

線形代数学 講義ノート

はじめに

これは大学初年度級に相当する線形代数学の講義内容をまとめたものである。本論は、簡単な計算演習はある程度こなせるものの、線形代数学で扱う数学的諸概念の意義が分からずに苦しんでいる者を主な対象としている。ゆえに天下りの定義はなるべく控え、その概念を与える理由について出来る限り説明するよう心がけた。また、普段であれば講義において口頭で説明すれば十分であり、一般の参考書等には記述されないような事実についても、あえて述べている。したがって、全体にわたって非常に冗長な内容となっており、それは、枝葉末節を切り捨て簡潔な記述を好む数学の美意識を貶めるものである。しかしながら初学者の理解を優先する立場から、あえてこのような記述を試みた。

なお、本論は理論的見地から述べたものであり、講義で行う計算演習については殆ど触れていない。また本論は各概念の意義について焦点を当てるが、それらの意味の理解のための説明は標準的な参考書のそれと変わらない。計算演習のために多くの例題を必要とする者、あるいは定義や定理の意味それ自体が不明な者は、それらの用途に特化した参考書を各自に参照すること。もちろん、後者については講義中に質問してもらっても構わない。

本論が学習の一助になれば幸いである。

担当: 嶺 幸太郎

1 線形代数学とは何か

始めに、線形代数学とはどんな理論であり、学問全体の中でどういう位置を占めているかについて簡単に述べておきたい。そのためには次の二つの視点から眺めるのがよいように思う。一つは大学教育における線形代数の役割について、もう一つは数学の諸分野の中での線形代数の占める位置である。前者については線形代数に限らず、まず、大学における数学教育の役割を述べる。また後者を論じる前提として、数学の分野がどのように大別されているか説明する。すなわち、線形代数という言葉はいったん忘れて、まずはこれらの大枠について俯瞰する。

1.1 大学で学ぶということ

大学で学ぶとはどういう事か考えると、そもそも大学とは何かという「大学論」を避けては通れない。すなわち、大学の歴史やその存在意義について問わねばならなくなる。ただ、この手の話はあまり風呂敷を広げすぎると收拾がつかなくなり、線形代数学の講義の中で述べるには適切ではない。そこで、ここでは中世・近代における西洋の大学とはどんなものであったかを少しだけ説明しておこう。もちろん、明治に作られた我が国の大学の元々の理念は西洋の知識を効率的に吸収し富国強兵を担う国家のための人材を提供することにあり、したがって西洋のそれとは事情が異なっている。しなしながら、我が国の大学も西洋の大学に多くを手本としたことは事実であるから、近代以前の大学について考えることは無意味ではない。なお、この辺りのくい違いが、我が国における大学論を複雑にしているようである。

では、中世における大学とは何を学ぶ場所であったのだろうか。それは高度知識人になるための教養を学ぶ場であった。ここでいう教養とは何かという問いはこれまた難しいのだが、簡単にまとめれば、物事をきちんと把握し、適切な判断を下すことのできる能力のことである。したがって教養とは広い知識だけを指すのではなく、それを活用する能力のことも含んでいる。そして、大学で教養を身につけたのちに、専門職教育機関(大学院¹)にて専門課程について学び、それぞれの職業に就くのであった。教養が必要とされる専門職は当初は神学・法学・医学に関するものが主であった。のちに社会が専門化・多様化したことにより、様々な職業において高度な知識人が求められるようになり、教養を必要とする者の多くが大学に足を運んだのである。大学とは、どのような職に就くにせよ必要となる学力を身につける場であると見なされていた。

なお、当時の教養教育はリベラル・アーツ(自由七科)と呼ばれ、これはギリシャのプラトンまでさかのぼる思想である。自由というのは、偏見なく自らの判断で物事を見定めることができるという意味が込められている。また、七科とは具体的な学科のことであり、言語に関わる三学(文法・論理・修辞)と数理に関わる四科(算術・幾何・天文・音楽)を指す。これらの知識を身につけていることが当時の知識人のあいだの常識であった。

1.2 数学教育とパッケージ化

もう既にお気付きの方も多いかと思われるが、大学の初年度における数学教育の役割は上述の教養教育の役割とかなり似ている。これは、自由七科のうち半分は数学的な学科であり、数学教育の歴史は古くから重要視されており、そして現在もそうあるべきであるといったセンチメンタルな話ではない。現代の自然科学の多くは数学を用いて表現されるため、サイエンスの言語としてまず学ばねばならない学科であり、つまり、どの専門学科に進むにせよ学ぶべきものという意味において似ているのである。もちろん、将来専攻する分野ではあまり数式は出てこないという人もいるだろう。それでも実験やアンケート調査を行えば、それらの結果にどの程度の信憑性があるかを知るには統計学の知識が必要となるだろうし、こんにちの情報化社会においてはそうしたデータが溢れかえっており、これらのデータを読み間違えないためにも日常生活上のリテラシーとして統計的な見方を知っておかねばならない。また、数学はあまたある学問の中でも厳密性が高い理論と考えられており、論理を展開するためのモデルケースとみなされている。つまり、論証の方法論を学ぶにあたり不可欠な学科なのである。中世のリベラル・アーツにおいて

¹大学院は professional school および graduate school の和訳に相当し、ここで professional school を指す。

数学が重視されたのもこのためであった。こうした事情を踏まえれば、現代においても数学は文理を問わず、ある程度学ばなければならない学科といえよう。

ここまでは中世の教養においても、またガリレオやニュートン以降の科学の時代においても数学は必須であるということ述べてきた。では、各大学において、どのような数学が実際に教えられているのだろうか。実は、現在では大学生に教えるべき内容の共通見解があたかも得られているかのような状況になっており、多くの数学の講義はパッケージ化され、どこの大学に行っても誰が教えても殆ど同じ内容について学ぶということになっている。特に理工系学科の1年次生向けの講義についてそれは顕著であり、ほとんどの大学において、微積分学(解析学の初歩)と線形代数学(行列と行列式の理論)を二つの柱としたカリキュラムを組んでいる。

パッケージ化の利点は、なんといっても効率的な点である。完成しきった理論であるから、講師は本に書いてあることだけを述べても講義として成立し、別の仕事に多くの時間を割くことができるようになった。また、扱うべき内容は決まっているため、参考書業界においては読者の用途が内容の争点とみなされ、様々な差別化が図られている。つまり、講義用のものや自習に適したもの、あるいは分かりやすさに特化したものなど多種多様な要請に応じた参考書が数多く出版されており、学習する側の環境はこの上なく整っている。

一方でパッケージ化による弊害は、内容が縦割りになってしまふことにある。有機的な繋がりを持っている各分野がそれぞれ独立・分断されたものであるかのように錯覚し、また講義も内容消化を優先して進めるため視野の広い立場から論ずる機会が失われがちになる。更に、パッケージ化された教育が長い間続くと、下手をすると、それらを学ぶべきことは理由なく当然であるといった考えに講師・受講者共に陥ってしまう可能性がある。これはある種の思考停止であり、思考停止は学習意欲の低下(どうして学ぶのか分からない)に繋がるように思う。

この講義ではこうした状況を鑑み、何故、どうして、といったそもそも論や、パッケージ化された線形代数の外にある世界にも焦点を当てる予定である。受講者には視野を広く持って講義に臨んでもらいたい。

1.3 数学概論

線形代数学はその名前から想像するに代数学の一部であり、代数学はもちろん数学の一部である。数学における線形代数の位置を知るために、数学の各分野について簡単に触れておこう。なお、この講義では、いくつかの数学的概念について、それが数学のどの分野へ繋がっていくかを後で解説する予定であり、その際の予備知識という意味も込めてこれを書いている。

さて、伝統的には、数学は代数・解析・幾何の三分野に大別される。もちろん、これは大まかな分類であり、数学の各分野はすべてこのいずれかに属するというわけではない。むしろ数学は、この三分野の考え方を駆使して研究されていると考えるべきである。これから三分野の簡単な説明を与えるが、ここで述べていることは、予備知識の無い初学者には想像しにくいことかもしれない。しかしながら、数学をある程度学び終えた後でもう一度読んで頂ければ、より深い理解が得られるはずである。

代数 代数学とは、簡単に説明すれば四則演算の技法を高める学問ということになる。例えば小中学校で学んだ計算問題などがこれに相当する。しかしながら代数学の神髄は、二つの異なる世界を一つの見方で繋げることにあると言えるだろう。これについては本節の後半で例を挙げて説明する。さて、代数学の中には数論・群論・体論・環論などがある。数論は素数の性質を調べる分野で、最大公約数や最小公倍数の問題を扱った経験のある一般の人にとって最もなじみの深い数学である。群論とは、図形をはじめとする様々な数学的構造の対称性を研究する分野であり、体論とは四則演算が成立する世界をいくつも考えだし、それらの間にある関係を群論を通して調べるものである。環論の説明を予備知識なしに述べるのは難しい。線形代数をこれら四分野のどこに入れるか、あえて考えると、環論に属することになる。

解析 高校で学んだ微分や積分などに現れる極限操作を扱う数学を解析学という。もちろん複素数の範囲も含めた関数の解析も扱われる(関数論)。自然科学の法則(物理法則だけとは限らない)を記述する式の多くは微分積分の記号を用いて表され、これらは微分(積分)方程式と呼ばれる。こうした方

程式の解を探す手法や、解が満たす性質を研究することが解析学の主な目的であり、したがって実用的な諸科学と最も関係の深い分野とも言えるだろう。解析学において厳密な論理展開を行うには ε - δ 論法の会得はもちろんのこと、関数の列に関する収束・発散の精緻な議論（関数解析学）が必須であり、そのための基礎としてルベーグ積分というキーワードがあることを覚えておくといよい。また積分論は、統計学の基礎となる確率論とも深い関わりを持っている。

幾何 空間図形を扱う数学を幾何学といい、現代の幾何学は微分幾何学と位相幾何学（トポロジー）に大別されている。前者は面積や体積など量的な調べかたを下地にした幾何学であり、後者は図形の持っている性質の違いに着目する幾何学である。図形の性質とは、例えば円上の1点を切り離してもまだ繋がったままだが、線分で同じことを考えると二つに分離されてしまうといった具合である。いずれの幾何学も多様体の構造を調べるのが念頭にある。大航海時代以前の人々は、世界の形が平らで海が無限に広がっているのか、それとも球の形をしているか、あるいは第三の可能性はあるか（例えばドーナツ型など）という問題に挑むには、限られた観測結果と頭の中の想像を頼りに結論づけるしかなかった。多様体論とはこれの多次元版に相当する。つまり、宇宙の形の可能性について追求する数学である。

いま挙げたのは数学のほんの一部であり、すべてが列挙されたわけではない。例えば複数の分野にまたがる数学については何一つ述べていないし、特に応用数学については何も述べていない。このほか、数学それ自体を問う分野もある。一つは数学の歴史を紐解く数学史に関する分野であり、もう一つは数学の証明の厳密性について論じる数学基礎論（数理論理学）である。

最後に線形代数学について簡単に説明しよう。線形代数学とは、線形写像（線形関数）を解析するための理論の総称である。線形写像とは、大雑把に言えば比例関数の多変数化に相当し、ゆえに線形写像は定数関数の次に単純な関数といえる。自然科学が、自然界の現象を出来る限り単純なモデルに落とし解析する学問のことであるとすれば、定数関数の次に単純な構造を持つ線形関数がそこで大きな役割を果たすであろうことは想像できるだろう。また、それゆえに線形代数学は理工系分野で求められる基本的な素養の一つとなっているのである。

それでは、線形写像の説明を試みるために、やや退屈ではあるが、集合や写像、そしてベクトルの和とスカラー倍について復習しよう。

1.4 ユークリッド空間における和とスカラー倍

いくつかのものの集まりのことを集合 (set) という。集合を構成しているもの一つ一つを要素 (element) または元という。集合の表記の仕方の一つとして、集合を構成する要素をすべて並べて中括弧でくくる方法がある。例えば、りんご、みかん、スイカの3つの要素からなる集合は、

$$\{ \text{りんご, みかん, スイカ} \}$$

と表される。こうした表し方は、この講義では多くは使わないものの、稀に用いるゆえ忘れないでほしい。

数を構成要素とする集合のうちいくつかは特別なアルファベットが割り当てられており、この講義では次のような記号を用いる²:

- \mathbb{N} : 自然数³(natural number) 全体のなす集合のこと。
- \mathbb{Z} : 整数 (integer, integral number) 全体のなす集合のこと。
- \mathbb{Q} : 有理数 (rational number) 全体のなす集合のこと。
- \mathbb{R} : 実数 (real number) 全体のなす集合のこと。

²太字を用いる場合もある。なお、このアルファベットの使い方は世界共通ゆえ覚えておいて損は無い。

³集合論を学ぶと、自然数に0を含めたほうが多くの表記において整合性が取れることが分かる。しかし、ここでは高校までの慣例に従い、自然数に0は含まれないものとする。

- \mathbb{C} : 複素数 (complex number) 全体のなす集合のこと.

\mathbb{R} や \mathbb{C} においては, 加減乗除の四則演算が定まっている. このことは既知のことであるとして, 話を進めよう⁴.

ある x が集合 X の元であるとき $x \in X$ と書く. そうでないとき, $x \notin X$ と書く.

例 1.4.1. $5 \in \mathbb{N}$, $-1 \notin \mathbb{N}$, $\frac{12}{13} \in \mathbb{Q}$, $\sqrt{2} \notin \mathbb{Q}$.

二つの実数 $x, y \in \mathbb{R}$ による並び順を込めた意味での組 (x, y) たち全体からなる集合を \mathbb{R}^2 と表す. ここで, “並び順を込めた意味” というのは, (x, y) と (y, x) は違うものと見なすということである⁵. \mathbb{R}^2 は平面上の点全体に一致している. 同様に, 各 $n \in \mathbb{N}$ について, n 個の実数の並び順を込めた意味での組 (x_1, x_2, \dots, x_n) たち全体からなる集合を \mathbb{R}^n と表し, これを **n次元ユークリッド空間** という. また, \mathbb{R}^n の元のことをベクトルと呼ぶ. 高校で学習したように, \mathbb{R}^2 や \mathbb{R}^3 のベクトルの間には和とスカラー倍が定まっているのであった. 同様のことが \mathbb{R}^n においても定義される. すなわち, \mathbb{R}^n の二つのベクトル $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathbb{R}^n$ および実数 $r \in \mathbb{R}$ に対して, ベクトルの和 $(x_1, \dots, x_n) + (y_1, \dots, y_n)$ およびベクトルのスカラー倍 $r(x_1, \dots, x_n)$ を次で定める:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n), \quad r(x_1, \dots, x_n) := (rx_1, \dots, rx_n).$$

上で用いた記号 $:=$ は, 新たな概念である左辺を右辺によって定義するという意味を表すものである.

ベクトルを一文字で表す場合は, $\mathbf{x} = (x_1, \dots, x_n)$ のように太字で書く. 太字を用いるのは1変数と混同しないようにするための措置であり, これは1年次向け教育における慣例となっている. $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ に対して, $\mathbf{0}, \mathbf{x}, \mathbf{x} + \mathbf{y}, \mathbf{y}$ の4点を頂点とする四角形が平行四辺形となることは既に高校で学習した通りである. 我々は三次元の空間に住んでいるため, 高次元の世界を直接見ることはできないけれども, このように高次元の空間がもつ性質のいくつかを想像することができる.

なお, 微積分ではベクトルを横書きにするのが慣例である一方で, 次節で定める行列の積との関係から線形代数ではベクトルを縦書きにしたほうが都合が良いことが多い. 横に並べたベクトルを行ベクトルといい縦に並べたベクトルを列ベクトルという. 以降ではどちらも \mathbb{R}^n の元とみなし, 用途に応じて使い分けることがある.

$$\text{行ベクトル: } (x_1, \dots, x_n), \quad \text{列ベクトル: } \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

1.5 写像とその合成

高校までの数学で現れる写像 (関数) はほとんどが1変数であり, 多変数の場合についても実数値関数しか扱うことはなかった. それゆえ写像についてことさらに細かい概念は必要なかったのであるが, これからは \mathbb{R}^n のベクトルを代入すると \mathbb{R}^m のベクトルが与えられるような写像を考えるため, 何を代入すると何が得られるのか明確にする必要が生じる. そこで, 写像について改めて定義を述べておこう.

定義 1.5.1. 集合 X の各元 x に対して集合 Y の元を一つ与える操作 (対応) を考える. このような操作を写像 (**map, mapping**) と呼び, このとき X をこの写像の定義域 (**domain**) という. 写像を記号 f を用いて表す場合, x に対応する Y の元を $f(x)$ と書く. この表記を通して, “ x を f で写像する” あるいは, “ f に x を代入する” といった表現もなされる. また, どの集合の元に対してどの集合の元を対応させる操作なのか明示するために, 次のような記号・図式が用いられる:

$$f: X \rightarrow Y \quad f: X \ni x \mapsto f(x) \in Y \quad \begin{array}{ccc} f: X & \longrightarrow & Y \\ \cup & & \cup \\ x & \longmapsto & f(x) \end{array}$$

⁴このようなことを書く理由には, 数とは何かという哲学的問いを再考し, より厳密な立場から数を定義するという思想があるからである.

⁵より正確には, $x = y$ であったときを除いて (x, y) と (y, x) を異なるものと見なすということ.

なお、写像と関数 (function) はほぼ同義語である。対応される元が数となるような写像 (すなわち上の定義において集合 Y が数を要素とする集合である場合) のことを関数と呼ぶことが多い。

定義域の元がベクトル \mathbf{x} の場合、 $f(\mathbf{x})$ を成分表示して正確に書けば $f((x_1, \dots, x_n))$ となり二重括弧が煩わしい。そこで、括弧を一つ減らして $f(x_1, \dots, x_n)$ と書くのが慣例となっている。

例 1.5.2. 各実数 x に対して、 $f(x) := 3x$ と定めれば、これは 3 倍の実数を対応させる写像 $f: \mathbb{R} \rightarrow \mathbb{R}$ である。

いくつかの写像が与えられているとき、それらを用いて新たな写像を構成する操作を数学では頻繁に行う。こうした操作の中で最も基本的なものが写像の合成である。

定義 1.5.3. 二つの写像 $f: X \rightarrow Y$ および $g: Y \rightarrow Z$ が与えられているとする。このとき、各 $x \in X$ に対して、 Z の元 $g(f(x))$ を対応させる写像を f と g の合成と呼び、記号 $g \circ f: X \rightarrow Z$ で表す。すなわち、 $(g \circ f)(x) := g(f(x))$ である。

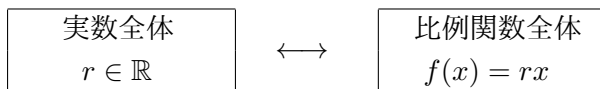
合成 $g \circ f$ を定めるには、各 $f(x)$ が g の定義域の要素でなければならない。ところで、 $g \circ f$ で一つの写像を表しているから、誤解が無い限り $(g \circ f)$ と括弧つきで書く必要はない。そこで、以下 $(g \circ f)(x)$ を $g \circ f(x)$ と書く。合成関数の簡単な例を、比例関数を用いて見てみよう。比例関数の定義も述べておく。

定義 1.5.4. ある実数 a を用いて $f(x) := ax$ と定められる関数 $f: \mathbb{R} \rightarrow \mathbb{R}$ を比例関数という。

例 1.5.5. 比例関数 $g: \mathbb{R} \rightarrow \mathbb{R}$ および $f: \mathbb{R} \rightarrow \mathbb{R}$ を $g(x) := ax$, $f(x) := bx$ と定めれば $g \circ f$ も比例関数であり、 $g \circ f(x) = (ab)x$ である。実際、

$$g \circ f(x) = g(f(x)) = g(bx) = a(bx) = (ab)x.$$

さて、比例関数の例をいくつか列挙しているうちに、次の対応に気がつくのではなからうか。



すなわち、実数全体と比例関数全体は 1 対 1 に対応しているのである。しかも、この対応は数の間の掛け算と関数の間の合成も上手く対応している。つまり、比例関数 g および f に対応する実数をそれぞれ a, b とすると、 $g \circ f$ に対応する実数は ab である (例 1.5.5)。あまりに簡単なことを述べているため拍子抜けしてしまうかもしれない。しかしながら、これこそが代数学の説明で述べた“二つの異なる世界を一つの見方で繋げる”ことなのである。今の話では実数をただの数と思うだけでなく、比例関数であるとも思えるということであり、これは実数に対する見方を広げたことを意味している。こうした考え方の多次元版として行列の概念が現れる。これを次項で詳しく述べよう。

1.6 そして線形代数へ

比例関数の多変数版に相当する線形写像は次のように定義される:

定義 1.6.1. 次の性質 (i) および (ii) を持つ写像 $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ を線形写像という:

- (i) すべての $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ に対して、 $f(\mathbf{x} + \mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$,
- (ii) すべての $\mathbf{x} \in \mathbb{R}^n$ および各 $r \in \mathbb{R}$ について、 $f(r\mathbf{x}) = rf(\mathbf{x})$.

すなわち、ベクトルの和を取ってから代入しても代入してから和を取っても同じ結果が得られ、また、スカラー倍をほどこしてから代入したものは代入してからスカラー倍をほどこしたものに一致するような写像のことである。上の二つの性質を線形性という。比例関数が線形写像であることを確認してみよう。

練習 1.6.2. 比例関数 $f(x) = ax$ は線形写像である。

Proof. 線形写像の性質 (i) および (ii) が成立することを確認すればよい.

(1) 各 $x, y \in \mathbb{R}$ に対して, $f(x+y) = a(x+y) = ax + ay = f(x) + f(y)$. ゆえに (i) は成立する.

(2) 各 $x \in \mathbb{R}$ および $r \in \mathbb{R}$ に対して, $f(rx) = a(rx) = r(ax) = rf(x)$. ゆえに (ii) は成立する.

以上より f は, 性質 (i) および (ii) を持つことが分かった. ゆえに f は線形写像である. \square

上の証明の最後に用いた記号 \square は証明終 (q.e.d. ...quod erat demonstrandum) を意味する.

線形写像の重要な例は後期で扱う. ここでは \mathbb{R}^2 の間の線形写像を挙げよう.

例 1.6.3. あらかじめ実数 a, b, c, d を与えておく. $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ を $f \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$ と定めればこれは線形写像である (各自確認せよ).

実は, \mathbb{R}^2 の線形写像はこの形のものですべて出つくしている. すなわち, $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ を任意の線形写像として, $\begin{pmatrix} a \\ c \end{pmatrix} := g \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ および $\begin{pmatrix} b \\ d \end{pmatrix} := g \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ とおくと $g \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$ が各 $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$ について成立する. これは線形写像の性質 (i) および (ii) を用いて次のように確かめられる:

$$\begin{aligned} g \begin{pmatrix} x \\ y \end{pmatrix} &= g \left(x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = g \begin{pmatrix} x \\ 0 \end{pmatrix} + g \begin{pmatrix} 0 \\ y \end{pmatrix} \\ &= xg \begin{pmatrix} 1 \\ 0 \end{pmatrix} + yg \begin{pmatrix} 0 \\ 1 \end{pmatrix} = x \begin{pmatrix} a \\ c \end{pmatrix} + y \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}. \end{aligned}$$

上の議論により, 線形写像 $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ と 2×2 行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ が対応することが分かった. 比例関数と実数の間の 1 対 1 対応のように, 写像の合成と演算を対応させるには, 行列の掛け算 (積) を定める必要がある. 一般の行列の演算は次節で学ぶとして, ここでは 2×2 行列の和と積の定義を述べよう.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} := \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} := \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

行列の和の定義が自然なものと思える一方で, 積の定義はなにゆえ複雑なのか. その理由は次の命題を成立させることが行列理論の前提だからである:

命題 1.6.4. \mathbb{R}^2 から \mathbb{R}^2 への線形写像全体と 2×2 行列全体の間で定まる先程の対応は 1 対 1 である. また, 二つの線形写像 $g, f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ に対応する行列をそれぞれ A, B とすれば, 合成 $g \circ f$ もまた線形写像であり, $g \circ f$ に対応する行列は AB である.

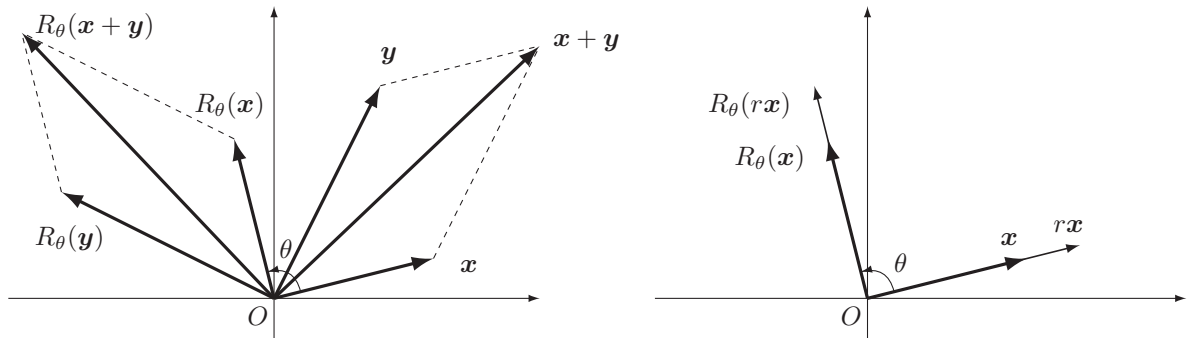
この対応は 2 変数に限らず, \mathbb{R}^n から \mathbb{R}^m への線形写像全体と $m \times n$ 行列全体の間関係として一般に成り立つことを, ここで予告しておく.

以上により行列とは線形写像をデータ化するために考えだされた概念であることが分かった. 抽象的な線形写像を行列によって数値化することで, 写像を見やすくするというのが行列理論の目的である. 前期の講義では, 行列に関する計算を理解することを目標とする. そして後期において, 行列を駆使した線形写像の分析について学ぶ. 今後の講義において, しばらくのあいだ線形写像そのものは表立って出てこないが, 行列理論の目的が線形写像の分析にあるということを念頭において学習してもらいたい.

練習 1.6.5. 二つの線形写像 $g, f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ を $g \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$, $f \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} ex + fy \\ gx + hy \end{pmatrix}$ で定める. このとき $g \circ f \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (ae + bg)x + (af + bh)y \\ (ce + dg)x + (cf + dh)y \end{pmatrix}$ となることを確かめよ.

よりみち (加法定理).

\mathbb{R}^2 の各ベクトル \mathbf{x} に対して、原点 O を中心に \mathbf{x} を θ 回転させたベクトルを対応させる写像 $R_\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ を考える. これは明らかに線形写像である. 実際, 定義 1.6.1 における線形性 (i) および (ii) が成り立つことは次のようにして理解できる. O を頂点に持つ平行四辺形を O を中心に回転させれば, これも O を頂点に持つ平行四辺形である. ゆえに $R_\theta(\mathbf{x} + \mathbf{y})$ は二つのベクトル $R_\theta(\mathbf{x}), R_\theta(\mathbf{y})$ で張られる平行四辺形の頂点となる. これは $R_\theta(\mathbf{x} + \mathbf{y}) = R_\theta(\mathbf{x}) + R_\theta(\mathbf{y})$ を意味している. また, 回転によってベクトルの長さが変化することはない. したがって \mathbf{x} と $r\mathbf{x}$ における長さの比と, これらを R_θ で写像した $R_\theta(\mathbf{x})$ と $R_\theta(r\mathbf{x})$ における長さの比は共に $1 : r$ である. 更に, \mathbf{x} と $r\mathbf{x}$ は平行ゆえ θ 回転後の $R_\theta(\mathbf{x})$ と $R_\theta(r\mathbf{x})$ も平行である. 以上のことから $R_\theta(r\mathbf{x}) = rR_\theta(\mathbf{x})$ が成り立つ.



ベクトル $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ および $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ を θ 回転させたベクトルはそれぞれ $\begin{pmatrix} \cos \theta \\ \sin \theta \end{pmatrix}, \begin{pmatrix} -\sin \theta \\ \cos \theta \end{pmatrix}$ であるから,

線形写像 R_θ に対応する行列は $A_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ となる.

さて, ベクトルを β 回転させた後に α 回転させることと, 一度に $\alpha + \beta$ 回転させることは同じ操作である. これは $R_\alpha \circ R_\beta = R_{\alpha+\beta}$ を意味する. $R_{\alpha+\beta}$ に対応する行列は $A_{\alpha+\beta} = \begin{pmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{pmatrix}$ であり, $R_\alpha \circ R_\beta$ に対応する行列は $A_\alpha A_\beta$ ゆえ

$$\begin{aligned} A_\alpha A_\beta &= \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix} \\ &= \begin{pmatrix} \cos \alpha \cos \beta - \sin \alpha \sin \beta & -\cos \alpha \sin \beta - \sin \alpha \cos \beta \\ \sin \alpha \cos \beta + \cos \alpha \sin \beta & -\sin \alpha \sin \beta + \cos \alpha \cos \beta \end{pmatrix}. \end{aligned}$$

$A_{\alpha+\beta} = A_\alpha A_\beta$ の成分を比較することで加法定理:

$$\cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta,$$

$$\sin(\alpha + \beta) = \sin \alpha \cos \beta + \cos \alpha \sin \beta.$$

を得る. 線形写像を知る者にとって加法定理は自明の理といえるだろう.

2 行列の演算

ここでは行列 (matrix) に関する演算, すなわち和・スカラー倍・積を定める. 前節で見たように, これらの演算は, 線形写像に対して定義される演算を行列の言葉で読み替えたものに相当している.

2.1 行列の行と列

$m \times n$ 個の数を矩形に並べ括弧で囲んだものを m 行 n 列の行列 ((m, n) -行列, $m \times n$ 行列) という. 数学書は横書きで記述するゆえ横に並ぶ文字列が行であり, 縦に並ぶ文字列が列である. 行の数と列の数の組 (m, n) を行列の型 (あるいはサイズ) という.

例 2.1.1. 4行5列の行列:

$$A = \begin{pmatrix} 1 & 0 & 4 & 2 & 1 \\ 5 & 7 & 1 & 0 & 9 \\ 4 & 3 & 2 & 9 & 8 \\ 3 & 1 & 1 & 2 & 4 \end{pmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 4 & 2 & 1 \\ 5 & 7 & 1 & 0 & 9 \\ 4 & 3 & 2 & 9 & 8 \\ 3 & 1 & 1 & 2 & 4 \end{bmatrix}.$$

行列の成分を囲む括弧は柔らかいものでも堅いものでも構わない. 板書では黒板の余白を有効に利用するため堅い括弧を用いることが多いと思うが, 気分によっては柔らかいほうを用いることもある. 前節で定めた行ベクトルとは $1 \times n$ 行列であり, 列ベクトルとは $n \times 1$ 行列のことである. 今後, 成分が n 個あるベクトルを n 次ベクトルと呼ぶことにしよう.

A を (m, n) -行列とする. 各 $i = 1, \dots, m$ および $j = 1, \dots, n$ について, A の i 行 j 列目の数を (i, j) -成分と呼ぶ. 例 2.1.1 における行列 A の 3 行目とは 5 次行ベクトル $(4, 3, 2, 9, 8)$ のことであり, 2 列目とは

4 次列ベクトル $\begin{pmatrix} 0 \\ 7 \\ 3 \\ 1 \end{pmatrix}$ のことである. A の $(3, 2)$ -成分は 3 である.

一般の $m \times n$ 行列 A を成分表示すると次のようになる:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}.$$

毎回このような表示を用いると手間がかかるゆえ, 場合によっては, これを $A = [a_{ij}]$ と略記する. ただし, i, j は $i = 1, \dots, m, j = 1, \dots, n$ を動く. 二つの行列が等しいことを次で定める.

定義 2.1.2. $m \times n$ 行列 $A = [a_{ij}]$ および $\ell \times r$ 行列 $B = [b_{kh}]$ が等しいとは, A, B のサイズが等しく, さらに各 (i, j) -成分が一致することである. すなわち, $m = \ell$ かつ $n = r$ であり, 更に各 i, j について $a_{ij} = b_{ij}$ が成り立つということである. A, B が等しい行列であるとき, $A = B$ と書く.

したがって, 例 2.1.1 における行列 A, B について, $A = B$ である. 上の定義によれば, n 次列ベクトルと n 次行ベクトルは, 行列としては異なるものである. しかしながら, これらはユークリッド空間 \mathbb{R}^n の元としては同じ位置を示す場合があり, 同じ位置を指すベクトルを異なると考えれば混乱が生じる恐れがあるだろう. そこで, \mathbb{R}^n のベクトルについて論じる場合は, 縦横どちらを用いてもよいが, その議論の最中はいずれか一方のみを用いると約束したい.

2.2 行列の和とスカラー倍

行列の和とスカラー倍の定義は, \mathbb{R}^n のベクトルのそれとほとんどかわらない.

定義 2.2.1. 二つの $m \times n$ 行列 $A = [a_{ij}]$ および $B = [b_{ij}]$ の和 $A + B = [z_{ij}]$ は $z_{ij} := a_{ij} + b_{ij}$ で定められる $m \times n$ 行列である。また各 $r \in \mathbb{R}$ について、スカラー倍 $rA = [w_{ij}]$ は $w_{ij} := ra_{ij}$ で定められる $m \times n$ 行列である。

上の定義を成分表示して書けば次のようになる:

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

$$r \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = \begin{bmatrix} ra_{11} & ra_{12} & \cdots & ra_{1n} \\ ra_{21} & ra_{22} & \cdots & ra_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ ra_{m1} & ra_{m2} & \cdots & ra_{mn} \end{bmatrix}.$$

A と B の和が定まるのは A, B のサイズが一致する場合のみである。

2.3 行列の積

何度も言うように、行列の演算とは線形写像のそれに対応するものである。 \mathbb{R}^2 を定義域とする線形写像のベクトル値は、 $ax + by$ という形の数をもつことを前節で見た。これは 1 個 a 円のリンゴ x 個に 1 個 b 円のメロン y 個を購入するには合わせていくら必要か (答えは $ax + by$ 円) というたぐいの計算を複数回行うことに相当している。行列の理論とは、このように小学校の算数で扱う文章題のような単純計算をいかに一般化し、奥深い理論に昇華するかということにほかならない。つまり基本は子供でも十分理解できる話であり、また予備知識も必要なく学べる理論となっている。

さて、まずは $m \times n$ 行列 $A = [a_{ij}]$ と n 次列ベクトル $\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ の間の積 $A\mathbf{x}$ を、やや天下りの的では

あるものの定義してしまおう。 $A\mathbf{x}$ は次で定義される m 次列ベクトルである:

$$A\mathbf{x} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} := \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix}.$$

ここで A の列の数と \mathbf{x} の成分数が等しく、 A の行の数と $A\mathbf{x}$ の成分数が等しいことに注意しておく。

例 2.3.1.

$$\begin{bmatrix} 1000 & 500 & 0 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 1000 \cdot 4 + 500 \cdot 5 + 0 \cdot 1 \\ 3 \cdot 4 + 2 \cdot 5 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 6500 \\ 23 \end{bmatrix}.$$

例 2.3.2. 日帰りの団体旅行の計画があり、一人あたり次のような準備が必要であると見積もられている。また参加家族は次のように構成されているとする。

	大人	小人	見習熟児		斎藤	田端	嶺	...
交通費 (円)	1000	500	0	大人	4	1	2	...
おにぎり (個)	3	2	1	小人	5	2	2	...
⋮	⋮	⋮	⋮	見習熟児	1	1	0	...

例えば斎藤家に必要な準備を知るには、見積もり表の数値を成分とする行列と斎藤家の構成データによる列ベクトルの積を取ればよい。その計算は例 2.3.1 の通りであり、従って交通費 6500 円、おにぎり 23 個が必要となる。同様の計算が田端家 (交通費 2000 円、おにぎり 8 個) や嶺家 (交通費 3000 円、おにぎり 10 個) においてもなされ、これらの計算を一度に行うものとして行列の積は定義される。つまり、次のような計算を想定している。

$$\begin{bmatrix} 1000 & 500 & 0 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 4 & 1 & 2 \\ 5 & 2 & 2 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 6500 & 2000 & 3000 \\ 23 & 8 & 10 \end{bmatrix}.$$

いよいよ行列の積の定義に入る。

定義 2.3.3. $m \times n$ 行列 $A = [a_{ij}]$ と $n \times \ell$ 行列 $B = [b_{jk}]$ の積 $AB = [z_{ik}]$ は次で定められる $m \times \ell$ 行列である: $z_{ik} := a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}$.

すなわち、 AB の (i, k) -成分とは、 A の i 行目 (これは n 次元行ベクトル) と B の k 列目 (これは n 次元列ベクトル) の積⁶である。行列 AB を定めるには、 A の列の数と B の行の数が一致せねばならないことに注意せよ。これは、線形写像 f と g の合成 $g \circ f$ を考えるとき、 f に代入して得られたベクトルが g の定義域の元でなければならないことに対応している。また A の行の数や B の列の数はいくらあってもよい。これは例 2.3.2 において、見積もり表にお茶 (ml)、お菓子代 (円)、入場料 (円) などのデータを加えたり、家族の構成表に別の家族のデータを加えたりしても同様に上手く計算ができることに対応している。

行列の積の計算を行うには、単純ではあるものの多くの計算を繰り返さなければならない。例えば 3 次正方行列どうしの積を計算するには、一つの成分を求めるのに掛け算を 3 回、足し算を 2 回、合わせて 5 回の計算を行う。したがって、すべての成分を求めるには計 45 回の計算が必要になる。このうち一つでも計算を誤れば正しい結果は得られない。理論の理解と計算の正確性は別次元の話であり、計算練習によって自身の計算精度を確かめておくことよい (試験対策のためである)。

例 2.3.4. 行列の積の計算に慣れないうちは次のように補助線を引いておくと見やすく計算できる。左側の行列を行について分割し、右側の行列を列について分割している。

$$\begin{bmatrix} \hline 1 & 0 & 1 \\ 3 & 2 & 0 \\ \hline 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 & 3 & 1 \\ \hline 2 & 0 & 1 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 + 0 \cdot 2 + 1 \cdot 0 & 1 \cdot 3 + 0 \cdot 0 + 1 \cdot 2 & 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 \\ 3 \cdot 0 + 2 \cdot 2 + 0 \cdot 0 & 3 \cdot 3 + 2 \cdot 0 + 0 \cdot 2 & 3 \cdot 1 + 2 \cdot 1 + 0 \cdot 0 \\ 1 \cdot 0 + 1 \cdot 2 + 2 \cdot 0 & 1 \cdot 3 + 1 \cdot 0 + 2 \cdot 2 & 1 \cdot 1 + 1 \cdot 1 + 2 \cdot 0 \end{bmatrix} \\ = \begin{bmatrix} 0 & 5 & 1 \\ 4 & 9 & 5 \\ 2 & 7 & 2 \end{bmatrix}$$

上の一つ目のイコールの後の細かい計算はノートに書かずに暗算できるようにしておくこと。

例 2.3.5. 次の二つの計算を混同しないよう注意せよ。

$$\begin{bmatrix} a & b & c \end{bmatrix} \begin{bmatrix} d \\ e \\ f \end{bmatrix} = ad + be + cf, \quad \begin{bmatrix} a \\ b \\ c \end{bmatrix} \begin{bmatrix} d & e & f \end{bmatrix} = \begin{bmatrix} ad & ae & af \\ bd & be & bf \\ cd & ce & cf \end{bmatrix}$$

2.4 行列演算の性質

行列に関するいくつかの概念をここでまとめて定めておく。

- すべての成分がゼロになる $m \times n$ 行列を零行列とよび O_{mn} と書く。行列のサイズに誤解が生じない場合は O と略記する。

⁶これは \mathbb{R}^n の内積に相当していると考えられることもできる。

- $n \times n$ 行列のことを n 次正方行列という.
- n 次正方行列 $A = [a_{ij}]$ において (i, i) -成分 a_{ii} ($i = 1, \dots, n$) を A の対角成分という.
- すべての対角成分が 1 で、それ以外の成分がすべてゼロとなる n 次正方行列を n 次単位行列といい、これを E_n と書く. 行列のサイズに誤解が生じない場合は E と略記する⁷.

$$E_1 = 1, \quad E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad E_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

- $(-1)A$ を $-A$ と書く. また, $A + (-B)$ のことを $A - B$ と書く.

命題 2.4.1. 行列の演算は次の性質を満たす. ただし, 行列 A, B, C の各サイズは演算が定義されることを前提とし, a, b を実数とする.

- (1) $A + B = B + A$, (2) $A + O = A$, (3) $(A + B) + C = A + (B + C)$, (4) $A + (-A) = O$,
 (5) $AE = A$ (6) $EA = A$, (7) $AO = O$, (8) $OA = O$,
 (9) $0A = O$, (10) $1A = A$, (11) $(ab)A = a(bA)$, (12) $(aA)B = a(AB)$,
 (13) $(aA)(bB) = (ab)(AB)$, (14) $a(A + B) = aA + aB$, (15) $(a + b)A = aA + bA$,
 (16) $A(B + C) = AB + AC$, (17) $(A + B)C = AC + BC$, (18) $(AB)C = A(BC)$.

A が正方行列でない場合は (5) と (6) における E のサイズが異なることに注意せよ. また (7) における左辺の O と右辺の O もサイズが違う可能性がある. (8) についても同様である.

上の性質のうち (3) および (11), (12), (18) は結合律と呼ばれる. これは, どちらの演算を先に行っても結果が同じことを意味し, それゆえ $A + B + C$ という表記が許されることになる. 同様のことが abA , aAB , ABC についても言える. また, 正方行列 A の k 個の積を取る演算はどの部分の積から順に計算しても性質 (18) により結果は同じであり, これを A^k と書く. すなわち,

$$A^k := \underbrace{AA \cdots A}_{k \text{ 個の積}}.$$

また, A の k 個の和を kA と書く. この表記は性質 (10) および (15) との整合性が取れている:

$$\underbrace{A + A + \cdots + A}_{k \text{ 個の和}} = 1A + 1A + \cdots + 1A = (1 + 1 + \cdots + 1)A = kA.$$

(14) から (17) までの 4 つの性質は分配律と呼ばれる. (13) をスカラー律という. (4) は, (9) および (10), (15) から導ける:

$$A + (-A) = 1A + (-1)A = (1 + (-1))A = 0A = O.$$

このように演算の性質を抽出する利点は, 一つには行列の演算の定義の詳細に触れずとも議論を進められることにある (練習 2.4.3 も見よ).

さて, 本来ならば, 命題 2.4.1 に挙げた性質すべてが成立することを証明しなければならない. しかし, すべてに時間を割く暇はないから, ここでは証明が最も簡単な (1) と最も難しい (18) について紹介するにとどめる. この二つの証明ができれば, おそらく他の性質も容易に証明できよう.

⁷単位行列を表す記号には, 通常 I あるいは E , $\mathbf{1}$ などを用いる. これは identity matrix (英) あるいは Einheitsmatrix (独) の頭文字による. 一般に, 代数演算においてどこでも変わらない元のことを単位元 (identity element) という. 数の単位である 1 は実数の積に関する単位元であり, 単位行列 E_n は n 次正方行列の積に関する単位元である.

$A + B = B + A$ の証明. $A = [a_{ij}]$, $B = [b_{ij}]$ とおくと, $A + B = [a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}] = [b_{ij} + a_{ij}] = [b_{ij}] + [a_{ij}] = B + A$. \square

結合律 (18) の証明は次節で \sum 記号の使い方を復習したうえで行おう.

例 2.4.2. サイズが同じ正方行列 A, B について, $AB = BA$ は一般には成り立たない. 例えば $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ とすれば, $AB = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$, $BA = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ である.

練習 2.4.3. A, B を n 次正方行列とする. 次の等式が成り立つか述べ, 正しければ証明し, 正しくなければ反例を挙げよ.

$$(a) (A + 2E)(A + E) = A^2 + 3A + 2E, \quad (b) (A + B)^2 = A^2 + 2AB + B^2.$$

(a) : 正しい. 実際, 次のように計算する. 誤解がないよう $C = (A + E)$ とおく.

$$\begin{aligned} (A + 2E)(A + E) &= (A + 2E)C = AC + 2EC = AC + 2C = A(A + E) + 2(A + E) \\ &= A^2 + A + 2A + 2E = A^2 + 3A + 2E. \end{aligned}$$

(b) : 一般には成立しない. $C = (A + B)$ とおき左辺を展開してみると,

$$(A + B)^2 = (A + B)C = AC + BC = A(A + B) + B(A + B) = A^2 + AB + BA + B^2.$$

したがって, 仮に式 (b) 左辺と右辺が等しいとすれば, 両辺から $A^2 + AB + B^2$ を引くことで $BA = AB$ を得る. しかし例 2.4.2 で見たように, これは一般には成り立たない.

発展 (代数構造).

代数構造とは集合の元に対して定義される何らかの演算のことであり, 数学では色々な代数構造を持った集合が扱われている. 一番なじみが深いものは \mathbb{R} や \mathbb{C} , \mathbb{Q} のように加減乗除の四則演算が成立する世界のことで, これを体 (**field**) という. \mathbb{Z} は体ではない. 何故なら, 整数どうしの割り算が整数にならないからである. 無理数全体も体ではない.

ある集合の各元どうしについて和, 差, 積の演算および二つの特別な元 O と E (これらをそれぞれ零元, 単位元という) が定義されており, 命題 2.4.1 の性質 (1) から (8), および (16) から (18) が成立する代数構造を環 (**ring**) という. 例えば, \mathbb{Z} は零元 O として 0 を, 単位元 E として 1 を採用することで環とみなせる. なお, 環の定義に単位元の存在を外す立場もある. この立場では, 例えば偶数全体は単位元を含まない環である.

練習 2.4.3 は, 行列に限らず一般に, 環に対して問われるべき問題である. まったく同じ議論により, 任意の環において等式 (a) は正しいことが分かる. 等式 (b) についてはどうだろうか. すべての元について $AB = BA$ を満たす環を可換環といい, 可換環においては (b) は成立する (ゆえに \mathbb{Z} においても成り立つ). そうでない環において等式 (b) は一般には成り立たない. その理由も練習 2.4.3 で述べた通りである. このように, 抽象的に性質を挙げておくと, 全く同じ論法で別の世界の話についても同時に議論することができる. 数学において抽象的な定義を採用する理由は, こうした汎用性を考慮したことによるのである.

他にも, まだまだ代数構造はたくさんある. 例えば, ある体の元によるスカラー倍が環の中で定まっており, 命題 2.4.1 の性質 (9) から (15) が成立する (したがって 2.4.1 の性質すべてを満たす) 代数構造を多元環または代数 (**algebra**) という. 例えば, 自然数 n を固定しておき, 各成分に実数を持つ n 次正方行列全体を $M_n(\mathbb{R})$ とすれば, これは \mathbb{R} の元についてスカラー倍が定まった多元環である. また, 体自身は, 元々与えられている積をスカラー倍でもあると思うことで多元環ともみなせる.

いま, かなり抽象性の高い話をしており, 読者は既に食傷気味になっているかもしれない. ちなみに, 線形代数学で主として扱う代数構造は線形空間 (ベクトル空間) と呼ばれるものである. また, あまたある代数構造のうち最も重要なものは, 対称性を記述する群と呼ばれるものである. 線形空間については後期に, 群については行列式の定義の前あたりで紹介する.

3 行列の表し方

行列の表し方および記号の使い方について、いくつかの補足次項を説明する。ここで述べられていることは約束事であって、数学的に深い意味があるというわけではない。

3.1 \sum 記号の使い方

和の記号 \sum や積の記号 \prod の使い方を詳しく説明しておこう。 n 個の数 a_1, \dots, a_n たちの和 $a_1 + a_2 + \dots + a_n$ を

$$\sum_{i=1}^n a_i \quad \text{あるいは} \quad \sum_{i=1, \dots, n} a_i$$

と表す。積 $a_1 a_2 \dots a_n$ については $\prod_{i=1}^n a_i$ あるいは $\prod_{i=1, \dots, n} a_i$ と表す。また、 a_{ij} ($i = 1, \dots, m, j = 1, \dots, n$)

たちの総和を $\sum_{\substack{i=1, \dots, m, \\ j=1, \dots, n}} a_{ij}$ と書く。こうした表記をより一般的な立場から眺めると、次のような説明ができる。

P を、ある変数に関する条件とする。ここで変数は多変数としてもよい。

例 3.1.1. P の具体例に以下のようなものがある：

- $P(i)$: “ $i \in \mathbb{N}$ ”
- $P(i)$: “ $i = 1$ または $i = 2$ または \dots または $i = n$ ”
注: この条件文 $P(i)$ を略して、我々は “ $i = 1, \dots, n$ ” と書いている。
- $P(i)$: “ $i \neq 1$ かつ $i \neq 2$ ”
注: この条件文 $P(i)$ は “ $i = 1, 2$ ” の否定に相当するから、これを略して、 “ $i \neq 1, 2$ ” と書く⁸。
- $P(i, j)$: “ $i = 1, \dots, m$ かつ $j = 1, \dots, n$ ”
注: 通常は「かつ」を省略して記述することが多い。一方、「または」は勝手に略してはならない。更に $m = n$ のとき、この条件文 $P(i)$ を略して “ $i, j = 1, \dots, n$ ” と書く。
- $P(i, j)$: “ $1 \leq i \leq j \leq 3$ ”
- $P(i, j)$: “ $1 \leq i \leq 5$ かつ $1 \leq j \leq 5$ ”
注: この条件文 $P(i, j)$ を略して、 “ $1 \leq i, j \leq 5$ ” と書く。

定義 3.1.2. $P(i)$ たちが成立するような i をすべて動かして a_i の総和を取るとき、これを $\sum_{P(i)} a_i$ と書く。

$\prod_{P(i)} a_i$ についても同様に定める。

例えば $P(i)$ として “ $i = 1, \dots, n$ ” を考えれば、 $\sum_{i=1, \dots, n} a_i = a_1 + \dots + a_n$ を得る。ほかにも次のような使い方があ

例 3.1.3. • $X = \{1, 2, 3\}$ のとき、 $\sum_{i \in X} a_i = a_1 + a_2 + a_3$.

⁸この文と “ $i \neq 1$ または $i \neq 2$ ” を混同しないよう注意すること。なお余談になるが、 “ $i \neq 1$ または $i \neq 2$ ” とは、 i はどんな数でもよいことを意味している。

- $\sum_{1 \leq i \leq 5} a_i = a_1 + a_2 + a_3 + a_4 + a_5$.
 $1 \leq i \leq 5$ かつ i は整数
ただし、通常は i が整数であることは暗黙裡に認めていることが多く、「かつ i は整数」の部分は省略される.
- $\sum_{i=1,2, j=1,2,3} a_{ij} = a_{11} + a_{12} + a_{13} + a_{21} + a_{22} + a_{23}$,
- $\sum_{1 \leq i \leq j \leq 3} a_{ij} = a_{11} + a_{12} + a_{13} + a_{22} + a_{23} + a_{33}$,
- $\prod_{1 \leq i < j \leq 3} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$,
- $\sum_{\substack{i=1, \dots, n, \\ j=1, \dots, n}} a_{ij} = \sum_{i,j=1, \dots, n} a_{ij} = \sum_{1 \leq i, j \leq n} a_{ij}$.

例 3.1.4.

$$\begin{aligned}
\sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} \right) &= \sum_{i=1}^m (a_{i1} + a_{i2} \cdots + a_{in}) \\
&= (a_{11} + a_{12} \cdots + a_{1n}) + (a_{21} + a_{22} \cdots + a_{2n}) + \cdots + (a_{m1} + a_{m2} \cdots + a_{mn}) \\
&= \sum_{\substack{i=1, \dots, m, \\ j=1, \dots, n}} a_{ij} \\
&= (a_{11} + a_{21} \cdots + a_{m1}) + (a_{12} + a_{22} \cdots + a_{m2}) + \cdots + (a_{1n} + a_{2n} \cdots + a_{mn}) \\
&= \sum_{j=1}^n (a_{1j} + a_{2j} \cdots + a_{mj}) = \sum_{j=1}^n \left(\sum_{i=1}^m a_{ij} \right)
\end{aligned}$$

行列の積の結合律 $(AB)C = A(BC)$ を証明しよう.

$(AB)C = A(BC)$ の証明. $A = [a_{ij}]$ を $m \times n$ 行列, $B = [b_{jk}]$ を $n \times \ell$ 行列, $C = [c_{kh}]$ を $\ell \times r$ 行列とし, $(AB)C$ および $A(BC)$ の各成分を積の定義にしたがって計算すると次のようになる.

$$\begin{aligned}
(AB)C &= \left([a_{ij}][b_{jk}] \right) [c_{kh}] = \left[\sum_{j=1}^n a_{ij} b_{jk} \right] [c_{kh}] \quad \left(\text{ここで } x_{ik} := \sum_{j=1}^n a_{ij} b_{jk} \text{ とおく} \right) \\
&= [x_{ik}] [c_{kh}] = \left[\sum_{k=1}^{\ell} x_{ik} c_{kh} \right] = \left[\sum_{k=1}^{\ell} \left(\left(\sum_{j=1}^n a_{ij} b_{jk} \right) c_{kh} \right) \right] = \left[\sum_{k=1}^{\ell} \left(\sum_{j=1}^n a_{ij} b_{jk} c_{kh} \right) \right].
\end{aligned}$$

$$\begin{aligned}
A(BC) &= [a_{ij}] \left([b_{jk}] [c_{kh}] \right) = [a_{ij}] \left[\sum_{k=1}^{\ell} b_{jk} c_{kh} \right] \quad \left(\text{ここで } y_{jh} := \sum_{k=1}^{\ell} b_{jk} c_{kh} \text{ とおく} \right) \\
&= [a_{ij}] [y_{jh}] = \left[\sum_{j=1}^n a_{ij} y_{jh} \right] = \left[\sum_{j=1}^n \left(a_{ij} \sum_{k=1}^{\ell} b_{jk} c_{kh} \right) \right] = \left[\sum_{j=1}^n \left(\sum_{k=1}^{\ell} a_{ij} b_{jk} c_{kh} \right) \right].
\end{aligned}$$

$(AB)C$ と $A(BC)$ の各 (i, h) -成分が等しいことは例 3.1.4 より分かる. □

発展 (写像の合成の結合律).

結合律 $(AB)C = A(BC)$ を線形写像の言葉で述べれば, それは写像の合成に関する結合律 $(h \circ g) \circ f = h \circ (g \circ f)$ である. 合成に関する結合律は, 線形写像に限らずとも一般の写像について成立する:

命題 3.1.5. 三つの写像 $f: X \rightarrow Y, g: Y \rightarrow Z, h: Z \rightarrow W$ について, $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof. 二つの写像が等しいとは, いかなる元を代入してもその結果が一致するということである. f の定義域のいかなる元 $x \in X$ についても $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$ となることを示そう. まず $h \circ g$ を $\phi, f(x)$ を y とおくことで

$$((h \circ g) \circ f)(x) = \phi \circ f(x) = \phi(f(x)) = (h \circ g)(y) = h(g(y)) = h(g(f(x))).$$

次に $\psi = g \circ f$ とおくことで

$$(h \circ (g \circ f))(x) = h \circ \psi(x) = h(\psi(x)) = h((g \circ f)(x)) = h(g(f(x))).$$

ゆえに $(h \circ g) \circ f = h \circ (g \circ f)$ である. □

線形写像の合成と行列の積が対応することを知っている者にとっては, 行列の積の結合律は写像の合成に関する結合律から直ちに理解される.

3.2 転置行列

(m, n) -行列 $A = [a_{ij}]$ に対して, 次のような行列が新たに定義できる:

定義 3.2.1. (n, m) -行列 $[a_{ji}]$ を A の転置行列 (**transposed matrix**) といい, tA と書く.

$$B = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \end{bmatrix}, \quad {}^tB = \begin{bmatrix} 1 & 6 & 11 \\ 2 & 7 & 12 \\ 3 & 8 & 13 \\ 4 & 9 & 14 \\ 5 & 10 & 15 \end{bmatrix}, \quad {}^t(x_1, \dots, x_n) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

列ベクトルをそのまま書くと行数を稼いでしまうため, 上のように行ベクトルの転置で表すことがある. 成分数が等しい二つの行ベクトル \mathbf{x}, \mathbf{y} に対して, これらの内積を $\mathbf{x} \mathbf{y}$ で定める. また, 成分数が等しい二つの列ベクトル \mathbf{x}, \mathbf{y} に対して, これらの内積を ${}^t\mathbf{x} \mathbf{y}$ で定める.

転置行列の真の意味, すなわち線形写像としての意味をここで述べるのは難しい⁹. いまは, A 自身の各行 (あるいは列) に関する内積の情報を得るための操作と考えておけばよいだろう. A の各行 (あるいは各列) の間の内積を成分とする (m, m) -行列 (あるいは (n, n) -行列) は $A {}^tA$ (あるいは ${}^tA A$) で与えられる.

3.3 成分の空白と任意性

行列 $A = [a_{ij}]$ を成分表示するとき, 成分が 0 となる部分は何も書かずに空白で表すことがある. また, まとまった領域においてすべての成分が 0 のとき, これらをまとめて O で表す. 例えば, 単位行列は次のように書かれる.

$$\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & & O \\ & 1 & O \\ O & & \ddots \\ O & & & 1 \end{bmatrix}$$

⁹これは与えられた線形写像の双対写像と呼ばれるものに相当する.

あまり重要でない成分は*と書かれる. 同じ記号*を用いるものの, 各成分において異なる数が入っていてもよいと考える. 例えば, $B = \begin{bmatrix} 2 & 0 & 1 \\ 0 & 3 & 2 \\ 0 & 0 & 4 \end{bmatrix}$ を略して $\begin{bmatrix} 2 & * & * \\ & 3 & * \\ & & 4 \end{bmatrix}$ と書く. このように略しても, B^n の対角成分は計算できる:

$$B^2 = \begin{bmatrix} 2 & * & * \\ & 3 & * \\ & & 4 \end{bmatrix} \begin{bmatrix} 2 & * & * \\ & 3 & * \\ & & 4 \end{bmatrix} = \begin{bmatrix} 2^2 & * & * \\ & 3^2 & * \\ & & 4^2 \end{bmatrix}, \quad B^n = \begin{bmatrix} 2^n & * & * \\ & 3^n & * \\ & & 4^n \end{bmatrix}.$$

また, まとまった領域において成分情報が不要であるとき, これらをまとめて*と書く.

定義 3.3.1. 対角成分より下の成分がすべて0なる行列を上三角行列という. すなわち, 次のような行列のことである:

$$\begin{bmatrix} a_1 & & & \\ & a_2 & * & \\ & & \ddots & \\ O & & & a_n \end{bmatrix}.$$

3.4 行列の分割

次のように行列をいくつかの小さい行列に分割し, あたかも行列を成分にもつ行列であるかのように見なして計算してもよい.

$$\begin{aligned} \left[\begin{array}{cc|cc|c} 1 & 2 & 3 & 4 & 5 \\ \hline 6 & 7 & 8 & 1 & 0 \\ \hline 11 & 12 & 13 & 0 & 1 \end{array} \right] \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ \hline 6 & 7 \\ \hline 1 & 2 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} [1 \ 2] \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 3[6 \ 7] + [4 \ 5] \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \\ \hline [6 \ 7] \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + [8] [6 \ 7] + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \\ \hline \end{bmatrix} \\ &= \begin{bmatrix} [1 \ 2] + [18 \ 21] + [4 \ 13] \\ \hline [6 \ 7] + [48 \ 56] + [1 \ 2] \\ \hline [11 \ 12] + [78 \ 91] + [0 \ 1] \end{bmatrix} = \begin{bmatrix} 23 & 36 \\ 55 & 65 \\ 89 & 104 \end{bmatrix} \end{aligned}$$

こうした分割による積の計算と元々の定義による積の計算が一致することは, 各成分がどのような成分の積たちの和になっているか調べれば分かる. 分割計算を行う際の留意点は, 積がきちんと定まるような分割を行う必要があることである. なお, 分割計算は, 行列の性質を帰納法を用いて示す際に威力を発揮する. 行列のサイズに関する帰納法において, 分割によって小さくなった行列に帰納法の仮定を適用するという論法がよく使われている.

4 連立1次方程式と行列

前期の目標の一つは、連立1次方程式の一般解の解法を理解することにある。一般解を求めるということは、すべての解を出しつくすことを意味する。あてずっぽうで解の一つや二つを見つけるのではなく、理論的な見地から、解はこれ以外にはありえないということまで我々は示さねばならない。一般に、方程式の解は無限にたくさんあるかもしれないし、一つも存在しないということもあり得る。この事実を次の三つの方程式を例に確かめてみよう。

$$(1) \begin{cases} x + y = 1 \\ 2x + 2y = 4 \end{cases} \quad (2) \begin{cases} x + y = 1 \\ 2x + 2y = 2 \end{cases} \quad (3) \begin{cases} x + y = 1 \\ x - y = 1 \end{cases}$$

方程式(1)の解は存在しない。何故なら、 xy 平面において直線 $x + y = 1$ と直線 $2x + 2y = 4$ は平行ゆえ交わらないことが図を描けば分かるからである。図の助けを借りずに論証する場合は次のようになるだろう。図は理解を助けるうえで重要ではあるが、錯覚している可能性が残されていることを忘れてはならない。

解の非存在証明。仮に方程式(1)に解 $(x, y) = (a, b)$ が存在すると仮定すると、上段の式を2倍することで $2a + 2b = 2$ を得る。また、下段の式からは $2a + 2b = 4$ を得る。以上より $4 = 2$ となる。これは明らかにおかしい。ゆえに方程式(1)の解は存在しない。□

一方で、方程式(2)の上下の式は互いに定数倍した関係にあるから、二つの式の意味は同じであり、ゆえに直線 $x + y = 1$ 上の点 $(a, 1 - a)$ が方程式(2)の解となる。 a は任意の実数を取り得るため、この方程式の解は無数にある。方程式(3)の解は二つの直線 $x + y = 1$ および $x - y = 1$ の交点である。すなわち、解は唯一つ $(x, y) = (1, 0)$ のみである。

いまの例によって、解の形には色々な可能性がありうるということが分かった。この単元における目標は、連立1次方程式と行列の関係を見極め、方程式の解全体の形がどのようなようになるか理論立てて理解することにある。さて、連立1次方程式と行列の関係は次のように与えられる。 x, y, z を変数とする連立方程式

$$\begin{cases} a_{11}x + a_{12}y + a_{13}z = b_1 \\ a_{21}x + a_{22}y + a_{23}z = b_2 \end{cases}$$

を解くことと、

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

を満たす3次元ベクトル $\mathbf{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ を探すことは同じことである。以後、連立1次方程式を解くことは、既知の行列 A および列ベクトル \mathbf{b} が与えられたとき、 $A\mathbf{x} = \mathbf{b}$ を満たす未知のベクトル \mathbf{x} を求めることと解釈し、話を進めよう。

4.1 逆行列を持つ場合

まずは最も簡単な場合の解法を紹介する。それは A が正方行列であり、更に $AB = BA = E$ を満たす正方行列 B が存在する場合である。このような B のことを A の逆行列という。このとき、列ベクトル \mathbf{a} が方程式 $A\mathbf{x} = \mathbf{b}$ の解であると仮定すれば(すなわち $A\mathbf{a} = \mathbf{b}$ を満たす)、この両辺に左から B をかけることで $BA\mathbf{a} = B\mathbf{b}$ を得る。左辺を計算すると $BA\mathbf{a} = E\mathbf{a} = \mathbf{a}$ ゆえ $\mathbf{a} = B\mathbf{b}$ である。したがって方程式に解が存在するとすれば、その解は唯一解 $\mathbf{x} = B\mathbf{b}$ のみであることが分かった。また、実際に $\mathbf{x} = B\mathbf{b}$ はこの方程式の解である。何故なら、 $A\mathbf{x} = AB\mathbf{b} = E\mathbf{b} = \mathbf{b}$ ゆえ $A\mathbf{x} = \mathbf{b}$ を満たすからである。以上より次を得る。

命題 4.1.1. 正方行列 A の逆行列 B が存在するとき、連立 1 次方程式 $Ax = b$ は唯一解 $x = Bb$ を持つ。

この命題は理論的にはすっきりとしているものの、いくつかの欠点がある。一つは、そもそも逆行列が存在するかどうかをどうやって判断するのかということである。また、逆行列 B を求める方法も今はまだ分からない。更に、逆行列が存在しない場合に、そうとも知らずに上の命題に準じた方向で挑んでしまったら、計算が徒労に終わってしまうのだろうか。実は、理論を進めていくと、これらの問題はすべて繋がっていることが分かる。

4.2 行列の行基本変形

A を (m, n) -行列とする。このとき $Ax = b$ は、変数の数が n 個、式の数 m 個の連立 1 次方程式である。方程式を解くにあたり、各係数に現れる数が単純 (例えば係数に 0 が多く現れる場合) なほど解は求めやすい。そこで、係数なるべく単純になるよう式を変形する方法を考えたい。そのためには、方程式を変形してもその式の本質的な意味が変わらない操作が何かをまず考える必要がある。例えば、次の 3 つの操作 (式の書き換え) は方程式の意味を変えない。すなわち、変形する前と後で解の形が変わらない。

- (i) 実数 $r \neq 0$ について、一つの式を両辺を r 倍した式に書き換える、
- (ii) m 個の式の順番を並べ替える、
- (iii) ある式の何倍かを別の式に加えることで、新しい式に書き換える。

上の 3 つの操作で解の形が変化しない理由は、再び 3 つの操作のいずれかを行うことで元の方程式の形に戻ることができるからである。この 3 つの操作に対応する行列の変形操作を行基本変形という。すなわち、次の 3 つの変形のことである：

- (1) 実数 $r \neq 0$ について、一つの行を r 倍する、
- (2) 二つの行を入れ替える
- (3) ある行の何倍かを別の行に加える。

(m, n) -行列 A と m 次列ベクトル b を並べた、 $(m, n + 1)$ -行列 $[A|b]$ を考えよう。

$$[A|b] := \left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array} \right].$$

これを方程式 $Ax = b$ に関する拡大係数行列という。行列 $[A|b]$ に行基本変形の操作 (1) から (3) のいずれかを一回ほどこした行列を $[A'|b']$ としよう。このとき、 n 次列ベクトル a について、 a が方程式 $Ax = b$ の解であることと、 a が方程式 $A'x = b'$ の解であることは同値である。これは、連立 1 次方程式に対して (i) から (iii) のいずれの式変形を行っても解が変化しないことから明らかである。また、行基本変形を $[A|b]$ に何度ほどこしてもこの状況は変わらない。したがって次を得る：

命題 4.2.1. 行列 $[A|b]$ に有限回の行基本変形をほどこしたものを $[A'|b']$ とすれば、方程式 $Ax = b$ の解全体と方程式 $A'x = b'$ の解全体は一致する。

さて、連立方程式 $Ax = b$ を解くには、行基本変形を用いてより簡単な連立方程式 $A'x = b'$ に帰着させればよいことが分かった。では、ここでいう「簡単」とはどういう意味だろうか。例えば A が正方行列であり、 $[A|b]$ を運よく $[E|b']$ に変形できたとすれば、これは簡単だと言えるだろう (実際、 $x = b'$ が唯一の解である)。一般の場合には単位行列になることは望めないものの (そもそも正方行列でなければ絶対に不可能である)、方程式の解が直ちに分かるような行列の形があり、それは簡約行列と呼ばれている。

4.3 簡約行列

簡約行列を定義するために、まず主成分なる概念を導入する。行列 A の零ベクトルでない各行ベクトルに対して、その行のゼロでない最初の成分のことを、その行の主成分と呼ぶ。次の行列において下線が引かれた成分が各行の主成分である。

$$\begin{bmatrix} \underline{2} & 0 & 1 & 5 & 4 \\ 0 & 0 & \underline{1} & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \underline{1} \end{bmatrix}$$

定義 4.3.1. 次の (I) から (IV) すべてを満たす行列 $[a_{ij}]$ を簡約行列という。

- (I) 零ベクトルとなる行は零ベクトルでない行よりも下段にある,
- (II) 零ベクトルでない行の主成分は 1 である.
- (III) 第 i 行の主成分が第 j_i 列にあるとすれば, $j_1 < j_2 < j_3 < \dots$ が成り立つ. つまり, 各行の主成分は下にある行ほど右側にある.
- (IV) ある行の主成分を含む列について, その列ベクトルの成分は主成分を除いてすべて 0 である. すなわち, (III) における記号および (II) の条件を合わせれば, 第 i 行が零ベクトルでないとき, 第 j_i 列は i 行成分が 1 でそれ以外の成分は 0 となる.

上の性質を満たす行列の名前は参考書によってまちまちであり, 例えば簡約階段行列, 既約行階段行列など様々な呼ばれかたをしている. また, 主成分についても同様で, 行に関するかなめあるいは先頭の列など色々な呼び方がある.

練習 4.3.2. 次の行列のうち簡約行列はどれか.

$$(1) \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (2) \begin{bmatrix} 1 & 2 & -3 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad (3) \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$
$$(4) \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad (5) \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad (6) \begin{bmatrix} 0 & 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

答え. (1) は (I) が成立しない. (2) は 2 列目について (IV) が不成立. (3) は 2 行目において (II) が不成立で, 更に 3 列目において (IV) も成り立たない. (4) は (III) が不成立, (5) は (II) が不成立である. (6) は (I) から (IV) すべてを満たすゆえ簡約行列である.

行列 A に行基本変形を何回かほどこして簡約行列 B に変形させる操作を A を簡約化るといい, B を A の簡約化と呼ぶ. 簡約化の方法は次の手順で得られる. ただし, これはあくまでもアルゴリズムであり, 実際に簡約化を行う際は, 各自の判断で手順を入れ替えたほうが効率が良い場合もある.

- (1) 零ベクトルとなる行たちが下段に並ぶよう行の入れ替えを行う.
- (2) 主成分を含む行について, 第 i 行の主成分が j_i 列目にあるとする. このとき $j_1 \leq j_2 \leq j_3 \leq \dots$ が成り立つように行の入れ替えを行う.
- (3) $j_i = j_{i+1}$ となる場合は i 行の何倍かを $i+1$ 行に加え, $i+1$ 行目の主成分であった $(i+1, j_i)$ -成分を 0 にする.
- (4) $j_1 < j_2 < j_3 < \dots$ となるまで上の (1) から (3) の操作を繰り返す.
- (5) 行のスカラー倍を行い, 各行の主成分を 1 にする.

(6) ある行 (これを第 i 行とする) の主成分を含む列において, その主成分以外の成分が 0 になるよう i 行の何倍かを他の行に加える.

例 4.3.3. 次は簡約行列への行基本変形の一例である. 実際の変形においては, 2 目と 3 目の変形を, 4 目と 5 目の変形を同時に行うなどして, 計算過程をできるだけ省略する.

$$\begin{aligned} \begin{bmatrix} 2 & 0 & 1 & 5 & 4 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} &\xrightarrow{1 \text{ 行} \times \frac{1}{2} \text{ 行}} \begin{bmatrix} 2 & 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} &\xrightarrow{1 \text{ 行} \times \frac{1}{2} \text{ 行}} \begin{bmatrix} 2 & 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ &\xrightarrow{2 \text{ 行} \times \frac{1}{2} \text{ 行} \times 3} \begin{bmatrix} 2 & 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} &\xrightarrow{\text{入れ替え}} \begin{bmatrix} 2 & 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} &\xrightarrow{1 \text{ 行} \times \frac{1}{2}} \begin{bmatrix} 1 & 0 & 0 & \frac{3}{2} & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

なお, 行列の簡約化は唯一通りに定まる. これは, どのような行基本変形の手順を踏もうとも, 最終的に得られる簡約化は必ず一致するということである. この証明は後で行う (定理 6.1.1).

4.4 連立 1 次方程式の解法

簡約行列 $[B|\mathbf{b}]$ における連立 1 次方程式 $B\mathbf{x} = \mathbf{b}$ の解法を具体例を通して説明する. $[B|\mathbf{b}]$ の主成分に関するある条件について, 二つのケースに分けて考える.

(ケース 1): まずは $[B|\mathbf{b}]$ の最後の列 \mathbf{b} に主成分が含まれる場合である. 例えば,

$$[B|\mathbf{b}] = \left[\begin{array}{cccc|c} 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right] \text{ のとき, } B\mathbf{x} = \mathbf{b} \text{ は } \begin{bmatrix} 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

このとき, 最後の行に関する等式を方程式の言葉で書き直せば, $0x_1 + 0x_2 + 0x_3 + 0x_4 = 1$ となる. このような式を満たす \mathbf{x} は存在しないゆえ, したがって方程式 $B\mathbf{x} = \mathbf{b}$ の解は存在しない.

(ケース 2): 次に $[B|\mathbf{b}]$ の最後の列 \mathbf{b} に主成分が含まれない場合を考える. 例えば,

$$[B|\mathbf{b}] = \left[\begin{array}{cccc|c} 0 & 1 & 3 & 0 & 2 & 4 \\ 0 & 0 & 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right] \text{ のとき, } B\mathbf{x} = \mathbf{b} \text{ は, } \begin{bmatrix} 0 & 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \\ 0 \end{bmatrix}.$$

このとき, 主成分のない B の列に対応する変数 x_i を任意定数とおく と簡単に解が得られることをこれから見ていこう. いま, ベクトル \mathbf{x} が方程式 $B\mathbf{x} = \mathbf{b}$ を満たしているとする. この例では主成分を含む B の列は第 2 列と第 4 列であるから, そうでない 1, 3, 5 列に対応する変数 x_1, x_3, x_5 について $c_1 := x_1, c_2 := x_3, c_3 := x_5$ とおこう. すると, 残りの x_2 および x_4 は 1 行目と 2 行目に対応する方程式

$$(\#1) \begin{cases} 0x_1 + 1x_2 + 3x_3 + 0x_4 + 2x_5 = 4, \\ 0x_1 + 0x_2 + 0x_3 + 1x_4 + 1x_5 = 5, \end{cases}$$

を移項することで次を満たさねばならないことが分かる.

$$(\#2) \begin{cases} x_2 = 4 - 3x_3 - 2x_4 = 4 - 3c_2 - 2c_3, \\ x_4 = 5 - x_5 = 5 - c_3, \end{cases}$$

なお、このように簡単に整理できる理由は簡約行列が特殊な形をしているためである。以上により、方程式 $B\mathbf{x} = \mathbf{b}$ の解 \mathbf{x} が存在するとすれば、ベクトル \mathbf{x} は次の形になっていることが分かった:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} c_1 \\ 4 - 3c_2 - 2c_3 \\ c_2 \\ 5 - c_3 \\ c_3 \end{bmatrix}.$$

また、今度は実数 c_1, c_2, c_3 を勝手に選び、上の式によって \mathbf{x} を定めてみよう。このとき \mathbf{x} が方程式 $B\mathbf{x} = \mathbf{b}$ を満たすことは明らかである。何故なら、上でもって \mathbf{x} を定めるということは、式 (♯₂) が満たされるように定めたことを意味し、式 (♯₂) を移項すれば元々の連立方程式 (♯₁) が得られるからである。これまでの議論により、方程式 $B\mathbf{x} = \mathbf{b}$ の解は存在し、しかも解の形は次のもので出してくされている (これを方程式の一般解という) ことが分かった:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} c_1 \\ 4 - 3c_2 - 2c_3 \\ c_2 \\ 5 - c_3 \\ c_3 \end{bmatrix}, \quad \text{ただし } c_1, c_2, c_3 \text{ は任意の定数である.}$$

また、一般解を次のように整理しておくとも後々の議論において都合が良い。

$$\begin{bmatrix} c_1 \\ 4 - 3c_2 - 2c_3 \\ c_2 \\ 5 - c_3 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 4 \\ 0 \\ 5 \\ 0 \end{bmatrix} + c_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ -2 \\ 0 \\ -1 \\ 1 \end{bmatrix}$$

上のような解の表記が何を意味するのか説明するために、次元を落として \mathbb{R}^3 のベクトルについて考えてみよう。まず二つの平行でないベクトル $\mathbf{x}, \mathbf{y} \in \mathbb{R}^3$ を取って固定しよう。次に $a\mathbf{x} + b\mathbf{y}$ なる \mathbb{R}^3 の点 (ただし a, b は任意の数) 全体の集合 H を考えると、 H は \mathbb{R}^3 の中で原点を通る平面になる。さらにもう一つ $\mathbf{z} \in \mathbb{R}^3$ を取り、 $\mathbf{z} + a\mathbf{x} + b\mathbf{y}$ なる点全体を考えれば、これは平面 H をベクトル \mathbf{z} 方向に平行移動した平面である。連立方程式の解全体の集合はこのような形をしている。それは、いまのような考察を \mathbb{R}^n において行えば理解できる。 (m, n) -行列 A による方程式 $A\mathbf{x} = \mathbf{b}$ の解全体を W としよう。一般解の表示における任意定数の数を k とすれば、 W は \mathbb{R}^n の原点を含む k 次元の空間 H を、あるベクトルの方向へ平行移動した集合となる。

例 4.4.1. 上で解いた連立方程式 $\begin{bmatrix} 0 & 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 4 \\ 3 \\ 0 \end{bmatrix}$ の解全体の集合は、 \mathbb{R}^5 の原点を通り、 $c_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ -2 \\ 0 \\ -1 \\ 1 \end{bmatrix}$ で表される 3次元の空間 H を、 $\begin{bmatrix} 0 \\ 4 \\ 0 \\ 5 \\ 0 \end{bmatrix}$ 方向に平行移動した集合 W に一致する。

連立 1 次方程式の解法をまとめておこう。

連立1次方程式の解法 (ガウス・ジョルダンの消去法)

連立1次方程式 $Ax = b$ の解法は次のとおりである。まず拡大係数行列 $[A|b]$ の簡約化 $[B|b']$ を求める。このとき、 $Ax = b$ の解全体と $Bx = b'$ の解全体は一致する。 $[B|b']$ の最後の列 b' に主成分がある場合は方程式の解は存在しない。そうでない場合は解は存在し、方程式 $Bx = b'$ の解は、 B における主成分を含まない列に対応する変数を任意定数とおくことで簡単に表せる。なお、 B のすべての列に主成分がある場合、任意定数の数は0で、方程式の解は唯一つである。また、方程式の一般解をベクトルの和に分解しておく、解全体の集合が見やすくなる。

連立1次方程式の解法を知ることの重要性は、応用の立場からは論ずるまでもない。一方で、線形代数の枠組みにおいては、簡約化が線形写像の像の次元を調べるための手段となる。これに同次形連立1次方程式¹⁰の解における任意定数の個数を合わせることで、線形写像の次元公式を得る。また、次元公式は、線形写像の準同型定理を次元の立場から理解する上でかかせない。そして、準同型定理は線形空間の枠組みのみならず、群論や環論など様々な代数理論の上で認められる定理であり、抽象代数学における基本的な考え方となる。

さて、いま述べたことと重複するが、後期の講義において、行基本変形や連立1次方程式の一般解が度々登場する。その際に、講義中にいちいち復習する余裕はないゆえ、本節で述べたことを自ら説明できるくらい咀嚼していることが、今後の学習において望まれる。

¹⁰同次形の方程式は6.2項で扱う。

5 可逆行列

ここでは逆行列を持つ行列の性質について詳しく扱う。また、前節で学んだ行基本変形を理論的な立場から再考する。これによって、行列の簡約化を用いた逆行列の解法が理解される。

5.1 逆行列の性質

逆行列の定義をもう一度書いておこう。

定義 5.1.1. n 次正方行列 A が可逆 (invertible) である (または正則 (non-singular, regular) である) とは、 $AB = E = BA$ を満たす n 次正方行列 B が存在することである。このとき、 B を A の逆行列という。

なお、線形写像の言葉に戻すと、逆行列とは、逆写像 (逆関数) と呼ばれるものに相当している。

命題 5.1.2. A の逆行列は唯一つである。

Proof. B, C が共に A の逆行列であるとすると、 $B = C$ が簡単に確かめられる。実際、 $B = BE = B(AC) = (BA)C = EC = C$ である。□

このように、条件を満たすものが唯一つしかないことを示す場合、条件を満たすものを二つ挙げ、それが一致することを言うのは数学の常套手段の一つである。ほかに、条件を満たし互いに異なるものがあると仮定し、矛盾を導くという手もある。

さて、可逆行列 A の唯一つの逆行列を A^{-1} と表すことにしよう。今後の議論の中で A^{-1} という記号が出てきたときは、それは A が可逆行列であることを前提とした議論であることに注意せよ。

例 5.1.3. 逆行列に関する簡単な性質をここでまとめておく。

- (1) E は E の逆行列である。
- (2) A の逆行列を B とすれば、 B の逆行列は A である。つまり B も可逆行列であり、 $(A^{-1})^{-1} = B^{-1} = A$ が成り立つ。
- (3) A, B が共に可逆ならば AB も可逆であり、 $(AB)^{-1} = B^{-1}A^{-1}$ である。実際、 $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E$ 。また $(B^{-1}A^{-1})(AB) = E$ も同様の計算で確かめられる。
- (4) $AB = O$ なる行列 $B \neq O$ が存在すれば、 A は可逆でない。何故なら、仮に可逆であるとする、 $AB = O$ の両辺に左から A^{-1} を掛けることで $B = O$ となり、これは $B \neq O$ に矛盾するからである。ここで、 B は正方行列でなくてもよいことに注意せよ。この議論は逆行列を持たない正方行列の存在も述べている。例えば、 $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ とすれば $A^2 = O$ ゆえ A は可逆でない。
- (5) 可逆行列 A について、 $(A^{-1})^k$ のことを A^{-k} と書き、また $A^0 = E$ と書くとすれば、整数 p, q について指数法則 $A^{p+q} = A^p A^q$ および $(A^p)^q = A^{pq}$ が成り立つ。

5.2 行基本変形再考

(m, n) -行列 A の行基本変形について再考する。まず次のような特別な正方行列を考えよう。

定義 5.2.1. 次の三種類の m 次正方行列 $S_m(i; r)$, $W_m(i, j)$, $K_m(i, j; r)$ を基本行列という。なお、この記号は、この講義でのみ通じる記号である。

- (1) $S_m(i; r)$: E_m の i 行目を r 倍した行列。ただし $r \neq 0$ とする。

(2) $W_m(i, j)$: E_m の i 行と j 行を入れ替えた行列.

(3) $K_m(i, j; r)$: E_m において, i 行目の r 倍を j 行目に加えた行列.

基本行列を左から掛けることは, 行基本変形を行っていることに他ならない. すなわち次が成り立つ. 各自, 実際に計算して確かめてみる.

命題 5.2.2. (m, n) -行列 A と基本行列の積について, 次が成り立つ.

(1) $S_m(i; r)A$ は A の i 行目を r 倍した行列である.

(2) $W_m(i, j)A$ は A の i 行と j 行を入れ替えた行列である.

(3) $K_m(i, j; r)A$ は A の i 行目の r 倍を j 行目に加えた行列である.

したがって, 行基本変形によりある行列を別の行列に変形させることは, いくつかの基本行列を左から何度もかけることに他ならない. また, 基本行列自身に基本変形をほどこすことを考えると, 上の命題から次が直ちに分かる.

例 5.2.3. 基本行列の逆行列は次のようになる.

(1) $S_m(i; r^{-1})S_m(i; r) = E_m = S_m(i; r)S_m(i; r^{-1})$. ゆえに $S_m(i; r)^{-1} = S_m(i; r^{-1})$.

(2) $W_m(i, j)W_m(i, j) = E_m$. ゆえに $W_m(i, j)^{-1} = W_m(i, j)$.

(3) $K_m(i, j; -r)K_m(i, j; r) = E_m = K_m(i, j; r)K_m(i, j; -r)$. ゆえに $K_m(i, j; r)^{-1} = K_m(i, j; -r)$.

行列 A が k 回の行基本変形によって B に変形できるとする. 行基本変形は左から基本行列を掛けることに他ならないから, このことは次が成り立つことを意味する:

$$X_k X_{k-1} \cdots X_2 X_1 A = B,$$

ここで, 各 X_i は A を行基本変形する際に実際に行った操作に対応する基本行列である. このとき, 可逆行列たちの積 $P = X_k X_{k-1} \cdots X_2 X_1$ は可逆であり, $PA = B$ と表せる. また, B に $X_k^{-1}, X_{k-1}^{-1}, \dots, X_1^{-1}$ に対応する基本変形を順次ほどこせば A を得る. 実際,

$$X_1^{-1} X_2^{-1} \cdots X_{k-1}^{-1} X_k^{-1} B = (X_1^{-1} X_2^{-1} \cdots X_{k-1}^{-1} X_k^{-1})(X_k X_{k-1} \cdots X_2 X_1) A = EA = A.$$

以上を整理すると次のような主張になる.

命題 5.2.4. (m, n) -行列 A が行基本変形により B に変形するならば, $PA = B$ を満たす m 次可逆行列 P が存在する. また, B を行基本変形することにより A に戻すこともできる.

行基本変形と基本行列の関係から, 可逆行列の逆行列を求めることができる. これを次項で見よう.

5.3 逆行列の求め方

ここでは, n 次正方行列 A に対して $BA = E$ を満たす正方行列 B の求め方を考察する. まず, 行列 A が k 回の行基本変形によって E に変形できたと仮定しよう. すなわち, A の簡約化は E であり, また前項での考察により次のように書ける:

$$X_k X_{k-1} \cdots X_2 X_1 A = E,$$

ここで, 各 X_i は A を行基本変形する際に実際に行った操作に対応する基本行列である. したがって, $B = X_k X_{k-1} \cdots X_2 X_1$ とおけば $BA = E$ を満たすことが分かる. この B を求めるには次の式を考えればよい.

$$B = X_k X_{k-1} \cdots X_2 X_1 E.$$

この式は, A を行基本変形によって E に変形した操作と全く同じ手順で E を変形すると B が求まることを述べている. なお, A の E への変形を確認した後で, 同様の手順で E を変形するという二度手間は不要である. なぜなら A と E を横に並べた $(n, 2n)$ -行列 $[A|E]$ についての行基本変形を行い, 左半分が単位行列となる $[E|X]$ が得られれば,

$$[E|X] = B[A|E] = [BA|BE] = [BA|B].$$

つまり X は我々が求める B に他ならない. また, $[E|X]$ は明らかに簡約行列であり, したがって $[A|E]$ の簡約化である.

次の定理は行列式の項目に入ってから証明する. この定理を認めれば, いま求めた B が A の逆行列であることが分かる.

定理 5.3.1. 二つの n 次正方行列 A, B について $BA = E$ が成り立てば $AB = E$ も成り立つ. したがって A, B は共に可逆であり, $A^{-1} = B$.

逆行列の求め方.

A を n 次正方行列とする. A の逆行列を求めるには, $(n, 2n)$ -行列 $[A|E_n]$ を簡約化すればよい. $[A|E_n]$ の簡約化が $[E_n|B]$ なる形をしているならば, B が A の逆行列となる.

ちなみに, $[A|E_n]$ の簡約化が $[E_n|B]$ という形にならない場合, すなわち A の簡約化が E_n でない場合は A は可逆ではない. その理由は次節で述べる定理 6.2.2 による. これを認めれば, 任意の可逆行列の簡約化は単位行列であり, したがって次を得る.

定理 5.3.2. 可逆行列は基本行列の積で表せる.

Proof. B を可逆行列とし, $A := B^{-1}$ とする. 可逆行列 A を行基本変形で単位行列に変形する手順に対応する基本行列たちの積は, これまでの議論により A の逆行列, すなわち B に一致することが分かっている. 以上より B は基本行列の積で表すことができる. \square

6 行列の階数

連立方程式の一般解の任意定数の数と関係する量として、行列の階数と呼ばれる概念がある。実は、階数とは線形写像の像の次元として本来は定義されるものである。しかしながら、ここでは行列の言葉に翻訳したうえでの定義を述べなければならず、そのためには簡約化の一意性について言及する必要がある。

階数を用いると連立方程式の解に関する言明を簡潔に述べることができる(命題 6.2.1)。しかし、だからといって、階数を用いて述べられた命題を丸暗記しても理解が深まることはない。階数という便利な言葉に頼らずに、連立方程式の解法がどんな手順であったか常に頭の中で意識しつつ命題を解釈してもらいたい。

6.1 簡約化の一意性

定理 6.1.1. 行列の簡約化は唯一通りに定まる。

Proof. 列の数に関する帰納法で示す。まず、列の数が 1 の場合、すなわち列ベクトル \boldsymbol{x} の簡約化について考える。列ベクトルのうちで簡約なものは、その定義から 1 行成分が 1 で他の成分がすべて 0 の列ベクトル \boldsymbol{e}_1 か $\mathbf{0}$ に限る。 $\boldsymbol{x} = \mathbf{0}$ の場合、 $\mathbf{0}$ に基本変形をいくらほどこしても変化せず、 $\mathbf{0}$ の簡約化は $\mathbf{0}$ 自身以外にありえない。また、 $\boldsymbol{x} \neq \mathbf{0}$ の場合、 \boldsymbol{x} を $\mathbf{0}$ に行基本変形することはできない。何故なら、もし $\mathbf{0}$ が \boldsymbol{x} の簡約化であるならば、命題 5.2.4 により $\mathbf{0}$ を行基本変形して $\boldsymbol{x} \neq \mathbf{0}$ が得られるが、先の議論によりこれは不可能だからである。ゆえに \boldsymbol{x} の簡約化は \boldsymbol{e}_1 のみである。以上より、列ベクトルの簡約化は唯一つであることが分かった。

列の数が n なる行列について簡約化が一意的であると仮定し、列の数が $n+1$ の行列についてもそうであることを示そう。 A を (m, n) -行列、 \boldsymbol{a} を m 次列ベクトルとし、 $(m, n+1)$ -行列 $[A|\boldsymbol{a}]$ の簡約化について考える。 $[B|\boldsymbol{b}]$ および $[C|\boldsymbol{c}]$ を $[A|\boldsymbol{a}]$ の簡約化としよう。このとき、 (m, n) -行列 B, C は共に簡約行列であり、とくに A の簡約化であるから、帰納法の仮定により $B = C$ である。 B の中にどの行の主成分も含まない列がある場合とそうでない場合に分けて考えよう。

まずは、 B の第 j 列が主成分を含まない場合である。各 A, B, C から第 j 列を除いた $(m, n-1)$ -行列をそれぞれ A', B', C' とする。このとき、 (m, n) -行列 $[B'|\boldsymbol{b}']$ は簡約行列であり、これはとくに行列 $[A'|\boldsymbol{a}']$ の簡約化である。 $B = C$ ゆえ同様のことが C' についても成り立ち、 $[C'|\boldsymbol{c}']$ も $[A'|\boldsymbol{a}']$ の簡約化となる。したがって帰納法の仮定より、 $[B'|\boldsymbol{b}'] = [C'|\boldsymbol{c}']$ である。すなわち、 $\boldsymbol{b} = \boldsymbol{c}$ ゆえ $[B|\boldsymbol{b}] = [C|\boldsymbol{c}]$ 。

次に、 B のどの列にも主成分が含まれている場合を考える。すなわち、 $[B|\boldsymbol{b}]$ および $[C|\boldsymbol{c}]$ が次の形をしている場合である：

$$\left[\begin{array}{ccc|c} 1 & & & * \\ & \ddots & & * \\ & & 1 & * \\ & & & * \end{array} \right] = \left[\begin{array}{cc|c} E_n & & * \\ O_{m-n,n} & & * \end{array} \right]$$

更に次の二つに場合分けをして考える。

- (i) $\boldsymbol{b}, \boldsymbol{c}$ がともに、ある主成分を含む場合。

この場合は簡約行列の定義から、 $\boldsymbol{b}, \boldsymbol{c}$ は $n+1$ 行目が 1 でそれ以外の成分が 0 の列ベクトルであり、 $\boldsymbol{b} = \boldsymbol{c}$ を得る。

- (ii) $\boldsymbol{b}, \boldsymbol{c}$ のいずれか一方が、主成分を含まない場合。

仮に \boldsymbol{b} が主成分を含まないとして話を進める。このとき、 $[B|\boldsymbol{b}]$ および $[C|\boldsymbol{c}]$ は次の形をしている。

$$[B|\boldsymbol{b}] = \left[\begin{array}{cc|c} E_n & & \boldsymbol{b}' \\ O_{m-n,n} & & O_{m-n,1} \end{array} \right], \quad [C|\boldsymbol{c}] = \left[\begin{array}{cc|c} E_n & & \boldsymbol{c}'_1 \\ O_{m-n,n} & & \boldsymbol{c}'_2 \end{array} \right].$$

$[B|\mathbf{b}], [C|\mathbf{c}]$ はともに $[A|\mathbf{a}]$ を行基本変形を繰り返して得られる行列である。ゆえに $[B|\mathbf{b}]$ に行基本変形を繰り返すことで $[C|\mathbf{c}]$ を得ることができる。したがって、ある m 次可逆行列 X によって $X[B|\mathbf{b}] = [C|\mathbf{c}]$ となる (命題 5.2.4)。 X を次のように分割する:

$$X = \begin{bmatrix} P_{n,n} & Q_{n,m-n} \\ R_{m-n,n} & S_{m-n,m-n} \end{bmatrix} = \begin{bmatrix} P & Q \\ R & S \end{bmatrix},$$

ここで、真ん中の行列に現れる P, Q, R, S の添え字は行列のサイズを意味し、煩雑ゆえ以降は省略する。 $X[B|\mathbf{b}]$ を計算すると次のようになる。

$$X[B|\mathbf{b}] = \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \left[\begin{array}{c|c} E_n & \mathbf{b}' \\ \hline O_{m-n,n} & O_{m-n,1} \end{array} \right] = \begin{bmatrix} P & P\mathbf{b}' \\ R & R\mathbf{b}' \end{bmatrix}.$$

$[C|\mathbf{c}] = X[B|\mathbf{b}]$ について成分比較すれば

$$\left[\begin{array}{c|c} E_n & \mathbf{c}'_1 \\ \hline O_{m-n,n} & \mathbf{c}'_2 \end{array} \right] = [C|\mathbf{c}] = X[B|\mathbf{b}] = \begin{bmatrix} P & P\mathbf{b}' \\ R & R\mathbf{b}' \end{bmatrix},$$

$P = E_n, R = O_{m-n,n}$ が得られる。ゆえに $\mathbf{c}'_1 = P\mathbf{b}' = E_n\mathbf{b}' = \mathbf{b}', \mathbf{c}'_2 = R\mathbf{b}' = O_{m-n,n}\mathbf{b}' = O_{m-n,1}$ である。つまり、 $\mathbf{b} = \mathbf{c}$ が示された。

\mathbf{c} が主成分を含まない場合は、 \mathbf{b} と \mathbf{c} の役割を入れ替えていまと同様の議論を行えばよい。

以上により、いずれの場合においても $[B|\mathbf{b}] = [C|\mathbf{c}]$ となる。すなわち、 $(m, n+1)$ -行列 A の簡約化は唯一通りに定まる。 \square

定義 6.1.2. A の簡約化を B とする。次で定める三つの数はすべて同じ値となり、これを A の階数 (**rank**) とよび $\text{rank } A$ と書く。

- (1) B の零ベクトルでない行の数,
- (2) B の主成分の数,
- (3) B の主成分を含む列の数.

上で定める数のうち、一般の行列においても (1) と (2) は等しい。これらが (3) と等しいのは、簡約行列 B において主成分を二つ以上含む列は存在しないからである。

仮に A の簡約化が二通りあるとし、それらの主成分の数が異なっていたとすれば A の階数を定めようがない。また、これは連立 1 次方程式において任意定数の数が異なる二通りの一般解が存在することも意味する。このようなことが起こり得ないという主張が簡約化の一意性にほかならない。

A を行基本変形することで C が得られるならば、 A と C の簡約化は一致する。したがって、 $\text{rank } A = \text{rank } C$ である。また、 (m, n) -行列 A について次は明らかである。

$$\text{rank } A \leq \min\{m, n\}.$$

ここで \min は最小値を表す記号である。すなわち、実数を要素とする集合 X に対して、 X の中で最も小さい数が存在するとき、これを X の最小値とよび $\min X$ と書く。同様に X の最大値も定められ、これを $\max X$ と書く。

6.2 連立 1 次方程式と階数

連立 1 次方程式 $A\mathbf{x} = \mathbf{b}$ の解の形は、拡大係数行列 $[A|\mathbf{b}]$ の簡約化の形によって、解が存在する場合とそうでない場合、および解が存在する場合における任意定数の数が決まるのであった。これを階数の言葉を用いて言いなおすと次の命題になる。

命題 6.2.1. A を (m, n) -行列とする. 連立 1 次方程式 $Ax = b$ において次が成り立つ.

- (1) $Ax = b$ の解が存在するための必要十分条件は $\text{rank}[A|b] = \text{rank } A$ である.
- (2) $Ax = b$ の解が存在するとき, 一般解の任意定数の個数は $n - \text{rank } A$ である.
- (3) $Ax = b$ の解が唯一つであるための必要十分条件は, $\text{rank}[A|b] = \text{rank } A = n$ である.

とくに, A が正方行列の場合は逆行列との関係を含めて次の主張を得る.

定理 6.2.2. n 次正則行列 A において次は同値である.

- (1) $\text{rank } A = n$, (2) A の簡約化は E である,
- (3) 任意の n 次列ベクトル b について方程式 $Ax = b$ は唯一つの解を持つ,
- (4) 方程式 $Ax = 0$ は唯一つの解 0 を持つ, (5) A は可逆である.

Proof. (1) から (4) までの同値性は既に述べたことのまとめにほかならない. しかしながら, 確認のために証明する.

(1) \Rightarrow (2): $\text{rank } A = n$ とすれば, A の簡約化 B の主成分の数は n である. B は $n \times n$ 行列であるゆえ, $B = E$ となる.

(2) \Rightarrow (3): まず $\text{rank } A = \text{rank } E = n$ に注意する. $[A|b]$ の簡約化を $[E|b']$ とすれば, $\text{rank}[E|b'] = n$ である. ゆえに $\text{rank}[A|b] = \text{rank}[E|b'] = n = \text{rank } A$. よって, 命題 6.2.1(3) より方程式は唯一つの解を持つ.

(3) \Rightarrow (4): (4) は (3) における $b = 0$ という特別の場合ゆえ明らか.

(4) \Rightarrow (1): 仮定より, 一般解の任意定数の数は 0 である. したがって, 命題 6.2.1(2) より $0 = n - \text{rank } A$. ゆえに $\text{rank } A = n$.

(2) \Rightarrow (5): 逆行列の求め方より明らか. ただしこれは, まだ証明していない定理 5.3.1 を認めたくえで話であることを忘れないこと.

(5) \Rightarrow (4): $x = 0$ が方程式 $Ax = 0$ の解であることは明らかである. また, 解の一意性も直ちに分かる. 実際, $Ax = 0$ の両辺に左から A^{-1} を掛けることで $x = 0$ を得る.

以上によって, すべての条件の同値性が示された. □

いまの定理において $Ax = 0$ なる方程式が現れた. このような型の方程式を同次形 (または斉次形) の方程式という. 証明の中でも述べたように, 同次形の方程式は $x = 0$ を解に持つ. 連立 1 次方程式の解法を同次形の場合に適用してみよう. 拡大係数行列 $[A|0]$ の簡約化は $[B|0]$ なる形になっている. ゆえに一般解の形は

$$c_1 \mathbf{a}_1 + c_2 \mathbf{a}_2 + \cdots + c_k \mathbf{a}_k \quad \text{ただし } c_1, \dots, c_k \text{ は任意定数.}$$

となることが分かる. すなわち, 解全体の集合は, \mathbb{R}^n の原点を含む k 次元の空間となる.

同次形の方程式とそうでない方程式の解の間には次のような関係がある.

命題 6.2.3. 方程式 $Ax = b$ の解 a を一つ取って固定しよう. このとき次が成り立つ.

- (1) 方程式 $Ax = 0$ の任意の解 z に対し, $a + z$ は方程式 $Ax = b$ の解である.
- (2) 方程式 $Ax = b$ の任意の解 y は, 方程式 $Ax = 0$ のとある解 z を用いて $y = a + z$ と表せる.

Proof. (1): z を $Ax = 0$ の解とすると, $A(a + z) = Aa + Az = b + 0 = b$. ゆえに, $a + z$ は方程式 $Ax = b$ の解である.

(2): y を $Ax = b$ の解とする. ここで $z := y - a$ とおこう. このとき z は $Ax = 0$ の解である. 何故なら, $Az = A(y - a) = Ay - Aa = b - b = 0$ ゆえ z は $Az = 0$ を満たすからである. また, z の定め方から $y = a + z$ であり, 我々は主張を得た. □

上の命題は、同次形の方程式の解全体の集合を W とすれば、 $A\mathbf{x} = \mathbf{b}$ の解全体の集合は W を \mathbf{a} 方向に平行移動した集合に一致することを言っている。方程式 $A\mathbf{x} = \mathbf{0}$ の解法は、方程式 $A\mathbf{x} = \mathbf{b}$ の解法より幾分か易しい。そこで、あらかじめ易しい方程式 $A\mathbf{x} = \mathbf{0}$ の一般解を求めておき、更に、何らかの方法で $A\mathbf{x} = \mathbf{b}$ の解 \mathbf{a} を一つでよいから見つけてくる。すると、 $A\mathbf{x} = \mathbf{b}$ の一般解は、 $A\mathbf{x} = \mathbf{0}$ の解の \mathbf{a} 方向への平行移動によってすべて得られるのである。

しかし、既に連立1次方程式の一般解の解法を知っている我々にとっては、このような考え方は不要にも思える。そこで、次の命題を考えてみよう。

命題 6.2.4. $\alpha(x), \beta(x), \gamma(x), \delta(x)$ を既知の関数とし、2階微分可能な未知の関数 $f(x)$ に関する次の二つの微分方程式¹¹を考える。

$$(I) \alpha(x)f''(x) + \beta(x)f'(x) + \gamma(x)f(x) = \delta(x), \quad (II) \alpha(x)f''(x) + \beta(x)f'(x) + \gamma(x)f(x) = 0.$$

方程式 (I) の解 $a(x)$ を一つとって固定しよう。このとき次が成り立つ。

- (1) 微分方程式 (II) の任意の解 $z(x)$ に対し、 $a(x) + z(x)$ は微分方程式 (I) の解である。
- (2) 微分方程式 (I) の任意の解 $y(x)$ は、微分方程式 (II) のとある解 $z(x)$ を用いて $y(x) = a(x) + z(x)$ と表せる。

Proof. (1) : $z(x)$ を (II) の解とすると、

$$\begin{aligned} & \alpha(x)(a(x)+z(x))'' + \beta(x)(a(x)+z(x))' + \gamma(x)(a(x)+z(x)) \\ &= \left(\alpha(x)a''(x) + \beta(x)a'(x) + \gamma(x)a(x) \right) + \left(\alpha(x)z''(x) + \beta(x)z'(x) + \gamma(x)z(x) \right) \\ &= \delta(x) + 0 = \delta(x). \end{aligned}$$

ゆえに、 $a(x) + z(x)$ は微分方程式 (I) の解である。

(2) : $y(x)$ を (I) の解とする。ここで $z(x) := y(x) - a(x)$ とおこう。このとき $z(x)$ は (II) の解である。何故なら、

$$\begin{aligned} & \alpha(x)(y(x)-a(x))'' + \beta(x)(y(x)-a(x))' + \gamma(x)(y(x)-a(x)) \\ &= \left(\alpha(x)y''(x) + \beta(x)y'(x) + \gamma(x)y(x) \right) - \left(\alpha(x)a''(x) + \beta(x)a'(x) + \gamma(x)a(x) \right) \\ &= \delta(x) - \delta(x) = 0. \end{aligned}$$

ゆえ $z(x)$ は (II) を満たすからである。また、 $z(x)$ の定め方から $y(x) = a(x) + z(x)$ であり、我々は主張を得た。 □

命題 6.2.3 と 6.2.4 の証明が平行であることに着目せよ。これはベクトル \mathbf{x} に対して $A\mathbf{x}$ を対応させる操作と、関数 $f(x)$ に対して関数 $\alpha(x)f''(x) + \beta(x)f'(x) + \gamma(x)f(x)$ を対応させる操作が共に線形性を満たしていることに起因する。このように、似たような証明を何度も繰り返し行う手間を省くために、我々は線形空間と呼ばれる代数構造を提案することになる。

¹¹この形の微分方程式は、線形常微分方程式と呼ばれている。

7 行列式とは何か

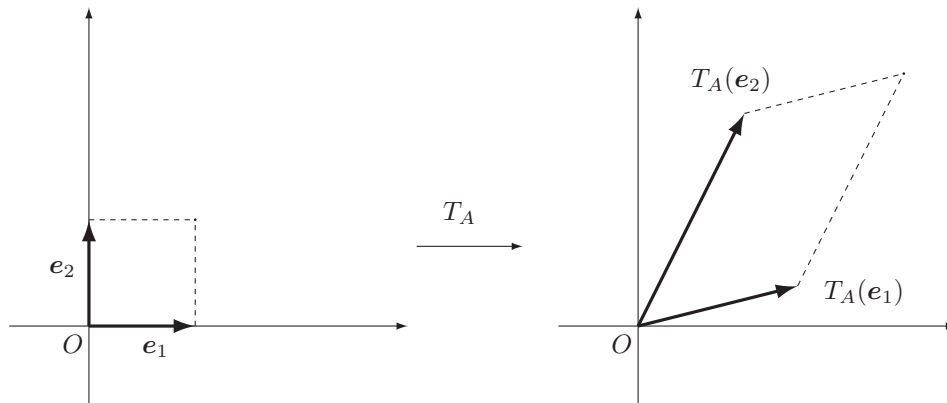
行列式とは、正方行列に対して定められるある量のことであり、 $\det A$ もしくは $|A|$ と書く。その定義の詳細は一言で述べるには難しく、厳密な定義については後で議論するとして、本節では行列式を持つ意味、および微積分学における扱われ方について導入的な紹介をしよう。

行列は matrix の和訳であり行列式は determinant の和訳である。このように外国語と和訳でニュアンスが異なるのは歴史的な事情がある。もともと行列と行列式は別の目的をもって定められたものであった。歴史的には行列式のほうが先に生まれた。それは連立1次方程式の解の公式(クラメルの公式)を得るために考え出されたものである。一方、matrix という用語は行列式の理論の中で生まれたのちに、数を矩形に並べた概念の総称として用いられるようになった。その後、線形写像の数値化に相当するものとして演算が定められ、今日の行列の定義に至っている。これら二語の和訳も紆余曲折があったが、これらの関係性が十分に理解されたことにより、行列・行列式なる訳が定着した。

行列式の意味を理解する見方は大きく分けて二つある。したがって、行列式の定義の仕方にも二つの方法があると考えてよいだろう。一つは歴史的な経緯である方程式論から見る方法で、もう一つは幾何学的な観点によるものである。後者のほうがイメージが描きやすいゆえ、まずそちらから解説しよう。

7.1 線形写像の面積拡大率

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ とし、線形写像 $T_A: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ を $T_A(\mathbf{x}) := A\mathbf{x}$ で定める。このとき、 $\det A$ とは、 \mathbb{R}^2 における1辺の長さが1の単位正方形の面積が T_A で写像されると何倍になるかを表す量である。すなわち、行列式とは線形写像の面積拡大率である。



$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad T_A(\mathbf{e}_1) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}, \quad T_A(\mathbf{e}_2) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix}.$$

単位正方形とは $\mathbf{e}_1, \mathbf{e}_2$ で張られる平行四辺形のことであり、これを T_A で写像すると $T_A(\mathbf{e}_1)$ と $T_A(\mathbf{e}_2)$ で張られる平行四辺形になる。ここで、積分において負の面積を考えたように、平行四辺形についても向きを込めた面積を導入する。面積の符号は、半周未満の回転によってベクトル $T_A(\mathbf{e}_1)$ を $T_A(\mathbf{e}_2)$ に重ねるとき、その回転が反時計回りになるか時計回りになるかで判断すればよい。 $\mathbf{e}_1, \mathbf{e}_2$ について同じことを考えればこの回転は反時計回りであるから、 $T_A(\mathbf{e}_1), T_A(\mathbf{e}_2)$ についても反時計回りならば正、そうでなければ負の面積を対応させる。図1の平行四辺形の面積は、原点と $T_A(\mathbf{e}_1) + T_A(\mathbf{e}_2)$ を頂点に持つ長方形の面積からいくつかの台形や三角形の面積を引くことで得られるから、

$$\begin{aligned} \begin{vmatrix} a & b \\ c & d \end{vmatrix} &= \text{“}T_A(\mathbf{e}_1) \text{ と } T_A(\mathbf{e}_2) \text{ で張られる平行四辺形の面積”} \\ &= (a+b)(c+d) - \left(\frac{ac}{2} + \frac{(c+c+d)b}{2} + \frac{bd}{2} + \frac{(b+a+b)c}{2} \right) \\ &= ac + ad + bc + bd - \frac{ac + 2cb + db + bd + 2bc + ac}{2} = ad - bc. \end{aligned}$$

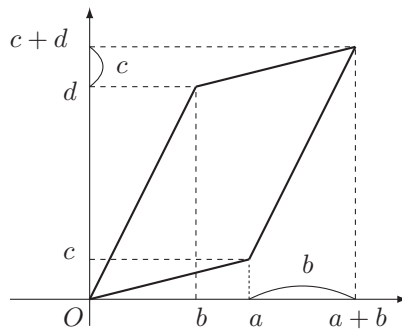


図 1: 平行四辺形の各頂点の座標表示

一般の n 次正方行列 A の行列式も同様に与えられる。すなわち、線形写像 $T_A: \mathbb{R}^n \rightarrow \mathbb{R}^n$ を $T_A(\boldsymbol{x}) := A\boldsymbol{x}$ で定め、 T_A の体積拡大率を $\det A$ と定める。ここで、1次元において長さ、2次元において面積、3次元において体積とそれぞれ異なる呼ばれ方をしていた各次元に関する量は、4次元以上においてはすべて体積と呼ぶことにする。また n 次元空間において、次元が n 未満の図形を面と呼ぶことにしよう。3次元空間における2次元の図形が通常の意味での面であった。 $n = 3$ の場合、 $\det A$ は A の3つの列ベクトルで張られる平行六面体の体積に相当し、図形の体積計算が得意な者は次を得ることができるだろう:

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

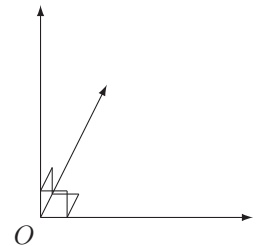
体積拡大率を直接求める方法で4次以上の行列式を定めるのは難しい。 \mathbb{R}^n において、 n 個のベクトルで張られる図形 (これは $n - 1$ 次元の $2n$ 個の面で囲まれる) の体積の計算式はかなり複雑であり、また、普段3次元の空間に住む我々が高次元の図形を想像すること自体に困難な部分がある。そこで、 n 次元の図形の体積が持つべき性質をいくつか列挙することにより、その性質をもとに低次元の図形の体積計算に帰着させることで、求める体積を得るという方法が考えられる。この具体的方法については後で述べることにしよう。

さて、行列式が体積拡大率を意味するのであれば、 T_E は元を動かさない恒等写像ゆえ $|E| = 1$ である。また、 $|AB|$ は合成写像 $T_A \circ T_B$ の体積拡大率であるから、積をとって $|AB| = |A||B|$ となる。よって A が可逆であるとき、 $|A||A^{-1}| = |AA^{-1}| = |E| = 1$ より $|A^{-1}| = |A|^{-1}$ 、とくに $|A| \neq 0$ である。逆に、 $|A| \neq 0$ ならば A が可逆であることも後で示され、したがって $|A|$ は A が可逆であるかどうかを知るための指標となる。

よりみち (多次元空間を見る.)

n 本のベクトルで張られる n 次元の図形の体積計算を考えるうえで最も基本的な指針となるのはカヴァリエリの原理 (切り口の面積が常に等しい2つの立体の体積は等しい) である. これにより, 角柱や円柱など柱状の図形の体積公式を得る. すなわち, n 次元柱の n 次元体積は, 底面となる $n-1$ 次元図形の面積 ($n-1$ 次元体積) に高さを掛けたものに等しい. これは, 特別な形の n 次行列式は $n-1$ 次行列式の計算に帰着できることを意味している. 更に, カヴァリエリの原理を順次適用することで計算できる n 次行列式の種類が増えていき, 最終的にはすべての行列式の値が定められる. 実は, 行列式の実際の計算演習においても, これと同等のことを繰り返すことになる.

ところで, 3次元の空間に住む我々が n 次元の世界を想像する何か良い方法はないだろうか. 右は, 原点 O において3本の直線が互いに垂直に交わる様子を図示したものである. ただし, これは2次元の平面に描かれた模式的なものであり, 正確な図ではない. しかしながらこのことは, 3次元空間において模式的に4次元を見る方法があることを示唆している. 4次元空間は座標軸が4つあるから, 4本の直線が O で互いに垂直に交わることができる. この図においてそのような直線を1本加えるにはどうすればよいか考えてみよう.



物理学における第4の次元とは時間のことであった. 時間の流れを記録したものの例として, 我々は音楽や動画などを知っている. とくに動画には空間と時間の両方が記録されており, 4次元を理解するには最良の例である. 映画のフィルムを1枚ずつ重ねて束にしてみよう. これはフィルムと並行な方向に空間 (2次元のフィルムに射影された3次元空間) が広がっており, 束の重なる方向が時間を表している. このことから4次元の世界とは, フィルムのように薄っぺらくなった3次元空間たちの束を重ねた空間であると想像できる. したがって, 先の図における第4の方向とは, 束が重なって高くなる方向, すなわち, この紙面に垂直に鉛筆を立てた方向ということになる.

それでは, 5本の直線が互いに垂直に交わる5次元の図を描くにはどうすればよいだろうか. それは先程の鉛筆を立てた状態, すなわち4本の直線が垂直に交わった状態を写真に撮って印刷し, 4次元空間を薄っぺらい空間とみなし, 写真が印刷された紙に垂直な方向に新たな鉛筆を立てればよい. これを順次繰り返して, 我々は多次元空間の模式図を得る.

7.2 クラメル公式

歴史的には, 行列式とは連立1次方程式の解の公式を与えるための道具として生み出されたのであった. そこで, 今度はこの方針をたどってみよう. 方程式の解が唯一であることは A が可逆であることと同値であり (定理 6.2.2), これは $|A| \neq 0$ と同値であることは先に述べた通りである.

簡単のため, 次の2変数連立1次方程式が唯一解を持つ場合を考える:

$$A := \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}.$$

いま, A は可逆としているから $|A| = ad - bc \neq 0$, つまり $a \neq 0$ または $c \neq 0$ である. $a \neq 0$ の場合について拡大係数行列を簡約化してみよう. $a \neq 0$ ゆえ a で割り算ができることに注意すると,

$$\begin{aligned} \left[\begin{array}{cc|c} a & b & y_1 \\ c & d & y_2 \end{array} \right] &\rightarrow \left[\begin{array}{cc|c} 1 & \frac{b}{a} & \frac{y_1}{a} \\ c & d & y_2 \end{array} \right] \rightarrow \left[\begin{array}{cc|c} 1 & \frac{b}{a} & \frac{y_1}{a} \\ 0 & d - \frac{bc}{a} & y_2 - \frac{y_1c}{a} \end{array} \right] = \left[\begin{array}{cc|c} 1 & \frac{b}{a} & \frac{y_1}{a} \\ 0 & \frac{ad-bc}{a} & \frac{ay_2-y_1c}{a} \end{array} \right] \\ &= \left[\begin{array}{cc|c} 1 & \frac{b}{a} & \frac{y_1}{a} \\ 0 & \frac{|A|}{a} & \frac{ay_2-y_1c}{a} \end{array} \right] \rightarrow \left[\begin{array}{cc|c} 1 & \frac{b}{a} & \frac{y_1}{a} \\ 0 & 1 & \frac{ay_2-y_1c}{|A|} \end{array} \right] \rightarrow \left[\begin{array}{cc|c} 1 & 0 & \frac{y_1}{a} - \frac{ay_2-y_1c}{|A|} \frac{b}{a} \\ 0 & 1 & \frac{ay_2-y_1c}{|A|} \end{array} \right]. \end{aligned}$$

ここで、上式の最後の (1, 3)-成分は

$$\begin{aligned} \frac{y_1}{a} - \frac{ay_2 - y_1c}{|A|} \cdot \frac{b}{a} &= \frac{y_1|A| - (ay_2 - y_1c)b}{|A|a} = \frac{y_1(ad - bc) - (ay_2 - y_1c)b}{|A|a} \\ &= \frac{y_1ad - y_1bc - ay_2b + y_1cb}{|A|a} = \frac{y_1ad - ay_2b}{|A|a} = \frac{y_1d - y_2b}{|A|}. \end{aligned}$$

以上より、行列式の言葉で方程式の解を表すと次のようになる:

$$x_1 = \frac{\begin{vmatrix} y_1 & b \\ y_2 & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}, \quad x_2 = \frac{\begin{vmatrix} a & y_1 \\ c & y_2 \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}.$$

また、 $c \neq 0$ の場合も同様の行基本変形により上の解を得る (各自確かめよ). 上の解の公式をクラメルの公式という. 3変数の場合は次で与えられる (証明は後で述べる):

定理 7.2.1 (クラメルの公式). 3次正方行列を $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ とおく. $|A| \neq 0$ ならば連立1次

方程式 $A \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$ の解は唯一であり、次で表される:

$$x_1 = \frac{\begin{vmatrix} y_1 & a_{12} & a_{13} \\ y_2 & a_{22} & a_{23} \\ y_3 & a_{32} & a_{33} \end{vmatrix}}{|A|}, \quad x_2 = \frac{\begin{vmatrix} a_{11} & y_1 & a_{13} \\ a_{21} & y_2 & a_{23} \\ a_{31} & y_3 & a_{33} \end{vmatrix}}{|A|}, \quad x_3 = \frac{\begin{vmatrix} a_{11} & a_{12} & y_1 \\ a_{21} & a_{22} & y_2 \\ a_{31} & a_{32} & y_3 \end{vmatrix}}{|A|}.$$

もちろん4次以降についても同様の主張が成り立つ. このように、解の唯一性の判別式として、そして解の公式を一言で述べるための関数として行列式は導入された. ただし、その定義の複雑さから、実際に解を求めるための公式としてはあまり適さないであろう.

7.3 微積分学における行列式

本節の最後に、多変数の微積分学において比較的早い段階で学習する行列式の使用例について紹介する. 簡単のため2変数の場合に限って述べるが、いずれも一般の n 変数関数の議論にまで拡張されるものである. 証明を含めたそれらの詳細は、解析系の講義に譲ろう.

- ヘッセ行列式

C^2 級関数 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ の極値判定において行列式が現れる. 1変数関数のときもそうであったように、点 (a, b) における1階の偏導関数がすべて0だからといって、 $f(a, b)$ が極値を取るとは限らない. 2変数関数の極値判定も1変数の場合 (局所的に凸関数になるかどうか) と同様にテーラーの定理の2次の項を調べることでなされる. その具体的議論は省略するが、次で定めるヘッセ行列 (Hessian matrix) の行列式 (これをヘッセ行列式 (Hessian) という):

$$H_f(a, b) := \begin{bmatrix} \frac{\partial^2 f}{\partial x^2}(a, b) & \frac{\partial^2 f}{\partial x \partial y}(a, b) \\ \frac{\partial^2 f}{\partial y \partial x}(a, b) & \frac{\partial^2 f}{\partial y^2}(a, b) \end{bmatrix}, \quad |H_f(a, b)| = f_{xx}(a, b)f_{yy}(a, b) - f_{xy}(a, b)^2$$

の値によって判定される。 C^2 級ゆえ $f_{xy} = f_{yx}$ に注意せよ。 なお、3変数以上の場合には行列式の値のみでは判定できず、更にヘッセ行列の固有値¹²に関する議論が必要となる。ヘッセ行列式は、その性質から判別式 (discriminant) とも呼ばれている。

- ヤコビ行列式

面積拡大率の意味において最も重要な例は積分の変数変換である。 D および K を \mathbb{R}^2 における長方形で囲まれた集合とし、 C^1 級関数による 1 対 1 写像

$$T: K \rightarrow D, \quad T(u, v) = (\phi(u, v), \psi(u, v))$$

が与えられているとする。このとき、 D 上の 2 変数関数 $f: D \rightarrow \mathbb{R}$ の重積分、すなわち xy -平面 ($z = 0$ 平面) 上の長方形 D と曲面 $z = f(x, y)$ で挟まれた図形の体積

$$\iint_D f(x, y) \, dx dy$$

を変数変換によって K 上の関数 $f(T(u, v)) = f(\phi(u, v), \psi(u, v))$ に関する積分として表したい。 K が D に写像される際の局所的な面積拡大率は各座標に関する偏微分によって次のように計算される:

$$J_T(u, v) := \begin{bmatrix} \frac{d\phi}{du} & \frac{d\phi}{dv} \\ \frac{d\psi}{du} & \frac{d\psi}{dv} \end{bmatrix}, \quad |J_T(u, v)| = \frac{d\phi}{du} \frac{d\psi}{dv} - \frac{d\phi}{dv} \frac{d\psi}{du}.$$

この $J_T(u, v)$ はヤコビ行列 (**Jacobian matrix**) と呼ばれ、 $|J_T(u, v)|$ をヤコビ行列式 (**Jacobian**) という。変数変換による面積の拡大分を掛けることで次の置換積分公式を得る:

$$\iint_D f(x, y) \, dx dy = \iint_K f(\phi(u, v), \psi(u, v)) |J(u, v)| \, du dv.$$

なお、上の公式は D, K がもっと一般の集合の場合 (例えば縦線形集合など) においても成り立つ。

¹²固有値は後期の講義で扱う。

8 置換

行列式の定義への道は長く険しい。ここでは行列式の定義に必要な置換について述べる。置換とはその名の通り置き換え、あるいは入れ替え方を意味する。線形代数においては行列式の定義以外に置換が現れることは稀であるが、数学を記述する言葉として重要である。とくに、群を説明する道具として初等的役割を担う。

なお、置換に関する話題は組み合わせ論的な色彩が強く、苦手意識を持つ読者も多いように思う。しかしながら本論において置換は、行列式の定義とその性質を調べる際に用いられるのみであり、それ以降の行列式の実際の計算においては、組み合わせ論的な素養の多くを必要とするわけではない。苦手意識を克服できずとも、今後の線形代数の学習にあまり支障はないだろう。

8.1 置換の表示

n 個の元からなる集合 X を考える。ここで、 X の構成要素は何でも構わないものの、記述の都合上、 $X_n := \{1, 2, \dots, n\}$ とする。

定義 8.1.1. X_n から X_n 自身への写像 $\sigma: X_n \rightarrow X_n$ において、 $\sigma(1), \dots, \sigma(n)$ の中に重複がないとき σ を X_n 上の置換という。

X_n 上の置換 σ において、文字列 $\sigma(1), \sigma(2), \dots, \sigma(n)$ は 1 から n までの文字が重複なくすべて並んでいる。したがって、 σ は 1 対 1 写像である。

例 8.1.2. 次で定める写像 $\sigma: X_3 \rightarrow X_3$ のうち (1), (2) は置換であり、(3) は置換でない。

$$(1) \begin{cases} 1 \mapsto \sigma(1) = 2 \\ 2 \mapsto \sigma(2) = 3 \\ 3 \mapsto \sigma(3) = 1 \end{cases}, \quad (2) \begin{cases} 1 \mapsto \sigma(1) = 1 \\ 2 \mapsto \sigma(2) = 3 \\ 3 \mapsto \sigma(3) = 2 \end{cases}, \quad (3) \begin{cases} 1 \mapsto \sigma(1) = 3 \\ 2 \mapsto \sigma(2) = 3 \\ 3 \mapsto \sigma(3) = 2 \end{cases}.$$

$\sigma(1) = k_1, \sigma(2) = k_2, \dots, \sigma(n) = k_n$ なる置換 $\sigma: X_n \rightarrow X_n$ を

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

と表す。ここで、右辺の 2 行目 k_1, k_2, \dots, k_n は文字列 $1, 2, \dots, n$ を並び変えたものである。置換の表記は行列と区別がつかないため、文脈でどちらを考えているのか留意すること。

例 8.1.3. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ のとき、 $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 2$ である。

置換の表示を扱いやすくするために、次の表示の仕方を許すとする。

- 置換の表し方は上下の対応のみが本質的であり、列の並び順はあまり重要ではない。そこで、列を入れ替えた書き方を許すとする。これによって、後で定める逆置換の定義が簡明になる。
- σ で動かない元 ($\sigma(i) = i$ なる i のこと) に対応する列は省略してもよいとする。これは後で定める巡回置換の表記を見やすくするための措置である。

以上二つの表示の仕方を認めると、次で表示された置換はすべて同じ写像を表す：

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix}.$$

また、次の二つの置換 $\sigma: X_4 \rightarrow X_4$ および $\tau: X_3 \rightarrow X_3$ の区別がつかなくなる:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

そこで、 $m > n$ のとき、置換 $\sigma: X_n \rightarrow X_n$ は X_m 上の置換でもあると考える。すなわち $i > n$ について $\sigma(i) = i$ となる置換 $\sigma: X_m \rightarrow X_m$ と見なす。

8.2 置換の積

二つの置換 $\sigma, \tau: X_n \rightarrow X_n$ に対して、これらの合成 $\sigma \circ \tau$ もまた置換となる。これを置換どうしの積演算とみなし、 $\sigma\tau$ と書く。すなわち、 $\sigma\tau := \sigma \circ \tau$ 。

例 8.2.1. $\sigma = \begin{pmatrix} 1 & 3 & 4 \\ 4 & 1 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ のとき、

$$\begin{aligned} \sigma\tau(1) &= \sigma(\tau(1)) = \sigma(2) = 2, & \sigma\tau(2) &= \sigma(3) = 1, \\ \sigma\tau(3) &= \sigma(4) = 3, & \sigma\tau(4) &= \sigma(1) = 4, \end{aligned}$$

となるから、 $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ である。なお、 σ の上段が τ の下段と同じ並びになるよう並び変えておくと、合成の計算が簡単になる。 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ であり、 τ と σ を縦に並べると

$$\begin{aligned} \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\ \sigma &= \begin{pmatrix} 2 & 3 & 4 & 1 \\ 2 & 1 & 3 & 4 \end{pmatrix} \end{aligned}$$

ここで真ん中の二段を消して、 $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ を得る。

例 8.2.2. $\sigma = \begin{pmatrix} 2 & 4 & 9 \\ 4 & 9 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 3 & 6 & 7 & 8 \\ 8 & 3 & 6 & 7 \end{pmatrix}$ のとき $\sigma\tau = \tau\sigma$ である。このように、二つの置換 σ, τ の表示において、同じ文字が一つも重複しないとき $\sigma\tau = \tau\sigma$ が成り立つ。

次の二つの概念は、本来は写像に関する一般論において定められるものである。ここでは置換の積演算と関連して、次の呼び方を与える:

定義 8.2.3. • どの元も動かさない X_n 上の恒等写像 $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ を恒等置換 (または単位置換) と呼び、これを id_{X_n} で表す。また、定義域 X_n に誤解がない場合はこれを略して id と書く。

- 置換 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$ の逆写像 $\begin{pmatrix} k_1 & k_2 & \cdots & k_n \\ 1 & 2 & \cdots & n \end{pmatrix}$ を σ の逆置換と呼び σ^{-1} で表す。
- σ の n 回の合成 $\sigma \circ \cdots \circ \sigma$ を σ^n と書く。

逆置換は、置換の表示において行を入れ替えることによって得られる。ゆえに $(\sigma^{-1})^{-1} = \sigma$ である。また、 $\sigma\sigma^{-1} = \text{id} = \sigma^{-1}\sigma$ もすぐに分かる。

8.3 巡回置換

定義 8.3.1. X_n の元のうち k_1, k_2, \dots, k_r 以外の元は動かさず, $\sigma(k_1) = k_2, \sigma(k_2) = k_3, \dots, \sigma(k_{r-1}) = k_r, \sigma(k_r) = k_1$ と順にずらす置換 $\begin{pmatrix} k_1 & k_2 & \cdots & k_{r-1} & k_r \\ k_2 & k_3 & \cdots & k_r & k_1 \end{pmatrix}$ を巡回置換といい, これを省略して (k_1, k_2, \dots, k_r) と書く. また, 二つの文字からなる巡回置換 (i, j) を互換という.

巡回置換を省略して書くのは, 同じ文字を何度も書く手間を省くためである. いま, 置換の表示の仕方がいくつも提示され, ここで錯綜する読者も多いように思う. 様々な表記法があっても, 基本は最初に述べた表示に戻って考えるようにすれば誤解は少なくなるであろう.

例 8.3.2. ● 次の巡回置換はすべて同じ置換を意味する:

$$(2, 5, 3) = (5, 3, 2) = (3, 2, 5) = \begin{pmatrix} 2 & 3 & 5 \\ 5 & 2 & 3 \end{pmatrix}.$$

- $(k_1, k_2, \dots, k_r)^{-1} = (k_r, k_{r-1}, \dots, k_2, k_1)$. 特に $(i, j)^{-1} = (j, i) = (i, j)$.

練習 8.3.3. $\sigma : X_5 \rightarrow X_5$ を $\sigma := (3, 2, 4)(2, 3, 5)$ で定める. このとき, σ を $\begin{pmatrix} 1 & \cdots & n \\ k_1 & \cdots & k_n \end{pmatrix}$ の形で表せ. また, この σ は巡回置換であるか.

答え. X_n の各元を代入して確認する.

$$\begin{aligned} \sigma(1) &= (3, 2, 4)(2, 3, 5)(1) = (3, 2, 4)(1) = 1, & \sigma(2) &= (3, 2, 4)(2, 3, 5)(2) = (3, 2, 4)(3) = 2, \\ \sigma(3) &= (3, 2, 4)(2, 3, 5)(3) = (3, 2, 4)(5) = 5, & \sigma(4) &= (3, 2, 4)(2, 3, 5)(4) = (3, 2, 4)(4) = 3, \\ \sigma(5) &= (3, 2, 4)(2, 3, 5)(5) = (3, 2, 4)(2) = 4. \end{aligned}$$

したがって, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix} = (3, 5, 4)$. ゆえに σ は巡回置換である.

複雑な事象をより単純なものに分解して考えることは科学の基本である. これを置換の場合にも適用し, 任意の置換をより単純な置換に分解する方法を考える.

命題 8.3.4. 任意の置換は互いに文字を共有しない巡回置換の積に分解する.

上の命題を $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix}$ において確かめよう. まず 1 に σ をほどこし続けるとどのように移り変わるか, すなわち数列 $a_m := \sigma^m(1)$ がどう動くかを見る. すると, $1 \mapsto 4 \mapsto 2 \mapsto 1 \mapsto 4 \mapsto 2 \mapsto \dots$ と繰り返される. どうして繰り返されるのだろうか. X_n は有限集合ゆえ数列 a_m はどこかで重複する元が現れる. つまり $\sigma^k(1) = \sigma^\ell(1) = i$ なる二つの自然数 $k > \ell$ が見つかる. このとき $\sigma^{k-\ell}(1) = 1$ である. 何故なら, 置換 σ^ℓ に X_n の元である 1 および $\sigma^{k-\ell}(1)$ を代入すると, いずれも i になり, $\sigma^\ell(1), \dots, \sigma^\ell(n)$ の中に重複はないゆえ $\sigma^{k-\ell}(1) = 1$ でなければならない. いま, 数列 a_m において少なくとも $k - \ell$ 項目までに 1 が現れることが分かった. そして, a_m に初めて 1 が現れた項より先について, a_m は巡回し続ける.

さて, 1 に σ を繰り返してほどこしたときの動きは巡回置換 $(1, 4, 2)$ の働き方と同じである. 次に 1, 4, 2 に現れなかった文字, 例えば 3 について同様に移動の仕方を見てみると $3 \mapsto 6 \mapsto 5 \mapsto 7 \mapsto 3 \mapsto \dots$ を得る. これは巡回置換 $(3, 6, 5, 7)$ と同じ働きをしている. 1, 4, 2 と 3, 6, 5, 7 の間には重複する元は一つもない. これは何故だろうか. 仮に重複する元があったとして, 最初に現れる重複元を j としよう. いま 1 と 3 という異なる文字の動きを見ていたのであるから, j は二番目以降に現れている. また, j は初めて現れる重複元ゆえ j の一つ前は互いに異なる元である. これらを共に σ に代入すると, それは j ゆえ等しい. これは $\sigma(1), \dots, \sigma(n)$ の中に重複はないことに矛盾する. ゆえに 1, 4, 2 に現れない元を取りだして動きを追うと, その中に 1, 4, 2 が現れることはない.

まだ X_n の文字が出つくしていない場合は、そのような文字の移動の仕方を順次見ていく。すると、 X_n の各元が σ による動き方で重複なく分類されることが分かる。いまの例では $\{1, 4, 2\}$ と $\{3, 6, 5, 7\}$ の二つに分類される。このとき、 $\sigma = (1, 4, 2)(3, 6, 5, 7)$ と分解されることはすぐに分かる。

命題 8.3.5. 巡回置換について、 $(k_1, k_2, \dots, k_r) = (k_1, k_r)(k_1, k_{r-1}) \cdots (k_1, k_2)$ 。

上の命題の右辺は、文字列 $k_1 k_2 \cdots k_r$ を文字列 $k_2 \cdots k_r k_1$ に入れ替える次の操作を意味している：

$$k_1 k_2 \cdots k_r \xrightarrow{(k_1, k_2)} k_2 k_1 k_3 \cdots k_r \xrightarrow{(k_1, k_3)} \cdots \xrightarrow{(k_1, k_{r-1})} k_2 \cdots k_{r-1} k_1 k_r \xrightarrow{(k_1, k_r)} k_2 \cdots k_r k_1.$$

ここで、記号 $\xrightarrow{(k_i, k_j)}$ は文字 k_i と文字 k_j の入れ替えを表す。

命題 8.3.4 および 8.3.5 より直ちに次を得る：

系 8.3.6. 任意の置換は互換の積に分解する。

練習 8.3.7. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix}$ を互換の積に分解せよ。

答え.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix} = (1, 4, 2)(3, 6, 5, 7) = (1, 2)(1, 4)(3, 7)(3, 5)(3, 6).$$

8.4 置換の符号

定義 8.4.1. 置換 σ が m 個の互換の積で表されるとき、 $\text{sgn}(\sigma) := (-1)^m$ と定め、これを σ の符号という。 $\text{sgn}(\sigma) = 1$ なる置換 σ を偶置換、 $\text{sgn}(\sigma) = -1$ なる置換 σ を奇置換という。また、単位置換 id は偶置換であると約束する。実際、 $n \geq 2$ ならば $\text{id}_{X_n} = (1, 2)(1, 2)$ ゆえ偶数個の互換の積に分解する。

次の例(練習 8.3.3 と同じ置換)からも分かるように、置換の互換の積への分解は一意的ではない。

$$(3, 2, 4)(2, 3, 5) = (3, 4)(3, 2)(2, 5)(2, 3) = (3, 4)(3, 5).$$

したがって、 σ が奇数個の互換の積で表せ、更に偶数個の互換の積でも表せるとなると、 σ の符号を定めることはできない。しかしながら、このようなことは起こらず、置換を互換の積で表した際の互換の個数の偶奇は必ず一致することが知られている。この事実の証明にはいくつか道具が必要となるゆえ、次節にまわそう。

命題 8.4.2. X_n 上の置換 σ, τ について $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \text{sgn}(\tau)$ 。

Proof. σ が k 個、 τ が l 個の互換の積で表されるとすれば、 $\sigma\tau$ は $k + l$ 個の互換の積で書ける。ゆえに $\text{sgn}(\sigma\tau) = (-1)^{k+l} = (-1)^k (-1)^l = \text{sgn}(\sigma) \text{sgn}(\tau)$. \square

X_n 上の置換全体のなす集合を \mathfrak{S}_n と書き、これを n 次対称群という。 \mathfrak{S}_n の元のうち偶置換のみをすべて集めた集合を A_n と書き、これを n 交代群という。 \mathfrak{S}_n の元の個数はいくつだろうか。置換の表示を $\begin{pmatrix} 1 & \cdots & n \\ k_1 & \cdots & k_n \end{pmatrix}$ の形に限定すると、置換の総数は n 個の文字による列 $k_1 k_2 \cdots k_n$ の総数に一致する。ゆえに \mathfrak{S}_n の元の総数は $n! = n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1$ 個である。例えば \mathfrak{S}_4 の元の個数は $4! = 24$ 個である。 $n \geq 2$ について、 A_n の個数は \mathfrak{S}_n の元の個数のちょうど半分だけある(この事実は後で示す)。

例 8.4.3.

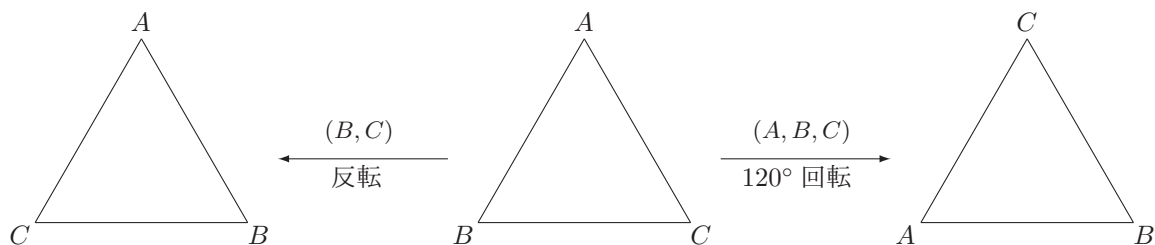
$$\begin{aligned} \mathfrak{S}_3 &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \\ &= \{ \text{id}, (2, 3), (1, 2), (1, 2, 3) = (1, 3)(1, 2), (1, 3, 2) = (1, 2)(1, 3), (1, 3) \}. \\ A_3 &= \{ \text{id}, (1, 3)(1, 2), (1, 2)(1, 3) \}. \end{aligned}$$

本節の最後に群という言葉が出てきた。群とは対称性を記述する数学用語である。群の厳密な定義はこのコラムの最後に述べるとして、その前に対称性とは何かについて再考しよう。

一般に、いくつかの物事の立場が対等であるとき、それらの関係は対称であると言われる。対称と聞いてすぐに思いつく事象は線対称や点対称など図形的・視覚的なものであろう。しかし視覚に訴えない対称性もある。例えば、式 $x^2 + xy + y^2 + zw$ において変数 x と y は対称である。何故なら、 x と y を入れ替えると $y^2 + yx + x^2 + zw$ となり、式の見た目は変化するものの、この式はもとの式と同じ意味を表すからである。同様に z と w は対称であり、 x と z は対称でない。また、“対” という字から対称とは二物の間のみの関係と思われがちであるが、そうではない。例えばジャンケンを考えよう。ジャンケンで出す二つの手の間には勝ち負けの関係があり、これらは対等ではない。しかしながら三つの手の間の関係という意味で、これらの立場は対等であり、したがってジャンケンの手は対称であると考えられる。

さて、これらに共通する性質は何であろうか。それは立場を入れ替えても本質的な変化が無いということである。そこで数学や物理においては、ある構造が与えられた対象に対して、その構造が変化しない入れ替え、およびそうした入れ替えの性質のことを対称性と呼んでいる。例えば原点において点対称な平面上の図形は、ベクトルの -1 倍によってお互いが入れ替わる。また、式 $x^2 + xy + y^2 + zw$ においては、式の意味が変わらないような変数の入れ替えを考えていた。ジャンケンにおいても同様である。命題「 A は B に勝ち、 B は C に勝ち、 C は A に勝つ」が成り立つよう A, B, C にそれぞれジャンケンの手を対応させる。このとき、この命題が成立し続けるような A, B, C の入れ替えがジャンケンの対称性を記述する。なお、対称性とは入れ替えの総数のみを考えるのではなく、入れ替えの相互関係についても考慮する概念である。

簡単な数学的構造の対称性は置換を用いて記述することができる。そこで具体的な図形の対称性を列挙してみよう。始めに正三角形 ABC を例にとろう。 $\triangle ABC$ の頂点を別の頂点へ移動させて再び正三角形を得る操作を考える。例えば $\triangle ABC$ を 120° 回転させると頂点 A, B, C はそれぞれ B, C, A に移動する。この置き替えは巡回置換 (A, B, C) に相当している。また、頂点 A を動かさずに裏表を反転させる操作は頂点 B, C の入れ替えを意味し、これは互換 (B, C) に相当する。

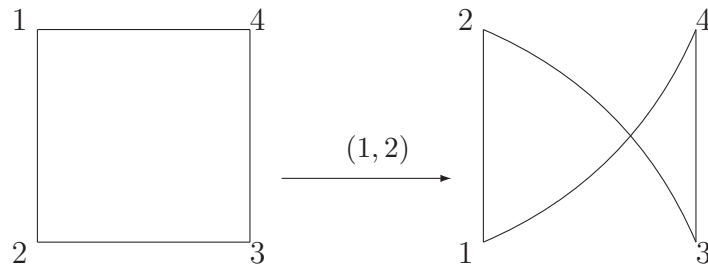


他に考えられる操作は 240° 回転に相当する巡回置換 (A, C, B) , 360° 回転 (結果的にこれは頂点を全く動かさない操作 id に等しい), B, C のいずれかを固定した反転に相当する互換 (A, C) および (A, B) であり、次の計 6 つである。

$$\{ \text{id}, (B, C), (A, B), (A, B, C), (A, C, B), (A, C) \}$$

なお、逆の操作、例えば 120° 回転の逆の操作として -120° 回転が考えられる。しかし、これは 240° 回転と結果が等しいから既に数え上げている。また、 120° 回転の後に元々 A のあった位置で頂点を固定して反転するという操作も考えられるが、この操作を全体として見ると結局、頂点 A, C の入れ替えに過ぎず、したがってこれも数え上げている。ここで、操作の組み合わせと置換の合成が対応していること $(B, C)(A, B, C) = (A, C)$ に注意したい。正三角形における頂点の移動は上の 6 種類で全てつくしている。実際、文字 A, B, C を文字 $1, 2, 3$ に置き換えれば、いま考えている置換の集合は S_3 に等しく、頂点の入れ替えをこれ以上考えることは出来ない。以上の考察により、正三角形の対称性は 3 次対称群で与えられることが分かった。

同様の考察を 1, 2, 3, 4 を頂点にもつ正方形に対して行ってみよう. たとえば互換 (1, 2) は正方形を不変にする入れ替えではない.



何故なら, 頂点 1 と 2 のみを入れ替えると, 図形 1, 2, 3, 4 は正方形でなくなるからである. このような置換に注意して正方形の対称性を列挙すると, S_4 の元のうち次の計 8 つに数え上げられる:

$$\begin{aligned} & \{ \text{動かさない, 上下反転, 左右反転, 対角線 2-4 を軸に反転,} \\ & \quad \text{対角線 1-3 を軸に反転, } 90^\circ \text{ 回転, } 180^\circ \text{ 回転, } 270^\circ \text{ 回転} \}, \\ & = \{ \text{id, (1, 2)(3, 4), (1, 4)(2, 3), (1, 3), (2, 4), (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)} \}. \end{aligned}$$

ちなみに円や球には対称性が無限にあり, 置換を用いて記述するのは難しい. これらの対称性は, 行列式が 1 なる n 次直交行列全体 $SO(n)$ で記述されることを後で学ぼう. 図形以外の対称性はどうか. 式 $x^2 + xy + y^2 + zw$ の対称性は $\{ \text{id, (x, y), (z, w), (x, y)(z, w)} \}$ で与えられ, ジャンケンの対称性は $\{ \text{id, (1, 2, 3), (1, 3, 2)} \}$ となる. なお, 線形代数学で主に扱う構造は線形空間の構造である. \mathbb{R}^n における線形空間の構造を変えない変換の全体は, n 次可逆行列全体 $GL(n)$ と同一視され, これを一般線形群と呼ぶ.

このような“構造を変えない入れ替え全体”を抽象的に記述する言葉として, 群と呼ばれる代数構造が生みだされた. 集合 G の各元の間には演算 (演算記号はドット \cdot で表すか, あるいは省略することが多い) および単位元と呼ばれる特別な元 $e \in G$ 与えられており, 次の条件を満たすとき G を群 (group) という:

- (1) 各 $g \in G$ について $g \cdot e = e \cdot g = g$,
- (2) 各 $g \in G$ に対して, 次の条件を満たす逆元 g^{-1} が存在する: $g^{-1} \cdot g = g \cdot g^{-1} = e$,
- (3) 各 $g, h, f \in G$ に対して, $(g \cdot h) \cdot f = g \cdot (h \cdot f)$ が成り立つ.

すなわち, (1) 何も入れ替えない操作 e があり, (2) 各入れ替え g に対してそれを元に戻す逆の入れ替え g^{-1} が定まっており, (3) 操作の組み合わせに関して結合律が満たされることを上の定義は述べている.

対称群や交代群, あるいはこれまで挙げてきた対称性を記述する置換の集合は, id を単位元とし, 写像の合成を演算とする群である. また, $GL(n)$ は単位行列 E_n を単位元とし, 行列の積を演算とする群である. 整数全体 \mathbb{Z} は, 0 を単位元とし, 足し算を演算とする群である. このように, 群は数学のいたるところに溢れている.

9 置換の符号について

本節では、まずはじめに前節で定めた置換の符号の定義に矛盾がないこと、すなわち、置換を互換の積に分解する際における互換の個数の偶奇は分解の仕方によらないことを示す。次に、置換を文字列の並び替え操作であると考え、この立場から互換の積への分解について再考する。ここでは転倒数と呼ばれる数が導入され、その議論を通してより単純な互換による分解が与えられる。

一方、転倒数を用いることで、置換の符号を別の視点から定義する方法がある。これは互換の積への分解の仕方をあらかじめ一つだけ定めておくことにより、その偶奇によって符号を定めるという方法である。そこで、こちらの方向で定義した符号が従来の性質を満たすことを再確認しておく。この方法の利点は、置換を文字列とみなすことで、置換の詳細を語らずとも次節の冒頭で行列式が定められることにある。置換を苦手とする初学者への、ある種の教育的配慮ともいえるだろう。

なお、符号の定義に矛盾が無いと根拠なく盲信する者にとって、本節の9.1項は不要である。また、9.2項以降で述べることは置換に関する補足事項といった意味合いが強く、線形代数の議論を進める上で必ずしも必須の内容というわけではない。あえて述べたのは次の二つの理由による。一つは参考書の違いにより符号の定義が違って読者が迷わずに済むための配慮である。もう一つは、数学を応用する立場から見ても文字列の並び替えは基本的な考え方・道具となりうるからである。本論は線形代数の理論の習得を目指すために書かれているが、必ずしもそれだけに目的を絞っているわけではない。

9.1 符号の正当性

置換 $\sigma \in \mathfrak{S}_n$ に対して、次の数を考える：

$$s(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

例 9.1.1. $\sigma = (1, 2)(3, 4) \in \mathfrak{S}_n$ とすれば、

$$\begin{aligned} s(\sigma) &= \frac{\sigma(2) - \sigma(1)}{2 - 1} \cdot \frac{\sigma(3) - \sigma(1)}{3 - 1} \cdot \frac{\sigma(4) - \sigma(1)}{4 - 1} \cdot \frac{\sigma(3) - \sigma(2)}{3 - 2} \cdot \frac{\sigma(4) - \sigma(2)}{4 - 2} \cdot \frac{\sigma(4) - \sigma(3)}{4 - 3} \\ &= \frac{1 - 2}{2 - 1} \cdot \frac{4 - 2}{3 - 1} \cdot \frac{3 - 2}{4 - 1} \cdot \frac{4 - 1}{3 - 2} \cdot \frac{3 - 1}{4 - 2} \cdot \frac{3 - 4}{4 - 3} = 1. \end{aligned}$$

例 9.1.2. 恒等置換 $\text{id} \in \mathfrak{S}_n$ において、 $s(\text{id}) = \prod_{1 \leq i < j \leq n} \frac{j - i}{j - i} = 1$.

$s(\sigma)$ が符号を意味することをこれから見ていく¹³。さて、 $s(\sigma)$ が ± 1 の値しか取らないことはほとんど明らかであるが、念のため確認しておこう。

補題 9.1.3. $s(\sigma) = 1$ または $s(\sigma) = -1$.

Proof. $k < l$ としよう。このとき、 $s(\sigma)$ の定義式の分母において1回だけ $l - k$ が現れている。また、分子においても、 $\sigma^{-1}(l)$ と $\sigma^{-1}(k)$ のどちらが大きいかは分からないが、 $\sigma(\sigma^{-1}(l)) - \sigma(\sigma^{-1}(k)) = l - k$ あるいは $\sigma(\sigma^{-1}(k)) - \sigma(\sigma^{-1}(l)) = k - l$ のうちいずれか一方が1回だけ現れる。したがって、分母 $(l - k)$ または $(k - l)$ と分子 $(l - k)$ が相殺されて1または -1 となる。このようなことがすべての項の分母・分子について言えるため、結局、上の式は1または -1 のいずれかのみを取り得る。□

次は命題 8.4.2 を $s(\sigma)$ の言葉で言い換えたものに相当している。

補題 9.1.4. 置換 $\sigma, \tau \in \mathfrak{S}_n$ について $s(\tau\sigma) = s(\tau)s(\sigma)$.

¹³したがって、 $s(\sigma)$ でもって置換の符号を定義してもよいことが分かる。

Proof. 次のように計算できる. 三行目の二つ目の積において, 分母・分子それぞれに -1 を掛けている.

$$\begin{aligned}
s(\tau\sigma) &= \prod_{1 \leq i < j \leq n} \frac{\tau\sigma(j) - \tau\sigma(i)}{j - i} = \left(\prod_{1 \leq i < j \leq n} \frac{\tau\sigma(j) - \tau\sigma(i)}{\sigma(j) - \sigma(i)} \right) \left(\prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \right) \\
&= \left(\prod_{\substack{1 \leq i < j \leq n, \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{\substack{1 \leq i < j \leq n, \\ \sigma(j) < \sigma(i)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \right) \cdot s(\sigma) \\
&= \left(\prod_{\substack{1 \leq i < j \leq n, \\ \sigma(i) < \sigma(j)}} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \prod_{\substack{1 \leq i < j \leq n, \\ \sigma(j) < \sigma(i)}} \frac{\tau(\sigma(i)) - \tau(\sigma(j))}{\sigma(i) - \sigma(j)} \right) \cdot s(\sigma) \\
&= \left(\prod_{1 \leq k < \ell \leq n} \frac{\tau(\ell) - \tau(k)}{\ell - k} \right) \cdot s(\sigma) = s(\tau)s(\sigma).
\end{aligned}$$

ここで, 三行目から四行目への式変形は次の理由による: 1 から n の中にある二つの数の組 $i < j$ すべてを重複なく動かすとき, $k = \min\{\sigma(i), \sigma(j)\}$ および $\ell = \max\{\sigma(i), \sigma(j)\}$ とおくと, 組 $k < \ell$ も 1 から n の中を重複なくすべて動く. ゆえにこれらは同じ積を考えている. \square

上の補題を有限回適用することで, 置換 $\sigma_1, \dots, \sigma_n$ について $s(\sigma_1, \dots, \sigma_n) = s(\sigma_1) \cdots s(\sigma_n)$ を得る.

補題 9.1.5. $1 \leq k < \ell \leq n$ とする. 互換 $\sigma = (k, \ell) \in \mathfrak{S}_n$ について $s(\sigma) = -1$.

Proof. $s(\sigma)$ に現れる各項を, いくつかの場合に分けよう. まず, k, ℓ が絡まない場合と絡む場合に分けて, さらに k, ℓ と絡む場合を $i = k$ かつ $j = \ell$ の場合, そしてそれ以外の場合に細かく分ける. 次の分類は $i < j$ なる組すべてを重複なく分類している.

- $i \neq k, \ell$ かつ $j \neq k, \ell$ の場合,
- $i = k$ かつ $j = \ell$ の場合,
- $i = k$ であり $j \neq \ell$ の場合, このとき $k < j \leq n$ かつ $j \neq \ell$,
- $i = \ell$ であり $j \neq k$ の場合, このとき $\ell < j \leq n$,
- $j = k$ であり $i \neq \ell$ の場合, このとき $1 \leq i < k$,
- $j = \ell$ であり $i \neq k$ の場合, このとき $1 \leq i < \ell$ かつ $i \neq k$.

このように $s(\sigma)$ に現れる各項を分類して計算すると次のようになる:

$$\begin{aligned}
s(\sigma) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \left(\prod_{\substack{1 \leq i < j \leq n, \\ i \neq k, \ell, j \neq k, \ell}} \frac{\sigma(j) - \sigma(i)}{j - i} \right) \left(\frac{\sigma(\ell) - \sigma(k)}{\ell - k} \right) \\
&= \left(\prod_{\substack{k < j \leq n, \\ j \neq \ell}} \frac{\sigma(j) - \sigma(k)}{j - k} \right) \left(\prod_{\ell < j \leq n} \frac{\sigma(j) - \sigma(\ell)}{j - \ell} \right) \left(\prod_{1 \leq i < k} \frac{\sigma(k) - \sigma(i)}{k - i} \right) \left(\prod_{\substack{1 \leq i < \ell, \\ i \neq k}} \frac{\sigma(\ell) - \sigma(i)}{\ell - i} \right) \\
&= \left(\prod_{\substack{1 \leq i < j \leq n, \\ i \neq k, \ell, j \neq k, \ell}} \frac{j - i}{j - i} \right) \left(\frac{k - \ell}{\ell - k} \right) \\
&\quad \left(\prod_{\substack{k < j \leq n, \\ j \neq \ell}} \frac{j - \ell}{j - k} \right) \left(\prod_{\ell < j \leq n} \frac{j - k}{j - \ell} \right) \left(\prod_{1 \leq i < k} \frac{\ell - i}{k - i} \right) \left(\prod_{\substack{1 \leq i < \ell, \\ i \neq k}} \frac{k - i}{\ell - i} \right) \\
&= 1 \cdot (-1) \cdot \left(\prod_{k < j < \ell} \frac{j - \ell}{j - k} \right) \left(\prod_{k < i < \ell} \frac{k - i}{\ell - i} \right) = -1 \cdot \left(\prod_{k < j < \ell} \frac{j - \ell}{j - k} \right) \left(\prod_{k < i < \ell} \frac{i - k}{i - \ell} \right) \\
&= -1 \cdot \left(\prod_{k < p < \ell} \frac{p - \ell}{p - k} \right) \left(\prod_{k < p < \ell} \frac{p - k}{p - \ell} \right) = -1.
\end{aligned}$$

最後の段への変形では、変数を置き換えて見やすくした。 \square

定理 9.1.6. 置換を互換の積に分解する際における互換の個数の偶奇は分解の仕方によらない。

Proof. 置換 σ が k 個の互換 $\sigma_1, \dots, \sigma_k$ の積に分解できるとすれば、先の二つの補題から

$$s(\sigma) = s(\sigma_1 \cdots \sigma_k) = s(\sigma_1) \cdots s(\sigma_k) = (-1)^k$$

を得る。ゆえに、 σ が偶数個の置換の積でも奇数個の置換の積にも分解できると仮定すると、 $s(\sigma) = 1$ かつ $s(\sigma) = -1$ 、つまり $1 = -1$ が示され、しかしこれは起こり得ない。したがって互換の個数の偶奇は一意的である。 \square

上の定理の証明から直ちに次を得る。

系 9.1.7. 置換 σ について $\text{sgn}(\sigma) = s(\sigma)$ 。

9.2 文字列の並び替え

さて、置換とは文字列を並べ替える操作とも考えられる。これを少し詳しく見てみよう。 X_n 上の置換 σ を一つ固定する。 n 個の文字を重複なく並べた任意の文字列 $l_1 \cdots l_n$ を別の文字列に並べ替える操作を考える。ここで、 σ に対応する並び替えとは何かを考えよう。その対応のさせ方は幾つかあり、とくに自然と思われるのは次の2種類の方法である。この二つの方法を混同しないよう注意を促すことがこの項の目的である。ここでは具体的な $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix}$ を通して、置換 σ がどういう並び替えを与えるか説明しよう。

(1) 文字 i のあった場所に文字 $\sigma(i)$ を並べる操作とみなす.

上の σ を例にとれば, 文字 1 のあった場所に文字 4 を置き, 文字 2 のあった場所に文字 1 を置き, ..., 文字 7 のあった場所に文字 3 を置く並べ替えになる. したがって, これは文字列 1234567 を文字列 4162753 に並べ替える操作である. 抽象的に言えば, 文字列 $l_1 \cdots l_n$ を文字列 $\sigma(l_1) \cdots \sigma(l_n)$ に並べ替える操作である.

(2) 第 i 列目にあった文字を $\sigma(i)$ 列目に移動させる並べ替え操作とみなす.

上の σ を例にとれば, 第 1 列目にあった文字を 4 列目に置き, 第 2 列目にあった文字を 1 列目に置き, ..., 第 7 列目にあった文字を 3 列目に置くことを意味する. したがって, 文字列 $l_4 l_1 l_6 l_2 l_7 l_5 l_3$ を文字列 $l_1 l_2 l_3 l_4 l_5 l_6 l_7$ に並べ替える操作, とくに文字列 4162753 を文字列 1234567 に並べ替える操作である. また, この操作について文字列 1234567 を並び変えると 2471635 となる. これを抽象的に述べるのはやや難しく, しいて言えば文字列 $l_{\sigma(1)} \cdots l_{\sigma(n)}$ を文字列 $l_1 \cdots l_n$ に並べ替える操作, あるいは文字列 $l_1 \cdots l_n$ を文字列 $l_{\sigma^{-1}(1)} \cdots l_{\sigma^{-1}(n)}$ に並べ替える操作となる.

上の二つの並べ替え方を念頭におきながら, 置換を互換の積に分解する方法について再考してみよう. 文字列 $123 \cdots n$ において, 隣り合う二つの文字の入れ替えのみを繰り返して任意の文字列 $k_1 k_2 k_3 \cdots k_n$ に変形する操作を考える. 例えば, まず文字 k_1 を先頭まで移動させ, 次に文字 k_2 が 2 列目になるよう移動させ... という操作を繰り返していけばよい.

まずは (1) の立場での入れ替えを検討する. 文字列 1234567 を 4162753 に変えるには次のような入れ替えを行えばよい.

$$(1) \quad 1234567 \xleftrightarrow{(3,4)} 1243567 \xleftrightarrow{(2,4)} 1423567 \xleftrightarrow{(1,4)} 4123567 \xleftrightarrow{(5,6)} 4123657 \\ \xleftrightarrow{(3,6)} 4126357 \xleftrightarrow{(2,6)} 4162357 \xleftrightarrow{(5,7)} 4162375 \xleftrightarrow{(3,7)} 4162735 \xleftrightarrow{(3,5)} 4162753$$

ここで, 記号 $\xleftrightarrow{(i,j)}$ は文字 i と文字 j を入れ替える変形, すなわち (1) の意味で互換 (i, j) に対応する文字列の入れ替えを意味する. したがって, σ は上の変形を合成した互換の積に分解される:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix} = (3, 5)(3, 7)(5, 7)(2, 6)(3, 6)(5, 6)(1, 4)(2, 4)(3, 4).$$

このとき隣り合う列の入れ替えは何回行われるのだろうか. いまの入れ替えにおいて文字 k_i を i 列目に移動させるために行った入れ替えの回数は, k_{i+1}, \dots, k_n 中にある k_i より小さな数の個数に一致している. ゆえに, 入れ替えの総数は次の $\text{inv}(k_1, \dots, k_n)$ で与えられる:

$$\text{inv}(k_1, \dots, k_n) := \sum_{i=1}^n (k_{i+1}, \dots, k_n \text{ のうち } k_i \text{ より小さな数の個数}), \\ = i < j \text{ かつ } k_i > k_j \text{ を満たす組 } (i, j) \text{ の総数.}$$

例えば $\text{inv}(4, 1, 6, 2, 7, 5, 3) = 3 + 0 + 3 + 0 + 2 + 1 = 9$ であり, 確かに σ は 9 つの互換の積に分解されている. $\text{inv}(k_1, \dots, k_n)$ は転倒数 (**inversion number**) と呼ばれる.

次に (2) の立場において文字列の入れ替えをしてみよう. σ による文字列の入れ替えは, 4162753 を 1234567 に入れ替える操作であった. すなわち, 先程の各変形を順次逆に辿っていくことに他ならない.

$$(2) \quad 4162753 \xleftrightarrow{(6,7)} 4162735 \xleftrightarrow{(5,6)} 4162375 \xleftrightarrow{(6,7)} 4162357 \xleftrightarrow{(3,4)} 4126357 \\ \xleftrightarrow{(4,5)} 4123657 \xleftrightarrow{(5,6)} 4123567 \xleftrightarrow{(1,2)} 1423567 \xleftrightarrow{(2,3)} 1243567 \xleftrightarrow{(3,4)} 1234567$$

ここで, いま (2) に対応する文字の入れ替えを考えているから, 変形 (2) における記号 $\xleftrightarrow{(i,j)}$ は i 列と j 列を入れ替える互換を指していることに注意する. これら各々の列の入れ替えの合成が σ であり, ゆえに次を得る:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix} = (3, 4)(2, 3)(1, 2)(5, 6)(4, 5)(3, 4)(6, 7)(5, 6)(6, 7).$$

以上は一般の置換においても成立し、とくに (2) の立場から眺めることで次を得る:

定理 9.2.1. 任意の置換 $\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$ は $(i, i+1)$ なる形の $\text{inv}(k_1, \dots, k_n)$ 個の互換の積に分解する.

9.3 転倒数による符号の定義

転倒数を用いても置換の符号が定まることを見ておこう. すなわち, 置換 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$ に対して \tilde{s} を次で定める:

$$\tilde{s}(\sigma) := (-1)^{\text{inv}(k_1, \dots, k_n)}.$$

既に我々は定理 9.1.6 および 9.2.1 を得ているから, 上の $\tilde{s}(\sigma)$ が $\text{sgn}(\sigma)$ に一致することは分かっている. しかしながら, これらの知識を仮定せずとも符号における最も重要な性質である命題 8.4.2 が直接得られることを示そう.

例 9.3.1. 恒等置換 $\text{id} \in \mathfrak{S}_n$ において, $\tilde{s}(\text{id}) = (-1)^{\text{inv}(1, \dots, n)} = (-1)^0 = 1$

例 9.3.2. 互換 $\sigma = (i, j)$ (ただし $i < j$) について $\tilde{s}(\sigma)$ を計算しよう. σ は

$$\sigma = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots & n \end{pmatrix}.$$

と書ける. また文字列 $Z = 1, \dots, i-1, j, i+1, \dots, j-1, i, j+1, \dots, n$ の転倒数を数えると, j より右側にある j 未満の数は $(j-i)$ 個. $i < \ell < j$ なる ℓ については, ℓ の右側にある ℓ 未満の数は i のみであり, このような ℓ は全部で $(j-i-1)$ 個ある. また, これら以外の文字については数えなくてよいゆえ $\text{inv}(Z) = (j-i) + (j-i-1) = 2(j-i) - 1$. これは奇数である. ゆえに $\tilde{s}(\sigma) = -1$.

補題 9.3.3. 置換 $\sigma \in \mathfrak{S}_n$ および互換 τ に対して, $\tilde{s}(\sigma\tau) = -\tilde{s}(\sigma)$.

Proof. $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$, $\tau = (i, j)$ と置く (ただし $i < j$). このとき, $\sigma\tau$ の表示は次のようになる:

$$\sigma\tau = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ k_1 & \cdots & k_{i-1} & k_j & k_{i+1} & \cdots & k_{j-1} & k_i & k_{j+1} & \cdots & k_n \end{pmatrix}.$$

二つの文字列 $X = k_1, \dots, k_n$ と $Y = k_1, \dots, k_{i-1}, k_j, k_{i+1}, \dots, k_{j-1}, k_i, k_{j+1}, \dots, k_n$ における転倒数の差 $\text{inv}(X) - \text{inv}(Y)$ を計算する. 転倒数とは, 各文字の右側にある自分より小さな数の個数の総数であったから, $\text{inv}(X)$ および $\text{inv}(Y)$ におけるそれぞれの和に関する各項の違いは k_i と k_j の間にある文字 k_ℓ ($i \leq \ell \leq j$) においてしか現れない. 文字列 X を Y に変えたときに, 文字 k_ℓ の右側にある k_ℓ より小さい数の個数がどれだけ変化するか見積もると次のようになる.

- k_i について.

$k_i > k_p$ を満たす p (ただし $i < p \leq j$) の個数ぶんだけ減る. 今の議論において k_j は特別な文字であるから個別に考えることにして, $k_i > k_p$ を満たす p ($i < p < j$) の個数を a 個とし, $k_i > k_j$ ならば $x = 1$, $k_i < k_j$ ならば $x = 0$ とおく. すると $k_i > k_p$ を満たす p ($i < p \leq j$) の個数は $a + x$ 個であり, 個数の変化としては $-(a + x)$ となる.

- k_j について

$k_p < k_j$ を満たす p (ただし $i \leq p < j$) の個数ぶんだけ増える. 上と同様の考えで, $k_p < k_j$ を満たす p ($i < p < j$) の個数を b 個とし, $k_i < k_j$ ならば $y = 1$, $k_i > k_j$ ならば $y = 0$ とおく. すると $k_p < k_j$ を満たす p ($i \leq p < j$) の個数は $b + y$ 個であり, ゆえに個数の変化も $b + y$ である.

- k_ℓ (ただし ℓ は $i < \ell < j$ を満たす $j - i - 1$ 個の文字のいずれか) について.

$k_i > k_\ell$ ならば k_i の移動による変化はない. $k_i < k_\ell$ ならば k_i が k_ℓ よりも右側に移動したことにより 1 つ増える. なお, $k_i < k_\ell$ なる ℓ の個数は $j - i - 1 - a$ 個である. また, $k_\ell < k_j$ ならば k_j の移動による変化はなく, $k_\ell > k_j$ ならば k_j が移動して k_ℓ の右側から消えることにより 1 つ減る. $k_\ell > k_j$ なる ℓ の個数は $j - i - 1 - b$ 個である. 以上の考察から, 文字 k_ℓ たちにおける変化は, $i < \ell < j$ について総和を取り, $(j - i - 1 - a) - (j - i - 1 - b) = b - a$.

以上の変化の総和が $\text{inv}(X) - \text{inv}(Y)$ にあたるから

$$\text{inv}(X) - \text{inv}(Y) = -(a + x) + (b + y) + (b - a) = 2(b - a) + (y - x).$$

x, y の定め方より, $k_i < k_j$ のとき $(y - x) = (1 - 0) = 1$, $k_i > k_j$ のとき $(y - x) = 0 - 1 = -1$ ゆえいずれの場合においても $\text{inv}(X) - \text{inv}(Y)$ は奇数となる. したがって $\text{inv}(Y) - \text{inv}(X)$ も奇数であり,

$$\tilde{s}(\sigma\tau) = (-1)^{\text{inv}(Y)} = (-1)^{\text{inv}(Y) - \text{inv}(X)} \cdot (-1)^{\text{inv}(X)} = (-1) \cdot \tilde{s}(\sigma).$$

□

上の定理は $\text{inv}(X)$ と $\text{inv}(Y)$ の値を直接提示せずに, したがって $\tilde{s}(\sigma)$ および $\tilde{s}(\sigma\tau)$ の値を求めずに証明がなされている. 証明において鍵となるのは $\text{inv}(Y) - \text{inv}(X)$ という量であった. このように, 何が本質的に重要かを見極めることが我々には求められている. いまの証明では, $\text{inv}(X)$ や $\text{inv}(Y)$ 自身, すなわち絶対的な量よりも, これらの間の関係 $\text{inv}(Y) - \text{inv}(X)$, つまり相対的な量が本質的なのであった.

最後に, 命題 8.4.2 に対応する性質は次のように示される.

命題 9.3.4. 置換 σ, τ について $\tilde{s}(\sigma\tau) = \tilde{s}(\sigma) \cdot \tilde{s}(\tau)$.

Proof. $\tau = \begin{pmatrix} 1 & \cdots & n \\ k_1 & \cdots & k_n \end{pmatrix}$ と置くと, 定理 9.2.1 により τ は $\text{inv}(k_1, \dots, k_n)$ 個の互換の積で書ける. ゆえに補題 9.3.3 を $\text{inv}(k_1, \dots, k_n)$ 回適用することで次の式の最初の等式が得られ

$$\tilde{s}(\sigma\tau) = (-1)^{\text{inv}(k_1, \dots, k_n)} \tilde{s}(\sigma) = \tilde{s}(\tau) \cdot \tilde{s}(\sigma) = \tilde{s}(\sigma) \cdot \tilde{s}(\tau),$$

我々は求める主張を得る.

□