行列を用いた多項式のべき乗演算法

西岡 弘明†

従来，多項式間の加減乗除等の演算は，多項式に含まれる係数同士の組合せにおける演算に分解して行われてきた．本論文では，一変数多項式の係数からなる行列（係数行列）を定義することにより，多項式間のさまざまな演算を係数行列間の演算として記述できることを証明する．本方法は多項式演算の結果のすべての項の係数を求める方法ではなく，多項式の一定次数以下の項の係数のみが計算可能な制限付きの多項式演算である．さらに，係数行列の応用として，多項式のべき乗計算を取りあげる．本論文では多項式のべき乗の計算法として，係数行列の最小多項式に基づく方法と係数行列の二項展開による方法の2方法を提案し，これらのアルゴリズムの計算量の評価を行っている．係数行列は多項式演算と行列演算とを理論的に結びつけるものであり，行列におけるさまざまな計算法を多項式演算に応用する橋渡しの役割を果たす．係数行列は，数値解析や物理学における近似計算等にも応用可能である．

Efficient Computation of Power of Polynomial using Coefficient Matrix

HIROAKI NISHIOKA†

Usually, arithmetic operations of polynomials are executed by means of combinations of arithmetic operations between their coefficients. In this paper, we define "coefficient matrix" of which elements are coefficients of polynomial. We can calculate sum, difference and product of coefficient matrices which correspond to sum, difference and product of original polynomials respectively. Moreover, it is shown that power of coefficient matrix corresponds to that of polynomial. Coefficient matrix method is very efficient in lower-order term calculation. By using coefficient matrix, we propose several algorithms for power of polynomial. Furthermore we evaluate efficiency (time order) of these algorithms. This method can be applied to the field of physics and numerical analysis.

1. まえがき

多項式の算術演算を行列演算に置き換えるいくつかの試みは，Knuth[7] に紹介されている．しかしながら，これらの方法はいずれも多項式の変数に具体的な値を代入して多項式を評価するものであり，変数を含んだ状態のままでの多項式演算を行列乗算で代行するものではない．

変数を含んだ状態での多項式演算を行列演算に置き換えて実行するためには，多項式と係数行列との対応関係（写像）を示す必要がある．この対応関係のもとで多項式演算における加算・減算・乗算の計算結果が係数行列における加算・減算・乗算の結果に対応することが示される．ただし，この対応は1対1対応ではないため，多項式演算のすべての特性が行列演算でも受け継がれるわけではない．この対応によって保存される性質がどのようなものであるのかを，実際の演算との係わりとともに明らかにする．

多項式乗算を行列演算以外の方法で行うものとしては，離散的フーリエ変換（FFT）を用いる方法（Aho ら[8]，Pollard[10] 参照）やソーティングアルゴリズム（Horowitz[11]）がある．ソーティングアルゴリズムは完全に稠密またはきわめて疎な多項式の場合に有利な計算法である．また，FFT 法は非常に大きな次数の多項式の乗算にのみ有効であり，小規模な計算では他の方法よりもかえって計算効率が悪くなる．したがって実践的な多項式乗算法は FFT 法を基礎とし，これに古典的アルゴリズム（たたみ込みによる計算法）等を巧みに組み合わせた複合アルゴリズムとなっている（Moenck[9] 参照）．

本研究で示す乗算法は，単独で用いる場合には FFT 法等と比較して特に計算効率が良いとはいえない．しかしながら，本方法は多項式のべき乗の計算法に応用した場合にきわだった特長を示す．

† 奈良女子大学理学部
Faculty of Science, Nara Women's University

係数行列に基づく多項式のべき乗法は，一定の次数以下の項の計算だけが可能であるが，きわめて高いべき乗でも容易に計算ができるという特長を持っている．ここでは，べき乗計算に必要な係数行列の最小多項式や係数行列の再帰的な関係式（漸化式）について言及し，併せてそれらの多項式べき乗計算への応用の手法とアルゴリズムの定式化およびその評価も併せて行う．

2. 多項式の係数行列

ここでは，一変数多項式の一定次数以下の項の係数を蓄える係数行列を定義する．そして，係数行列間の演算と元の多項式間の演算との対応関係を示し，係数行列を用いた多項式演算の有効性を明らかにする．なお，行列に関する諸定義については藤岡[4]および斎藤[5]に従い，代数に関する諸定義は成田[1]，永田[2]，Waerden[3]，Berge[6]に従うものとする．

〔定義1〕（多項式の係数行列）

x についての一変数多項式 $p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ に対して，$p(x)$ の k 階の係数行列 $cmat_k(p(x))$ は $(k+1)$ 次の正方行列として次のように定義される．

$cmat_k(p(x))$ の i 行 j 列の要素 $c_{i,j}$ $(1\leqq i,j\leqq k+1)$ は次のように定義される．

$$c_{i,j}=\begin{cases}0 & (i<j \text{ のとき})\\ a_{i-j} & (i\geqq j \text{ のとき})\end{cases}$$

（ここで a_{i-j} は多項式 $p(x)$ の $(i-j)$ 次項の係数である．ただし，$i-j>n$ の場合には，$a_{i-j}=0$ とする）．

$cmat_k(p(x))$ を行列の形で書くと次のような下三角行列になる．

$$\begin{bmatrix} a_0 & 0 & \cdots & 0 & 0 & 0\\ a_1 & a_0 & & & & 0\\ \vdots & & & & & \vdots\\ a_{k-2} & & & a_0 & 0 & 0\\ a_{k-1} & a_{k-2} & & & a_0 & 0\\ a_k & a_{k-1} & a_{k-2} & \cdots & a_1 & a_0 \end{bmatrix}$$

〔例1〕

$p(x)=7x^5+3x^3+4x^2+5$ のとき，$p(x)$ の3階の係数行列 $cmat_3(p(x))$ は次のようになる．

$$cmat_3(p(x))=\begin{bmatrix}5&0&0&0\\0&5&0&0\\4&0&5&0\\3&4&0&5\end{bmatrix}$$

〔定理1〕

$p(x)$，$q(x)\in R[x]$ とすると，次の関係式が成立する．

$$cmat_k(p(x))+cmat_k(q(x))=cmat_k(p(x)+q(x))$$
$$cmat_k(p(x))\cdot cmat_k(q(x))=cmat_k(p(x)q(x)) \qquad k\geqq 0$$

（証明）

行列の定義より自明．

定理1の2つの関係式により，k 階係数行列の演算では，元の多項式間の加算・乗算の k 次以下の演算結果が保存されることがわかる（厳密な証明については付録の定理 2〜6 を参照のこと）．

3. 多項式のべき乗計算

多項式の計算を行う場合に，計算の手数の面で最も問題となるのが高次のべき乗計算である．

ここでは多項式のべき乗のすべての項の係数ではなく，一定の次数以下の項の係数のみが求められる算法に限って議論する．従来は，このような場合にはべき級数の乗算による方法が用いられてきた．

ここでは，Hamilton-Cayley の定理および行列の最小多項式を用いて係数行列のべき乗を計算し，これを用いて多項式の高次のべき乗計算を行う方法について述べる．本方法はアルゴリズムが単純であるため，計算を自動化することが容易である．

〔定理7〕（Hamilton-Cayley の定理）

n 次の正方行列 A はその固有方程式 $\det(\lambda I_n-A)=0$ の根である（ここで，λ は方程式の変数と考える）．ただし，I_n は n 次の単位行列であり，$\det(X)$ は正方行列 X と同じ要素からなる行列式を表す．

（証明は藤岡[4]の“4.8 固有値・固有ベクトルの性質”または斎藤[5]の系 3.5 参照）

一般に，n 次の固有多項式の係数は n^3 のオーダーで求められることが知られている（Knuth[7] 参照）．

次に，定理7により多項式のべき乗の係数を求める例を示す．

〔例2〕

$p(x)=7x^5+3x^3+4x^2+5$ とする．このとき，$\{p(x)\}^7$ の3次以下の項の係数を求めてみる．

まず，$p(x)$ の3階係数行列を求め，これを A とおく．

$$A=cmat_3(p(x))=\begin{bmatrix}5&0&0&0\\0&5&0&0\\4&0&5&0\\3&4&0&5\end{bmatrix}$$

$$\det(\lambda I_4-A)=(\lambda-5)^4$$
$$=\lambda^4-20\lambda^3+150\lambda^2-500\lambda+625$$

したがって，行列 A に対して定理7を適用すると，$A^4-20A^3+150A^2-500A+625I_4=0$ となる．すなわち，$A^4=20A^3-150A^2+500A-625I_4$ という関係式を繰り返し用いることにより，A^7 を求めることができる．

$$A^5=A\cdot A^4$$
$$=250A^3-2500A^2+9375A-12500I_4$$

以下同様にして A^6, A^7 も計算することができる．

$$A^7=21875A^3-262500A^2$$
$$+1093750A-1562500I_4$$

ここで，A^2, A^3 を行列乗算によって計算し，その値を上の関係式に代入することにより，A^7 の値は次のようになる．

$$A^7=\begin{bmatrix}78125 & 0 & 0 & 0\\ 0 & 78125 & 0 & 0\\ 437500 & 0 & 78125 & 0\\ 328125 & 437500 & 0 & 78125\end{bmatrix}$$

ゆえに $\{p(x)\}^7$ の3次以下の項は $328125x^3+437500x^2+78125$ となる．

定理7（Hamilton-Cayley の定理）を用いて係数行列のべき乗を求める方法は，多項式のべき乗を直接展開するのに較べると効率がよい．なぜなら，$\{p(x)\}^n$ の k 次以下の項を求める場合には，k 階係数行列 $cmat_k(p(x))=A$ およびそのべき乗 $A^2, A^3, \cdots, A^k$ は一度だけ計算しておけばよく，後は定理7から得られる漸化式を用いて A^n を $A^k, A^{k-1}, \cdots, A^2, A, I_{k+1}$ の一次結合として計算できるためである．

それでも漸化式を繰り返し適用していく計算はかなり大変である．したがって漸化式を簡略化する方法が必要とされる．

一般に定理7から得られる関係式よりも簡単な低い次数の行列関係式が存在することが知られている．それは最小多項式と呼ばれている．

〔定義2〕（最小多項式）

正方行列 A に対して，$g(A)=0$ となる多項式 $g(\lambda)$ の内でべき次数が最小でかつ最高次項の係数が1であるものを A の最小多項式という．

〔定理8〕

最小多項式は Hamilton-Cayley の定理から導かれる多項式（固有多項式）の因数となる（斎藤[5]の定理3.2 参照）．

一般に n 次の正方行列 A の最小多項式は，A の特性行列 (λI_n-A) の最後の単因子に等しい[5]ことが知られているが，この方法から最小多項式を求めるのは困難である．しかしながら，係数行列のような特殊な形式の行列の場合に限定すれば，さらに容易に最小多項式を求める方法が存在する．

〔定理9〕

多項式 $f(x)$ の定数項を a とするとき，$f(x)-a$ の最小次数の項の次数が u ならば，$f(x)$ の k 階係数行列 $cmat_k(f(x))$ の最小多項式は $(\lambda-a)^r$ となる（ここで r は $r>k/u$ を満たす最小の整数である）．

（証明）

定理8より $cmat_k(f(x))$ の最小多項式は $cmat_k(f(x))$ の固有多項式 $\det(\lambda I_{k+1}-cmat_k(f(x)))=(\lambda-a)^{k+1}$ の因数となる．よって $cmat_k(f(x))$ の最小多項式は $(\lambda-a)^i$（ただし $i\leqq k+1$）となる．よって，i の値が確定されれば最小多項式の実際の形が定まる．

定理1より，

$$cmat_k(f(x))-aI_{k+1}$$
$$=cmat_k(f(x))+cmat_k(-a)$$
$$=cmat_k(f(x)-a)$$

となる．

一方，$f(x)-a$ の最小次数の項の次数は u であるので，明らかに $\{cmat_k(f(x)-a)\}^{r-1}\neq 0$ かつ $\{cmat_k(f(x)-a)\}^r=0$ となる．

したがって，$\{cmat_k(f(x))-aI_{k+1}\}^{r-1}\neq 0$ かつ $\{cmat_k(f(x))-aI_{k+1}\}^r=0$ となる．

よって，定義2より $(\lambda-a)^r$ が $cmat_k(f(x))$ の最小多項式となる．（証明終）

〔定理10〕

定理9の最小多項式から $\{f(x)\}^n$ の k 次以下の項の各係数を n のオーダーの計算量で計算可能である．

（証明）

多項式のべき乗の k 次以下の項のみを求めるので，k を固定して考えることができる．

n 階係数行列 A の最小多項式が $g(\lambda)=\lambda^r+g_{r-1}\lambda^{r-1}+\cdots+g_2\lambda^2+g_1\lambda+g_0$（ここで $g_{r-1}, \cdots, g_2, g_1, g_0$ は定数）である場合に，最小多項式の定義より $g(A)=0$ が成立するので，$A^r=-g_{r-1}A^{r-1}-\cdots-g_2A^2-g_1A-g_0I_{k+1}$ が成り立つ（I_{k+1} は $(k+1)$ 次の単位行列を表す）．

この関係式を漸化式として必要に応じて繰り返し用いることにより，係数行列 A の任意のべき乗を計算することができる．例えば，

$$A^{r+1}=A\cdot A^r$$
$$=-g_{r-1}A^r-\cdots-g_2A^3-g_1A^2-g_0A$$

$$= -g_{r-1}(-g_{r-1}A^{r-1} - \cdots - g_2A^2 - g_1A$$
$$- g_0I_{k+1}) - g_{r-2}A^{r-1} - \cdots - g_2A^3$$
$$- g_1A^2 - g_0A$$
$$= \sum_{i=1}^{r-1} \{(g_{r-1}g_i - g_{i-1})A^i\} + g_{r-1}g_0I_{k+1}$$

となる．このときの係数の計算には，乗算 r 回，加算 $(r-1)$ 回を必要とする．以下同様の手順で $A^{r+2}, A^{r+3}, \cdots$ も計算できるので，A^n を $A^{r-1}, \cdots, A^2, A, I_{k+1}$ の一次結合として表す場合の係数を求めるまでには，乗算 $r(n-r)$ 回，加算 $(r-1)(n-r)$ 回を必要とする．一方，k が固定されているために，r も一定となり，$A^{r-1}, \cdots, A^2$ の計算時間は n には無関係に一定である．したがって，A^n の計算は n のオーダーの計算時間で行うことができる． (証明終)

(注意)

定理9の最小多項式は非展開型（$(\lambda-a)^r$ の形式）ならば r を k/u の1回の除算（商は切り上げを行う）で求めることで得られ，これを展開したとしても高々 k についての多項式時間で最小多項式を求めることができ，上記の $f(x)$ のべき乗数 n の関数とはならない．したがって，定理 10 では，最小多項式自体の係数計算のオーダーは無視することができる．

〔例3〕

$p(x)=7x^5+3x^3+4x^2+5$ とする．

$\{p(x)\}^7$ を展開して3次以下の項を求めることを最小多項式を用いて行う．

定理9により，この場合の3階係数行列 $A=cmat_3(p(x))$ の最小多項式は $(\lambda-5)^2=\lambda^2-10\lambda+25$ となる．したがって，$A^2-10A+25I_4=0$ が成立する．この関係式 $A^2=10A-25I_4$ を繰り返し用いて，A^7 を求めることができる．

$$A^3=A\cdot A^2=A(10A-25I_4)$$
$$=10A^2-25A=75A-250I_4$$

以下同様にして A^4, A^5, A^6, A^7 も計算できる．

$$A^7=109375A-468750I_4$$

したがって，A^7 の値は次のようになる．

$$A^7=\begin{bmatrix} 78125 & 0 & 0 & 0 \\ 0 & 78125 & 0 & 0 \\ 437500 & 0 & 78125 & 0 \\ 328125 & 437500 & 0 & 78125 \end{bmatrix}$$

ゆえに $\{p(x)\}^7$ の3次以下の項は $328125x^3+437500x^2+78125$ となる．

ここで，係数行列のべき乗の二項展開という観点から多項式のべき乗を求める方法を考える．

〔定理 11〕

多項式 $f(x)$ の定数項を a とするとき，$a\neq 0$ でありかつ $f(x)-a$ の最小次数の項の次数が u であるならば，次のような関係式が成立する．

$$\{cmat_k(f(x))\}^n$$
$$= \sum_{m=0}^{r-1} {}_nC_m a^{n-m} \{cmat_k(f(x)) - aI_{k+1}\}^m$$

（ここで r は $r>k/u$ を満たす最小の整数であり，${}_nC_m=n!/(n-m)!m!$ であり，I_{k+1} は $k+1$ 次の単位行列である）

(証明)

係数行列は加法だけでなく乗法に関しても可換であるので，次のようにして二項展開することができる．

$$\{cmat_k(f(x))\}^n$$
$$= [\{cmat_k(f(x)) - aI_{k+1}\} + aI_{k+1}]^n$$
$$= \sum_{m=0}^{n} {}_nC_m (aI_{k+1})^{n-m} \{cmat_k(f(x)) - aI_{k+1}\}^m$$
$$= \sum_{m=0}^{n} {}_nC_m a^{n-m} \{cmat_k(f(x)) - aI_{k+1}\}^m$$

ここで，$r\leqq m\leqq n$ の範囲の m については $\{cmat_k(f(x))-aI_{k+1}\}^m = O_{k+1}$ となる（O_{k+1} は $(k+1)$ 次の零行列を表す）ので，これを用いて式を簡略化すると次のような関係式が導かれる．

$$\{cmat_k(f(x))\}^n$$
$$= \sum_{m=0}^{r-1} {}_nC_m a^{n-m} \{cmat_k(f(x)) - aI_{k+1}\}^m$$

(証明終)

(注) 定理 11 において $f(x)$ の定数項 a が0でないという仮定は不自然なものではない．なぜなら $a=0$ ならば，$f(x)$ のある次数以上のべき乗では k 次以下の項の係数がすべて0となり，べき乗を計算する必要がないためである．

多項式 $f(x)$ の k 次以下の項のみからなる部分を $\overline{f(x)}^k$ で表すと定理 11 から次の系1が導かれる．

〔系1〕

多項式 $f(x)$ の定数項を a とするとき，$a\neq 0$ でありかつ $f(x)-a$ の最小次数の項の次数が u であるならば，次のような関係式が成立する．

$$\{\overline{f(x)}^k\}^n = \sum_{m=0}^{r-1} {}_nC_m a^{n-m} \{\overline{f(x)-a}^k\}^m$$

（ここで r は $r>k/u$ を満たす最小の整数であり，${}_nC_m=n!/(n-m)!m!$ である）

(証明)

定理 11 の関係式を多項式で表現することにより明

らかである．　　(証明終)

次の定理は多項式のべき乗計算の計算量の評価を行うものである．

〔定理 12〕

定理 11 の系 1 の方法によって $\{f(x)\}^n$ の k 次以下の項を求める場合，$\log_2 n$ のオーダーの計算量で計算可能である．

(証明)

多項式のべき乗の k 次以下の項のみを求めるので，k を固定して考えることができる．したがって，系 1 の関係式の右辺の $\overline{\{\overline{f(x)}^k-a\}^m}^k$ はすべて k 次以下の定係数多項式であり，この部分の計算量は $f(x)$ のべき乗数 n には関係せず一定である（この計算量を定数 c_1 とする）．したがって ${}_nC_m a^{n-m}$ の部分の計算量および ${}_nC_m a^{n-m}$ と $\overline{\{\overline{f(x)}^k-a\}^m}^k$ の積和（一次結合）の計算量によって $\overline{\{f(x)\}^n}^k$ 全体の計算量が定まる．

$a^2=a\cdot a, a^4=a^2\cdot a^2, \cdots$ のように計算し，これらの値を適当に組み合わせて a^{n-m} を計算すると，その計算量は $\log_2(n-m)$ に比例したものになる．したがって，${}_nC_m a^{n-m}$ の部分は高々 $c_2\log_2(n-m)+c_3 m$ 回（ここで c_2, c_3 は n の値によらない定数）の乗除算で計算可能である．

ゆえに，$\overline{\{f(x)\}^n}^k$ 全体の計算量は $\sum_{m=0}^{r-1}\{c_1+c_2\log_2(n-m)+c_3 m\}+c_4 \leqq c_5\log_2 n+c_6$ となる（ここで c_5, c_6 は n の値によらない定数である．また c_4 は積和をつくるのに要する計算量を表す）．したがって，$\{f(x)\}^n$ の k 次以下の部分は $\log_2 n$ のオーダーの計算時間で計算可能である．　　(証明終)

(注)　定理 11 とその系 1 との違いは，べき乗を多項式の和で計算するか係数行列の和から計算するかの違いだけであり，いずれの場合もこの部分の計算量は n に無関係であるので，定理 11 の方法の場合も $\log_2 n$ のオーダーの計算量となる．

〔例 4〕

例 3 と同じく，$p(x)=7x^5+3x^3+4x^2+5$ として，$\{p(x)\}^7$ の 3 次以下の項を求める．

ここでは定理 11 の系 1 の関係式を用いる．系 1 により，次の式が成立する．

$$\overline{\{p(x)\}^7}^3=\sum_{m=0}^{r-1}{}_7C_m 5^{7-m}\overline{\{\overline{p(x)}^3-5\}^m}^3$$

r は $r>3/2$ を満たす最小の整数すなわち 2 であるので，

$$\begin{aligned}\overline{\{p(x)\}^7}^3&=\sum_{m=0}^{1}{}_7C_m 5^{7-m}\overline{\{\overline{p(x)}^3-5\}^m}^3\\&={}_7C_0 5^7\\&\quad+{}_7C_1 5^6\overline{\{(3x^3+4x^2+5)-5\}}^3\\&=328125x^3+437500x^2+78125\end{aligned}$$

となる．

他の方法では多項式の高次のべき乗を求めることは実際には困難であるが，定理 11 の系 1 の方法を用いれば，上の例と同様にして $\{p(x)\}^{100}$ の 3 次以下の項なども次のように容易に求められる．

$$\begin{aligned}\overline{\{p(x)\}^{100}}^3&=\sum_{m=0}^{1}{}_{100}C_m 5^{100-m}\overline{\{\overline{p(x)}^3-5\}^m}^3\\&={}_{100}C_0 5^{100}+{}_{100}C_1 5^{99}(3x^3+4x^2)\\&=300\cdot 5^{99}x^3+400\cdot 5^{99}x^2+5^{100}\end{aligned}$$

4. むすび

係数行列を用いることにより，一変数多項式間の加減算および乗算における演算結果である多項式の一定次数以下の項の係数が容易に求められることを示した．係数行列は多項式の高次項の係数の情報を捨てることによって得られる．付録の定理 6 において，係数行列による高次項を除いた演算の正当性が厳密に示されている．これにより係数行列では多項式の一定の次数以下の項の係数だけを計算可能であることが理論的に保証される．

係数行列による演算は多項式の高次のべき乗計算に応用した場合に特に有効性が高い．

従来の計算方法で多項式の高次のべき乗の一定の次数以下の項を求めるにはべき級数の乗算等のアルゴリズムを必要とした．

定理 9, 10 および例 3 で示したように，係数行列の最小多項式に関する関係式を用いれば，多項式のべき乗計算を漸化式の計算に置き換えて容易に行うことができる．この方法はべき乗数 n に比例した計算時間を必要とするために，n が比較的小さくかつ係数行列の階数が大きい場合に有効である．

定理 11 系 1 の方法は直接的には係数行列を用いていないが，その基礎理論は定理 11 の係数行列の関係式によっている．さらに，定理 12 に示したように，定理 11 系 1 の方法を用いれば $\{f(x)\}^n$ の k 次以下の項を $\log_2 n$ のオーダーの計算量で計算できる．

完全に同じ条件ではなく k の値を n に固定した形での比較になるが，同様の計算を従来の方法で行うと次のようになる．$P(s)=f(s)$, $Q(s)=s^n$ とすると，

$Q(P(x))=\{f(x)\}^n$ となるので，Brent, Kung[12]の関数合成（composition）の第二アルゴリズム（アルゴリズム 2.2）を用いて多項式のべき乗 $\{f(x)\}^n$ の n 次以下の項の係数を求めることができる．この場合の演算回数は $\mathrm{COMP}(n)=O((n\cdot\log_2 n)^{1/2}M(n))$ である（ここで $M(n)$ は積の n 次以下の項のみを求める場合の演算回数である）．乗算に FFT を用いた場合，$\mathrm{COMP}(n)=O((n\cdot\log_2 n)^{3/2})$ となる[12]が，これよりも定理 11 系 1 の方法の方が計算量が少ないことがわかる．

理工学における各種の近似計算では，結果的に見ると多項式の低次項のみが必要とされる場合が多い．したがって，実用面から見ても係数行列に基づく多項式のべき乗計算はこれらの近似計算にきわめて有効性が高いと考えられる．今後の課題としては，多変数の多項式への定義の拡張が挙げられる．

参考文献

1) 成田正雄：イデアル論入門，共立出版（1970）．
2) 永田雅宜：抽象代数への入門，朝倉書店（1967）．
3) van der Waerden, B. L.: *Moderne Algebra*, Springer (1937).
4) 藤岡 茂：線形代数入門，培風館（1968）．
5) 斎藤正彦：線形代数入門，東京大学出版会（1966）．
6) Berge, C.: *Principes de Combinatoire*, DUNOD (1968).
7) Knuth, D. E.: *The Art of Computer Programming*, Vol. II, *Seminumerical Algorithms*, 2nd ed., Addison Wesley (1969).
8) Aho, A. V., Hopcroft, J. E. and Ullman, J. D.: *The Design and Analysis of Computer Algorithms*, Addison-Wesley (1974).
9) Moenck, R. T.: Practical Fast Polynomial Multiplication, *Proc. ACM SYMSAC '76*, pp. 136-148 (1976).
10) Pollard, J. M.: The Fast Fourier Transform in a Finite Field, *Math. Comp.*, Vol. 25, No. 114, pp. 365-374 (1971).
11) Horowitz, E.: A Sorting Algorithm for Polynomial Multiplication, *J. ACM*, Vol. 22, No. 4, pp. 450-462 (1975).
12) Brent, R. P. and Kung, H. T.: Fast Algorithms for Manipulating Formal Power Series, *J. ACM*, Vol. 25, No. 4, pp. 581-595 (1978).

付　録

k 階係数行列と元の多項式間の関係を厳密に示すと次のようになる．

〔定理 2〕

n 階係数行列の集合 C_n は行列の加法に関して可換群をなす（これを係数行列群と呼ぶ）．

（証明）

行列の定義より自明．

〔定理 3〕

n 階係数行列の集合 C_n は行列の加法・乗法に関して可換環をなす（これを係数行列環と呼ぶ）．

（証明）

行列の積の定義よりただちにわかる．

加法に関する多項式群 $G[x]$ に対応する n 階係数行列群を $M_n[G[x]]$ で表す．

〔定理 4〕

多項式群 $G[x]$ から n 階係数行列群 $M_n[G[x]]$ への全射準同型写像が存在する．

（証明）

$cmat_{n,G}: G[x]\rightarrow M_n[G[x]]$ が全射となることは，定義 1 より明らかである．$cmat_{n,G}$ が準同型写像となることは定理 1 より明らかである．　（証明終）

多項式環 $R[x]$ に対応する n 階係数行列環を $M_n[R[x]]$ で表す．

〔定理 5〕

多項式環 $R[x]$ から n 階係数行列環 $M_n[R[x]]$ への環全準同型写像が存在する．

（証明）

$cmat_{n,R}: R[x]\rightarrow M_n[R[x]]$ が全射となることは，定義 1 より明らかである．$cmat_{n,R}$ が環準同型写像となることは，定理 1 より明らかである．　（証明終）

（注意）　上記の定理では，写像 $cmat_n$ が群の演算を含めた写像であることを強調するために，$cmat_{n,G}$ と表している．同様の理由で，写像 $cmat_n$ が環の演算を含めた写像であることを強調するために，$cmat_{n,R}$ と表している．

〔定理 6〕

n 階係数行列環 $M_n[R[x]]$ は余剰環 $R[x]/Ker(cmat_{n,R})$ と環同型である．

（証明）

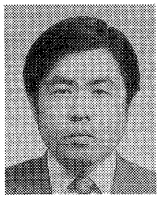
定理 5 より $cmat_{n,R}$ は環全準同型写像となるので，環における準同型定理（成田[1]の定理 1.23 参照）により，$R[x]/Ker(cmat_{n,R})$ から $M_n[R[x]]$ への同型写像が存在することが証明される．　（証明終）

定理 6 は，多項式における加算・乗算と係数行列における加算・乗算との重要な関係を示している．写像の核 $Ker(cmat_{n,R})$ は n 次以下の項の係数がすべて

0であるような多項式全体からなる集合であるので，$R[x]/Ker(cmat_{n,R})$ の各要素は多項式の集合 $R[x]$ の要素の内で n 次よりも大きい次数の項を無視すると同じ多項式となるようなものをひとまとめにした同値類を表している（例えば，$7x^5+3x^3+4x^2+5$ と $8x^7+4x^5+3x^3+4x^2+5$ は $R[x]$ の異なる要素であるが，$R[x]/Ker(cmat_{3,R})$ においては一つの類に属し，同一視される）．

定理6はこの同値類と n 階係数行列が環同型であることを示している．このことは，n 階係数行列における演算は元の多項式の演算に対応するが，その対応は多項式の n 次以下の項の係数だけに限られることを示している．これは，係数行列での演算が元の多項式よりも少ない情報に基づいて行われることによる．

(平成5年4月28日受付)
(平成6年3月17日採録)



西岡 弘明（正会員）

昭和27年12月生．昭和51年大阪大学工学部通信工学科卒業．昭和56年大阪大学大学院工学研究科通信工学専攻博士課程修了（工学博士）．同年山口大学理学部助手．昭和61年福井大学工学部助教授．昭和62年奈良女子大学理学部助教授，現在に至る．人工知能，自動定理証明，プログラム理論，記号処理，組合せ理論の応用に関する研究に従事．電子情報通信学会，人工知能学会，IEEE 各会員．