行列の導入時におけるいくつかの例

藤堂　最音 *

Some examples of matrix at first step

TOHDOH Saion

概要

Matrix is difficult to understand and hard to calculate only except adding. Multpling of matrices needs very many multipling and adding of numbers.
For example, the componets of the power of a matrix may be very big. But this difficulty is not essential to understand matrices. We try to simplify culculating of matrices for beginners to understand mathematic of matrix.

1　はじめに

線形代数は，解析とならんで高専数学の一つの大きな柱になっている．解析幾何とベクトルの導入に始まり，形式的に導入された行列は，連立一次方程式の解法の一つとして，あるいはベクトルに対するパラメータ付きの作用素として，その必要性が強調されることになる．代数的にも幾何学的にも，行列は教科数学の中ではきわめて多角的な側面を持っている．
しかし，授業などでそのような数学的内容に立ち入ろうとするとき，その計算量がきわめて大きいという障害にぶつかることになる．ごく簡単な例は別として，大半は算術的な計算にかかりきりになってしまう．
線形代数といっても，ベクトルまでは計算上の困難はそうない．しかし，行列に入ると，線形性や一次変換のように，概念的なむずかしさもさることながら，計算における面倒さが学習を進める障害になっているのではないか．
線形代数において，どのような内容を教えることが適切なのか，許される期間でどこまで教えることができるのか．1学年末あるいは2学年から学習が始まることを念頭にして，考慮すべきことは少なくない．

行列の計算で使用されるのは，基本的に加減乗除の四則だけではあるが，計算量が多い．最も簡単な2次の正方行列の積でも，掛け算8回・足し算4回，最大限計12回の演算が必要である．3次なら，$5 \times 9 = 45$ 回，4次なら，$7 \times 16 = 112$ 回も必要になる．
また，ミスが一ヶ所生じると，その後の計算が無意味になる場合も多く，ストレスも多い．かといって，導入段階で計算ソフトに頼ることは，初学者にとっては行列の概念になれることに資することにはならないであろう．やはり，数学的な概念ができあがってからの方が望ましい．

* 一般科目　数学

計算量そのものはいかんともしがたいが，せめて四則の計算をなるべく簡単なものに限定させることによって，計算の負担を軽くし，なお数学的な香りを残すことはできないであろうか．

そのための試みの一つとして，行列成分を通常の整数や実数ではなく，素数 p を法とする剰余類 $Z_p = Z/pZ$ にすることを考えてみた．そうすれば行列の成分は，0 から $p-1$ までの，たかだか p 個だけだから，見た目にもすっきりしている．

特に，行列 A の累乗 A^n は，回転行列以外は通常成分も当然指数関数的に肥大していくので面倒だが，数を Z_p にとると，成分の見た目が大きくなっていかず，循環的に推移する．その変化が視覚的に面白く，いろいろな数学的な興味のきっかけになりうる．

日本の初等教育では伝統的に，剰余類に代表される整数論に立ち入ることがほとんど無かったようである．せいぜい，素数や約数・倍数数，最大公約数や最小公倍数の程度であろうか．剰余類は「数学教育の現代化」の時代に，若干扱われていたが，紹介程度であり，数学といえるものではなかった．高校以上で学ぶのは，ロジックにおける Z_2 の演算くらいだろうか．
時計や曜日とか，三角関数における一般角と関数値の関係など，周期的なものをはじめとして，日常的にも剰余類的なことは少なくないので，初等教育の現場でも motivation を明確に示して，もう少し深く扱ってもよいのではないだろうか．

2 $GL(n, Z_p)$

以下，等号 $=$ と合同 $\equiv$ を，混乱のない範囲で混用することとする．また，$mod\ p$ も混乱のない範囲で省略する．

Z_p上の n 次の正則行列全体を，$GL(n, Z_p)$ と記し，$GL(n, Z_p)$ において，単位行列を e，零行列を o とする．

Z_2において，$a = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ とする．このとき，

$$a^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, a^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

さらに，

$$e + a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = a^2$$

$$e + a^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = a$$

であるから，$Z_2 = \{o, e\}$ に a を添加した $Z_2(a) = \{o, e, a, a^2 \mid a^4 = a\}$ は，$2^2 = 4$ 元からなる有限体の例になる．

これは，実数体の $x^2 + 1 = 0$ の解 i による代数拡大 $R(i) =$ 複素数体 C を，

$$i^2 = -1, a^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = -e : i \to a$$

$$z=x+yi \to xe+ya=x\begin{pmatrix}1&0\\0&1\end{pmatrix}+y\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}x&-y\\y&x\end{pmatrix}$$

と, i を使わないで, $GL(2,R)\cup\{o\}$ に埋め込んでしまうことの再現である.

この 4 個の行列を使うと, 4 元からなる体の演算表（乗法表と加法表）が簡単に得られる.
a は Z_2上の 4 次方程式 $x^4=x$ の解の中で,

$$x^4-x=x^4+x=x(x^3+1)=x(x+1)(x^2+x+1)=0$$

つまり, Z_2にふくまれない, $x^2+x+1=0$ の解と考えることができる.

Z_3においても, $a=\begin{pmatrix}0&1\\1&1\end{pmatrix}$ とすると,

$$a^4=2e, a^8=(a^4)^2=2^2e=4e=e$$

となり, $\{o,e,a,a^2,,\cdots,a^7 \mid a^9=a\}$ は, $3^2=9$ 元からなる体である.
乗法表は行列の積である.

$$e=\begin{pmatrix}1&0\\0&1\end{pmatrix}, a=\begin{pmatrix}0&1\\1&1\end{pmatrix}, a^2=\begin{pmatrix}1&1\\1&2\end{pmatrix}, a^3=\begin{pmatrix}1&2\\2&0\end{pmatrix},$$

$$a^4=\begin{pmatrix}2&0\\0&2\end{pmatrix}=2e, a^5=\begin{pmatrix}0&2\\2&2\end{pmatrix}, a^6=\begin{pmatrix}2&2\\2&1\end{pmatrix}, a^7=\begin{pmatrix}2&1\\1&0\end{pmatrix}$$

加法表は行列の和として容易に確かめられる.

$$e+a=a^2, e+a^2=a^7, e+a^3=a^6, e+a^4=o, e+a^5=a^3, e+a^6=a^5, e+a^7=a$$

一般に,

$$a^i+a^j=a^i(e+a^{j-i})=a^ia^k=a^{i+k}$$

により, 加法の規則はすべて得られ演算表が完成する. また, この行列表現を使えば, 生成元 a,a^3,a^5,a^7について, a,a^3は Z_3上の既約方程式 $x^2+2x+2=0$ の 2 解, かつ, a^5,a^7は $x^2+x+2=0$ の 2 解であることも容易に確認できる.

3 $GF(p^2)$

Galois によれば, 任意の素数 p と自然数 n に対して, p^n個の元からなる有限体が存在し, それは, Z_p上の方程式, $x^{p^n}=x$ の分解体である.
その乗法群は一つの元 a で生成される巡回群であり, 体としてはすべて同型である.（*Moore*）
このような有限体を,（素体 Z_p上の）位数 p^nのガロア体とよび, $GF(p^n)$ と記す.
以下, 体 F の乗法群 $F-\{o\}$ を $F^{\#}$と記す.

前節の結果から, $GF(2^2)^{\#}$は, Z_2上, $a=\begin{pmatrix}0&1\\1&1\end{pmatrix}$ で生成され, $a^{2^2}=a^4=a, a^3=e$.
$GF(3^2)^{\#}$は, Z_3上, $a=\begin{pmatrix}0&1\\1&1\end{pmatrix}$ で生成され, $a^{3^2}=a^9=a, a^8=e$ である. $a^4=2e$ なので, a の位数はちょうど 8.

より一般的な $GL(2,Z_p)$ の中で，$GF(p^2)^{\#}$を生成するような元を探してみれば，次のようなものが見つかる．ただし，手計算の省力化のために生成元 a として，$\begin{pmatrix}0 & 1\\ x & y\end{pmatrix}$ の形の行列を選んでみた．a^iの第 2 行が a^{i+1}の第 1 行にそのまま移行するので，計算が 2 項分ですむ．
以下，混乱のない範囲で，体 F とその乗法群 $F^{\#}$を混用して，単に F と記すこととする．

整数環 Z において，素数 p に対して n と p がたがいに素であるとき，$n^p \equiv n\ (mod\ p)$,つまり，$n^{p-1} \equiv 1\ (mod\ p)$ が成り立つ ($Fermat$ の「小定理」) ことを注意しておこう．

$$Z_2\text{上，}GF(4)=GF(2^2):a=\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix},a^3=e$$

$$Z_3\text{上，}GF(9)=GF(3^2):a=\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix},a^4=2e,a^8=(a^4)^2=2^2e=e$$

$$Z_5\text{上，}GF(25)=GF(5^2):a=\begin{pmatrix}0 & 1\\ 2 & 3\end{pmatrix},a^6=3e,a^{24}=(a^6)^4=3^4e=e$$

$\{o,e,a,a^2,\cdots,a^{p^n-2} \mid a^{p^n}=a\}$ が標数 p の有限体であることを確認しておく．
乗法に関しては，巡回群なので問題はない．加法に関して，Z_p上，

$$(e+a^i)^{p^n}=e+(a^i)^{p^n}=e+(a^{p^n})^i=e+a^i$$

さらに，行列 a^i,a^jは可換なので，

$$(a^i+a^j)^{p^n}=(a^i)^{p^n}+(a^j)^{p^n}=(a^{p^n})^i+(a^{p^n})^j=a^i+a^j$$

であるから，加法に関しても閉じており，たしかに位数 p^nの体である．

$GL(2,Z_p)$ の中で位数がちょうど p^2-1 でないような元が生成する巡回群は，加法に関しては閉じていないので，体の乗法群にはならない．たとえば，$GL(2,Z_5)$ において，$a=\begin{pmatrix}0 & 1\\ 2 & 1\end{pmatrix}$ とすると，$a^3=2e,a^{12}=(a^3)^4=2^4e=e$ より，その位数は 12 である．このとき，$e+a=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+\begin{pmatrix}0 & 1\\ 2 & 1\end{pmatrix}=\begin{pmatrix}1 & 1\\ 2 & 2\end{pmatrix}$であり，$GL(2,Z_5)$ の外に出る．

$$Z_7\text{上，}GF(49)=GF(7^2):a=\begin{pmatrix}0 & 1\\ 2 & 2\end{pmatrix},a^8=5e,a^{48}=(a^8)^6=5^6e=e$$

$$\text{他に，}\begin{pmatrix}0 & 1\\ 2 & 3\end{pmatrix}^8=\begin{pmatrix}0 & 1\\ 2 & 4\end{pmatrix}^8=\begin{pmatrix}0 & 1\\ 2 & 5\end{pmatrix}^8=5e$$

$$Z_{11}\text{上，}GF(121)=GF(11^2):a=\begin{pmatrix}0 & 1\\ 4 & 1\end{pmatrix},a^{12}=7e,a^{120}=(a^{12})^{10}=7^{10}e=e$$

$$\text{他に，}\begin{pmatrix}0 & 1\\ 4 & 4\end{pmatrix}^{12}=\begin{pmatrix}0 & 1\\ 4 & 7\end{pmatrix}^{12}=\begin{pmatrix}0 & 1\\ 4 & 10\end{pmatrix}^{12}=7e$$

さらに，それらの行列式を調べると，

$$Z_2 : \det\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = -1 = 1,\ Z_3 : \det\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = -1 = 2,$$

$$Z_5 : \det\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = -2 = 3,\ Z_7 : \det\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = -2 = 5,$$

$$Z_{11} : \det\begin{pmatrix} 0 & 1 \\ 4 & 7 \end{pmatrix} = -4 = 7$$

となるので，次のように予想できる．
$< p >$ を素数 p の直前の素数とすると，

$GF(p^2)$ の乗法群は，$GL(2, Z_p)$ の中の位数 $p^2 - 1$ の巡回部分群であり，

その生成元は，$a = \begin{pmatrix} 0 & 1 \\ - < p > & r \end{pmatrix}$ の形で，$a^{p+1} =< p > e$ となる．

さらに，このとき，$p^2 - 1 = (p+1)(p-1)$ に注意すれば，p と $< p >$ はたがいに素なので，

$$a^{p+1} =< p > e, a^{p^2-1} = (a^{p+1})^{p-1} =< p >^{p-1} e = e$$

となる（？）予想が正しいのか，r にはどのような数が許されるのかは，今後の課題．他の例としては，

$$Z_{13}\text{上，}\ GF(169) = GF(13^2) : a = \begin{pmatrix} 0 & 1 \\ 2 & 4 \end{pmatrix}, a^{14} = 11e, a^{168} = (a^{14})^{12} = 11^{12}e = e$$

$$Z_{17}\text{上，}\ GF(289) = GF(17^2) : a = \begin{pmatrix} 0 & 1 \\ 4 & 7 \end{pmatrix}, a^{18} = 13e, a^{288} = (a^{18})^{16} = 13^{16}e = e$$

$$Z_{19}\text{上，}\ GF(361) = GF(19^2) : a = \begin{pmatrix} 0 & 1 \\ 2 & 9 \end{pmatrix}, a^{20} = 17e, a^{360} = (a^{20})^{18} = 17^{18}e = e$$

$$Z_{97}\text{上，}\ GF(9409) = GF(97^2) : a = \begin{pmatrix} 0 & 1 \\ 8 & 3 \end{pmatrix}, a^{98} = 89e, a^{9408} = (a^{98})^{96} = 89^{96}e = e$$

4 $GF(p^3)$

前節の例から，$GL(3, Z_p)$ では，$a = \begin{pmatrix} 0 & 0 & 1 \\ 0 & - < p > & r \\ 1 & r & s \end{pmatrix}$ として生成元を探す．それは，第 1 行が $(0, 0, 1)$ ，行列式 $=< p >$ である対称行列である．このとき，累乗の結果も対称行列となり，a をかけるときの成分の計算が 3 回ですむ．手計算のチェックもしやすい．
次のような例が見つかる．

$$Z_2\text{上，}\ GF(8) = GF(2^3) : a = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, a^7 = e$$

$$Z_3\text{上, } GF(27)=GF(3^3):a=\begin{pmatrix}0&0&1\\0&1&1\\1&1&0\end{pmatrix},a^{13}=2e,a^{26}=(a^{13})^2=2^2e=e$$

$$Z_5\text{上, } GF(125)=GF(5^3):a=\begin{pmatrix}0&0&1\\0&2&2\\1&2&0\end{pmatrix},a^{31}=3e,a^{124}=(a^{31})^4=3^4e=e$$

$$Z_7\text{上, } GF(343)=GF(7^3):a=\begin{pmatrix}0&0&1\\0&2&3\\1&3&0\end{pmatrix},a^{57}=5e,a^{342}=(a^{57})^6=5^6e=e$$

$$Z_{11}\text{上, } GF(1331)=GF(11^3):a=\begin{pmatrix}0&0&1\\0&4&3\\1&3&2\end{pmatrix},a^{133}=7e,a^{1330}=(a^{133})^{10}=7^{10}e=e$$

$$Z_{13}\text{上, } GF(2197)=GF(13^3):a=\begin{pmatrix}0&0&1\\0&2&2\\1&2&2\end{pmatrix},a^{183}=11e,a^{2196}=(a^{183})^{12}=11^{12}e=e$$

$GF(p^2)$ のときと同じように，$GF(p^3)$ は，$GL(3,Z_p)$ においてこのような形の行列によって，次のように実現できそうである．r と s に関する条件は不明．

$p^3-1=(p-1)(p^2+p+1)$ であるから，

$$a^{p^2+p+1}=<p>e,a^{p^3-1}=(a^{p^2+p+1})^{p-1}=<p>^{p-1}e=e$$

5 $GF(2^n)$

Z_2上，$GF(2^n)$ の生成元の例は，次のようである．位数がちょうど，2^n-1 の元．

$$GF(4)=GF(2^2):\begin{pmatrix}0&1\\1&1\end{pmatrix}^3=e$$

$$GF(8)=GF(2^3):\begin{pmatrix}0&0&1\\0&1&1\\1&1&0\end{pmatrix}^7=\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}^7=e$$

$$GF(16)=GF(2^4):\begin{pmatrix}0&0&0&1\\0&0&1&1\\0&1&1&1\\1&1&1&0\end{pmatrix}^{15}=e\text{ であるが，}$$

$$\begin{pmatrix}0&0&0&1\\0&0&1&1\\0&1&1&0\\1&1&0&0\end{pmatrix}^7=\begin{pmatrix}0&0&0&1\\0&0&1&1\\0&1&1&1\\1&1&1&1\end{pmatrix}^7=e\text{ で，これらは生成元ではない．}$$

$$GF(32)=GF(2^5):\begin{pmatrix}0&0&0&0&1\\0&0&0&1&1\\0&0&1&1&0\\0&1&1&0&0\\1&1&0&0&0\end{pmatrix}^{31}=\begin{pmatrix}0&0&0&0&1\\0&0&0&1&1\\0&0&1&1&1\\0&1&1&1&1\\1&1&1&1&1\end{pmatrix}^{31}=e\text{ であるが,}$$

$$\begin{pmatrix}0&0&0&0&1\\0&0&0&1&1\\0&0&1&1&1\\0&1&1&1&0\\1&1&1&0&0\end{pmatrix}^{5}=\begin{pmatrix}0&0&0&0&1\\0&0&0&1&1\\0&0&1&1&1\\0&1&1&1&1\\1&1&1&1&0\end{pmatrix}^{12}=e\text{ で，生成元ではない.}$$

$$GF(64)=GF(2^6):\begin{pmatrix}0&0&0&0&0&1\\0&0&0&0&1&1\\0&0&0&1&1&0\\0&0&1&1&0&0\\0&1&1&0&0&0\\1&1&0&0&0&0\end{pmatrix}^{63}=\begin{pmatrix}0&0&0&0&0&1\\0&0&0&0&1&1\\0&0&0&1&1&1\\0&0&1&1&1&1\\0&1&1&1&1&1\\1&1&1&1&1&1\end{pmatrix}^{63}=e\text{ であるが,}$$

$$\begin{pmatrix}0&0&0&0&0&1\\0&0&0&0&1&1\\0&0&0&1&1&1\\0&0&1&1&1&0\\0&1&1&1&0&0\\1&1&1&0&0&0\end{pmatrix}^{15}=\begin{pmatrix}0&0&0&0&0&1\\0&0&0&0&1&1\\0&0&0&1&1&1\\0&0&1&1&1&1\\0&1&1&1&1&0\\1&1&1&1&0&0\end{pmatrix}^{8}=\begin{pmatrix}0&0&0&0&0&1\\0&0&0&0&1&1\\0&0&0&1&1&1\\0&0&1&1&1&1\\0&1&1&1&1&1\\1&1&1&1&1&0\end{pmatrix}^{9}=e\text{ で，生成元ではない.}$$

すべての n に対して，$GF(2^n)$ は生成元としてこのような形の行列をとれそうである．右下の 0 からなる三角形の大きさをどうすればよいのか，不明である．$GF(2^4)$ だけが特異なのかもしれない．

6　おわりに

今後の課題は，

1. 任意の n,p について，$GF(p^n)^{\#}$ は，$GL(n,Z_p)$ の中にふくまれているかどうか.
   つまり，位数がちょうど p^n-1 の行列が $GL(n,Z_p)$ に少なくとも一つ存在するかどうか.
2. あるとしたら，そのような行列の例を実際に構成する公式があるか.
3. 一般に，$GL(n,Z_p)$ の任意の行列の位数を，実際に累乗をせずに直接求める方法があるか.

を，肯定的か否定的か示すことになる.
また，$GF(2^n)$ の累乗の変化は，模様としても面白いので，学生の興味を引くかもしれない.

(2006. 11. 24 受理)