線形代数学Ｂ１講義ノート

安藤哲哉

注意: (1) 校正をあまりきちんとしていないので，誤植等に注意して利用して下さい．
(2) 講義中に配布した演習問題と解答は含まれていません．

1. 集合と写像

★ 基本的な記号や用語.
集合の要素のことを**元** (element) ともいい，a が集合 A の元であるとき $a \in A$ とか $A \ni a$ と書き，a が A の元でないとき $a \notin A$ とか $A \not\ni a$ と書く．

等号 $a = b$ は,「a と b は等しい」という意味と,「a を b として定義する」の 2 つの意味で用いられる．後者は「a に b を代入する」というのと実質的には同じである．前者を「条件 (式) の等号」，後者を「代入の等号」という．

$$a := b \quad \text{とか} \quad b =: a$$

という記号は後者の「a を b として定義する」という代入の等号として用いられる．例えば「$a := 1$ とおく」というように使う．ただ，$=$ を前者の「条件の等号」と「代入の等号」の両方に意味で使うことは結構あって，そこは文脈で判断してほしい．

(**差集合**) 集合 A, B はある全体集合の部分集合とする．A に属していて B には属さない元全体の集合を

$$A - B := \{x \in A \mid x \notin B\}$$

と書き，A から B を取り除いた**差集合**という．

(**直積集合**) 集合 A_1, A_2,..., A_n は集合とする．A_1, A_2,..., A_n からそれぞれ 1 つずつ元 $x_1 \in A_1$, $x_2 \in A_2$,..., $x_n \in A_n$ を取り，それを並べた順列 $(x_1, x_2, \ldots, x_n)$ 全体の集合を

$$A_1 \times A_2 \times \cdots \times A_n := \{(x_1, x_2, \ldots, x_n) \mid x_1 \in A_1,\, x_2 \in A_2, \ldots, x_n \in A_n\}$$

を A_1, A_2,..., A_n の**直積集合**という．また，

$$A^n := \underbrace{A \times A \times \cdots \times A}_{n\ \text{個}}$$

と書く．A^n の元は $(x_1, x_2, \ldots, x_n)$ という行ベクトルの形で表わしているが，行列を扱うときは，列ベクトルの形に表すことが多いので注意してほしい．

★ 基本的な論理記号.
A が集合で，A の元 a に関する命題 $P(a)$ があるとする.「A のすべての (任意の) 元 $a \in A$ に対して命題 $P(a)$ が成り立つ」ことを，

「$\forall a \in A\ P(a)$」とか「$P(a)\ (\forall a \in A)$」

と書く．$\forall$ は All の A を上下逆にした文字である．

また,「少なくとも 1 つの元 $a \in A$ に対して命題 $P(a)$ が成り立つ」，言い換えると「$P(a)$ が成り立つような $a \in A$ が (少なくとも 1 つ) 存在する」とき，

「$\exists a \in A\ P(a)$」とか「$P(a)\ (\exists a \in A)$」

と書く．$\exists$ は Exist (Exists) の E を上下逆にした文字である．

「すべての $a \in A$ に対して $P(a)$ が成り立つ」の否定は「$P(a)$ が成り立たないような $a \in A$ が存在する」なので，否定を「Not」で表わせば，

Not「$\forall a \in A\ P(a)$」 $\Longleftrightarrow$ 「$\exists a \in A$ Not $P(a)$」

である．同様に，

Not「$\exists a \in A\ P(a)$」 $\Longleftrightarrow$ 「$\forall a \in A$ Not $P(a)$」

である．このあたりの論理が無意識のうちに展開できないと，数学の理解が無茶苦茶になってしまう．

★ 数の集合等の記号.
1 以上の整数を自然数 (natural number) というが，自然数全体の集合を $\mathbb{N}$ と書く．整数全体の集合は $\mathbb{Z}$ と書くが，これはドイツ語の Zahl の先頭の文字である．整数の分数で表せる数を有理数というが，有理数全体の集合を $\mathbb{Q}$ と書く．イタリア語の Quoziente の先頭の文字で，英語の Quotient に対応し，

整数の商という気持ちを表わしている．実数 (real number) 全体の集合を $\mathbb{R}$ と書き，複素数 (complex number) 全体の集合を $\mathbb{C}$ と書く．この講義では，自然数 n に対し，実数，あるいは，複素数を成分とする n 行の列ベクトル全体の集合を

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \;\middle|\; x_1, x_2, \ldots, x_n \in \mathbb{R} \right\}, \quad \mathbb{C}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \;\middle|\; x_1, x_2, \ldots, x_n \in \mathbb{C} \right\}$$

と書く．列ベクトルに比べて行ベクトルは少ししか用いない．解析のほうでは，n 列からなる行ベクトル全体の集合のほうを $\mathbb{R}^n$ とか $\mathbb{C}^n$ と書くので注意してほしい．後でだんだん分かってくると思うが，行列を扱うときは，行ベクトルより列ベクトルのほうが便利である．

実数のみを成分とするベクトルを**実ベクトル**とか $\mathbb{R}$-ベクトルといい，複素数を成分とするベクトルを**複素ベクトル**とか $\mathbb{C}$-ベクトルという．**有理ベクトル**, **整数ベクトル**という言葉もある．一般に，集合 K があって，K の元のみを成分とするベクトルを K-**ベクトル**という．n 行からなる K-ベクトル (列ベクトル) 全体の集合を K^n と書く．

線形代数 B1 の範囲では，ベクトルや行列の成分を実数で考えても複素数で考えても，あまり違いはないが，線形代数 B2 で内積や固有値を学習する頃になると，実数と複素数でかなり異なってくる．ベクトルには**和**と**スカラー倍**が定義されていて，

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}, \quad a \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{pmatrix}$$

である．ここで，a は数であって，ベクトルに対して普通の数を**スカラー**とも言う．

★ 写像.

関数と似た概念に「写像」というものがある．A, B は集合で，A の元 x に対し B の元 (それを $f(x)$ としよう) を対応させる規則を $f\colon A \to B$ と書き，A から B への**写像**という．$x \in A$ に $y \in B$ が対応するとき

$$y = f(x) \quad \text{とか} \quad f(x) = y$$

と書く．ひとつの $x \in A$ に B の 2 つ以上の元が対応することは許されない．また，対応する B の元がないような $x \in A$ があってはいけない．A を f の**定義域**, B を f の**終域**という．$f\colon A \to B$ を $A \xrightarrow{f} B$ と書くこともある．

関数という用語は若干曖昧に使われるが，写像 f の終域 B が数の集合 ($\mathbb{R}$ や $\mathbb{C}$ の部分集合) である場合に，写像 f を関数と呼ぶ場合が多い．ただし，下記のように「関数」については定義域が A に一致することが必ずしも要求されない場合がある．

例えば $A = B = \mathbb{R}$ の場合を考える．$f(x) = \dfrac{1}{x}$ という規則は $0 \in A$ に対して対応する B の元がないので $f\colon A \to B$ という写像にはならない．もっとも，この場合は $A := \mathbb{R} - \{0\}$ と定義域を制限すれば，$f\colon A \to B$ は写像になる．$f(x) = 1/x$ を関数と考える場合には，定義域を気にしないで「$\mathbb{R}$ 上の関数」と考えてしまうことも多いが，このように必ずしも $f(x)$ が定義されていないが定義域を含み f を考察している集合のことを，f の**始域**という．$f(x) = 1/x$ の場合 $\mathbb{R}$ が始域，$\mathbb{R} = \{0\}$ が定義域である．

今，A, B は一般の集合で，$f\colon A \to B$ は写像とする．また，$C \subset A$, $D \subset B$ は部分集合とする．

$$f(C) := \bigl\{ f(x) \in B \bigm| x \in C \bigr\} \subset B$$
$$f^{-1}(D) := \bigl\{ x \in A \bigm| f(x) \in D \bigr\} \subset A$$

と定義し，$f(C)$ を f による C の**像**といい，$f^{-1}(D)$ を f による D の**逆像**とか**原像**という．$f(C)$ や $f^{-1}(D)$ は集合であって，$f(x)$ のように 1 つの元を表すわけではない．

$f(A)$ を f の**値域**という．終域 B と値域 $f(A)$ は一致するとは限らないことに注意しよう．(このあたりの用語は，高校までは混乱しているので，ここで修正しておいてほしい.)

ここから，重要な概念の定義になるので，強調して見出しをつけておく．

定義 1.1. A, B は一般の集合で，$f\colon A \to B$ は写像とする．

(1) $x, y \in A$, $x \neq y$ ならば $f(x) \neq f(y)$ を満たすとき，f は**単射** (injection) であるという．対偶命題で書けば,「$x, y \in A$, $f(x) = f(y)$ ならば $x = y$ を満たすとき f を単射という」と言ってもよい．
(2) $f(A) = B$ を満たすとき，f は**全射** (surjection) であるという．
(3) $f: A \to B$ が単射かつ全射のとき，f は**全単射** (bijection) であるという．
(4) $f: A \to B$ は全単射であると仮定する．すると，各 $y \in B$ に対して $f(x) = y$ を満たす $x \in A$ が 1 つだけ存在する (数学では「一意的に存在する」という言い方をする)．そこで，$y \in B$ に対して $f(x) = y$ を満たす $x \in A$ を対応させる写像を $f^{-1}(y) = x$, $f^{-1}: B \to A$ と書き，f^{-1} を f の**逆写像**という．

2. 行列の定義と和

集合 K は実数全体の集合 $\mathbb{R}$ か，複素数全体の集合 $\mathbb{C}$ などであるとする．もっと一般に，K 上に和 (足し算) と積 (掛け算) が定義されていて，結合法則，交換法則，分配法則など一定の条件を満たせば何でもかまわないが，このあたりのことは，また後で説明する．

n 個の K の元を表すとき $x_1, x_2, \ldots, x_n$ のように添え字 $1, 2, \ldots, n$ を利用することが多いが，K の元を縦横に並べて表 (ひょう) の様に表すときは，$x_{i,j}$ のように添え字 i と j を 2 つ並べて表すと便利である．誤解の恐れがないときは，$x_{i,j}$ のコンマを省略して x_{ij} と書くことが多い．ただし，ij が (i, j) の意味ではなく，積 (掛け算) ij だと誤解される恐れのある場面では，$x_{i,j}$ とか $x_{(i,j)}$ のように書くべきである．

m, n は自然数 (1 以上の整数) とし，各 $1 \leqq \forall i \leqq m$ と $1 \leqq \forall j \leqq n$ に対して $a_{i,j}$ は K の元であるとし，それを以下のように縦 m 行，横 n 列に並べて，それを括弧でくくって A を作る．

$$A := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \tag{①}$$

点点点の部分や中央の空白部分は適当に推測せよ，という不親切な書き方であるが，直感的にはこう書いたほうが目に印象強く飛び込んでくる．このような A を (K 上の) m 行 n 列の**行列**とか，(m, n)-型行列という．(m, n) を行列 A の**サイズ**とか**型**という．$K = \mathbb{R}$ のとき A を**実行列**, $K = \mathbb{C}$ のとき A を**複素行列**という．A の第 i 行第 j 列の成分 $a_{i,j}$ を A の (i, j)-**成分**という.「行」と「列」は上のように厳密に使い分けるので注意してほしい．横方向に伸びるのが**行**で，縦方向に伸びるのが**列**であって，日常用語のように曖昧に使ってはならない．

K の元を成分とする m 行 n 列の行列全体の集合を

$$M_{mn}(K)$$

と書く．行列 A を書くとき，毎回 ① のように書くのは大変面倒で，紙面を浪費するので，誤解の恐れがなければシンプルに

$$A = (a_{ij}) \quad \text{とか} \quad A := (a_{i,j}) \in M_{mn}(K)$$

などと略記する．

1 行 n 列の行列が (n 列の) **行ベクトル**で，m 行 1 列の行列が (m 行の) **列ベクトル**である．このように，行ベクトルや列ベクトルも行列の一種と考える．ただ，スカラー a と，(a) という 1 行 1 列の行列は区別して考える場合が多い．

$m = n$ の場合には A を n 次の**正方行列**という．K の元を成分とする n 次正方行列全体の集合を

$$M_n(K) := M_{nn}(K)$$

と書く．

定義 2.1.(行列の和とスカラー倍) K は同上とし，$c \in K$ で，$A = (a_{ij})$ と $B = (b_{ij})$ は同じサイズの m 行 n 列の行列で，各成分は K の元とする．そのとき，

$$A + B = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

$$
:= \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}
$$

$$
cA := c\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = \begin{pmatrix} ca_{11} & ca_{12} & \cdots & ca_{1n} \\ ca_{21} & ca_{22} & \cdots & ca_{2n} \\ \vdots & \vdots & & \vdots \\ ca_{m1} & ca_{m2} & \cdots & ca_{mn} \end{pmatrix}
$$

として，行列の**和** (加法, 足し算) $A+B$ と，A の c による**スカラー倍** cA を定義する．$(-1)A$ を $-A$ とも書く．

また，すべての成分が 0 である行列を**ゼロ行列**といい O 等で表す．m 行 n 列のゼロ行列の場合は O_{mn} などと書いてサイズを明記する．

命題 2.2. $A, B, C \in M_{mn}(K)$; $\alpha, \beta \in K$ とするとき，以下が成り立つ．
(1) (結合法則) $(A+B)+C = A+(B+C)$
(2) $A+O_{mn} = A$, $O_{mn}+A = A$
(3) $A+(-A) = O_{mn}$, $(-A)+A = O_{mn}$
(4) (交換法則) $A+B = B+A$
(5) (スカラー倍の結合法則) $(\alpha\beta)A = \alpha(\beta A)$
(6) (スカラー倍の分配法則) $(\alpha+\beta)A = \alpha A+\beta A$, $\alpha(A+B) = \alpha A+\alpha B$
(7) $1 \in K$ に対して $1A = A$ (ただし，この場合 $1A$ を $1 \cdot A$ と書くことが多い.)

証明は自明なので省略する．結合法則 $(A+B)+C = A+(B+C)$ のおかげで，これを $A+B+C$ と書いてよいし，$(\alpha\beta)A = \alpha(\beta A)$ なので $\alpha\beta A$ と書いても矛盾しない．4 個以上の行列の和についても同様である．$A_1, A_2, \ldots, A_r \in M_{mn}(K)$ のとき，

$$
\sum_{k=1}^{r} A_k := A_1 + A_2 + \cdots + A_r
$$

として総和記号を定める．

今後，上の命題のような演算規則に関する法則がよく登場するので,「群」(ぐん, group) という用語を導入しておく．演算は $+$ 以外に $\times$ とか，それ以外の演算の場合も考えるので，仮想的に $*$ という記号で表わされる演算があるとして定義を述べる．$a+b$ とか $a \times b$ のように，K の 2 つの元 a, b に対し，$a+b$ や $a \times b$ のような K の元が 1 つ対応するとき，$+$ や $\times$ のようなものを (**二項**) **演算**という．上で登場したスカラー倍は二項演算ではなく「作用」と呼ばれる別種の演算である．

定義 2.3. (I) 集合 G 上に (二項) 演算 $*$ が定められていて，また，$e \in G$ であるとする．さらに，以下の法則が成立していると仮定する．
(0) (G は $*$ について閉じている) $x, y \in G$ ならば $x * y \in G$.
(1) (結合法則) $x, y, z \in G$ ならば $(x*y)*z = x*(y*z)$
(2) (e は単位元) $x \in G$ ならば $e*x = x$, $x*e = x$.
(3) (逆元の存在) $x \in G$ ならば，ある $y \in G$ が存在して，$x*y = e$, $y*x = e$.
このときとき，G は演算 $*$ について e を単位元とする**群** (group) であるという．(3) において，y を $*$ に関する x の**逆元**という．G が $*$ について群であって，
(4) (交換法則) $x, y \in G$ ならば $x*y = y*x$.
が成り立つとき，G は **Abel** 群であるという．

この言葉を使うと「$M_{mn}(K)$ は行列の和 $+$ について，O_{mn} を単位元とするアーベル群になっていて，$A \in M_{mn}(K)$ の $+$ に関する逆元は $-A$ である」と記述することができる．

なお，命題 2.2 の (5), (6), (7) の規則 (法則) が成り立つとき,「K が $M_{mn}(K)$ にスカラー倍によって**作用している**」と言い表す．

定義 2.4. (II) 集合 K に和 $+$ と積 (掛け算) $\times$ ($x \times y$ は $x \cdot y$ とか xy とも書く) が与えられていて，
(1) K は加法 $+$ について 0 を単位元とする Abel 群である．

(2) $K^\times := \{x \in K \mid x \neq 0\}$ とおくとき，$K^\times$ は積について 1 を単位元とする Abel 群である．また，$0 \neq 1$ である．

(3) (分配法則) $x, y, z \in K$ ならば $(x+y)z = xz + yz$.

を満たすとき，K は**体** (たい，field) であるという．

例えば，実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$, 有理数全体の集合 $\mathbb{Q}$ はいずれも体である．体の意味がよくわからない人は，この授業では，$\mathbb{R}$ と $\mathbb{C}$ が体であると思って聞いてもらっても構わない.「体」という用語を導入しておくと，いろいろ記述が簡単になる．

★ 記号の約束.

本講義では，列ベクトルを表すとき $\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ のように，$\mathbf{b}$, $\mathbf{x}$ のようなボールド体を用いることが多い．K^n の中で，1 つの成分だけが 1 で，他の成分が 0 であるベクトルを，

$$\mathbf{e}_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ \mathbf{e}_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots,\ \mathbf{e}_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

と書き，$\mathbf{e}_1, \dots, \mathbf{e}_n$ を**基本ベクトル**と呼ぶ．第 i 番目の $\mathbf{e}_i$ を**第 i 基本ベクトル**とか，**第 i 単位ベクトル**というが，こちらの用語は滅多に使わない．上の $\mathbf{a}$ は，

$$\mathbf{a} = \sum_{i=1}^{n} a_i \mathbf{e}_i = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \cdots + a_n\mathbf{e}_n$$

と表すことができることに注意する．

3. 行列の積

K は体 ($\mathbb{R}$ や $\mathbb{C}$) であるとする．

定義 3.1.(行列の積) $l, m, n \in \mathbb{N}$ (自然数) とし，$A \in M_{lm}(K)$, $B \in M_{mn}$ とする．A の列の個数と B の行の個数が一致していないといけないことを強調しておく．A, B の (i, j)-成分を $a_{ij} = a_{i,j}$, $b_{ij} = b_{i,j}$ とする．このとき，

$$a_{i,1}b_{1,j} + a_{i,2}b_{2,j} + a_{i,3}b_{3,j} + \cdots + a_{i,m}b_{m,j}$$

を (i, j)-成分とする l 行 n 列の行列を

$$AB := \begin{pmatrix} \sum_{k=1}^{m} a_{1,k}b_{k,1} & \sum_{k=1}^{m} a_{1,k}b_{k,2} & \cdots & \sum_{k=1}^{n} a_{1,k}b_{k,n} \\ \sum_{k=1}^{m} a_{2,k}b_{k,1} & \sum_{k=1}^{m} a_{2,k}b_{k,2} & \cdots & \sum_{k=1}^{n} a_{2,k}b_{k,n} \\ \vdots & \vdots & & \vdots \\ \sum_{k=1}^{m} a_{l,k}b_{k,1} & \sum_{k=1}^{m} a_{l,k}b_{k,2} & \cdots & \sum_{k=1}^{n} a_{l,k}b_{k,n} \end{pmatrix}$$

と定義し，A と B の**積**という．

なお，行列とベクトルの積や，ベクトルとベクトルの積も，ベクトルを行列の一種と考えて，上の定義によって定義する．(サイズが上の条件を満たす時のみ積が定義できる.)

また，A が正方行列の場合には，自然数 r に対し

$$A^r := \underbrace{AA\cdots A}_{r\text{ 個}}$$

として A の r 乗を定める．

上の定義で，$l \neq n$ のときは，積 BA は**定義できない**．また，仮に $l = m$ であっても，後で例示するように交換法則 $BA = AB$ は**一般には成立しない**．

定理 3.2. K は体とし，l, m, n, p は自然数とする．このとき，以下が成り立つ．
(1) $A \in M_{lm}(K)$, $B \in M_{mn}(K)$, $C \in M_{np}(K)$ のとき，

$$(AB)C = A(BC)$$

(2) $A \in M_{lm}(K)$; $B, C \in M_{mn}(K)$ のとき，

$$A(B+C) = AB + AC$$

(3) $A, B \in M_{lm}(K)$, $C \in M_{mn}(K)$ のとき，

$$(A+B)C = AC + BC$$

(4) $A \in M_{lm}(K)$, $B \in M_{mn}(K)$, $\alpha \in K$ のとき，

$$(\alpha A)B = A(\alpha B) = \alpha(AB)$$

証明. (1) $A = (a_{i,j})$, $B = (b_{i,j})$, $C = (c_{i,j})$ とする．$1 \leqq i \leqq l$, $1 \leqq t \leqq n$ とし，AB の (i, t)-成分を $d_{i,t}$ とすると，$d_{i,t} = \displaystyle\sum_{s=1}^{m} a_{i,s} b_{s,t}$ である．よって，$(AB)C$ の (i, j)-成分 $(1 \leqq j \leqq p)$ は，

$$\sum_{t=1}^{n} d_{i,t} c_{t,j} = \sum_{t=1}^{n} \left(\sum_{s=1}^{m} a_{i,s} b_{s,t} \right) c_{t,j} = \sum_{s=1}^{m} \sum_{t=1}^{n} a_{i,s} b_{s,t} c_{t,j} \qquad ①$$

である．同様に，BC の (s, j)-成分を $e_{s,j}$ $(1 \leqq s \leqq m)$ とすると，$e_{s,j} = \displaystyle\sum_{t=1}^{n} b_{s,t} c_{t,j}$ である．よって，$A(BC)$ の (i, j)-成分は，

$$\sum_{s=1}^{m} a_{i,s} e_{s,j} = \sum_{s=1}^{m} a_{i,s} \sum_{t=1}^{n} b_{s,t} c_{t,j} = \sum_{s=1}^{m} \sum_{t=1}^{n} a_{i,s} b_{s,t} c_{t,j}$$

となり，①と一致する．よって，$(AB)C = A(BC)$ が成り立つ．

(2) 両辺の (i, j)-成分は

$$\sum_{k=1}^{m} a_{i,k}(b_{k,j} + c_{k,j}) = \sum_{k=1}^{m} a_{i,k} b_{k,j} + \sum_{k=1}^{m} a_{i,k} + c_{k,j}$$

なので，$A(B+C) = AB + AC$ である．

(3) は (2) と同様に証明できる．(4) はもっと簡単．　□

例 3.3. $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ とし，$O = O_{22}$ は 2 行 2 列のゼロ行列とする．

$$AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad BA = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

なので，$AB \neq BA$ である．また，

$$A^2 = AA = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O$$

となる．これは，**ゼロ行列でない 2 つの行列の積がゼロ行列になることがある**ことを意味している．ついでに，$B^2 = O$ である．

そのため，$AB = AC$, $A \neq O$ であっても $B \neq C$ となることもある．例えば，上の例で，$A^2 = O = AO$ であるが，$A \neq O$ である．

命題 3.4. $A=(a_{ij})\in M_{lm}(K)$, $B=(b_{ij})\in M_{mn}(K)$ とし，A, B の第 j 列目の列ベクトルを $\mathbf{a}_j=\begin{pmatrix}a_{1,j}\\a_{2,j}\\\vdots\\a_{l,j}\end{pmatrix}\in K^l$ $(1\leqq j\leqq m)$, $\mathbf{b}_j=\begin{pmatrix}b_{1,j}\\b_{2,j}\\\vdots\\b_{m,j}\end{pmatrix}\in K^m$ $(1\leqq j\leqq n)$ とする．また，$\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_m\in K^m$ を m 行からなる基本ベクトルとする．行列 A は列ベクトル $\mathbf{a}_1,\ldots,\mathbf{a}_m$ を並べたものだと考えることができ，その意味で，

$$A=(\mathbf{a}_1,\,\mathbf{a}_2,\ldots,\,\mathbf{a}_m)$$

とも書く．この時，以下が成り立つ．
(1) $A\mathbf{e}_j=\mathbf{a}_j$ $(1\leqq\forall j\leqq m)$ である．
(2) AB の第 j 列は $A\mathbf{b}_j$ $(1\leqq\forall j\leqq n)$ であり，

$$AB=(A\mathbf{b}_1,\,A\mathbf{b}_2,\ldots,\,A\mathbf{b}_n)$$

と書ける．

上の命題は定義に従って計算してみれば自明な事実を書いただけで，特に証明を要するところはない．ただ，上の事実はよく使う．

定義 3.5.(合成写像) X, Y, Z は集合で，$f\colon X\to Y$ と $g\colon Y\to Z$ は写像とする．今 $x\in X$ に対し $g(f(x))\in Z$ を対応させる写像を $g\circ f\colon X\longrightarrow Z$ と書き，$g\circ f$ を f と g の**合成写像**という．
写像としては，$x\in X$ に先に f を作用させて $y=f(x)$ を作ってから，次に g を作用させて $g(y)=g(f(x))=(g\circ f)(x)$ を作るので「f と g の合成写像」と言うのであるが，記号で $g\circ f$ と書くときは，g が先で f が後になるので注意してほしい．合成関数の場合と同様である．

定理 3.6.(行列が定める写像) $A\in M_{lm}(K)$ で $\mathbf{x}\in K^m$ は列ベクトルとする．このとき，積 $A\mathbf{x}$ が定まり $A\mathbf{x}\in K^l$ で l 行の列ベクトルになる．今，$f_A(\mathbf{x})=A\mathbf{x}$ により写像 $f_A\colon K^m\to K^l$ を定める．この f_A を行列 A が定める (線形) 写像という．同様にして $B\in M_{mn}(K)$ に対し $f_B(\mathbf{y})=B\mathbf{y}$ $(\mathbf{y}\in K^n)$ で写像 $f_B\colon K^n\to K_m$ を定める．また，積 AB から同様にして写像 $f_{(AB)}\colon K^n\to K^l$ を定める．このとき，

$$f_{(AB)}=f_A\circ f_B$$

が成り立つ．つまり，AB が定める写像は，f_B が定める写像と f_A が定める写像の合成写像である．

上の定理は結合法則 $(AB)\mathbf{y}=A(B\mathbf{y})$ を言い換えただけで，自明なことを述べたにすぎない．しかし，**行列の積は写像の合成に対応している**という事実は大切なことである．

4. 逆行列

定義 4.1.(トレース) 一般に，n 次正方行列 $A=(a_{i,j})$ に対し，$i=j$ を満たす成分 $a_{1,1}$, $a_{2,2}$, $a_{3,3},\ldots$, $a_{n,n}$ の**対角 (線) 成分**という．また，A の対角成分の和を

$$\operatorname{tr}A:=a_{1,1}+a_{2,2}+a_{3,3}+\cdots+a_{n,n}$$

という記号で表し，$\operatorname{tr}A$ を A の**トレース**という．

定義 4.2.(単位行列)
整数 i, j に対し，$i=j$ ならば $\delta_{i,j}:=1$, $i\neq j$ ならば $\delta_{i,j}:=0$ として $\delta_{i,j}$ を定める．$\delta_{i,j}$ を**クロネッカーのデルタ**という．今，n を自然数とし，n 次正方行列 $A=(a_{i,j})$ が $a_{i,j}=\delta_{i,j}$ $(1\leqq\forall i\leqq n,\ 1\leqq\forall j\leqq n)$ を満たすとき，A を (n 次の) **単位行列**といい，A を I_n とか I とか E とか E_n という記号で表す．この講義では I_n と I を用いる．単位行列は，対角成分がすべて 1 で，それ以外の成分がすべて 0 であるような正方行列，と言ってもよい．

命題 4.3. K は体，I_n は n 次の単位行列，$A\in M_{mn}(K)$, $B\in M_{nl}(K)$ とする．すると，

$$AI_n=A,\quad I_nB=B$$

が成り立つ．また，ベクトル $\mathbf{x}\in K^n$ に対して $I_n\mathbf{x}=\mathbf{x}$ である．

証明. 行列の積の定義に戻って計算してみれば，すぐわかる． □

定義 4.4. X は空でない集合とする．写像 $f\colon X \to X$ が任意の $x \in X$ に対して $f(x) = x$ を満たすとき，f は**恒等写像**であるといい，f を id_X とか id などと書く．K が体のとき，単位行列 I_n が定める写像 $f_{I_n}\colon K^n \to K^n$ は恒等写像 id である．

命題 4.5. A, B, C, D は集合で，$f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$ は写像とする．このとき結合法則

$$(h \circ g) \circ f = h \circ (g \circ f)$$

が成り立つ．

証明. $x \in A$ に対し，

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h\bigl(g(f(x))\bigr) = h\bigl((g \circ f)(x)\bigr) = (h \circ (g \circ f)(x)$$

なので，$(h \circ g) \circ f = h \circ (g \circ f)$ である． □

命題 4.6. X は空でない集合とし，$f\colon X \to X$, $g\colon X \to X$, $h\colon X \to X$ は写像とする．今，

$$f \circ g = \mathrm{id}_X, \quad h \circ f = \mathrm{id}_X$$

が成り立つと仮定する．すると，f は全単射で，

$$g = h = f^{-1}$$

が成り立つ．

証明. 一般に，任意の写像 $\varphi\colon X \to X$ に対して，$\mathrm{id}_X \circ \varphi = \varphi$, $\varphi \circ \mathrm{id}_X = \varphi$ である．前命題より，

$$g = \mathrm{id}_X \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ \mathrm{id}_X = h$$

である．$f(x) = y$ $(x \in X)$ のとき，$g(y) = g(f(x)) = (g \circ f)(x) = \mathrm{id}_X(x) = x$ なので，$g = f^{-1}$ である． □

正確に言うと，$f \circ g = \mathrm{id}_X$ となる g が存在すると f が全射であることがわかり，$h \circ f = \mathrm{id}_X$ となる h が存在すると f が単射であることがわかる．$f \circ g = \mathrm{id}_X$ だけだと f の単射性が保障されないので，$g = f^{-1}$ とは言えない．

定義 4.7. K は体 ($\mathbb{R}$ や $\mathbb{C}$) であるとし，n 次正方行列 $A, B \in M_n(K)$ は，

$$AB = I_n, \quad BA = I_n$$

を満たすとする．このとき B を A^{-1} と書き，A の**逆行列**という．A が逆行列を持つための必要十分条件は A が定める写像 $f_A\colon K^n \longrightarrow K^n$ が全単射であることであり，このとき A^{-1} は f_A の逆写像 f_A^{-1} を定める行列である．特に，行列 A の逆行列 A^{-1} が存在すれば，A^{-1} は A に対して 1 つしか存在しない (「一意的である」という言い方をする)．

正方行列 A が逆行列 A^{-1} を持つとき，A は**可逆行列**であるとか**正則行列**である．A が可逆行列の場合には，自然数 r に対し，

$$A^0 = I_n, \quad A^{-r} := (A^{-1})^r = (A^r)^{-1}$$

と，0 や負の整数に対する A の累乗も定める．

なお，n 次正方行列 A に対しては，n 次正方行列 B が $BA = I_n$ または $AB = I_n$ の一方を満たせば，$B = A^{-1}$ となり，他方も満たすのであるが，それは後の定理 8.6 で行列式を用いて証明される．また，具体的な A^{-1} の計算方法は，掃き出し法を使う方法や，行列式を使う方法などがあるが，いずれも後の回の講義で解説する．

定理 4.8. A と B は n 次正方行列で，いずれも逆行列を持つとする．すると，AB や A^{-1} も逆行列を持ち，

$$(AB)^{-1} = (B^{-1})(A^{-1}), \quad (A^{-1})^{-1} = A$$

が成り立つ．

証明. $(AB)((B^{-1})(A^{-1})) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$, $((B^{-1})(A^{-1}))(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$ なので，$(AB)^{-1} = (B^{-1})(A^{-1})$ である．$AA^{-1} = I_n$, $A^{-1}A = I_n$ なので，$(A^{-1})^{-1} = A$ である． □

定理&定義 4.9. $A = (a_{i,j}) \in M_{mn}(K)$ (m 行 n 列行列) とする．$b_{i,j} := a_{j,i}$ (i と j の順番に注意せよ．$1 \leqq i \leqq n$, $1 \leqq j \leqq m$) として n 行 m 列の行列 $B = (b_{i,j}) \in M_{nm}(K)$ を作る．この B を ${}^tA$ という記号で表し，A の**転置行列**という．転置行列 ${}^tA$ を「A の行と列を入れ替えてできる行列」というような言い方をすることも多い．A の j 列目の列ベクトルは ${}^tA$ の j 行目の行ベクトルになる．

例えば，

$${}^t\begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix} = \begin{pmatrix} a & x \\ b & y \\ c & z \end{pmatrix}$$

である．

定理 4.10. K は体とする．

(1) $A \in M_{lm}(K)$, $B \in M_{mn}(K)$ のとき，

$${}^t(AB) = ({}^tB)({}^tA)$$

(2) A が正方行列で逆行列 A^{-1} を持つ場合は，${}^tA$ も逆行列を持ち，

$$({}^tA)^{-1} = {}^t(A^{-1})$$

が成り立つ．

証明. (1) $A = (a_{i,j})$, $B = (b_{i,j})$ とおく．AB の (j, i)-成分は $\displaystyle\sum_{k=1}^{m} a_{j,k}b_{k,i}$ で，これが ${}^t(AB)$ の (i, j)-成分である．

他方，${}^tB$, ${}^tA$ の (i, j)-成分は $b_{j,i}$, $a_{j,i}$ なので，$({}^tB)({}^tA)$ の (i, j)-成分は，$\displaystyle\sum_{k=1}^{m} b_{k,i}a_{j,k}$ で，これは ${}^t(AB)$ の (i, j)-成分と一致する．よって，${}^t(AB) = ({}^tB)({}^tA)$ である．

(2) $I_n = AA^{-1}$ より，$I_n = {}^tI_n = {}^t(AA^{-1}) = \bigl({}^t(A^{-1})\bigr)({}^tA)$, $I_n = {}^tI_n = {}^t(A^{-1}A) = ({}^tA)\bigl({}^t(A^{-1})\bigr)$ なので，$({}^tA)^{-1} = {}^t(A^{-1})$ である． □

5. 置換

定義 5.1. n を自然数とし，一時的に $X_n = \{1, 2, \ldots, n\}$ (n 以下の自然数全体の集合) とおく．全単射 $f\colon X_n \to X_n$ を n 次の**置換**とか，$1, \ldots, n$ の置換という．後者の言い方をする場合，$1, \ldots, n$ の部分は別の n 個のものに変わる場合も多い．置換はギリシャ文字の小文字 σ (シグマ．大文字は Σ), τ (タウ), ρ (ロー) などを用いて表すことが多い．n 次の置換は全部で $n!$ 個ある．n 次の置換はすべての集合を

$$\mathfrak{S}_n = \bigl\{\sigma\colon X_n \to X_n \bigm| \sigma \text{ は全単射}\bigr\}$$

と書く．$\mathfrak{S}$ はドイツ亀の甲文字の S の大文字であるが，書きにくいので手で書くときは S_n と書いておくとよい．$\mathfrak{S}_n$ の代わりに S_n と書いてある文献も多いが，S_n をいう記号はいろいろな意味で用いるので，$\mathfrak{S}_n$ と書いておくと誤認が少ない．

$\sigma, \tau \in \mathfrak{S}_n$ とする．σ と τ は X_n から X_n への写像なので，その合成写像 $\sigma \circ \tau\colon X_n \to X_n$ (つまり $k \in X_n$ に対して $(\sigma \circ \tau)(k) = \sigma(\tau(k))$) を考えると，$\sigma \circ \tau$ も全単射で，$\sigma \circ \tau \in \mathfrak{S}_n$ となる．合成写像の記号 $\circ$ を書くのを省略して，単に $\sigma\tau$ と書くことが多い．$\sigma\tau$ を置換の**積**という．なお，$k \in \mathbb{N}$ に対し，

$$\sigma^k = \underbrace{\sigma\sigma\cdots\sigma}_{k\text{ 個}}$$

と書く．

また，$\sigma\colon X_n \to X_n$ は全単射なので，逆写像 $\sigma^{-1}\colon X_n \to X_n$ が存在し，σ^{-1} も全単射である．よって，$\sigma^{-1} \in \mathfrak{S}_n$ である．σ^{-1} を σ の**逆置換**ともいう．

X_n から X_n への恒等写像を $\mathrm{id}, \mathrm{id}_n, \mathrm{id}_{X_n}, \iota_n$ などと書き，(n 次の) **恒等置換**という．つまり，任意の $k \in X_n$ に対し $\mathrm{id}_n(k) = k$ である．

$\sigma\sigma^{-1} = \mathrm{id}_n$, $\sigma^{-1}\sigma = \mathrm{id}_n$ であることに注意する．また，$\sigma^0 = \mathrm{id}_n$ と約束し，$n \in \mathbb{N}$ に対し，

$$\sigma^{-n} = (\sigma^{-1})^n$$

と定める．容易にわかるように，$\sigma^{-n} = (\sigma^{-1})^n = (\sigma^n)^{-1}$ が成立する．

命題 5.2. n 次の置換全体の集合 $\mathfrak{S}_n$ は積 (写像の合成) を演算として群になる．単位元は恒等置換 id_n で，$\sigma \in \mathfrak{S}_n$ の逆元は逆置換 σ^{-1} である．この意味で，$\mathfrak{S}_n$ を n **次対称群**という．なお，$n \geqq 2$ のとき，$\mathfrak{S}_n$ では交換法則 $\sigma\tau = \tau\sigma$ は一般には成立せず，$\mathfrak{S}_n$ はアーベル群ではない．

証明. 群の定義の中の結合法則だけ示してなかったが，そでは写像の合成が結合法則を満たすことからわかる． □

$n \geqq 2$ のとき，X_n の中から相異なる 2 つの元 i, j を選び，i と j だけを交換する置換 $f \colon X_n \to X_n$ を考える．つまり，$k \in X_n$ に対して，

$$f(k) = \begin{cases} k & (k \neq i, j \text{ のとき}) \\ j & (k = i \text{ のとき}) \\ i & (k = i \text{ のとき}) \end{cases}$$

と定める．この f を i と j の**互換**といい，$f = (i, j)$ と書く．(i, j) という記号はいろいろな意味で用いるので，少し判別しにくい記号である．i と j を互換して，もう一度 i と j を互換すると最初の状態に戻るので，$(i, j) \circ (i, j) = \mathrm{id}_n$ である．$(i, j)^{-1} = (i, j)$ とも言い替えられる．

定理 5.3. $n \geqq 2$ のとき，任意の置換 $\sigma \in \mathfrak{S}_n$ は何個かの互換の積として表すことができる．つまり，ある自然数 $r \in \mathbb{N}$ と，互換 $\tau_k = (i_k, j_k)$ $(i_k, j_k \in X_n; k = 1, 2,\ldots, r)$ が存在して，$\sigma = \tau_1\tau_2\cdots\tau_n$ となる．

証明. n に関する帰納法で証明する．$n = 2$ のときは，$\mathfrak{S}_2 = \{\mathrm{id}_2, (1, 2)\}$ であって，$\mathrm{id}_2 = (1, 2)^2 = (1, 2) \circ (1, 2)$ なので，定理は成立する．

今 $n \geqq 3$ とし $\mathfrak{S}_{n-1}$ の元は互換の積で書けると仮定する．$f \in \mathfrak{S}_{n-1}$ は $f(n) = n$ と約束することによって $f \in \mathfrak{S}_n$ と考えることができる．この約束で $\mathfrak{S}_{n-1} \subset \mathfrak{S}_n$ と考える．$\mathfrak{S}_{n-1}$ 内の互換 (i, j) も，i と j を互換する $\mathfrak{S}_n$ 内の互換と考えることができる．

さて，勝手な $\sigma \in \mathfrak{S}_n$ を取る．もし $\sigma(n) = n$ ならば，σ は $1,\ldots, n-1$ の置換になっているので $\sigma \in \mathfrak{S}_{n-1}$ と考えることができる．帰納法の仮定から σ は何個かの互換の積で表せる．

以下，$\sigma(n) \neq n$ の場合を考える．$m := \sigma(n) < n$ とし，$\tau = (m, n)$ (m と n の互換) とする．$\tau\sigma(n) = \tau(\sigma(n)) = \tau(m) = n$ なので，$\tau\sigma(n)$ は $1,\ldots, n-1$ の置換になっている．帰納法の仮定から何個かの互換 $\tau_1,\ldots, \tau_r$ により，$\tau\sigma = \tau_1\tau_2\cdots\tau_r$ と書ける．$\tau^2 = \mathrm{id}_n$ に注意して，上の等式の左から τ を掛けると，

$$\sigma = \mathrm{id}_n\sigma = \tau^2\sigma = \tau\tau\sigma = \tau\tau_1\tau_2\cdots\tau_r$$

となる．上式の右辺は互換の積である． □

なお，上の証明を注意して分析すると，n 次の置換 $\sigma \in \mathfrak{S}_n$ は，$(n-1)$ 個以下の互換の積として表せることがわかる．

定義 5.4. n は 2 以上の整数とし，$x_1,\ldots, x_n$ を変数とする次のような多項式 $\Delta_n(x_1,\ldots, x_n)$ を考える．$1 \leqq i < j \leqq n$ を満たす整数の組 (i, j) (これは互換ではない) は全部で $\dfrac{n(n-1)}{2}$ 個存在するが，そのすべての (i, j) に対して $(x_i - x_j)$ を掛けて得られる多項式を

$$\Delta_n(x_1, \ldots, x_n) = \prod_{1 \leqq i < j \leqq n} (x_i - x_j)$$

と書く．ここで，$\displaystyle\prod_{1\leqq i<j\leqq n}$ は $1\leqq i<j\leqq n$ を満たすすべての $(i,\,j)$ について，その後に書かれている式の積を取ることを表す記号で，**相乗記号**と呼ばれる．誤解の恐れがなければ単に $\displaystyle\prod_{i<j}$ とも書く．この $\Delta_n(x_1,\ldots,x_n)$ を，$x_1,\ldots,x_n$ の**差積**とか**基本交代式**という．

$\sigma\in\mathfrak{S}_n$ のとき，

$$\sigma(\Delta_n(x_1,\ldots,x_n))=\prod_{1\leqq i<j\leqq n}\left(x_{\sigma(i)}-x_{\sigma(j)}\right)$$

と約束する．

定理 5.5. 記号は上の通りとする．

(1) $\sigma(\Delta_n(x_1,\ldots,x_n))=\pm\Delta_n(x_1,\ldots,x_n)$ である．ここで，$\pm$ は $+$ か $-$ か，いずれか一方について等式が成立することを意味する．

(2) $\tau\in\mathfrak{S}_n$ が互換ならば，$\tau(\Delta_n(x_1,\ldots,x_n))=-\Delta_n(x_1,\ldots,x_n)$ である．

証明. (1) プラスマイナスの符号を気にしないで (x_j-x_i) も (x_i-x_j) も同じ因子と考えれば，因子 $\left(x_{\sigma(i)}-x_{\sigma(j)}\right)$ $(1\leqq i<j\leqq n)$ 全体は，因子 (x_i-x_j) 全体と一致する．よって (1) が成立する．

(2) 上の考察において，$\left(x_{\sigma(i)}-x_{\sigma(j)}\right)$ と (x_i-x_j) で符号が反転するものが何個あるか考える．符号が反転する $(i,\,j)$ 全体の集合を M とし，符号が変わらない $(i,\,j)$ 全体の集合を P とする．M の元の個数が奇数であることを確認すればよい．$\tau=(k,\,l)$ $(1\leqq k<l\leqq n)$ としておく．

$\{i,\,j\}\cap\{k,\,l\}=\emptyset$ ならば，$\tau(x_i-x_j)=(x_i-x_j)$ なので $(i,\,j)\in P$ である．

$\{i,\,j\}\cap\{k,\,l\}\neq\emptyset$ の場合を考える．$i<j,\,k<l$ なので，$i,\,j,\,k,\,l$ の大小関係は，以下の 7 通りがあり得る．(i) $i=k<j<l$, (ii) $i=k<j=l$, (iii) $i=k<l<j$, (iv) $i<k=j<l$, (v) $i<k<j=l$, (vi) $k<i<j=l$, (vii) $k<i=l<j$.

$(i,\,j)$ が (i) 〜 (vii) のどの場合も，$\tau(x_i-x_j)=(x_j-x_i)=-(x_i-x_j)$ となるので，$(i,\,j)\in M$ である．M の元は (i) 〜 (vii) 以外にない．(i) の $(i,\,j)$ は $(l-k-1)$ 個である．(ii) の $(i,\,j)$ は $(i,\,j)=(k,\,l)$ の 1 個である．以下同様，(iii) の $(i,\,j)$ は $(n-l-1)$ 個，(iv) の $(i,\,j)$ は $(k-1)$ 個，(v) の $(i,\,j)$ も $(k-1)$ 個，(vi) の $(i,\,j)$ は $(l-k-1)$ 個，(vii) の $(i,\,j)$ は $(n-l-1)$ 個である．全部あわせると M の元は，$2(l-k-1)+2(n-l-1)+2(k-1)+1$ 個で，奇数個である．よって，(2) がわかる． □

定義 5.6. $\sigma\in X_n$ に対し，
$\sigma(\Delta_n(x_1,\ldots,x_n))=\Delta_n(x_1,\ldots,x_n)$ であるとき $\mathrm{sign}(\sigma)=1$,
$\sigma(\Delta_n(x_1,\ldots,x_n))=-\Delta_n(x_1,\ldots,x_n)$ であるとき $\mathrm{sign}(\sigma)=-1$
と定める．言い換えると，

$$\sigma(\Delta_n(x_1,\ldots,x_n))=\mathrm{sign}(\sigma)\Delta_n(x_1,\ldots,x_n)$$

である．$\mathrm{sign}(\sigma)$ を σ の**符号**という．$\mathrm{sign}(\sigma)$ を $\varepsilon(\sigma)$ などとも書く．$\mathrm{sign}(\sigma)=1$ のとき σ を**偶置換**といい，$\mathrm{sign}(\sigma)=-1$ のとき σ を**奇置換**という．

前定理より，互換は奇置換である．

なお，写像 $\sigma\colon X_n\to X_n$ が全単射でないとき (つまり $\sigma\notin\mathfrak{S}_n$ のとき)，$\mathrm{sign}(\sigma)=0$ と約束しておくと，後で行列式の計算で利用するとき便利になる．

定理 5.7. $\sigma,\,\tau\in\mathfrak{S}_n$ とする．すると，$\mathrm{sign}(\sigma\tau)=\mathrm{sign}(\sigma)\,\mathrm{sign}(\tau)$ が成り立つ．

証明.

$$\begin{aligned}(\sigma\tau)(\Delta_n(x_1,\ldots,x_n))&=\prod_{1\leqq i<j\leqq n}\left(x_{\sigma\tau(i)}-x_{\sigma\tau(j)}\right)\\&=\sigma\left(\prod_{1\leqq i<j\leqq n}\left(x_{\tau(i)}-x_{\tau(j)}\right)\right)\\&=\sigma\bigl(\tau(\Delta_n(x_1,\ldots,x_n))\bigr)\\&=\sigma(\mathrm{sign}(\tau)\Delta_n(x_1,\ldots,x_n))\end{aligned}$$

$$
\begin{aligned}
&= \operatorname{sign}(\tau)\sigma(\Delta_n(x_1,\dots,x_n)) \\
&= \operatorname{sign}(\tau)\operatorname{sign}(\sigma)\Delta_n(x_1,\dots,x_n) \\
&= \operatorname{sign}(\sigma\tau)\Delta_n(x_1,\dots,x_n)
\end{aligned}
$$

とい，$\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)$ である． □

互換は奇置換であり，上の定理から σ が r 個の互換の積で表わせるならば $\operatorname{sign}(\sigma) = (-1)^r$ である．これより，次の定理が得られる．

定理 5.8. σ が偶数個の互換の積で表わせるならば σ は偶置換であり，σ が奇数個の互換の積で表わせるならば σ は奇数換である．逆に，$\tau_1,\dots,\tau_r$ が互換で $\sigma = \tau_1\tau_2\cdots\tau_r$ のとき，σ が偶置換ならば r は偶数で，σ が奇置換ならば r は奇数である．

6. 行列式の定義

K は実数全体の集合 $\mathbb{R}$ か，複素数全体の集合 $\mathbb{C}$ か，有理数全体の集合 $\mathbb{Q}$ か，または一般の体とする．毎回そう書くのは面倒なので，単に「K は体とする」と書くが，あまり気にしないで，$K = \mathbb{R}$ か $K = \mathbb{C}$ だと思って読んでもらえばいい．ただ，$K = \mathbb{C}$ の場合もあるので，K の元に対しては不等号は使えない．線形代数 B2 で内積を導入するとき，$K = \mathbb{R}$ か $K = \mathbb{C}$ かで違いが発生するが，線形代数 B1 の範囲では，それが問題になることはほとんどない．

定義 6.1. n は自然数，K は体とし，K の元を成分とする n 次正方行列

$$
A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in M_n(K)
$$

を取る．$X_n = \{1, 2,\dots, n\}$ とする．$i_1, i_2,\dots, i_n \in X_n$ (同じ数が 2 度以上登場してもよい) に対して，$\mathbf{i} = (i_1,\dots, i_n)$ とおき，$\sigma_{\mathbf{i}}(k) = i_k$ $(1 \leqq \forall k \leqq n)$ で定まる写像 (置換) $\sigma_{\mathbf{i}}\colon X_n \to X_n$ を，

$$
\sigma_{\mathbf{i}} = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}
$$

と書くことにする．行列と同じ記号で書いているが，行列ではない．もし，$\sigma_{\mathbf{i}}$ が $1,\dots, n$ の置換のときは，$\operatorname{sign}(\sigma_{\mathbf{i}})$ は置換 $\sigma_{\mathbf{i}}$ の符号とし，$\sigma_{\mathbf{i}} \notin \mathfrak{S}_n$ ときは，$\operatorname{sign}(\sigma_{\mathbf{i}}) = 0$ とする．$\operatorname{sign}(\sigma_{\mathbf{i}})$ は $\operatorname{sign}\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ とも書かれる．今，

$$
\det A = \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n} \operatorname{sign}\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} a_{i_1,1}a_{i_2,2}\cdots a_{i_n,n} \tag{①}
$$

と定義し，$\det A$ を A の**行列式**という．$\det A$ を $|A|$ とか，

$$
\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \tag{②}
$$

とも書く．ただ，$|A|$ は別の目的 (行列 A のノルムなど) でも用いるので，この講義では $\det A$ か ② の書き方を用いる．$\sigma_{\mathbf{i}} \notin \mathfrak{S}_n$ の場合，$\operatorname{sign}(\sigma_{\mathbf{i}}) = 0$ なのでその項は足さなくでよいから，

$$
\det A = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sign}(\sigma) a_{\sigma(1),1}a_{\sigma(2),2}\cdots a_{\sigma(n),n}
$$

と書くこともできる．ここで，$\displaystyle\sum_{\sigma\in\mathfrak{S}_n}$ はすべての $\mathfrak{S}_n$ の元 σ について，シグマ記号の後に続く式の和を取ることを表す総和記号である．その流儀で書くと，① は，

$$
\det A = \sum_{(i_1,\dots,i_n)\in X_n^n} \operatorname{sign}\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} a_{i_1,1}a_{i_2,2}\cdots a_{i_n,n}
$$

とも書ける．また，

$$a_{i_1,1}a_{i_2,2}\cdots a_{i_n,n}=\prod_{k=1}^{n}a_{i_k,k},\quad a_{\sigma(1),1}a_{\sigma(2),2}\cdots a_{\sigma(n),n}=\prod_{k=1}^{n}a_{\sigma(k),k}$$

と書き直してもよい．

行列 A の第 j 列を $\mathbf{a}_j=\begin{pmatrix}a_{1,j}\\a_{2,j}\\\vdots\\a_{n,j}\end{pmatrix}$ とおいて，行列 A を $A=(\mathbf{a}_1,\,\mathbf{a}_2,\ldots,\,\mathbf{a}_n)$ と書くと便利なことが多い．この場合，$\det A$ は

$$\det(\mathbf{a}_1,\,\mathbf{a}_2,\ldots,\,\mathbf{a}_n)$$

と書かれる．

行列式 $\det A$ を上の定義式を用いて計算することは希で，これから説明する様々な公式を用いて計算するのが普通である．

例 6.2. $n=1$ で $A=(a_{11})$ のときは $\det A=a_{11}$ である．$n=2$ のときは，$\mathfrak{S}_2=\{\mathrm{id}_2,\,(1,2)\}$ なので，

$$\begin{vmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{vmatrix}=a_{11}a_{22}-a_{12}a_{21},\quad\begin{vmatrix}a&b\\c&d\end{vmatrix}=ad-bc$$

である．$n=3$ のときは，

$$\begin{vmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{vmatrix}=a_{11}a_{22}a_{33}+a_{12}a_{23}a_{31}+a_{21}a_{32}a_{13}-a_{31}a_{22}a_{31}-a_{12}a_{21}a_{33}-a_{11}a_{32}a_{23}$$

である．

定理 6.3. 正方行列 A や，関連する諸記号は上の定義の中のものと同じとする．そのとき，以下が成り立つ．

(1) $1\leqq j\leqq n$ をひとつ固定して，A の第 j 列目が，$\mathbf{a}_j=\beta\mathbf{b}+\gamma\mathbf{c}$ ($\beta,\,\gamma\in K;\,\mathbf{b},\,\mathbf{c}\in K^n$ と 2 つのベクトルの線形結合で表せるとき，次の等式が成り立つ．

$$\begin{aligned}&\det(\mathbf{a}_1,\ldots,\,\mathbf{a}_{j-1},\,\beta\mathbf{b}+\gamma\mathbf{c},\,\mathbf{a}_{j+1},\ldots,\,\mathbf{a}_n)\\&=\beta\det(\mathbf{a}_1,\ldots,\,\mathbf{a}_{j-1},\,\mathbf{b},\,\mathbf{a}_{j+1},\ldots,\,\mathbf{a}_n)+\gamma\det(\mathbf{a}_1,\ldots,\,\mathbf{a}_{j-1},\,\mathbf{c},\,\mathbf{a}_{j+1},\ldots,\,\mathbf{a}_n)\end{aligned}$$

(2) 上と同様に，$\mathbf{a}_j=\sum_{k=1}^{r}\beta_k\mathbf{b}_k$ ($\beta_l\in K,\,\mathbf{b}_k\in K^n$ と線形結合で表せるとき，次の等式が成り立つ．

$$\det\left(\mathbf{a}_1,\ldots,\,\mathbf{a}_{j-1},\,\sum_{k=1}^{r}\beta_k\mathbf{b}_k,\,\mathbf{a}_{j+1},\ldots,\,\mathbf{a}_n\right)=\sum_{k=1}^{r}\beta_k\det(\mathbf{a}_1,\ldots,\,\mathbf{a}_{j-1},\,\mathbf{b}_k,\,\mathbf{a}_{j+1},\ldots,\,\mathbf{a}_n)$$

(3) $\tau\in\mathfrak{S}_n$ に対し，次の等式が成り立つ．

$$\det(\mathbf{a}_{\tau(1)},\,\mathbf{a}_{\tau(2)},\ldots,\,\mathbf{a}_{\tau(n)})=\mathrm{sign}(\tau)\det(\mathbf{a}_1,\ldots,\,\mathbf{a}_n)$$

証明. (1) $\mathbf{b},\,\mathbf{c}$ の i 行目の成分を $b_i,\,c_i$ とする．$a_{i,j}=\beta b_i+\gamma c_i$ である．よって，

$$\begin{aligned}\det A&=\sum_{\sigma\in\mathfrak{S}_n}\mathrm{sign}(\sigma)a_{\sigma(1),1}\cdots a_{\sigma(j),j}\cdots a_{\sigma(n),n}\\&=\sum_{\sigma\in\mathfrak{S}_n}\mathrm{sign}(\sigma)a_{\sigma(1),1}\cdots(\beta b_{\sigma(j)}+\gamma c_{\sigma(j)})\cdots a_{\sigma(n),n}\\&=\beta\sum_{\sigma\in\mathfrak{S}_n}\mathrm{sign}(\sigma)a_{\sigma(1),1}\cdots b_{\sigma(j)}\cdots a_{\sigma(n),n}+\gamma\sum_{\sigma\in\mathfrak{S}_n}\mathrm{sign}(\sigma)a_{\sigma(1),1}\cdots c_{\sigma(j)}\cdots a_{\sigma(n),n}\\&=\beta\det(\mathbf{a}_1,\ldots,\,\mathbf{a}_{j-1},\,\mathbf{b},\,\mathbf{a}_{j+1},\ldots,\,\mathbf{a}_n)+\gamma\det(\mathbf{a}_1,\ldots,\,\mathbf{a}_{j-1},\,\mathbf{c},\,\mathbf{a}_{j+1},\ldots,\,\mathbf{a}_n)\end{aligned}$$

である．

(2) は (1) を用いて，r に関する帰納法ですぐわかる．

(3) $\det(\mathbf{a}_{\tau(1)}, \ldots, \mathbf{a}_{\tau(n)}) = \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sign}(\sigma) a_{\sigma(1),\tau(1)} \cdots a_{\sigma(n),\tau(n)} = \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sign}(\sigma) \prod_{i=1}^{n} a_{\sigma(i),\tau(i)}$ である．ところで，順列 $\tau(1),\ldots, \tau(n)$ は順列 $1,\ldots, n$ を置換 τ で並び変えたこのだから，$j = \tau(i)$ とおくと $i = \tau^{-1}(j)$ で，

$$\prod_{i=1}^{n} a_{\sigma(i),\tau(i)} = \prod_{j=1}^{n} a_{\sigma(\tau^{-1}(j)),j} = \prod_{j=1}^{n} a_{(\sigma\tau^{-1})(j),j} \qquad ①$$

が成り立つ．今，$\rho = \sigma\tau^{-1}$ とおく．σ が $\mathfrak{S}_n$ 全体を動くとき，ρ も $\mathfrak{S}_n$ 全体を動く．また，$\sigma = \rho\tau$ である．よって，

$$\begin{aligned}
\det(\mathbf{a}_{\tau(1)}, \ldots, \mathbf{a}_{\tau(n)}) &= \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sign}(\sigma) \prod_{j=1}^{n} a_{(\sigma\tau^{-1})(j),j} \\
&= \sum_{\rho\in\mathfrak{S}_n} \mathrm{sign}(\rho\tau) \prod_{j=1}^{n} a_{\rho(j),j} \\
&= \mathrm{sign}(\tau) \sum_{\rho\in\mathfrak{S}_n} \mathrm{sign}(\rho) \prod_{j=1}^{n} a_{\rho(j),j} \\
&= \mathrm{sign}(\tau) \det A
\end{aligned}$$

である． □

7. 行列式の性質

前回と同じく，n は自然数，K は体とし，K の元を成分とする n 次正方行列

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in M_n(K)$$

を取る．A の (i, j)-成分を $a_{ij} = a_{i,j}$ とし，A の第 j 列の列ベクトルを $\mathbf{a}_j = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ \vdots \\ a_{n,j} \end{pmatrix}$ とおいて，$A = (\mathbf{a}_1, \mathbf{a}_2,\ldots, \mathbf{a}_n)$ とも書く．

定理 7.1. ある $1 \leqq k < l \leqq n$ を満たす 1 組の整数 k, l に対して $\mathbf{a}_k = \mathbf{a}_l$ (つまり，A の k 列目と l 列目が同じ) が成り立てば，$\det A = 0$ である．

証明. 今，K においては $-1 \neq 1$, つまり $1 + 1 = 2 \neq 0$ であると仮定する．k と l の互換を $\tau = (k, l)$ とする．A の k 列目と l 列目を交換して得られる行列を B とする．定理 6.3 より，$\det B = \mathrm{sign}(\tau) \det A$ が成り立つ．$\mathrm{sign}(\tau) = -1$ で，$B = A$ であるので，$\det A = -\det A$ となる．すると，$2 \det A = 0$ となる．$2 \neq 0$ だから $\det A = 0$ である．

実は $-1 = 1$ を満たす体もあって，その場合，上の証明は使えないので，別の証明を与える必要があるが，話が長くなるので割愛する． □

$K = \{0, 1\}$ とし，掛け算 $\times$ は普通の掛け算で，足し算は $1 + 1 = 0$ と定める以外は普通の足し算と同じ，と約束しておくと，この K は体になる．$1 + 1 = 0$ より $-1 = 1, 2 = 0$ であって，上の証明の最後で言及した $-1 = 1$ を満たす体の 1 例になる．標数 2 の素体と呼ばれ，$K = \mathbb{F}_2$ と書かれる．情報科学で頻繁に使われる体である．$\mathbb{F}_2$ の元を成分とする行列式でも，上の定理は成立する．

上の定理と定理 6.3 を組み合わせると，次の定理が得られる．

定理 7.2. k, l は相異なる n 以下の自然数で，$c \in K$ とする．n 次正方行列 A の k 列目を c 倍して A の l 列目に加えた (または，l 列目から引いた) 行列を B とする．このとき，

$$\det B = \det A$$

である．

証明. 引く場合は c の代わりに $-c$ を使えばいいので，B の l 列目は $(\mathbf{a}_l + c\mathbf{a}_k)$ であるとする．あとは，定理 6.3(1) の公式を B に適用して，上の定理を使えばよい． □

$a_{j,i}$ を $(i,\, j)$-成分とする n 次正方行列を ${}^tA$ と書き，A の転置行列といった．

定理 7.3. $A \in M_n(K)$ のとき，$\det({}^tA) = \det A$ が成り立つ．

証明. $b_{i,j} = a_{j,i}$ とおくと，${}^tA = (b_{i,j})$ と書ける．

$$\det({}^tA) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} b_{\sigma(i),i} = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

である．$\displaystyle\prod_{i=1}^{n} a_{i,\sigma(i)}$ の因子 $a_{1,\sigma(1)},\ a_{2,\sigma(2)}, \ldots,\ a_{n,\sigma(n)}$ を並べ替えて 2 つ目の添え字が $1,\ 2, \ldots,\ n$ の順に並ぶようにするには，σ^{-1} によってこれらを並び変えればよく，そのように並び替えると，$a_{\sigma^{-1}(1),1}$, $a_{\sigma^{-1}(2),2}, \ldots,\ a_{\sigma^{-1}(n),n}$ となる．よって，

$$a_{1,\sigma(1)}a_{2,\sigma(1)} \cdots a_{n,\sigma(n)} = a_{\sigma^{-1}(1),1}a_{\sigma^{-1}(2),2} \cdots a_{\sigma^{-1}(n),n}$$

となる．また，σ が $\mathfrak{S}_n$ の元全体を動くことと，σ^{-1} が $\mathfrak{S}_n$ の元全体を動くこととは同値である．さらに，$\operatorname{sign}(\sigma)\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma\sigma^{-1}) = \operatorname{sign}(\mathrm{id}_n) = 1$ なので，$\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma)$ である．よって，

$$\begin{aligned}
\det {}^tA &= \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{\sigma^{-1}(i),i} \\
&= \sum_{\sigma^{-1} \in \mathfrak{S}_n} \operatorname{sign}(\sigma^{-1}) \prod_{i=1}^{n} a_{\sigma^{-1}(i),i} = \sum_{\tau \in \mathfrak{S}_n} \operatorname{sign}(\tau) \prod_{i=1}^{n} a_{\tau(i),i} = \det A
\end{aligned}$$

である．上で最後の式変形は σ^{-1} を τ と書き換えたものである． □

上の定理から，行列式については，**列について成り立つ性質は行についても成り立つ**ことに注意する．例えば，A の 2 つの行が等しければ $\det A = 0$ である．また，A のある 1 つの行ベクトルを c 倍して得られる行列を B とすると，$\det B = c \det A$ である．

定理 7.4. $A,\, B \in M_n(K)$ に対して，

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

が成り立つ．

証明. $A,\, B$ の $(i,\, j)$-成分を $a_{i,j},\, b_{i,j}$ とし，$A,\, B$ の第 j 列目の列ベクトルを $\mathbf{a}_j,\, \mathbf{b}_j$ とする．また，$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $\mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots,\ \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ とおく．$\mathbf{b}_j = \displaystyle\sum_{i=1}^{n} b_{i,j}\mathbf{e}_i$ である．AB の第 j 列目は $A\mathbf{b}_j$ であることに注意する．$\mathbf{c}_j := A\mathbf{b}_j$ とおく．

$$\mathbf{c}_j = A\sum_{i=1}^{n} b_{i,j}\mathbf{e}_i = \sum_{i=1}^{n} b_{i,j}A\mathbf{e}_i = \sum_{i=1}^{n} b_{i,j}\mathbf{a}_i$$

である．よって，

$$\det(AB)=\det(\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_n)=\det\left(\sum_{i_1=1}^{n}b_{i_1,1}\mathbf{a}_{i_1},\ \sum_{i_2=1}^{n}b_{i_2,2}\mathbf{a}_{i_2},\ \ldots,\ \sum_{i_n=1}^{n}b_{i_n,n}\mathbf{a}_{i_n}\right)$$
$$=\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n}b_{i_1,1}b_{i_2,2}\cdots b_{i_n,n}\det(\mathbf{a}_{i_1},\,\mathbf{a}_{i_2},\,\ldots,\,\mathbf{a}_{i_n})$$

となる．$\sigma(k)=i_k$ で定まる写像を $\sigma=\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}$ とする．σ が置換でないときは，σ は単射でないから，ある $k\neq l\in X_k$ で $i_k=\sigma(k)=\sigma(l)=i_l$ となるものがある．このとき，$\mathbf{a}_{i_k}=\mathbf{a}_{i_l}$ なので，$\det(\mathbf{a}_{i_1},\,\mathbf{a}_{i_2},\ldots,\,\mathbf{a}_{i_n})=0$ である．また，$\sigma\in\mathfrak{S}_n$ のときは，

$$\det(\mathbf{a}_{i_1},\,\mathbf{a}_{i_2},\,\ldots,\,\mathbf{a}_{i_n})=\det(\mathbf{a}_{\sigma(1)},\,\mathbf{a}_{\sigma(2)},\,\ldots,\,\mathbf{a}_{\sigma(n)})$$
$$=\operatorname{sign}(\sigma)\det(\mathbf{a}_1,\,\mathbf{a}_2,\ldots,\,\mathbf{a}_n)=\operatorname{sign}(\sigma)\det A$$

となる．前に書いたように，$\sigma\notin\mathfrak{S}_n$ のときは $\operatorname{sign}(\sigma)=0$ と約束しておけば，$\sigma\notin\mathfrak{S}_n$ でも上の等式は成り立つ．よって，

$$\det(AB)=\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n}b_{i_1,1}b_{i_2,2}\cdots b_{i_n,n}\operatorname{sign}\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}\det A$$
$$=(\det A)\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n}\operatorname{sign}\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}b_{i_1,1}b_{i_2,2}\cdots b_{i_n,n}$$
$$=(\det A)\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n}\operatorname{sign}\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}b_{i_1,1}b_{i_2,2}\cdots b_{i_n,n}$$
$$=(\det A)(\det B)$$

である． □

8. 行列式の展開公式

前回までと同じく，n は自然数，K は体とし，K の元を成分とする n 次正方行列

$$A=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}\in M_n(K)$$

を考える．A の $(i,\,j)$-成分を $a_{ij}=a_{i,j}$ とし，A の第 j 列の列ベクトルを $\mathbf{a}_j=\begin{pmatrix}a_{1,j}\\ a_{2,j}\\ \vdots\\ a_{n,j}\end{pmatrix}$ とおいて，$A=(\mathbf{a}_1,\,\mathbf{a}_2,\ldots,\,\mathbf{a}_n)$ とも書く．また，$\mathbf{e}_1=\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix}$, $\mathbf{e}_2=\begin{pmatrix}0\\1\\ \vdots\\0\end{pmatrix}$,…, $\mathbf{e}_n=\begin{pmatrix}0\\0\\ \vdots\\1\end{pmatrix}$ とおく．

展開公式の証明のための準備から始める．

補題 8.1. $(n+1)$ 次正方行列 $B=(b_{ij})$ (b_{ij} は B の $(i,\,j)$-成分) を次のように定める．$i\leqq n$ かつ $j\leqq n$ のときは $b_{ij}=a_{ij}$ とする．$b_{n+1,n+1}=1$ とする．$1\leqq i\leqq n$ のとき $b_{i,n+1}=0$ とする．それ以外の成分は何でもかまわない．つまり，

$$B=\begin{pmatrix}a_{1,1}&\cdots&a_{1,n}&0\\ \vdots&&\vdots&\vdots\\ a_{n,1}&\cdots&a_{n,n}&0\\ b_{n+1,1}&\cdots&b_{n+1,n}&1\end{pmatrix}$$

とおく．すると，
$$\det B = \det A$$
が成り立つ．

証明. $\det B = \sum_{\sigma\in\mathfrak{S}_{n+1}} \mathrm{sign}(\sigma)\prod_{i=1}^{n+1} b_{\sigma(i),i}$ である．もし $\sigma(n+1)\neq n+1$ ならば $b_{\sigma(n+1),n+1}=0$ なので，$\sigma(n+1)=n+1$ を満たす $\sigma\in\mathfrak{S}_{n+1}$ についてのみ和 $(\sum)$ を取ればよい．$\sigma(n+1)=n+1$ を満たす σ は $\sigma\in\mathfrak{S}_n$ と考えることができる．そのとき $b_{\sigma(n+1),n+1}=b_{n+1,n+1}=1$ である．よって，
$$\det B = \sum_{\sigma\in\mathfrak{S}_n}\mathrm{sign}(\sigma)\left(\prod_{i=1}^{n} b_{\sigma(i),i}\right)\cdot b_{n+1,n+1} = \sum_{\sigma\in\mathfrak{S}_n}\mathrm{sign}(\sigma)\prod_{i=1}^{n} a_{\sigma(i),i} = \det A$$
である． □

補題 8.2. $n\geqq 2$ とし，整数 $1\leqq k\leqq n$ と $1\leqq l\leqq n$ を固定する．$A\in M_n(K)$ の第 l 列目の列ベクトル $\mathbf{a}_l$ のところを $\mathbf{e}_k$ で置き換えてできる n 次正方行列を $B_{k,l}$ とおく．つまり，
$$B_{k,l} = (\mathbf{a}_1,\dots,\mathbf{a}_{l-1},\mathbf{e}_k,\mathbf{a}_{l+1},\dots,\mathbf{a}_n)$$
である．また，A の k 行目と l 列目を取り除いてできる $(n-1)$ 次の行列を $A_{k,l}$ とおく (取り除いた行や列の間は詰める．$A_{k,l}$ を A の**小行列**という)．このとき，
$$\det A_{k,l} = (-1)^{k+l}\det B_{k,l}$$
が成り立つ．$A_{k,l}$ を A_{kl} と書くことも多い．

証明. 整数 $1\leqq m<n$ に対し，
$$\sigma_m := \begin{pmatrix} 1 & 2 & \cdots & m-1 & m & m+1 & m+2 & \cdots & n \\ 1 & 2 & \cdots & m-1 & n & m & m+1 & \cdots & n-1\end{pmatrix}$$
という置換 $\sigma_m\in\mathfrak{S}_n$ を考える．ただし，$\sigma_n=\mathrm{id}_n$ とする．σ は $\sigma=(m,\,n)(m+1,\,n)\cdots(n-2,\,n)(n-1,\,n)$ と $(n-m-1)$ 個の互換の積で表すことができる．よって，$\mathrm{sign}(\sigma_m)=(-1)^{n-m-1}$ である．

今，$B_{k,l}$ の列ベクトルを置換 σ_k で並び替え，その後，行ベクトルを置換 σ_l で並べ替えで得られる n 次正方行列を C とする．
$$\det C = (-1)^{n-k-1}(-1)^{n-l-1}\det B_{k,l} = (-1)^{k+l}\det B_{k,l}$$
である．C の $(i,\,j)$-成分を $c_{i,j}$ とする．$i\leqq n-1$ かつ $j\leqq n-1$ ならば $c_{i,j}$ は $A_{k,l}$ の $(i,\,j)$-成分と一致している．また，C の n 列目は $\mathbf{e}_n$ である．よって，前補題から，$\det A_{k,l}=\det C$ が成り立つ．よって，$\det A_{k,l}=(-1)^{k+l}\det B_{k,l}$ である． □

定理 8.3.(展開公式) 前補題のように，$A\in M_n(K)$ の k 行目と l 列目を取り除いてできる $(n-1)$ 次の小行列を $A_{k,l}$ とする．また，A の $(i,\,j)$-成分を $a_{i,j}$ とする．このとき以下が成り立つ．

(1) $\det A = \sum_{i=1}^{n}(-1)^{i+l}a_{i,l}\det A_{i,l}$

(2) $\det A = \sum_{j=1}^{n}(-1)^{k+j}a_{k,j}\det A_{k,j}$

なお，(1) を $\det A$ を第 l 列で**展開**するといい，(2) を $\det A$ を第 k 行目で展開するという．

証明. (1) $B_{k,l}$ は前定理と同じとする．$\mathbf{a}_l=\sum_{i=1}^{n}a_{i,l}\mathbf{e}_i$ なので，
$$\begin{aligned}\det A &= \det\left(\mathbf{a}_1,\dots,\mathbf{a}_{l-1},\sum_{i=1}^{n}a_{i,l}\mathbf{e}_i,\mathbf{a}_{l+1},\dots,\mathbf{a}_n\right)\\ &= \sum_{i=1}^{n}a_{i,l}\det(\mathbf{a}_1,\dots,\mathbf{a}_{l-1},\mathbf{e}_i,\mathbf{a}_{l+1},\dots,\mathbf{a}_n)\end{aligned}$$

$$= \sum_{i=1}^{n} a_{i,l} \det B_{i,l} = \sum_{i=1}^{n} (-1)^{i+l} a_{i,l} \det A_{i,l}$$

である．

(2) は両辺の転置行列を考えれば，(1) に帰着される． □

系 8.4. 単位行列 I_n については $\det I_n = 1$ である．

証明. 上の展開公式を用いて，n に関する帰納法ですぐわかる．

定義 8.5.(余因子行列) n 次正方行列 $A \in M_n(K)$ に対し，A の j 行目と i 列目を取り除いてできる $(n-1)$ 次の小行列を $A_{j,i}$ とする．$(1 \leqq i \leqq n,\ 1 \leqq j \leqq n)$ そして，

$$b_{i,j} = (-1)^{i+j} \det A_{j,i}$$

とおく．$b_{i,j}$ と $A_{j,i}$ で添え字 i と j の順序が反対になることを注意せよ．そして，このように $b_{i,j}$ を (i,j)-成分とする n 次正方行列を B とする．この B を A の**余因子行列**といい，$b_{i,j}$ を A の**余因子**という．この B は $\widetilde{A}$ などと書かれることが多いが，余因子行列を表す記号は特に定まっていない．

定理 8.6.(逆行列の公式) $A \in M_n(K)$ の余因子行列を $\widetilde{A}$ とする．また，I_n は n 次の単位行列とする．このとき，次が成り立つ．

$$\widetilde{A}A = (\det A)I_n, \quad A\widetilde{A} = (\det A)I_n \qquad ①$$

したがって，$\det A \neq 0$ ならば A は逆行列を持ち，

$$A^{-1} = \frac{1}{\det A}\widetilde{A} \qquad ②$$

が成り立つ．逆に，A が逆行列を持つならば $\det A \neq 0$ である．また，

$$\det(A^{-1}) = \frac{1}{\det A} \qquad ③$$

である．

証明. $\widetilde{A}$ の (i,j)-成分を $b_{i,j} = (-1)^{i+j} \det A_{j,i}$ とする．また，$\widetilde{A}A$ の (i,j)-成分を $c_{i,j}$ とする．$i = j$ のときは，

$$c_{i,i} = \sum_{k=1}^{n} b_{i,k} a_{k,i} = \sum_{k=1}^{n} (-1)^{i+k} a_{k,i} \det A_{k,i} = \det A$$

である．

$i \neq j$ の場合を考える．A の j 列目を $\mathbf{a}_i$ で置換えた行列を D とする．$d_{k,j} = a_{k,i}$ で $l \neq j$ のとき $d_{k,l} = a_{k,l}$ である．D の i 列目と j 列目はともに $\mathbf{a}_i$ で等しいので，$\det D = 0$ である．D の j 列目以外は A と同じだから $\det D$ を j 列目で展開すると，

$$0 = \det D = \sum_{k=1}^{n} (-1)^{k+j} d_{k,j} \det A_{k,j} = \sum_{k=1}^{n} (-1)^{k+j} a_{k,i} \det A_{k,j}$$
$$= \sum_{k=1}^{n} b_{j,k} a_{k,i} = c_{j,i}$$

よって，$\widetilde{A}A = (\det A)I_n$ である．

$A\widetilde{A} = (\det A)I_n$ は，行列式の列による展開公式の代わりに，行による展開公式を使って，上と同様に証明できる．

したがって，$\det A \neq 0$ ならば ② が成立する．

A^{-1} が存在すれば

$$1 = \det I_n = \det(AA^{-1}) = (\det A)(\det A^{-1})$$

なので，$\det A \neq 0$ で ③ が成り立つ． □

定理 8.7. n 次正方行列 $A, B \in M_n(K)$ が $AB = I_n$ または $BA = I_n$ のいずれか一方を満たせば A は可逆行列 (逆行列を持つ行列) で，$B = A^{-1}, A = B^{-1}$ である．

証明. $AB = I_n$ とすると，上で述べたように $(\det A)(\det B) = \det I = 1$ だから，$\det A \neq 0, \det B \neq 0$ で A も B も逆行列を持つ．逆行列の一意性から $B = A^{-1}$, $A = B^{-1}$ である．

$BA = I_n$ の場合も同様である． □

9. 展開公式の応用

定義 9.1.(上半三角行列) K は体，$A = (a_{i,j}) \in M_n(K)$ は n 次正方行列とする．もし，$i < j$ のとき $a_{i,j} = 0$ であるならば A は**上半三角行列**であるという．反対に，$i > j$ のとき $a_{i,j} = 0$ であるならば A は**下半三角行列**であるという．例えば，$n = 3$ の時の上半三角行列 A と下半三角行列 B は以下の形である．

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & 0 & 0 \\ b_{21} & b_{22} & 0 \\ b_{31} & b_{32} & a_{33} \end{pmatrix}$$

定理 9.2. n 次正方行列 $A = (a_{i,j}) \in M_n(K)$ が上半三角行列であるか，または，下半三角行列であるならば，

$$\det A = a_{1,1}a_{2,2}a_{3,3}\cdots a_{n,n}$$

と，$\det A$ は A の対角成分の積になる．

証明. A が上三角行列の場合に，n に関する帰納法で証明する．$n = 1$ ならば $A = (a_{1,1}) \in M_1(K)$ だから，$\det A = a_{1,1}$ である．

$n \geqq 2$ とし，A の n 行目と n 列目を取り除いてできる $(n-1)$ 次の小行列を A_{nn} とする．$\det A$ を n 行目で展開すると，A の n 行目は $(0, 0,\ldots, 0, a_{nn})$ だから，$\det A = (-1)^{n+n}a_{nn}\det A_{nn}$ となる．帰納法の仮定から，$\det A_{nn} = a_{11}a_{22}\cdots a_{n-1,n-1}$ である．よって，$\det A = a_{11}a_{22}\cdots a_{nn}$ である．

下半三角行列の場合は，転置行列を取れば上半三角行列になるので，上の結果に帰着される． □

次に以下のような連立方程式を解くことを考える．

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

ここで，各 a_{ij} と b_i は体 K に属する与えられた定数で，$x_1,\ldots, x_n$ は未知数で，これを求めるのが目標である．

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

とおけば，上の連立方程式は，

$$A\mathbf{x} = \mathbf{b}$$

とシンプルに書き直せる．今回は $\det A \neq 0$ の場合のみを考え，$\det A = 0$ の場合は，後の回で掃き出し法を用いて解法を考える．

$\det A \neq 0$ の場合は，$\widetilde{A}$ を A の余因子行列とすると，$A^{-1} = \dfrac{1}{\det A}\widetilde{A}$ であるので，

$$\mathbf{x} = \frac{1}{\det A}\widetilde{A}\mathbf{b}$$

となる．これでもいいのだが，以下の公式も有名である．

定理 9.3. (クラメルの公式) 記号は上と同じとし，$\det A \neq 0$ を仮定する．A の第 i 列 $\mathbf{a}_i$ のところを列ベクトル $\mathbf{b}$ に置き換えてできる n 次正方行列を A_i とする $(1 \leqq i \leqq n)$．すると，

$$x_i = \frac{\det A_i}{\det A} = \frac{\begin{vmatrix} a_{1,1} & \cdots & a_{1,i-1} & b_1 & a_{1,i+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,i-1} & b_n & a_{n,i+1} & \cdots & a_{n,n} \end{vmatrix}}{\begin{vmatrix} a_{1,1} & \cdots & a_{1,i-1} & a_{1,i} & a_{1,i+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,i-1} & a_{n,i} & a_{n,i+1} & \cdots & a_{n,n} \end{vmatrix}} \quad (1 \leqq i \leqq n)$$

である．

証明. A の j 行目と i 列目を取り除いてできる $(n-1)$ 次の小行列を $A_{j,i}$ とし，$c_{i,j} = (-1)^{i+j} \det A_{j,i}$ とするとき，$\widetilde{A} = (c_{i,j})$ であった．$\mathbf{x} = (1/\det A)\widetilde{A}\mathbf{b}$ なので，この等式の k 行目を比較すると，

$$x_k = (1/\det A) \sum_{j=1}^{n} c_{k,j} b_j = (1/\det A) \sum_{j=1}^{n} (-1)^{k+j} (\det A_{j,k}) b_j \qquad ①$$

である．他方，$\det A_k$ を第 k 列で展開すると，A の $(i,\, k)$-成分は b_k で，第 i 列以外は A と同じなので，

$$\det A_i = \sum_{i=1}^{n} (-1)^{i+k} b_j \det A_{i,k} = \sum_{j=1}^{n} (-1)^{k+j} \det A_{j,k} b_j$$

となる，よって，$x_k = (\det A_k)/(\det A)$ である． $\square$

10. 掃き出し法 (1)

以下のような連立方程式を解くことを考える．

$$\begin{cases} \quad a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ \quad a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

ただし，$m = n$ は仮定せず，$m < n$ や $m > n$ の場合も含めて考える．中学で習った数学の範囲で解こうとすると，以下の操作を繰り返して行って，未知数 x_i の前の係数が，できるだけ沢山 0 になるように変形する．以下の操作のうち (L3) は意味がないが，後の説明のために書いてある．

(L1) ある方程式の両辺に，ある数 c を掛け，それを他の方程式の両辺に足す (または引く)．

(L2) ある方程式の両辺に，0 でないある数 c を書ける (または c で割る)．

(L3) m 個の方程式の中から 2 つを選んで，その書いてある行を入れ替える．

このような操作を**掃き出し**という．(L1) で「引く」という部分は c の代わりに $-c$ を考えると「足す」操作になるので，考えなくてよい．(L2) でも，c で「割る」のは $1/c$ を「掛ける」のと同じだから，考えなくてよい．ところで，この計算の途中で何回も $x_1, \ldots, x_n$ を書くのは面倒なので，係数 $a_{i,j}$ と b_j だけを抜き出して

$$A' := (A, \mathbf{b}) := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_n \end{pmatrix}$$

という行列を作って，この行列に対して以下の操作を行っても，実質的に上の操作と同じである．

(L1) A' の第 i 行に定数 c を掛け，それを第 j 行目に足す $(1 \leqq i \leqq m,\, 1 \leqq j \leqq m,\, i \neq j)$．

(L2) A' の第 i 行に定数 $c \neq 0$ を掛ける．

(L3) A' の第 i 行と第 j 列を交換する．

この 3 種類の操作を行列に対する**行基本操作**とか**行基本変形**という．なお，$(A,\, \mathbf{b})$ を**拡大行列**ともいう．

命題 10.1. 上の操作 (L3)「i 行と第 j 列を交換する」は，(L1)「第 i 行に 1 を掛け第 j 行目に足す」，(L1)「第 j 行に (-1) を掛け第 i 行目に足す」，(L1)「第 i 行に 1 を掛け第 j 行目に足す」，(L2)「第 i 行に -1 を掛ける」という操作を順に行うことによって得られる．

記号設定 10.2. 掃き出し法のために持ちいる特別な行列に対して記号を設定しておく．一般的な記号ではなく，ここだけの一時的な記号である．

(1) k, l を固定した自然数とし，(k, l)-成分だけが 1 で，それ以外の成分が 0 である行列を $E_{k,l}$ と書くことにする．それが m 行 n 列行列のときは $E^{(m,n)}_{k,l}$ とも書くことにし，n 次正方行列のときは $E^{(n)}_{k,l}$ とも書く．一般に $A = (a_{i,j}) \in M_{mn}(K)$ に対し，

$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{i,j}E^{(m,n)}_{i,j}$$

である．

(2) k, l は固定した自然数で $k \neq l$ とする．また $c \in K$ とする．

$$\varLambda_{k,l}(c) = \varLambda^{(n)}_{k,l}(c) := I_n + cE^{(n)}_{k,l}$$

と定める．

(3) $1 \leqq k \leqq n$ は固定した自然数で，$0 \neq c \in K$ とする．単位行列 I_n の (k, k)-成分だけを c でおきかえた行列を

$$M_k(c) = M^{(n)}_k(c) := I_n + (c-1)E^{(n)}_{k,k}$$

とおく．

命題 10.3. $A' = (A, \mathbf{b})$ は上の行基本操作の説明のところと同じとする．

(1) A' に (L1)「第 i 行に定数 c を掛け第 j 行目に足す」ことによって行列 B' が得られたとする．このとき，

$$B' = (\varLambda^{(n)}_{j,i}(c))A'$$

が成り立つ．

(2) A' に (L2)「第 i 行に定数 $c \neq 0$ を掛ける」ことによって行列 B' が得られたとする．このとき，

$$B' = (M^{(n)}_i(c))A'$$

が成り立つ．

証明は，実際に上の掛け算を実行してみればわかる．言いたいことは「行基本変形は $\varLambda^{(n)}_{j,i}(c)$ や $M^{(n)}_i(c)$ とういう形の行列を左から掛けることによって得られる」ということである．また，

$$(\Lambda^{(n)}_{j,i}(c))^{-1} = \varLambda^{(n)}_{j,i}(-c), \quad (M^{(n)}_i(c))^{-1} = M^{(n)}_i(1/c), \quad \det \Lambda^{(n)}_{j,i}(c) = 1, \quad \det M^{(n)}_i(c) = c$$

である．また，上の等式は，掃き出し (行基本変形) は，それを逆に実行して元に戻すことができることを意味していて，それが同値変形であることを保障している．

掃き出し法の 1 つの目的は，行列 A' に行基本変形を上手に繰り返して行って，以下のような階段行列に変形することである．掃き出しは連立方程式を解く以外に，行列式の計算や逆行列の計算など，複数の用途があるので，$A' = (A, \mathbf{b})$ から離れて，以下，m 行 n 列の行列 A に対する掃き出し法を説明する．そのほうが，$\mathbf{b}$ を別に書かなくてもいいので，説明しやすい．目的によっては，必ずしも階段行列になるところまで計算しなくてもよいが，それは後で個別に説明する．

定義 10.4. (階段行列) $B = (b_{i,j}) \in M_{mn}(K)$ は以下の条件を満たすとき**階段行列**であるという．なお，B の第 j 列の列ベクトルを $\mathbf{b}_j$ とする．

(1) $1 \leqq r \leqq m$ を満たす自然数 r がある．また，$1 \leqq s_1 < s_2 < \cdots < s_r \leqq n$ を満たす自然数 $s_1, s_2, \ldots, s_r$ がある．

(2) $\mathbf{b}_{s_1} = \mathbf{e}_1, \mathbf{b}_{s_2} = \mathbf{e}_2, \ldots, \mathbf{b}_{s_r} = \mathbf{e}_r$ (基本ベクトル) である．$b_{i,s_i} = 1$ の箇所を i 番目の**階段**という．

(3) $j < s_1$ ならば $\mathbf{b}_j = \mathbf{0}$ である．

(4) $1 \leqq k < r$ で $s_k < j < s_{k+1}$ ならば，$i > k$ のとき $b_{i,j} = 0$ である．つまり，$\mathbf{b}_j = \displaystyle\sum_{i=1}^{k} b_{i,j}\mathbf{e}_i$ である．

(5) $j > s_r$ ならば，$i > s_r$ のとき $b_{i,j} = 0$ である．

この r を階段行列 B の**ランク**または**階数**といい，$r = \operatorname{rank} B$ という記号で表す．定まった用語は決まっていないが，後の説明の便宜上，$\mathbf{b}_{s_i} = \mathbf{e}_i$ を i **段目の段の列ベクトル**と呼ぶことにする．

例えば，次の B は階段行列である．

$$B = \begin{pmatrix} 0 & 1 & b_{13} & 0 & b_{15} & b_{16} & 0 & 0 & b_{19} \\ 0 & 0 & 0 & 1 & b_{25} & b_{26} & 0 & 0 & b_{29} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & b_{39} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & b_{49} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

この例の場合，$\operatorname{rank} B = r = 4$ で，$s_1 = 2, s_2 = 4, s_3 = 7, s_4 = 8$ である．b_{ij} と書いてある部分は，そこにどんな数があっても構わない．(特に 0 であってもよい.)

定理 10.5. (階段行列の一意性) $B \in M_{mn}(K)$ と $C \in M_{mn}(K)$ はいずれも階段行列で，ある可逆行列 $P \in M_m(K)$ により $C = PB$ が成立すると仮定する．すると，$B = C$ である．($P = I_m$ とは限らない)

証明. B について，r と $1 \leqq s_1 < s_2 < \cdots < s_r \leqq n$ は上の定義の通りの自然数であるとする．$C = (c_{ij})$ の j 列目の列ベクトルを $\mathbf{c}_j$ とする．$C = PB$ より $\mathbf{c}_j = P\mathbf{b}_j$ $(1 \leqq \forall j \leqq n)$ である．すべての j に対して $\mathbf{c}_j = \mathbf{b}_j$ が成り立つことを示せばよい．

(1) $j < s_1$ のとき $\mathbf{b}_j = \mathbf{0}$ だから，$\mathbf{c}_j = \mathbf{0}$ である．

(2) $\mathbf{c}_{s_1} = P\mathbf{b}_{s_1} = P\mathbf{e}_1, \mathbf{e}_1 = \mathbf{b}_{s_1} = P^{-1}\mathbf{c}_{s_1}$ だから，$\mathbf{c}_{s_1} \neq \mathbf{0}$ である．B は階段行列だから，B の 1 段目の階段は $\mathbf{c}_{s_1}$ のところにくるしかない．よって，$\mathbf{c}_{s_1} = \mathbf{e}_1 = \mathbf{b}_{s_1}$ である．また，$P\mathbf{e}_1 = P\mathbf{b}_{s_1} = \mathbf{c}_{s_1} = \mathbf{e}_1$ が成り立つ．P は可逆なので，$P^{-1}\mathbf{e}_1 = \mathbf{e}_1$ である．

(3) さて，いま，帰納的に $j \leqq s_k$ のとき $\mathbf{c}_j = \mathbf{b}_j$ で，$1 \leqq \forall i \leqq k$ に対し $\mathbf{c}_{s_i} = \mathbf{e}_i = \mathbf{b}_{s_i}$, $P\mathbf{e}_i = \mathbf{e}_i$, $P^{-1}\mathbf{e}_i = \mathbf{e}_i$ が成り立つことが証明されたとする．(4) $s_k < j < s_{k+1}$ ならば $\mathbf{c}_j = \mathbf{b}_j$ であること (ただし，形式的に $s_{r+1} = n + 1$ と考える) と，(5) $k < r$ ならば，$\mathbf{c}_{s_{k+1}} = \mathbf{e}_{k+1} = \mathbf{b}_{s_{k+1}}$, $P\mathbf{e}_{k+1} = \mathbf{e}_{k+1}$, $P^{-1}\mathbf{e}_{k+1} = \mathbf{e}_{k+1}$ が成り立つことを証明する．

(4) $s_k < j < s_{k+1}$ とする．定義 10.4(4) より $\mathbf{b}_j = \displaystyle\sum_{i=1}^{k} b_{i,j}\mathbf{e}_i$ である．したがって，

$$\mathbf{c}_j = P\mathbf{b}_j = \sum_{i=1}^{k} b_{i,j}P\mathbf{e}_i = \sum_{i=1}^{k} b_{i,j}\mathbf{e}_i = \mathbf{b}_j$$

である．

(5) $k < r$ とする．$\mathbf{c}_{s_{k+1}} = P\mathbf{b}_{s_{k+1}} = P\mathbf{e}_{k+1}$ である．もし $\mathbf{c}_{s_{k+1}} = \displaystyle\sum_{i=1}^{k} b_{i,s_{k+1}}\mathbf{e}_i$ と i 段の高さだったとすると，

$$P^{-1}\mathbf{c}_{s_{k+1}} = \sum_{i=1}^{k} \mathbf{c}_{i,s_{k+1}}P^{-1}\mathbf{e}_i = \sum_{i=1}^{k} \mathbf{c}_{i,s_{k+1}}\mathbf{e}_i \neq \mathbf{e}_{k+1}$$

となって矛盾する．よって，$\mathbf{c}_{s_{k+1}}$ は始めて登場する $(k+1)$ 段以上の列ベクトである．階段行列の定義からここが $(k+1)$ 段目の階段で $\mathbf{c}_{s_{k+1}} = \mathbf{e}_{k+1}$ である．よって，$\mathbf{c}_{s_{k+1}} = \mathbf{e}_{k+1} = \mathbf{b}_{s_{k+1}}$, $P\mathbf{e}_{k+1} = P\mathbf{b}_{s_{k+1}} = \mathbf{c}_{s_{k+1}} = \mathbf{e}_{k+1}$, $P^{-1}\mathbf{e}_{k+1} = \mathbf{e}_{k+1}$ である．

以上より $B = C$ が証明された． □

11. 掃き出し法 (2)

アルゴリズム 11.1. 行列 $A_0 = A = (a_{i,j}) \in M_{mn}(K)$ から始めて，行基本変形を繰り返して階段行列に変形するアルゴリズムを述べる．行列 $A_r \in M_{mn}(K)$ の (i, j)-成分を $a^{(r)}_{i,j}$ と書くことにする．以下のアルゴリズムはインデントして書いてある．

(1) $r = 0, k = 1, l = 1$ から始めて $k \leqq m, l \leqq n$ である限り，以下の操作を繰り返す．

　(2) $a^{(r)}_{k,l} = 0$ ならば (3) に移動する．$a^{(r)}_{k,l} \neq 0$ ならば (4) に移動する．

(3) $k+1 \leqq i \leqq m$ の中で $a_{i,l}^{(r)} \neq 0$ となるような i をさがし，そのような i があれば，A_r の i 行目と k 行目を交換した行列を A_{r+1} とおき，r の値を 1 大きくして (4) に移動する．$a_{k,l}^{(r)} = a_{k+1,l}^{(r)} = a_{k+2,l}^{(r)} = \cdots = a_{m,l}^{(r)} = 0$ の場合には，l の値を 1 大きくし，$l \leqq n$ だったら (2) に移動する．$l > n$ だったら (9) に移動する．

(4) ここに到着したときは $a_{k,l}^{(r)} \neq 0$ なので，A_r の第 k 行を $1/a_{k,l}^{(r)}$ 倍して得られる行列を A_{r+1} とし，r の値を 1 大きくした後，次の (5) に移動する．

(5) $i = 1, 2, \ldots, k-1, k+1, \ldots, m$ (つまり $i = k$ 以外のすべての $1 \leqq i \leqq m$) に対して次の (6) の操作を行う．

  (6) A_r の第 k 行に $(-a_{i,l}^{(r)})$ を掛け i 行目に加えた行列を A_{r+1} とおく．$a_{i,l}^{(r+1)} = 0$ であることに注意する．そして r の値を 1 大きくする．

(7) この段階では $\mathbf{a}_l^{(r)} = \mathbf{e}_k$ となることに注意する．k の値を 1 大きくし，l の値も 1 大きくして，$k \leqq m$ かつ $l \leqq n$ だったら (2) に移動する．

(9) ここに到達したときには A_r は階段行列になっている．

C++ で上のアルゴリズムのコーディングすると下記のようになる．ただ，実数だと計算誤算の関係で $a_{k,l} = 0$ かどうかの判定がうまくいかないので，有理数を成分とする行列で書いてある．また，配列 A[i][j] の添え字は C++ では $0 \leqq i < m, 0 \leqq j < n$ の範囲を動くので，-1 ずれることに注意する．

```
/* m と n は定数の整数として定義されているとする */
rational A[m][n]; /* 誤算がでないように A は有理数を成分とする行列とする */
rational x;       /*  作業用変数 */
int i, j, k, l;
/* 掃き出し法を実行する */
for(k=l=0; k<m && l<n; ){
   if(A[k][l]==0){  /* 階段成分が 0 の場合．実数の場合は誤差に注意 */
      for(i=k+1; A[i][l]==0 && i<m; i++);
      if(i==m){l++; continue;} /* 階段が横に長くなる */
      /* A の第 i 行と第 k 行を入れ替える */
      for(j=l; j<n; j++){x=A[i][j]; A[i][j]=A[k][j]; A[k][j]=x;}
   }
   /* A の第 k 行を A[k][l] で割る */
   x=A[k][l]; A[k][l]=1;
   for(j=l+1; j<n; j++) A[k][j]=A[k][j]/x;
   for(i=0; i<m; i++){
      if(i==k) continue;
      /* 第 i 行から第 k 行を a[i][l] 倍して引く */
      x=A[i][l];
      for(j=l; j<n; j++) A[i][j]=A[i][j]-x*A[k][j];
   }
   k++; l++;
}
/* 以上で A は階段行列になる */
```

この計算は人間が手計算で行うと計算ミスが多く，計算機に任せたほうがよいが，試験のときだけは諦めてほしい．

定理 11.2. $A \in M_{mn}$ から掃き出し法によって階段行列 B が得られたとする．

(1) ある可逆な m 次正方行列 P により，$B = PA$ と書ける．

(2) A から掃き出し法で得られる階段行列 B は，計算の手順に依存せずに一定である．そこで，短く B を A の**階段行列**と呼ぶ．

証明. (1) 掃き出しの過程は $A_{i,j}(c)$, $M_i(c)$ $(c \neq 0)$ という形の行列を左から掛けることであったから，それらの積を P とすればよい．

(2) B_1, B_2 が A から得られる階段行列とする．ある可逆行列 $P_1, P_2 \in M_m(K)$ により，$B_1 = P_1A$, $B_2 = P_2A$ と書ける．$B_2 = (P_2P_1^{-1})B_1$ である．定理 10.5 より $B_1 = B_2$ となる． □

階段行列が計算できたとき，何がわかるかを定理として書いておく．連立方程式より，行列式や行列式の計算のほうが簡明なので，先に説明する．

定理 11.3.(行列式の計算) n 次正方行列 $A \in M_n(K)$ に対して上のアルゴリズムを実行する過程で次の操作を行う．最初 $d = 1$ としておく．掃き出し法の過程で 2 つの行を交換する操作を行ったら，そのたびに d を (-1) 倍する．また，ある行を c 倍する操作を行ったら d を c で割る．最後に A の階段行列 B が得られたとき，$B = I_n$ (単位行列) であれば $\det A = d$ である．$B \neq I_n$ のときは $\det A = 0$ である．なお，上のアルゴリズムの (2) の段階で $k \neq l$ となることが起きたら $\det A = 0$ である．

証明. A_r の 2 つの行を交換した行列を A_{r+1} の場合，$\det A_{r+1} = -\det A_r$ である．また，A_r のある行を c 倍した行列を A_{r+1} とする操作を行った場合，$\det A_{r+1} = c \det A_r$ である．他方，A_r のある行を c 倍して他の行に足す操作を行って得られた行列が A_{r+1} である場合は，$\det A_{r+1} = \det A_r$ である．$B \neq I_n$ のときは，B の対角線上に 0 が登場するので $\det B = 0$ である．このことから，上の定理がわかる． □

行列式を手計算で計算する場合は，A を階段行列まで変形しなくても，上の掃き出し法の精神を生かしながら，あまり分数が登場しないように工夫しながら，上半三角行列になるところまで変形すればよい．

定理 11.4.(逆行列の計算) n 次正方行列 $A \in M_n(K)$ に対し，A と単位行列 I_n を並べてできる n 行 $2n$ 列の行列を (A, I_n) と書くことにする．(A, I_n) に掃き出し法を実行して得られた階段行列を (B, C) とする．ここで，B, C は n 次正方行列とする．A が可逆行列であるための必要十分条件は $B = I_n$ となることで，$B = I_n$ のとき $C = A^{-1}$ となる．

証明. 前定理のように A に掃き出し法を行って得られる階段行列は B と一致する．$B = I_n$ と $\det A \neq 0$ は同値であった．これは A が可逆であることと同値である．

$C = A^{-1}$ を証明する．ある可逆行列 $P \in M_n(K)$ により，$(B, C) = P(A, I_n)$ と書ける．行列の積の定義から，$B = PA, C = PI_n = P$ である．$B = I_n$ だから $P = A^{-1}$ であり，$C = A^{-1}$ がわかる． □

12. 連立方程式の解集合

K は体，$A \in M_{mn}(K)$ と $\mathbf{b} \in K^m$ は与えられた行列とベクトルで，$\mathbf{x} \in K^n$ は未知数を縦に並べた列ベクトルとし，連立方程式

$$A\mathbf{x} = \mathbf{b}$$

を解くことを考える．そもそも，$m < n$ や $m > n$ の場合も含めて考えているので，解は 1 通りとは限らず沢山あるかもしれないし，1 つもない (解なし) かもしれない．**解の集合**

$$W := \{\mathbf{x} \in K^n \mid A\mathbf{x} = \mathbf{b}\}$$

を $A\mathbf{x} = \mathbf{b}$ の**解集合**とか**解空間**という.「空間」という単語がついているが，3 次元の空間という意味ではない．この解集合の構造を述べるため，少し用語を導入しておく．

定義 12.1. K^n の部分集合 V が次の (1), (2) を満たすとき，V は K^n の**部分ベクトル空間**であるという．

(1) $\mathbf{x} \in V, \mathbf{y} \in V$ ならば $\mathbf{x} + \mathbf{y} \in V$.

(2) $\mathbf{x} \in V, a \in K$ ならば $a\mathbf{x} \in V$.

W が K^n の部分集合で，K^n のある部分ベクトル空間 V と，あるベクトル $\mathbf{c} \in K^n$ が存在して，

$$W = \{\mathbf{x} + \mathbf{c} \mid \mathbf{x} \in V\}$$

と書けるとき，W は**アフィン空間** (affine space) であるという．上の W を $W = V + \mathbf{c}$ とか $W = \mathbf{c} + V$ とも書き，V をベクトル $\mathbf{c}$ で**平行移動**して得られるアフィン空間であるという．

なお，$\mathbf{c} = \mathbf{0}$ の場合を考えれば，部分ベクトル空間はアフィン空間である．また，アフィン空間 W がゼロベクトル $\mathbf{0}$ を含めば，$\mathbf{c} = \mathbf{0}$ と選べるので，W は部分ベクトル空間になる．

また，
$$\operatorname{Ker} A := \{\mathbf{x} \in K^n \mid A\mathbf{x} = \mathbf{0}\}$$
という記号を導入し，$\operatorname{Ker} A$ を A の**カーネル** (kenel) とか**核**という．

命題 12.2. $A \in M_{mn}(K)$ に対し，$\operatorname{Ker} A$ は K^n の部分ベクトル空間である．$\mathbf{0} \in \operatorname{Ker} A$ なので，$\operatorname{Ker} A \neq \emptyset$ である．

証明. $\mathbf{x}, \mathbf{y} \in \operatorname{Ker} A$ ならば $A\mathbf{x} = \mathbf{0}$, $A\mathbf{y} = \mathbf{0}$ である．よって $A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y} = \mathbf{0} + \mathbf{0} = \mathbf{0}$ であり，$A(\mathbf{x}+\mathbf{y}) \in \operatorname{Ker} A$ となる．また，$a \in K$ ならば $A(a\mathbf{x}) = a(A\mathbf{x}) = a\mathbf{0} = \mathbf{0}$ となるので $a\mathbf{x} \in \operatorname{Ker} A$ である．$\operatorname{Ker} A$ は上の定義の (1), (2) を満たすので K^n の部分ベクトル空間である． □

命題 12.3. A, $\mathbf{x}$, $\mathbf{b}$ は本章の最初のほうで書いた通りとし，連立方程式 $A\mathbf{x} = \mathbf{b}$ の解の集合
$$W := \{\mathbf{x} \in K^n \mid A\mathbf{x} = \mathbf{b}\}$$
を考える．もし，W が空集合でなければ，随意に $\mathbf{x}_0 \in W$ を選ぶと，
$$W = \mathbf{x}_0 + (\operatorname{Ker} A)$$
となり，W はアフィン空間になる．$\mathbf{x}_0$ を $A\mathbf{x} = \mathbf{b}$ の**特殊解**と呼ぶことにすると，それに対して W の一般の元は**一般解**と呼ばれる．

証明. $W \neq \emptyset$ とし，$\mathbf{x}_0 \in W$ を固定する．
$$V := \{\mathbf{x} - \mathbf{x}_0 \mid \mathbf{x} \in W\}$$
とおく．$W = V - \mathbf{x}_0$, $V = W + \mathbf{x}_0$ である．$\mathbf{y} \in V$ を取ると，ある $\mathbf{x} \in W$ により，$\mathbf{y} = \mathbf{x} - \mathbf{x}_0$ と書ける．
$$A\mathbf{y} = A(\mathbf{x} - \mathbf{x}_0) = A\mathbf{x} - A\mathbf{x}_0 = \mathbf{b} - \mathbf{b} = \mathbf{0}$$
である．よって，$V \subset \operatorname{Ker} A$ である．逆に $\mathbf{z} \in \operatorname{Ker} A$ とする．$A\mathbf{z} = \mathbf{0}$ であるので，$\mathbf{x} := \mathbf{z} + \mathbf{x}_0$ とおくと，$A\mathbf{x} := A\mathbf{z} + A\mathbf{x}_0 = \mathbf{0} + \mathbf{b} = \mathbf{b}$ となる．よって，$\mathbf{x} \in W$ である．$\mathbf{z} = \mathbf{x} - \mathbf{x}_0$ なので $\mathbf{z} \in V$ である．したがって，$\operatorname{Ker} A \subset V$ である．$\operatorname{Ker} A \supset V$ かつ $\operatorname{Ker} A \subset V$ なので $\operatorname{Ker} A = V$ である．前命題より V は K^n の部分ベクトル空間なので，$W = V + \mathbf{x}_0$ はアフィン空間である． □

定義 12.4. 行列 $A \in M_{mn}(K)$ の階段行列を B とする．B のゼロベクトルでない行ベクトルの個数が $\operatorname{rank} B$ であった．B は A から一意的に定まるから，$\operatorname{rank} A := \operatorname{rank} B$ として A の**ランク** (または**階数**) を定義する．

命題 12.5. m 行 n 列の行列 $A \in M_{mn}(K)$ に対して，$\operatorname{rank} A \leqq m$ かつ $\operatorname{rank} A \leqq n$ である．

証明. A の階段行列を B とする．$\operatorname{rank} A$ は B のゼロベクトルでない行の個数なので，$\operatorname{rank} A \leqq m$ である．また，$r = \operatorname{rank} B = \operatorname{rank} A$ のとき，B の列ベクトルの中には基本ベクトル $\mathbf{e}_1, \ldots, \mathbf{e}_r$ が含まれるので，$r \leqq n$ である． □

定理 12.6. n 次正方行列 $A \in M_n(K)$ に対し，A が可逆行列であるための必要十分条件は $\operatorname{rank} A = n$ が成り立つことである．

証明. B を A の階段行列とする．定理 11.3 より，A^{-1} が存在することと $\det A \neq 0$ と $B = I_n$ は同値であった．また $\operatorname{rank} I_n = n$ である．逆に $\operatorname{rank} B = n$ となるような n 次正方階段行列は $B = I_n$ しかない． □

次は連立方程式 $A\mathbf{x} = \mathbf{b}$ の解法の説明の前半部分である．記号の設定を定理の中で書くと長くて定理が読みづらくなるので，ここに書く．A の階段行列を $B = (b_{i,j}) = (\mathbf{b}_1 \ldots, \mathbf{b}_n) \in M_{mn}(K)$ とする．$r = \operatorname{rank} B = \operatorname{rank} A$ とし，定義 10.4 のような $1 \leqq s_1 < s_2 < \cdots < s_r \leqq n$ を選び，$\mathbf{b}_{s_i} = \mathbf{e}_i$ $(1 \leqq \forall i \leqq r)$, $j < s_1$ ならば $\mathbf{b}_j = \mathbf{0}$, $s_k < j < s_{k+1}$ (形式的に $s_{r+1} = n+1$ とおく) ならば，$\mathbf{b}_j = \displaystyle\sum_{i=1}^{k} b_{i,j}\mathbf{e}_i$ であるとする．また，$\mathbf{c} \in K^m$ が登場したとき，その i 行目の成分を c_i とする．$x_{s_i} := c_i$

$(1 \leqq \forall i \leqq r)$ で，$i \in \{1, \ldots, m\} - \{s_1, \ldots, s_r\}$ のとき $x_i := 0$ として定めた x_i を i 行目の成分とする列ベクトルを $\mathbf{x}_0 \in K^n$ とおく．例えば，定義 10.4 のところで例示した B については，

$$\mathbf{x}_0 = \begin{pmatrix} 0 \\ c_1 \\ 0 \\ c_2 \\ 0 \\ 0 \\ c_3 \\ c_4 \\ 0 \end{pmatrix}, \quad B\mathbf{x}_0 = \begin{pmatrix} 0 & 1 & b_{13} & 0 & b_{15} & b_{16} & 0 & 0 & b_{19} \\ 0 & 0 & 0 & 1 & b_{25} & b_{26} & 0 & 0 & b_{29} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & b_{39} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & b_{49} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ c_1 \\ 0 \\ c_2 \\ 0 \\ 0 \\ c_3 \\ c_4 \\ 0 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ 0 \end{pmatrix}$$

である．

定理 12.7. (連立方程式の特殊解) $A \in M_{mn}(K)$, $\mathbf{b} \in K^m$ で $\mathbf{x} \in K^n$ は未知数を縦に並べた列ベクトルとする．$(A, \mathbf{b})$ は A と $\mathbf{b}$ を並べて書いた m 行 $(n+1)$ 列行列とする．また，$(A, \mathbf{b})$ の階段行列を $(B, \mathbf{c})$ とする．ただし，$B \in M_{mn}(K)$, $\mathbf{c} \in K^m$ とする．それ以外の設定は定理の直前の通りとする．このとき，以下が成り立つ．

(1) $A\mathbf{x} = \mathbf{b}$ と $B\mathbf{x} = \mathbf{c}$ は同値である．
(2) $\operatorname{rank} A \leqq \operatorname{rank}(A, \mathbf{b})$ である．
(3) $r = \operatorname{rank} B = \operatorname{rank} A$ とするとき，すべての $r < i \leqq m$ に対して $c_i = 0$ が成り立つならば，$A\mathbf{x}_0 = \mathbf{b}$ が成り立つ．つまり，$\mathbf{x}_0$ は $A\mathbf{x} = \mathbf{b}$ の**特殊解**である．
(4) 連立方程式 $A\mathbf{x} = \mathbf{b}$ が解を持つための必要十分条件は

$$\operatorname{rank} A = \operatorname{rank}(A, \mathbf{b})$$

が成り立つことである．逆に，$A\mathbf{x} = \mathbf{b}$ が「解なし」になる必要十分条件は $\operatorname{rank} A < \operatorname{rank}(A, \mathbf{b})$ である．

証明. (1) ある可逆行列 $P \in M_m(K)$ により $(B, \mathbf{c}) = P(A, \mathbf{b})$ と書ける．$B = PA$, $\mathbf{c} = P\mathbf{b}$ である．$A\mathbf{x} = \mathbf{b}$ のとき $B\mathbf{x} = PA\mathbf{x} = P\mathbf{b} = \mathbf{c}$ である．逆に $B\mathbf{x} = \mathbf{c}$ のとき $A\mathbf{x} = P^{-1}B\mathbf{x} = P^{-1}\mathbf{c} = \mathbf{b}$ である．

(2) B は A の階段行列である．階段行列のランクはゼロベクトルでない行の個数だから，$\operatorname{rank} B \leqq \operatorname{rank}(B, \mathbf{c})$ である．よって，$\operatorname{rank} A \leqq \operatorname{rank}(A, \mathbf{b})$ である．

(3) $B\mathbf{x}_0 = \mathbf{c}$ は自明な等式である．例えば，定理の直前の例で確認してほしい．(2) の結果から $A\mathbf{x}_0 = \mathbf{b}$ である．

(4) $r = \operatorname{rank} A = \operatorname{rank}(A, \mathbf{b})$ ならば $r = \operatorname{rank} B = \operatorname{rank}(B, \mathbf{c})$ なので，すべての $r < i \leqq m$ に対して $c_i = 0$ である．(3) より $A\mathbf{x}_0 = \mathbf{b}$ で解を持つ．

$r := \operatorname{rank} A \neq \operatorname{rank}(A, \mathbf{b})$ ならば，(1) より $\operatorname{rank} B < \operatorname{rank}(B, \mathbf{c})$ となる．これは，$c_{r+1} \neq 0$ を意味する．B の $(r+1)$ 行目はゼロベクトルなので，$B\mathbf{x} = \mathbf{c}$ の $(r+1)$ 行目の等式は $0 = c_{r+1}$ となり，矛盾する． □

13. Ker A

K は体，$A \in M_{mn}(K)$ と $\mathbf{b} \in K^m$ は与えられた行列とベクトルで，$\mathbf{x} \in K^n$ は未知数を縦に並べた列ベクトルとし，連立方程式

$$A\mathbf{x} = \mathbf{b}$$

の解が存在するための条件と，存在した場合の特殊解 $\mathbf{x} = \mathbf{x}_0$ の求め方を前章で解説した．$A\mathbf{x} = \mathbf{b}$ の解集合は $\mathbf{x}_0 + \operatorname{Ker} A$ であった．そこで，本章では $\operatorname{Ker} A$ を決定する方法について考察する．まず，定理 12.7(1) より，次の命題が成り立つ．

命題 13.1. 記号は上の通りとし，行列 A の階段行列を B とする．すると，

$$\operatorname{Ker} A = \operatorname{Ker} B$$

である．(これは，集合として等しいという意味である.)

したがって，$A\mathbf{x}=\mathbf{0}$ を解くには，A の階段行列 B について $B\mathbf{x}=0$ の解をすべて求めればよい．定義 10.4 のように B の記号を設定する．

$B=(b_{i,j})=(\mathbf{b}_1 ..., \mathbf{b}_n)\in M_{mn}(K)$, $r=\operatorname{rank}B=\operatorname{rank}A$ とし，定義 10.4 のような $1\leqq s_1<s_2<\cdots<s_r\leqq n$ を選び，$\mathbf{b}_{s_i}=\mathbf{e}_i$ $(1\leqq\forall i\leqq r)$, $j<s_1$ ならば $\mathbf{b}_j=\mathbf{0}$, $s_k<j<s_{k+1}$ (形式的に $s_{r+1}=n+1$ とおく) ならば，$\mathbf{b}_j=\displaystyle\sum_{i=1}^{k}b_{i,j}\mathbf{e}_i$ であるとする．$N:=\{1, 2,..., n\}$ における $S:=\{s_1, s_2,..., s_r\}$ の補集合を $T=\{t_1, t_2,..., t_{n-r}\}:=N-S$ とする．ただし，$1\leqq t_1<t_2<\cdots<t_{n-r}\leqq n$ と並べておく．各 $t\in T$ に対して，ベクトル $\mathbf{x}_t=\begin{pmatrix}x_{1,t}\\ \vdots\\ x_{n,t}\end{pmatrix}$ を以下の (1), (2), (3) のように定める．

(1) $x_{t,t}:=1$

(2) $i\in S$ ならば，$x_{i,t}:=-b_{i,t}$ とおく．ただし，$i>t$ のときは階段行列の定義から $x_{i,t}=-b_{i,t}=0$ である．

(3) $i\neq t$ かつ $i\notin S$ ならば，$x_{i,t}:=0$

このとき，次の定理が成り立つ．

定理 13.2. 記号は直前の説明のとおりとする．

(1) もし $r=n$ ならば，$A\mathbf{x}=\mathbf{0}$ の解は，$\mathbf{x}=\mathbf{0}$ 以外に存在しない．

(2) $r<n$ の場合，各 $t\in\{t_1,..., t_{n-r}\}$ に対し，$c_t\in K$ を自由変数 (任意の値を取れる変数) とし，

$$\mathbf{x}=\sum_{t\in T}c_t\mathbf{x}_t$$

とおくと，$A\mathbf{x}=\mathbf{0}$ であり，

$$\operatorname{Ker}A=\left\{\sum_{t\in T}c_t\mathbf{x}_t\;\middle|\;c_t\in K\ (\forall t\in T)\right\}$$

である．

証明. (1) $r=n$ のときは，$B\mathbf{x}=\mathbf{0}$ の第 i 行目は $x_i=0$ という方程式になっている．i は $1\leqq i\leqq r=n$ の範囲を動くので，$\mathbf{x}=\mathbf{0}$ である．

(2) c_t を x_t と書き直すと，

$$B\mathbf{x}=\mathbf{x}-\sum_{t\in T}x_t\mathbf{x}_t$$

となる．これより，結論が得られる． □

例えば，定義 10.4 のところで例示した B については，

$$B\mathbf{x}=\begin{pmatrix}0&1&b_{13}&0&b_{15}&b_{16}&0&0&b_{19}\\0&0&0&1&b_{25}&b_{26}&0&0&b_{29}\\0&0&0&0&0&0&1&0&b_{39}\\0&0&0&0&0&0&0&1&b_{49}\\0&0&0&0&0&0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\ \vdots\\x_9\end{pmatrix}=\begin{pmatrix}0\\0\\ \vdots\\0\end{pmatrix}$$

の解は，$S=\{2, 4, 7, 8\}$, $T=\{1, 3, 5, 6, 9\}$ なので，

$$\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=c_1\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}+c_3\begin{pmatrix}0\\-b_{13}\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}+c_5\begin{pmatrix}0\\-b_{15}\\0\\-b_{25}\\1\\0\\0\\0\\0\end{pmatrix}+c_6\begin{pmatrix}0\\-b_{16}\\0\\-b_{26}\\0\\1\\0\\0\\0\end{pmatrix}+c_9\begin{pmatrix}0\\-b_{19}\\0\\-b_{29}\\0\\0\\-b_{39}\\-b_{49}\\1\end{pmatrix}\qquad\begin{pmatrix}t_1\text{行目}\\s_1\text{行目}\\t_2\text{行目}\\s_2\text{行目}\\t_3\text{行目}\\t_4\text{行目}\\s_3\text{行目}\\s_4\text{行目}\\t_6\text{行目}\end{pmatrix}$$

(c_1, c_3, c_5, c_6, c_9 は勝手な K の元) である．

一般のベクトル空間における 1 次独立の概念は「線形代数学 B2」で学習するが，ここでは最低限必要な数ベクトルの 1 次独立の話をしておく．

定義 13.3.(1 次独立) K は体とし，$\mathbf{x}_1,\ldots,\mathbf{x}_m \in K^n$ とする．あるスカラー $a_1,\ldots,a_m \in K$ で
(1) $a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_m\mathbf{x}_m = \mathbf{0}$
(2) $a_1, a_2,\ldots, a_m$ の中に 0 でないものが，少なくとも 1 つは存在する．
を満たすとき，$\mathbf{x}_1, \mathbf{x}_2,\ldots, \mathbf{x}_m$ は (K 上)**1 次従属**であるとか**線形従属**であるという．(1) を $\mathbf{x}_1,\ldots,\mathbf{x}_m$ の間の**線形関係**という．$\mathbf{x}_1, \mathbf{x}_2,\ldots, \mathbf{x}_m$ が 1 次従属でないとき，$\mathbf{x}_1, \mathbf{x}_2,\ldots, \mathbf{x}_m$ は (K 上)**1 次独立**であるとか**線形独立**であるという．言い換えると，(1) を満たす $a_1,\ldots, a_m \in K$ が $a_1 = \cdots = a_m = 0$ 以外に存在しないとき，$\mathbf{x}_1, \mathbf{x}_2,\ldots, \mathbf{x}_m$ は 1 次独立である．

定理 13.4. 定理 13.2 において $\mathrm{Ker}\,A$ に属するベクトル $\mathbf{x}_{t_1}, \mathbf{x}_{t_2}, \ldots, \mathbf{x}_{t_{n-r}}$ は 1 次独立である．

証明. $a_1\mathbf{x}_{t_1} + a_2\mathbf{x}_{t_2} + \cdots + a_{n-1}\mathbf{x}_{t_{n-r}} = \mathbf{0}$— ① ($a_1, a_2,\ldots, a_{n-r} \in K$) であるとする．① の両辺の t_i 行目 ($1 \leqq i \leqq n-r$) の成分を比較する．$\mathbf{x}_{t_j}$ の t_i 行目の成分は $j = i$ のとき 1 で，$j \neq i$ のとき 0 である．よって，① の左辺のベクトルの和の t_i 行目は a_i である．これが，① の右辺の t_i 行目の 0 に等しいから，$a_i = 0$ ($0 \leqq \forall i \leqq n-r$) である．よって，$\mathbf{x}_{t_1},\ldots, \mathbf{x}_{t_{n-r}}$ は 1 次独立である． □

上の定理は，

$$\mathrm{Ker}\,A = \left\{ \sum_{t\in T} c_t\mathbf{x}_t \;\middle|\; c_t \in K\ (\forall t \in T) \right\}$$

という解空間の表わし方において，$\mathbf{x}_t$ 達の中のどれも取り除けないことを意味している．

定理 13.5. K は体，$\mathbf{x}_1,\ldots, \mathbf{x}_m \in K^n$ は 1 次独立であると仮定する．$a_1,\ldots, a_m, b_1,\ldots, b_m \in K$,

$$a_1\mathbf{x}_1 + \cdots + a_m\mathbf{x}_m = b_1\mathbf{x}_1 + \cdots + b_m\mathbf{x}_n$$

ならば，$a_1 = b_1,\ldots, a_m = b_m$ である．

証明. $(a_1 - b_1)\mathbf{x}_1 + \cdots + (a_m - b_m)\mathbf{x}_n = \mathbf{0}$ だから，1 次独立の定義から $a_1 - b_1 = 0,\ldots, a_m - b_m = 0$ となる． □

定理 13.6. K は体，$\mathbf{x}_1,\ldots, \mathbf{x}_m \in K^n$ とする．一般に，この m 個の列ベクトル $\mathbf{x}_1,\ldots, \mathbf{x}_m$ を左から右に並べてできる n 行 m 列の行列を $(\mathbf{x}_1,\ldots, \mathbf{x}_m)$ と書く．今，$A = (\mathbf{x}_1,\ldots, \mathbf{x}_m)$ とする．
(1) $\mathbf{x}_1,\ldots, \mathbf{x}_m$ が 1 次独立であるための必要十分条件は $\mathrm{rank}\,A = m$ が成り立つことである．
(2) 特に $m = n$ の場合には，$\mathbf{x}_1,\ldots, \mathbf{x}_n$ が 1 次独立であるための必要十分条件は $\det A \neq 0$ が成り立つことである．これは，A の逆行列 A^{-1} が存在することと同値である．

証明. (1-1) 定理 11.2 より，ある可逆な m 次正方行列 P により $B = PA$ と書ける．また，階段行列 $B = (b_{i,j}) \in M_{mn}(K)$ は以下の条件を満たす．
(i) $1 \leqq r \leqq m$ を満たす自然数 r と，$1 \leqq s_1 < s_2 < \cdots < s_r \leqq n$ を満たす自然数 $s_1, s_2,\ldots, s_r$ が存在し，$\mathbf{b}_{s_1} = \mathbf{e}_1, \mathbf{b}_{s_2} = \mathbf{e}_2, \ldots, \mathbf{b}_{s_r} = \mathbf{e}_r$ である．
(ii) $j < s_1$ ならば $\mathbf{b}_j = \mathbf{0}$ である．
(iii) $1 \leqq k < r$ で $s_k < j < s_{k+1}$ ならば，$i > k$ のとき $b_{i,j} = 0$ である．つまり，$\mathbf{b}_j = \displaystyle\sum_{i=1}^{k} b_{i,j}\mathbf{e}_i$ である．
(iv) $j > s_r$ ならば，$i > s_r$ のとき $b_{i,j} = 0$ である．

(1-2) したがって，$r = \mathrm{rank}\,B = \mathrm{rank}\,A = m$ ならば，$s_1 = 1, s_2 = 2,\ldots, s_m = m$ で，$\mathbf{b}_1 = \mathbf{e}_1$, $\mathbf{b}_2 = \mathbf{e}_2, \ldots, \mathbf{b}_m = \mathbf{e}_m$ である．$a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m = \mathbf{0}$ ($a_1,\ldots, a_m \in K$) とすると，$\mathbf{e}_i = \mathbf{b}_i = P\mathbf{x}_i$ だから，$a_1\mathbf{e}_1 + \cdots + a_m\mathbf{e}_m = P(a_1\mathbf{x}_1 + \cdots + a_m\mathbf{x}_m) = P\mathbf{0} = \mathbf{0}$ なので，$a_1 = \cdots = a_m = 0$ となる．よって，$\mathbf{x}_1,\ldots, \mathbf{x}_m$ は 1 次独立である．

(1-3) 逆に，$\mathbf{x}_1,\ldots,\mathbf{x}_m$ は 1 次独立であると仮定する．$a_1\mathbf{b}_1+\cdots+a_m\mathbf{b}_m=\mathbf{0}$ $(a_1,\ldots,a_m\in K)$ とすると，$\mathbf{x}_i=P^{-1}\mathbf{x}_i$ だから，$a_1\mathbf{x}_1+\cdots+a_m\mathbf{x}_m=P^{-1}(a_1\mathbf{b}_1+\cdots+a_m\mathbf{b}_m)=\mathbf{0}$ なので，$a_1=\cdots+a_m=0$ となる．よって，$\mathbf{b}_1,\ldots,\mathbf{b}_m$ は 1 次独立である．このとき，$\mathbf{b}_i=\mathbf{e}_i$ $(1\leqq\forall i\leqq m)$ であることを i に関する帰納法で示す．$\mathbf{b}_1\neq\mathbf{0}$ と (ii) より $s_1=1$ で，(i) より $\mathbf{b}_1=\mathbf{e}_1$ である．

$2\leqq i\leqq m$ とし，$1\leqq j<i$ のとき $\mathbf{b}_j=\mathbf{e}_j$ と仮定する．もし $s_i>i$ とすると，(iii) より $\mathbf{b}_1,\ldots,\mathbf{b}_i$ は 1 次従属になってしまう．よって，$s_i=i$ で (i) より $\mathbf{b}_i=\mathbf{e}_i$ である．

以上より，$\operatorname{rank}A=\operatorname{rank}B=m$ である．

(2) $\mathbf{x}_1,\ldots,\mathbf{x}_n$ が 1 次独立ならば，上の議論から，B は単位行列 I になる．このとき $PA=B=I$ だから P は A の逆行列である．

逆に，A^{-1} が存在すると仮定する．$A^{-1}A=I$ だから $A^{-1}\mathbf{x}_i=\mathbf{e}_i$ である．$a_1,\ldots,a_n\in K$, $a_1\mathbf{x}_1+\cdots+a_n\mathbf{x}_n=\mathbf{0}$ が成り立つとする．

$$\mathbf{0}=A^{-1}\big(a_1\mathbf{x}_1+\cdots+a_n\mathbf{x}_n\big)=a_1A^{-1}\mathbf{x}_1+\cdots+a_nA^{-1}\mathbf{x}_n=a_1\mathbf{e}_1+\cdots+a_n\mathbf{e}_n$$

で，$\mathbf{e}_1,\ldots,\mathbf{e}_n$ は 1 次独立だから，$a_1=\cdots=a_n=0$ となる．よって $\mathbf{x}_1,\ldots,\mathbf{x}_n$ は 1 次独立である． □

14. 解空間の次元

定義 14.1. K は体とし，$\mathbf{x}_1,\ldots,\mathbf{x}_m\in K^n$ とする．

$$V:=\left\{\sum_{i=1}^m a_i\mathbf{x}_i\;\middle|\;a_1,\ldots,a_m\in K\right\}$$

とおく．すると V は K^n の部分空間になる．この V を $K\mathbf{x}_1+\cdots+K\mathbf{x}_m$ とか $\displaystyle\sum_{i=1}^m K\mathbf{x}_i$ とか $\langle\mathbf{x}_1,\ldots,\mathbf{x}_m\rangle$ と書き，$\mathbf{x}_1,\ldots,\mathbf{x}_m$ によって**生成される** V の部分空間という．また，組 (集合) $\mathbf{x}_1,\ldots,\mathbf{x}_m$ は V の**生成系**であるとか，**生成元**であるという．

$\mathbf{x}_1,\ldots,\mathbf{x}_m\in V$ が 1 次独立であって，かつ，V の生成系であるとき，組 (集合) $\mathbf{x}_1,\ldots,\mathbf{x}_m$ は V の (K 上の) **基底** (base) であるという．

例 14.2. $V=K^n$ の場合には，基本ベクトルを $\mathbf{e}_1:=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$, $\mathbf{e}_2:=\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}$,$\ldots$, $\mathbf{e}_n:=\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}$ とおくと，$\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_n$ は K^n の基底になる．これを K^n の**標準基底**という．

定理 14.3. K は体，$\mathbf{x}_1,\ldots,\mathbf{x}_m\in K^n$ とする．$A=(\mathbf{x}_1,\ldots,\mathbf{x}_m)$ とする．$r=\operatorname{rank}A$ とし，A から作られる階段行列を B とする．B の j 列目の列ベクトルを $\mathbf{b}_j$ とする．$\operatorname{rank}B=r$ だから，B の列ベクトルの中に基本ベクトル $\mathbf{e}_1,\ldots,\mathbf{e}_r$ が現れるが，いま $\mathbf{b}_{s_1}=\mathbf{e}_1,\ldots,\mathbf{b}_{s_r}=\mathbf{e}_r$ であるとする．このとき，以下が成り立つ．

(1) A の列の列ベクトル $\mathbf{x}_{s_1},\ldots,\mathbf{x}_{s_r}$ は 1 次独立である．

(2) B の (i,j)-成分を b_{ij} とするとき，

$$\mathbf{x}_k=b_{1,k}\mathbf{x}_{s_1}+\cdots+b_{r,k}\mathbf{x}_{s_r}$$

が成り立つ．

(3) $\mathbf{x}_{s_1},\ldots,\mathbf{x}_{s_r}$ は $\operatorname{Im}A$ の基底である

証明. ある可逆行列 $P\in M_m(K)$ により，$B=PA$ と書けるすると，$\mathbf{b}_j=P\mathbf{x}_j$, $\mathbf{x}_j=P^{-1}\mathbf{b}_j$ $(j=1,\ldots,m)$ である．

(1) $\mathbf{x}_{s_1},\ldots,\mathbf{x}_{s_r}$ が 1 次独立であることを示す．

$a_1,\ldots, a_r \in K$, $a_1\mathbf{x}_{s_1} + \cdots + a_r\mathbf{x}_{s_r} = \mathbf{0}$ であるとする．P を左から書けると，

$$\mathbf{0} = P\big(a_1\mathbf{x}_{s_1}+\cdots+a_r\mathbf{x}_{s_r}\big) = a_1P\mathbf{x}_{s_1}+\cdots+a_rP\mathbf{x}_{s_r} = a_1\mathbf{b}_{s_1}+\cdots+a_r\mathbf{b}_{s_r} = a_1\mathbf{e}_1+\cdots+a_r\mathbf{e}_r = \begin{pmatrix} a_1 \\ \vdots \\ a_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

となる．よって，$a_1 = \cdots = a_r = 0$ となり，$\mathbf{x}_{s_1},\ldots, \mathbf{x}_{s_r}$ は 1 次独立である．

(2) $\mathbf{x}_k = b_{1,k}\mathbf{x}_{s_1} + \cdots + b_{r,k}\mathbf{x}_{s_r}$ を証明する．

$$\mathbf{b}_k = \begin{pmatrix} b_{1,k} \\ \vdots \\ b_{r,k} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = b_{1,k}\mathbf{e}_1 + \cdots + b_{r,k}\mathbf{e}_r = b_{1,k}\mathbf{b}_{s_1} + \cdots + b_{r,k}\mathbf{b}_{s_r}$$

である．左から P^{-1} を掛けると，

$$\mathbf{x}_k = P^{-1}\mathbf{b}_k = b_{1,k}P^{-1}\mathbf{b}_{s_1} + \cdots + b_{r,k}P^{-1}\mathbf{b}_{s_r} = b_{1,k}\mathbf{x}_{s_1} + \cdots + b_{r,k}\mathbf{x}_{s_r}$$

となる．

(3) 定義から，$\operatorname{Im} A$ は $\mathbf{x}_1,\ldots, \mathbf{x}_m$ で生成される．(2) より，$\mathbf{x}_{s_1},\ldots, \mathbf{x}_{s_r}$ は $\operatorname{Im} A$ の生成系である．(1) とあわせると (3) を得る． □

定理 14.4. $\mathbf{x}_1,\ldots, \mathbf{x}_r \in K^r$ は 1 次独立で，$\mathbf{y}_1,\ldots, \mathbf{y}_s \in K^r$ も 1 次独立と仮定する．さらに，

$$K\mathbf{x}_1 + \cdots + K\mathbf{x}_r = K\mathbf{y}_1 + \cdots + K\mathbf{y}_s$$

が成立すると仮定すると，$r = s$ である．

証明. $r \neq s$ と仮定して矛盾を導く．議論は対称だから $r < s$ と仮定してよい．$K\mathbf{x}_1 + \cdots + K\mathbf{x}_r = K\mathbf{y}_1 + \cdots + K\mathbf{y}_s$ より，$\mathbf{y}_j = \displaystyle\sum_{i=1}^{r} a_{ij}\mathbf{x}_i$ を満たす $a_{ij} \in K$ が存在する $(1 \leqq \forall j \leqq s)$．$a_{ij}$ を (i, j)-成分とする r 行 s 列の行列 $A = (a_{ij}) \in M_{rs}(K)$ を作る．$b_1\mathbf{y}_1 + \cdots + b_s\mathbf{y}_s = \mathbf{0}$ を満たす $b_1,\ldots, b_s \in K$ を考える．

$$\mathbf{0} = \sum_{j=1}^{s} b_j\mathbf{y}_j = \sum_{j=1}^{s} b_j \left(\sum_{i=1}^{r} a_{ij}\mathbf{x}_i\right) = \sum_{i=1}^{r} \left(\sum_{j=1}^{s} a_{ij}b_j\right) \mathbf{x}_i$$

であるが，$\mathbf{x}_1,\ldots, \mathbf{x}_r \in K^r$ は 1 次独立なので，$\displaystyle\sum_{j=1}^{s} a_{ij}b_j = 0$ が各 $i = 1,\ldots, r$ に対して成り立つ．これを行列とベクトルで表すと，$\mathbf{b} := \begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix}$ として，$A\mathbf{b} = \mathbf{0}$ と書ける．A の階段行列は r 個以下の行しか持たないから，$\operatorname{rank} A \leqq r$ である．$s > r$ だから，$A\mathbf{b} = \mathbf{0}$, $\mathbf{b} \neq \mathbf{0}$ を満たす $\mathbf{b} \in K^s$ が存在する．このとき，$b_1\mathbf{y}_1 + \cdots + b_s\mathbf{y}_s = \mathbf{0}$ という等式は，$\mathbf{y}_1,\ldots, \mathbf{y}_s \in K^r$ が 1 次独立でないことを表わし，矛盾する． □

定義 14.5. K は体，V は K^n の部分ベクトル空間とする．V が m のベクトルからなる基底 $\mathbf{x}_1,\ldots, \mathbf{x}_m$ を持つとき，m を V の**次元**といい，$\dim V = m$ とか $\dim_K V = m$ と書く．また，ある $\mathbf{x}_0 \in K^n$ によって $W = V + \mathbf{x}_0$ と書けるアフィン空間 W に対しては，$\dim W := \dim V$ として W の次元を定義する．

定理 14.6. K は体，$A \in M_{mn}(K)$, $\operatorname{rank} A = r$ とすると，以下が成り立つ．

(1) $\dim(\operatorname{Im} A) = r$
(2) $\dim(\operatorname{Ker} A) = n - r$

証明. (1) は定理 14.3 からわかる．
(2) は定理 13.2 と定理 13.4 からわかる． □

定理 14.7. K は体，V は K^n の部分ベクトル空間とする．また，$\mathbf{x}_1,\ldots,\mathbf{x}_m \in V$ とする．これらの列ベクトルを並べてできる行列を $A = (\mathbf{x}_1,\ldots,\mathbf{x}_m)$ とする．このとき，$\mathbf{x}_1,\ldots,\mathbf{x}_m$ が V の生成系であるための必要十分条件は，$\operatorname{rank} A = \dim V$ が成り立つことである．特に，$m = \operatorname{rank} A = \dim V$ ならば，$\mathbf{x}_1,\ldots,\mathbf{x}_m$ は V の基底である．

証明. $\mathbf{x}_1,\ldots,\mathbf{x}_m$ で生成される K^n の部分ベクトル空間を W とする．$W \subset V$ である．$A = (\mathbf{x}_1,\ldots,\mathbf{x}_m)$, $r = \operatorname{rank} A$ とし，A から作られる階段行列を B とする．$\mathbf{b}_{s_1} = \mathbf{e}_1,\ldots,\mathbf{b}_{s_r} = \mathbf{e}_r$ であるとすると，$\mathbf{x}_{s_1},\ldots,\mathbf{x}_{s_r}$ は 1 次独立である．$\mathbf{x}_k = b_{1,k}\mathbf{x}_{s_1} + \cdots + b_{r,k}\mathbf{x}_{s_r}$ が成り立つから，$\mathbf{x}_{s_1},\ldots,\mathbf{x}_{s_r}$ は W の基底である．特に，$\dim W = r$ である．
(1) $\mathbf{x}_1,\ldots,\mathbf{x}_m$ が V の生成系ならば，$W = V$ であるから，$\dim V = r = \operatorname{rank} A$ である．
(2) 逆に，$\dim V = \operatorname{rank} A$ ならは，$W = V$ となるから，$\mathbf{x}_{s_1},\ldots,\mathbf{x}_{s_r}$ は V の基底である．よって，$\mathbf{x}_1,\ldots,\mathbf{x}_m$ は V の生成系である． □