愛知工業大学研究報告
第３８号Ａ平成１５年

ある行列等式に関する環論と圏論の試み
A ring-theoretical and categorical attempt concerning a certain matrix equation

濱井健人・隅山孝夫・鈴木元・吉田英弘
Taketo Hamai, Takao Sumiyama, Gen Suzuki, Hidehiro Yoshida

2つの n 次正方行列 A, B が $AB = E_n$ をみたせば必然的に $BA = E_n$ となることはよく知られた事実である。このことの証明は, 行列式を用いて大学初年級程度の線形代数学の知識の範囲内でできる。しかしこの命題は本来行列式とは無関係であり, より一般的な代数学の定理から導くことができる。この論文においては, 上の命題を系として含む一般的な代数学の定理を提示する。同時に, 工学部系の数学教育では扱い難い環と圏の理論を, 上述のことに関連させて教育内容とし得ることを示す。

この論文は, 愛知工業大学情報通信工学科平成12年度と平成13年度の卒業論文（参考文献[2], [6]）を発展させたものである。

§0. 問題の所在

複素数を成分とする n 次正方行列全体の集合を $M_n(\mathbf{C})$ で表す。n 次単位行列を E_n で表わす。よく知られているように, 集合 $M_n(\mathbf{C})$ において, 行列の積 XY を定義することができる。この積は結合法則 $(XY)Z = X(YZ)$ をみたすが, 交換法則 $XY = YX$ はみたさない。従って, 次の事実は初めて線形代数学を学ぶ学生にとって決して自明なことではない。

事実(F) 実数または複素数を成分とする行列 A, B が $AB = E_n$ をみたすならば, $BA = E_n$ である。

通常, 上の事実(F)は行列式(det)を用いて次のように証明される。

$AB = E_n$ とする。ならば,

$\det(A)\det(B) = \det(AB) = \det(E_n) = 1$

より $\det(A) \neq 0$。

$G = (\det(A))^{-1}(\tilde{a}_{ji})$　　（$\tilde{a}_{ji}$ は A の (j,i) 余因子）

とおくと, 行列の成分を計算することによって

$AG = GA = E_n$

であることがわかる。

$B = E_nB = (GA)B = G(AB) = GE_n = G$

であるから,

$BA = GA = E_n$。

この証明は行列式の知識がない者には理解できない。また, 基礎体（上の実数体, 複素数体に相応するもの）が非可換な場合, 例えばHamiltonの4元数体（後述）を成分とする行列についても上の事実は成立するのであるが, 非可換な場合は通常の仕方では行列式が定義できないために, この証明は無効である。

§1. 基本概念

以下, 自然数全体の集合を $\mathbf{N}$ で表わす。$\mathbf{N} = \{0, 1, 2, \cdots\}$。$\phi$ は空集合を表わす。

集合 A, B に対して, 集合

$\{(a,b) \mid a \in A, b \in B\}$

をAとBの直積集合といい, $A \times B$ で表わす。

ϕでない集合Mに内算法

$\sigma : M \times M \to M$

$(x,y) \longmapsto x+y$

が定義されていて, 次の(1)-(4)の公理がみたされるとき, Mは加群であるという。

(1) $(x+y)+z = x+(y+z)$

(2) $x+y=y+x$

(3) Mの任意の元xについて

$x+n=x$

となるようなMの特定の元nが存在する。

(4) Mの任意の元xに対して,

$x+x'=n$

となるようなMの元x'が存在する。

Mが加群であるとき, 内算法$\sigma(x,y)=x+y$をMにおける和という。(3)の性質をみたす元nはMに唯一である。この元nをMの零元といい, 記号0で表わす。(4)の性質をみたすMの元x'は, xに対して一意的である。この元x'を$-x$と表わす。$x+(-y)$を$x-y$と表わす。

Mは加群であるとする。Mのϕでない部分集合M'が次の条件(5)をみたすとき, M'はMの部分加群であるという。

(5) $x, y \in M'$ ならば$x-y \in M'$

Rは和$x+y$が定義された加群であるとする。集合Rにもうひとつの内算法

$\pi : R \times R \to R \quad (x,y) \longmapsto xy$

が定義されていて, 次の公理がみたされるとき, Rは環であるという。

(6) $(xy)z = x(yz)$

(7) $(x+y)z = xz+yz$

(8) $x(y+z) = xy+xz$

これだけで環という場合もあるが, 通常は次の公理を付け加える。

(9) Rの任意の元xについて

$ex = xe = x$

となるようなRの特定の元eが存在する。

(10) 上の(4)における元nは(9)における元eの条件をみたさない。

ここでは上の(9), (10)の条件を込めて環と呼ぶことにする。

Rが環であるとき, 内算法$\pi(x,y)=xy$をRにおける積という。(8)の性質をみたす元eはRに唯一である。この元eをRの単位元と呼ぶ。

環Rの任意の元x, yについて

(11) $xy=yx$

が成り立つとき, Rは可換環であるという。

Rは環であるとし, Mは加群であるとする。算法

$\mu : R \times M \to M \quad (a, x) \longmapsto ax$

が定義されていて, 次の(12)-(15)の公理がみたされるとき, MはR-左加群であるという。

(12) $(a+b)x = ax + bx\ (a, b \in R, x \in M)$

(13) $a(x+y) = ax + ay\ (a \in R, x, y \in M)$

(14) $(ab)x = a(bx)\ (a, b \in R, x \in M)$

(15) $1x = x\ (x \in M)$

Rは環, M, M'はR-左加群であるとする。写像$f : M \to M'$が次の条件(16),(17)をみたすとき, fはR-準同形写像であるという。

(16) $f(x+y) = f(x) + f(y)$

(17) $f(ax) = af(x)\ (a \in R, x \in M)$

Rは環, MはR-左加群であるとする。Mの部分加群M'が次の条件(18)をみたすとき, M'はMのR-左部分加群であるという。

(18) $a \in R, x \in M'$ ならば$ax \in M'$。

Mを左R-加群とする。$x_1, x_2, \cdots, x_n$ をMの固定された元とするとき,

$a_1x_1 + a_2x_2 + \cdots + a_nx_n\ (a_1, a_2, \cdots, a_n \in R)$

の形に書かれるMの元の全体はMのR-左部分加群である。このR-左部分加群を

$Rx_1 + Rx_2 + \cdots + Rx_n$

と表わす。

R-左加群Mが有限生成であるとは,

$M = Rx_1 + Rx_2 + \cdots + Rx_n$

となるようなMの固定された有限個の元$x_1, x_2, \cdots, x_n$ が存在することをいう。

R-左加群$M = Rx_1 + Rx_2 + \cdots + Rx_n$ において, $r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0\ \ (r_1, r_2, \cdots, r_n \in R)$ となるのが, $r_1 = r_2 = \cdots = r_n = 0$ のときに限るならば, $M = Rx_1 + Rx_2 + \cdots + Rx_n$は直和であるという。このとき, R-左加群Mを$M = R^n$ と表わし, 階数nの自由R-左加群という。

MはR-左加群, M'はそのR-左部分加群であるとする。Mの元x, y の間に

$x \sim y \Longleftrightarrow x - y \in M'$

によって同値関係$\sim$を定義することができる。$x \in M$ と$x \sim x'$の関係にあるMの元x'の全体をxの同値類といい, $x + M'$ で表わす。このような同値類全体の集合をM/M' で表わすことにする。

M/M' の元（同値類）の間に,

$(x + M') + (y + M') = (x + y) + M'$

によって和$+$を定義すると, 集合M/M'はこの和によってR-左加群となる。このR-左加群をMのM'による剰余類群という。

Mは$\{0\}$と異なるR-左加群であって, MのR-左部分加群はMと$\{0\}$ 以外にないとき, Mは単純R-左加群であるという。

MはR-左加群であるとする。MのR-左部分加群の列

(19) $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$

があって, 各$M_i/M_{i-1}\ (1 \leq i \leq n)$ が単純R-左加群であるとき, R-左部分加群の列(19)をMの組成列と呼ぶ。nを組成列(19)の長さという。

定理 1. (Jordan-Hölder Theorem, 参考文献[1], Chapter 3, §11, p. 135) M は R-左加群とする。

$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_{s-1} \subset M_s = M$

$\{0\} = N_0 \subset N_1 \subset \cdots \subset N_{t-1} \subset N_t = M$

がどちらも M の組成列であるとすれば, $s = t$ である。

M は R-左加群とし, M の R-左部分加群の列

(20) $M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$

を, M の R-左部分加群の上昇列という。ある自然数 N が存在して,

$m \geq N$ ならば $M_m = M_N$

となるとき, R-左部分加群の上昇列(20)は滞状であるという。

R-左加群 M の任意の R-左部分加群の上昇列が滞状であるとき, R-左加群 M はNoether的であるという。

M は R-左加群とし, M の R-左部分加群の列

(21) $M_1 \supset M_2 \supset \cdots \supset M_n \supset \cdots$

を, M の R-左部分加群の下降列という。ある自然数 N が存在して,

$m \geq N$ ならば $M_m = M_N$

となるとき, R-左部分加群の下降列(21)は滞状であるという。

R-左加群 M の任意の R-左部分加群の下降列が滞状であるとき, R-左加群 M はArtin的であるという。

R は環とする。R は作用 ax $(a, x \in R)$ によりそれ自身 R-左加群と見ることができる。このように R-左加群と見て R がNoether的であるとき, 環 R は左Noether的であるという。また, R-左加群と見て R がArtin的であるとき, 環 R は左Artin的であるという。

定理 2. (参考文献[1], Chapter 4, §15, p. 174, Corollary 15.21) R が左Artin的環であるとするならば, R-左加群 M に関する次の(i)-(iv)の条件は互いに同値である。

(i) M は有限生成である。

(ii) M はNoether的である。

(iii) M はArtin的である。

(iv) M の組成列が存在する。

以下, R は環とする。a は環 R の元として,

$ab = e, \ ca = e$

をみたす R の元 b, c が存在するとき, a は R の正則元であるという。このとき,

$b = eb = (ca)b = c(ab) = ce = c$

となる。b を a の逆元という。

元 a に対して, a の逆元はもし存在すれば一意的である。環 R の 0 でない任意の元が正則元であるとき, R は斜体であるという。可換環かつ斜体である環を体という。

実数の全体 $\mathbf{R}$ (実数体), 複素数の全体 $\mathbf{C}$ (複素数体) 等は体の例である。

$\{1, e_1, e_2, e_3\}$ を基底とする実数体 $\mathbf{R}$ 上の線形空間に,

$e_1^2 = e_2^2 = e_3^2 = -1,$

$e_1 e_2 = -e_2 e_1 = e_3,$

$e_2e_3 = -e_3e_2 = e_1,$

$e_3e_1 = -e_1e_3 = e_2$

によって積を定義することができる。これがHamiltonの4元数体であり, 体ではない斜体の例である。

環Rの元fが$f^2 = f$をみたすとき, fは冪等元であるという。環Rの冪等元からなる集合$\{f_i\}_{i\in I}$が条件$f_if_j = 0\ \ (i \neq j)$をみたすとき, $\{f_i\}_{i\in I}$を互いに直交する冪等元の集合という。

環Rの元を成分とするn次正方行列全体を$M_n(R)$で表わす。$M_n(R)$における和を

$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$

で定義する。また, $M_n(R)$の2つの元$A = (a_{ij})$, $B = (b_{ij})$に対して, (i, j)成分が$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$で与えられる$n$次正方行列$C = (c_{ij})$を$A$と$B$の積とする。

集合$M_n(R)$は上で定義された和と積について環となる。この環$M_n(R)$を環R上のn次行列環という。$M_n(R)$の単位元は単位行列

$E_n = (\delta_{ij}),$

$\delta_{ij} = 0\ (i \neq j), \delta_{ij} = 1\ (i = j)$

である。

$A = (a_{ij})$を$M_n(R)$の元とする。$R^n = Rx_1 + Rx_2 + \cdots + Rx_n$は階数$n$の自由$R$-左加群とし, R^nの元xに対して,

$$Ax = \sum_{i=1}^{n}(\sum_{j=1}^{n} a_{ij}r_j)x_i$$

と定めることにより, R^nは$M_n(R)$-左加群となる。

環Rは, Rの積$ax\ (a, x \in R)$によってR-左加群と見ることができる。RをR-左加群と見たときの, RのR-左部分加群をRの左イデアルという。R-左加群と見てRがNoether的であるとき, 環Rは左Noether的であるといわれる。また, R-左加群と見てRがArtin的であるとき, 環Rは左Artin的であるといわれる。もし環Rが左Artin的であれば, Rは左Noether的である（参考文献[4], p. 148, 定理5.4.1）。

§2. 環の立場から

定理 3. もしRが左Artin的ならば, R上のn次行列環$M_n(R)$も左Artin的である。

証明. 定理1により, R-左加群Rの組成列

$\{0\} = I_0 \subset I_1 \subset \cdots \subset I_{m-1} \subset I_m = R$

が存在する。第i行がI_jの元より成り, 他の行の成分は全て0である行列全体を$A_{j,i}$とすると, ·

$\{0\} \subset A_{1,1} \subset A_{2,1} \subset \cdots \subset A_{m,1} \subset$

$A_{1,2} + A_{m,1} \subset A_{2,2} + A_{m,1} \subset \cdots \subset A_{m,2} + A_{m,1} \subset \cdots$

$A_{1,n} + A_{m,n-1} + \cdots + A_{m,1} \subset A_{m-1,n} + A_{m,n-1} + \cdots + A_{m,1} \subset A_{m,n} + A_{m,n-1} + \cdots + A_{m,1}$

$= M_n(R)$

は$M_n(R)$-左加群$M_n(R)$のひとつの組成列である。

命題 4. 左Artin的環Rにおいて, $ab = e$ならば, $ba = e$である。

証明. Rの左イデアルの下降列

$Ra \supset Ra^2 \supset \cdots \supset Ra^n \supset \cdots$

は滞状であるから, $Ra^n = Ra^{n+1}$ となる正整数nが存在する。従って, $a^n = ua^{n+1}$ となる$u \in R$ が存在する。

$0 = (e - ua)a^n = (e - ua)a^{n-1}ab$

$= (e - ua)a^{n-1} = \cdots = e - ua$

より$ua = e$。従って,

$b = eb = (ua)b = u(ab) = ue = u$。よって$ba = e$である。

定理3と命題4から次の定理を得る。

定理 5. Rは左Artin的環であるとする。$M_n(R)$ において$AB = E_n$ であれば, $BA = E_n$ である。

実数体$\mathbf{R}$, 複素数体$\mathbf{C}$はいずれも体であり, 体は左Artin的環である（体Kの左イデアルは$\{0\}$ とKしかない）から, 上の定理5は冒頭の事実(F)を特殊な場合として含んでいる。

また, 定理5は次の様に拡張できる。

定理 6. Rは左Noether的環であるとする。$M_n(R)$ において$AB = E_n$ であれば, $BA = E_n$ である。

証明. 自由R-左加群R^nは有限生成であるから, Noether的である（参考文献[3], p. 30, 命題6.2)。

先ず, 環$M_n(R)$ には, 互いに直交する冪等元の無限集合が含まれないことを示す。仮に, $e_1, e_2, \cdots, e_m, \cdots$ が$M_n(R)$の互いに直交する冪等元の無限集合であるとする。ならば,

$e_1(R^n) \subset e_1(R^n) + e_2(R^n) \subset \cdots \subset e_1(R^n) + e_2(R^n) + \cdots + e_m(R^n)$

$\subset e_1(R^n) + e_2(R^n) + \cdots + e_m(R^n) + e_{m+1}(R^n) \subset \cdots$

はR^nのR-左部分加群の滞状でない上昇列である。これは, R^nがNoether的であることに反する。

$M_n(R)$の元A, Bが$AB = E_n,\ BA \neq E_n$ をみたすとする。このとき, 容易に確かめられるように,

$e_1 = E_n - BA, e_2 = BA - B^2A^2, \cdots, e_m = B^{m-1}A^{m-1} - B^mA^m, \cdots$

は, 互いに直交する$M_n(R)$の冪等元の無限集合であり, 上に示したことと矛盾する。

以上, 左Artin的または左Noether的な環について述べたことは全て, 定義から始めて左右対称に入れ替えることにより, 右Artin的または右Noether的な環についても同様に主張される。

§3. 圏の立場から

以下において, 領域という言葉は無定義用語とする（参考文献[3], 第4章 §22 参照)。

次のものが与えられているとき, $\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ は圏(category)であるという。

(1) $\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ の対象(object)と呼ばれる領域Kがある。Aが$\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ の対象であることを$A \in K$ と表わす。

(2) $\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ の2つの対象A, Bに対して, 射型(morphism)と呼ばれるものの集合$mor_{\mathsf{K}}(A, B)$が決まる。

(3) $\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ の３つの対象 A, B, C に対して, 合成(composition)と呼ばれる写像

$mor_{\mathsf{K}}(A,B) \times mor_{\mathsf{K}}(B,C) \to mor_{\mathsf{K}}(A,C)$

が定められている。

$f \in mor_{\mathsf{K}}(A,B)$ であるとき, $f : A \to B$ と表す。$f : A \to B$ と $g : B \to C$ の合成を $g \circ f$ と表す。

更に, 次がみたされるものとする。

(i) $(A,B) \neq (A',B')$ のとき, $mor_{\mathsf{K}}(A,B) \cap mor_{\mathsf{K}}(A',B') = \phi$。

(ii) 任意の $B \in K$ に対して, 次をみたす $I_B \in mor_{\mathsf{K}}(B,B)$ が存在する。

任意の $f : A \to B$ に対し, $I_B \circ f = f$。

任意の $g : B \to C$ に対し, $g \circ I_B = g$。

(iii) 任意の $f : A \to B$, $g : B \to C$, $h : C \to D$ について, $h \circ (g \circ f) = (h \circ g) \circ f$。

$B \in K$ に対して(iii)の $I_B \in mor_{\mathsf{K}}(B,B)$ は一意的に決まることがわかる。

領域を無定義用語としたので, 圏の例を挙げる。

例1. 集合の圏。対象は集合, 射型は写像である。

例2. 実数体 $\mathbf{R}$ 上の線形空間の圏。対象は実数体 $\mathbf{R}$ 上の線形空間, 射型は $\mathbf{R}$-線形写像である。

$\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ は圏であるとし, $A, B \in K$ とする。$f \in mor_{\mathsf{K}}(A,B)$ に対して, $g \in mor_{\mathsf{K}}(B,A)$ で $g \circ f = I_A$, $f \circ g = I_B$ をみたすものが存在するとき, f を同等射と呼ぶ。f が同等射であれば, f に対して上の条件をみたす g は一意的に定まる。この g を $g = f^{-1}$ と表わす。同等射 $f : A \to B$ が存在するとき, A と B は同型であるという。

$f : B \to C$ が,

「$g, g' \in mor_{\mathsf{K}}(A,B)$, $f \circ g = f \circ g'$ ならば $g = g'$ である」

という条件をみたすとき, f は単型であるという。

$f : B \to C$ が,

「$h, h' \in mor_{\mathsf{K}}(B,C)$, $h \circ f = h' \circ f$ ならば $g = g'$ である」

という条件をみたすとき, f は全型であるという。

圏 $\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ があるとする。K から集合の圏への写像 u で, 次の条件(i)-(iii)をみたすものがあるとき, 圏 K は実現的(concrete)であるという。

(i) $mor_{\mathsf{K}}(A,B)$ は $u(A)$ から $u(B)$ への写像全体の集合の部分集合である。

(ii) $I_A = I_{u(A)}$

(iii) 合成 $\circ$ は写像の合成である。

$\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ が実現的圏であれば, K における同等射 $f : A \to B$ は $u(A)$ から $u(B)$ への全単射である。

以下においては, $\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ は実現的圏であるとする。

$A, B \in K$, $u(A) \subset u(B)$, $\iota : u(A) \to u(B)$ を標準的単射とするとき, $\iota \in mor_{\mathsf{K}}(A,B)$ ならば, A は B の部分対象であるという。

圏 $\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ が次の(i), (ii)の条件をみたすとき, K は有限決定的であるという。

(i) $A \in K$ に対して自然数値 $d(A)$ を対応させる関数 d が存在し, 次をみたす。

(ia) A が B の部分対象ならば, $d(A) \leq d(B)$。

(ib) AとBが同型ならば, $d(A) = d(B)$。
(ic) AがBの部分対象で, $d(A) = d(B)$ならば, $A = B$。
(ii) $f \in mor_{\mathsf{K}}(A, B)$ で, fが単型かつ全型ならば, fは同等射である。
圏$\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ が,
「$A \in K$, $f \in mor_{\mathsf{K}}(A, A)$が単型であれば$f$は同等射である」
という条件をみたすとき, Kは自己完結的であるという。

定理 7. 有限決定的な圏は自己完結的である。

証明. 圏$\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ は有限決定的であるとする。$A \in K$とし, $f : A \to A$ を単型とする。$f(A) = A'$ はAの部分対象である。先に述べた関数dが存在して, $d(A') \leq d(A)$。$f : A \to A'$ は単型かつ全型であるから, 同等射である。よって, $d(A') = d(A)$。従って, $A = A'$であり, $f : A \to A$は同等射である。

命題 8. Rを左Artin的環とする。次のように定められる圏$\mathsf{K} = (K, mor_{\mathsf{K}}, \circ)$ は有限決定的である。
K の対象は有限生成R-左加群である。$A, B \in K$ に対し, $mor_{\mathsf{K}}(A, B)$ の元fは, AからBへのR-準同形写像である。

証明. §1の定理2により, Kの対象Aに対してはAの組成列が存在する。Aの組成列の長さを$d(A)$とする（§1 定理1参照)。

上の定理7と命題8から次のようにして, 冒頭の事実(F)が導かれる。
複素数を成分とする行列が$AB = E_n$ をみたすとする。Vは複素数体上のn次元線形空間とする。VからVへの線形写像と$M_n(\mathbf{C})$の元とは1対1に対応がつく。行列Aに対応するVの線形写像をL_Aで表わすと, 上の式は$L_A \circ L_B = I$ であることを表わしている（IはVの恒等写像)。これより, L_Bは単射であることがわかる。
$\mathbf{C}$上の有限次元線形空間とそれらの間の線形写像は, 命題8により, 有限決定的な圏である。従って, 定理7によりL_Bは同型写像であり, L_Bの逆写像が存在する。この逆写像に対応する行列はB^{-1}であり,

$$BB^{-1} = B^{-1}B = E_n$$

が成立する。

$$A = AE_n = A(BB^{-1}) = (AB)B^{-1} = E_nB^{-1} = B^{-1}$$

であるから, $BA = E_n$である。

参考文献

[1] F. W. Anderson and K. R. Fuller, Rings and Categories of Modules, Springer-Verlag (1974)
[2] 濱井健人　代数系とある行列等式の導出について　愛知工業大学情報通信工学科平成12年度卒業論文　2001年

[3] 服部昭　現代代数学（近代数学講座１）　朝倉書店　1968年
[4] 永田雅宜　抽象代数への入門　朝倉書店　1967年
[5] 齋藤正彦　線形代数入門（基礎数学１）　東京大学出版会　1966年
[6] 鈴木元, 吉田英弘　逆写像と逆行列に関するある定理について　愛知工業大学情報通信工学科平成13年度卒業論文　2002年

（受理　平成15年３月19日）