ケーリー・ハミルトンの定理とその周辺

雲 幸一郎

今月は，行列を扱います．とはいっても，行列について述べるべきことはたくさんあるので，今回は，話題を「ケーリー・ハミルトンの定理とその周辺」に限ることにしたいと思います．

以下，行列といえば，成分が実数であるような２次正方行列（2×2 行列）を意味することとし，単位行列，零行列をそれぞれ $E=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$O=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ で表すことにします．

1．行列式

行列 $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ に対して，$ad-bc$ を A の行列式といい，$\det A$（あるいは $\det(A)$）という記号で表します．すなわち，

$$\det A=ad-bc$$

です．

行列式について，次のことが成り立ちます．

> 行列 A，B に対して，
> $$\det(AB)=\det A\cdot\det B$$

これを，行列式の乗法性といいます．

［証明］ $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$，$B=\begin{pmatrix}e&f\\g&h\end{pmatrix}$ とおくと

$$AB=\begin{pmatrix}ae+bg&af+bh\\ce+dg&cf+dh\end{pmatrix}$$

であるから，

$$\begin{aligned}&\det(AB)\\&=(ae+bg)(cf+dh)-(af+bh)(ce+dg)\\&=(acef+adeh+bcfg+bdgh)\\&\qquad-(acef+adfg+bceh+bdgh)\\&=ad(eh-fg)+bc(fg-eh)\\&=(ad-bc)(eh-fg)=\det A\cdot\det B\quad\blacksquare\end{aligned}$$

この性質から，

$$\det(A^2)=\det A\cdot\det A=(\det A)^2$$
$$\begin{aligned}\det(A^3)&=\det(A^2A)=\det(A^2)\cdot\det A\\&=(\det A)^2\cdot\det A=(\det A)^3\end{aligned}$$

……………………………………………………

一般に，任意の正の整数 n に対して，

$$\det(A^n)=(\det A)^n$$

が成り立ちます．

2．ケーリー・ハミルトンの定理

一般に，多項式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

と行列 A に対して，行列

$$a_0A^n+a_1A^{n-1}+\cdots+a_{n-1}A+a_nE$$

を $f(x)$ の x に A を代入した行列といい，$f(A)$ で表します．すなわち，

$$f(A)=a_0A^n+a_1A^{n-1}+\cdots+a_{n-1}A+a_nE$$

です（$f(x)$ の定数項 a_n を a_nE でおきかえることに注意しましょう）．

さて，行列 $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ に対して，多項式

$$\begin{aligned}\det(xE-A)&=\det\begin{pmatrix}x-a&-b\\-c&x-d\end{pmatrix}\\&=(x-a)(x-d)-(-b)(-c)\\&=x^2-(a+d)x+ad-bc\end{aligned}$$

を A の特性多項式（あるいは固有多項式）といいます．

ここに現れた $a+d$ を A のトレース（あるいは跡）といい，$\mathrm{tr}A$（あるいは $\mathrm{tr}(A)$）という記号で表します．すなわち，

$$\mathrm{tr}A=a+d$$

です．

すると，行列 A の特性多項式は，

$$x^2-(\mathrm{tr}A)x+\det A$$

と表されます．

以上の準備のもとで，ケーリー・ハミルトンの定理は，次のように述べられます．

> 行列 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ に対して，その特性多項式を
> $$\varphi(x)=x^2-(a+d)x+ad-bc$$
> とおくと，
> $$\varphi(A)=O$$
> すなわち，
> $$A^2-(a+d)A+(ad-bc)E=O$$
> が成り立つ．

［**証明**］ $A^2-(a+d)A=A\{A-(a+d)E\}$

$$=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} -d & b \\ c & -a \end{pmatrix}$$
$$=\begin{pmatrix} bc-ad & 0 \\ 0 & bc-ad \end{pmatrix}$$
$$=-(ad-bc)E$$

であるから，

$$A^2-(a+d)A+(ad-bc)E=O$$

が成り立つ．■

ケーリー・ハミルトンの定理からの帰結で最も重要なことは，

“行列 A の多項式は，$pA+qE$ の形に変形できる”

ことの認識です．

> **例題 1.** $A=\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$ とするとき，
> $B=A^3+A^2-5A+3E$ を求めよ．

正直に成分計算して B を求めるのは面倒です．

ケーリー・ハミルトンの定理から，

$$A^2-2A+5E=O \qquad ①$$

が成り立ちます．

①より，A^2 が

$$A^2=2A-5E \qquad ②$$

と表されますから，A^3 が

$$A^3=A^2A=(2A-5E)A=2A^2-5A$$
$$=2(2A-5E)-5A=-A-10E \qquad ③$$

と表されることになります．

②，③より，

$$B=(-A-10E)+(2A-5E)-5A+3E$$
$$=-4A-12E \qquad ④$$

となりますから，結局，

$$B=-4\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}-12\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} \mathbf{-16} & \mathbf{-8} \\ \mathbf{8} & \mathbf{-16} \end{pmatrix}$$

となります．

また，多項式の割り算を利用する次のような方法もあります．

x^3+x^2-5x+3 を x^2-2x+5 で割って商と余りを求めることにより，

$$x^3+x^2-5x+3$$
$$=(x^2-2x+5)(x+3)-4x-12 \qquad ⑤$$

が成り立つことが分かります（確かめましょう）．

このとき，⑤の x に A を代入した

$$A^3+A^2-5A+3E$$
$$=(A^2-2A+5E)(A+3E)-4A-12E \qquad ⑥$$

が成り立ちます．というのも，A と E が可換（行列 C，D に対して $CD=DC$ が成り立つとき，C と D は可換であるといいます）なことから，⑥の右辺を展開して整理する計算が，⑤の右辺を展開して整理する計算と同様にして行われるからです（心配な人は，⑥の右辺を展開して確かめてみましょう）．

ここで，①を用いると，⑥より，

$$A^3+A^2-5A+3E=-4A-12E$$

すなわち，④が得られます．あとは，はじめの解法と同様です．

> **例題 2.** $A=\begin{pmatrix} 1 & 4 \\ 1 & -2 \end{pmatrix}$ とする．正の整数 n に対して，A^n を求めよ．

例題 1 の多項式の割り算を利用する方法を使ってみましょう．

行列 A に対して，

$$A^2+A-6E=O \qquad ①$$

が成り立ちます．

x^n を x^2+x-6 で割ったときの商を $Q(x)$，余りを $px+q$ とすると，

$$x^n=(x^2+x-6)Q(x)+px+q \qquad ②$$

が成り立ちます（例題 1 の解答から分かるように，商 $Q(x)$ は求める必要がありません）．

$$x^2+x-6=(x-2)(x+3)$$

に注意して，②に $x=2$，$x=-3$ を代入すると，

$$\begin{cases} 2^n=2p+q \\ (-3)^n=-3p+q \end{cases}$$

となりますから，

$$p=\frac{1}{5}\{2^n-(-3)^n\},\ q=\frac{1}{5}\{3\cdot 2^n+2\cdot(-3)^n\}$$

が得られます．

②の x に A を代入して①を用いると，

$$A^n=pA+qE=\cdots$$
$$=\frac{1}{5}\begin{pmatrix} 4\cdot 2^n+(-3)^n & 4\cdot 2^n-4\cdot(-3)^n \\ 2^n-(-3)^n & 2^n+4\cdot(-3)^n \end{pmatrix}$$

となります．

以上から分かるように，多項式 $f(x)$ と行列 A に対して，$f(x)$ を A の特性多項式で割った余りを $px+q$ とすると，

$$f(A)=pA+qE$$

となります．

それでは，$f(A)$ を $pA+qE$ の形に表すとき，p，q は1通りに定まるのでしょうか？ これについては，次のことが成り立ちます．

> 行列 A が単位行列 E の実数倍でないとき，
> $$\alpha A+\beta E=\alpha' A+\beta' E$$
> $$\Longrightarrow \alpha=\alpha' \text{ かつ } \beta=\beta'$$

［**証明**］ $$\alpha A+\beta E=\alpha' A+\beta' E \qquad ①$$

とすると，

$$(\alpha-\alpha')A=(\beta'-\beta)E$$

である．ここで，$\alpha-\alpha'\neq 0$ とすると $A=\dfrac{\beta'-\beta}{\alpha-\alpha'}E$

となり，A が E の実数倍でないことに反するので，

$$\alpha-\alpha'=0 \qquad \therefore\ \alpha=\alpha'$$

であり，このとき，①より，

$$\beta E=\beta' E \qquad \therefore\ \beta=\beta' \ ■$$

上の事実は，次節の“行列の方程式”において，重要な役割を果たします．

3．行列の方程式

> **例題** 3．行列 $A=\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ が方程式
> $A^3-3A+2E=O$ を満たすとき，実数 a，b の値を求めよ．

与えられた方程式

$$A^3-3A+2E=O \qquad ①$$

の左辺を“因数分解”して

$$(A-E)^2(A+2E)=O \qquad ②$$

とする変形は，A と E が可換なことから正当です．しかし，行列の世界には零因子（すなわち，$C\neq O$，$D\neq O$ であっても $CD=O$ となるような行列 C，D）が存在しますから，②から

$$A=E \text{ または } A=-2E$$

と結論することはできません！

そこで，ケーリー・ハミルトンの定理による“次数下げ”を利用します．

まず，$A=kE$（k：実数）と表される場合（なぜこの場合を特別扱いするのかは，すぐに分かります），①に $A=kE$ を代入して，

$$(kE)^3-3kE+2E=O$$
$$\therefore\ (k^3-3k+2)E=O$$
$$\therefore\ k^3-3k+2=0 \qquad \therefore\ (k-1)^2(k+2)=0$$
$$\therefore\ k=1,\ -2 \qquad \therefore\ A=E,\ -2E$$
$$\therefore\ (\boldsymbol{a},\ \boldsymbol{b})=(\mathbf{1},\ \mathbf{0}),\ (\mathbf{-2},\ \mathbf{0}) \qquad ③$$

となります．

次に，$A=kE$（k：実数）と表されない場合を考えます．

ケーリー・ハミルトンの定理から，

$$A^2=2aA-(a^2-b^2)E$$

が成り立ちますから，

$$A^3=A^2A=\{2aA-(a^2-b^2)E\}A$$
$$=2aA^2-(a^2-b^2)A$$
$$=2a\{2aA-(a^2-b^2)E\}-(a^2-b^2)A$$
$$=(3a^2+b^2)A-2a(a^2-b^2)E$$

となります．よって，①より，

$$(3a^2+b^2-3)A-2\{a(a^2-b^2)-1\}E=O$$

となります．

ここで，$A\neq kE$ の登場です！ 上式の右辺の O を $0A+0E$ とみて，左段で述べたことを用いると，

$$\begin{cases} 3a^2+b^2-3=0 & ④ \\ a(a^2-b^2)-1=0 & ⑤ \end{cases}$$

が得られます（これで，なぜ $A=kE$ と $A\neq kE$ で場合を分けたのか分かったでしょう）．

④より $b^2=-3a^2+3$ で，これを⑤に代入して整理すると，

$$(a-1)(2a+1)^2=0 \qquad \therefore\ a=1,\ -\frac{1}{2}$$

となります．$A\neq kE$ より $b\neq 0$ ですから，

$$(\boldsymbol{a},\ \boldsymbol{b})=\left(-\frac{\mathbf{1}}{\mathbf{2}},\ \pm\frac{\mathbf{3}}{\mathbf{2}}\right) \qquad ⑥$$

となります．

以上から，③，⑥が答です．

多項式の割り算による次数下げを徹底すれば，次のようなほとんど計算のいらない解答に到達します．

$$f(x)=x^3-3x+2$$

とおくと，与えられた方程式は

$$f(A)=O \qquad ⑦$$

と表せます．

まず，$A=kE$ のとき，$A=kE$ を⑦に代入すると，

$$f(k)E=O \qquad \therefore\ f(k)=0$$

となるので，

$$f(x)=(x-1)^2(x+2) \qquad ⑧$$

に注意すると，

$$k=1,\ -2 \qquad \therefore\ A=E,\ -2E$$

$$\therefore\ (\boldsymbol{a},\ \boldsymbol{b})=(\mathbf{1},\ \mathbf{0}),\ (\mathbf{-2},\ \mathbf{0})$$

が得られます（ここまでは，はじめの解答と同じです）．

次に，$A\neq kE$ のときを考えます．

A の特性多項式を

$$\varphi(x)=x^2-2ax+a^2-b^2$$

として，$f(x)$ を $\varphi(x)$ で割った余りを $px+q$ とおくと，前ページで述べたように，

$$f(A)=pA+qE$$

となりますから，⑦より，

$$pA+qE=O$$

です．

ここで，$A\neq kE$ であることを用いると，

$$p=0 \text{ かつ } q=0$$

となります．

これは，$f(x)$ が $\varphi(x)$ で割り切れること，すなわち，$\varphi(x)$ が $f(x)$ の因数であることを意味しています．

⑧より，$f(x)$ の2次の因数は

$$(x-1)^2 \text{ または } (x-1)(x+2)$$

ですから，

$$x^2-2ax+a^2-b^2=(x-1)^2$$

または

$$x^2-2ax+a^2-b^2=(x-1)(x+2)$$

であり，したがって，

$$(2a,\ a^2-b^2)=(2,\ 1)$$

または

$$(2a,\ a^2-b^2)=(-1,\ -2)$$

となりますが，$A\neq kE$ より $b\neq 0$ ですから，後者のみが適し，

$$(\boldsymbol{a},\ \boldsymbol{b})=\left(-\frac{\mathbf{1}}{\mathbf{2}},\ \pm\frac{\mathbf{3}}{\mathbf{2}}\right)$$

となります．

この解法の場合，$f(x)$ の因数分解がポイントになります．

まとめると，多項式 $f(x)$ に対して，

$$f(A)=O$$

を満たす行列 A は，

（ｉ） $A=kE$ で，k は $f(x)=0$ の解

（ii） $A\neq kE$ で，A の特性多項式は $f(x)$ の因数

となります．

最後に，次の問題をやってみましょう．

例題 4． 行列 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ が，ある自然数 n に対して $A^n=O$ を満たすならば，$A^2=O$ であることを証明せよ．

$n=1,\ 2$ のときは，証明すべきことは当然成り立ちますから，以下，$n\geqq 3$ のときを考えます．

この例題の直前にまとめたことを利用すれば，すぐに証明できてしまいます．

$A=kE$ のとき，$k^n=0$ より $k=0$ となりますから，

$$A=O \qquad \therefore\ A^2=O$$

が成り立ちます．

$A\neq kE$ のとき，A の特性多項式 $\varphi(x)$ は x^n の2次の因数ですから $\varphi(x)=x^2$ となり，したがって，ケーリー・ハミルトンの定理より，

$$\varphi(A)=O \qquad \therefore\ A^2=O$$

が成り立ちます．

それでは，例題3のはじめの解法のような方法でこの例題を解くことを考えてみましょう．

まず，

$$A^n=O \qquad ①$$

から，

$$\det A=0 \qquad ②$$

が導かれます．というのも，①の両辺の行列式を考えると，54ページで述べたことを用いて，

$$\det(A^n)=0 \qquad \therefore\ (\det A)^n=0$$

となるからです．

すると，ケーリー・ハミルトンの定理より

$$A^2=(a+d)A \qquad ③$$

となりますから，帰納的に，

$$A^n=(a+d)^{n-1}A$$

が成り立ちます（確かめましょう）．よって，①より，

$$a+d=0 \text{ または } A=O$$

となりますが，いずれにしても，③より $A^2=O$ が成り立ちます．

（くも こういちろう，予備校講師）