して $W(t_0) \neq 0$ であれば, 任意の $t \in \boldsymbol{R}$ に対して $W(t) \neq 0$ である.

$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n \in \boldsymbol{C}^n$ を 1 次独立なベクトルとする. また, $\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \ldots, \boldsymbol{x}_n(t)$ を初期条件

$$\boldsymbol{x}_i(t_0) = \boldsymbol{a}_i \quad (1 \leqq i \leqq n)$$

を満たす (9.9) の解とする. このとき, 任意の $t \in \boldsymbol{R}$ に対して $\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \ldots, \boldsymbol{x}_n(t)$ は 1 次独立である. $\boldsymbol{x}(t)$ を (9.9) の 1 つの解とすると,

$$\boldsymbol{x}(t) = c_1\boldsymbol{x}_1(t) + c_2\boldsymbol{x}_2(t) + \cdots + c_n\boldsymbol{x}_n(t) \quad (t \in \boldsymbol{R})$$

を満たす定数 $c_i \in \boldsymbol{C}$ $(1 \leqq i \leqq n)$ が一意的に定まる (練習問題 9.5). この意味で, $\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \ldots, \boldsymbol{x}_n(t)$ を (9.9) の解空間 V の**基底**という.

例 9.2.5 (定数変化法). 次に方程式 $\boldsymbol{x}'(t) = A(t)\boldsymbol{x}(t) + \boldsymbol{b}(t)$ の解について考察する. 斉次方程式 $\boldsymbol{x}'(t) = A(t)\boldsymbol{x}(t)$ の解空間の基底を $\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \ldots, \boldsymbol{x}_n(t)$ とする. これらの 1 次結合

$$\boldsymbol{x}(t) = c_1(t)\boldsymbol{x}_1(t) + c_2(t)\boldsymbol{x}_2(t) + \cdots + c_n(t)\boldsymbol{x}_n(t)$$

として $\boldsymbol{x}'(t) = A(t)\boldsymbol{x}(t) + \boldsymbol{b}(t)$ の解を求めよう. ただし, ここでは係数 $c_i(t)$ $(1 \leqq i \leqq n)$ は定数ではなく, t の値によって変化する関数である.

$$\begin{aligned}\boldsymbol{x}'(t) &= \sum_{i=1}^{n} c_i'(t)\boldsymbol{x}_i(t) + \sum_{i=1}^{n} c_i(t)\boldsymbol{x}_i'(t) \\ &= \sum_{i=1}^{n} c_i'(t)\boldsymbol{x}_i(t) + \sum_{i=1}^{n} c_i(t)A(t)\boldsymbol{x}_i(t) \\ &= \sum_{i=1}^{n} c_i'(t)\boldsymbol{x}_i(t) + A(t)\boldsymbol{x}(t)\end{aligned}$$

であるから, $\boldsymbol{x}'(t) = A(t)\boldsymbol{x}(t) + \boldsymbol{b}(t)$ が成り立つための条件は

$$\boldsymbol{c}(t) = \begin{pmatrix} c_1(t) \\ c_2(t) \\ \vdots \\ c_n(t) \end{pmatrix}$$

とおいて,

$$(\boldsymbol{x}_1(t)\ \boldsymbol{x}_2(t)\ \cdots\ \boldsymbol{x}_n(t))\,\boldsymbol{c}'(t) = \sum_{i=1}^{n} c_i'(t)\boldsymbol{x}_i(t) = \boldsymbol{b}(t)$$

と表せる. 行列 $X(t) = (\boldsymbol{x}_1(t)\ \boldsymbol{x}_2(t)\ \cdots\ \boldsymbol{x}_n(t))$ は常に正則であるから, 両辺に $X(t)^{-1}$ をかけて

$$\boldsymbol{c}'(t) = X(t)^{-1}\boldsymbol{b}(t)$$

を得る. したがって, 両辺を積分して (ベクトルの積分は成分ごとの積分のこととする)

$$\boldsymbol{c}(t) = \int_{t_0}^{t} X(t)^{-1}\boldsymbol{b}(t)dt$$

が求めるものである.

9.2.2 定数係数の 1 階連立線形微分方程式

連立微分方程式 (9.9) の各係数 $a_{ij}(t)$ $(1 \leqq i,\ j \leqq n)$ が定数の場合には, 解を具体的に求めることができる.

$A = (a_{ij})$ を数行列として,

$$\frac{d}{dt}\boldsymbol{x}(t) = A\boldsymbol{x}(t) \tag{9.12}$$

について考える.

定理 9.2.6. $\boldsymbol{c} \in \boldsymbol{C}^n$ とする. 初期条件 $\boldsymbol{x}(0) = \boldsymbol{c}$ を満たす (9.12) の解は

$$\boldsymbol{x}(t) = \exp(tA)\boldsymbol{c}$$

である.

証明 $\boldsymbol{x}(t) = \exp(tA)\boldsymbol{c}$ とおけば,

$$\frac{d}{dt}\boldsymbol{x}(t) = \left(\frac{d}{dt}\exp(tA)\right)\boldsymbol{c} = A\exp(tA)\boldsymbol{c} = A\boldsymbol{x}(t)$$

である (2 番目の等号は (9.4) による). また, $t = 0$ とすると $\exp(0A) = \exp O = I$ であるから, $\boldsymbol{x}(t)$ の初期値 $\boldsymbol{x}(0)$ は $\boldsymbol{c}$ に一致する. 逆に, 初期条件 $\boldsymbol{x}(0) = \boldsymbol{c}$ を満たす (9.12) の解が $\boldsymbol{x}(t) = \exp(tA)\boldsymbol{c}$ であることは解の一意性による. □

注意 9.2.7. $A = (a_{ij})$ が実行列のときは, $x_1(t)$, $x_2(t)$, ..., $x_n(t)$ を実数値関数として, 微分方程式 (9.12) を考えることができる. この場合も, 初期条件 $\boldsymbol{x}(0) = \boldsymbol{c} \in \boldsymbol{R}^n$ を満たす (9.12) の解は $\boldsymbol{x}(t) = \exp(tA)\boldsymbol{c}$ と表される.

以上により, 方程式 (9.12) を解くためには, $\exp(tA)$ を求めればよいことが分かった.

例 9.2.8. 次の連立微分方程式を解いてみよう.

$$\begin{cases} x_1'(t) = -x_2(t) + x_3(t) \\ x_2'(t) = 2x_1(t) - 3x_2(t) + x_3(t) \\ x_3'(t) = x_1(t) - x_2(t) - x_3(t) \end{cases}$$

右辺の係数の行列 A は, 例 6.2.7 の行列である. したがって, 例 8.3.2 より A のジョルダン標準形 J と変換行列 P は次の通りである.

$$J = P^{-1}AP = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

命題 9.1.3 の 2) より, $\exp(tA) = P\exp(tJ)P^{-1}$ であるから, (9.6) と合わせて

$$\boldsymbol{x}(t) = P\begin{pmatrix} e^{-t} & te^{-t} & 0 \\ 0 & e^{-t} & 0 \\ 0 & 0 & e^{-2t} \end{pmatrix} P^{-1}\boldsymbol{x}(0)$$

を得る. ここで, 初期値 $\boldsymbol{x}(0)$ にこだわる必要がなければ,

$$P^{-1}\boldsymbol{x}(0) = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

とおいて, 問題の方程式の一般解

$$\boldsymbol{x}(t) = P\begin{pmatrix} e^{-t} & te^{-t} & 0 \\ 0 & e^{-t} & 0 \\ 0 & 0 & e^{-2t} \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = c_1\begin{pmatrix} e^{-t} \\ e^{-t} \\ 0 \end{pmatrix} + c_2\begin{pmatrix} te^{-t} \\ te^{-t} \\ e^{-t} \end{pmatrix} + c_3\begin{pmatrix} 0 \\ e^{-2t} \\ e^{-2t} \end{pmatrix}$$

が得られる. よって, 解空間の基底は

$$\boldsymbol{x}_1(t) = \begin{pmatrix} e^{-t} \\ e^{-t} \\ 0 \end{pmatrix},\ \boldsymbol{x}_2(t) = \begin{pmatrix} te^{-t} \\ te^{-t} \\ e^{-t} \end{pmatrix},\ \boldsymbol{x}_3(t) = \begin{pmatrix} 0 \\ e^{-2t} \\ e^{-2t} \end{pmatrix}$$

であり, c_1, c_2, c_3 が複素数の全体を動くときに, $x_1(t)$, $x_2(t)$, $x_3(t)$ を複素数値関数とする場合の一般解を与え, c_1, c_2, c_3 が実数の全体を動くときに, $x_1(t)$, $x_2(t)$, $x_3(t)$ を実数値関数とする場合の一般解を与える.

注意 9.2.9. 上の例で分かるように, $A = (a_{ij})$ が実行列でその固有値がすべて実数のときは, A のジョルダン標準形および変換行列が実行列に取れるので, $\exp(tA)$ を実行列の範囲で計算できて, $x_1(t)$, $x_2(t)$, …, $x_n(t)$ を実数値関数として, 方程式 (9.12) を解くことができるのである. 実は A が虚数の固有値を持つ場合にも, A の**実ジョルダン標準形**と呼ばれるものが存在して, それを使って $\exp(tA)$ を (実行列の範囲で) 計算して, (9.12) を解くことができるのだが, ここでは立ち入らないことにする.

問 9.6. 次の連立微分方程式の解空間の基底を求めよ.

1) $\begin{cases} x_1' = x_2 \\ x_2' = x_3 \\ x_3' = x_1 \end{cases}$ 2) $\begin{cases} x_1' = x_1 + x_2 + 2x_3 \\ x_2' = x_2 + x_3 \\ x_3' = x_3 \end{cases}$ 3) $\begin{cases} x_1' = x_2 + x_3 \\ x_2' = x_1 + x_3 \\ x_3' = x_1 + x_2 + 2x_3 \end{cases}$

$y = y(t)$ $(t \in \boldsymbol{R})$ を複素数値関数で, $a_0, a_1, \ldots, a_{n-1}$ を t によらない定数とする. $y^{(i)} = y^{(i)}(t)$ $(0 \leqq i \leqq n)$ として, 微分方程式

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y = 0 \tag{9.13}$$

を考えよう. このような微分方程式を $\boldsymbol{n}$ **階の定数係数線形微分方程式**という. この微分方程式の解の全体は, 例 4.4.1 で述べたように抽象的ベクトル空間になる.

$y_1 = y$, $y_2 = y'$, $\ldots$, $y_{n-1} = y^{(n-2)}$, $y_n = y^{(n-1)}$ とおくと, 連立微分方程式

$$\begin{cases} y_1' = y_2 \\ y_2' = y_3 \\ \quad\vdots \\ y_{n-1}' = y_n \\ y_n' = -a_0y_1 - a_1y_2 - \cdots - a_{n-2}y_{n-1} - a_{n-1}y_n \end{cases}$$

が得られる. 右辺の係数行列 A は

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

である. これは, 例 8.1.8 の行列の転置行列であるから, A の固有多項式 $\Phi_A(t)$ は,

$$\Phi_A(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 \tag{9.14}$$

に等しい.

A の相異なる固有値を $\lambda_1, \lambda_2, \ldots, \lambda_r$ として, その重複度をそれぞれ $m_1, m_2, \ldots, m_r$ とする. λ_1 に対する固有ベクトル (の一つ) を, $\boldsymbol{p} = {}^t(p_1, p_2, \ldots, p_n)$ とおく. このとき条件 $A\boldsymbol{p} = \lambda_1\boldsymbol{p}$ より,

$$p_i = \lambda_1 p_{i-1} \ (2 \leqq i \leqq n)$$

が成り立つ. よって,

$$\boldsymbol{p} = p_1 \begin{pmatrix} 1 \\ \lambda_1 \\ \vdots \\ \lambda_1^{n-1} \end{pmatrix}$$

となるので, λ_1 に対する固有空間は 1 次元である. したがって, 命題 8.3.1 より固有値 λ_1 に対する A のジョルダン細胞はただ 1 つで, $J(\lambda_1, m_1)$ である.

他の固有値についても同様であるから, A のジョルダン標準形 $J = P^{-1}AP$ は,

$$J = \begin{pmatrix} J(\lambda_1, m_1) & & & \\ & J(\lambda_2, m_2) & & \\ & & \ddots & \\ & & & J(\lambda_r, m_r) \end{pmatrix}$$

となる. したがって,

$$\boldsymbol{y}(t) = \begin{pmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_n(t) \end{pmatrix} = \begin{pmatrix} y(t) \\ y'(t) \\ \vdots \\ y^{(n-1)}(t) \end{pmatrix}$$

とおくと, 定理 9.2.6 により

$$\boldsymbol{y}(t) = \exp(tA)\boldsymbol{y}(0) = P\exp(tJ)P^{-1}\boldsymbol{y}(0)$$

が成り立つ.

例として, $n=3$, $J=\begin{pmatrix}\lambda & 1 & 0\\ 0 & \lambda & 1\\ 0 & 0 & \lambda\end{pmatrix}$ の場合を考える. 前のように, $P^{-1}\boldsymbol{y}(0)=\begin{pmatrix}c_1\\ c_2\\ c_3\end{pmatrix}$ とおく. また, $P=(\boldsymbol{p}_1\ \boldsymbol{p}_2\ \boldsymbol{p}_3)$ とおくと $A\boldsymbol{p}_1=\lambda\boldsymbol{p}_1$ であるから, 前に見たように $\boldsymbol{p}_1={}^t(1,\lambda,\lambda^2)$ に取れる. $\boldsymbol{p}_j={}^t(p_{1j},p_{2j},p_{3j})$ $(j=2,3)$ とおく. このとき,

$$\boldsymbol{y}(t)=P\exp(tJ)P^{-1}\boldsymbol{y}(0)=\begin{pmatrix}1 & p_{12} & p_{13}\\ \lambda & p_{22} & p_{23}\\ \lambda^2 & p_{32} & p_{33}\end{pmatrix}\begin{pmatrix}e^{t\lambda} & te^{t\lambda} & \dfrac{t^2}{2!}e^{t\lambda}\\ 0 & e^{t\lambda} & te^{t\lambda}\\ 0 & 0 & e^{t\lambda}\end{pmatrix}\begin{pmatrix}c_1\\ c_2\\ c_3\end{pmatrix}$$

の両辺の第 1 成分を比較して, 求める解

$$y(t)=(c_1+p_{12}c_2+p_{13}c_3)e^{t\lambda}+(c_2+p_{12}c_3)te^{t\lambda}+c_3\frac{t^2}{2!}e^{t\lambda}$$

を得る. これを $y(t)=d_1e^{t\lambda}+d_2te^{t\lambda}+d_3\dfrac{t^2}{2!}e^{t\lambda}$ と表すとき, ${}^t(d_1,d_2,d_3)$ と ${}^t(c_1,c_2,c_3)$ の間には

$$\begin{pmatrix}d_1\\ d_2\\ d_3\end{pmatrix}=\begin{pmatrix}1 & p_{12} & p_{13}\\ 0 & 1 & p_{12}\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}c_1\\ c_2\\ c_3\end{pmatrix}$$

の関係がある.

n と J が一般の場合も同様である. (9.6) より, $\exp(tJ)$ の成分は

$$\frac{t^j}{j!}e^{\lambda_i t}\quad(1\leqq i\leqq r;\ 0\leqq j\leqq m_i-1)\tag{9.15}$$

であるから, $y(t)$ はこれらの 1 次結合で

$$y(t)=\sum_{i=1}^{r}\sum_{j=0}^{m_i-1}d_{ij}\frac{t^j}{j!}e^{\lambda_i t}\tag{9.16}$$

と表せる. (9.16) の係数 $\boldsymbol{d} = {}^t(d_{01}, \ldots, d_{1m_1-1}, \ldots, d_{01}, \ldots, d_{rm_r-1})$ と $\boldsymbol{c} = P^{-1}\boldsymbol{y}(0) = {}^t(c_1, c_2, \ldots, c_n)$ の間には

$$\boldsymbol{d} = Q\boldsymbol{c}$$

という関係がある. ただし, Q は対角成分がすべて 1 に等しい上三角行列であり, 当然正則行列である. すなわち, $\boldsymbol{d}$ は $\boldsymbol{c}$ によって, したがって初期条件 $y(0), y'(0), \ldots, y^{(n-1)}(0)$ によって一意的に定まる. また, $\boldsymbol{d}$ は $\boldsymbol{C}^n$ 全体を動く. この意味で, (9.15) を微分方程式 (9.13) の解空間の**基底**という.

$a_0, a_1, \ldots, a_{n-1}$ が実数のとき, $y = y(t)$ を実変数 t に関する実数値関数として (9.13) を解いてみよう. 定理 6.4.10 の前で述べたように, 虚数 μ が A の固有方程式 (9.14) の k 重解のとき, 複素共役 $\overline{\mu}$ も k 重解である. したがって, A の固有方程式の相異なる実数解の全体を $\lambda_1, \lambda_2, \ldots, \lambda_r$ として λ_i の重複度を m_i $(1 \leqq i \leqq r)$, 相異なる虚数解の全体を $\mu_1, \overline{\mu_1}, \mu_2, \overline{\mu_2}, \ldots, \mu_s, \overline{\mu_s}$ として $\mu_i, \overline{\mu_i}$ の重複度を k_i $(1 \leqq i \leqq s)$ とすることができる. ただし,

$$m_1 + m_2 + \cdots + m_r + 2(k_1 + k_2 + \cdots + k_s) = n$$

である.

このとき, (9.16) は

$$y(t) = \sum_{i=1}^{r}\sum_{j=0}^{m_i-1} d_{ij}\frac{t^j}{j!}e^{\lambda_i t} + \sum_{i=1}^{s}\sum_{j=0}^{k_i-1} e_{ij}\frac{t^j}{j!}e^{\mu_i t} + \sum_{i=1}^{s}\sum_{j=0}^{k_i-1} f_{ij}\frac{t^j}{j!}e^{\overline{\mu_i} t}$$

の形になる. ただし, 各 d_{ij}, e_{ij}, f_{ij} は複素数である.

$$\overline{y(t)} = \sum_{i=1}^{r}\sum_{j=0}^{m_i-1} \overline{d_{ij}}\frac{t^j}{j!}e^{\lambda_i t} + \sum_{i=1}^{s}\sum_{j=0}^{k_i-1} \overline{e_{ij}}\frac{t^j}{j!}e^{\overline{\mu_i} t} + \sum_{i=1}^{s}\sum_{j=0}^{k_i-1} \overline{f_{ij}}\frac{t^j}{j!}e^{\mu_i t}$$

であるから, $\overline{y(t)} = y(t)$ であることと, $y(t)$ の上の形の 1 次結合としての表し方が一意的であることにより,

$$d_{ij} = \overline{d_{ij}}, \quad e_{ij} = \overline{f_{ij}}$$

が各 i, j について成り立つ. したがって, d_{ij} は実数である. また, 各 e_{ij} の実部を g_{ij}, 虚部を h_{ij} とおくと,

$$e_{ij} = g_{ij} + \sqrt{-1}h_{ij}, \quad f_{ij} = g_{ij} - \sqrt{-1}h_{ij}$$

が各 i, j について成り立つ[3)].

各 i $(1 \leqq i \leqq s)$ に対して $\mu_i = \rho_i + \sqrt{-1}\theta_i$ $(\rho_i,\ \theta_i \in \boldsymbol{R})$ とおく. このとき, オイラーの公式より

$$e^{t\mu_i} = e^{\rho_i t}\left(\cos(\theta_i t) + \sqrt{-1}\sin(\theta_i t)\right) \quad (1 \leqq i \leqq s)$$

が成り立つ. 以上をまとめて

$$\begin{aligned} y(t) = &\sum_{i=1}^{r}\sum_{j=0}^{m_i-1} d_{ij}\frac{t^j}{j!}e^{\lambda_i t} + \sum_{i=1}^{s}\sum_{j=0}^{k_i-1} 2g_{ij}\frac{t^j}{j!}e^{\rho_i t}\cos(\theta_i t) \\ &- \sum_{i=1}^{s}\sum_{j=0}^{k_i-1} 2h_{ij}\frac{t^j}{j!}e^{\rho_i t}\sin(\theta_i t) \end{aligned}$$

を得る. ここで, 各 d_{ij}, g_{ij}, $h_{ij} \in \boldsymbol{R}$ は一意的に定まる. したがって, $y(t)$ を実数値関数とする場合の微分方程式 (9.13) の解空間の基底は

$$\begin{aligned} &t^j e^{\lambda_i t} && (1 \leqq i \leqq r;\ 0 \leqq j \leqq m_i - 1), \\ &t^j e^{\rho_i t}\cos(\theta_i t) && (1 \leqq i \leqq s;\ 0 \leqq j \leqq k_i - 1), \\ &t^j e^{\rho_i t}\sin(\theta_i t) && (1 \leqq i \leqq s;\ 0 \leqq j \leqq k_i - 1) \end{aligned}$$

である.

問 9.7. 次の微分方程式の一般解を求めよ. ただし, $x = x(t)$ は実数値関数とする.

1) $x''' - x'' + 3x' + 5x = 0$ 2) $x''' - 3x' + 2x = 0$ 3) $x'''' + 4x'' + 4x = 0$

[3)] 添字の i と区別するために虚数単位を $\sqrt{-1}$ で表した.

練習問題

9.1. A が歪エルミート行列 $(A + A^* = O)$ であるとき, $\exp A$ はユニタリ行列であることを示せ. とくに, A が実交代行列であれば, $\exp A$ は直交行列である.

9.2. $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ とする. また, $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ とおく. $A = aI + bJ$ である. このとき, $\exp A = e^a((\cos b)I + (\sin b)J)$ であることを証明せよ. $((aI)(bJ) = (bJ)(aI)$ に注意.)

9.3. A を 2 次の実正方行列で, その固有値は虚数 $a \pm bi$ $(b \neq 0)$ とする. このとき, $P^{-1}AP = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ である, 実正則行列 P が存在することを示せ. これが注意 9.2.9 で述べた実ジョルダン標準形の一例である. これにより, 前問を使えば $\exp A$ が計算できる.

9.4. 行列のべき級数 $I + A + A^2 + \cdots + A^n + \cdots$ が収束するための A の条件を求めよ. またそのときの和を求めよ.

9.5. $\boldsymbol{x}_1(t)$, $\boldsymbol{x}_2(t)$, …, $\boldsymbol{x}_n(t)$ を (9.9) の解空間 V の基底とし, $\boldsymbol{x}(t)$ を (9.9) の 1 つの解とする. このとき,

$$\boldsymbol{x}(t) = c_1\boldsymbol{x}_1(t) + c_2\boldsymbol{x}_2(t) + \cdots + c_n\boldsymbol{x}_n(t) \quad (t \in \boldsymbol{R})$$

を満たす定数 $c_i \in \boldsymbol{C}$ $(1 \leqq i \leqq n)$ が一意的に定まることを示せ.

問題解答

問 9.1 1) A の固有値は -2, -1, 2 であるから, J^n は (したがって A^n も) 収束しない. 2) A の固有値は $1/2$ (重複度 2), $-1/3$ であり, $A-(1/2)I$ の階数は 2 であるから, $J=\begin{pmatrix}1/2 & 1 & 0\\ 0 & 1/2 & 0\\ 0 & 0 & -1/3\end{pmatrix}$ である. よって, $J^n=\begin{pmatrix}1/2^n & n/2^{n-1} & 0\\ 0 & 1/2^n & 0\\ 0 & 0 & (-1)^n/3^n\end{pmatrix}$ であり, $\lim_{n\to\infty}J^n=O$. したがって, $\lim_{n\to\infty}A^n=O$. 3) A の固有値は 1 (重複度 2), $1/2$ であり, $A-I$ の階数は 1 であるから, $J=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1/2\end{pmatrix}$ である. よって, $\lim_{n\to\infty}J^n=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{pmatrix}$ である. $P=\begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}$ にとれるので, $\lim_{n\to\infty}A^n=P\lim_{n\to\infty}J^nP^{-1}=\begin{pmatrix}2 & -1 & -1\\ 1 & 0 & -1\\ 1 & -1 & 0\end{pmatrix}$.

問 9.2 $x(iy)=(iy)x$ であるから定理 9.1.4 より $\sum_{n=0}^{\infty}\frac{z^n}{n!}=\sum_{n=0}^{\infty}\frac{x^n}{n!}\cdot\sum_{n=0}^{\infty}\frac{(iy)^n}{n!}$ が成り立つ. $\sum_{n=0}^{\infty}\frac{x^n}{n!}=e^x$ であり, また $\cos y$, $\sin y$ のテイラー展開より $\sum_{n=0}^{\infty}\frac{(iy)^n}{n!}=\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}y^{2n}+i\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}y^{2n+1}=\cos y+i\sin y$ である.

問 9.3 変換行列 P, ジョルダン標準形 $J=P^{-1}AP$, A^n, $\exp A$ の順に次の通り (一部計算省略).

1) $\begin{pmatrix}1 & 2 & -1\\ -1 & -1 & 1\\ 1 & 1 & 0\end{pmatrix}$, $\begin{pmatrix}5 & 0 & 0\\ 0 & 3 & 1\\ 0 & 0 & 3\end{pmatrix}$, $P\begin{pmatrix}5^n & 0 & 0\\ 0 & 3^n & n3^{n-1}\\ 0 & 0 & 3^n\end{pmatrix}P^{-1}$, $P\begin{pmatrix}e^5 & 0 & 0\\ 0 & e^3 & e^3\\ 0 & 0 & e^3\end{pmatrix}P^{-1}$

2) $\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 2\\ 2 & 0 & 1\end{pmatrix}$, $\begin{pmatrix}2 & 1 & 0\\ 0 & 2 & 1\\ 0 & 0 & 2\end{pmatrix}$, $P\begin{pmatrix}2^n & n2^{n-1} & n(n-1)2^{n-3}\\ 0 & 2^n & n2^{n-1}\\ 0 & 0 & 2^n\end{pmatrix}P^{-1}$, $P\begin{pmatrix}e^2 & e^2 & e^2/2\\ 0 & e^2 & e^2\\ 0 & 0 & e^2\end{pmatrix}P^{-1}$

問 9.4 $A(t)$, $B(t)$ をそれぞれ $(a_{ij}(t))$, $(b_{ij}(t))$ とおくと, $\frac{d}{dt}(A(t)B(t))$ の (i,j) 成分は $(a_{i1}(t)b_{1j}(t)+\cdots+a_{in}(t)b_{nj}(t))'=(a'_{i1}(t)b_{1j}(t)+\cdots+a'_{in}(t)b_{nj}(t))+(a_{i1}(t)b'_{1j}(t)+\cdots+a_{in}(t)b'_{nj}(t))$ で $\frac{d}{dt}A(t)\cdot B(t)+A(t)\cdot\frac{d}{dt}B(t)$ の (i,j) 成分に等しい. 2) $A(t)A(t)^{-1}=I$ の両辺を微分して 1) を適用すると, $\frac{d}{dt}A(t)\cdot A(t)^{-1}+A(t)\cdot\frac{d}{dt}A(t)^{-1}=O$.

問 9.5 $\boldsymbol{y}(t)$ を (9.9) の任意の解とすれば, $\boldsymbol{y}'(t)+\boldsymbol{x}_0'(t)=A(t)\boldsymbol{y}(t)+(A(t)\boldsymbol{x}_0(t)+\boldsymbol{b}(t))=A(t)(\boldsymbol{y}(t)+\boldsymbol{x}_0(t))+\boldsymbol{b}(t)$ より $\boldsymbol{y}(t)+\boldsymbol{x}_0(t)$ は (9.7) の解である. 逆に, $\boldsymbol{x}(t)$ を (9.7) の解として, $\boldsymbol{y}(t)=\boldsymbol{x}(t)-\boldsymbol{x}_0(t)$ とおけば, $\boldsymbol{y}'(t)=\boldsymbol{x}'(t)-\boldsymbol{x}_0'(t)=(A(t)\boldsymbol{x}(t)+\boldsymbol{b}(t))-(A(t)\boldsymbol{x}_0(t)+\boldsymbol{b}(t))=A(t)(\boldsymbol{x}(t)-\boldsymbol{x}_0'(t))=A(t)\boldsymbol{y}(t)$ より $\boldsymbol{y}(t)$ は (9.9) の解である.

問 9.6 係数行列を A とすると, 変換行列 P, ジョルダン標準形 $J=P^{-1}AP$, 基底の順に次の通り. ただし, $\omega=e^{2\pi i/3}=(-1+\sqrt{3}i)/2$ とする.

1) $\begin{pmatrix}1 & \omega & \omega^2\\ 1 & \omega^2 & \omega\\ 1 & 1 & 1\end{pmatrix}$, $\begin{pmatrix}1 & 0 & 0\\ 0 & \omega & 0\\ 0 & 0 & \omega^2\end{pmatrix}$, $\begin{pmatrix}e^t\\ e^t\\ e^t\end{pmatrix}$, $\begin{pmatrix}\omega e^{\omega t}\\ \omega^2 e^{\omega t}\\ e^{\omega t}\end{pmatrix}$, $\begin{pmatrix}\omega^2 e^{\omega^2 t}\\ \omega e^{\omega^2 t}\\ e^{\omega^2 t}\end{pmatrix}$

2) $\begin{pmatrix}1&0&0\\0&1&-2\\0&0&1\end{pmatrix}, \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}, \begin{pmatrix}e^t\\0\\0\end{pmatrix}, \begin{pmatrix}te^t\\e^t\\0\end{pmatrix}, \begin{pmatrix}t^2e^t/2\\te^t-2e^t\\e^t\end{pmatrix}$

3) $\begin{pmatrix}-1&-1&1\\-1&1&1\\1&0&2\end{pmatrix}, \begin{pmatrix}0&0&0\\0&-1&0\\0&0&3\end{pmatrix}, \begin{pmatrix}-1\\-1\\1\end{pmatrix}, \begin{pmatrix}-e^{-t}\\e^{-t}\\0\end{pmatrix}, \begin{pmatrix}e^{3t}\\e^{3t}\\2e^{3t}\end{pmatrix}$

問 9.7 1) $c_1e^{-t}+c_2e^t\cos(2t)+c_3e^t\sin(2t)$ 2) $c_1e^t+c_2te^t+c_3e^{-2t}$ 3) $c_1\cos(\sqrt{2}t)+c_2\sin(\sqrt{2}t)+c_3t\cos(\sqrt{2}t)+c_4t\sin(\sqrt{2}t)$

練習問題

9.1 任意の自然数 n に対して $(A^*)^n=(A^n)^*$ が成り立つ. よって, $\exp A^*=(\exp A)^*$ が成り立つ. したがって, $U=\exp A$ とおくと, $U^*=(\exp A)^*=\exp A^*=\exp(-A)=U^{-1}$ である.

9.2 $(aI)(bJ)=(bJ)(aI)$ より, $\exp A=\exp(aI+bJ)=\exp(aI)\exp(bJ)$ である. 明らかに $\exp(aI)=e^aI$ である. また, $\exp(bJ)=(\cos b)I+(\sin b)J$ であることは $J^2=-I$ により問 9.2 と同様に示せる.

9.3 $\boldsymbol{u}$ を固有値 $a+bi$ に対応する A の固有ベクトルとする. このとき, 例 6.3.3 と同様にして $\overline{\boldsymbol{u}}$ は固有値 $a-bi$ に対応する A の固有ベクトルである. よって, 定理 6.2.9 より $\boldsymbol{u}$ と $\overline{\boldsymbol{u}}$ は 1 次独立である. $\boldsymbol{u}=\boldsymbol{p}+\boldsymbol{q}i$ ($\boldsymbol{p}$, $\boldsymbol{q}$ は実ベクトル) とおくと, $A(\boldsymbol{u}\ \overline{\boldsymbol{u}})=(\boldsymbol{u}\ \overline{\boldsymbol{u}})\begin{pmatrix}a+bi&0\\0&a-bi\end{pmatrix}$ より $A\boldsymbol{p}=a\boldsymbol{p}-b\boldsymbol{q}$, $A\boldsymbol{q}=b\boldsymbol{p}+a\boldsymbol{q}$ が成り立つ. よって, $A(\boldsymbol{p}\ \boldsymbol{q})=(\boldsymbol{p}\ \boldsymbol{q})\begin{pmatrix}a&b\\-b&a\end{pmatrix}$ を得る. $\boldsymbol{u}$, $\overline{\boldsymbol{u}}$ は 1 次独立であるから, $\boldsymbol{p}$, $\boldsymbol{q}$ も 1 次独立である. したがって, $P=(\boldsymbol{p}\ \boldsymbol{q})$ とおけばよい.

9.4 $J=P^{-1}AP$ を A のジョルダン標準形とする. $P^{-1}(I+A+A^2+\cdots+A^n+\cdots)P=I+J+J^2+\cdots+J^n+\cdots$ の対角成分は $1+\lambda+\lambda^2+\cdots+\lambda^n+\cdots$ の形である (λ は A の固有値). これが収束しなければならないので, 各固有値 λ に対して $|\lambda|<1$ であることが必要である. 逆にこれが成り立つとき, (9.5) より J^n の成分は $\lambda^n\times$ (n の多項式) の形であるから, $n\to\infty$ のとき 0 に収束する. よって, $\lim_{n\to\infty}A^n=\lim_{n\to\infty}PJ^nP^{-1}=O$ が成り立つ. これを $(I+A+A^2+\cdots+A^{n-1})(I-A)=I-A^n$ に適用して $(I+A+A^2+\cdots+A^n+\cdots)(I-A)=I$ を得る. したがって, $I+A+A^2+\cdots+A^n+\cdots$ は収束して和は $(I-A)^{-1}$ である.

9.5 $\boldsymbol{x}(t)$ を (9.9) の 1 つの解とする. $t_0\in\boldsymbol{R}$ を 1 つ定める. $\boldsymbol{x}_1(t_0)$, $\boldsymbol{x}_2(t_0)$, …, $\boldsymbol{x}_n(t_0)$ は 1 次独立であるから, $\boldsymbol{x}(t_0)=c_1\boldsymbol{x}_1(t_0)+c_2\boldsymbol{x}_2(t_0)+\cdots+c_n\boldsymbol{x}_n(t_0)$ である c_1, c_2, …, c_n が一意的に定まる. $\boldsymbol{x}(t)$ と $c_1\boldsymbol{x}_1(t)+c_2\boldsymbol{x}_2(t)+\cdots+c_n\boldsymbol{x}_n(t)$ は共に (9.9) の解であって初期条件が等しいので, 解の一意性により恒等的に等しい. (別解) 任意の $t\in\boldsymbol{R}$ に対して $\boldsymbol{x}_1(t)$, $\boldsymbol{x}_2(t)$, …, $\boldsymbol{x}_n(t)$ は 1 次独立であるから, $\boldsymbol{x}(t)=c_1(t)\boldsymbol{x}_1(t)+c_2(t)\boldsymbol{x}_2(t)+\cdots+c_n(t)\boldsymbol{x}_n(t)$ である $c_1(t)$, $c_2(t)$, …, $c_n(t)$ が一意的に定まる. このとき, 例 9.2.5 を $\boldsymbol{b}(t)$ が恒等的に 0 ベクトルの場合に適用して, $c_i'(t)$ ($1\leqq i\leqq n$) は恒等的に 0 に等しいことが分かる. したがって, $c_i(t)$ ($1\leqq i\leqq n$) は定数である.

第10章

体と多項式

10.1 体の概念

整数 m, n $(\neq 0)$ の比で $\dfrac{m}{n}$ と表される実数を**有理数**という. 有理数全体の集合を $\boldsymbol{Q}$ で表す. $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ には四則演算 (加法・減法・乗法・除法) が定義される. 減法・除法はそれぞれ加法・乗法の逆であるから, 加法・乗法の 2 つが本質的である. このような, 四則演算を持つ集合を抽象化して体の概念を定義する.

体の公理 F を 2 つ以上の元を持つ集合とする. F が次の条件を満たすとき, F は**体**であるという.

加法 $a, b \in F$ に対して, $a+b \in F$ が定義され, これに関して次の法則が成立する. ($a+b$ を a, b の**和**という.)

$$(a+b)+c = a+(b+c) \qquad \text{(結合法則)} \tag{10.1}$$

$$a+b = b+a \qquad \text{(交換法則)} \tag{10.2}$$

特別な元 $0 \in F$ が存在して, 任意の $a \in F$ に対して次が成り立つ.

$$a+0 = a \tag{10.3}$$

任意の $a \in F$ に対して次を満たす元 $x \in F$ が存在する. この x を $-a$ で表す.

$$a+x = 0 \tag{10.4}$$

乗法 $a, b \in F$ に対して, $ab \in F$ が定義され, これに関して次の法則が成立する. (ab を a, b の**積**という.)

$$(ab)c = a(bc) \qquad \text{(結合法則)} \tag{10.5}$$

特別な元 $1 \in F$ が存在して, 任意の $a \in F$ に対して次が成り立つ.

$$a1 = 1a = a \tag{10.6}$$

0 と異なる任意の $a \in F$ に対して次を満たす元 $x \in F$ が存在する. この x を a^{-1} で表す.

$$ax = xa = 1 \tag{10.7}$$

分配法則 $a, b, c \in F$ に対して次が成り立つ.

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc \tag{10.8}$$

F を体とする. このとき, 任意の $a, b \in F$ に対して

$$x + a = b \tag{10.9}$$

を満たす $x \in F$ がただ 1 つ存在する. 何故ならば, x が (10.9) を満たすとすると, 両辺に $-a$ を加えて

$$x = x + 0 = x + (a + (-a)) = (x + a) + (-a) = b + (-a)$$

となるので $x = b + (-a)$ でなければならない. 逆に, $x = b + (-a)$ は (10.9) を満たす. $b + (-a)$ を $b - a$ で表し, b と a の**差**という. すなわち, 体には**減法**が定義される.

F を体とし, $a, b \in F$ $(a \neq 0)$ とする. このとき,

$$ax = b \tag{10.10}$$

を満たす $x \in F$ が唯 1 つ存在する. 何故ならば, x が (10.10) を満たすとすると, 両辺に左から a^{-1} をかけて,

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b \tag{10.11}$$

が成り立つ. 逆に, $x = a^{-1}b$ は (10.10) を満たす.

F が体の公理に加えて乗法の交換法則

$$ab = ba \quad (a,\ b \in F) \tag{10.12}$$

を満たすとする. このとき, F は**可換体**であるという. $a,\ b \in F\ (a \neq 0)$ に対して (10.10) の解 $a^{-1}b = ba^{-1}$ を b と a の**商**といい, $\dfrac{b}{a}$ で表す. すなわち, 可換体には**除法**が定義される. 可換でない体を**斜体**という.

問 10.1. F を体とする. 体の公理を満たす $0,\ 1 \in F$ はそれぞれ唯一であることを示せ. また, $a \in F$ に対する $-a,\ a \in F\ (a \neq 0)$ に対する a^{-1} はそれぞれ唯一に定まることを示せ.

F を体とし, K を 2 つ以上の元を持つ F の部分集合とする. さらに,

$$a,\ b \in K \text{ ならば } a+b,\ ab \in K, \tag{10.13}$$

$$a \in K \text{ ならば } -a \in K, \tag{10.14}$$

$$a \in K\ (a \neq 0) \text{ ならば } a^{-1} \in K \tag{10.15}$$

が成り立つとき, K は F の加法・乗法に関して体になる. 何故ならば, $a \in K$ とすると (10.14) より $-a \in K$ であり, さらに (10.13) より $a+(-a) = 0 \in K$ である. 同様に $1 \in K$ が示される. 公理の他の条件は K においても成り立つので K は体である. このとき, K は F の**部分体**であるといい, F は K の**拡大体**であるという.

例 10.1.1. $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ は通常の演算に関して体である. $\boldsymbol{Q}$ は $\boldsymbol{R}$ の部分体であり, $\boldsymbol{Q}$, $\boldsymbol{R}$ は $\boldsymbol{C}$ の部分体である.

問 10.2. $\boldsymbol{C}$ の部分体は $\boldsymbol{Q}$ を含むことを示せ.

$a+b\sqrt{2}\ (a,\ b \in \boldsymbol{Q})$ の全体を $\boldsymbol{Q}(\sqrt{2})$ で表す. $\boldsymbol{Q}(\sqrt{2})$ は $\boldsymbol{R}$ の部分体であることを示す. $\alpha,\ \beta \in \boldsymbol{Q}(\sqrt{2})$ とする. $\alpha = a+b\sqrt{2},\ \beta = c+d\sqrt{2}\ (a,\ b,\ c,\ d \in \boldsymbol{Q})$ とおく. このとき

$$\alpha + \beta = (a+c) + (b+d)\sqrt{2}$$

$$\alpha\beta = (ac + 2bd) + (ad + bc)\sqrt{2}$$
$$-\alpha = (-a) + (-b)\sqrt{2}$$

は $\boldsymbol{Q}(\sqrt{2})$ に属するから, $F = \boldsymbol{R}$, $K = \boldsymbol{Q}(\sqrt{2})$ として (10.13), (10.14) が成り立つ. また, $\alpha \neq 0$ のとき

$$\frac{1}{\alpha} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}$$

と**分母を有理化**することによって, $\dfrac{1}{\alpha} \in \boldsymbol{Q}(\sqrt{2})$ となるので (10.15) も成り立つ. よって, $\boldsymbol{Q}(\sqrt{2})$ は $\boldsymbol{R}$ の部分体である.

$a + b\sqrt[3]{2} + c\sqrt[3]{4}$ $(a,\ b,\ c \in \boldsymbol{Q})$ の全体を $\boldsymbol{Q}(\sqrt[3]{2})$ とおく. $\boldsymbol{Q}(\sqrt[3]{2})$ が (10.13), (10.14) を満たすことは前と同様にして容易に示せる. また, $\boldsymbol{Q}(\sqrt[3]{2})$ においても分母の有理化が可能である. 例えば

$$\frac{1}{2 - \sqrt[3]{2} + \sqrt[3]{4}} = \frac{6 + 4\sqrt[3]{2} - \sqrt[3]{4}}{22}$$

が成り立つ (分母を払って両辺が等しいことを確かめよ). したがって, (10.15) も成り立ち $\boldsymbol{Q}(\sqrt[3]{2})$ は $\boldsymbol{R}$ の部分体である. $\boldsymbol{R}$, $\boldsymbol{C}$ は部分体をたくさん持っている.

例 10.1.2 (斜体の例). $a, b, c, d \in \boldsymbol{R}$ であるときの 2 次複素正方行列

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \tag{10.16}$$

の全体を F とする. $A, B \in F$ として

$$A = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}, \quad B = \begin{pmatrix} x + yi & z + wi \\ -z + wi & x - yi \end{pmatrix}$$

とおくとき,

$$A + B = \begin{pmatrix} (a + x) + (b + y)i & (c + z) + (d + w)i \\ -(c + z) + (d + w)i & (a + x) - (b + y)i \end{pmatrix}$$

$$AB = \begin{pmatrix} \alpha+\beta i & \gamma+\delta i \\ -\gamma+\delta i & \alpha-\beta i \end{pmatrix}$$

となる. ただし,

$$\alpha = ax - by - cz - dw, \quad \beta = ay + bx + cw - dz,$$
$$\gamma = az - bw + cx + dy, \quad \delta = aw + bz - cy + dx$$

とおいた. よって, $A+B$, AB は (10.16) の形であるので F に属し, F には加法・乗法が定義される.

また, $a=b=c=d=0$ とおくと $O \in F$, $a=1$, $b=c=d=0$ とおくと $I \in F$ が分かる. O は (10.3) における 0 の条件を満たし, I は (10.6) における 1 の条件を満たす. さらに

$$-A = \begin{pmatrix} (-a)+(-b)i & (-c)+(-d)i \\ -(-c)+(-d)i & (-a)-(-b)i \end{pmatrix}$$

は F に属し, (10.4) における x の条件を満たす. 結合法則・加法の交換法則・分配法則は 2 次正方行列全体で成り立つので F においても成り立つ. したがって, 体の公理の中で (10.7) 以外は成り立つことが分かった.

(10.7) を確かめよう. $A \neq O$ とする. すなわち, $a=b=c=d=0$ ではない. よって, $a^2+b^2+c^2+d^2 > 0$ である. A^{-1} を計算すると

$$A^{-1} = \frac{1}{a^2+b^2+c^2+d^2} \begin{pmatrix} a+(-b)i & (-c)+(-d)i \\ -(-c)+(-d)i & a-(-b)i \end{pmatrix}$$

となる. よって, A^{-1} は存在して F に属する. よって, F は体である. さらに, $a=c=d=x=y=w=0$, $b=z=1$ とおくと

$$AB = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad BA = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

であるから, F は可換ではない. すなわち, F は斜体である. F は**ハミルトンの四元数体**という斜体と本質的に同じである.

以後は, 体は可換であると仮定する.

問 10.3. F を体とし, $a, b \in F$ とする. 体の公理から次を証明せよ.

1) $-(-a) = a, \quad (a^{-1})^{-1} = a \ \ (a \neq 0)$.

2) $0a = a0 = 0$.

3) $(-a)b = a(-b) = -ab$.

4) $(-a)(-b) = ab$.

注意 10.1.3. 体の公理において $1 = 0$ であると, 任意の $a \in F$ に対して

$$a = a1 = a0 = 0$$

となる. ただし, 最後の等号は問 10.3 の 2) による. よって, $F = \{0\}$ となって F が 2 つ以上の元を持つことに反する. したがって, $1 \neq 0$ である.

10.2　ユークリッドの互除法と因数分解の一意性

F を体, x を 1 つの文字として, 順序の決まった F の元の組 $a_0, a_1, \ldots, a_n$ に対して形式的な式

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n \tag{10.17}$$

を F に係数を持つ x の**多項式**といい $f(x)$ 等で表す. x を**不定元**, $a_i x^i$ を**第 i 項**, a_i を第 i 項の**係数**という. また, a_0 を**定数項**という. このようなすべての多項式の集合を $F[x]$ で表す. すべての係数が 0 である多項式を**零多項式**といい 0 で表す.

$f(x), g(x) \in F[x]$ を

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{i=0}^{m} b_i x^i, \quad m \geqq n$$

として,

$$a_i = b_i \ (0 \leqq i \leqq n), \quad b_j = 0 \ (n < j \leqq m)$$

のとき $f(x)$ と $g(x)$ は**等しい**といい, $f(x) = g(x)$ で表す.

$f(x)$ と $g(x)$ の**和**を

$$f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i+\sum_{i=n+1}^{m}b_ix^i$$

で定義し, $f(x)$ と $g(x)$ の**積**を

$$f(x)g(x)=\sum_{i=0}^{m+n}\left(\sum_{k+l=i}a_kb_l\right)x^i \tag{10.18}$$

で定義する. さらに, $\alpha\in F$ と $f(x)$ の積を

$$\alpha f(x)=\sum_{i=0}^{n}(\alpha a_i)x^i \tag{10.19}$$

で定義する. $\alpha\in F$ は定数項のみからなる多項式 $f(x)=\alpha$ と見なすことができるから, $F\subset F[x]$ と考えてよい. この場合 (10.19) は (10.18) の特別な場合と考えることができる.

以上の加法・乗法に関してそれぞれ結合法則・交換法則が成り立つ. また, 加法と乗法の間に分配法則が成り立つ.

(10.17) において $a_n\neq 0$ のとき, $f(x)$ の**次数**は n であるという. $f(x)$ の次数を $\deg f(x)$ で表す. さらに $a_n=1$ であるとき, すなわち最高次の係数が 1 のとき, $f(x)$ は**モニック**であるという. 零多項式の次数は定義しない. 次数について次の関係が成り立つ (両辺の次数は定義されるものとする).

$$\deg(f(x)+g(x))\leqq\max\{\deg f(x),\ \deg g(x)\}$$
$$\deg(f(x)g(x))=\deg f(x)+\deg g(x)$$

定理 10.2.1 (**割り算のアルゴリズム**)**.** $f(x),\ g(x)\in F[x]\ (g(x)\neq 0)$ であるとき,

$$f(x)=q(x)g(x)+r(x)$$

であって, $r(x)=0$ または $\deg r(x)<\deg g(x)$ を満たす $q(x),\ r(x)\in F[x]$ が一意的に定まる. この表し方を $f(x)$ の $g(x)$ による**割り算**といい, $q(x),\ r(x)$ をそれぞれ**商**, **余り**という.

証明　まず $q(x)$, $r(x)$ の存在を $\deg f(x)$ に関する帰納法で示す．$f(x) = 0$ または $\deg f(x) < \deg g(x)$ の場合は $q(x) = 0$, $r(x) = f(x)$ とすればよい．

$n = \deg f(x)$, $m = \deg g(x)$ とし，$n \geqq m$ と仮定する．

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

とする．次数が n より小さい $f(x)$ については定理が成り立つとしよう．

$$h(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

とすると，$h(x) = 0$ または $\deg h(x) < n$ であるから，帰納法の仮定によって

$$h(x) = q_0(x) g(x) + r_0(x)$$

となる．ここで $r_0(x) = 0$ または $\deg r_0(x) < \deg g(x)$ である．よって

$$\begin{aligned} f(x) &= h(x) + \frac{a_n}{b_m} x^{n-m} g(x) \\ &= \left(q_0(x) + \frac{a_n}{b_m} x^{n-m} \right) g(x) + r_0(x) \end{aligned}$$

となるので，$q(x) = q_0(x) + \dfrac{a_n}{b_m} x^{n-m}$, $r(x) = r_0(x)$ とすればよい．

次に一意性を示す．$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$ とすると，

$$(q(x) - q'(x))g(x) = r'(x) - r(x)$$

となる．もし $q(x) - q'(x) \neq 0$ であると，

$$\deg g(x) \leqq \deg(q(x) - q'(x))g(x) = \deg(r'(x) - r(x)) < \deg g(x)$$

となって矛盾である．よって，$q(x) = q'(x)$ であって，したがって $r(x) = r'(x)$ となる．　□

$f(x)$ を $g(x)$ $(g(x) \neq 0)$ で割った余りが 0 であるとき，$f(x)$ は $g(x)$ で**割り切れる**とう．

$f(x)=\sum_{i=0}^{n}a_ix^i\in F[x]$ とする. $\alpha\in F$ に対して $\sum_{i=0}^{n}a_i\alpha^i$ は F の元である. これを $f(\alpha)$ で表し $f(x)$ の x に α を**代入**した値という. $f(x), g(x), h(x)\in F[x]$ および $\alpha\in F$ に対して次が成り立つ.

$$f(x)=g(x)+h(x)\quad\Rightarrow\quad f(\alpha)=g(\alpha)+h(\alpha). \tag{10.20}$$

$$f(x)=g(x)h(x)\quad\Rightarrow\quad f(\alpha)=g(\alpha)h(\alpha). \tag{10.21}$$

$f(x)\in F[x]$ に対して $f(\alpha)=0$ となる F の元 α を F における $f(x)$ の**解**という. 定理 10.2.1 によって

$$f(x)=q(x)(x-\alpha)+r,\quad q(x)\in F[x],\quad r\in F$$

とすれば, (10.20), (10.21) より

$$f(\alpha)=q(\alpha)(\alpha-\alpha)+r=r$$

となる. したがって, $f(x)$ が $x-\alpha$ で割り切れるための必要十分条件は $f(\alpha)=0$ である (**因数定理**).

任意の多項式 $f(x)\in F[x]$ が F の中に解を持つとは限らない. 例えば, $x^2+1\in\boldsymbol{R}[x]$ は $\boldsymbol{R}$ の中に解を持たない. $F[x]$ の次数が 1 以上の任意の多項式が F の中で解を持つとき F は**代数的閉体**であるという. $\boldsymbol{C}$ は代数的閉体である (定理 1.2.4). F が代数的閉体のとき $f(x)\in F[x]$, $n=\deg f(x)\geqq 1$ ならば, 因数定理を繰り返し適用して

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\quad \alpha_i\in F\ (1\leqq i\leqq n)$$

という $f(x)$ の分解を得る. $\alpha_1, \alpha_2, \ldots, \alpha_n$ は $f(x)$ の解である. また, $f(x)$ は $\alpha_1, \alpha_2, \ldots, \alpha_n$ 以外に解を持たない. ここで, $x-\alpha_1, x-\alpha_2, \ldots, x-\alpha_n$ の中で同じものをまとめると

$$f(x)=a_n(x-\alpha_1)^{l_1}(x-\alpha_2)^{l_2}\cdots(x-\alpha_r)^{l_r}$$

と書ける. α_i は $f(x)$ の $\boldsymbol{l_i}$ **重解**といわれる. とくに $l_i=1$ のとき α_i は $f(x)$ の**単解**であるという.

$f(x)$ が $g(x)$ で割り切れるとき, $f(x)$ を $g(x)$ の**倍数**, $g(x)$ を $f(x)$ の**約数**という[1]. $f_1(x),\ f_2(x),\ \ldots,\ f_k(x) \in F[x]$ とする. $f_1(x),\ f_2(x),\ \ldots,\ f_k(x)$ の共通の倍数を**公倍数**という. ただし, $f_i(x) \neq 0\ (1 \leqq i \leqq k)$ とする. $f_1(x)f_2(x)\cdots f_k(x)$ は公倍数である. 0 を除く公倍数の中で次数が最小のものを**最小公倍数**という. また, $f_1(x),\ f_2(x),\ \ldots,\ f_k(x)$ の共通の約数を**公約数**という. ただし, $f_1(x) = f_2(x) = \cdots = f_k(x) = 0$ ではないとする. 1 は公約数である. 次数が最大の公約数を**最大公約数**という. 最小公倍数・最大公約数に 0 でない定数 (F の元) をかけてもやはり最小公倍数・最大公約数であるから, 最小公倍数・最大公約数はモニックであると約束することにする.

命題 10.2.2. $f(x),\ a_i(x),\ g_i(x) \in F[x]\ (i = 1, 2)$ とし,

$$f(x) = a_1(x)g_1(x) + a_2(x)g_2(x)$$

とする. このとき, $h(x) \in F[x]$ が $g_1(x),\ g_2(x)$ の約数であれば, $h(x)$ は $f(x)$ の約数でもある. とくに, $h(x)$ は $g_1(x) + g_2(x),\ g_1(x) - g_2(x)$ の約数である.

証明 仮定より $g_i(x) = q_i(x)h(x),\ q_i(x) \in F[x]\ (i = 1, 2)$ と表せる. このとき,

$$f(x) = a_1(x)g_1(x) + a_2(x)g_2(x) = (a_1(x)q_1(x) + a_2(x)q_2(x))h(x)$$

であるから, $h(x)$ は $f(x)$ の約数である. 後半は $a_1(x) = a_2(x) = 1$ または $a_1(x) = 1,\ a_2(x) = -1$ とした場合である. □

定理 10.2.3. $f_1(x),\ f_2(x),\ \ldots,\ f_k(x) \in F[x],\ f_i(x) \neq 0\ (1 \leqq i \leqq k)$ の最小公倍数 $l(x)$ は一意的に定まる. また, 任意の公倍数は最小公倍数の倍数である.

証明 $l_1(x),\ l_2(x)$ を最小公倍数とする. 命題 10.2.2 より $l_1(x) - l_2(x)$ は $f_i(x)\ (1 \leqq i \leqq k)$ の公倍数である. $l_1(x),\ l_2(x)$ は次数が同じでモニックであるから, $l_1(x) \neq l_2(x)$ であれば $l_1(x) - l_2(x)$ はより次数が低い公倍数となる

[1] $f(x),\ g(x)$ は式であって数ではないのであるが, 整数の場合と同様に倍数・約数と呼ぶことにする. 倍元・約元とか倍式・約式と呼ぶ本もある.

ので矛盾が生ずる．$L(x)$ を $f_i(x)$ $(1 \leqq i \leqq k)$ の公倍数とする．$L(x)$ を $l(x)$ で割って

$$L(x) = q(x)l(x) + r(x)$$

とする．命題 10.2.2 より $r(x) = L(x) - q(x)l(x)$ は公倍数である．$r(x) \neq 0$ であれば, $r(x)$ は $l(x)$ より次数が低い公倍数となるので矛盾である． □

次に最大公約数について考察する．$f(x)$, $g(x) \in F[x]$ $(g(x) \neq 0)$ とする．まず, $f_1(x) = f(x)$, $f_2(x) = g(x)$ とおいて割り算

$$f_1(x) = q_1(x)f_2(x) + f_3(x) \tag{10.22}$$

を行う．ここで $f_3(x) = 0$ または $\deg f_3(x) < \deg f_2(x)$ である．$h(x)$ を $f_2(x)$, $f_3(x)$ の公約数とすると, 命題 10.2.2 より $h(x)$ は $f_1(x)$ の約数である．よって, $h(x)$ は $f_1(x)$, $f_2(x)$ の公約数である．逆に, $h(x)$ を $f_1(x)$, $f_2(x)$ の公約数とすると, $f_3(x) = f_1(x) - q_1(x)f_2(x)$ より $h(x)$ は $f_3(x)$ の約数である．よって, $h(x)$ は $f_2(x)$, $f_3(x)$ の公約数である．したがって, $f_1(x)$, $f_2(x)$ の公約数の全体と $f_2(x)$, $f_3(x)$ の公約数の全体は一致する．

余りが 0 でなければ, さらに割り算を続行して

$$\begin{aligned} f_2(x) &= q_2(x)f_3(x) + f_4(x) \\ f_3(x) &= q_3(x)f_4(x) + f_5(x) \\ &\vdots \end{aligned}$$

とすることができるが,

$$\deg f_3(x) > \deg f_4(x) > \deg f_5(x) > \cdots$$

と無限に減少することはあり得ないので, 何回目かには割り切れる．すなわち, ある k があって

$$f_k(x) = q_k(x)f_{k+1}(x) \tag{10.23}$$

となる．前と同様に, $f_2(x)$, $f_3(x)$ の公約数の全体は $f_3(x)$, $f_4(x)$ の公約数の全体と一致し, $\ldots$, $f_k(x)$, $f_{k+1}(x)$ の公約数の全体と一致する．ところが, (10.23)

より $f_k(x)$, $f_{k+1}(x)$ の公約数の全体は $f_{k+1}(x)$ の約数の全体である．その中の次数が最大のものは $f_{k+1}(x)$ 自身であるから，$f(x) = f_1(x)$ と $g(x) = f_2(x)$ の最大公約数は，$f_{k+1}(x)$ の最高次の係数を e とすると，$e^{-1}f_{k+1}(x)$ である．よって，$f(x)$ と $g(x)$ の最大公約数は一意的に定まることが示された．それを $\gcd(f(x), g(x))$ で表す．このように，割り算の繰り返しで最大公約数を求めることができる．この最大公約数の求め方を**ユークリッドの互除法**という．

(10.22) を次の形に書き直すことができる．

$$\begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix} = \begin{pmatrix} q_1(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_2(x) \\ f_3(x) \end{pmatrix}.$$

これを続けると

$$\begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix} = \begin{pmatrix} q_1(x) & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_{k-1}(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_k(x) \\ f_{k+1}(x) \end{pmatrix}$$

を得る．左から逆行列 $\begin{pmatrix} q_1(x) & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1(x) \end{pmatrix}$ 等を順次かけると

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1}(x) \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1(x) \end{pmatrix} \begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix} = \begin{pmatrix} f_k(x) \\ f_{k+1}(x) \end{pmatrix}$$

となる．左辺の行列の積を $\begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix}$ とおいて第 2 行を比較すると

$$c(x)f_1(x) + d(x)f_2(x) = f_{k+1}(x)$$

が成り立つ．両辺に e^{-1} をかけて $c(x)$, $d(x)$ を取り替えると次の定理を得る．

定理 10.2.4. $f(x)$, $g(x) \in F[x]$ とし，$f(x) = g(x) = 0$ ではないとする．このとき，

$$c(x)f(x) + d(x)g(x) = \gcd(f(x), g(x))$$

を満たす $c(x)$, $d(x) \in F[x]$ が存在する．

命題 10.2.2 より次の系を得る[2].

系 10.2.5. $f(x)$, $g(x)$ の任意の約数は最大公約数の約数である.

例 10.2.6. $f(x) = x^{33} - 1$, $g(x) = x^{18} - 1 \in \boldsymbol{Q}[x]$ の最大公約数を求めよう.

$$\begin{aligned} x^{33} - 1 &= x^{15}(x^{18} - 1) + (x^{15} - 1), \\ x^{18} - 1 &= x^3(x^{15} - 1) + (x^3 - 1), \\ x^{15} - 1 &= (x^{12} + x^9 + x^6 + x^3 + 1)(x^3 - 1) \end{aligned}$$

より, 最大公約数は $x^3 - 1$ である. また, $q_1(x) = x^{15}$, $q_2(x) = x^3$ であるから,

$$\begin{pmatrix} 0 & 1 \\ 1 & -x^3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -x^{15} \end{pmatrix} = \begin{pmatrix} 1 & -x^{15} \\ -x^3 & x^{18} + 1 \end{pmatrix}$$

の第 2 行を使って

$$-x^3 f(x) + (x^{18} + 1)g(x) = x^3 - 1$$

を得る.

問 10.4. 次の多項式 $f(x)$, $g(x)$ の最大公約数 $\gcd(f(x), g(x))$ を求めよ. また, $c(x)f(x) + d(x)g(x) = \gcd(f(x), (g(x))$ を満たす $c(x)$, $d(x)$ を求めよ.
1) $f(x) = x^5 + 2x^4 - 4x^3 + 3x^2 - 3x - 5$, $g(x) = x^4 + 3x^3 - 2x^2 - 3x - 5$
2) $f(x) = 2x^4 + (6\sqrt{2}+11)x^3 + (24\sqrt{2}+23)x^2 + (24\sqrt{2}+32)x + (11\sqrt{2}+18)$, $g(x) = x^3 + (2\sqrt{2}+6)x^2 + (7\sqrt{2}+10)x + (4\sqrt{2}+5)$

$f(x) \in F[x]$ $(\deg f(x) \geqq 1)$ とする. $f(x)$ がより次数の低い多項式の積で表せるとき, すなわち

$$f(x) = g_1(x)g_2(x)$$

を満たす $g_i(x) \in F[x]$, $\deg g_i(x) < \deg f(x)$ $(i = 1, 2)$ が存在するとき, $f(x)$ は**可約**であるという. $f(x)$ が可約でないとき $f(x)$ は**既約**であるという. 既

[2] 定理 10.2.3 および系 10.2.5 を満たす多項式として最小公倍数・最大公約数を定義する本もある. この場合, 最小公倍数・最大公約数の一意性は明らかであるが, 存在が明らかではない.

約な $f(x)$ の約数は $f(x)$ と 1 (およびそれらの 0 でない定数倍) のみである. $f(x)$, $g(x)$ の最大公約数が 1 のとき, $f(x)$, $g(x)$ は**互いに素**であるという.

$f(x)$ が可約か既約かは $f(x)$ をどの範囲で考えるかによって変わる. 例えば, x^2-2 を $\boldsymbol{Q}[x]$ の元と考えれば既約であるが, $\boldsymbol{R}[x]$ の元と考えれば $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$ と分解するので可約である. 考える範囲を明確にしたい場合は, x^2-2 は $\boldsymbol{Q}$ 上既約であるとか, x^2+1 は $\boldsymbol{R}$ 上既約であるなどという.

定理 10.2.7. $f(x)$, $g(x)$, $h(x) \in F[x]$ で $f(x)$, $g(x)$ は互いに素であるとする. このとき, $f(x)$ が $g(x)h(x)$ を割り切れば $f(x)$ は $h(x)$ を割り切る.

証明　$f(x)$, $g(x)$ は互いに素であるから定理 10.2.4 より

$$c(x)f(x)+d(x)g(x)=1$$

を満たす $c(x)$, $d(x) \in F[x]$ が存在する. 両辺に $h(x)$ をかけて

$$c(x)f(x)h(x)+d(x)g(x)h(x)=h(x)$$

とすると, 仮定より左辺の 2 項はそれぞれ $f(x)$ の倍数であるから, 命題 10.2.2 より右辺の $h(x)$ も $f(x)$ の倍数である. □

系 10.2.8. $f(x)$ を既約とする. このとき, $f(x)$ が $g(x)h(x)$ を割り切れば, $f(x)$ は $g(x)$ または $h(x)$ を割り切る.

証明　$f(x)$ が $g(x)$ を割り切れば主張は成り立つ. よって, $f(x)$ は $g(x)$ を割り切らないとする. このとき, $f(x)$, $g(x)$ の公約数は 0 でない定数のみであるから, 最大公約数は 1 である. したがって, 定理 10.2.7 より $f(x)$ は $h(x)$ を割り切るので, この場合も主張は成り立つ. □

定理 10.2.9 (因数分解の一意性). 任意の多項式 $f(x) \in F[x]$ $(\deg f(x) \geqq 1)$ は既約な多項式の積に分解される. またこの分解は, 積の順序と定数倍を除いて一意的である.

証明　まず, 前半を $\deg f(x)$ に関する帰納法で証明する. $\deg f(x)=1$ ならば $f(x)$ は既約なので明らかである. $n=\deg f(x)$ であるとして, $n-1$ 次以

下の多項式に関しては正しいと仮定する. $f(x)$ が既約ならば, 明らかである. $f(x)$ が可約で $f(x) = g(x)h(x)$ と分解すると, 帰納法の仮定により, $g(x)$ と $h(x)$ は既約な多項式の積で表されるので, $f(x)$ についても同様である.

後半を示そう. $f(x)$ が次のように 2 通りに分解したとする.

$$f(x) = p_1(x)p_2(x)\cdots p_k(x) = q_1(x)q_2(x)\cdots q_l(x).$$

ただし, $p_i(x)$ $(1 \leqq i \leqq k)$ と $q_j(x)$ $(1 \leqq j \leqq l)$ は既約な多項式である. $p_1(x)$ は既約で, $f(x) = q_1(x)q_2(x)\cdots q_l(x)$ を割り切るから, 系 10.2.8 よりある $q_j(x)$ を割り切る. 順番を交換して $q_1(x)$ を割り切るとして良い. よって, $q_1(x) = a(x)p_1(x)$ と表せる. ところが $q_1(x)$ も既約であるから, $a(x)$ は定数である. 故に $a(x)$ を a で表す. このとき,

$$p_1(x)p_2(x)\cdots p_k(x) = ap_1(x)q_2(x)\cdots q_l(x)$$

より,

$$p_2(x)\cdots p_k(x) = aq_2(x)\cdots q_l(x)$$

が成り立つ. これを繰り返して行くと, $k = l$ であって各 i $(1 \leqq i \leqq k)$ に対して $p_i(x)$ は $q_i(x)$ の定数倍となる. □

定理 10.2.4 を一般の場合に別の方法で証明しよう.

定理 10.2.10. *$f_1(x)$, $f_2(x)$, ..., $f_k(x) \in F[x]$ とし, $f_1(x) = f_2(x) = \cdots = f_k(x) = 0$ ではないとする. このとき, $f_1(x)$, $f_2(x)$, ..., $f_k(x)$ の最大公約数 $\gcd(f_1(x), f_2(x), \ldots, f_k(x))$ は一意的に定まり,*

$$\sum_{i=1}^{k} c_i(x)f_i(x) = \gcd(f_1(x), f_2(x), \ldots, f_k(x)) \tag{10.24}$$

を満たす $c_1(x)$, $c_2(x)$, ..., $c_k(x) \in F[x]$ が存在する.

証明 (10.24) の左辺の形に表せる多項式の全体を I とおく. 仮定より $I = \{0\}$ ではない. I に属する最低次のモニックな多項式を $g(x)$ とする. $g(x)$ は

$$g(x) = \sum_{i=1}^{k} d_i(x)f_i(x), \quad d_i(x) \in F[x] \ (1 \leqq i \leqq k) \tag{10.25}$$

と表せる. 任意の $h(x) \in I$ は $g(x)$ で割り切れることを示す. $h(x)$ は

$$h(x) = \sum_{i=1}^{k} c_i(x) f_i(x), \quad c_i(x) \in F[x] \ (1 \leqq i \leqq k) \tag{10.26}$$

と表せる. $h(x)$ を $g(x)$ で割って

$$h(x) = q(x)g(x) + r(x) \tag{10.27}$$

とする. (10.25), (10.26), (10.27) より

$$\sum_{i=1}^{k} (c_i(x) - d_i(x)q(x)) f_i(x) = r(x)$$

を得る. この左辺は I に属するので, $r(x) \neq 0$ であれば, $g(x)$ が I に属する最低次の多項式であることに矛盾する. よって, $r(x) = 0$ であり, $h(x)$ は $g(x)$ で割り切れる. (10.26) で $c_i(x) = 1$, $c_j(x) = 0$ $(j \neq i)$ とおくと $h(x) = f_i(x)$ であるから, いま示したことにより $f_i(x)$ $(1 \leqq i \leqq k)$ は $g(x)$ で割りきれる. よって, $g(x)$ は $f_i(x)$ $(1 \leqq i \leqq k)$ の公約数である.

$h(x)$ を $f_i(x)$ $(1 \leqq i \leqq k)$ の公約数とすると, (10.25) と命題 10.2.2 より $h(x)$ は $g(x)$ の約数である. このことから $g(x)$ は $f_i(x)$ $(1 \leqq i \leqq k)$ の最大公約数であることが従い, 最大公約数が一意的に定まることも従う. □

この I を $f_1(x), f_2(x), \ldots, f_k(x)$ で生成される $F[x]$ の**イデアル**という. イデアルは現代代数学の重要な概念である.

この節で述べたことは整数についても同様の結果が成り立つ. というより, 整数の場合の方が原形である. 整数の全体を $\boldsymbol{Z}$ とおく. $\boldsymbol{Z}$ においても加法・乗法が定義され, 体の公理の (10.7) 以外を満たす. $\boldsymbol{Z}$ を**整数環**という. $F[x]$ においても加法・乗法が定義され, 体の公理の (10.7) 以外を満たす. $F[x]$ を **1 変数多項式環**という. 一般に, 加法・乗法が定義された代数系で体の公理の (10.7) 以外を満たすものを**環**という[3]. さらに, 環において積の交換法則 (10.12) が成り立つとき, その環を**可換環**という.

正の整数を**自然数**という. 自然数の全体を $\boldsymbol{N}$ で表す. $\boldsymbol{N}$ においても加法・乗法が定義されるが, (10.3), (10.4) が成り立たないので $\boldsymbol{N}$ は環ではない.

[3] 環の場合は 1 つしか元を持たない, すなわち $1 = 0$ であるものものも許す. このような環を**零環**という.

定理 10.2.11. m を整数, n を自然数とする. このとき,

$$m = qn + r, \quad 0 \leqq r < n$$

を満たす整数 q, r が一意的に定まる. この表し方を m の n による**割り算**といい, q を**商**, r を**余り**という.

証明 0 以上の整数の全体を $\boldsymbol{Z}_{\geqq 0}$ で表す. $q \to -\infty$ のとき $m - qn \to \infty$ であるから,

$$S = \{m - qn \mid q \in \boldsymbol{Z}\} \cap \boldsymbol{Z}_{\geqq 0}$$

は空集合ではない. S の最小元を $m - q_0 n$ とする. このとき, 仮定より $m - q_0 n \geqq 0$ である. さらに, $m - q_0 n < n$ である. 何故ならば, $m - q_0 n \geqq n$ とすると, $m - q_0 n > m - (q_0 + 1)n \geqq 0$ となるから, $m - q_0 n$ が S の最小元であることに反する. $r_0 = m - q_0 n$ とおくと, q_0, r_0 は定理の条件を満たす.

次に一意性を示す.

$$m = q_1 n + r_1 = q_2 n + r_2, \quad 0 \leqq r_1,\ r_2 < n$$

とする. このとき,

$$(q_1 - q_2)n = r_2 - r_1$$

である. この右辺は $-n < r_2 - r_1 < n$ であるから絶対値は $n - 1$ 以下である. ところが, $q_1 \neq q_2$ であれば左辺の絶対値は n 以上となるので, $q_1 = q_2$ でなければならない. よって $r_1 = r_2$ である. □

整数の割り算については小学校以来周知のことであるが, m が負の場合の割り算は見慣れないことかも知れない. 例えば

$$-1 = (-1)4 + 3$$

であるから, -1 を 4 で割った商は -1 で余りは 3 である.

m を n で割った余りが 0 のとき, m は n で**割り切れる**といい, m を n の**倍数**, n を m の**約数**という. $m_1, m_2, \ldots, m_k \in \boldsymbol{Z}$ とする. $m_1, m_2, \ldots, m_k$ の共通の倍数を**公倍数**という. ただし, $m_i \neq 0$ $(1 \leqq i \leqq k)$ とする. $m_1 m_2 \cdots m_k$

は公倍数である．正の最小の公倍数を**最小公倍数**という．また, m_1, m_2, ..., m_k の共通の約数を**公約数**という．ただし, $m_1 = m_2 = \cdots = m_k = 0$ ではないとする．1 は公約数である．最大の公約数を**最大公約数**という．この場合の最小公倍数・最大公約数の存在と一意性は明らかである．

以下結果だけ述べる．

命題 10.2.12. a_i, $m_i \in \boldsymbol{Z}$ $(i = 1, 2)$ とし, $n \in \boldsymbol{N}$ とする．n が m_1, m_2 の約数であれば, n は $a_1m_1 + a_2m_2$ の約数である．とくに, n は $m_1 + m_2$, $m_1 - m_2$ の約数である．

定理 10.2.13. m_1, m_2, ..., $m_k \in \boldsymbol{Z}$, $m_i \neq 0$ $(1 \leqq i \leqq k)$ の最小公倍数を n とする．任意の m_1, m_2, ..., m_k の公倍数は n の倍数である．

$\boldsymbol{Z}$ においてもユークリッドの互除法が適用できて 2 つの整数 m_1, m_2 の最大公約数 $\gcd(m_1, m_2)$ を計算することができる．また, 次の定理および系も同様に証明できる．

定理 10.2.14. m_1, $m_2 \in \boldsymbol{Z}$ とし, $m_1 = m_2 = 0$ ではないとする．このとき,

$$a_1m_1 + a_2m_2 = \gcd(m_1, m_2)$$

を満たす a_1, $a_2 \in \boldsymbol{Z}$ が存在する．

系 10.2.15. m_1, m_2 の任意の公約数は最大公約数 $\gcd(m_1, m_2)$ の約数である．

定理 10.2.10 と同様にして次の定理が証明できる．

定理 10.2.16. m_1, m_2, ..., $m_k \in \boldsymbol{Z}$ とし, $m_1 = m_2 = \cdots = m_k = 0$ ではないとする．

$$a_1m_1 + a_2m_2 + \cdots + a_km_k, \quad a_i \in \boldsymbol{Z} \ (1 \leqq i \leqq k)$$

の形の整数の全体を I とする．I に属する最小の自然数は m_1, m_2, ..., m_k の最大公約数である．m_1, m_2, ..., m_k の任意の公約数は最大公約数の約数である．

この I を $m_1, m_2, \ldots, m_k$ で生成された $\boldsymbol{Z}$ の**イデアル**という.

n を 2 以上の自然数とする. n の正の約数が 1 と n しか存在しないとき n は**素数**であるという. 素数は p や q で表すのが習慣である. n が素数でないとき n は**合成数**であるという. $m, n \in \boldsymbol{Z}$ の最大公約数が 1 のとき, m, n は**互いに素**であるという.

定理 10.2.17. *$l, m, n \in \boldsymbol{Z}$ で l, m は互いに素であるとする. このとき, l が mn を割り切れば, l は n を割り切る.*

系 10.2.18. *$p, m, n \in \boldsymbol{Z}$ で p を素数とする. このとき, p が mn を割り切れば, p は m または n を割り切る.*

定理 10.2.19 (算術の基本定理). *2 以上の任意の自然数は素数の積で表され, その表し方は素数の順序を除いて一意的である.*

整数 n を

$$n = \pm p_1 p_2 \cdots p_k, \quad p_i \text{ は素数 } (1 \leqq i \leqq k)$$

と素数の積で表す表し方を n の**素因数分解**という.

問 10.5. 次の整数 m, n の最大公約数 $\gcd(m, n)$ を求めよ. また, $cm + dn = \gcd(m, n)$ を満たす整数 c, d を求めよ.

1) $m = 254939, n = 72806$ 2) $m = 253313, n = 184943$

10.3 代数学の基本定理

この節では, 定理 1.2.4 で述べた代数学の基本定理を証明する.

定理 1.2.4 *n を自然数とし, $a_0, a_1, \ldots, a_n \in \boldsymbol{C}$, $a_n \neq 0$ とする. このとき, n 次方程式*

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0 \tag{10.28}$$

は必ず複素数の中に解を持つ.

証明 関数 $f : \boldsymbol{C} \longrightarrow \boldsymbol{C}$ を

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0, \quad z \in \boldsymbol{C}$$

で定める. $f(z)$ は $\boldsymbol{C}$ 上の連続関数である. したがって, $|f(z)|$ は $\boldsymbol{C}$ 上の実数値連続関数である.

$a_0 = 0$ であれば, (10.28) は $z = 0$ を解に持つので定理は成り立つ. したがって, $a_0 \neq 0$ の場合を考える. まず, 関数 $|f(z)|$ が $\boldsymbol{C}$ において最小値 $|f(\alpha)|$ をとることを示す. すなわち, ある $\alpha \in \boldsymbol{C}$ が存在して, 任意の $z \in \boldsymbol{C}$ に対して

$$|f(z)| \geqq |f(\alpha)|$$

が成り立つことを示す.

$f(z)$ を

$$f(z) = z^n \left(a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right)$$

と変形して考えれば, $|z| \to \infty$ のとき

$$|f(z)| \to \infty$$

であることが分かる. すなわち, ある正数 R が存在して, $|z| > R$ である z に対して

$$|f(z)| > |a_0| = |f(0)| \tag{10.29}$$

が成り立つ[4]. $D = \{z \in \boldsymbol{C} \mid |z| \leqq R\}$ は有界閉集合であるから, 連続関数 $|f(z)|$ は D において最小値をとる[5]. すなわち, ある $\alpha \in D$ が存在して, 任意の $z \in D$ に対して $|f(z)| \geqq |f(\alpha)|$ が成り立つ. $0 \in D$ より $|f(0)| \geqq |f(\alpha)|$ であるから, (10.29) より任意の $z \in \boldsymbol{C}$ に対して $|f(z)| \geqq |f(\alpha)|$ が成り立つ. すなわち, $|f(\alpha)|$ は $|f(z)|$ の $\boldsymbol{C}$ における最小値である. $|f(\alpha)| = 0$ であれば, $z = \alpha$ が (10.28) の解である.

$b = f(\alpha) \neq 0$ として矛盾を導こう. $g(y) = f(y + \alpha)$ とおくと, $g(y)$ は y に関する n 次式であって, $g(0) = f(\alpha) = b$ であるから,

$$g(y) = b(1 + c_1 y + \cdots + c_{n-1} y^{n-1} + c_n y^n) \tag{10.30}$$

---

[4] $\varepsilon = |a_0|$ として $\varepsilon - \delta$ 論法を適用した.

[5] 微分積分学の教科書を参照せよ.

と書ける. ただし, $c_i \in \boldsymbol{C}$ $(1 \leqq i \leqq n)$, $c_n \neq 0$ である. また, $|g(y)|$ の最小値は $|g(0)| = |f(\alpha)| = |b|$ である.

$c_1, c_2, \ldots, c_n$ の中で 0 でない最初のものを c_m とし, $c_m = \rho e^{i\theta}$ $(\rho > 0,\ 0 \leqq \theta < 2\pi)$ と極形式で表す. このとき, (10.30) は

$$g(y) = b(1 + c_m y^m + y^{m+1} h(y))$$

と書ける. $h(y)$ は $n - m - 1$ 次多項式である. $y = re^{\frac{\pi-\theta}{m} i}$ $(r > 0)$ とすれば,

$$g(y) = b(1 - \rho r^m + r^{m+1} e^{i\theta'} h(y)), \quad \theta' = \frac{(m+1)(\pi - \theta)}{m}$$

となる. r を小さくとって $1 > \rho r^m$ とすれば,

$$\begin{aligned} |g(y)| &\leqq |b| \left(|1 - \rho r^m| + |r^{m+1} e^{i\theta'} h(y)| \right) \\ &= |b| \left(1 - \rho r^m + r^{m+1} |h(y)| \right) \end{aligned}$$

が成り立つ. $r \to 0$ のとき $-\rho + r|h(y)| \to -\rho$ であるから, r を十分小さくとると,

$$|g(y)| \leqq |b| \left(1 - \rho r^m + r^{m+1} |h(y)| \right) < |b| = |g(0)|$$

となって, $|g(0)|$ が最小値であったことに矛盾する. よって, $b = g(0) = 0$ でなければならない. □

問題解答

問 10.1　0, $0'$ がともに (10.3) を満たすと仮定する．すなわち, 任意の a, $b \in F$ に対して $0+a=a$, $0'+b=b$ が成り立つ．$a=0'$, $b=0$ とすると, $0'=0+0'=0$．1 が唯一であることも同様．また, x, y がともに (10.4) を満たすとすると, $x=x+0=x+(a+y)=(x+a)+y=0+y=y$．$a^{-1}$ が唯一に定まることも同様．

問 10.2　F を $\boldsymbol{C}$ の部分体とする．$1 \in F$ より, 任意の $n \in \boldsymbol{N}$ に対して $n=1+1+\cdots+1$ (n 個) は F に属する．また, $-n$, $1/n$ も F に属する．よって, 任意の m/n ($m \in \boldsymbol{Z}$, $n \in \boldsymbol{N}$) も F に属する．したがって, F は $\boldsymbol{Q}$ を含む．

問 10.3　1)　$a+(-a)=0$ で $-a$ を主役と見れば $-(-a)=a$ が分かる．$(a^{-1})^{-1}=a$ も同様．　2)　$0+0=0$ の両辺に a をかけて $0a=(0+0)a=0a+0a$．両辺から $0a$ を引くと $0a=0$．　3)　$0=a+(-a)$ の両辺に b をかけて $0=(a+(-a))b=ab+(-a)b$．よって, $(-a)b=-ab$．　4)　$0=a+(-a)$ の両辺に $-b$ をかけて $0=a(-b)+(-a)(-b)$．よって, $(-a)(-b)=-a(-b)=-(-ab)=ab$．

問 10.4　$\gcd(f(x),g(x))$, $c(x)$, $d(x)$ の順に次の通り．　1)　x^2+2x-5, $(-x+1)/3$, $(x^2-2x+2)/3$　2)　$x+\sqrt{2}+1$, $-x+\sqrt{2}-2$, $2x^2+3x+5\sqrt{2}-5$

問 10.5　$\gcd(m,n)$, c, d の順に次の通り．1)　59, 309, -1082　2)　43, 376, -515