現 代 数 学 の 基 礎 知 識 (web版)

和久井道久

平成 21 年 3 月 10 日

はじめに

本書は平成 15 年度、平成 16 年度、平成 18 年度の 3 年間にわたって、大阪大学で行なわれた 1 年生向けの授業「数学の楽しみ」のために筆者が作成したプリントに基づいている。平成 18 年度のシラバスには「数学の楽しみ」の「授業の目的、ねらい」が次のように書かれている。基本的な数学の題材を少人数のセミナー、演習形式で学ぶ。通常の講義では深入りでできない数学の基礎的な概念を習得することを目指す。数学のプロを目指す人達のための基礎セミナーで理学部数学科とは限らない学生も対象とする。

ひとりひとりの学生に数学の基礎的な事柄をしっかり理解してもらうために、授業を「チェック形式」で行った。「チェック形式」とは、一言で言えば、個別指導法のことである。以下では「数学の楽しみ」で採用したチェック方式を書き記しておく。

- 配付されるプリントを読み、演習問題を解く。
- 演習問題の答案用紙 (レポート用紙、ルーズリーフ等) は各自で用意し、各用紙ごとに学籍番号 (下２ケタ) と氏名を記入する。
- 演習問題は＊印のついている問題と何もついていない問題の２つがある。
- ＊印のついている演習問題はチェック形式で行う。チェック形式とは：
  - 学生が自分の解答を教員のところに見せに来て、質議応答を受ける。
  - 教員は、それが正しいか間違っているか、計算や証明にギャップがないか、不十分な点はないかなどをチェックし、学生に伝える。
  - ＯＫがもらえれば、その問題は修了。再度修正して持って来るように言わたら、直してまたチェックを受けに来る。ＯＫという返事がもらるまで、これを繰り返す。
- 指定された１問を先に解き、遅くとも午後２時までに最低１回はチェックを受けに来るようにする。ＯＫをもらったら、残りの＊印のついている問題を解き、さらに、時間が余れば、＊印のついていない問題を解く。
- チェックを受けた分も含めて、その日に配ったプリントの中の演習問題の答案は、(途中のものも含めて) すべて、授業の最後に提出する。添削して次回の授業時に返却する。
- 解答例として、提出された学生の解答の中から、最もよく書けていると思われるものをコピーして受講者全員に配付する（次回の授業時)。

目　　次

§1. 数学の教科書や授業に出てくる文字と用語

大学の数学では英語のアルファベットの他にギリシア文字が頻繁に使われます。そこで、まず、ギリシア文字の読み方を覚えて、それを書くことができるようにしましょう。次に、数学の教科書や授業に繰り返し出てくる用語—命題、証明、定理、定義、公理など—の意味を学びます。最後に、大学で数学を学ぶ際の心構えやヒントのようなものを紹介します。

§1-1 数学の教科書や授業に出てくる文字

数学の教科書には、英語のアルファベットや演算記号 $+, -, \times$ などの他に様々な記号や文字が登場します。ここではその中の代表的なものを紹介します。

●ギリシア文字

大文字	小文字	対応する アルファベット	読み方
A	α	a	alpha (アルファ)
B	β	b	beta （ベータ）
Γ	γ	c	gamma（ガンマ）
Δ	δ	d	delta （デルタ）
E	ϵ（あるいは ε）	e	epsilon（イプシロン、エプシロン）
Z	ζ	z	zeta （ゼータ）
H	η	h	eta （エータ、イータ）
Θ	θ（あるいは ϑ）		theta （シータ、テータ）
I	ι	i	iota （イオタ）
K	κ	k	kappa （カッパ）
Λ	λ	l	lambda （ラムダ）
M	μ	m	mu（ミュー）
N	ν	n	nu（ニュー、ヌー）
Ξ	ξ	x	xi（クシー、グザイ）
O	o	o	omicron（オミクロン）
Π	π（あるいは ϖ）	p	pi（パイ）
P	ρ（あるいは ϱ）	r	rho（ロー）
Σ	σ（あるいは ς）	s	sigma （シグマ）
T	τ	t	tau （タウ）
Υ	υ	u	upsilon（ウプシロン）
Φ	ϕ （あるいは φ）		phi （ファイ）
X	χ		chi （カイ）
Ψ	ψ		psi （プサイ、プシー）
Ω	ω		omega （オメガ）

注意：1. 上の表の空欄は、そのギリシア文字に対応するアルファベットが存在しないことを意味します。

2. 読み方の欄のカタカナ表記は、１つの目安と考えてください (２通りの読み方が記載されているものについては、そのどちらでも構いません)。

3. ϕ と φ のように、小文字のギリシア文字の中には２種類の字体を持つものがありますが、これらを記号として数学で使う場合には、原則として区別して扱います。ϵ と ε など、似た字体については、どちらか一方だけを使うのがふつうです。

演習 1-1 * 小文字のギリシア文字を (小声で読みながら) すべて書け。

●筆記体とボールド体

アルファベットの大文字は通常の斜体 (イタリック体) の他に筆記体、ボールド体が使われます。これらの書体を、数学では、どれも違う対象を表わす記号として扱います (同じ A という文字を使っていても、A, $\mathcal{A}$, $\boldsymbol{A}$, $\mathbb{A}$ で表わされるものは全部違うという意味です)。

斜体	A	B	C	D	E	F	G	H	I	J	K	L	M
筆記体	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{D}$	$\mathcal{E}$	$\mathcal{F}$	$\mathcal{G}$	$\mathcal{H}$	$\mathcal{I}$	$\mathcal{J}$	$\mathcal{K}$	$\mathcal{L}$	$\mathcal{M}$
ボールド体	$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{C}$	$\boldsymbol{D}$	$\boldsymbol{E}$	$\boldsymbol{F}$	$\boldsymbol{G}$	$\boldsymbol{H}$	$\boldsymbol{I}$	$\boldsymbol{J}$	$\boldsymbol{K}$	$\boldsymbol{L}$	$\boldsymbol{M}$
板書ボールド体	$\mathbb{A}$	$\mathbb{B}$	$\mathbb{C}$	$\mathbb{D}$	$\mathbb{E}$	$\mathbb{F}$	$\mathbb{G}$	$\mathbb{H}$	$\mathbb{I}$	$\mathbb{J}$	$\mathbb{K}$	$\mathbb{L}$	$\mathbb{M}$

斜体	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
筆記体	$\mathcal{N}$	$\mathcal{O}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{R}$	$\mathcal{S}$	$\mathcal{T}$	$\mathcal{U}$	$\mathcal{V}$	$\mathcal{W}$	$\mathcal{X}$	$\mathcal{Y}$	$\mathcal{Z}$
ボールド体	$\boldsymbol{N}$	$\boldsymbol{O}$	$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{R}$	$\boldsymbol{S}$	$\boldsymbol{T}$	$\boldsymbol{U}$	$\boldsymbol{V}$	$\boldsymbol{W}$	$\boldsymbol{X}$	$\boldsymbol{Y}$	$\boldsymbol{Z}$
板書ボールド体	$\mathbb{N}$	$\mathbb{O}$	$\mathbb{P}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{S}$	$\mathbb{T}$	$\mathbb{U}$	$\mathbb{V}$	$\mathbb{W}$	$\mathbb{X}$	$\mathbb{Y}$	$\mathbb{Z}$

注意：1. 筆記体については、特に、板書では個性が強く出るため、上記の表にある表示と一致しない場合があります。

2. $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y}$ など、小文字のボールド体もよく使われます。最近はあまり見かけなくなりましたが、$\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{S}$ などのドイツ文字も使われることがあります。

3. 教科書に印字されている (板書) ボールド体を手書きするときは、原則として文字の左側を 2 重にします。

$\mathbb{R}$　$\mathbb{S}$　$\mathbb{Z}$　$\mathbb{U}$　$\mathbb{V}$　$\mathbb{W}$

演習 1-2* 上の例に習って、C, N, Q, R, Z のボールド体、a, b, x, y のボールド体を書け。

●文字の装飾

英語のアルファベットやギリシア文字に、次のような装飾を加えた記号もよく使われます。

装飾	名称	用例	読み方
$\prime$	プライム (prime)	a'	エイ プライム
$-$	バー (bar)	$\overline{a}$	エイ バー
$*$	アスタリスク (asterisk)	a^*	エイ スター
$\wedge$	ハット (hat)	$\widehat{a}$	エイ ハット
$\sim$	ティルダ (tilde)	$\widetilde{a}$	エイ ティルダ

§1-2 定理と定義の違い

数学の教科書を見ると、「**定義**」「**定理**」「**補題**」「**命題**」「**証明**」といった言葉が太字で何度も登場します。数学の授業の中でも、これらの言葉が繰り返し出てきます。ここでは、簡単にそれらの意味について説明します。「命題」という言葉には 2 通りの意味があることに注意してください。

●命題 (proposition)：広い意味での命題

一般に、数や図形などの数学的対象について、いくつかの“基本的な接続詞と述語”や演算記号を用いて記述される曖昧さのない文章のことを数学的**命題**といいます。ここで、“基本的な接続詞と述語”とは、「ならば」「または」「かつ」「である」「ではない」「存在する」などの論理的な文章でよく使われる言葉を指します。演算記号とは「$=$」「$\neq$」「$<$」「$+$」などの数学で

よく使われる記号を指します。以後、単に命題と呼べば、それは数学的命題のことを意味することとします。

例 1-1 次の 3 つのうち、(1)(2) は命題であるが、(3) は命題ではない。
(1) 二等辺三角形は正三角形である。
(2) n が奇数ならば、n^2-1 は 8 の倍数である。
(3) 1 年生が取らなければならない必修科目数はとても多い。

P を 1 つの命題とするとき、「P ではない」という命題を考えることができます。この命題を $\overline{P}$ と書き表わすことにします。今後は常に、命題について、次の事柄が満たされているという前提のもとで議論します。

排中律（はいちゅうりつ）：命題 P について、P または $\overline{P}$ のどちらかが成り立ち、それらの両方が同時に成り立つことはない。

命題 P が成り立つとき、「P は**真**（しん）(true) である」といい、P が成り立たないとき、「P は**偽**（ぎ）(false) である」といいます。排中律により、私たちが扱う命題には、真であるか偽であるかのどちらか一方のみが定まっていなければなりません。しかしながら、「$x^3+y^3=z^3$ を満たす自然数の組 (x,y,z) は存在しない」のように、真であるか偽であるかが直ちには判定できない文章があります。このような文章であっても、真であるか偽であるかのどちらか一方のみが成り立つはずであると推察される曖昧さのない文章は、私たちの扱う命題に含まれます。

演習 1-3* 次の文章は命題と呼べるか？判定せよ。
(1) $1+1=3$ である。
(2) 数学科の生徒は数学が得意である。
(3) 互いに素な 2 つの整数 a と b に対して、$ua+vb=1$ となる整数 u と v が存在する。

●証明

証明 (proof) とは、真の命題が与えられたとき、それが成り立つことを他者および自分に納得させるためになされる、客観的な説明のことをいいます。その説明の中には、論理展開の飛躍している箇所があったり、2 通りの意味に解釈可能な記述があってはいけません。

証明の構成要素は命題と推論です。**推論** (inference) とは、いくつかの命題を「…と仮定すれば」「したがって」などでつなぐことによって新しい命題を導き出す方法のことをいいます。推論の仕方としては**三段論法** (syllogism) や**背理法**（はいりほう）(reductio ad absurdum) などがあります。これらを使って、いくつかの命題を積み重ねることにより、証明が完成されます。

三段論法：3 つの命題 P,Q,R について、「P ならば Q」が成り立ち、「Q ならば R」が成り立つときに、「P ならば R」が成り立つことを結論とする推論のこと。

背理法：命題 P が成り立つことを証明するのに、P が成り立たないと仮定して、**矛盾** (contradiction) を導く推論のこと。

注意：矛盾とは、「Q かつ $\overline{Q}$」という形の命題のことです。

例 1-2　素数は無限個存在することを証明せよ。

(証明)

背理法で証明する。

素数は有限個しか存在しなかったと仮定する。

$2, 3, 5, \cdots, p$ を素数のすべてであるとする。このとき、これらの積に 1 を加えた数

$$n = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p + 1$$

を考える。すると、この n は $2, 3, 5, \cdots, p$ のどれによっても割り切れない、すなわち、どんな素数でも割り切れない。

一方、n は 2 以上の自然数なので、ある素数を約数として持つ (実際、n の約数は有限個しかないので、その中の 1 でない最小の数を q とおけば、これが条件を満たす素数となる)。ここに、矛盾が生じた。よって、仮定「素数は有限個しか存在しない」は誤りであり、「素数は無限個存在する」ことが証明された。　□

演習 1-4　背理法を使って、$\sqrt{2}$ は無理数であることを証明せよ。

● 定理(ていり)、補題、命題、系(けい)

成り立つことが誰かの手によってすでに証明されている命題のことを**定理**といいます。したがって、「定理」と見出しがついている命題は真の命題です。状況により、定理のかわりに補題、命題、系という言葉も使われます。これらには次のようなニュアンスの違いがあります。

定理 (theorem)	成り立つことがすでに証明されている命題の中で、特に重要であると認識されるものに使われます。
命題 (proposition) (狭い意味での命題)	定理と呼ぶほどではないけれども、1 つのまとまった主張が成り立つ場合に使われます。したがって、この場合の命題とは、すでに証明されている真の命題を指します。
補題 (lemma)	定理や (狭い意味での) 命題の証明の際、その証明の見通しをよくするために設けられる補助的な定理のことをいいます。 補助定理と呼ばれることもあります。
系 (corollary)	定理や (狭い意味での) 命題、補題から、直ちに、成り立つことが証明される命題のことをいいます。「定理の副産物」と思ってよいでしょう。

例 1-3

定理　平面上の 2 つのベクトル $\overrightarrow{a}$, $\overrightarrow{b}$ に対して、

$$|\overrightarrow{a} \cdot \overrightarrow{b}| \leq |\overrightarrow{a}||\overrightarrow{b}|$$

である。ここで、$\overrightarrow{a} \cdot \overrightarrow{b}$ はベクトルの内積、$|\overrightarrow{a}|$ はベクトル $\overrightarrow{a}$ の大きさを表わす。

系　平面上の 2 つのベクトル $\overrightarrow{a}$, $\overrightarrow{b}$ に対して、

$$|\overrightarrow{a} + \overrightarrow{b}| \leq |\overrightarrow{a}| + |\overrightarrow{b}|$$

である。

演習 1-5　上の例で述べられている系をそのすぐ上にある定理から導け。

真であることが証明されている命題を定理、(狭い意味での) 命題、補題、系のどれを使って呼ぶか、についてはかなり主観が入ります。教科書の著者や授業の担当教員によって様々です。同じ著者であっても、ある状況で定理と呼んでいたものが、別の状況では補題と呼んでいたりする場合があります。

● 定義（ていぎ）

定義 (definition) とは、新たに導入しようとする述語や単語に、すでに意味が確立されている (性質、もの、量などに関する) 述語や単語を使って、正確な意味を与えることをいいます。したがって、定義とされた文章には、定理と違い、証明をつける必要はありません。

例 1-4

定義　$f(x)$ が区間 $[a,b]$ 上で定義された連続関数とする。$[a,b]$ の点 c において、十分小さいすべての正の数 h に対して

$$f(c-h) \leq f(c) \quad \text{かつ} \quad f(c) \geq f(c+h)$$

が満たされるならば、$f(x)$ は $x=c$ において**極大**であるといい、$f(c)$ を**極大値**であるという。

定義は、上記のような表現形式の他に、本文中にさりげなく書かれている場合もあります。

例 1-5

(1) **有理数**とは、正の整数 s と整数 r を使って、$\frac{r}{s}$ のように分数として表わされる数のことをいう。
(2) n を正の整数とするとき、a を n 個掛け合わせたものを a の n **乗**といい、a^n と書く。数 b が与えられたとき、n 乗して b となる数 x のことを b の n **乗根**という。
(3) $f(x) = x - \sin x$ とおく（関数 $f(x)$ を $x - \sin x$ と定義する)。

注意：例 1-4 のように、「定義」と宣言してからその内容が書き始められている場合、一冊の教科書または半年間の講義を通して、そこに述べられている以外の意味で、その用語を使うことはありません。

● 公理（こうり）

公理 (axiom) とは、これから考えようとする理論の土台となる約束ごと・前提のことです。

しばらくした後に、私たちが関係する公理は次の実数の連続性に関する公理です。

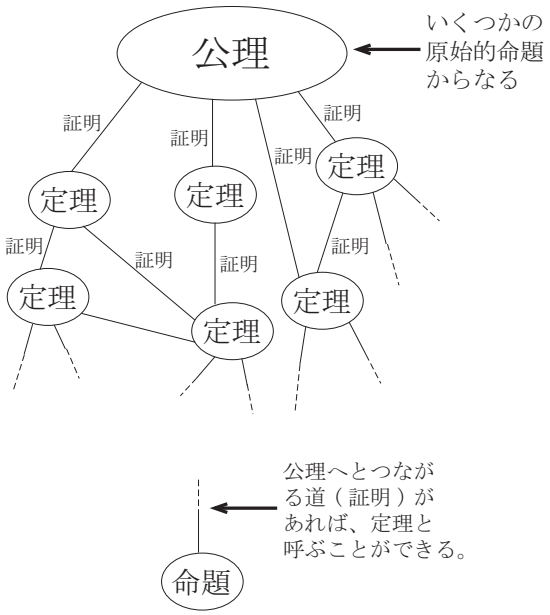
例 1-6 (**アルキメデスの公理**)
２つの正の実数 a,b に対して、$a < nb$ となる自然数 n が存在する。

１つの理論を形成するために必要な公理は、通常、複数の“原始的な命題”からなります。公理に掲げられている命題は無条件にすべて正しいと認めます。したがって、それらを証明する必要はありません。

数学では、原則として、次のような手順で理論が構築されていきます。まず最初に、公理とすべき命題を決めます (すでに確立されている理論の場合、歴史的な経緯などから、何を公理として採用するかはもう決まっています)。次に、その公理から、三段論法や背理法などの定められた推論を通して証明された命題のみを定理と認めていきます。得られた定理を集大成することにより、1 つの理論が形成されていくのです。

通常の教科書では、公理から述べ始めることはほとんどありませんが、“はじめに”などに、「この本では○○○については既知とする」のように書かれている部分が、公理に該当する箇所であるとみなしてもよいでしょう。

公理についての興味深い叙述が、彌永昌吉・著『数の体系（上)』(岩波新書), 1972 年, p.65 の前後や寺坂英孝・著『初等幾何学　第 2 版』(岩波全書), 1973 年, p.1–8 にあります。一読をお勧めします。



日本語	英語	省略形
公理	Axiom	
定義	Definition	Def.
定理	Theorem	Th.
補題	Lemma	Lem.
命題	Proposition	Prop.
系	Corollary	Cor.
証明	Proof	Pf.
注意	Remark	Rem.
例	Example	Ex.
演習	Exercise	Ex.

演習 1-6 * 公理、定義、補題、(狭い意味の) 命題、(広い意味の) 命題、定理、系のうちで、証明された真の命題だけにしかつけることができないものをすべて挙げよ。

§1-3 大学で学ぶ心構え

大学では、高校までとは比較にならないくらいの早いスピードで授業が進行します。各科目を半年間（約 15 週）で学ぶのですが、1 コマの授業時間は 90 分ですから、講義を聴く時間は、1 科目について合計 22 時間 30 分程度 (1 日にも満たない！) しかありません。教科書の膨大な内容をわずか 1 日で理解することは不可能ですから、単に講義を聴くだけではなく、各自でわからないことを調べたり勉強したりする必要があります。ここでは、その手助けとなりそうなヒントを挙げてみます。

●文献検索

授業の中でわからない単語や概念が出て来たら、その意味を調べましょう。ここでは、文献検索の方法をいくつか紹介します。

(1) 教科書や参考書を見る。

まず最初にやってみるべき方法です。大抵の教科書や参考書には後ろの方に**索引** (index) がついています。索引はその本で扱われている大切な用語が参照ページと一緒に記された一覧表です。そこに調べたい用語が載っているかもしれません。索引に載っていなくても本文中に説明されていることもあるので、すぐにあきらめず、関連する単語やよく似た単語を索引で引いたり、目次を眺めたりして、捜してみましょう。(授業で習った記号や概念がその本では違う記号や言葉で表わされていることもあるので注意しましょう)。

演習 1-7 線形代数学の教科書または参考書を用意し、その索引を用いて、「固有値」が説明されているページ数とそこに書かれている「固有値」の定義を書け (使用した教科書名、著者名、出版社名も書くこと)。

(2) 図書館を利用する。

調べたい事柄が教科書に載っていなかったり、教科書に載ってはいるものの満足のいく説明でなかったりする場合には、**大学の附属図書館**を活用しましょう。そうは言っても、図書館に所蔵されている文献の量は膨大なので、いったいどの本を参照すればよいのか、見当がつかないかもしれません。そのようなときには先生に相談したり先輩や友達に尋ねたりするとよいでしょう。

内容が少し専門的な数学については附属図書館に文献がない場合もあります。このようなときには理学部 E 棟 5 階にある**数学教室の図書室**を利用しましょう。数学教室の図書室には洋書を中心に数学に関する専門書や専門誌が“ぎっしり”収められています。

(3) 本屋さんへ行く。

数学書のコーナーを設けている本屋さんに行って、調べることも方法の 1 つです。一番身近には、**大学生協の書籍部**があります。梅田 (大阪) 駅周辺には、**淳久堂書店**、**旭屋書店**といった大型書店があり、現在入手可能な数学書のほとんどが揃っています。

(4) インターネットを利用する。

インターネットを使える環境があれば、Google などの検索エンジンにキーワードを入力して、調べることができます。但し、キーワードをうまく絞り込まないと検索結果が大量になり、知りたい所になかなか辿り着けないことがあるので注意しましょう (検索を掛ける際に複数のキーワードを、キーワードとキーワードの間に半角または全角のスペースキーを入れて入力すると、検索件数を絞り込むことができます)。

各教員が作成しているホームページから有益な情報が得られる場合もあります。例えば、大阪大学理学部数学教室のホームページアドレスは http://www.math.sci.osaka-u.ac.jp/ です。まだ気が早いかもしれませんが、過去の大学院試問題がここから入手できます。

●先生への質問と友達との議論

先生に質問したり、学生同士で議論をすることは、数学の理解を深めていく上で、とても大切なことです。一人ではどうにもならなかったことが、他人とコミュニケーションをとることにより、よいアイデアが浮かび、解決の糸口がみつかったりすることがあります。大いに質問をし、議論しましょう。ただ、質問するとき、教科書やノートのある部分を指すなり、「ここがわかりません」といって、質問を“丸投げ”することは避けましょう。その教科書は、質問を受けた先生が読んだことのない本の可能性がありますし、仮に読んだことがあったとしても、

本の内容をすべて記憶しているわけではないので、その部分を見てもすぐに内容を理解できないことがあるからです。聞きたい事柄の前後の状況や記号について一通り説明するようにしましょう。そして、「ここまでは理解できるのですが、このあとに何故こう書いてあるのかわかりませんでした」のように、質問は具体的にしましょう。

●雑誌

ここでは数学に関する日本語で書かれた啓蒙的な雑誌を紹介します。

・「**数学セミナー**」は日本評論社が刊行している月刊誌です。毎号さまざまなテーマの特集が組まれています。授業では教わらない興味深い話題を知ることができます。書評欄には最近売れている数学書やお薦めの数学書が紹介されていたり、ニュース欄には各地で行われている公開講座やサークルの案内などが掲載されています。

・「**数理科学**」はサイエンス社が刊行している月刊誌です。数学に限らず、物理、化学、生物など幅広い分野が扱われています。内容は「数学セミナー」よりも専門的です。

・その他、「**理系の数学**」「**数学文化**」や「**数学のたのしみ**」という雑誌もあります。

●ノートを作る

深い理解を得るために、講義で執ったノートをあとからまとめ直すことをお勧めします。全体の構成を見直して、次のようなことに気をつけて自分のためのノートを作成するとよいでしょう。

- 補題を作る (わかりやすくなる場合)。また、補題、命題、定理、系を使い分ける。
- 定義をきちんと書く。また、その意味を考える。
- 例を作る。
- 定理の逆が成り立つかどうかを考えてみる。
- 証明のアイデアやあらすじを書いておく (長い証明の場合に有効)。
- 定理の主張だけを書いて、自分で証明をつけるように努力する。
- 長々と文章を書かず、適度に記号化する。
- 大切と思われる式や主張は行変えをして、中央に置く。

●数学書を読むときや授業を聴くときの心構え

数学の本は、随筆や小説を読むように、スラスラと読むことはできません。数学の教科書や講義では、

- 容易に説明はできるけれども、実際に書くとなると少し面倒である、
- この程度のことはお互い既知としておきたい、
- 実際に説明しようとすると、読者や聴講者の知識を大幅に超える事柄が必要である、
- それをいちいち書くと、証明の本質的な部分が見えなくなってしまう、

などさまざまな理由から、定理の証明の細部が省略されている場合があります (まれに、著者の勘違いや思い込みにより省略されてしまっていて、しかも、間違っていることもあります)。このような箇所は「明らかに」「容易に」「〜を証明すれば十分である」「したがって」などと書かれている部分に多くみられます。勉強の初期段階では、このような箇所を簡単に通り過ぎず、著者はこう書いているが「なんでだろう？」と立ち止まって考えることが重要です。そして、納得のいく説明をつける努力をしましょう。逆に、自分が証明を書くときも、安易に「明らかに」や「自明」という言葉を使わないようにしましょう。

§2. 命題と論理

定理の証明や定義された概念を理解するには、命題の否定を作り、それを同じ内容のよりわかりやすい表現の命題に書き換える、という作業が不可欠です。ここでは、論理の基礎を学びながら、その練習をします。後半では、命題の同値について説明します。この節では、命題という言葉を広い意味で用います。

§2-1 命題論理

与えられたいくつかの命題に、「ではない」「または」「かつ」「ならば」という言葉をつなげて、新しい命題を作ることができます。ここでは、それらの用例を見ていくと同時に、その否定の作り方についても勉強していきましょう。

私たちは排中律が満たされている命題だけについて議論していること思い出しましょう。

> 排中律：命題 P について、P または $\overline{P}$ のどちらかが成り立ち、それらの両方が同時に成り立つことはない。但し、$\overline{P}$ は「P ではない」という命題を表わす。

命題 P が成り立つとき、P は**真**である (true) といい、P が成り立たないとき、P は**偽**である (false) というのでした。

●否定

上で述べたように、命題 P に対して「P ではない（not P)」という命題 $\overline{P}$ を作ることができます。$\overline{P}$ は、より詳しく言えば、「P (が成り立つ)、ということではない」という意味の命題です。$\overline{P}$ を P の**否定** (negation) と呼びます。

排中律により、命題 P に対して、次が成り立つことがわかります。

P が真のとき、$\overline{P}$ は偽であり、P が偽のとき、$\overline{P}$ は真である。

この事実を右表のように表わします。右表を $\overline{P}$ の**真理表** (truth table) といいます（表は各行ごとに左から右へ読みます。縦棒は「…のとき」を意味します。T は真であることを F は偽であることを表わしています)。

P	$\overline{P}$
T	F
F	T

$\overline{P}$ の真理表

例 2-1 次の命題の否定を、それと同じ内容を持つわかりやすい文章の命題に、書き換えよ。

(1) $\sqrt{5}$ は有理数である。

(2) 二等辺三角形は正三角形である。

解；

(1) 与えられた命題の否定は

「“ $\sqrt{5}$（という実数）は有理数である ”ということではない」

である。有理数でない実数は無理数であるから、「$\sqrt{5}$ は無理数である」と書き換えても内容は変わらない。

(2) 与えられた命題の否定は

「“ 二等辺三角形は (必ず) 正三角形である ”ということではない」

である。これを

「“（どんな）二等辺三角形も正三角形である ”ということではない」

と書き換えても、内容は変わらない。さらに、これを

「二等辺三角形の中には正三角形でないものがある」

と書き換えても同じ内容を持つ命題である。 □

演習 2-1 *

(1) 命題「7 は 3 で割ると 1 余るような整数である」の否定を、それと同じ内容を持つわかりやすい文章の命題に、書き換えよ。

(2) A 君は、命題「関数 $f(x)$ は単調増加関数である」の否定は、要するに、「関数 $f(x)$ は単調減少関数である」ということだと言った。A 君の主張は正しいか？

●「かつ」と「または」

2 つの命題 P と Q に対して「P かつ Q（P and Q)」という命題を作ることができます。これは「P であって、かつ、Q である」という意味の命題です。これを P と Q の**論理積** (logical product) と言い、$P \wedge Q$ という記号で書き表わします。$P \wedge Q$ が真であるのは、P も Q もともに真であるときであり、かつ、そのときに限ります (これが $P \wedge Q$ の真偽の定義と思って下さい)。

2 つの命題 P と Q に対して「P または Q（P or Q)」という命題を作ることができます。これは「P であるか、または、Q である」という意味の命題です。これを P と Q の**論理和** (logical sum) と言い、$P \vee Q$ という記号で書き表わします。$P \vee Q$ が真であるのは、P と Q の少なくとも一方が真であるときであり、かつ、そのときに限ります (これが $P \vee Q$ の真偽の定義と思って下さい)。

上で述べた事実を、真理表としてまとめておきましょう。

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

$P \wedge Q$ の真理表

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

$P \vee Q$ の真理表

例 2-2 n を 1 つの自然数とする。次の各命題の否定を、それと同じ内容を持つわかりやすい文章の命題に、書き換えよ。

(1) n は 2 の倍数であり、かつ、100 より小さい。

(2) $n = 2$ または $n = -2$ である。

解；

(1) 与えられた命題を P とおくと、その否定 $\overline{P}$ は、

「“n は 2 の倍数であり、かつ、100 より小さい”ということではない」

となる。これは、命題「n が 2 の倍数である」と命題「n が 100 より小さい」が同時には成り立たないことを意味するから、$\overline{P}$ を

「n は 2 の倍数ではないか、または、100 より小さくはない」

と書き換えてもその内容は変わらない。ここで、自然数が「2 の倍数ではない」とは「奇数である」ことと同じであり、「100 より小さくはない」とは「100 以上である」ことと同じであるから、結局、$\overline{P}$ は、

「n は奇数であるか、または、100 以上である」

と書き換えることができる。

(2) 与えられた命題を P とおくと、その否定 $\overline{P}$ は、

「“$n=2$ または $n=-2$ である”ということではない」

となる。これは、「$n=2$ である」と「$n=-2$ である」のどちらでもないことを意味する。よって、$\overline{P}$ は、

「$n \neq 2$ かつ $n \neq -2$ である」

と書き換えることができる。 □

演習 2-2 * x を 1 つの実数、△ABC を 1 つの三角形とするとき、次の各命題の否定を、それと同じ内容を持つわかりやすい文章の命題に、書き換えよ。

(1) x は $x < -5$ または $x \geq 2$ を満たす。

(2) △ABC は 2 辺の長さが等しく、かつ、1 つの角が 90° である。

●ならば

2 つの命題 P と Q に対して「P ならば Q（P implies Q)」という命題を作ることができます。これは「P が成り立てば Q が成り立つ」という意味の命題です。この命題を「$P \Rightarrow Q$」あるいは「$Q \Leftarrow P$」と書き表わします。「$P \Rightarrow Q$」の真理表は次で与えられます (これが「$P \Rightarrow Q$」の真偽の定義と思って下さい)。

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

$P \Rightarrow Q$ の真理表

この表から、

P が偽であれば、Q の真偽にかかわらず、命題「$P \Rightarrow Q$」は真となる

ことがわかります。このことに違和感を覚える人もいるかもしれないので、ここで、何故「$P \Rightarrow Q$」の真偽をこのように定めるのか、納得するための材料を提供しておきます。

例 2-3 ある科目の授業を受けていた A 君は、期末試験が近づいてきたある日、その科目を教えている先生に成績について相談に行きました。そして、「君が期末試験で 80 点以上をとれば、この科目の成績に優を受け取とることができる」と言われたとします。その後 A 君は期末試験を受け、1 カ月後に成績を受け取りました。成績を見た A 君は先生の言ったことを正しかったと思うでしょうか、思わないでしょうか？

このことについて考えるために、P, Q をそれぞれ次のようにおきます。

P：A 君が期末試験で 80 点以上をとる

Q：A 君がこの科目の成績に優を受け取とる

このとき、P が真であるか偽であるか、Q が真であるか偽であるかに応じて、4 つの場合が考えられます。

① P と Q がともに真の場合：

この場合、A 君は期末試験で 80 点以上をとり、この科目の成績に優を受け取とることができたことになります。先生は言った通りのことを実行したのですから、疑うことなく、A 君は先生の言ったことは正しかったと思うでしょう。

② P が真で、Q が偽の場合：

この場合、A 君は期末試験で 80 点以上をとったのに、この科目の成績が優でなかったことになります。先生は明らかに嘘を言ったことになるので、A 君は先生が言ったことは正しくなかったと思うでしょう。

③ P が偽で、Q が真の場合：

この場合、A 君は期末試験で 80 点に満たなかったにもかかわらず、この科目の成績に優を受け取ったことになります。先生は「期末試験で 80 点以上をとったとしたら、優を受け取とることができる」ということを言ったのであり、期末試験で 80 点をとれなかった場合については何も言っていません。したがって、80 点に満たなかったとしても、なんらかの理由 (例えば、期末試験以外の部分の評価がよかった結果) で優をとることができたと考えられるので、A 君は先生の発言に間違っているところはなかった、つまり正しかった、と思うでしょう。

④ P と Q がともに偽の場合：

この場合、A 君は期末試験で 80 点に満たず、この科目の成績が優でなかったことになります。A 君は期末試験で 80 点に満たなかったので、優が取れなかったのは仕方がないと納得し、先生の言ったことは正しかったと思うでしょう。

P	Q	$P \Rightarrow Q$
80 点以上をとった	優を受け取った	先生の言ったことは正しかった
80 点以上をとった	優を受け取らなかった	先生の言ったことは正しくなかった
80 点未満だった	優を受け取った	先生の言ったことは正しかった
80 点未満だった	優を受け取らなかった	先生の言ったことは正しかった

さて、A 君が「先生は正しいことを言った」と思ったときを真、そう思えなかったときを偽として、先生の言ったことを「$P \Rightarrow Q$」という命題とみなしてみましょう。するとその真偽は、P, Q の真偽がいずれであっても、「$P \Rightarrow Q$」の真理表にある結果と一致することがわかります。 □

次に、「ならば」の否定について考えます。

例 2-4 n を 1 つの自然数とする。このとき、次の命題 R について考える。

R：「n が奇数であるならば n^2 は奇数である。」

(1) $n = 2$ のとき、R は真か偽かを判定せよ。

(2) R の否定を、それと同じ内容を持つわかりやすい文章の命題に、書き換えよ。

解;

(1) 2 は奇数ではないので、「⇒」の真理表により、R は真である。

(2) 命題 R の否定は

「“n が奇数であるならば n^2 は奇数である”ということではない」

となる。これは

「“n が奇数である”、にもかかわらず、“n^2 は奇数である、ということではない”」

つまり、

「n が奇数である、にもかかわらず、n^2 は偶数である」

ということを意味する。結局、$\overline{R}$ は、その内容を変えずに、

「n は奇数であって、かつ、n^2 は偶数である」

と書き換えられる。 □

注意：(1) は (2) を使って説明することもできます。背理法を使います。$n=2$ のとき、R は偽であったと仮定します。すると、$\overline{R}$ は真になります。(2) の解より、$\overline{R}$ は「n は奇数であって、かつ、n^2 は偶数である」と同じ内容を持っていましたから、「2 は奇数であって、かつ、2^2 は偶数である」が成り立たなければなりません。しかし、これは 2 が偶数であるということに矛盾します。よって、背理法により、$n=2$ のとき、R は真であることがわかります。

演習 2-3* n を 1 つの自然数として、命題

「n が偶数ならば $\dfrac{n^2}{4}$ は偶数である」

について考える。$n=1$ のとき、$n=2$ のとき、$n=3$ のとき、$n=4$ のときの各場合について、上の命題の真偽を判定せよ。

演習 2-4* 2 つの命題 P と Q に対して、$\overline{P}\vee Q$ の真理表を作成し、$\overline{P}\vee Q$ の真偽と $P\Rightarrow Q$ の真偽が一致することを確かめよ。(ヒント：$\overline{P}\vee Q$ の真理表を書くときは、$P, Q, \overline{P}, \overline{P}\vee Q$ と最上行に書くことから始めるとよい。)

命題 P と Q の間に何の関係がなくても「P ならば Q」という命題をいつでも作ることができるので、論理の形式的面から言えば、命題「P ならば Q」において P が「原因 (条件)」で Q がその「結果」を表わしているわけではありません。しかしながら、次の節の冒頭で説明するように、数学の証明や説明において接続詞「ならば」が用いられる場合、“P という命題や条件から Q という命題や条件が導かれる”というニュアンスが含まれることがしばしばあります。

§2-2 命題の同値

2 つの命題 P, Q について、それらの文章表現は違っていても、“論理的な内容が同じ”であるとき、P と Q は同値であるといいます。私たちが、2-1 節の例や演習において観察したことは、命題の否定を意味のわかりやすい同値な命題に書き換えるということだったのです。ここでは、命題の同値という概念について説明します。

●仮定と結論

数学では、定理を述べるときに、

- 「もし、○○○ (という条件や命題) が成り立つならば、このとき、△△△△ (という条件や命題) が成り立つ」とか
- 「○○○と仮定すると、△△△△が成り立つ (あるいは、△△△△となる)」

という言い方をよくします。これは、命題「○○○ $\Rightarrow$ △△△△」が真である、ということを意味しています。「○○○」を定理の**仮定** (assumption) といい、「△△△△」を定理の**結論** (conclusion) と言います。

この言い方に習って、2つの命題 P, Q について、命題「$P \Rightarrow Q$」が真であるとき、“P という仮定から Q という結論が導かれる”と言うことがあります。

●同値

2つの命題 P, Q について、命題「$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$」が真であるとき、$P$ は Q と**同値** (equivalent) である、あるいは、P が成り立つことと Q が成り立つこととは同値である、あるいは、P は Q であるための**必要十分条件** (necessary and sufficient condition) であると言います。P が Q と同値であることを

$$(P \text{ と } Q \text{ の間に}) \quad P \Longleftrightarrow Q \quad (\text{という関係}) \text{が成り立つ}$$

と書き表わします。

同値の定義により、P が Q と同値であるのは、P と Q の真偽が一致するとき（つまり、真理表が右表のようになるとき)、かつ、そのときに限ります。真理表を書くことにより、次を証明することができます。

P	Q
T	T
F	F

定理 2-5

(1) 命題 P に対して、$P \Longleftrightarrow P$ が成り立つ。

(2) 2つの命題 P, Q の間に、$P \Longleftrightarrow Q$ が成り立つならば、

(a) $Q \Longleftrightarrow P$ も成り立つ。

(b) $\overline{P} \Longleftrightarrow \overline{Q}$ も成り立つ。

(c) 勝手な命題 R に対して、$P \wedge R \Longleftrightarrow Q \wedge R$ が成り立つ。

(d) 勝手な命題 R に対して、$P \vee R \Longleftrightarrow Q \vee R$ が成り立つ。

(3) 3つの命題 P, Q, R の間に、$P \Longleftrightarrow Q$ が成り立ち、$Q \Longleftrightarrow R$ が成り立つならば、$P \Longleftrightarrow R$ も成り立つ。

例 2-6 命題 P, Q について次が成り立つ。

(1) (**ド・モルガンの法則**) $\overline{P \wedge Q} \iff \overline{P} \vee \overline{Q}$, $\overline{P \vee Q} \iff \overline{P} \wedge \overline{Q}$

(2) $P \Rightarrow Q \iff \overline{P} \vee Q$

解；

(1) $\overline{P \wedge Q}$ と $\overline{P} \vee \overline{Q}$ の真理表が下のようになることから、「$\overline{P \wedge Q} \iff \overline{P} \vee \overline{Q}$」が成り立つことがわかる。

P	Q	$P \wedge Q$	$\overline{P \wedge Q}$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

P	Q	$\overline{P}$	$\overline{Q}$	$\overline{P} \vee \overline{Q}$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

$\overline{P \vee Q}$ と $\overline{P} \wedge \overline{Q}$ の真理表が下のようになることから、「$\overline{P \vee Q} \iff \overline{P} \wedge \overline{Q}$」が成り立つことがわかる。

P	Q	$P \vee Q$	$\overline{P \vee Q}$
T	T	T	F
T	F	T	F
F	T	T	F
F	F	F	T

P	Q	$\overline{P}$	$\overline{Q}$	$\overline{P} \wedge \overline{Q}$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

(2) が成り立つことは演習 2-4 ですでに確かめられている。 □

上の例のように真理表を書くことにより、次の定理を証明することができます。

定理 2-7

命題 P, Q, R に対して次が成り立つ。

(1) (二重否定の除去) $\overline{\overline{P}} \iff P$

(2) (冪等律) $P \wedge P \iff P$,
$P \vee P \iff P$

(3) (交換律) $P \wedge Q \iff Q \wedge P$,
$P \vee Q \iff Q \vee P$

(4) (結合律) $(P \wedge Q) \wedge R \iff P \wedge (Q \wedge R)$,
$(P \vee Q) \vee R \iff P \vee (Q \vee R)$

(5) (分配律) $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$,
$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$

演習 2-5 命題 P, Q について、次が成り立つことを示せ (定理 2-5、例 2-6、定理 2-7 から導いてもよいし、真理表を書いて確かめてもよい)。

(1) $\overline{P \Rightarrow Q} \iff P \wedge \overline{Q}$

(2) $P \Rightarrow Q \iff \overline{Q} \Rightarrow \overline{P}$

注意：上の問題の (1) は背理法と関連があります。定理が「P ならば Q」という形で与えられているとき、P と $\overline{Q}$ が同時に成り立つと仮定して、矛盾を導くという証明法が背理法でした。矛盾が起きれば、仮定「P と $\overline{Q}$ が同時に成り立つ」は誤りということになりますから、(1) によって、$\overline{P \Rightarrow Q}$ が成り立たない、つまり、$P \Rightarrow Q$ が成り立つことになります。

●逆と対偶

2 つの命題 P, Q が与えられたとき、「$P \Rightarrow Q$」という命題を考えることができました。これ以外にも、「$Q \Rightarrow P$」「$\overline{Q} \Rightarrow \overline{P}$」「$\overline{P} \Rightarrow \overline{Q}$」といった命題を考えることができます。

命題「$Q \Rightarrow P$」を命題「$P \Rightarrow Q$」の**逆** (converse) といい、
命題「$\overline{Q} \Rightarrow \overline{P}$」を命題「$P \Rightarrow Q$」の**対偶** (contraposition) といいます。

「ならば」を含む命題については、命題「$P \Rightarrow Q$」の真偽とその対偶「$\overline{Q} \Rightarrow \overline{P}$」の真偽はぴったり一致する (演習 2-5(2) 参照)、という事実が重要です。このことから、命題「$P \Rightarrow Q$」が真であることを証明するために、その対偶「$\overline{Q} \Rightarrow \overline{P}$」が真であることを証明してもよいことがわかります。つまり、

“P という仮定から Q という結論が導かれること”

を示す代わりに、

“Q ではないという仮定から P ではないという結論を導いてもよい”

のです。

一方、命題「$P \Rightarrow Q$」の真偽とその逆「$Q \Rightarrow P$」の真偽は必ずしも一致しません。このことは、定理の逆を証明しても、その定理自体を証明したことにならないことを意味します。命題「$P \Rightarrow Q$」の真偽とその逆「$Q \Rightarrow P$」の真偽が一致するのは、P と Q が同値な命題の場合に限ります。

演習 2-6 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ を成分が実数からなる 2 つの 2×2 行列とするとき、
①次の命題 R の対偶、および、逆を書け。

$$R : 「A = B = O \text{ ならば } AB = O \text{ である。}」$$

ここで、O は零行列を表わす。
②そして、R の対偶を、それと同じ内容を持つわかりやすい文章の命題に、書き換えよ。
③さらに、対偶、逆のそれぞれについて、真か偽かを判定せよ (理由も簡単につけること)。

● 恒真式（トートロジー）

文字 P, Q, R に関する次の 3 つの“式”を考えてみましょう。

$$\begin{aligned} f(P,Q) &= (\overline{P} \Rightarrow (Q \wedge \overline{Q})) \Rightarrow P \\ g(P,Q) &= (P \wedge (P \Rightarrow Q)) \Rightarrow Q \\ h(P,Q,R) &= ((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R) \end{aligned}$$

$f(P,Q),\ g(P,Q),\ h(P,Q,R)$ は、P, Q, R に具体的な命題を代入するごとに 1 つの命題を与える式になっています。一般に、いくつかの文字と論理記号からなるこのような式を**論理式** (formula) といいます。真理表を作成することにより、$f(P,Q),\ g(P,Q),\ h(P,Q,R)$ は、どのような命題 P, Q, R についても常に真であることがわかります。このような論理式を**恒真式** (tautology) と呼びます。

$f(P,Q)$ は「P ではないという仮定から Q かつ $\overline{Q}$ という結論が導かれたとしたら、P が成り立つ」ということを意味している論理式であると解釈できます。つまり、恒真式 $f(P,Q)$ は背理法を論理式で表わしたものと思うことができます。同様の解釈により、恒真式 $g(P,Q),\ h(P,Q,R)$ は三段論法を論理式で表わしたものと思うことができます。

演習 2-7 上で与えた 3 つの論理式 $f(P,Q),\ g(P,Q),\ h(P,Q,R)$ がいずれも恒真式になっていることを確かめよ。

§3. 集合の概念と習慣的に使われる記号

集合は現代数学の根幹に位置するとても大切な概念です。そこで、この節の前半では、集合についての基礎（集合の書き表わし方や空集合、部分集合、集合の相等などの概念）を身につけましょう。後半では、$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ や $:=$, $\forall$, $\exists$, $\because$ などの、数学の授業で日常的・習慣的によく使われる記号の意味や使い方を学びましょう。

§3-1 集合の記法と概念

集合 (set) とは、“もの”の集まりであって、その集まりがどのような“もの”からなるかが「客観的に規定されているもの」をいいいます。集合 A に対して、それを構成している個々の“もの”を A の**元**(げん)(element) または**要素**といいます。

例 3-1　次はいずれも集合である。

(1) 数 $1, 2, 3, 4$ からなる集まり
(2) 3 で割って 2 余る自然数の集まり
(3) ひらがなの集まり

これに対して、次はどれも集合でない。

(4) 歌が上手な阪大生の集まり
(5) 大きな数の集まり

●集合の記法

集合は中括弧 { } を使って書き表わします。その書き表わし方には以下の２通りの方法があります。

①元を書き並べる方法（**外延的記法**と呼ばれます）

この記法は、集合を構成している元の個数が有限個である場合に可能です。例えば、数 $1, 2, 3, 4$ からなる集合は $\{1, 2, 3, 4\}$ のように書き表わします。

元を書き並べる順番は気にしません。$\{2, 3, 1, 4\}$, $\{4, 1, 3, 2\}$, $\{1, 2, 4, 3\}$ はすべて $1, 2, 3, 4$ からなる集合を表わします。

また、同じ元を２回以上書いても構いません。例えば、$\{2, 3, 1, 4, 4\}$ も $1, 2, 3, 4$ からなる集合を表わしています。

②条件を書き記す方法（**内包的記法**と呼ばれます）

例えば、正の偶数全体からなる集合は、$\{\, x \mid x$ は正の偶数である $\}$ のように書き表わします。一般に、○○○を満たすもの全部からなる集合を書き表わしたいとき、

$$\{\, x \mid x \text{ は○○○を満たす} \}\quad \text{あるいは}\quad \{\, x \mid x \text{ は○○○である} \}$$

という書き方をします。“ $\mid$ ”よりも“ $:$ ”を好む人は、

$$\{\, x : x \text{ は○○○を満たす} \}\quad \text{あるいは}\quad \{\, x : x \text{ は○○○である} \}$$

という書き方をします。

演習 3-1* 次の各集合を２通りの方法 (元を書き並べる方法と条件を書き記す方法) で表わせ。

(1) サイコロの目の数からなる集合
(2) アルファベットの母音からなる集合

x が集合 A の元であることを x は A に**属する** (x belongs to A) または A は x を (元として) **含む**といい、$x \in A$ または $A \ni x$ と書き表わします。逆に、x が集合 A の元でないことを $x \notin A$ または $A \not\ni x$ のように書き表わします。

例 3-2　A を偶数全体からなる集合としたとき、$2 \in A$ であるが $1 \notin A$ である。

x と y がともに集合 A の元であることを、記号で、$x \in A,\ y \in A$ や $A \ni x,\ A \ni y$ のように表わしますが、これを $x, y \in A$ または $A \ni x, y$ と略記します。同様に、x, y, z がともに集合 A の元であることを $x, y, z \in A$ や $A \ni x, y, z$ と略記します。もっと個数が増えた場合も同様の略記の仕方をします。

集合の書き表わし方のバリエーション

① ある集合 A が与えられているときに、A の元であって、○○○という条件を満たすようなもの全体からなる集合を考えたい場合があります。このようなときには、

$$\{\ x \in A \mid x \text{ は○○○を満たす}\ \}$$

という書き方をよくします。これは、もともとの書き方で、

$$\{\ x \mid x \in A\text{、かつ、}x \text{ は○○○を満たす}\ \}$$

と書いていたものと同じ集合を表わします。例えば、集合 A を偶数全体からなる集合としたとき、A の元であって、3 で割り切れるものだけを集めて作った集合は、

$$\{\ x \in A \mid x \text{ は } 3 \text{ で割り切れる}\ \}$$

のように書き表わされます。

② 奇数をすべて集めた集合を書き表わしたい場合には、$\{\ x \mid x \text{ は奇数である}\ \}$ と書くのが正式ですが、これを

$$\{\ 2n+1 \mid n \text{ は整数}\ \}$$

と書いたりします。もっと大胆に、{ 奇数の全体 } のように書いてしまうこともあります。但し、後者の書き方は、「奇数の全体」を 1 つの元とみて、その元だけからなる集合を表わしているとも解釈することができるので、誤解が生じ得る状況では使えません。

③ 0 以上 1000 以下の整数からなる集合を $\{0, 1, 2, \cdots, 1000\}$ のように書くことがあります。また、1 以上の整数全体からなる集合を $\{1, 2, 3, \cdots\cdots\}$ のように書くことがあります。この記法は、前後の記述から「$\cdots$」に入るべきものが明確な場合に限り、使うことができます。

演習 3-2　$\{\ 2m+3n \mid m \text{ と } n \text{ は整数}\ \}$ と表わされる集合に 1 は属するか？

● 空集合（くうしゅうごう）

$\{\ x \mid x \text{ は } x^2 = -1 \text{ を満たす実数}\ \}$ のような、元をまったく持たない集合を**空集合** (empty set) といい、$\varnothing$（本によっては $\emptyset$）という記号で書き表わします。記号 $\varnothing$ はギリシア文字の ϕ と区別して使われますが、授業で板書するときは ϕ で代用することもあるようです。

空集合でない集合（すなわち、少なくとも 1 つは元を持つ集合）のことを **空(くう) でない** (non-empty) 集合とも呼びます。

注意：空集合 $\varnothing$ を $\{\varnothing\}$ のように書いてはいけません。集合 $\{\varnothing\}$ は $\varnothing$ という元を持っている集合であり、空集合とは異なります。$\varnothing$ はそれ自体で 1 つも元を持たない集合を表わしています。

●部分集合

集合 B が集合 A の**部分集合** (subset) であるとは、B に属するどの元も A の元になっているときをいいます。「集合 B に属するどの元も集合 A の元である」という事実を、論理記号の「$\Rightarrow$」を借用して、

$$\text{“}x \in B \ \Rightarrow \ x \in A\text{”}$$

と書き表わします。B が A の部分集合であるとは、条件“$x \in B \ \Rightarrow \ x \in A$”が成り立つときである、と言い換えることができます。

集合 B が集合 A の部分集合であることを、$B \subset A$ あるいは $A \supset B$ のように書き表わし、「B は A に**含まれる** (B is contained in A)」または「A は B を**含む**」と読みます。また、B が A の部分集合でないことを $B \not\subset A$ あるいは $A \not\supset B$ と書き表わします。

例 3-3　3 つの集合 $A = \{1, 3, 6\},\ B = \{1, 2, 4, 6\},\ C = \{1, 2, 3, 6\}$ を考える。

(1) A は C の部分集合である（記号を使って書くと、$A \subset C$ である）。なぜならば、A に属するどの元（つまり、1, 3, 6 のいずれについて) もすべて C の元になっているからである。

(2) B は C の部分集合ではない（記号を使って書くと、$B \not\subset C$ である）。なぜならば、B に属する元 4 は C に属さないからである。

注意：「$\subset$」「$\supset$」のことを「包む」「包まれる」と呼ぶ教科書もあります。また、「$\subset$」「$\supset$」の代わりに「$\subseteq$」「$\supseteq$」や「$\subseteqq$」「$\supseteqq$」を使う教科書もあります。これらの記号を用いる教科書においては、「$\subset$」「$\supset$」はそれぞれ「$\subseteq$ かつ $\neq$ 」「$\supseteq$ かつ $\neq$ 」の意味で使われるので注意しましょう。

部分集合に関しては次の 2 つの事実が基本的です。

❶ どのような集合 A に対しても、空集合 $\varnothing$ は A の部分集合である（と約束する）。
❷ どのような集合 A に対しても、A は A 自身を部分集合として含む、すなわち、$A \subset A$ である。

❷が成立することは部分集合の定義から疑う余地のないことですが、❶に関しては疑問に思う人もいるのではないでしょうか。このように約束する理由（正当性・妥当性）を簡単に説明しておきましょう。

仮に $B = \varnothing$（空集合）が集合 A の部分集合でなかったとすると、どのようなことが起こるのかを考察してみましょう。部分集合の定義により、$B \subset A$ は B に属するどのような元も A の元であることを意味するのでしたから、その否定 $B \not\subset A$ は、B の元の中には A の元でないものがある、ということになります。このことを $B = \varnothing$ の場合に当てはめると、空集合 B の中に（A に属さない）元があることが結論されます。これは空集合の定義に矛盾します。このような理由から、「空集合はどんな集合の部分集合にもなっている」（と約束しておく）のです。

演習 3-3　集合 {1,2,3} の部分集合をすべて書け。

●集合の相等

２つの集合 A と B が**等しい**とは、$A \subset B$ かつ $B \subset A$ が成り立つときをいいます。このことを $A = B$ と書き表わします。また、２つの集合 A と B が等しくないことを $A \neq B$ と書き表わします。

例 3-4

(1) ２つの集合 $A = \{1, 2, 3, 4\}$ と $B = \{\ x \mid x$ は 1 以上 4 以下の整数 $\}$ は等しい、すなわち、$A = B$ である。

(2) ２つの集合

$A = \{\ x \mid x$ は単語 *ishibashi* に使われているアルファベット $\}$,

$B = \{\ x \mid x$ は単語 *toyonaka* に使われているアルファベット $\}$

は等しくない、すなわち、$A \neq B$ である。なぜならば、$s \in A$ であるのに、$s \notin B$ であるからである。

演習 3-4* 集合

$A = \{1, 4, 7\}$,

$B = \{\ x \mid x$ は 3 で割ると 1 余る整数 $\}$,

$C = \{\ x \mid\ x$ は $x^2 = 4$ を満たす奇数 $\}$,

$D = \{1, 4\}$

について、次は成り立つか？簡単な理由をつけて答えよ。

(1) $A \subset B$　　(2) $A \supset C$　　(3) $A = D$

(4) $D \not\subset A$　　(5) $D \not\supset B$　　(6) $D \neq C$

§3-2 習慣的に使われる記号

数学の教科書や授業は、沢山の記号で溢れています。記号を上手に使うと、書く時間の節約になるばかりでなく、命題や推論を明解に表現できるようになります。ここでは、特に多く使われる記号について、その意味と使い方を説明します。

●数の集合を表わす記号

数の集合に関しては、習慣的に次の記号を用います。

$\mathbb{N} = \{$ 自然数 (natural number) の全体 $\} = \{1, 2, 3, \cdots\cdots\}$

$\mathbb{Z} = \{$ 整数 (integer) の全体 $\} = \{\cdots\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\cdots\}$

$\mathbb{Q} = \{$ 有理数 (rational number) の全体 $\} = \{\ \frac{r}{s} \mid r, s \in \mathbb{Z}$ かつ $s \neq 0\ \}$

$\mathbb{R} = \{$ 実数 (real number) の全体 $\}$

$\mathbb{C} = \{$ 複素数 (complex number) の全体 $\} = \{a + ib \mid a, b \in \mathbb{R}\ \}$ (但し、i は虚数単位)

注意：1. 整数全体からなる集合を $\mathbb{Z}$ で表わし、有理数全体からなる集合を $\mathbb{Q}$ で表わすのは、それぞれ、数を意味するドイツ語 Zahl と商を意味する英語 quotient の頭文字に由来します。

2. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ が成り立っています。
3. 教科書によっては、$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ の代わりに $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ が使われます。
4. この授業では自然数に 0 を含めていませんが、自然数に 0 を含める流儀もあります。

●カンマによる「かつ」の省略

一般に、2つ以上の条件がカンマ「,」で区切られている場合、そのカンマ「,」は「かつ」を意味します。

例 3-5 $0 < |x-1| < 2,\ x \geq 0$ を満たす実数 x を考える、と書いてあれば、それは、
「$0 < |x-1| < 2$ かつ $x \geq 0$」を満たす実数 x を考える、ということを意味します。

カンマを使って「かつ」を省略することはできますが、「または」を省略することは (方程式の解を書き並べるときなどの慣例を除いて) できません。

例 3-6 集合 $\{\, x \in \mathbb{R} \mid -1 \leq x < 2 \text{ または } x \geq 3 \,\}$ を $\{\, x \in \mathbb{R} \mid -1 \leq x < 2,\ x \geq 3 \,\}$ のように書くことはできません。これは $\{\, x \in \mathbb{R} \mid -1 \leq x < 2 \text{ かつ } x \geq 3 \,\}$ という集合を表わし、もともとの集合とは違う集合です。

●「$\Longrightarrow$」という論理記号

数学の授業で使われる記号「$\Longrightarrow$」は、2-1 節で説明した論理における「ならば」として使われるよりも、

「○○○という条件や命題から△△△という条件や命題が得られる」

という意味を暗示的に含んで使われることが多いようです (2-2 節における仮定と結論の説明を参照)。このような「$\Longrightarrow$」の使い方は、特に、証明の記述の中に顕著に見られます。

●「$\Longleftrightarrow$」という論理記号

記号「$\Longleftrightarrow$」は、2-2 節で説明したように、2つの命題が同値であることを表わすときに使います。必要十分であることを強調したいときには、$\underset{\text{iff}}{\Longleftrightarrow}$ や $\overset{\text{iff}}{\Longleftrightarrow}$ という記号を使うこともあります。ここで、「iff」は「if and only if」の略です。

例 3-7 (ピタゴラスの定理) △ABC について、

$$\angle \mathrm{A} = 90^\circ \iff \mathrm{AB}^2 + \mathrm{AC}^2 = \mathrm{BC}^2$$

が成り立つ。

読み方と意味: △ABC について、$\angle \mathrm{A} = 90^\circ$ であるための必要十分条件は、$\mathrm{AB}^2 + \mathrm{AC}^2 = \mathrm{BC}^2$ が成り立つことである。

コメント：数学の教科書や授業では“ が成り立つ。”という部分はしばしば省略されます。

●「存在」と「任意」を表わす記号

記号「∃」は「○○○が存在する」ということを意味する記号です。「∃」という記号は、“exist”の頭文字の大文字 E を左右反転して作られています。

記号「∀」は「すべての○○○について……」ということを意味する記号です。「∀」という記号は、“ all ”の頭文字の大文字 A を上下反転して作られています。

例 3-8

(1) $\forall\,\alpha \in \mathbb{R},\ \exists\, n \in \mathbb{Z}$ s.t. $n \leq \alpha < n+1$

英文：For all $\alpha \in \mathbb{R}$ there exists an element $n \in \mathbb{Z}$ such that $n \leq \alpha < n+1$.

読み：すべての実数 α に対して、整数 n が存在して、$n \leq \alpha < n+1$ である。

意味：すべての実数 α に対して、$n \leq \alpha < n+1$ を満たす、整数 n が存在する。

(2) $0 \neq z \in \mathbb{C} \implies \exists\, r, \theta \in \mathbb{R}$ s.t. $z = r(\cos\theta + i\sin\theta),\ r > 0$

英文：If a complex number z is not zero, then there exist real numbers r and θ such that $z = r(\cos\theta + i\sin\theta)$ and $r > 0$.

読み：複素数 z が 0 でないならば、実数 r と実数 θ が存在して、$z = r(\cos\theta + i\sin\theta)$ であり、かつ、$r > 0$ である。

意味：複素数 z が 0 でなければ、$z = r(\cos\theta + i\sin\theta)$ を満たす正の実数 r と実数 θ が存在する。

コメント：1.「∀」は「すべての」と読むよりもむしろ、「任意の」と読むことのほうが多いかもしれません。**任意** (any, arbitrary) とは、作為性がないという意味です。

“$\forall\, s \in S$”＝“集合 S に属するすべての元 s について”

＝“集合 S から任意に取った (つまり、無作為に選んだ) s について”

2.“s.t.”は“such that”の略です。“〜 such that ―”は“― であるような 〜”という意味を持っています。

●唯一つ存在することを意味する記号

数学では、条件△△△を満たすものが唯一つしかないことを、

「条件△△△を満たすものは**一意的**(いちいてき)(unique) である」

と表現します。例えば、例 3-8(1) において、実数 α に対して条件 $n \leq \alpha < n+1$ を満たす整数 n は唯一つですから、このことを“$n \leq \alpha < n+1$ を満たす整数 n は一意的である”と表現します。

ここで 1 つ注意して欲しいことは、「一意的である」とは、「もし、その条件を満たすものがあれば、それは唯一つである」ということであって、実際にその条件を満たすものが存在するかどうかは問わない ということです。

「条件△△△を満たす○○○が存在して、かつ、その条件を満たす○○○が唯一つしかない」ことを言い表わしたいときには、

「△△△を満たす○○○は一意的に存在する」

といいます。「一意的に存在する」ことを意味する記号としては「∃!」や「∃1」が用いられます。例えば、

$$\forall\, \alpha \in \mathbb{R},\ \exists!\, n \in \mathbb{Z}\ \ \text{s.t.}\ \ n \leq \alpha < n+1$$

のように書きます。なお、「一意的である」ことのみを意味する記号はありません。

演習 3-5 *

(1) 次の文章を、$\forall, \exists$ などの論理記号を使って書き直せ。

どんな自然数 n に対しても、$|\sqrt{2} - r| < \frac{1}{n}$ となる有理数 r が存在する。

(2) 次の論理記号で表わされた文章を、論理記号のない文章に書き直せ。

$$a, b \in \mathbb{Z},\ b > 0 \implies \exists!\, q, r \in \mathbb{Z}\ \ \text{s.t.}\ \ a = qb + r,\ 0 \leq r < b$$

●何かを定義したいときに使われる記号

次のような記号がよく使われます。

$$:=,\quad \underset{\text{def}}{=},\quad \overset{\text{def}}{=},\quad \underset{\text{def}}{\Longleftrightarrow},\quad \overset{\text{def}}{\Longleftrightarrow}$$

使い方

① $A := B$ または $A \underset{\text{def}}{=} B$ または $A \overset{\text{def}}{=} B$ と書いて、「A を B によって定義する」ということを表わします。

② $A \underset{\text{def}}{\Longleftrightarrow} B$ または $A \overset{\text{def}}{\Longleftrightarrow} B$ と書いて、「A を B によって定義する」ということを表わします。

注意：1. B の方に既知の量、もの、性質が入り、A の方にこれから定めようとする量、もの、性質に対する名前や記号が入ります。

2. ②の書き方で、定義を書いていることが前後の文脈から明確な場合、単に、$A \iff B$ と書く場合もあります。

例 3-9

(1) $S := \{\, x \in \mathbb{R} \mid x^2 + ax + b > 0 \,\}$

読み：S を、x という実数であって、$x^2 + ax + b > 0$ を満たすもの全体からなる集合として定義する。

意味：右辺の集合を S という記号で書く。

(2) $n, q \in \mathbb{Z},\ q \neq 0$ とする。このとき、

$$q : n \text{ の } \textbf{約数} \overset{\text{def}}{\Longleftrightarrow} \exists\, p \in \mathbb{Z}\ \ \text{s.t.}\ \ n = pq$$

読み：「q が n の約数である」ということを次のように定義する、「ある p という整数が存在して、$n = pq$ を満たす。」

意味：q が n の約数であるとは、$n = pq$ となる整数 p が存在するときをいう。

演習 3-6　次の記号化された文章の意味を書け。

(1) 平面上の 3 点 A, B, C に対して、

$$\text{A, B, C が同一直線上にある} \overset{\text{iff}}{\iff} \exists k \in \mathbb{R} \ \text{ s.t. } \overrightarrow{\text{AC}} = k\overrightarrow{\text{BC}}$$

(2) $f(x)$：$\mathbb{R}$ 上で定義された関数　とする。このとき、

$$f(x)：\textbf{奇関数} \overset{\text{def}}{\iff} \forall x \in \mathbb{R},\ f(-x) = -f(x)$$

●「故に」と「何故ならば」

「$\therefore$」は「ゆえに (therefore)」、「$\because$」は「何故ならば (because)」と読みます。記号の意味は、その読み方の通りです。

大学の授業では、「$\therefore$」よりも「$\because$」という記号の方が多く用いられます。最初に、証明したい命題を提示し、次に、「$\because$」と書いて、それを証明していきます。

例 3-10　$a, b, c \in \mathbb{R}$ に対して、

$$a^2 + b^2 + c^2 \geq ab + bc + ca$$

が成り立つ。

$\because$

$$\begin{aligned} a^2 + b^2 + c^2 - (ab + bc + ca) &= \frac{1}{2}(a^2 - 2ab + b^2 + b^2 - 2bc + c^2 + c^2 - 2ca + a^2) \\ &= \frac{1}{2}\big((a-b)^2 + (b-c)^2 + (c-a)^2\big) \\ &\geq 0 \end{aligned}$$

$\therefore \quad a^2 + b^2 + c^2 \geq ab + bc + ca$　□

●証明の開始と終了を表わす記号

定理の証明を開始するときには、

$$\text{(Proof)},\quad \text{(証明)},\quad \because$$

などと宣言してから書き始めます。そして、定理の証明の最後には「ここで証明が完了した」ということを知らせるための印しを置きます。その印しとしては、

$$\square,\quad \blacksquare,\quad \text{(Q.E.D.)},\quad \text{(q.e.d.)},\quad \text{(証明終)},\quad //$$

が主に使われます。“Q.E.D.”とは、ラテン語の “quod erat demonstrandum”(これが証明されるべきことであった) の略です。

●「…」という記号

「…」という記号は便利なのでよく使われます。但し、この記号を使うことができるのは、前後の記述から「…」に入るべきものが明確な場合に限られます (集合の書き方のバリエーションの第③項を参照)。例えば、自然数 n に対して、「$a_1, \cdots, a_n$ を実数とする」あるいは「$a_1, \cdots, a_n \in \mathbb{R}$ とする」あるいは「$a_i \in \mathbb{R}\ \ (i = 1, \cdots, n)$ とする」のような記述は、1 から n までの各自然数 i について a_i と名付けられた実数が 1 つずつ定められている、ということを表わしています。

§4. 述語論理

数学における定理や定義は“すべての〜について…であるような—が存在する”という形で記述されることが少なくありません。“すべての〜について”という文章を書きたいときは記号 $\forall$ を使い、“—が存在する”という文章を書きたいときは記号 $\exists$ を使うのでした (第3節参照)。この節では、$\forall$ と $\exists$ の論理学上の扱い方を勉強します。$\forall$ と $\exists$ を含む命題の内容を正しく読み取り、その否定を書けるようになることがここでの目標です。

●命題関数

まず、x についての次の条件（文章）を考えてみましょう。

$$P(x) : x+3<7 \quad (x+3 \text{ は } 7 \text{ より小さい})$$

この $P(x)$ 自体は、命題というよりは、x を変数とする“命題関数”と見る方が自然です。というのは、$P(x)$ における x のところに、$1, \sqrt{2}, -\frac{3}{4}$ などの具体的な数 x_0 を代入することによって、命題 $P(x_0)$ が得られるからです。

一般に、x についての文章 $P(x)$ が集合 X を定義域とする**命題関数**（propositional function）であるとは、$P(x)$ における x のところに、X の元 x_0 を代入して得られる文章 $P(x_0)$ が、すべての $x_0 \in X$ について命題となるときをいいます。x をその命題関数の（X 内を動く）変数と呼びます。変数 x は好きな文字に変えても構いません。一方、文章が同じであっても、定義域が異なっていれば、異なる命題関数と考えます。これは、命題関数を x についての文章 $P(x)$ とその定義域 X との組 $(P(x),\ X)$ として捉えるということです。例えば、$P(x) : x+3<7$ の定義域として、実数全体 $\mathbb{R}$ を採用する命題関数と、整数全体 $\mathbb{Z}$ を採用する命題関数は異なった命題関数です。

演習 4-1　自然数全体 $\mathbb{N}$ を定義域とする、次のような命題関数 $P(n)$ を考える。

$$P(n)：n \text{ は偶数である} \ \Rightarrow\ \frac{n^2}{4} \text{ は偶数である}$$

$P(n_0)$ が真であるような $\mathbb{N}$ の元 n_0 全体からなる集合 T_P を求めよ。

●全称命題と存在命題

集合 X を定義域とする命題関数 $P(x)$ が与えられたとき、次のような2つの命題を作ることができます。

❶ すべての $x \in X$ について $P(x)$ である。

❷ ある $x \in X$ について $P(x)$ である。

❶の形の命題を**全称命題**（universal proposition）といい、❷の形の命題を**存在命題**（existential proposition）といいます。

全称命題は記号で

$$\forall x \in X,\ P(x) \quad \text{または} \quad P(x) \ \text{ for } {}^{\forall}x \in X \quad \text{または} \quad P(x) \ \text{ for all } x \in X$$

のように書き表わします。これらの記号は、“任意の $x \in X$ に対して、$P(x)$ である”とか“どのような $x \in X$ に対しても、$P(x)$ である”などとも読みます。

全称命題「$\forall\, x \in X,\ P(x)$」が真であるのは、X のどのような元 x_0 に対しても $P(x_0)$ が真であるときであり、全称命題「$\forall\, x \in X,\ P(x)$」が偽であるのは、$P(x_0)$ が偽であるような $x_0 \in X$ が少なくとも 1 つ存在するときです（これを全称命題の真偽の定義と思って下さい)。

一方、存在命題は記号で

$$\exists\, x \in X \text{ s.t. } P(x) \quad \text{または} \quad P(x) \ \text{ for } {}^{\exists} x \in X \quad \text{または} \quad P(x) \ \text{ for some } x \in X$$

のように書き表わします。これらの記号は、“ある $x \in X$ が存在して、$P(x)$ である”とか、“$P(x)$ であるような $x \in X$ が存在する”などとも読みます。

存在命題「$\exists\, x \in X$ s.t. $P(x)$」が真であるのは、$P(x_0)$ が真であるような元 $x_0 \in X$ が少なくとも 1 つ存在するときであり、存在命題「$\exists\, x \in X$ s.t. $P(x)$」が偽であるのは、X のどのような元 x_0 に対しても $P(x_0)$ が偽であるときです（これを存在命題の真偽の定義と思って下さい)。

全称命題と存在命題の真偽は、定義域である集合 X に依存する、ということに注意しましょう。

例 4-1

$$P(n)：n \text{ は素数である。}$$

とおく。各自然数 $n_0 \in \mathbb{N}$ について、$P(n_0)$ は命題となる。$\mathbb{N}$ の部分集合として、

$$A := \{\, n \in \mathbb{N} \mid n \text{ は偶数} \,\}, \quad B := \{2, 3, 5, 7, 11, 13\}$$

を考える。

(1) 全称命題「$\forall\, n \in A,\ P(n)$」は偽であり、存在命題「$\exists\, n \in A$ s.t. $P(n)$」は真である。

(2) 全称命題「$\forall\, n \in B,\ P(n)$」は真であり、存在命題「$\exists\, n \in B$ s.t. $P(n)$」も真である。

解；

(1) 4 は偶数なので集合 A に属しているが、素数ではないので、$P(4)$ は偽である。したがって、全称命題「$\forall\, n \in A,\ P(n)$」は偽である。

一方、$2 \in A$ は素数なので、$P(2)$ は真である。したがって、存在命題「$\exists\, n \in A$ s.t. $P(n)$」は真である。

(2) 集合 B は自然数 $2, 3, 5, 7, 11, 13$ からなっており、そのいずれも素数である。つまり、命題 $P(2),\ P(3),\ P(5),\ P(7),\ P(11),\ P(13)$ はいずれも真である。したがって、全称命題「$\forall\, n \in B,\ P(n)$」は真である。

特に、B の元 2 について $P(2)$ は真であるから、存在命題「$\exists\, n \in B$ s.t. $P(n)$」も真である。 □

演習 4-2 *

$$P(x)：-7 \leq x + 3 < 7$$

とおく。各実数 $x_0 \in \mathbb{R}$ について、$P(x_0)$ は命題となる。

$A = \{\, x \in \mathbb{R} \mid x > 0 \,\}$ とおくとき、全称命題「$\forall\, x \in A,\ P(x)$」と存在命題「$\exists\, x \in A$ s.t. $P(x)$」のそれぞれについて、真であるか偽であるかを判定せよ。

全称命題・存在命題の書き表わし方には、いくつかのバリエーションがあります。ここでは、解析学の授業でよく使われる書き方を２つ紹介しておきます。

例 4-2

(1) 集合 $A = \{\, x \in \mathbb{R} \mid x > 0 \,\}$ を定義域とする命題関数 $P(x)$ が与えられたとき、全称命題「$\forall\, x \in A,\ P(x)$」と存在命題「$\exists\, x \in A$ s.t. $P(x)$」を、それぞれ、次のようにも書き表わします。

$$\text{全称命題：}\ {}^{\forall}x > 0,\ P(x) \quad \text{または} \quad P(x) \text{ for } {}^{\forall}x > 0$$

$$\text{存在命題：}\ {}^{\exists}x > 0 \ \text{ s.t. } P(x) \quad \text{または} \quad P(x) \text{ for } {}^{\exists}x > 0$$

(2) 集合 $B = \{\, x \in \mathbb{R} \mid a < x < b \,\}$（但し、$a, b$ は $a < b$ なる実数）を定義域とする命題関数 $P(x)$ が与えられたとき、全称命題「$\forall\, x \in B,\ P(x)$」と存在命題「$\exists\, x \in B$ s.t. $P(x)$」を、それぞれ、次のようにも書き表わします。

$$\text{全称命題：} a < {}^{\forall}x < b,\ P(x) \quad \text{または} \quad P(x) \ \text{ for } a < {}^{\forall}x < b$$

$$\text{存在命題：} a < {}^{\exists}x < b \ \text{ s.t. } P(x) \quad \text{または} \quad P(x) \ \text{ for } a < {}^{\exists}x < b$$

●ド・モルガンの法則 (de Morgan's law)

全称命題と存在命題の否定については、次が成り立ちます。

定理 4-3 (ド・モルガンの法則)

集合 X を定義域とする命題関数 $P(x)$ について、次が成り立つ。

(1) $\overline{\forall\, x \in X,\ P(x)} \iff \exists\, x \in X \text{ s.t. } \overline{P(x)}$

(2) $\overline{\exists\, x \in X \text{ s.t. } P(x)} \iff \forall\, x \in X,\ \overline{P(x)}$

例 4-4

$$P(n)：n \text{ は } 2 \text{ で割り切れるか、または、} 3 \text{ で割り切れる。}$$

とおく。各整数 $n_0 \in \mathbb{Z}$ について、$P(n_0)$ は命題となる。X を $\mathbb{Z}$ の部分集合とするとき、

(1) 全称命題「$\forall\, n \in X,\ P(n)$」の否定を、記号“$\forall$”や“$\exists$”を使わずに、わかりやすい同値な命題に書き換えよ。

(2) 存在命題「$\exists\, n \in X$ s.t. $P(n)$」の否定を、記号“$\forall$”や“$\exists$”を使わずに、わかりやすい同値な命題に書き換えよ。

解；

(1) ド・モルガンの法則により、全称命題「$\forall\, n \in X,\ P(n)$」の否定は、

$$\text{「}P(n) \text{ が成り立たないような } n \in X \text{ が存在する」}$$

と同値である。ここで、

$$P(n) \text{ が成り立たない} \iff n \text{ は } 2 \text{ でも、} 3 \text{ でも割り切れない} \quad \cdots\cdots\cdots (*)$$

であるから、全称命題「$\forall\, n \in X,\ P(n)$」の否定は、

$$\text{「}2 \text{ でも、} 3 \text{ でも割り切れないような、} X \text{ の元が存在する。」}$$

と書き換えることができる。

(2) ド・モルガンの法則により、存在命題「$\exists n \in X$ s.t. $P(n)$」の否定は、

「どのような $n \in X$ に対しても、$P(n)$ は成り立たない」

と同値である。$(*)$ により、これは、

「X のどのような元も、2 でも、3 でも割り切れない。」

と書き換えることができる。 □

演習 4-3 *

$$P(x) : x^2 \text{ は整数である。}$$

とおく。各実数 $x_0 \in \mathbb{R}$ について、$P(x_0)$ は命題となる。X を $\mathbb{R}$ の部分集合とするとき、次の問いに答えよ。

(1) 全称命題「$\forall x \in X,\ P(x)$」の否定を、記号“$\forall$”や“$\exists$”を使わずに、わかりやすい同値な命題に書き換えよ。

(2) 存在命題「$\exists x \in X$ s.t. $P(x)$」の否定を、記号“$\forall$”や“$\exists$”を使わずに、わかりやすい同値な命題に書き換えよ。

(3) $X = \mathbb{Q}$ の場合に、全称命題「$\forall x \in X,\ P(x)$」の否定と存在命題「$\exists x \in X$ s.t. $P(x)$」の否定のそれぞれについて、真であるか偽であるかを判定せよ。

●反例

集合 X を定義域とする命題関数 $P(x)$ が与えられているとします。このとき、$P(x_0)$ が偽であるような元 $x_0 \in X$ のことを、全称命題「$\forall x \in X,\ P(x)$」に対する**反例** (counterexample) といいます。

ド・モルガンの法則により、

$$\overline{\forall x \in X,\ P(x)} \iff \exists x \in X \text{ s.t. } \overline{P(x)}$$

が成り立つので、全称命題「$\forall x \in X,\ P(x)$」に対する反例を挙げる（すなわち、$P(x_0)$ が偽であるような元 $x_0 \in X$ を具体的に 1 つ与える）ことができれば、全称命題「$\forall x \in X,\ P(x)$」は偽であることが証明されたことになります。

例 4-5 次の各命題について、もし反例があるのであれば、それを 1 つ挙げよ。

(1) 任意の $x > 0$ について、$x^2 - 3x + 2 < 0$ である。

(2) $1 < x < \sqrt{2}$ を満たす任意の $x \in \mathbb{R}$ について、$x^2 - 3x + 2 < 0$ である。

解；

$x^2 - 3x + 2 = (x-1)(x-2)$ と因数分解できるから、実数 $x \in \mathbb{R}$ に対して、

$$x^2 - 3x + 2 < 0 \iff 1 < x < 2 \qquad \cdots\cdots\cdots\cdots (*)$$

となる。よって、$x_0 := 3\ (> 0)$ に対しては $x_0^2 - 3x_0 + 2 < 0$ が成り立たない。したがって、$3 \in \mathbb{R}$ は (1) の命題に対する 1 つの反例である。

一方、$x_0 \in \mathbb{R}$ が $1 < x_0 < \sqrt{2}$ であるならば、$1 < x_0 < 2$ であるから、$(*)$ によって、$x_0^2 - 3x_0 + 2 < 0$ となる。したがって、(2) の命題は真であり、反例はない。 □

演習 4-4　次の各命題について、真であるか偽であるかを判定せよ。また、偽の場合には反例を 1 つ挙げよ（ヒント：(2) については関数のグラフを考えるとよい)。

(1) 任意の $x > 0$ について、$x^3 - 3x + 2 > 0$ である。

(2) 任意の $x > 0$ について、$x \log x \geq 0$ である。

●「任意」と「存在」が混在する命題

次の 2 つの命題を考えてみましょう。

$$P: \ \forall x \in [-1,1],\ \exists y \in \mathbb{R} \ \text{ s.t. } \ x^2 + y^2 = 1$$
$$Q: \ \exists y \in \mathbb{R} \ \text{ s.t. } \forall x \in [-1,1],\ x^2 + y^2 = 1$$

但し、$[-1,1] := \{\, x \in \mathbb{R} \mid -1 \leq x \leq 1 \,\}$ と置きました。

この 2 つの命題 P と Q は、見かけはよく似ていますが、全く違う内容の命題です。実際、P は、

「任意の実数 $x \in [-1,1]$ に対して、“$x^2 + y^2 = 1$ であるような実数 y が存在する”」

ということを意味する命題ですが、Q は、

「“任意の実数 $x \in [-1,1]$ に対して、$x^2 + y^2 = 1$ である”ような実数 y が存在する」

ということを意味する命題です。その違いは、P における y は $x \in [-1,1]$ の選び方によって変わってもよいのに対し、Q における y は x に無関係でなければならない所にあります。

※まだ慣れていない人のために、命題の意味の取り方を復習しておきます。

論理記号を使って書かれた命題は、英語の文章を記号化したものなので、左から順に読んでいきます。

最初に命題 P について説明します。

$$P: \ \underbrace{\forall x \in [-1,1]}_{\parallel},\quad \underbrace{\exists y \in \mathbb{R}}_{\parallel} \quad \text{s.t.} \quad \underbrace{x^2 + y^2 = 1}_{\uparrow}$$
$$\left(\begin{array}{l}\text{集合 } [-1,1] \text{ に}\\ \text{属する任意の}\\ \text{元 } x \text{ に対して}\end{array}\right) \quad \left(\begin{array}{l}\text{実数 } y \text{ が}\\ \text{存在する}\end{array}\right) \quad y \text{ が満たすべき条件}$$

命題 P は“$\forall x \in [-1,1]$”で始まっているので、“集合 $[-1,1]$ に属する任意の元 x に対して”、つまり、“集合 $[-1,1]$ の中から元 x を任意にとったときに”「これこれしかじか」であるということを主張する命題であることがわかります。その次に書かれている“$\exists y \in \mathbb{R}$”は、どういうものかはわからないが何か実数 y が存在する、ということを意味しています。そして、それに続く“s.t.”＝“such that”以下で、その実数 y の満たすべき条件が述べられています。今の場合は“$x^2 + y^2 = 1$”と書かれていますから、“$\exists y \in \mathbb{R}$ s.t. $x^2 + y^2 = 1$”で“$x^2 + y^2 = 1$ を満たすような実数 y が存在する”という意味になります。結局、P は

どのような $x \in [-1,1]$ に対しても“$x^2 + y^2 = 1$ を満たすような実数 y が存在する”

ということを意味する命題であることがわかります。

次に命題 Q について説明します。

$$Q:\ \underbrace{\exists y \in \mathbb{R}}_{\parallel} \quad \text{s.t.} \quad \underbrace{\forall x \in [-1,1], \quad x^2+y^2=1}_{\uparrow}$$

$$\begin{array}{l} (\ \text{実数 } y \text{ が存在する}\ ) \\ \end{array} \qquad \begin{array}{c} y \text{ が満たすべき条件} \\ \parallel \\ \left(\begin{array}{l} \text{集合 } [-1,1] \text{ に属する任意の元} \\ x \text{ に対して } x^2+y^2=1 \text{ である} \end{array}\right) \end{array}$$

命題 Q は“$\exists y \in \mathbb{R}$”で始まっているので、どういうものかわからないがとにかく実数 y が存在する、ということを主張していることがわかります。その次に“s.t.”とあるので、その実数 y というのは、“s.t.”以下の条件を満たすものであることがわかります。今の場合、“s.t.”以下には

“$\forall x \in [-1,1],\ x^2+y^2=1$”

(=“$[-1,1]$ に属するすべての x に対して $x^2+y^2=1$ である”)

と書かれていますから、すべてをつなげて、Q は

“$[-1,1]$ に属するすべての x に対して $x^2+y^2=1$ である”ような実数 y 存在する

ということを主張する命題であることがわかります。

例 4-6 上で述べた２つの命題

$$P:\ \forall x \in [-1,1],\ \exists y \in \mathbb{R}\ \text{ s.t. }\ x^2+y^2=1$$

$$Q:\ \exists y \in \mathbb{R}\ \text{ s.t. } \forall x \in [-1,1],\ x^2+y^2=1$$

について、

P は真の命題である。一方、Q は偽の命題である。

解；

P が真であることを示す。そのためには、$x_0 \in [-1,1]$ を任意に 1 つ取ったときに、

$$\exists y \in \mathbb{R}\ \text{ s.t. }\ x_0^2+y^2=1$$

が成り立つことを示せばよい。

$x_0^2+y^2=1$ を y に関して解くと、$y=\pm\sqrt{1-x_0^2}$ である。そこで、

$$y_0 := \sqrt{1-x_0^2}$$

とおくと、$-1 \le x_0 \le 1$ により、y_0 は実数になり、$x_0^2+y_0^2=1$ を満たしていることがわかる。よって、P は真の命題である。

Q が偽の命題であることを示す。そのためには、

$$\forall x \in [-1,1],\ x^2+y_0^2=1 \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

を満たす $y_0 \in \mathbb{R}$ が存在しないことを示せばよい。これを背理法で示そう。

$(*)$ を満たす $y_0 \in \mathbb{R}$ が存在すると仮定する。すると、$(*)$ は $x=1$ のときにも $x=0$ のときにも成り立つことになるので、$1^2+y_0^2=1$ と $0^2+y_0^2=1$ が同時に成り立たなければならない。

$1^2 + y_0^2 = 1$ を解くことにより $y_0 = 0$ であることがわかる。一方、$0^2 + y_0^2 = 1$ を解くことにより $y_0 = 1$ かまたは $y_0 = -1$ であることがわかる。$y_0 = 1$ であっても $y_0 = -1$ であっても 0 でないことには変わりがない。ここに、$y_0 = 0$ であるということと $y_0 \neq 0$ であるということが同時に成立することになり、矛盾が生じた。よって、背理法の仮定は誤りであり、$(*)$ を満たす $y_0 \in \mathbb{R}$ は存在しないことがわかった。 □

上の例でわかるように、“∀”と“∃”が混在する命題では、その順番が大切です。順番を入れ換えてしまうと、まったく違った意味の命題になってしまいます。“∀”と“∃”が混在する命題を読み書きするとき、∃ と ∀ の順番をむやみに入れ替えないように気をつけましょう。

例 4-7 上で述べた 2 つの命題

$$P: \ \forall x \in [-1,1],\ \exists y \in \mathbb{R} \ \text{ s.t. } \ x^2 + y^2 = 1$$
$$Q: \ \exists y \in \mathbb{R} \ \text{ s.t. } \forall x \in [-1,1],\ x^2 + y^2 = 1$$

のそれぞれについて、その否定を、それと同値なわかりやすい命題に書き換えよ。

解；

• P の否定：

$[-1,1]$ を定義域とする命題関数

$$P(x) : \exists y \in \mathbb{R} \ \text{ s.t. } \ x^2 + y^2 = 1$$

を考えると、与えられた命題 P は全称命題「$\forall x \in [-1,1],\ P(x)$」の形に書くことができる。したがって、ド・モルガンの法則から、P の否定は「$\exists x \in [-1,1]$ s.t. $\overline{P(x)}$」、つまり、

「$P(x_0)$ が成り立たないような $x_0 \in [-1,1]$ が存在する」

となる。「$P(x_0)$ が成り立たない」とは、再び、ド・モルガンの法則から、

「すべての $y \in \mathbb{R}$ に対して、$x_0^2 + y^2 \neq 1$ となる」

ことであるから、P の否定は、

「“すべての $y \in \mathbb{R}$ に対して、$x_0^2 + y^2 \neq 1$ となる”ような $x_0 \in [-1,1]$ が存在する」

と書き換えられる。これを論理記号を使って書き直して、

$$\exists x \in [-1,1] \ \text{ s.t. } \ \forall y \in \mathbb{R},\ x^2 + y^2 \neq 1$$

を得る。

• Q の否定：

$\mathbb{R}$ を定義域とする命題関数

$$Q(y) : \forall x \in [-1,1],\ x^2 + y^2 = 1$$

を考えると、与えられた命題 Q は存在命題「$\exists y \in \mathbb{R}$ s.t. $Q(y)$」の形に書くことができる。したがって、ド・モルガンの法則から、Q の否定は「$\forall y \in \mathbb{R},\ \overline{Q(y)}$」、つまり、

「どんな $y_0 \in \mathbb{R}$ についても、$Q(y_0)$ は成り立たない」

となる。「$Q(y_0)$ が成り立たない」とは、再び、ド・モルガンの法則から、

「$x^2 + y_0^2 \neq 1$ となる $x \in [-1,1]$ が存在する」

ことであるから、Q の否定は、

「どんな $y_0 \in \mathbb{R}$ についても、“$x^2 + y_0^2 \neq 1$ となる $x \in [-1, 1]$ が存在する”」

と書き換えられる。これを論理記号を使って書き直して、

$$\forall\, y \in \mathbb{R},\ \exists\, x \in [-1, 1]\ \text{ s.t. }\ x^2 + y^2 \neq 1$$

を得る。 □

演習 4-5 * 次の 2 つの命題 P と Q について、以下の問いに答えよ。

$$P:\ \forall\, x > 0,\ \exists\, y \in \mathbb{R}\ \text{ s.t. }\ xy \geq 1$$

$$Q:\ \exists\, x \in \mathbb{R}\ \text{ s.t. }\ \forall\, y > 0,\ x > y$$

(1) 命題 P と Q について、真であるか、偽であるか判定せよ。
(2) 命題 P と Q について、その否定をそれと同値なわかりやすい命題に書き換えよ (「〜ではない」というような表現を用いずに書くこと)。

●付帯条件を伴う全称命題

集合 X を定義域とする 2 つの命題関数 $P(x)$ と $Q(x)$ が与えられたとします。このとき、

「$P(x)$ を満たすすべての $x \in X$ について $Q(x)$ である」

という命題を作ることができます。この命題は、

$$T_P = \{\ x_0 \in X \mid P(x_0) \text{ は真である}\ \}$$

という X の部分集合を考えるとき、「$\forall\, x \in T_P,\ Q(x)$」という全称命題に他なりません。

命題「$\forall\, x \in T_P,\ Q(x)$」の否定は、ド・モルガンの法則により「$\exists\, x \in T_P\ \text{ s.t. }\ \overline{Q(x)}$」です。これを文章に直せば、

「T_P の中に、$Q(x)$ ではない元 $x \in X$ が存在する」

となります。これは、さらに、

「$P(x)$ を満たす X の元 x であって、$Q(x)$ ではないものが存在する」

と書き換えることができます。結局、

$$\begin{aligned} &\overline{P(x) \text{ を満たすすべての } x \in X \text{ について } Q(x) \text{ である}} \\ \iff\ &P(x) \text{ を満たす } x \in X \text{ であって、} Q(x) \text{ ではないものが存在する} \\ \iff\ &\text{「}P(x) \text{ かつ } \overline{Q(x)}\text{」であるような } x \in X \text{ が存在する} \end{aligned}$$

であることがわかります。集合の演算と論理記号との関係をはっきりさせることにより、上で説明した事実をよりいっそう明解に理解できるようになるでしょう（次節で説明します)。

演習 4-6 次の命題 P の否定を、それと同値なわかりやすい命題に書き換えよ (「〜ではない」というような表現を用いずに書くこと)。また、その真偽を判定せよ。

P：$0 \leq x \leq 1$ を満たすすべての $x \in \mathbb{R}$ について、$x^2 < 2$ または $x^2 > 4$ である。

§5. 集合の演算

ここでの目標は２つあります。１つは、２つの集合 A と B が等しいことを証明するときは、“含む・含まれる”の両方、すなわち、$A \subset B$ と $A \supset B$ の両方を証明する必要がある、ということを沢山の例を見ながら学ぶことです（数や式が等しいことを証明するときのように、$=$ で結んでいって、証明するのとは違う！）。もう１つは、集合に対する演算記号 $\cap$, $\cup$, $-$, $\times$ の意味を正しく理解し、それを使いこなせるようになることです。

●集合の相等 (復習)

まず、次のことを思い出しておきましょう。

A と B を集合とするとき、

- $B \subset A$（または $A \supset B$） $\overset{\text{def}}{\iff}$ 「$x \in B$ ならば $x \in A$」
- $B = A$ $\overset{\text{def}}{\iff}$ 「$B \subset A$ かつ $B \supset A$」

例 5-1 $A = \{\, 3m + 2n \mid m, n \in \mathbb{Z} \,\}$ と定めるとき、$A = \mathbb{Z}$ であることを証明せよ。

解；

$A \subset \mathbb{Z}$ と $\mathbb{Z} \subset A$ の２つを示せばよい。

① $A \subset \mathbb{Z}$ であること：

A の定め方から、A のすべての元は整数である。よって、$A \subset \mathbb{Z}$ が成り立つ。

② $\mathbb{Z} \subset A$ であること：

$r \in \mathbb{Z}$ を任意にとる。このとき、

$$r = 3 \cdot r + 2 \cdot (-r)$$

と書き表わすことができる。

$m = r$, $n = -r$ とおくと、これらは確かに整数なので、$r = 3m + 2n \in A$ がわかる。よって、$\mathbb{Z} \subset A$ も示された。

①と②から、$A = \mathbb{Z}$ が示された。 □

演習 5-1 集合 A と集合 B をそれぞれ

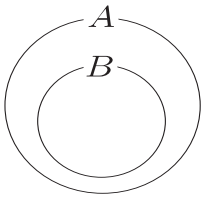
$$A = \left\{ \frac{1}{x^2 + 1} \;\middle|\; x \in \mathbb{R} \right\}, \qquad B = \{\, x \in \mathbb{R} \mid 0 < x \leq 1 \,\}$$

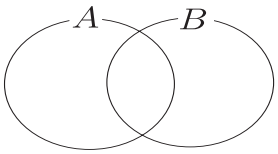
によって定義する。このとき、$A = B$ であることを証明せよ。

●ベン図

集合の間の関係をわかりやすく図で表わしたものに、**ベン図** (Venn diagram) というものがあります。ベン図では、集合を楕円や長方形で表わし、その内側にその集合の元があると考えます。

次のベン図のうち左図は B が A の部分集合である状態を表わしていて、右図は A は B の部分集合でもなく、かつ、B は A の部分集合でもない状態を表わしています。





●共通集合と和集合

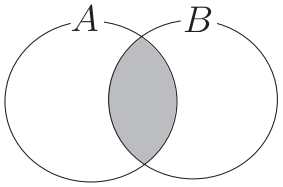
2つの集合 $A,\ B$ が与えられたとき、次のようにして、新たに2つの集合 $A\cap B$ と $A\cup B$ を作ることができます。

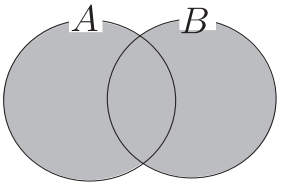
$$A\cap B=\{\ x\mid x\in A \text{ かつ } x\in B\ \}$$
$$A\cup B=\{\ x\mid x\in A \text{ または } x\in B\ \}$$

$A\cap B$ は A と B の両方に属するもの全体からなる集合を表わしていて、$A\cup B$ は A か、または、B の少なくとも一方に属するもの全体からなる集合を表わしています。

$A\cap B$ を A と B の**共通集合** (intersection) といい、$A\cup B$ を A と B の**和集合** (union) といいます。記号 $A\cap B$ は「A キャップ B」と呼んだり、「A と B の共通部分 (インターセクション)」と呼んだりします。記号 $A\cup B$ は「A カップ B」と呼んだり、「A と B の和 (ユニオン)」と呼んだりします。

共通集合と和集合をベン図を使って表わすと、次図のようになります (左のベン図の斜線部分が $A\cap B$ を表わし、右のベン図の斜線部分が $A\cup B$ を表わしています)。





例 5-2　集合 $A=\{\ 2,4,6,8,10,12\ \},\ B=\{\ 3,6,9,12\ \}$ に対して、

$A\cap B=\{\ 6,12\ \}$,

$A\cup B=\{\ 2,3,4,6,8,9,10,12\ \}$

である。

定理 5-3

A,B,C を集合とするとき、次が成り立つ。

(1) $A\cap B\subset A,\quad A\cap B\subset B,\quad A\subset A\cup B,\quad B\subset A\cup B$

(2) (冪等律) $A\cap A=A,\quad A\cup A=A$

(3) (交換律) $A\cap B=B\cap A,\quad A\cup B=B\cup A$

(4) (結合律) $(A\cap B)\cap C=A\cap(B\cap C),\quad (A\cup B)\cup C=A\cup(B\cup C)$

(5) (分配律) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C),\quad A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$

上の定理は、記号 $\cap,\cup,=$ の定義から直ちに証明することができますが、分配律だけは少し面倒なので、これを証明しておきましょう（2番目の等式は演習問題とします)。

例 5-4　$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ を証明せよ。

解；

$$\left.\begin{array}{l} ①\ A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C) \\ ②\ (A \cap B) \cup (A \cap C) \subset A \cap (B \cup C) \end{array}\right\}$$ の２つを証明すればよい。

①の証明：

$x \in A \cap (B \cup C)$ を任意にとる。このとき、

$$❶\ x \in A \quad \text{かつ} \quad ❷\ x \in B \cup C$$

が成り立つ。❷より、$x \in B$ または $x \in C$ が成り立つ。

$x \in B$ の場合は、❶と合わせて $x \in A \cap B$ であり、$x \in C$ の場合は、❶と合わせて $x \in A \cap C$ である。定理 5-3(1) より、

$$A \cap B \subset (A \cap B) \cup (A \cap C), \quad A \cap C \subset (A \cap B) \cup (A \cap C)$$

であるから、$x \in B$ であっても $x \in C$ であっても $x \in (A \cap B) \cup (A \cap C)$ となる。よって、①が証明された。

②の証明：

$x \in (A \cap B) \cup (A \cap C)$ を任意にとる。このとき、

$$❸\ x \in A \cap B \quad \text{または} \quad ❹\ x \in A \cap C$$

が成り立つ。

❸のとき、$x \in A$ かつ $x \in B \subset B \cup C$ となるので、$x \in A \cap (B \cup C)$ を得る。

❹のとき、$x \in A$ かつ $x \in C \subset B \cup C$ となるので、$x \in A \cap (B \cup C)$ を得る。

❸と❹のいずれの場合にも $x \in A \cap (B \cup C)$ が示されたから、②が証明された。　□

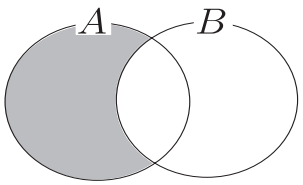
演習 5-2*　$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ を証明せよ。

●集合の差と補集合

２つの集合 A, B が与えられたとき、次のようにして、新たに集合 $A - B$ を作ることができます。

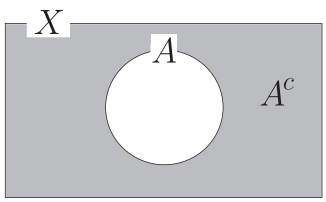
$$A - B = \{\ x \mid x \in A \text{ かつ } x \notin B\ \}.$$

$A - B$ は A に属する元であって、かつ、B には属さないもの全体からなる集合です。この集合を A から B を引いた**差** (difference) といいます。$A - B$ は「A マイナス B」と読みます。$A - B$ は、下のベン図において、斜線部分に対応します。



例 5-5　集合 $A = \{\ 2, 4, 6, 8, 10, 12\ \}$, $B = \{\ 3, 6, 9, 12\ \}$ に対して、$A - B = \{\ 2, 4, 8, 10\ \}$ である。

X が集合で、A がその部分集合であるとき、差 $X - A$ を X における A の**補集合** (complement) といいます。このとき、X を A に対する**全体集合** (universal set) といいます。補集合 $X - A$ を A^c という記号で書き表わすことがありますが、この記号を使うときには、全体集合としてどのような集合を考えているかが明確な場合に限られます。



例 5-6 $\mathbb{R}$ における $\mathbb{Q}$ の補集合 $\mathbb{R} - \mathbb{Q}$ は**無理数** (irrational number) 全体からなる集合に他ならない。

演習 5-3* 集合 X とその部分集合 A に対して、等式

$$X - (X - A) = A$$

が成り立つことを証明せよ。

注意：補集合の記号を使うと、上の等式は $(A^c)^c = A$ と書き直すことができます。

演習 5-4 集合 X とその部分集合 $A,\ B$ に対して、

$$A \subset B \iff X - A \supset X - B$$

が成り立つことを証明せよ。

ヒント：「$\Longrightarrow$」と「$\Longleftarrow$」の両方が成り立つことを証明します。この演習問題の場合には次の２つを証明します。

① $A \subset B$ が成り立つと仮定すると、$X - A \supset X - B$ が成り立つ。

② $X - A \supset X - B$ が成り立つと仮定すると、$A \subset B$ が成り立つ。

集合の演算に関する記法上の注意

集合 A, B, C に対して、定理 5-3(4) により、$(A \cap B) \cap C$ または $A \cap (B \cap C)$ を $A \cap B \cap C$ と書くことができます。同様に、$(A \cup B) \cup C$ または $A \cup (B \cup C)$ を $A \cup B \cup C$ と書くことができます。しかし、$A \cup B \cap C$ と書くことはできません。括弧のつく場所によって集合が変わってしまうからです。$\cap$ と $-$、あるいは $\cup$ と $-$ を同時に含む場合も、括弧のつく場所によって集合が変わります。しかし、これについては、記号の煩雑さを避けるため、「$-$ よりも $\cap, \cup$ を優先して行う」という規約を設けることにします。例えば、$C - A \cap B$ は $C - (A \cap B)$ という集合を表わし、$(C - A) \cap B$ のことではありません。

●ド・モルガンの法則 (de Morgan's law)

命題に関するド・モルガンの法則は例 2-6(1) と定理 4-3 で扱いました。これと同様のことが集合についても成り立ちます。

定理 5-7 (ド・モルガンの法則)

集合 X とその部分集合 A, B に対して次が成り立つ。

(1) $X - A \cap B = (X - A) \cup (X - B)$

(2) $X - A \cup B = (X - A) \cap (X - B)$

(**proof**)

ここでは (2) を演習問題として残し、(1) のみを証明しよう。

① $X - A \cap B \subset (X - A) \cup (X - B)$
② $(X - A) \cup (X - B) \subset X - A \cap B$
} の２つを証明すればよい。

①の証明：$x \in X - A \cap B$ を任意にとる。

このとき、$x \in X$ かつ $x \notin A \cap B$ である。ここで、$x \in X$ について、

$$x \notin A \cap B \iff x \notin A \text{ または } x \notin B$$

が成り立つので(∵命題 $P : x \in A$ と $Q : x \in B$ についてド･モルガンの法則「$\overline{P \wedge Q} \iff \overline{P} \vee \overline{Q}$」を適用)、$x \notin A$ と $x \notin B$ のうち、少なくとも一方が成り立つ。

$x \notin A$ の場合、$x \in X - A$ であり、$X - A \subset (X - A) \cup (X - B)$ であるから、$x \in (X - A) \cup (X - B)$ を得る。

$x \notin B$ の場合、$x \in X - B$ であり、$X - B \subset (X - A) \cup (X - B)$ であるから、$x \in (X - A) \cup (X - B)$ を得る。

いずれにしても、$x \in (X - A) \cup (X - B)$ であることがわかったので、①が証明された。

②の証明：$x \in (X - A) \cup (X - B)$ を任意にとる。

すると、$x \in X - A$ または $x \in X - B$ である。ここで、$A \cap B \subset A$ および $A \cap B \subset B$ であることから、

$$X - A \cap B \supset X - A, \qquad X - A \cap B \supset X - B$$

が成り立つ (演習 5-4)。よって、$x \in X - A$ の場合、$x \in X - B$ の場合のいずれの場合にも、$x \in X - A \cap B$ となる。故に、②が証明された。 □

演習 5-5 * 定理 5-7(2) を証明せよ。

注意：定理 5-7(2) は (1) と同様に証明することができますが、演習 5-3 の結果を用いて (1) から (2) を導くこともできます。逆に、演習 5-3 の結果を用いて (2) から (1) を導くこともできます。

●直積集合

２つの空でない集合 A, B が与えられたとき、A の元 a と B の元 b から組 (a, b) を作ることができます。$a \in A$, $b \in B$ から作られる組 (a, b) と $a' \in A$, $b' \in B$ から作られる組 (a', b') が**等しい**とは、$a = a'$ かつ $b = b'$ であるときをいい、このことを $(a, b) = (a', b')$ と書き表わします。すなわち、

$$(a, b) = (a', b') \overset{\text{def}}{\iff} a = a' \text{ かつ } b = b'$$

です。組 (a, b) を考えるときには元の並び方の順番が大切なので、それを強調して、(a, b) のことを a と b との**順序対** (ordered pair) とも呼ぶこともあります。

A の元と B の元との順序対をすべて集めて得られる集合を $A \times B$ と書き表わします：

$$A \times B = \{\ (a, b) \mid a \in A \text{ かつ } b \in B\ \}.$$

この集合を A と B の**直積集合** (direct product) といいます。

演習 5-6 $A = \{1, 2\}$ と $B = \{1, 2, 3\}$ について、元を書き並べる方法によって、直積集合 $A \times B$ を書き表わせ。

● 冪(べき) 集合

X を集合とするとき、X の部分集合全体からなる集合を考えることができます。これを X の**冪集合** (power set) といい、 $\mathcal{P}(X)$ または 2^X という記号で書き表わします。

例 5-8 $X = \{1, 2, 3\}$ のとき、X の冪集合 $\mathcal{P}(X)$ は次のようになる。

$$\mathcal{P}(X) = \{\varnothing,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{2,3\},\ \{1,3\},\ \{1,2,3\}\}.$$

X が n 個の元からなる集合のとき、冪集合 $\mathcal{P}(X)$ は 2^n 個の元からなります (これについては次節で考察します)。2^X という奇妙な記号は、この事実に由来しています。

●集合族

集合を元とする空でない集合のことを**集合族** (family of sets) といいます。特に、集合 X に対して、冪集合 $\mathcal{P}(X)$ の空でない部分集合は集合族です。このような集合族を X の**部分集合族** (family of subsets) と呼びます。

例 5-9

(1) 空集合だけからなる集合 $\{\varnothing\}$ や $\{\{1,2\},\ \{1,3\},\ \{4\}\}$ は集合族である。

(2) $\mathbb{R}$ の部分集合全体からなる集合、すなわち、冪集合 $\mathcal{P}(\mathbb{R})$ は $\mathbb{R}$ の部分集合族である。また、各自然数 n について、$\mathbb{R}$ の部分集合 $I_n = \{\ x \in \mathbb{R} \mid -\frac{1}{n} \leq x \leq \frac{1}{n}\ \}$ を考える。このとき、集合 $\{\ I_n \mid n \in \mathbb{N}\ \}$ は $\mathbb{R}$ の部分集合族である。

この節の最初の方で、2 つの集合 A, B に対して、共通集合や和集合と呼ばれる集合を定義しました。同様の概念を集合族に対して考えることができます。

集合族 $\mathcal{S}$ に対して、共通集合 $\bigcap_{A\in\mathcal{S}} A$ と和集合 $\bigcup_{A\in\mathcal{S}} A$ を

$$\bigcap_{A\in\mathcal{S}} A = \{\ x \mid \text{すべての } A \in \mathcal{S} \text{ に対して } x \in A \text{ である}\ \},$$

$$\bigcup_{A\in\mathcal{S}} A = \{\ x \mid \text{ある } A \in \mathcal{S} \text{ に対して } x \in A \text{ である}\ \}$$

によって定義します。1 年生の授業では、集合族 $\mathcal{S}$ として次の場合がよく使われます。

Case 1 ：$\mathcal{S}$ が有限個の集合 $A_1, A_2, \cdots, A_n$ からなる場合。つまり、$\mathcal{S} = \{\ A_1, A_2, \cdots, A_n\ \}$ の場合。

Case 2 ：各自然数 $n \in \mathbb{N}$ に対して集合 A_n が定められているとき、$\mathcal{S}$ が $\mathcal{S} = \{\ A_n \mid n \in \mathbb{N}\ \}$ によって与えられている場合。

Case 1 の集合族 $\mathcal{S} = \{\ A_1, A_2, \cdots, A_n\ \}$ に対しては、共通集合 $\bigcap_{A\in\mathcal{S}} A$ を

$$\bigcap_{k=1}^{n} A_k \qquad \text{や} \qquad A_1 \cap A_2 \cap \cdots \cap A_n$$

のように表わし、和集合 $\bigcup_{A\in\mathcal{S}} A$ を

$$\bigcup_{k=1}^{n} A_k \qquad \text{や} \qquad A_1 \cup A_2 \cup \cdots \cup A_n$$

のように表わします。

$$\bigcap_{k=1}^{n} A_k = \{\ x \mid \text{すべての } k = 1, 2, \cdots, n \text{ に対して } x \in A_k\ \}$$
$$= (A_1, A_2, \cdots, A_n \text{ のどの集合にも属する元全体からなる集合}),$$
$$\bigcup_{k=1}^{n} A_k = \{\ x \mid \text{ある } k = 1, 2, \cdots, n \text{ に対して } x \in A_k\ \}$$
$$= (A_1, A_2, \cdots, A_n \text{ の少なくともどれか 1 つには属する元全体からなる集合})$$

であり、特に、$n = 2$ のときには、$\bigcap_{A\in\mathcal{S}} A$, $\bigcup_{A\in\mathcal{S}} A$ はそれぞれ p.38 で定義した $A_1 \cap A_2$, $A_1 \cup A_2$ に一致します。

Case 2 の集合族 $\mathcal{S} = \{\ A_n \mid n \in \mathbb{N}\ \}$ に対しては、$\bigcap_{A\in\mathcal{S}} A$, $\bigcup_{A\in\mathcal{S}} A$ をそれぞれ

$$\bigcap_{n=1}^{\infty} A_k \qquad \bigcup_{n=1}^{\infty} A_k$$

のように表わします。

例 5-10 例 5-9(2) の集合族 $\{\ I_n \mid n \in \mathbb{N}\ \}$ については、

$$\bigcap_{n=1}^{\infty} I_n = \{0\}, \qquad \bigcup_{n=1}^{\infty} I_n = \{\ x \in \mathbb{R} \mid\ -1 \le x \le 1\ \ \}$$

となる。

解；

ここでは、和集合の方のみ示し、共通部分の方は各自の演習問題として残しておく。

いつものように「$\subset$」「$\supset$」の両方を示す。$[-1, 1] = \{\ x \in \mathbb{R} \mid\ -1 \le x \le 1\ \ \}$ とおく。

- $\bigcup_{n=1}^{\infty} I_n \subset [-1, 1]$ の証明：

任意に $x \in \bigcup_{n=1}^{\infty} I_n$ をとる。すると、x は $I_1, I_2, I_3 \cdots$ の中の少なくとも 1 つの集合には属している。I_n $(n \in \mathbb{N})$ が x を含んでいるとすると、I_n の定義から

$$-1 \le -\tfrac{1}{n} \le x \le \tfrac{1}{n} \le 1$$

が成り立つ。よって、$x \in [-1, 1]$ である。

- $\bigcap_{n=1}^{\infty} I_n \supset [-1, 1]$ の証明：

任意に $x \in [-1, 1]$ をとる。このとき、$n \in \mathbb{N}$ を十分に大きくとれば、$-\frac{1}{n} \le x \le \frac{1}{n}$ となる自然数 n を見つけることができる (アルキメデスの公理)。このような n について $x \in I_n$ となるから、$x \in \bigcup_{n=1}^{\infty} I_n$ である。したがって、$\bigcup_{n=1}^{\infty} I_n \supset [-1, 1]$ は示された。

以上により、$\bigcup_{n=1}^{\infty} I_n = [-1, 1]$ は証明された。 □

集合 X の部分集合族 $\mathcal{S}$ に対して、定理 5-7 と類似の結果、すなわち、ド・モルガンの法則が成り立ちます：

$$X - \bigcap_{A\in\mathcal{S}} A = \bigcup_{A\in\mathcal{S}} (X - A), \qquad X - \bigcup_{A\in\mathcal{S}} A = \bigcap_{A\in\mathcal{S}} (X - A).$$

証明は定理 5-7 の証明中のいくつかの文章と記号を手直しするだけです (意欲のある人は証明を書いてみましょう)。

●命題関数の真理集合

文字 x に関する条件 $P(x)$ と集合 X が与えられていて、X の各元 x_0 に対して $P(x_0)$ が命題になっているとします。このとき、X の部分集合

$$T_P(X) = \{\ x_0 \in X \mid P(x_0) \text{ は真}\ \}$$

を考えることができます。この集合を X を定義域とする命題関数 $P(x)$ の**真理集合** (truth set) と呼びます。命題関数に対して「ではない」「かつ」「または」「ならば」をとる操作と集合の演算「$-$」「$\cap$」「$\cup$」との間には次のような関係があります。

定理 5-11

集合 X を定義域とする 2 つの命題関数 $P(x),\ Q(x)$ を考える。

(1) x に関する 3 つの条件「$\overline{P(x)}$」「$P(x)$ かつ $Q(x)$ 」「$P(x)$ または $Q(x)$」をそれぞれ $\overline{P}(x)$, $(P \wedge Q)(x)$, $(P \vee Q)(x)$ で表わすとき、真理集合について次が成り立つ。

$$T_{\overline{P}}(X) = X - T_P(X),$$
$$T_{P \wedge Q}(X) = T_P(X) \cap T_Q(X),$$
$$T_{P \vee Q}(X) = T_P(X) \cup T_Q(X).$$

(2) x に関する条件「$P(x) \ \Rightarrow\ Q(x)$」を $R(x)$ で表わすとき、次が成り立つ。

$$T_R(X) = (X - T_P(X)) \cup T_Q(X).$$

したがって、

$$\text{全称命題「}\forall x \in X,\ R(x)\text{」が真} \iff T_P(X) \subset T_Q(X)$$

が成り立つ。

(**proof**)

(1) は定義にしたがって簡単に証明することができるので、ここでは (2) を示す。演習 2-3 と (1) により、

$$\begin{aligned} T_R(X) &= \{\ x_0 \in X \mid P(x_0) \ \Rightarrow\ Q(x_0) \text{ が真}\ \} \\ &= \{\ x_0 \in X \mid \overline{P(x_0)} \vee Q(x_0) \text{ が真}\ \} \\ &= \{\ x_0 \in X \mid \overline{P(x_0)} \text{ が真}\ \} \cup \{\ x_0 \in X \mid Q(x_0) \text{ が真}\ \} \\ &= (X - T_P(X)) \cup T_Q(X) \end{aligned}$$

となる。したがって、

$$\begin{aligned} \text{全称命題「}\forall x \in X,\ R(x)\text{」が真} &\iff T_R(X) = X \\ &\iff (X - T_P(X)) \cup T_Q(X) = X \\ &\iff T_P(X) \subset T_Q(X) \end{aligned}$$

が成り立つ。 □

上の定理 5-11(2) により、「$\forall x \in X,\ P(x) \ \Rightarrow\ Q(x)$」という形の全称命題が成り立つことを証明するためには、「$P(x_0)$ が成り立つようなすべての $x_0 \in X$ について、$Q(x_0)$ が成り立つ」ことを示せばよいことがわかります。つまり、2 つの命題「すべての $x \in X$ に対して“$P(x)$ ならば $Q(x)$ である”」と「$P(x)$ を満たすすべての $x \in X$ に対して $Q(x)$ である」とは同値な命題なのです。

§6. 数学的帰納法と整数論の基本定理

定理を証明したり、数や関数を定義したりする際に“帰納的方法”がしばしば使われます。その基礎になる原理、すなわち、帰納法の原理は、自然数全体からなる集合 $\mathbb{N}$ の持つ基本的な性質のうちの 1 つです。ここでは、様々な例、特に、素因数分解の可能性と一意性の定理の証明を通して、数学的帰納法を用いた証明法を身につけましょう。

§6-1 自然数の整列性と数学的帰納法

$\mathbb{N}$ は次の 2 条件を満たす $\mathbb{R}$ の部分集合 A の中で最小のもの（すなわち、次の 2 条件を満たす $\mathbb{R}$ の部分集合 A たちの共通部分）として特徴づけることができます：

$$\text{(i) } 1 \in A \qquad \text{(ii) } a \in A \text{ ならば } a+1 \in A\,.$$

ここでは、この特徴づけから得られる、$\mathbb{N}$ の重要な性質—整列性—について述べ、それを使って帰納法の原理を導きます。

●自然数の整列性

A を $\mathbb{R}$ の空でない部分集合とします。「すべての $a \in A$ に対して $a \geq m$」を満たす A に属する実数 m を A の**最小元** (minimal element) といいます。

$\mathbb{R}$ の空でない部分集合に対して、最小元が存在すれば一意的 (つまり、唯一つ) ですが、いつでもそれが存在するとは限りません。

例 6-1

(1) $\{-1, \sqrt{2}, 3\}$ や $\{0\} \cup \{\, x \in \mathbb{R} \mid x > 3 \,\}$ には最小元が存在する。これらの集合は、それぞれ、-1, 0 を最小元に持つ。

(2) $\{x \in \mathbb{R} \mid 2 < x \leq 4\}$ には最小元が存在しない。

なぜならば、$2 < a \leq 4$ を満たすどのような実数 a を持ってきても、$a' := \frac{2+a}{2}$ を考えると、$2 < a' < a \leq 4$ が満たされるからである。 □

ところが、$\mathbb{N}$ の部分集合に限定すると次が成り立ちます。

自然数の整列性

$\mathbb{N}$ の空でない任意の部分集合には最小元が存在する。すなわち、次が成り立つ。

$$\varnothing \neq M \subset \mathbb{N} \implies \exists\, m_0 \in M \ \text{ s.t. } \forall\, m \in M,\ m \geq m_0.$$

上と同様のことは $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ の部分集合については成り立たないので、整列性は $\mathbb{N}$ の持つ著しい特徴であるといえます。

●数学的帰納法

数学的帰納法 (mathematical induction) の原理は $\mathbb{N}$ の持つ重要な性質の 1 つです。数学的帰納法の「偉大な」ところは、$P(1), P(2), P(3), \cdots\cdots$ のような無限個の命題が真であることを、わずか 2 ステップで証明できてしまうことにあります。ここでは、$\mathbb{N}$ を

- $\mathbb{R}$ の中の整列性を持つ部分集合であって、
- 1 を最小元として持ち、
- 「$n \in \mathbb{N}$ ならば $n+1 \in \mathbb{N}$」を満たすもの

と捉え直して、帰納法の原理を導きましょう。

定理 6-2 (帰納法の原理)

$\mathbb{N}$ を定義域とする命題関数 $P(n)$ が与えられているとする。もし、次の I, II が示されたとすると、全称命題「$\forall n \in \mathbb{N},\ P(n)$」は真である、すなわち、命題 $P(1), P(2), P(3), \cdots\cdots$ はすべて成り立つ。

I. $P(1)$ は成り立つ。

II. $k \in \mathbb{N}$ について、$P(k)$ が成り立つと仮定すると、$P(k+1)$ も成り立つ。

(**proof**)

背理法で証明する。

$$M := \{\ n \in \mathbb{N} \mid P(n) \text{ は成り立たない}\ \}$$

とおき、$M \neq \varnothing$ であると仮定する。このとき、自然数の整列性から、M の中に最小の自然数 m が存在する。I により、$m > 1$ である。すると、$m-1 \in \mathbb{N}$ であるが、m の最小性から、$m-1 \notin M$ である。よって、$P(m-1)$ が成り立ち、したがって II により、$P(m) = P((m-1)+1)$ が成り立つ。これは $m \notin M$ を意味しており、$m \in M$ に矛盾する。よって、$M = \varnothing$ でなければならない。つまり、すべての $n \in \mathbb{N}$ に対して $P(n)$ が成り立つ。 □

注意：1. 定理の I,II をそれぞれ帰納法の第 1 段、第 2 段と呼びます。また、II における「$k \in \mathbb{N}$ について、$P(k)$ が成り立つと仮定する」という部分を**帰納法の仮定** (induction hypothesis) と呼びます。

2. 定理の証明は分かりにくかったかもしれませんが、それが成り立つ理由はとても単純です。まず、I により $P(1)$ が成り立ち、次に、II において $k=1$ の場合を考えて $P(2)$ が成り立つことがわかり、さらに II において $k=2$ の場合を考えて $P(3)$ が成り立つことがわかり $\cdots\cdots$ というように、次々と「成り立つ」ことが連鎖していくわけです。

例 6-3　すべての $n \in \mathbb{N}$ について、次の等式が成り立つことを証明せよ。

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

解；

証明すべき等式を $P(n)$ とおき、n についての数学的帰納法により証明する。

I. $n=1$ のとき：

$$(P(1) \text{ の左辺}) = 1, \quad (P(1) \text{ の右辺}) = \tfrac{1(1+1)(2+1)}{6} = 1$$

となり、等式 $P(1)$ が成り立つ。

II. $k \in \mathbb{N}$ とし、$P(k)$ が成り立っていると仮定する。このとき、

$$\begin{aligned}(P(k+1) \text{ の左辺}) &= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \qquad \text{(帰納法の仮定を適用)} \\ &= \frac{k+1}{6}(k(2k+1) + 6(k+1)) \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \\ &= (P(k+1) \text{ の右辺})\end{aligned}$$

が成り立つ。よって、$P(k+1)$ も成り立つ。

I と II から、すべての $n \in \mathbb{N}$ について $P(n)$ が成り立つことが示された。 □

演習 6-1　自然数 n について、$X = \{\, 1, 2, \cdots, n \,\}$ の冪集合 $\mathcal{P}(X)$ の元の個数は 2^n 個である。このことを数学的帰納法を用いて示せ。

●累積的帰納法

数学的帰納法を強化した次の累積的帰納法も、自然数に関する定理の証明にしばしば使われます。累積的帰納法の第 2 段では $P(1), P(2), \cdots, P(k)$ のすべてが成り立つことを仮定することができるので、これを使うと通常の帰納法よりも強力に証明を遂行することができます。

定理 6-4 (累積的帰納法)

$\mathbb{N}$ を定義域とする命題関数 $P(n)$ が与えられているとする。もし、次の I, II が示されたとすると、全称命題「$\forall\, n \in \mathbb{N},\ P(n)$」は真である、すなわち、命題 $P(1), P(2), P(3), \cdots\cdots$ はすべて成り立つ。

I. $P(1)$ は成り立つ。

II. $k \in \mathbb{N}$ について、$i \leq k$ を満たすすべての自然数 i に対して $P(i)$ が成り立つと仮定すると、$P(k+1)$ も成り立つ。

上の定理は定理 6-2 を用いて証明することができます（「$i \leq n$ を満たすすべての自然数 i について $P(i)$ である」という条件を $Q(n)$ とおき、それがすべての $n \in \mathbb{N}$ について真であることを示します)。累積的帰納法の使用例は 6-3 節で与えられます。累積的帰納法も数学的帰納法と呼ばれます。

§6-2 帰納的に定義される数

1 番目の数 a_1 が定義されていて、各自然数 n について、n 番目の数 a_n (あるいは、1 番目から n 番目の数 $a_1, \cdots, a_n$) から $(n+1)$ 番目の数 a_{n+1} を定義する方法が与えられているとき、一連の数 a_n $(n = 1, 2, \cdots)$ が定まります。このとき、これらの数 a_n $(n = 1, 2, \cdots)$ は「帰納的に定義されている帰納的に定義されている」といいます。ここでは、帰納的に定義される数の例を紹介します。

●累乗

a を 0 でない実数とします。このとき、自然数 n に対して、a^n とは、a を n 個掛け合わせて得られる実数のことを指しますが、この実数 a^n は、正式には、次のようにして帰納的に定義されます：

$$a^1 = a, \quad n \geq 2 \text{ に対して } a^n = a^{n-1} \cdot a.$$

さらに、n が 0 の場合には $a^0 := 1$、n が負の整数の場合には $a^n := (\frac{1}{a})^{-n}$ と定めることにより、任意の整数 n に対して、実数 a^n が定義されます。この実数 a^n を a **の** n **乗** (the n-th power of a) と呼びます。

任意の整数 n, m と 0 でない任意の実数 a, b に対して、**指数法則**

$$\text{① } a^{n+m} = a^n a^m \qquad \text{② } (a^n)^m = a^{nm} \qquad \text{③ } (ab)^n = a^n b^n$$

が成り立ちます（証明は帰納法によります)。

●階乗

自然数 n に対して、n の**階乗** (factorial) と呼ばれる自然数 $n!$ を

$$1! = 1, \quad n \geq 2 \text{ に対して } n! = (n-1)! \cdot n$$

によって帰納的に定義します。$n!$ は n 以下のすべての自然数の積 $1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$ に他なりません。便宜上、0 についても階乗 $0!$ を考え、$0! = 1$ と約束します。

演習 6-2* すべての自然数 n について $n! \geq 2^{n-1}$ が成り立つことを示せ。

●有限数列とその和

n を自然数とします。$1 \leq k \leq n$ を満たす各自然数 k について実数 a_k が定められているとき、これらを

$$a_1, a_2, a_3, \cdots, a_n$$

のように並べて実数の列を作ることができます。この列を**有限 (実) 数列** (finite sequence) と呼び、$\{a_k\}_{k=1}^n$ あるいは $(a_k)_{k=1}^n$ と書き表わします。また、左から k 番目に並ぶ実数 a_k のことをその数列の第 k 項と呼びます。

有限数列 $\{a_k\}_{k=1}^n$ の第 1 項から第 n 項までを順次加えていくことにより、1 つの実数 $a_1 + a_2 + \cdots + a_n$ が定まります。この実数を

$$(\sharp) \qquad \sum_{i=1}^{n} a_i$$

という記号で表わします。すなわち、この実数は

$$\sum_{i=1}^{1} a_i = a_1, \quad 2 \leq k \leq n \text{ に対して } \sum_{i=1}^{k} a_i = \sum_{i=1}^{k-1} a_i + a_k$$

によって帰納的に定義されています。なお、$(\sharp)$ において和の記号に付属している文字 i は、すでに意味が確定している n と a 以外であれば、好きな文字に置き換えることができます。

●数列

各自然数 n に対して実数 a_n が 1 つずつ定められているとき、これらを

$$a_1, a_2, a_3, \cdots, a_n, \cdots\cdots$$

のように“並べて”実数の列を作ることが“できます”(実際に全部を並べ尽くすことはできないので、これは観念的なものです。正確な定義は後の節で与えます。大切なことは、この列に対して第 n 番目の実数がきちんと定められている、ということです)。この列のことを (実) **数列** (sequence) と呼びます。左から n 番目に並ぶ数 a_n をこの数列の**第 n 項**といいます。特に、第 1 項のことを**初項**といいます。数列を $\{a_n\}_{n=1}^\infty$ または $(a_n)_{n=1}^\infty$ のように書き表わします。

例 6-5 $\{\sqrt{2^n - 1}\}_{n=1}^\infty$ は第 n 項が $\sqrt{2^n - 1}$ によって与えられる数列である。この数列の最初のいくつかの項は $1, \sqrt{3}, \sqrt{7}, \sqrt{15}, \sqrt{31}, \sqrt{63}, \cdots\cdots$ である。

2 つの数列 $\{a_n\}_{n=1}^\infty$, $\{b_n\}_{n=1}^\infty$ が**等しい**とは、すべての $n \in \mathbb{N}$ に対して $a_n = b_n$ となるときをいい、このことを $\{a_n\}_{n=1}^\infty = \{b_n\}_{n=1}^\infty$ と書き表わします。例えば、$\{(-1)^n\}_{n=1}^\infty$ と $\{(-1)^{n-1}\}_{n=1}^\infty$ は、$\mathbb{R}$ の部分集合として見るとどちらも $\{1, -1\}$ ですが、数列としては等しくありません。

●漸化式

しばしば、隣接する何項かの間の関係式、すなわち、**漸化式** (recurrence formula) と、はじめの何項かの値を指定することによって、数列を帰納的に定義することがあります。

例 6-6

(1) 2つの実数 a と d が与えられているとする。このとき、各 $n \in \mathbb{N}$ に対して実数 a_n を

$$a_1 = a, \quad a_n = a_{n-1} + d \quad (n = 2, 3, 4, \cdots\cdots)$$

によって帰納的に定義する。このようにして定義される数列 $\{a_n\}_{n=1}^{\infty}$ を初項 a、公差 d の**等差数列** (arithmetical progression) という。この等差数列の第 n 項は $a_n = a + (n-1)d$ によって与えられる。

(2) 2つの実数 a と r が与えられているとする。このとき、各 $n \in \mathbb{N}$ に対して実数 a_n を

$$a_1 = a, \quad a_n = ra_{n-1} \quad (n = 2, 3, 4, \cdots\cdots)$$

によって帰納的に定義する。このようにして定義される数列 $\{a_n\}_{n=1}^{\infty}$ を初項 a、公比 r の**等比数列** (geometrical progression) という。この等比数列の第 n 項は $a_n = ar^{n-1}$ によって与えられる。

(3) 各 $n \in \mathbb{N}$ に対して実数 F_n を

$$F_1 = 1,\ F_2 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n = 3, 4, 5, \cdots\cdots)$$

によって帰納的に定義する。このようにして定義される数列 $\{F_n\}_{n=1}^{\infty}$ を**フィボナッチ数列** (Fibonacci sequence) といい、各実数 F_n を**フィボナッチ数**という。

演習 6-3 $\{F_n\}_{n=1}^{\infty}$ をフィボナッチ数列とするとき、すべての自然数 n に対して、

$$F_{n+1}^2 + F_n^2 = F_{2n+1}$$

が成り立つことを示せ。

ヒント：示したい式を $P(n)$、$2F_{n+1}F_n + F_{n+1}^2 = F_{2n+2}$ を $Q(n)$ とおき、すべての $n \in \mathbb{N}$ について $P(n)$ と $Q(n)$ が成り立つことを帰納法でいっぺんに示す。

§6-3 整数論の基本定理

ここでは、整数について考察する上で基礎となる2つの定理—除法の原理と素因数分解の一意性—を、6-1 節で説明した自然数の整列性と数学的帰納法を用いて証明します。

●除法の原理

整数を 0 でない別の整数で割って「商」と「余り」を求めることは小学校以来よくやってきたと思います。実は、そのようなことを可能にする背後には、自然数の整列性が隠されています。

定理 6-7 (除法の原理)

任意の $a, b \in \mathbb{Z},\ a > 0$ に対して、次の条件を満たす整数 $q, r \in \mathbb{Z}$ が一意的に存在する。

$$b = qa + r, \quad 0 \leq r < a$$

(**proof**)

I. q, r の存在の証明：

集合

$$M = \{\ b - na \mid n \in \mathbb{Z},\ b - na \geq 0\ \}$$

を考える。$b-(-|b|)a \geq 0$ より、$M \neq \varnothing$ がわかる。よって、M に最小元 r が存在する (自然数の整列性)。

$r = b - qa$ $(q \in \mathbb{Z})$ と書く。この q と r が定理の条件を満たす２つの整数となる。実際にそうなっていることを示すには、$0 \leq r < a$ が満たされていることを確かめればよい。

$r \in M$ なので、$0 \leq r$ は満たされている。$r < a$ となることを証明する。

背理法で示す。$r \geq a$ であると仮定する。すると、$0 \leq r - a = b - (q+1)a$ となる。これは $r - a \in M$ を意味し、M が r より真に小さい元 $r - a$ を含むことになり、矛盾が生じる。よって、$r < a$ でなければならない。

Ⅱ. q, r の一意性の証明：

b が次のように二通りに表わされたとする。

$$b = qa + r, \quad 0 \leq r < a$$
$$b = q'a + r', \quad 0 \leq r' < a$$

このとき、$q = q'$ かつ $r = r'$ となることを証明すればよい。まず、式変形して、

$$(*) \qquad (q - q')a = r' - r$$

を得る。ここで、$q - q' \neq 0$ であると仮定すると、等式 $(*)$ の両辺の絶対値をとって、

$$|r' - r| = |q - q'|a \geq a$$

を得る。一方、$0 \leq r, r' < a$ であるから、$|r - r'| < a$ である。ここに矛盾が生じた。よって、$q = q'$ であり、したがってまた、等式 $(*)$ より、$r = r'$ である。 □

注意：上の定理において、$b \geq 0$ のときは $q \geq 0$ になります。

実際、$0 \leq b < a$ ならば $r = b,\ q = 0$ であり、$b \geq a$ ならば $q = \frac{b-r}{a} \geq \frac{a-r}{a} > 0$ となります。

定理 6-7 と累積的帰納法を使って、次を証明することができます。

例 6-8　$a \in \mathbb{N},\ a \neq 1$ を固定すると、任意の自然数 n は

$$n = r_0 + r_1 a + r_2 a^2 + \cdots + r_k a^k$$

(但し、$k \geq 0$ であり、$r_0, r_1, \cdots, r_k$ は $r_k \neq 0$ かつ $0 \leq r_0, r_1, \cdots, r_k < a$ を満たす整数)

の形に一意的に書き表わされる。この表示を n の a **進記数表示**という。

解；

すべての自然数 n に対して

$$P(n) : \begin{cases} n \text{ は } n = r_0 + r_1 a + r_2 a^2 + \cdots + r_k a^k \\ \left(\begin{array}{l} \text{但し、} k \geq 0 \text{ であり、} r_0, r_1, \cdots, r_k \in \mathbb{Z} \text{ は} \\ r_k \neq 0 \text{ かつ } 0 \leq r_0, r_1, \cdots, r_k < a \text{ を満たす} \end{array} \right) \\ \text{の形に一意的に書き表わされる。} \end{cases}$$

が成り立つことを帰納法で証明する。

I. $n = 1, 2, \cdots, a-1$ のとき、$P(n)$ は成り立つ $(k = 0,\ r_0 = n$ にとればよい)。

Ⅱ. $n \in \mathbb{N},\ n \geq a$ であるとし、$i < n$ を満たすすべての $i \in \mathbb{N}$ に対して $P(i)$ は成り立つと仮定する。定理 6-7 より、

$$n = r_0 + qa \qquad (0 \leq r_0 < a)$$

となる $r_0, q \in \mathbb{Z}$ が一意的に存在する。$n \geq a$ により $1 \leq q < n$ であるから、q について帰納法の仮定を適用することができて、q は

$$q = r_1 + r_2 a + \cdots + r_k a^{k-1}$$

（但し、$k \geq 1$ であり、$r_1, \cdots, r_k$ は $r_k \neq 0$ かつ $0 \leq r_1, \cdots, r_k < a$ を満たす整数）

のように一意的に書き表わされる。したがって、n は、$0 \leq r_0, r_1, \cdots, r_k < a$ かつ $r_k \neq 0$ を満たす整数 $r_0, r_1, \cdots, r_k$ によって、

$$n = r_0 + (r_1 + r_2 a + \cdots + r_k a^{k-1})a = r_0 + r_1 a + r_2 a^2 + \cdots + r_k a^k$$

のように書き表わされる。

次に、この書き表わし方が一意的であることを示す。n が $0 \leq s_0, s_1, \cdots, s_l < a$ かつ $s_l \neq 0$ を満たす整数 $s_0, s_1, \cdots, s_l$ によって

$$n = s_0 + s_1 a + s_2 a^2 + \cdots + s_l a^l$$

のようにも書き表わさたとする。$n \geq a$ により $l \geq 1$ でなければいけないことがわかる。$n = s_0 + (s_1 + s_2 a + \cdots + s_l a^{l-1})a$ と書けるので、定理 6-7 の一意性の部分から、$s_0 = r_0$ かつ $q = s_1 + s_2 a + \cdots + s_l a^{l-1}$ であることがわかる。さらに、帰納法の仮定により、q の書き表わし方は一意的であるから、$k = l$ かつ $r_i = s_i$ $(i = 1, \cdots, k)$ であることがわかる。これで、n の書き表わし方が一意的であることがわかった。

以上で、$P(n)$ が成り立つことが示された。

I, II から、すべての自然数 n に対して $P(n)$ は成り立つ。 □

●倍数、約数、素数、合成数

$a, b \in \mathbb{Z},\ a \neq 0$ とします。$b = ac$ となる $c \in \mathbb{Z}$ が存在するとき、a は b の**約数** (divisor) である、あるいは、b は a で**割り切れる** (divisible)、あるいは、b は a の**倍数** (multiple) であるといいます。

$p \in \mathbb{N}$ が**素数** (prime number) であるとは、$p \neq 1$ であって、1 と p 自身以外に正の約数を持たないときをいいます。1 でも素数でもない自然数を**合成数** (composite number) といいます。

●整数論の基本定理

素因数分解の一意性に関する定理は整数論の基本定理と呼ばれています。ここでは、この定理のツェルメロ（Zermelo, 1871–1953）による巧妙な証明を紹介します。

定理 6-9 (素因数分解の可能性と一意性)

1 以外の任意の自然数 n は、素数の冪の積として次のように表わすことができる：

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

但し、$k \geq 1$ であり、$p_1, p_2, \cdots, p_k$ は相異なる素数、$e_1, e_2, \cdots, e_k$ は自然数である。

さらに、この表わし方は、$p_1^{e_1}, p_2^{e_2}, \cdots, p_k^{e_k}$ の並べ方の順番を除いて一意的である。

右辺の表示を n の**素因数分解** (prime decomposition) といい、$p_1, p_2, \cdots, p_k$ のことを n の**素因数** (prime factor) という。

(**proof**)

I. 素因数分解の可能性：この証明は演習問題とする (演習 6-4)。

II. 書き表わし方の一意性：数学的帰納法で証明する。

第 1 段 ($n = 2$ のとき)：

2 は素数であるから、これを二個以上の素数の積として表わすことはできない。よって、2 を素数の積に書き表わす仕方は唯一通りである。

第2段：n を $n>2$ なる自然数とし、n よりも小さい 2 以上の任意の自然数については、素数の積への書き表わし方は (順番を無視すれば) 一意的であると仮定する。

• n が素数の場合：第 1 段と同様の理由で、n を素数の積に書き表わす仕方は一意的である。

• n が合成数の場合：n が素数の積に次のように 2 通りの仕方で書き表わされたと仮定する (n は合成数なので、下記の表示で、$r,s\geq 2$ に注意)。

$$n=p_1p_2\cdots p_r=q_1q_2\cdots q_s \qquad (p_1,\cdots,p_r,q_1,\cdots,q_s \text{ は素数})$$

このとき、もし、q_1 が $p_1,\ p_2,\cdots,p_r$ のどれかと一致することが示されれば、$\frac{n}{q_1}\in\mathbb{N}$ に帰納法の仮定を用いて、$r=s$ であって、かつ、順番を適当に並べ変えると $p_1=q_1,p_2=q_2,\cdots,p_r=q_r$ となることがわかる。したがって、q_1 が $p_1,\ p_2,\cdots,p_r$ のどれかと一致することが示されればよい。これを背理法で示す。

q_1 が $p_1,\ p_2,\cdots,p_r$ のどれとも一致しないと仮定する。すると、特に、$q_1\neq p_1$ である。

$q_1<p_1$ のとき、

$$m:=(p_1-q_1)p_2\cdots p_r$$

は $1<m<n$ を満たす自然数であるから、帰納法の仮定により、m を素数の積に分解する仕方は順番を無視すれば一意的である。この事実と

$$(p_1-q_1)p_2\cdots p_r=q_1(q_2\cdots q_s-p_2\cdots p_r)$$

と表せることから、q_1 は、p_1-q_1 の素因数か、または、$p_2,\cdots,p_r$ のどれかに一致しなければならない。仮定から、q_1 は $p_2,\cdots,p_r$ とは一致しないので、q_1 は、p_1-q_1 の素因数、つまり、q_1 は p_1-q_1 を割り切ることがわかる。これより、q_1 は p_1 を割り切ることになるが、p_1,q_1 はともに素数であるから、$p_1=q_1$ でなければならない。これは、$q_1\neq p_1$ に矛盾する。

$q_1>p_1$ のときは、m のかわりに、$(q_1-p_1)p_2\cdots p_r$ について上と同様の議論を行って、矛盾が出る。これで、帰納法が完成し、一意性の証明が終わった。 □

演習 6-4* 累積的帰納法を用いて、定理 6-9 における、素因数分解の可能性の部分を証明せよ。

例 6-10 $n\in\mathbb{N}$ が平方数でないとき、すなわち、$n=m^2$ となる $m\in\mathbb{N}$ が存在しないとき、$\sqrt{n}$ は無理数であることを証明せよ。

解；

背理法で示す。$\sqrt{n}$ は有理数であると仮定し、$\sqrt{n}=\frac{a}{b}$ $(a,b\in\mathbb{N})$ と既約分数の形に書く。このとき、$nb^2=a^2$ が成り立つ。

$b=1$ ならば、$n=a^2$ となり、n が平方数でないことに反する。

$a=1$ ならば、$nb^2=1$ となり、$n,b^2\in\mathbb{N}$ なので、$n=1$ となる。これも、n が平方数でないことに反する。よって、$a,b\geq 2$ である。そこで、a,b を

$$a=p_1^{e_1}\cdots p_k^{e_k} \quad (p_1,\cdots,p_k \text{ は相異なる素数、} e_1,\cdots,e_k\in\mathbb{N})$$
$$b=q_1^{f_1}\cdots q_l^{f_l} \quad (q_1,\cdots,q_l \text{ は相異なる素数、} f_1,\cdots,f_l\in\mathbb{N})$$

のように素因数の積に書き表わす。このとき、

$$nq_1^{2f_1}\cdots q_l^{2f_l}=p_1^{2e_1}\cdots p_k^{2e_k}$$

となるが、分解の一意性から、左辺の q_i は右辺の $p_1,\cdots,p_k$ のどれかと一致しなければならない。これは $\frac{a}{b}$ が既約であることに矛盾する。よって、$\sqrt{n}$ は無理数である。 □

演習 6-5 $\log_{10}2$ は無理数であることを証明せよ。

§7. 実数の連続性

しばしば、実数全体を数直線と対応させて考えます。このことによって、私たちは、実数全体は“切れ目なく連なっている”というイメージを強く持っています。ここでは、その直感的な理解を反省します。ここでの目標は、実数の連続性を基礎づける過程で現れる、上限と下限という新しい概念を理解することです。

●数の四則演算に関する性質と大小関係に関する性質

私たちが数の計算するときには、いろいろな法則を適用しながら行っています。普段はあまり意識しませんが、ここで、$\mathbb{R}$ の四則演算に関する性質と大小関係に関する性質をまとめておきましょう。下記の中に出てくる a, b, c は、特に断り書きのないものは、任意の実数とします。

性質１ 加法“$+$”と乗法“$\times$”が定まっていて、

(a) 加法について次が成り立つ。

(i) **０の性質**：$a+0=a=0+a$

(ii) **結合法則**：$(a+b)+c=a+(b+c)$

(iii) **交換法則**：$a+b=b+a$

(iv) **マイナスの存在**：$a\in\mathbb{R}$ に対して、$-a\in\mathbb{R}$ を考えると、
$a+(-a)=(-a)+a=0$ となる。

(b) 乗法について次が成り立つ。

(i) **１の性質**：$1\neq 0$ であって、$1\cdot a=a=a\cdot 1$

(ii) **結合法則**：$(ab)c=a(bc)$

(iii) **交換法則**：$ab=ba$

(iv) **逆数の存在**：$0\neq a\in\mathbb{R}$ に対して、その逆数 $\dfrac{1}{a}\in\mathbb{R}$ を考えると、
$a\cdot\dfrac{1}{a}=\dfrac{1}{a}\cdot a=1$ となる。

(c) 加法と乗法の間に**分配法則**が成り立つ：
$$a(b+c)=ab+ac,\quad (a+b)c=ac+bc.$$

性質２ 大小関係“$<$”が定まっていて、

(a) $a<b$ または $a=b$ または $a>b$
のいずれか１つが成り立ち、かつ、２つが同時に成り立つことはない。

(b) **推移性**を持つ：$a<b,\ b<c \implies a<c.$

性質３ 加法、乗法と大小関係について、次が成り立つ。

(a) $a<b \iff a+c<b+c$

(b) $c>0$ のとき、$a<b \iff ac<bc$

注意：1. 性質 3(b) から、$0<1$ であることがわかります。なぜならば、$1<0$ と仮定すると、$0=0\cdot(-1)<(-1)\cdot(-1)=1$ となり矛盾が生じるからです。また、$c<0$ のとき、「$a<b \iff ac>bc$」となることが性質 3(a) と性質 3(b) からわかります。

2. 上記の $\mathbb{R}$ の性質は、$\mathbb{Q}$ においてもすべて成立します。また、$\mathbb{N}$, $\mathbb{Z}$ においても

$\left.\begin{array}{l}\mathbb{Z}\text{ における逆数の存在}\\ \mathbb{N}\text{ におけるマイナスの存在、逆数の存在}\end{array}\right\}$ 以外は全部成立

します（0 は $\mathbb{N}$ の元ではないので、性質 1(a)(i) は考える必要がないことに注意しましょう）。

●区間

$\mathbb{R}$ の部分集合 I は、次の２つの条件を満たすとき、**区間** (interval) と呼ばれます。

(i) I は相異なる実数を少なくとも２つ含む。

(ii) $a, b \in I,\ a < b$ ならば、$a \leq x \leq b$ を満たす任意の $x \in \mathbb{R}$ について、$x \in I$ となる。

例 7-1　a, b を $a < b$ を満たす実数とする。このとき、次の (1) から (8) までの部分集合および $\mathbb{R}$ はすべて区間である。

(1) $[a,b] := \{\, x \in \mathbb{R} \mid a \leq x \leq b \,\}$　　(2) $(a,b) := \{\, x \in \mathbb{R} \mid a < x < b \,\}$

(3) $(a,b] := \{\, x \in \mathbb{R} \mid a < x \leq b \,\}$　　(4) $[a,b) := \{\, x \in \mathbb{R} \mid a \leq x < b \,\}$

(5) $(-\infty, a) := \{\, x \in \mathbb{R} \mid x < a \,\}$　　(6) $(a, \infty) := \{\, x \in \mathbb{R} \mid a < x \,\}$

(7) $(-\infty, a] := \{\, x \in \mathbb{R} \mid x \leq a \,\}$　　(8) $[a, \infty) := \{\, x \in \mathbb{R} \mid a \leq x \,\}$

(1) の形の区間を**有界閉区間**、または単に、**閉区間** (closed interval) といい、(2)(5)(6) の形の区間および $\mathbb{R}$ を**開区間** (open interval) という。

●実数の連続性

実数には、冒頭において述べた性質の他に、**連続性**と呼ばれる大切な性質—アルキメデスの公理とカントールの公理— があります。

アルキメデスの公理

２つの正の実数 a, b に対して、$a < nb$ となる自然数 n が存在する。

注意：アルキメデスの公理において a, b が有理数の場合には定理です。実際、有理数 $a = \frac{l}{m},\ b = \frac{p}{q}$ $(l, m, p, q \in \mathbb{N})$ に対して $n = 2lq \in \mathbb{N}$ をとれば $a < nb$ が満たされます。

また、アルキメデスの公理において a, b が $a \leq b$ を満たす場合にも定理になります。実際、n として 2 をとれば確かに $a < nb$ が満たされます。

アルキメデスの公理はことわざ「塵も積もれば山となる」に例えられることがあります。というのは、その公理が、本質的には、「a がどんなに大きな正の数であって、b がどんなに小さな正の数であっても、b を繰り返し繰り返し加えていけばいつかは a を超えることができる」ことを主張していると解釈されるからです。

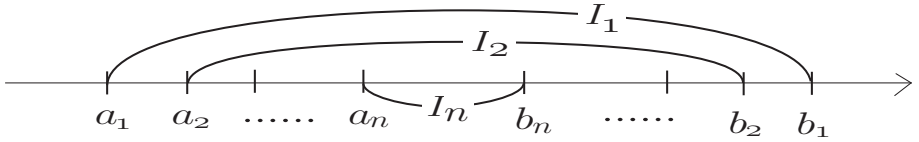
アルキメデスの公理は、上の注意で述べたように、$\mathbb{Q}$ においても成り立ちますが、次のカントールの公理は $\mathbb{Q}$ では成り立たない、$\mathbb{R}$ 固有の性質です。

カントールの公理（区間縮小法の原理）

閉区間の減少列

$$I_1 \supset I_2 \supset I_3 \supset \cdots\cdots \supset I_n \supset I_{n+1} \supset \cdots\cdots$$

が任意に与えられたとき、すべての I_n $(n = 1, 2, 3, \cdots)$ に共通に含まれる実数が存在する。すなわち、$\bigcap_{n=1}^{\infty} I_n \neq \varnothing$ である。



例えば、次のように定義される閉区間の減少列 $I_1 \supset I_2 \supset I_3 \supset \cdots\cdots$ を考えてみましょう。まず、$I_1 = [1, 2]$ と定めます。次に、I_1 を 10 等分して $(1 + \frac{a_1}{10})^2 < 2 < (1 + \frac{a_1+1}{10})^2$ を満たす $a_1 \in \{0, 1, \cdots, 9\}$ を探します。$a_1 = 4$ とわかります。そこで、$I_2 = [1.4, 1.5]$ とおきます。次に、I_2 を 10 等分して $(1.4 + \frac{a_2}{100})^2 < 2 < (1.4 + \frac{a_2+1}{100})^2$ を満たす $a_2 \in \{0, 1, \cdots, 9\}$ 探します。$a_2 = 1$ とわかります。そこで、$I_3 = [1.41, 1.42]$ とおきます。以下、同様にして閉区間 $I_4, \cdots, I_n, \cdots$ を帰納的に定めていきます。すると、カントールの公理から $\bigcap_{n=1}^{\infty} I_n$ は空でないことがわかりますが、それに属する元は $\sqrt{2}$ に他なりません。逆に言えば、自乗して 2 になる数 $\sqrt{2}$ の「存在」をカントールの公理が保証しているのです。

なお、カントールの公理において、閉区間を開区間に置き換えた命題は成り立ちません。例えば、$I_n = (0, \frac{1}{n})$ $(n = 1, 2, \cdots\cdots)$ に対しては、アルキメデスの公理により、$\bigcap_{n=1}^{\infty} I_n = \varnothing$ になってしまいます (確かめてみて下さい)。

●稠密性（ちゅうみつ）

アルキメデスの公理と自然数の整列性を使うと、どんな実数についても、そのいくらでも近くに有理数が存在するという、実数における有理数の稠密性を証明することができます。

補題 7-2

任意の実数 a に対して、$n \leq a < n + 1$ を満たす整数 n が一意的に存在する。

(**proof**)

I. n の存在：

(i) $a > 0$ の場合：アルキメデスの公理から、

$$A := \{\, n \in \mathbb{N} \mid a < n + 1 \,\}$$

は空ではない。したがって、自然数の整列性により、A には最小元 n が存在する。この n は $n \leq a < n + 1$ を満たす。

(ii) $a = 0$ の場合：$n = 0$ とおくと、 $n \leq a < n + 1$ を満たす。

(iii) $a < 0$ の場合：$-a > 0$ なので、アルキメデスの公理から、

$$B := \{\, n \in \mathbb{N} \mid -a \leq n \,\}$$

は空ではない。したがって、自然数の整列性により、B には最小元 m が存在する。この m は $m - 1 < -a \leq m$ を満たす。そこで、$n = -m$ とおけば、この $n \in \mathbb{Z}$ は $n \leq a < n + 1$ を満たす。

II. n の一意性：

$n, m \in \mathbb{Z}$ に対して、$n \leq a < n + 1$ かつ $m \leq a < m + 1$ が成り立っているとする。

ここで、$m < n$ であると仮定すると、$m + 1 \leq n$ である（$\because n - m \in \mathbb{N}$ より、$n - m \geq 1$）から、$n \leq a < m + 1 \leq n$ が得られて、矛盾が生じる。同様に、$n < m$ であると仮定しても矛盾が生じるので、$n = m$ でなければならない。 □

定理 7-3 (実数における有理数の稠密性)
任意の実数 a と任意の $\varepsilon > 0$ に対して、$|a - r| < \varepsilon$ となる有理数 r が存在する。

(**proof**)

(i) $a \geq 0$ の場合：アルキメデスの公理より、$1 < n\varepsilon$ となる $n \in \mathbb{N}$ が存在する。このとき、補題 7-2 により、$m - 1 \leq na < m$ を満たす整数 m が存在する。これより

$$\left|\frac{m}{n} - a\right| \leq \frac{1}{n} < \varepsilon$$

が成立するので、$r := \frac{m}{n} \in \mathbb{Q}$ が求める有理数である。

(ii) $a < 0$ の場合：$-a > 0$ であるから、(i) により、$|-a - s| < \varepsilon$ となる有理数 s が存在する。このとき、$|a - (-s)| < \varepsilon$ であるから、$r := -s \in \mathbb{Q}$ が求める有理数である。 □

注意： a のかわりに $a + \sqrt{2}$ について上の定理を適用して、任意の実数 a と任意の $\varepsilon > 0$ に対して、$|a - x| < \varepsilon$ となる無理数 x が存在することもわかります。

●最大元と最小元

A を $\mathbb{R}$ の空でない部分集合とします。A に属する元の中で最も小さい元が存在するとき、その元のことを A の**最小元** (minimum element) と呼びます (これについては第 6 節ですでに定義しました)。A の最小元を記号 $\min A$ によって書き表わします。A の最小元 $\min A$ とは次の 2 条件を満たす実数 m のことに他なりません。

$$\text{(i) } m \in A \qquad \text{(ii) } \forall\, a \in A,\ m \leq a.$$

上とは対照的に、A に属する元の中で最も大きな元が存在するとき、その元のことを A の**最大元** (maximum element) といい、記号 $\max A$ によって書き表わします。A の最大元 $\max A$ とは次の 2 条件を満たす実数 m のことに他なりません。

$$\text{(i) } m \in A \qquad \text{(ii) } \forall\, a \in A,\ m \geq a.$$

A に最小元が存在するならば、それは唯 1 つであり、A に最大元が存在するならば、やはりそれは唯 1 つであることに注意しましょう。

演習 7-1 a, b を $a < b$ を満たす実数とするとき、次が成り立つことを示せ。
(1) 閉区間 $[a, b]$ は最大元と最小元を持ち、$\min[a, b] = a,\ \max[a, b] = b$ である。
(2) 開区間 (a, b) は最大元も最小元も持たない。

ヒント：(2) は背理法で示す。

●有界

定義 7-4
A を $\mathbb{R}$ の部分集合とする。
(1) A が**上に有界** (bounded from above) であるとは、

$$\exists\, \alpha \in \mathbb{R} \ \text{ s.t. } \ \forall\, a \in A,\ a \leq \alpha$$

が成り立つときをいう。このような α を A の**上界**(じょうかい) (upper bound) という。

(2) A が**下に有界** (bounded from below) であるとは、

$$\exists \alpha \in \mathbb{R} \ \text{ s.t. } \ \forall a \in A,\ a \geq \alpha$$

が成り立つときをいう。このような α を A の**下界**(かかい)(lower bound) という。

(3) A が**有界** (bounded) であるとは、

$$\exists \alpha > 0 \ \text{ s.t. } \ \forall a \in A,\ -\alpha \leq a \leq \alpha$$

が成り立つときをいう。

注意：1. $\mathbb{R}$ の部分集合 A が有界であるための必要十分条件は、A が上に有界かつ下に有界であることです。

2. α が A の上界（resp. 下界）ならば、それよりも大きい（resp. 小さい）任意の実数もまた A の上界（resp. 下界）になります。

例 7-5 a, b を $a < b$ であるような２つの実数とするとき、４つの区間 $[a,b]$, (a,b), $(a,b]$, $[a,b)$ はすべて有界である。一方、区間 $(-\infty, a)$, $(-\infty, a]$ は上に有界であるが、下に有界ではない。また、区間 (a,∞), $[a,\infty)$ は下に有界であるが、上に有界ではない。

●上限と下限

演習 7-1 で観察したように、開区間 (a,b) には最大元も最小元も存在しません。しかしながら、a (resp. b) という最小元 (resp. 最大元) の「代役」を果たせそうな実数は存在します。ここでは、このような実数が、$\mathbb{R}$ の空でない有界な部分集合には常に存在することを示します。

定義 7-6

A を $\mathbb{R}$ の空でない部分集合とする。

(1) A の上界全体からなる $\mathbb{R}$ の部分集合

$$\{\ \alpha \in \mathbb{R} \mid \forall a \in A,\ a \leq \alpha\ \}$$

に最小元が存在するとき、その最小元を A の**上限**（supremum）といい、記号 $\sup A$ で表わす。

(2) A の下界全体からなる $\mathbb{R}$ の部分集合

$$\{\ \alpha \in \mathbb{R} \mid \forall a \in A,\ \alpha \leq a\ \}$$

に最大元が存在するとき、その最大元を A の**下限**（infimum）といい、記号 $\inf A$ で表わす。

例 7-7 A に最大元が存在するとき、$\sup A = \max A$ となり、A に最小元が存在するとき、$\inf A = \min A$ となる。

解；

$M := \{\ \alpha \in \mathbb{R} \mid \forall a \in A,\ a \leq \alpha\ \}$ とおく。A に最大元が存在する場合を考える。

$m := \max A$ とおくと、任意の $a \in A$ について、$a \leq m$ であるから、$m \in M$ である。また、$m \in A$ なので、任意の $\alpha \in M$ に対して、$m \leq \alpha$ である。故に、m は M の最小元、すなわち、$\sup A$ に一致する。

A に最小元が存在する場合も同様に考察すれば、$\inf A = \min A$ が示される。 □

上の例と演習 7-1(1) により、閉区間 $[a,b]$ について

$$\inf[a,b] = \min[a,b] = a, \qquad \sup[a,b] = \max[a,b] = b$$

となることがわかります。

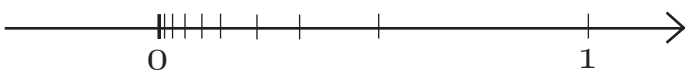
演習 7-2 * 開区間 (a,b) について、$\inf(a,b) = a,\ \sup(a,b) = b$ となることを示せ。

ヒント：$\inf(a,b) = a$ を示すには、次の 2 つを示せばよい。

① $\forall\, x \in (a,b),\ x \geq a$　　② $a < a' \ \Rightarrow\ \exists\, x \in (a,b)$ s.t. $x < a'$

例 7-8　$A = \{\ \frac{1}{n} \mid n \in \mathbb{N}\ \}$ について、$\sup A = 1,\ \inf A = 0$ である。

解；



A は 1 を最大元に持つから、例 7-7 により、$\sup A = \max A = 1$ である。

次に、$\inf A = 0$ を示す。

まず、任意の $n \in \mathbb{N}$ に対して $0 \leq \frac{1}{n}$ であるから、0 は A の下界である。

0 が A の最大下界であることを示すために、0 よりも大きな数 ε は A の下界ではないことを示す。1 と ε に対してアルキメデスの公理を適用して、$1 < n\varepsilon$ となる $n \in \mathbb{N}$ の存在がわかる。このとき、$\frac{1}{n} < \varepsilon$ となる。これは ε が A の下界ではないことを意味する。よって、0 は A の最大下界、すなわち、$\inf A = 0$ である。　□

アルキメデスの公理と区間縮小法の原理から、次の定理— 上限公理またはワイエルストラスの定理と呼ばれることもあります—が証明されます。

定理 7-9

A が $\mathbb{R}$ の空でない部分集合とする。このとき、

(1) A が上に有界ならば、上限 $\sup A$ が存在する。

(2) A が下に有界ならば、下限 $\inf A$ が存在する。

(**proof**)

(2) は A の代わりに $-A = \{-a \in \mathbb{R} \mid a \in A\ \}$ を考えれば (1) に帰着されるので (詳しくは下の演習 7-3 を参照)、ここでは、(1) のみ証明する。

$\varnothing \neq A \subset \mathbb{R}$ は上に有界であるとし、A の上界でない実数 a_1 と A の上界 b_1 を取る。

注)

このような実数 a_1, b_1 が存在することは、次のようにしてわかる。

$a \in A$ を 1 つとるとき、それよりも小さい実数は A の上界でない。したがって、その 1 つを a_1 と置けばよい。また、A は上に有界なので、上界が存在する。その 1 つを b_1 と置けばよい。　□

このとき、$a_1 < b_1$ となる。そこで、$I_1 := [a_1, b_1]$ とおく。

次に、自然数 $n \in \mathbb{N}$ に対して、閉区間 $I_n = [a_n, b_n]$ が構成されたとき、2 つの実数 a_{n+1}, b_{n+1} を次のように定義する。

$$\begin{cases} \dfrac{a_n+b_n}{2} \text{ が } A \text{ の上界である場合、} & a_{n+1} := a_n,\ b_{n+1} := \dfrac{a_n+b_n}{2} \\ \dfrac{a_n+b_n}{2} \text{ が } A \text{ の上界でない場合、} & a_{n+1} := \dfrac{a_n+b_n}{2},\ b_{n+1} := b_n \end{cases}$$

$a_{n+1} < b_{n+1}$ となるので、$I_{n+1} := [a_{n+1}, b_{n+1}]$ とおく。このようにして、$n = 1, 2, 3, \cdots$ に対して、閉区間 $I_n = [a_n, b_n]$ を帰納的に構成する。すると、次の2つが成り立つ。

(☆) $$I_1 \supset I_2 \supset I_3 \supset \cdots\cdots$$

(★) $$b_n - a_n = \frac{b_{n-1} - a_{n-1}}{2} = \cdots = \frac{b_1 - a_1}{2^{n-1}} \leq \frac{b_1 - a_1}{n} \qquad (n = 1, 2, 3, \cdots)$$

(☆) により、すべての I_n $(n = 1, 2, 3, \dots)$ に共通に含まれる実数 $\alpha \in \mathbb{R}$ が存在する（区間縮小法の原理)。このとき、$\alpha = \sup A$ であることを証明する。

• α が A の上界であること：

背理法で示す。α が A の上界でなかったと仮定する。すると、

$$\exists\, a \in A \ \text{ s.t. } \ \alpha < a$$

が成り立つ。(そこで、そのような $a \in A$ を1つとる。) ここで、2つの正の実数 $a - \alpha,\ b_1 - a_1$ に対して、アルキメデスの公理を適用すると、$b_1 - a_1 < n(a - \alpha)$ となる $n \in \mathbb{N}$ の存在がわかる。このとき、(★) により

$$b_n - a_n \leq \frac{b_1 - a_1}{n} < a - \alpha$$

を得る。一方、b_n は A の上界なので $a \leq b_n$ であり、$\alpha \in [a_n, b_n]$ なので $\alpha \geq a_n$ である。よって、$a - \alpha \leq b_n - a_n$ でなければならない。ここに矛盾が生じた。故に、α は A の上界である。

• α が A の最小上界であること：

背理法で示す。α が A の最小上界でないと仮定する。すると、$\beta < \alpha$ を満たす A の上界 β が存在する。アルキメデスの公理により、

$$\exists\, n \in \mathbb{N} \ \text{ s.t. } \ b_1 - a_1 < n(\alpha - \beta)$$

が成り立つ。(そこで、そのような $n \in \mathbb{N}$ を1つとる。) すると、(★) により

$$b_n - a_n \leq \frac{b_1 - a_1}{n} < \alpha - \beta$$

を得る。しかし、$\alpha \in [a_n, b_n]$ なので $\alpha \leq b_n$ であり、a_n は A の上界でなく、β は A の上界なので、$a_n < \beta$ である (定義 7-4 の下の注意 2 参照)。よって、$\alpha - \beta \leq b_n - a_n$ でなければならない。ここに矛盾が生じた。故に、α は A の最小上界である。 □

演習 7-3 A が $\mathbb{R}$ の空でない部分集合とする。

$-A := \{-a \in \mathbb{R} \mid a \in A\}$ とおくとき、次が成り立つことを示せ。

(1) A が下に有界 $\iff$ $-A$ が上に有界

(2) A が下に有界なとき、$\sup(-A) = -\inf A$

演習 7-4 A, B を $\mathbb{R}$ の空でない上に有界な2つの部分集合とする。

$A \subset B$ のとき、$\sup A \leq \sup B$ となることを示せ。

次の命題に書かれている言い換えはよく使われます。

命題 7-10

A を $\mathbb{R}$ の空でない部分集合とする。

(1) $\sup A$ は、次の２つの条件を満たす実数 α として特徴づけることができる。

(i) $\forall a \in A,\ a \leq \alpha$

(ii) $\forall \varepsilon > 0,\ \exists a \in A$ s.t. $\alpha - \varepsilon < a$

(2) $\inf A$ は、次の２つの条件を満たす実数 α として特徴づけることができる。

(i) $\forall a \in A,\ a \geq \alpha$

(ii) $\forall \varepsilon > 0,\ \exists a \in A$ s.t. $\alpha + \varepsilon > a$

(**proof**)

ここでは、(2) を演習問題として残し、(1) のみを証明する。次の２つを証明すればよい。

① $\sup A$ は (i)(ii) の条件を満たす。

② (i)(ii) の条件を満たす実数 α は $\sup A$ に一致する。

A の上界全体からなる集合を M とおく。すなわち、

$$M := \{\ \alpha \in \mathbb{R} \mid \forall a \in A,\ a \leq \alpha\ \}$$

とおく。上限の定義により、$\sup A$ は M の最小元である。

①の証明：$\sup A \in M$ なので、(i) が成り立つ。

次に、$\alpha = \sup A$ のとき、(ii) が成り立たないと仮定する。すると、

$$\exists \varepsilon > 0 \ \text{ s.t. } \ \forall a \in A,\ \sup A - \varepsilon \geq a$$

が成り立つ。（そこで、そのような ε を１つとる。）このとき、$\sup A - \varepsilon \in M$ となる。これは、$\sup A$ が M の最小元であることに反する。よって、$\alpha = \sup A$ のとき、(ii) は成り立つ。

②の証明：$\alpha \in \mathbb{R}$ が (i)(ii) を満たしているとする。

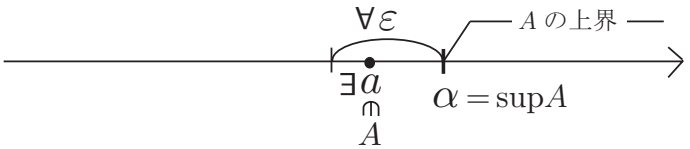
(i) によって、$\alpha \in M$ であることがわかる。α が M の最小元であることを証明するために、$\beta \in M$ を任意にとる ($\beta \geq \alpha$ を証明することが目標である)。

もし、$\beta < \alpha$ であったと仮定する。このとき、$\varepsilon := \alpha - \beta$ を考えると、これは正の実数であるから、(ii) により、

$$\exists a \in A \ \text{ s.t. } \ \alpha - (\alpha - \beta) < a$$

が成り立つ。これは $\beta \in M$ であることに矛盾する。よって、$\beta \geq \alpha$ でなければならない。

故に、$\alpha = \min M = \sup A$ である。 □



注意：(1)(i) は α が A の上界であることを表わしていて、(1)(ii) は、「α よりも少しでも小さい（任意に $\varepsilon > 0$ をとって $\alpha - \varepsilon$ を考える）と、それよりも大きな A の元 a が存在する（つまり、上界ではなくなる)」ということを表わしています。このことを考えれば、(1) の (i)(ii) の条件を満たす α が A の上限であることは容易に理解できるでしょう。

演習 7-5 * 命題 7-10(2) を証明せよ。

§8. 数列の極限

ここでは、前節で説明した実数の連続性 — アルキメデスの公理とカントールの公理（区間縮小法の原理）— を数列の収束という概念を使って言い換えます。ここでの目標は、数列の極限の厳密な定義およびその取り扱いを通じて、“$\varepsilon - N$ 論法”を使えるようになることです。

●絶対値の性質

すでに使っている記号ですが、実数 a に対して

$$|a| := \max\{a,\ -a\}$$

を a の**絶対値** (absolute value) といいます。今後、絶対値の記号はよく使うので、ここでその性質をまとめておきましょう。

補題 8-1

任意の $a, b \in \mathbb{R}$ に対して、次の 3 つが成り立つ。

(i) $|a+b| \leq |a| + |b|$　(**三角不等式**)

(ii) $|ab| = |a||b|$

(iii) $|-a| = |a|$

注意：(i) と (iii) から、任意の $a, b \in \mathbb{R}$ に対して、$|a| - |b| \leq |a+b|$ が成り立ちます。実際、

$$|a| = |(a+b)+(-b)| \leq |a+b| + |-b| = |a+b| + |b|$$

となります。

演習 8-1　任意 $\varepsilon > 0$ に対して $|a| < \varepsilon$ となるような実数 a は 0 であることを示せ。

●数列の有界性

数列 $\{a_n\}_{n=1}^{\infty}$ がそれぞれ、**上に有界**、**下に有界**、**有界**であるとは、$\mathbb{R}$ の部分集合 $\{a_n \mid n \in \mathbb{N}\}$ がそれぞれ上に有界、下に有界、有界であるときをいいます。

●単調増加数列と単調減少数列

数列 $\{a_n\}_{n=1}^{\infty}$ が**単調増加数列** (monotone increasing sequence) であるとは、

$$a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n \leq a_{n+1} \leq \cdots$$

が成り立つときをいいます。

数列 $\{a_n\}_{n=1}^{\infty}$ が**単調減少数列** (monotone decreasing sequence) であるとは、

$$a_1 \geq a_2 \geq a_3 \geq \cdots \geq a_n \geq a_{n+1} \geq \cdots$$

が成り立つときをいいます。

例 8-2　k を正の実数とし、漸化式 $a_1 = 1,\ a_{n+1} = \frac{1}{2}(a_n + \frac{k}{a_n})$ $(n = 1, 2, \cdots)$ により定義される数列 $\{a_n\}_{n=1}^{\infty}$ を考える。この数列は下に有界であり、第 2 項以降は単調減少である。

解；

まず、$\{a_n\}_{n=1}^{\infty}$ が下に有界であることを確かめる。(相加平均) $\geq$ (相乗平均) により、

$$a_{n+1} = \frac{1}{2}(a_n + \frac{k}{a_n}) \geq \sqrt{a_n \cdot \frac{k}{a_n}} = \sqrt{k} \qquad (n = 1, 2, \cdots\cdots)$$

を得る。したがって、$\{a_n\}_{n=1}^{\infty}$ は下に有界である。

次に、$\{a_n\}_{n=2}^{\infty}$ が単調減少数列であることを確かめる。$n \geq 2$ に対して、$a_n^2 \geq (\sqrt{k})^2 = k$ であるから、

$$a_{n+1} - a_n = \frac{1}{2}(a_n + \frac{k}{a_n}) - a_n = \frac{k - a_n^2}{2a_n} \leq 0$$

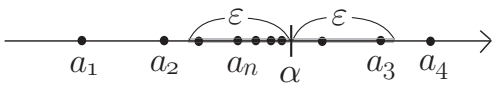
となる。故に、$\{a_n\}_{n=2}^{\infty}$ は単調減少数列である。 □

●数列の極限

高校の教科書では、数列の極限について、おおよそ次のように説明しています。

> 数列 $\{a_n\}_{n=1}^{\infty}$ において、項の番号 n を限りなく大きくするとき、a_n が一定の値 α に限りなく近づく 場合、α を数列 $\{a_n\}_{n=1}^{\infty}$ の極限値といい、
>
> $$\lim_{n\to\infty} a_n = \alpha \quad \text{または} \quad a_n \to \alpha \quad (n \to \infty)$$
>
> と書く。

「限りなく大きくする」「限りなく近づく」ということは直感的には理解できることですが、実際にこれを確かめようとした場合、何をすればよいのか困ります。そこで、このようなあいまい表現を使わずに極限の定義を定式化しましょう。



数列 $\{a_n\}_{n=1}^{\infty}$ について考えます。これが実数 α に収束する状況を思い浮かべてみましょう。まず、α のいくらでも近くに a_n がなければいけませんね。この「いくらでも近くに a_n がある」ということは、「どのような $\varepsilon > 0$ を与えても、開区間 $(\alpha - \varepsilon,\ \alpha + \varepsilon)$ の中に a_n がある」ということであると考えることができます。つまり、$\varepsilon = 1,\ \frac{1}{10},\ \frac{1}{100},\ \frac{1}{1000}, \cdots$ のように ε をどんどん小さくしていったとしても、開区間 $(\alpha - \varepsilon,\ \alpha + \varepsilon)$ の中には必ず a_n があるというわけです。でも、開区間 $(\alpha - \varepsilon,\ \alpha + \varepsilon)$ の中にただ a_n があるというのでは、「収束する」というイメージに合いません。例えば、数列 $\{(-1)^n(1 - \frac{1}{n})\}_{n=1}^{\infty}$ に対して 1 を考えると、どのような $\varepsilon > 0$ を与えても開区間 $(1 - \varepsilon,\ 1 + \varepsilon)$ の中に数列 $\{(-1)^n(1 - \frac{1}{n})\}_{n=1}^{\infty}$ の項が入っていますが、この数列は振動しているので 1 に収束するわけではありません。このような数列を排除して、「収束する」ということのイメージに合うようにするためには、ある番号から先の n についてはすべて、$a_n \in (\alpha - \varepsilon,\ \alpha + \varepsilon)$ となっている、すなわち、$|a_n - \alpha| < \varepsilon$ となっていることを要請すればよいでしょう。このような考察から、次の定義に到達します。

定義 8-3

数列 $\{a_n\}_{n=1}^{\infty}$ が実数 α に**収束する** (converge) とは、どのような実数 $\varepsilon > 0$ に対しても、次の条件 $(*)$ を満たす自然数 N が存在するときをいう：

$(*)$ $n > N$ を満たすすべての自然数 n について、$|a_n - \alpha| < \varepsilon$ である。

このとき、α を数列 $\{a_n\}_{n=1}^{\infty}$ の**極限** (limit) または**極限値** (limit value) といい、

$$\lim_{n\to\infty} a_n = \alpha \quad \text{または} \quad a_n \to \alpha \quad (n \to \infty)$$

のように書き表わす。

注意：1. 数列の極限は、それが存在するならば、一意的です（演習 8-2)。
2. 数列 $\{a_n\}_{n=1}^{\infty}$ が $\alpha \in \mathbb{R}$ に収束することを、論理記号を使って、

$$「\forall\, \varepsilon > 0,\ \exists\, N \in \mathbb{N}\ \text{ s.t. }\ n > N\ \Rightarrow\ |a_n - \alpha| < \varepsilon」\text{が成り立つ}$$

のように表現します。通常、“ が成り立つ ”の部分は省略します。
3. 数列 $\{a_n\}_{n=1}^{\infty}$ が**収束する**とは、$\lim_{n\to\infty} a_n = \alpha$ となる実数 α が存在するときをいいます。

演習 8-2　数列 $\{a_n\}_{n=1}^{\infty}$ が収束するならば、その極限は一意的であることを示せ。

演習 8-3* $\lim_{n\to\infty} \frac{1}{n} = 0$ であることを示せ（ヒント：アルキメデスの公理を用いる)。

●数列の収束と有界性

前節において、「上に有界な空でない部分集合 $A \subset \mathbb{R}$ には、いつでも上限 $\sup A$ が存在する」という定理を証明しました (定理 7-9)。このことを、数列を使って言い換えたものが次の定理です。

定理 8-4
上に有界な単調増加数列は収束する。

(**proof**)
数列 $\{a_n\}_{n=1}^{\infty}$ は上に有界で、かつ、単調増加であるとする。
数列 $\{a_n\}_{n=1}^{\infty}$ は上に有界なので、$\mathbb{R}$ の部分集合

$$A = \{\ a_n \mid n \in \mathbb{N}\ \}$$

は上に有界である。したがって、$\sup A$ が存在する (定理 7-9)。
$\{a_n\}_{n=1}^{\infty}$ は $\alpha := \sup A$ に収束することを示す。そのために、任意に $\varepsilon > 0$ を 1 つとる。このとき、命題 7-10 により、

(i) $\forall\, n \in \mathbb{N},\ a_n \le \alpha$
(ii) (上でとった $\varepsilon > 0$ に対して、) $\exists\, N \in \mathbb{N}$ s.t. $\alpha - \varepsilon < a_N$

が成り立つ。(そこで、(ii) の条件を満たす $N \in \mathbb{N}$ を 1 つとる。) ここで、$\{a_n\}_{n=1}^{\infty}$ が単調増加であることを使って、

$$\alpha - \varepsilon < a_N \le a_{N+1} \le a_{N+2} \le \cdots\cdots \le \alpha$$

がわかる。よって、$n > N$ を満たすすべての $n \in \mathbb{N}$ に対して $\alpha - \varepsilon < a_n \le \alpha$、すなわち、$|a_n - \alpha| < \varepsilon$ が成り立つ。これは、$\lim_{n\to\infty} a_n = \alpha$ であることを意味する。 □

注意：定理の証明から、上に有界な単調増加数列 $\{a_n\}_{n=1}^{\infty}$ の極限は $\sup\{\ a_n \mid n \in \mathbb{N}\ \}$ によって与えられることもわかります。

演習 8-4* 下に有界な単調減少数列は収束することを証明せよ。

数列が有界であっても収束するとは限りません (例えば $\{(-1)^n\}_{n=1}^{\infty}$ はそのような数列の 1 つです) が、次の命題で示すように、収束する数列は常に有界です。このことは、収束する数列については「とる値の範囲」が (際限なく大きなったり小さなったりせずに) ある一定の範囲内に限られることを意味しています。

命題 8-5

収束する数列は有界である。

(**proof**)

数列 $\{a_n\}_{n=1}^{\infty}$ が α に収束しているとすると、

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N}\ \text{ s.t. }\ n > N\ \Rightarrow\ |a_n - \alpha| < \varepsilon$$

が成り立つ。したがって、特に、$\varepsilon = 1$ に対して、「$n > N_0\ \Rightarrow\ |a_n - \alpha| < 1$」を満たす自然数 N_0 が存在する。このとき、

$$M := \max\{\ |a_1|, |a_2|, \cdots, |a_{N_0}|,\ |\alpha| + 1\ \}$$

とおくと、$M > 0$ であって、すべての $n \in \mathbb{N}$ について $|a_n| \leq M$ が成り立つ。よって、$\{a_n\}_{n=1}^{\infty}$ は有界である。 □

●数列の和、差、積、商

２つの数列 $\{a_n\}_{n=1}^{\infty},\ \{b_n\}_{n=1}^{\infty}$ が与えられたとき、新たに４つの数列

$$\{a_n + b_n\}_{n=1}^{\infty},\quad \{a_n - b_n\}_{n=1}^{\infty},\quad \{a_n b_n\}_{n=1}^{\infty},\quad \{\tfrac{a_n}{b_n}\}_{n=1}^{\infty}$$

を作ることができます（但し、４番目の数列は、すべての $n \in \mathbb{N}$ について $b_n \neq 0$ のときのみ作ることができます)。この４つの数列を、左から順に、$\{a_n\}_{n=1}^{\infty}$ と $\{b_n\}_{n=1}^{\infty}$ の**和、差、積、商**と呼びます。

命題 8-6

２つの数列 $\{a_n\}_{n=1}^{\infty},\ \{b_n\}_{n=1}^{\infty}$ が収束するとき、

$$\{a_n + b_n\}_{n=1}^{\infty},\quad \{a_n - b_n\}_{n=1}^{\infty},\quad \{a_n b_n\}_{n=1}^{\infty},\quad \{\tfrac{a_n}{b_n}\}_{n=1}^{\infty}$$

はすべて収束して、

(1) $\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$,
$\lim_{n\to\infty}(a_n - b_n) = \lim_{n\to\infty} a_n - \lim_{n\to\infty} b_n$

(2) $\lim_{n\to\infty}(a_n b_n) = (\lim_{n\to\infty} a_n)(\lim_{n\to\infty} b_n)$

(3) $\lim_{n\to\infty} \dfrac{a_n}{b_n} = \dfrac{\lim_{n\to\infty} a_n}{\lim_{n\to\infty} b_n}$

が成り立つ。但し、商については、すべての $n \in \mathbb{N}$ について $b_n \neq 0$、かつ、$\lim_{n\to\infty} b_n \neq 0$ であるとする。

(**proof**)

(1) については演習問題として残し、(2) と (3) について証明する。

(2) $\lim_{n\to\infty} a_n = \alpha,\ \lim_{n\to\infty} b_n = \beta$ とおく。

まず、三角不等式により、任意の $n \in \mathbb{N}$ について

$$|a_n b_n - \alpha\beta| \leq |a_n b_n - a_n\beta| + |a_n\beta - \alpha\beta| = |a_n||b_n - \beta| + |a_n - \alpha||\beta|$$

が成り立つことに注意する。

さて、任意に $\varepsilon > 0$ をとる。$\{a_n\}_{n=1}^{\infty}$ は収束するので有界である (命題 8-5)。したがって、

$$\exists M > 0\ \text{ s.t. }\ \forall n \in \mathbb{N},\ |a_n| \leq M$$

が成り立つ。（そこで、このような M を 1 つとる。）

$\lim_{n\to\infty} a_n = \alpha$, $\lim_{n\to\infty} b_n = \beta$ なので、$\varepsilon_0 := \frac{\varepsilon}{M+|\beta|+1} > 0$ に対して、

$$\exists N_1 \in \mathbb{N} \text{ s.t. } n > N_1 \Rightarrow |a_n - \alpha| < \varepsilon_0$$
$$\exists N_2 \in \mathbb{N} \text{ s.t. } n > N_2 \Rightarrow |b_n - \beta| < \varepsilon_0$$

が成り立つ。そこで、(上のような N_1, N_2 を 1 つずつとり、) $N := \max\{N_1, N_2\}$ とおくと、$N \in \mathbb{N}$ であって、$n > N$ を満たすすべての自然数 n に対して、

$$|a_n b_n - \alpha\beta| \le |a_n||b_n - \beta| + |a_n - \alpha||\beta| \le M\varepsilon_0 + \varepsilon_0|\beta| = (M + |\beta|)\frac{\varepsilon}{M + |\beta| + 1} < \varepsilon$$

となることがわかる。これで、$\{a_n b_n\}_{n=1}^{\infty}$ は収束し、$\lim_{n\to\infty} a_n b_n = \alpha\beta$ となることが示された。

(3) $\frac{a_n}{b_n} = a_n \cdot \frac{1}{b_n}$ と書けることと (2) から、すべての $n \in \mathbb{N}$ について $b_n \neq 0$、かつ、$\lim_{n\to\infty} b_n = \beta \neq 0$ であるとき、$\lim_{n\to\infty} \frac{1}{b_n} = \frac{1}{\beta}$ となることを証明すればよい。

まず、任意の $n \in \mathbb{N}$ について

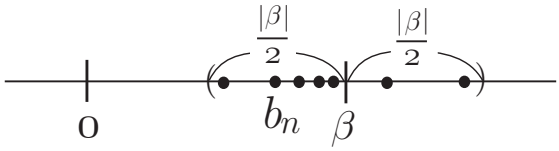
$$\Big|\frac{1}{b_n} - \frac{1}{\beta}\Big| = \frac{|\beta - b_n|}{|\beta||b_n|}$$

が成り立つことに注意する。

さて、任意に $\varepsilon > 0$ をとる。$\lim_{n\to\infty} b_n = \beta \neq 0$ なので、

$$\exists N_1 \in \mathbb{N} \text{ s.t. } n > N_1 \Rightarrow \frac{|\beta|}{2} \le |b_n|$$

が成り立つ。また、$\lim_{n\to\infty} b_n = \beta$ なので、



$\varepsilon_0 := \frac{|\beta|^2\varepsilon}{2} > 0$ に対して、

$$\exists N_2 \in \mathbb{N} \text{ s.t. } n > N_2 \Rightarrow |b_n - \beta| < \varepsilon_0$$

が成り立つ。そこで、(上のような N_1, N_2 を 1 つずつとり、) $N := \max\{N_1, N_2\}$ とおくと、$N \in \mathbb{N}$ であって、$n > N$ を満たすすべての自然数 n に対して、

$$\Big|\frac{1}{b_n} - \frac{1}{\beta}\Big| = \frac{|\beta - b_n|}{|\beta||b_n|} < \frac{2\varepsilon_0}{|\beta|^2} = \varepsilon$$

となることがわかる。これで、$\{\frac{1}{b_n}\}_{n=1}^{\infty}$ は収束し、$\lim_{n\to\infty} \frac{1}{b_n} = \frac{1}{\beta}$ となることが示された。 □

注意：数列 $\{a_n\}_{n=1}^{\infty}$ と実数 c に対して数列 $\{ca_n\}_{n=1}^{\infty}$ を作ることができます。この数列は、$c, c, c, c, \cdots$ という定数列と $\{a_n\}_{n=1}^{\infty}$ との積と考えることができます。したがって、上の命題 (2) の特別な場合として、数列 $\{a_n\}_{n=1}^{\infty}$ が収束するとき、任意の実数 c に対して数列 $\{ca_n\}_{n=1}^{\infty}$ は収束し、

$$\lim_{n\to\infty} ca_n = c \lim_{n\to\infty} a_n$$

が成り立つことがわかります。

演習 8-5* 2 つの数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ が収束するとき、$\{a_n + b_n\}_{n=1}^{\infty}$ も収束して、

$$\lim_{n\to\infty} (a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$$

が成り立つことを示せ。

演習 8-6 上の命題の証明の中の下線部分がなぜ成り立つのか、詳しく説明せよ。

例 8-7　数列 $\{\frac{3n^2-6n+1}{2n^2+5n-4}\}_{n=1}^{\infty}$ は収束することを示し、その極限を求めよ。

解；

まず、$2n^2+5n=4$ となる自然数 n は存在しないから数列 $\{\frac{3n^2-6n+1}{2n^2+5n-4}\}_{n=1}^{\infty}$ を考えることに意味があることに注意する。第 n 項の分子と分母を n^2 で割り、

$$\left\{\frac{3n^2-6n+1}{2n^2+5n-4}\right\}_{n=1}^{\infty} = \left\{\frac{3-\frac{6}{n}+\frac{1}{n^2}}{2+\frac{5}{n}-\frac{4}{n^2}}\right\}_{n=1}^{\infty}$$

と書き換える。ここで、演習 8-3 により $\{\frac{1}{n}\}_{n=1}^{\infty}$ は 0 に収束するから、命題 8-6 により $\{\frac{1}{n^2}\}_{n=1}^{\infty}$ も収束し、$\lim_{n\to\infty}\frac{1}{n^2}=(\lim_{n\to\infty}\frac{1}{n})^2=0$ となる。したがってまた命題 8-6 により $\{3-\frac{6}{n}+\frac{1}{n^2}\}_{n=1}^{\infty}$ と $\{2+\frac{5}{n}-\frac{4}{n^2}\}_{n=1}^{\infty}$ はともに収束し、

$$\lim_{n\to\infty}(3-\frac{6}{n}+\frac{1}{n^2})=3, \qquad \lim_{n\to\infty}(2+\frac{5}{n}-\frac{4}{n^2})=2$$

となる。再度命題 8-6 を用いて、数列 $\{\frac{3n^2-6n+1}{2n^2+5n-4}\}_{n=1}^{\infty}$ は収束し、

$$\lim_{n\to\infty}\frac{3n^2-6n+1}{2n^2+5n-4}=\lim_{n\to\infty}\frac{3-\frac{6}{n}+\frac{1}{n^2}}{2+\frac{5}{n}-\frac{4}{n^2}}=\frac{3}{2}$$

であることがわかる。　□

●はさみうちの原理

与えられた数列が扱いにくくても、それをよくわかっている数列で「上と下からはさみこむ」ことにより、収束することが証明できたり、極限が求められたりするときがあります。

命題 8-8 (はさみうちの原理)

3 つの数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$, $\{x_n\}_{n=1}^{\infty}$ が次の (i)(ii) を満たしているとする。

(i) 任意の $n\in\mathbb{N}$ に対して、$a_n\le x_n\le b_n$.

(ii) $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ はともに $\alpha\in\mathbb{R}$ に収束する.

このとき、$\{x_n\}_{n=1}^{\infty}$ も α に収束する。

(**proof**)

$\lim_{n\to\infty}a_n=\lim_{n\to\infty}b_n=\alpha$ であるから、任意に $\varepsilon>0$ を与えると、

$$\exists N_1\in\mathbb{N} \ \text{ s.t. } \ n>N_1 \ \Rightarrow \ |a_n-\alpha|<\varepsilon$$

$$\exists N_2\in\mathbb{N} \ \text{ s.t. } \ n>N_2 \ \Rightarrow \ |b_n-\alpha|<\varepsilon$$

が成り立つ。そこで、(上のような N_1, N_2 を 1 つずつとり、) $N:=\max\{N_1,N_2\}$ とおくと、$N\in\mathbb{N}$ であって、$n>N$ を満たすすべての自然数 n に対して、

$$\alpha-\varepsilon<a_n\le x_n\le b_n<\alpha+\varepsilon$$

が成り立つことがわかる。よって、$\{x_n\}_{n=1}^{\infty}$ は収束し、その極限は $\lim_{n\to\infty}x_n=\alpha$ である。　□

演習 8-7　2 つの数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ が条件

(i) 任意の $n\in\mathbb{N}$ に対して、$a_n\le b_n$.

(ii) $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ は収束する.

を満たしているとする。このとき、$\lim_{n\to\infty}a_n\le\lim_{n\to\infty}b_n$ となることを示せ。

例 8-9　k を正の実数とする。漸化式 $a_1 = 1,\ a_{n+1} = \frac{1}{2}(a_n + \frac{k}{a_n})$ $(n = 1, 2, \cdots)$ により定義される数列 $\{a_n\}_{n=1}^{\infty}$ は $\sqrt{k}$ に収束する。

解；

例 8-2 と演習 8-4 により与えられた数列は収束する。その極限を α とおく。

例 8-2 の解で示したように、$n \geq 2$ のとき $a_n \geq \sqrt{k}$ であるから、$\alpha \geq \sqrt{k}$ (> 0) が成り立つ (演習 8-7)。α は

$$\alpha = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} \frac{1}{2}(a_n + \frac{k}{a_n}) = \frac{1}{2}(\alpha + \frac{k}{\alpha})$$

を満たすから、これを解いて、$\alpha = \sqrt{k}$ を得る。　□

注意：上の数列は $\sqrt{k}$ の近似値を求めるときに使われます。

定理 8-4、命題 8-6(1)、演習 8-7 を組み合わせることにより、次が成り立つことがわかります。

定理 8-10 (区間縮小法の原理の精密化)

閉区間の減少列

$$I_1 \supset I_2 \supset I_3 \supset \cdots\cdots \supset I_n \supset I_{n+1} \supset \cdots\cdots$$

が与えられているとし、$I_n = [a_n, b_n]$ $(n = 1, 2, 3, \cdots)$ とおくとき、$\lim_{n\to\infty}(b_n - a_n) = 0$ であると仮定する。このとき、すべての I_n $(n = 1, 2, 3, \cdots)$ に共通に含まれる実数が唯一存在し、その実数は $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ によって与えられる。

●実数の連続性の公理の同値性

このプリントでは、

(1) アルキメデスの公理とカントールの公理（区間縮小法の原理）

から出発して、

(2) $\mathbb{R}$ の空でない上に有界な部分集合は上限を持つ (定理 7-9)。

(3) 上に有界な単調増加数列は収束する (定理 8-4)。

という２つの定理を証明しました。実は、(1)(2)(3) は実数の連続性を別の表現を使って言い換えているに過ぎません。実際、第７節の冒頭で挙げた実数の３つの性質だけを使って、(1)(2)(3) の３つが互いに同値であることを証明することができます。したがって、(1) の代わりに (2) や (3) を実数の連続性の公理として採用することもできます。この場合には、(1) は公理ではなく定理になります。連続性の公理と同値な命題は沢山あります。例えば、**デデキントの切断** (Dedekind cut) という概念を使って書かれた次の命題は、そのうちの１つです。

(4)（デデキントの切断）$\mathbb{R}$ を次の性質を持つ２つの空でない部分集合 A, B に分けたとする。

(i) $\mathbb{R} = A \cup B$,　　(ii) 任意の $a \in A$ と任意の $b \in B$ に対して、$a < b$

このとき、A に最大元が存在するか、B に最小元が存在する。

(4) が (1)(2)(3) と同値であることの証明は、田島一郎・著『解析入門』(岩波全書),1981 年等を参照して下さい。

最後に、「(3) ⇒ (1)」の証明を記しておきましょう (「(1) ⇒ (2)」と「(2) ⇒ (3)」はすでに証明済みなので、「(3) ⇒ (1)」を示せば、(1)(2)(3) が互いに同値であることが示されたことになります)。

「(3) $\Longrightarrow$ アルキメデスの公理」の証明

正の実数 a, b に対して、$a < nb$ となる $n \in \mathbb{N}$ が存在することを背理法で示す。

「すべての $n \in \mathbb{N}$ に対して $a \geq nb$」であると仮定する。このとき、数列 $\{nb\}_{n=1}^{\infty}$ は上に有界な単調増加数列である。したがって、仮定により、この数列には極限が存在する。その極限を α とおくと、

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N}\ \text{ s.t. }\ n > N\ \Rightarrow\ |nb - \alpha| < \varepsilon$$

が成り立つ。特に、$\varepsilon = \frac{b}{2}$ (> 0) に対して上のような $N \in \mathbb{N}$ が存在する (ので、そのような N を 1 つとる)。このとき、

$$|(N+1)b - \alpha| < \tfrac{b}{2} \quad \text{かつ} \quad |(N+2)b - \alpha| < \tfrac{b}{2}$$

が成り立つ。これらの右辺同士と左辺同士を加えて、三角不等式を使って、

$$\begin{aligned} b &= |((N+2)b - \alpha) - ((N+1)b - \alpha)| \\ &\leq |(N+2)b - \alpha| + |-(N+1)b + \alpha| < \tfrac{b}{2} + \tfrac{b}{2} = b \end{aligned}$$

を得る。これより、$b < b$ が得られて、矛盾が生じる。よって、$a < nb$ となる $n \in \mathbb{N}$ は存在する。 □

「(3) $\Longrightarrow$ カントールの公理」の証明

閉区間の減少列 $I_1 \supset I_2 \supset I_3 \supset \cdots\cdots$ を任意にとり、各 $n \in \mathbb{N}$ に対して、$I_n = [a_n, b_n]$ $(a_n < b_n)$ とおく。このとき、

$$a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n \leq \cdots \leq b_n \leq \cdots \leq b_3 \leq b_2 \leq b_1$$

となるので、数列 $\{a_n\}_{n=1}^{\infty}$ は上に有界な単調増加数列である。仮定により、極限 $\lim_{n\to\infty} a_n = \alpha$ が存在する。そこで、

$$(*) \qquad \text{任意の } n \in \mathbb{N} \text{ に対して、} a_n \leq \alpha \leq b_n$$

であることを示す（これが示されればカントールの公理が証明されたことになる)。

• 任意の $n \in \mathbb{N}$ に対して、$a_n \leq \alpha$ であること：

ある $N_0 \in \mathbb{N}$ に対して、$a_{N_0} > \alpha$ であったと仮定する。$\lim_{n\to\infty} a_n = \alpha$ であるから、$\varepsilon := a_{N_0} - \alpha$ (> 0) に対して、

$$\exists N \in \mathbb{N}\ \text{ s.t. }\ n > N\ \Rightarrow\ |a_n - \alpha| < \varepsilon = a_{N_0} - \alpha$$

が成り立つ。(そこで、そのような N を 1 つとる。) すると、$n > N$ を満たすすべての $n \in \mathbb{N}$ に対して、$a_n - \alpha \leq |a_n - \alpha| < a_{N_0} - \alpha$、すなわち、$a_n < a_{N_0}$ が成り立つ。特に、$n_0 := \max\{N+1, N_0\}$ に対して、$a_{n_0} < a_{N_0}$ となるが、これは数列 $\{a_n\}_{n=1}^{\infty}$ が単調増加であることに反する。故に、任意の $n \in \mathbb{N}$ に対して、$a_n \leq \alpha$ である。

• 任意の $n \in \mathbb{N}$ に対して、$\alpha \leq b_n$ であること：

ある $N_0 \in \mathbb{N}$ に対して、$\alpha > b_{N_0}$ であったと仮定する。$\lim_{n\to\infty} a_n = \alpha$ であるから、$\varepsilon := \alpha - b_{N_0}$ (> 0) に対して、

$$\exists N \in \mathbb{N}\ \text{ s.t. }\ n > N\ \Rightarrow\ |a_n - \alpha| < \varepsilon = \alpha - b_{N_0}$$

が成り立つ。(そこで、そのような N を 1 つとる。) すると、$n > N$ を満たすすべての $n \in \mathbb{N}$ に対して、$\alpha - a_n \leq |a_n - \alpha| < \alpha - b_{N_0}$、すなわち、$b_{N_0} < a_n$ が成り立つ。特に、$n_0 := \max\{N+1, N_0\}$ に対して、$b_{N_0} < a_{n_0} < b_{n_0}$ となるが、これは数列 $\{b_n\}_{n=1}^{\infty}$ が単調減少であることに反する。故に、任意の $n \in \mathbb{N}$ に対して、$\alpha \leq b_n$ である。 □

§9. 無限級数

高校の微分積分の授業で、$|a|<1$ のとき $\lim_{n\to\infty} a^n = 0$ となることを習いました。ここでは、まず、この事実を数列の収束の定義と実数の連続性に基づいて証明します。次に、無限級数の概念を導入して、その収束・発散の問題をゼータ関数値 $\zeta(2)$ や m 進小数表示、ネイピアの数 e などの具体例を通して考察します。ここでの目標は、数列や級数の収束・発散の問題を、“$\varepsilon - N$ 式”の議論によって扱えるようになることです。

§9-1 数列の発散

収束しない数列は発散していると呼ばれます。ここでは、特に、正の無限大に発散する数列について考察します。まず、前回の復習から始めましょう。

演習 9-1* (1) 数列 $\{a_n\}_{n=1}^{\infty}$ が収束するとはどういうときをいうのか。その定義を、まず、論理記号 $(\forall, \exists, \Rightarrow)$ や lim を使わずに文章で書け。次に、それを論理記号を使って書き直せ。
(2) 数列 $\{a_n\}_{n=1}^{\infty}$ が収束しないとはどういうときをいうのか。その定義を、まず、論理記号 $(\forall, \exists, \Rightarrow)$ や lim を使わずに文章で書け。次に、それを論理記号を使って書き直せ。

定義 9-1

数列 $\{a_n\}_{n=1}^{\infty}$ が**正の無限大 $(+\infty)$ に発散する** (diverge to positive infinity) とは、どのような実数 $K>0$ に対しても、次の条件 $(*)$ を満たす自然数 N が存在するときをいう。

$(*)$ $n>N$ を満たすすべての自然数 n について、$a_n > K$ である。

このことを次のように書き表わす：

$$\lim_{n\to\infty} a_n = +\infty \quad \text{または} \quad a_n \to +\infty \quad (n\to\infty)$$

注意：1. $\{a_n\}_{n=1}^{\infty}$ が $+\infty$ に発散することを、論理記号を使って、

$$\text{「}\forall K>0,\ \exists N\in\mathbb{N}\ \text{ s.t. }\ n>N \ \Rightarrow\ a_n > K\text{」が成り立つ}$$

のように表現します。通常、“ が成り立つ ”の部分は省略します。
2. $\{a_n\}_{n=1}^{\infty}$ が**負の無限大 $(-\infty)$ に発散する**とは、$\{-a_n\}_{n=1}^{\infty}$ が $+\infty$ に発散するときをいいます。このとき、$\lim_{n\to\infty} a_n = -\infty$ と書き表わします。

例 9-2 $a>1$ のとき、$\lim_{n\to\infty} a^n = +\infty$ である。

(**proof**)

$a>1$ だから、$a = 1+h$ $(h>0)$ と書くことができる。このとき、すべての自然数 n に対して、$a^n > nh$ が成り立つ（数学的帰納法による）。

任意に $K>0$ をとると、アルキメデスの公理により、

$$\exists N\in\mathbb{N}\ \text{ s.t. }\ Nh > K$$

が成り立つ。このとき、$n>N$ を満たすすべての自然数 n について

$$a^n > nh > Nh > K$$

となる。よって、$\lim_{n\to\infty} a^n = +\infty$ である。 □

演習 9-2* $|a|<1$ のとき、$\lim_{n\to\infty} a^n = 0$ であることを、例 9-2 を利用して、証明せよ。

ヒント：$a \neq 0$ の場合に、例 9-2 を $\frac{1}{|a|}$ に適用し、“$\varepsilon - N$ 式”の表現を使って書き換えよ。

例 9-3 任意の実数 $a>0$ について、$\lim_{n\to\infty} \dfrac{a^n}{n!} = 0$ である。

(**proof**)

アルキメデスの公理により、

$$\exists N \in \mathbb{N} \ \text{ s.t. } \ \frac{a}{N} < \frac{1}{2}$$

が成り立つ。このとき、$n > N$ を満たす任意の $n \in \mathbb{N}$ に対して、

$$\frac{a^n}{n!} = \frac{\overbrace{a\cdot a\ \cdots\ a}^{n-N+1}}{n\cdot(n-1)\cdots N}\,\frac{\overbrace{a\ \cdots\ a\cdot a}^{N-1}}{(N-1)\cdots 2\cdot 1} < \left(\frac{1}{2}\right)^{n-N+1}\frac{a^{N-1}}{(N-1)!}$$

となる。したがって、演習 9-2 により、

$$\lim_{n\to\infty} \frac{a^n}{n!} = 0$$

を得る。 □

演習 9-3 上の証明における、下線部分「したがって」の理由を詳しく説明せよ（任意に $\varepsilon>0$ が与えられたとき、「$n > N' \ \Rightarrow\ |\frac{a^n}{n!}| < \varepsilon$」をみたす $N' \in \mathbb{N}$ としてどのようなものを取ることができるか、答えよ）。

§9-2 無限級数

数列の各項を $+$ という記号で結び、形式和を考えることにより無限級数の概念が得られます。ここでは、各項が非負の無限級数に関する収束条件を考えます。また、実数の小数表示の意味を説明します。

●無限級数

数列 $\{a_n\}_{n=1}^{\infty}$ に対して、その各項を初項から順番に $+$ という記号でつないで、次のような‘形式和’を考えることができます。

$$a_1 + a_2 + \cdots + a_n + \cdots\cdots$$

この形式和のことを**無限級数** (infinite series)、または、単に、**級数** (series) と呼び、

$$\sum_{n=1}^{\infty} a_n$$

と書き表わします。ここで注意すべきことは、無限級数 $\sum_{n=1}^{\infty} a_n = a_1 + a_2 + \cdots + a_n + \cdots$ における足し算の記号 $+$ あるいは和の記号 $\sum$ は、初項から第 n 項までの和 $\sum_{k=1}^{n} a_k$ とは違って、足し算を実行した結果を表わしているわけではない、ということです。無限級数は無限個の実数を‘$+$ という記号でつないだ単なる式’に過ぎません。この意味では、無限級数 $\sum_{n=1}^{\infty} a_n$ は、数列 $\{a_n\}_{n=1}^{\infty}$ と何ら変わりはありません（表現の仕方を変えただけです）。

例 9-4

(1) 級数 $\sum_{n=1}^{\infty} \frac{1}{n}$ を**調和級数** (harmonic series) という。

(2) 実数 a, r に対して、級数 $\sum_{n=1}^{\infty} ar^{n-1}$ を初項 a、公比 r の (無限) **等比級数**という。

●級数の収束と発散

$\{a_n\}_{n=1}^{\infty}$ を実数列とします。各自然数 n に対して、実数 $S_n := \sum_{k=1}^{n} a_k$ を級数 $\sum_{n=1}^{\infty} a_n$ の**第 n 部分和** (the nth partial sum) といいます。第 n 部分和を第 n 項とする数列 $\{S_n\}_{n=1}^{\infty}$ が収束するとき、級数 $\sum_{n=1}^{\infty} a_n$ は**収束する** (converge) といい、$S := \lim_{n\to\infty} S_n$ を級数 $\sum_{n=1}^{\infty} a_n$ の**和** (sum of the series) といいます。和 S も級数と同じ記号 $\sum_{n=1}^{\infty} a_n$ で書き表わします。このことにより、収束する級数については、$\sum_{n=1}^{\infty} a_n$ という記号は形式和と実数 $\lim_{n\to\infty} S_n$ の 2 つの意味を持つことになります。どちらの意味で使っているのかは、前後の文脈で判断することになります。

級数 $\sum_{n=1}^{\infty} a_n$ が **$+\infty$ に発散する**とは、その第 n 部分和を第 n 項とする数列 $\{S_n\}_{n=1}^{\infty}$ が $+\infty$ に発散するときをいいます。このことを

$$\sum_{n=1}^{\infty} a_n = +\infty$$

と書き表わします。$-\infty$ に発散することも同様に定義し、$\sum_{n=1}^{\infty} a_n = -\infty$ と書き表わします。

例 9-5 無限等比級数 $\sum_{n=1}^{\infty} ar^{n-1}$ は $|r| < 1$ のとき収束し、そのときの和は $\frac{a}{1-r}$ となる。

(**proof**)

各自然数 n について、$S_n := \sum_{k=1}^{n} ar^{k-1}$ とおく。

$r \neq 1$ ならば、$S_n = \frac{a(1-r^n)}{1-r}$ となる。

この式と演習 9-2 から、$|r| < 1$ のとき、$\{S_n\}_{n=1}^{\infty}$ は収束して、

$$\sum_{n=1}^{\infty} ar^{n-1} = \lim_{n\to\infty} S_n = \lim_{n\to\infty} \frac{a(1-r^n)}{1-r} = \frac{a}{1-r}$$

となることがわかる。 □

●正項級数

級数 $\sum_{n=1}^{\infty} a_n$ が**正項級数** (series with nonnegative terms) であるとは、すべての $n \in \mathbb{N}$ について $a_n \geq 0$ であるときをいいます (注：本来は非負項級数と呼ぶべきかもしれませんが、このような呼び方が一般的です)。

正項級数については、収束するか、$+\infty$ に発散するか、のどちらか一方のみが成り立ちます。定理 8-4 により、正項級数 $\sum_{n=1}^{\infty} a_n$ が収束するための必要十分条件は、数列 $\{\sum_{k=1}^{n} a_k\}_{n=1}^{\infty}$ が上に有界になることです。

例 9-6　調和級数 $\sum_{n=1}^{\infty} \frac{1}{n}$ は $+\infty$ に発散する。

(**proof**)

自然数 n に対して、$S_n = \sum_{k=1}^{n} \frac{1}{k}$ とおく。このとき、任意の自然数 m に対して

$$\begin{aligned} S_{2^m} &= \Big(1+\frac{1}{2}\Big) + \Big(\frac{1}{3}+\frac{1}{4}\Big) + \Big(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\Big) + \Big(\frac{1}{9}+\cdots+\frac{1}{16}\Big) + \cdots\cdots \\ &\quad + \Big(\frac{1}{2^{m-1}+1}+\cdots+\frac{1}{2^m}\Big) \\ &> \Big(\frac{1}{2}+\frac{1}{2}\Big) + \Big(\frac{1}{4}+\frac{1}{4}\Big) + \Big(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\Big) + \Big(\frac{1}{16}+\cdots+\frac{1}{16}\Big) + \cdots\cdots \\ &\quad + \Big(\frac{1}{2^m}+\cdots+\frac{1}{2^m}\Big) \\ &= 1+\frac{1}{2}(m-1) \\ &= \frac{m+1}{2} \end{aligned}$$

となる。$\{\frac{m+1}{2}\}_{m=1}^{\infty}$ は $+\infty$ に発散するから、任意の $K>0$ に対して、

$$\exists N \in \mathbb{N} \ \text{ s.t. } \ m > N \ \Rightarrow \ S_{2^m} > K$$

となる。したがって、$\{S_n\}_{n=1}^{\infty}$ も $+\infty$ に発散する。　□

演習 9-4* 上の証明における、下線部分「したがって」の理由を詳しく説明せよ（任意に $K>0$ が与えられたとき、「$n > N' \ \Rightarrow \ S_n > K$」をみたす $N' \in \mathbb{N}$ としてどのようなものを取ることができるか、答えよ）。

演習 9-5　正項級数 $\sum_{n=1}^{\infty} \frac{1}{n^2} = 1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots$ は収束することを示せ。

ヒント：まず、$n \geq 2$ に対して $\sum_{k=2}^{n} \frac{1}{(k-1)k}$ を計算し、その値が 1 より小さいことを示せ。次に、これを用いて、数列 $\big\{\sum_{k=1}^{n} \frac{1}{k^2}\big\}_{n=1}^{\infty}$ が上に有界であることを示せ。

注意：一般に、2 以上の自然数 k について、無限級数 $\sum_{n=1}^{\infty} \frac{1}{n^k}$ は収束します。その和を $\zeta(k)$ と書きます。ちなみに、$\zeta(2) = \pi^2/6 = 1.644934066848226.....$ となります。

●実数の m 進小数表示

ここでは、$1/2 = 0.5$, $\sqrt{2} = 1.41421356.....$, $\pi = 3.14159265.....$ のような、実数の小数表示の正確な意味を説明します。

m を 2 以上の整数とします。$x \in [0,1]$ が次の形の無限級数の和

$$(\diamondsuit) \qquad x = \sum_{i=1}^{\infty} \frac{a_i}{m^i} \qquad (a_i \in \{0,1,\cdots,m-1\})$$

で表わされるとき、$x = [0.a_1a_2a_3\cdots]_m$ と書き、この表示を x の (無限) m **進小数表示**と呼びます。特に、$m=10$ のときは、単に $x = 0.a_1a_2a_3\cdots$ のように書き表わします。

例 9-7　$1 = [0.\ m{-}1\ m{-}1\ m{-}1\ \cdots\cdots]_m$ である。特に、$1 = 0.999\cdots\cdots$ と表わされる。

実際、

$$\sum_{i=1}^{\infty} \frac{m-1}{m^i} = (m-1)\sum_{i=1}^{\infty} \frac{1}{m^i} = (m-1)\frac{\frac{1}{m}}{1-\frac{1}{m}} = 1$$

となるからである。　□

命題 9-8

m を 2 以上の整数とするとき、任意の $x \in [0,1]$ は m 進小数表示を持つ。

(**proof**)

$x = 1$ が m 進小数表示を持つことは例 9-7 で示されているから、$x \in [0,1)$ が m 進小数表示を持つことを示す。

$x \in [0,1)$ とする。$mx \in [0,m)$ であるから、$a_1 \leq mx < a_1+1$ を満たす $a_1 \in \{0,1,\cdots,m-1\}$ が唯一存在する (補題 7-2)。このとき、$x_1 := mx - a_1$ とおくと、$x_1 \in [0,1)$ となる。今の操作を x_1 に対して行うことにより、$a_2 \leq mx_1 < a_2+1$ を満たす $a_2 \in \{0,1,\cdots,m-1\}$ が唯一存在し、$x_2 := mx_1 - a_2 \in [0,1)$ となる。以下同様にして、$\{0,1,\cdots,m-1\}$ の元からなる数列 $\{a_n\}_{n=1}^{\infty}$ と $[0,1)$ の元からなる数列 $\{x_n\}_{n=1}^{\infty}$ であって、$x_n = mx_{n-1} - a_n$ $(n = 1,2,\cdots)$ を満たすものを構成することができる。但し、$x_0 := x$ とおく。このとき、$n = 1,2,\cdots$ に対して、

$$x = \frac{a_1}{m} + \frac{x_1}{m} = \frac{a_1}{m} + \frac{a_2}{m^2} + \frac{x_2}{m^2} = \cdots\cdots = \frac{a_1}{m} + \frac{a_2}{m^2} + \cdots + \frac{a_n}{m^n} + \frac{x_n}{m^n}$$

となることがわかる。したがって、

$$\left|x - \sum_{i=1}^{n} \frac{a_i}{m^i}\right| = \frac{x_n}{m^n} < \frac{1}{m^n}$$

が成り立つ。$m \geq 2$ なので $\{\frac{1}{m^n}\}_{n=1}^{\infty}$ は 0 に収束する (演習 9-2)。よって、任意の $\varepsilon > 0$ に対して、「$n > N \ \Rightarrow\ \frac{1}{m^n} < \varepsilon$」となる $N \in \mathbb{N}$ が存在する。このとき、上で得られた不等式と合わせて、

$$n > N \text{ となるすべての } n \in \mathbb{N} \text{ に対して } \left|x - \sum_{i=1}^{n} \frac{a_i}{m^i}\right| < \varepsilon$$

がわかる。故に、x は $x = \sum_{n=1}^{\infty} \frac{a_n}{m^n}$ という表示を持つ。　□

演習 9-6　(◇) の形の無限級数は収束し、その和は $[0,1]$ に属することを示せ。

一般に、1 以上の正の実数 x は次の形の無限級数で表わされます。

(◆)　　$$x = \sum_{i=0}^{k} r_i m^i + \sum_{i=1}^{\infty} \frac{a_i}{m^i} \qquad (r_i, a_i \in \{0,1,\cdots,m-1\},\ k \geq 0,\ r_k \neq 0).$$

例えば、$n \leq x < n+1$ を満たす自然数 n をとり、$x - n \in [0,1)$ に命題 9-8 を適用し、n を例 6-8 のように m 進記数表示すれば、上のような表示を得ることができます。

x が (◆) のように表わされるとき、$x = [r_k r_{k-1}\cdots r_0.a_1a_2a_3\cdots\cdots]_m$ と書いて、これを $x \in [0,\infty)$ の (無限) m 進小数表示と呼びます。$m = 10$ のときには、単に $r_k r_{k-1}\cdots r_0.a_1a_2a_3\cdots\cdots$ のように書き表します。

●有限 m 進数

$x \in (0,\infty)$ が

$$\exists N \in \mathbb{N} \ \text{ s.t. } \ n > N \ \Rightarrow \ a_n = 0$$

となるような m 進小数表示 $x = [r_k r_{k-1} \cdots r_0 . a_1 a_2 a_3 \cdots]_m$ を持つとき、x は**有限 m 進数**であるといいます。例えば、自然数は有限 m 進数です。また、1/2 や 1/5 は有限 10 進数です。

m 進小数表示は一意的ではありませんが、次の命題で述べられているように、表示が一意的でないものは有限 m 進数に限られ、しかも、その表示の仕方は２通りしかありません。

命題 9-9

m を 2 以上の整数とする。

$x \in (0,\infty)$ の m 進小数表示が一意的でないための必要十分条件は、x が有限 m 進数であることであり、このとき、x の m 進小数表示はちょうど２通りある。

(**proof**)

最初に $x \in (0,1)$ の場合に証明する。

x が相異なる m 進小数表示 $x = [0.a_1 a_2 a_3 \cdots]_m = [0.b_1 b_2 b_3 \cdots]_m$ を持つとすると、

$$x = \sum_{i=1}^{\infty} \frac{a_i}{m^i} = \sum_{i=1}^{\infty} \frac{b_i}{m^i}$$

が成り立つ。一般性を失うことなく、$a_1 = b_1, \cdots, a_{p-1} = b_{p-1},\ a_p > b_p$ と仮定してよい。このとき、

$$\frac{a_p}{m^p} \le \frac{a_p}{m^p} + \sum_{i=p+1}^{\infty} \frac{a_i}{m^i} = \frac{b_p}{m^p} + \sum_{i=p+1}^{\infty} \frac{b_i}{m^i} \le \frac{b_p}{m^p} + \sum_{i=p+1}^{\infty} \frac{m-1}{m^i} = \frac{b_p}{m^p} + \frac{1}{m^p}$$

となるので、$a_p \le b_p + 1$、したがって、$b_p < a_p \le b_p + 1$ を得るが、$a_p, b_p \in \mathbb{Z}$ であるから、$a_p = b_p + 1$ でなければいけない。よって、上の不等式から、

$$\sum_{i=p+1}^{\infty} \frac{a_i}{m^i} = 0, \quad \sum_{i=p+1}^{\infty} \frac{b_i}{m^i} = \frac{1}{m^p}$$

を得る。この２式から、

$$\begin{cases} \bullet \text{ すべての } i \ge p+1 \text{ について } a_i = 0 \text{ であり} \\ \bullet \text{ すべての } i \ge p+1 \text{ について } b_i = m-1 \text{ である} \end{cases}$$

ことがわかる。(証明は背理法による。例えば２番目の主張を示すには、ある $q \in \mathbb{N}$ に対して $b_{p+1} = \cdots = b_{p+q-1} = m-1,\ b_{p+q} < m-1$ であると仮定して矛盾を導く。)

以上より、$x \in (0,1)$ が相異なる m 進小数表示 $x = [0.a_1 a_2 a_3 \cdots]_m = [0.b_1 b_2 b_3 \cdots]_m$ を持てば、ある $p \in \mathbb{N}$ が存在して、

$$a_i = b_i \ (i = 1, \cdots, p-1),\ a_p = b_p + 1,\ a_j = 0,\ b_j = m-1 \ (j = p+1, p+2, \cdots)$$

または

$$a_i = b_i \ (i = 1, \cdots, p-1),\ b_p = a_p + 1,\ a_j = m-1,\ b_j = 0 \ (j = p+1, p+2, \cdots)$$

となることがわかった。よって、x は有限 m 進数であり、x の m 進小数表示は

$x = [0.a_1 a_2 \cdots a_p 00 \cdots\cdots]_m$ と $x = [0.a_1 a_2 \cdots\ a_p{-}1\ m{-}1\ m{-}1\ \cdots\cdots]_m$（但し、$a_p \ne 0$）

の２通りのみである。

次に、$x \ge 1$ の場合を考える。

x が相異なる m 進小数表示 $x = [r_k r_{k-1} \cdots r_0 . a_1 a_2 a_3 \cdots\cdots]_m = [s_l s_{l-1} \cdots s_0 . b_1 b_2 b_3 \cdots\cdots]_m$ を持っているとする。$m^k \le x$ かつ $m^l \le x$ となる。

$x < m^c$ を満たす $c \in \mathbb{N}$ を 1 つ固定する。$\frac{x}{m^c} \in (0,1)$ であり、$x' := \frac{x}{m^c}$ は 2 通りの m 進小数表示

$$x' = [0.\overbrace{0\cdots\cdots0}^{c-k-1} r_k r_{k-1}\cdots r_0 a_1 a_2 a_3 \cdots\cdots]_m = [0.\overbrace{0\cdots\cdots0}^{c-l-1} s_l s_{l-1}\cdots s_0 b_1 b_2 b_3 \cdots\cdots]_m$$

を持つ。先に証明したことにより、x' は有限 m 進数であり、$s_l, s_{l-1}, \cdots, s_0,\ b_1, b_2, b_3, \cdots$ は $r_k, r_{k-1}, \cdots, r_0, a_1, a_2, a_3, \cdots$ によって決まる。したがってまた、x も有限 m 進数であって、その m 進小数表示は 2 通りしかない。

逆に、$x \in (0,\infty)$ を有限 m 進数とすると、x は

$$x = [a_{-k}a_{-(k-1)}\cdots a_0.a_1a_2\cdots a_p000\cdots\cdots]_m$$
$$(\text{但し、} a_i \in \{0,1,\cdots,m-1\} \quad (i = -k, -(k-1), \cdots, 0, 1, \cdots, p))$$

という m 進小数表示を持つ。$x \neq 0$ より、$a_{-k}, a_{-(k-1)}, \cdots, a_0, a_1, a_2, \cdots, a_p$ のうち 0 でないものが存在する。$a_i \neq 0$ であるような i のうち最大のものを改めて p とおく。このとき、x は

$$x = [a_{-k}\cdots a_0.a_1a_2\cdots\ a_p{-}1\ m{-}1\ m{-}1\ m{-}1\ \cdots\cdots]_m \text{ あるいは}$$
$$x = [a_{-k}\cdots\ a_p{-}1\ m{-}1\ \cdots\ m{-}1\ .\ m{-}1\ m{-}1\ \cdots\cdots]_m$$

のようにも表わすことができる。よって、有限 m 進数の表示は一意的でない。 □

例 9-10 1 の 10 進数表示は $1 = 1.000\cdots\cdots$ と $1 = 0.99999\cdots\cdots$ の 2 通りしかない。また、1/3 は有限 10 進数ではない。なぜならば、有限 10 進数の無限 10 進数表示はある桁から先がすべて 0 であるかすべて 9 になっていなければならないからである。

§9-3 ネイピアの数

自然対数の底 2.718281828459..... を e という記号で表わした人物は、Euler (1707–1783) ですが、この数 e は、対数の発見者 Napier (1550–1617) の名前に因んで、ネイピアの数と呼ばれています。ここでは、ネイピアの数を実数の連続性に基づいて定義します。

●二項係数

0 以上の整数 n と、$0 \leq r \leq n$ を満たす整数 r に対して、

$$\binom{n}{r} := \frac{n!}{r!(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}$$

と定め、これを**二項係数** (binomial coefficient) と呼びます。これは、高校の教科書で、${}_nC_r$ という記号で書かれているものと同じですが、大学では上記のような書き方が一般的です。二項係数 $\binom{n}{r}$ は、式 $(x+y)^n$ を展開したときの、$x^r y^{n-r}$ の係数になっています。すなわち、

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}\ .$$

●ネイピアの数

例 9-11 自然数 n に対して、

$$a_n = \left(1 + \frac{1}{n}\right)^n, \quad b_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$$

とおき、数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ を考える。この 2 つの数列はともに収束し、かつ、その極限は同じである。この極限を e と書き、**ネイピアの数** (Napierian number) と呼ぶ。

(**proof**)

次の順番で示す。

① $\{b_n\}_{n=1}^{\infty}$ は収束する。

② $a_n < a_{n+1}$ および $a_n \leq b_n$ が成り立つ。したがって、$\{a_n\}_{n=1}^{\infty}$ は収束する。

③ 任意の $n \in \mathbb{N}$ に対して $\lim_{m\to\infty} a_m \geq b_n$ が成り立つ。

①の証明：自然数 k に対して $k! \geq 2^{k-1}$ である (演習 6-2) から、任意の $n \in \mathbb{N}$ に対して

$$b_n = 1 + \sum_{k=1}^{n} \frac{1}{k!} \leq 1 + \sum_{k=1}^{n} \Big(\frac{1}{2}\Big)^{k-1} = 1 + 2\Big(1 - \frac{1}{2^n}\Big) < 3$$

を得る。故に、数列 $\{b_n\}_{n=1}^{\infty}$ は上に有界である。また、数列 $\{b_n\}_{n=1}^{\infty}$ は単調増加列である。よって、$\{b_n\}_{n=1}^{\infty}$ は収束する。

②の証明：$n \in \mathbb{N}$ に対して

$$\begin{aligned}
a_n &= \Big(1 + \frac{1}{n}\Big)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} \Big(\frac{1}{n}\Big)^k \\
&= 1 + \sum_{k=1}^{n} \frac{1}{k!} \cdot \frac{n-k+1}{n} \cdot \frac{n-k+2}{n} \cdots \frac{n-1}{n} \cdot \frac{n}{n} \\
&= 1 + \sum_{k=1}^{n} \frac{1}{k!} \Big(1 - \frac{k-1}{n}\Big)\Big(1 - \frac{k-2}{n}\Big) \cdots \Big(1 - \frac{1}{n}\Big)\Big(1 - \frac{0}{n}\Big) \\
&\leq 1 + \sum_{k=1}^{n} \frac{1}{k!} \Big(1 - \frac{k-1}{n+1}\Big)\Big(1 - \frac{k-2}{n+1}\Big) \cdots \Big(1 - \frac{1}{n+1}\Big)\Big(1 - \frac{0}{n+1}\Big) \\
&= \sum_{k=0}^{n} \binom{n+1}{k} \Big(\frac{1}{n+1}\Big)^k \\
&< \sum_{k=0}^{n+1} \binom{n+1}{k} \Big(\frac{1}{n+1}\Big)^k = \Big(1 + \frac{1}{n+1}\Big)^{n+1} \\
&= a_{n+1}
\end{aligned}$$

となる。また、

$$a_n = 1 + \sum_{k=1}^{n} \frac{1}{k!} \Big(1 - \frac{k-1}{n}\Big)\Big(1 - \frac{k-2}{n}\Big) \cdots \Big(1 - \frac{1}{n}\Big)\Big(1 - \frac{0}{n}\Big) \leq 1 + \sum_{k=1}^{n} \frac{1}{k!} = b_n$$

となる。したがって、$\{a_n\}_{n=1}^{\infty}$ は上に有界な単調増加列なので収束する。

③の証明は演習問題として残す。

証明を完成させるために、$\alpha := \lim_{n\to\infty} a_n$, $\beta := \lim_{n\to\infty} b_n$ とおく。③により、$\alpha \geq \beta$ となる。一方、②により $a_n \leq b_n$ であるから、$\alpha = \lim_{n\to\infty} a_n \leq \lim_{n\to\infty} b_n = \beta$ となる。故に、$\alpha = \beta$ を得る。 □

演習 9-7 $m > n$ のとき、$a_m \geq 1 + \sum_{k=1}^{n} \frac{1}{k!}\big(1 - \frac{k-1}{m}\big)\big(1 - \frac{k-2}{m}\big) \cdots \big(1 - \frac{1}{m}\big)\big(1 - \frac{0}{m}\big)$ が成り立つことに注意し、例 9-11 の証明における③を証明せよ。

§10. 和と積の記号

n 個の実数 $a_1, \cdots, a_n$ の和を第 6 節では $\sum_{i=1}^{n} a_i$ で表わしましたが、この和を n 以下の自然数からなる集合 $I = \{1, \cdots, n\}$ を用いて、$\sum_{i \in I} a_i$ と書き表わすこともできます。ここでは、この和の記号に込められている意味について考えます。そのための準備として、最初に、二項演算について勉強します。

§10-1 二項演算

実数の加法や乗法の持つ性質に結合法則や交換法則がありますが、ここでは少し、これらの性質を抽象的な立場から眺めます。

●二項演算

S を空でない集合とします。このとき、直積集合 $S \times S$ の各元 (a, b) に対して、S のある 1 つの元を対応させる規則のことを S 上の**二項演算** (binary operation) といいます。

例 10-1

(1) 各 $(a, b) \in \mathbb{R} \times \mathbb{R}$ に対して積 ab を対応させる規則は、$\mathbb{R}$ 上の二項演算である。
(2) 各 $(a, b) \in \mathbb{R} \times \mathbb{R}$ に対して和 $a + b$ を対応させる規則は、$\mathbb{R}$ 上の二項演算である。
(3) 各 $(a, b) \in \mathbb{R} \times \mathbb{R}$ に対して差 $a - b$ を対応させる規則は、$\mathbb{R}$ 上の二項演算である。
(4) X を集合として、その部分集合全体からなる集合 $\mathcal{P}(X)$ を考える。このとき、
  (a) 各 $(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X)$ に対して和集合 $A \cup B$ を対応させる規則は、$\mathcal{P}(X)$ 上の二項演算である。
  (b) 各 $(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X)$ に対して共通集合 $A \cap B$ を対応させる規則は、$\mathcal{P}(X)$ 上の二項演算である。

集合 S $(\neq \varnothing)$ 上に二項演算 $*$ が与えられたとすると、各 $(a, b) \in S \times S$ に対応して S の元が定まります。この元を $a * b$ と書き表わすことにします。$S \times S$ の元 (a, b) に S の元 $a * b$ を対応させることを a と b に二項演算 $*$ を施すといいます。

●結合法則

集合 S $(\neq \varnothing)$ 上に二項演算 $*$ が与えられているとします。S から元 a, b, c をとったとき、この並び方を変えないで二項演算 $*$ を施す方法は

・a と b に二項演算を施してから、$a * b$ と c に二項演算を施す方法
・b と c に二項演算を施してから、a と $b * c$ に二項演算を施す方法

の 2 通りがあります。前者の方法により得られる S の元を $(a * b) * c$ と書き、後者の方法により得られる S の元を $a * (b * c)$ と書きます。一般には、$(a * b) * c$ と $a * (b * c)$ が一致するとは限りませんが、すべての $a, b, c \in S$ について、

$$(a * b) * c = a * (b * c)$$

となるとき、与えらた二項演算は**結合法則** (associative law) を満たすといいます。

例 10-2

(1) $\mathbb{R}$ 上の二項演算を実数の積または和によって定義するとき、その二項演算は結合法則を満たす。一方、実数の差によって二項演算を定義するとき、これは結合法則を満たさない。実際、$(2-1)-2=-1\neq 3=2-(1-2)$ である。

(2) X を集合とする。このとき、$\mathcal{P}(X)$ 上の二項演算として部分集合の和をとる操作および共通部分をとる操作を考えるとき、それらは結合法則を満たす。

演習 10-1 * 集合 S $(\neq\varnothing)$ 上に結合法則を満たす二項演算 $*$ が与えられているとする。S から元 a,b,c,d をとったとき、この並び方を変えないで二項演算 $*$ を施す方法（括弧の付け方）をすべて書き、これらの方法で得られる S の元はすべて等しいことを証明せよ。

定理 10-3

集合 S $(\neq\varnothing)$ 上に結合法則を満たす二項演算 $*$ が与えられているとする。このとき、S から有限個の元を（重複も許して）任意にとって横一列に並べ、これらに二項演算 $*$ を何回か施して S の元を対応させるとき、途中で元の並べ方を変えなければ、括弧をどのように付けて計算しても、得られる S の元はすべて等しい。

(**proof**)

すべての $n\in\mathbb{N}$ について、次の条件 $P(n)$ が成り立つことを数学的帰納法で証明する。

$$P(n):\begin{cases} S \text{ から元を } n \text{ 個任意にとって横一列に並べ、これらに二項演算 } * \text{ を何回} \\ \text{か施して } S \text{ の元を対応させるとき、途中で元の並べ方を変えなければ、} \\ \text{括弧をどのように付けて計算しても、得られる } S \text{ の元はすべて等しい。} \end{cases}$$

I. $n=3$ のとき：二項演算 $*$ は結合法則を満たしているので、$P(3)$ は成り立つ。

II. $n>3$ とし、$3\leq k<n$ を満たすすべての自然数 k について、$P(k)$ は成り立つと仮定する。

$a_1,\cdots,a_n\in S$ を任意にとる。この並べ方を崩さずに二項演算 $*$ を何回か施したものは、ある $r\in\{1,\cdots,n-1\}$ によって

$$(a_1*\cdots*a_r)*(a_{r+1}*\cdots*a_n)$$

の形をしている。ここで、$a_1*\cdots*a_r$ と $a_{r+1}*\cdots*a_n$ は、それぞれ $a_1,\cdots,a_r$ と $a_{r+1},\cdots,a_n$ を並べ方を崩さずに二項演算 $*$ を何回か施して得られる S の元を表わしている（帰納法の仮定によって、これらは括弧の付け方によらずに定まっていることに注意）。このとき、$r\geq 2$ について

$$\begin{aligned}(a_1*\cdots*a_r)*(a_{r+1}*\cdots*a_n)&=(a_1*(a_2*\cdots*a_r))*(a_{r+1}*\cdots*a_n)\\&=a_1*((a_2*\cdots*a_r)*(a_{r+1}*\cdots*a_n))\\&=a_1*(a_2*\cdots*a_n)\end{aligned}$$

となる。よって、$P(n)$ も成り立つ。

I と II によって、帰納法は完成し、定理は証明された。 □

●交換法則

集合 S $(\neq\varnothing)$ 上に二項演算 $*$ が与えられているとします。一般には、$a*b$ と $b*a$ が一致するとは限りませんが、すべての $a,b\in S$ について、

$$a*b=b*a$$

となるとき、与えられた二項演算は**交換法則** (commutative law) を満たすといいます。

例 10-4

(1) $\mathbb{R}$ 上の二項演算を実数の積または和によって定義するとき、その二項演算は交換法則を満たす。一方、実数の差によって $\mathbb{R}$ 上の二項演算を定義するとき、それは交換法則を満たさない。実際、$2-1=1\neq -1=1-2$ である。

(2) X を集合とする。このとき、$\mathcal{P}(X)$ 上の二項演算として部分集合の和をとる操作および共通部分をとる操作を考えるとき、それらは交換法則を満たす。

例 10-5 集合 $S\ (\neq\varnothing)$ 上に結合法則と交換法則を満たす二項演算 $*$ が与えられているとする。S から元 a,b,c をとり、これらに何回か二項演算 $*$ を施して S の元を対応させるとき、途中で元の並べ方を変えることも許し、括弧をどのように付けて計算しても、得られる S の元はすべて等しい。

(**proof**)

$a,b,c\in S$ の並べ方は次の 6 種類ある。

$$\text{①}\ a,b,c\quad \text{②}\ a,c,b\quad \text{③}\ b,a,c\quad \text{④}\ b,c,a\quad \text{⑤}\ c,a,b\quad \text{⑥}\ c,b,a$$

①から⑥までの各並べ方において、その並べ方を変えなければ、結合法則によって、どのような括弧の付け方をしても、得られる S の元は等しい。すなわち、

$$\text{①}'\ (a*b)*c=a*(b*c)\qquad \text{②}'\ (a*c)*b=a*(c*b)$$
$$\text{③}'\ (b*a)*c=b*(a*c)\qquad \text{④}'\ (b*c)*a=b*(c*a)$$
$$\text{⑤}'\ (c*a)*b=c*(a*b)\qquad \text{⑥}'\ (c*b)*a=c*(b*a)$$

となる。ここで、交換法則により、

$$(\text{②}'\text{の右辺})=(\text{①}'\text{の右辺}),\qquad (\text{③}'\text{の左辺})=(\text{①}'\text{の左辺})$$
$$(\text{④}'\text{の右辺})=(\text{③}'\text{の右辺}),\qquad (\text{⑤}'\text{の左辺})=(\text{②}'\text{の左辺})$$
$$(\text{⑥}'\text{の左辺})=(\text{④}'\text{の左辺})$$

となるので、$a,b,c\in S$ に何回か二項演算 $*$ を施して S の元を対応させるときに、途中で元の並べ方を変えることを許し、括弧をどのように付けて計算しても、得られる S の元はすべて等しい。 □

演習 10-2 集合 $S\ (\neq\varnothing)$ 上に結合法則と交換法則を満たす二項演算 $*$ が与えられているとする。S から元 a,b,c,d をとり、これらに何回か二項演算 $*$ を施して S の元を対応させるとき、途中で元の並べ方を変えることを許し、括弧をどのように付けて計算しても、得られる S の元はすべて等しいことを証明せよ。

より一般に、次の定理が成り立ちます。

定理 10-6

集合 $S\ (\neq\varnothing)$ 上に結合法則と交換法則を満たす二項演算 $*$ が与えられているとする。このとき、S から有限個の元を（重複も許して）任意にとって横一列に並べ、これらに二項演算 $*$ を何回か施して S の元を対応させるとき、途中で元の順番を変えることも許し、括弧をどのように付けて計算しても、得られる S の元はすべて等しい。

(**proof**)

定理 10-3 と同様に、すべての $n \in \mathbb{N}$ について、次の $P(n)$ が成り立つことを数学的帰納法で証明する。

$$P(n):\begin{cases} S \text{ から元を } n \text{ 個任意にとって横一列に並べ、これらに二項演算 } * \text{ を何回} \\ \text{か施して } S \text{ の元を対応させるとき、途中で元の順番を変えることを許し、} \\ \text{括弧をどのように付けて計算しても、得られる } S \text{ の元はすべて等しい。} \end{cases}$$

I. $n = 3$ のとき：例 10-5 により、$P(3)$ は成り立つ。

Ⅱ. $n > 3$ とし、$3 \leq k < n$ を満たすすべての自然数 k について、$P(k)$ は成り立つと仮定する。

$a_1, \cdots, a_n \in S$ を任意にとる。並べ方の順番を変えることも許しながら、二項演算 $*$ を何回か施したものは、ある $r \in \{1, \cdots, n-1\}$ および $1, \cdots, n$ のある順列 $i_1, \cdots, i_n$ について

$$(a_{i_1} * \cdots * a_{i_r}) * (a_{i_{r+1}} * \cdots * a_{i_n})$$

という形をしている。ここで、$a_{i_1} * \cdots * a_{i_r}$ と $a_{i_{r+1}} * \cdots * a_{i_n}$ は、それぞれ $a_{i_1}, \cdots, a_{i_r}$ と $a_{i_{r+1}}, \cdots, a_{i_n}$ に（元の並び方の順番を変えることを許して）二項演算 $*$ を施して得られる S の元を表わしている（帰納法の仮定によって、これらは括弧の付け方や元の順番の入れ換えによらずに定まっていることに注意）。定理 10-3 の証明と同様にして、

$$(a_{i_1} * \cdots * a_{i_r}) * (a_{i_{r+1}} * \cdots * a_{i_n}) = a_{i_1} * (a_{i_2} * \cdots * a_{i_n})$$

となることがわかる。

Case 1. $i_1 = 1$ の場合：

この場合には、帰納法の仮定により $a_{i_2} * \cdots * a_{i_n} = a_2 * \cdots * a_n$ となるので、

$$(a_{i_1} * \cdots * a_{i_r}) * (a_{i_{r+1}} * \cdots * a_{i_n}) = a_1 * (a_2 * \cdots * a_n)$$

が成り立つ。

Case 2. $i_1 \neq 1$ の場合：

$i_2, \cdots, i_n$ を小さい順に並べ変えたものを $j_2 = 1,\ j_3, \cdots, j_n$ とおくと、帰納法の仮定により $a_{i_2} * \cdots * a_{i_n} = a_1 * a_{j_3} * \cdots * a_{j_n}$ となる。このとき、

$$\begin{aligned} a_{i_1} * (a_{i_2} * \cdots * a_{i_n}) &= a_{i_1} * (a_1 * a_{j_3} * \cdots * a_{j_n}) \\ &= a_{i_1} * (a_1 * (a_{j_3} * \cdots * a_{j_n})) \\ &= (a_{i_1} * a_1) * (a_{j_3} * \cdots * a_{j_n}) \qquad \text{(結合法則)} \\ &= (a_1 * a_{i_1}) * (a_{j_3} * \cdots * a_{j_n}) \qquad \text{(交換法則)} \\ &= a_1 * (a_{i_1} * (a_{j_3} * \cdots * a_{j_n})) \qquad \text{(結合法則)} \\ &= a_1 * (a_{i_1} * a_{j_3} * \cdots * a_{j_n}) \\ &= a_1 * (a_2 * \cdots * a_n) \qquad (\because \text{Case 1}) \end{aligned}$$

となる。よって、

$$(a_{i_1} * \cdots * a_{i_r}) * (a_{i_{r+1}} * \cdots * a_{i_n}) = a_1 * (a_2 * \cdots * a_n)$$

が成り立つ。

Case 1、Case 2 のいずれの場合にも $(a_{i_1} * \cdots * a_{i_r}) * (a_{i_{r+1}} * \cdots * a_{i_n})$ は $a_1 * (a_2 * \cdots * a_n)$ に等しいから、$P(n)$ も成り立つことが示された。

I と Ⅱ によって、帰納法は完成し、定理は証明された。 □

§10-2 和と積の記号

有限個の実数についての和と積はそれぞれ $\sum$, $\prod$ という記号を使って表わされます。記号 $\sum$, $\prod$ は、それぞれ、和、積を意味する英語 summation, product の頭文字 S, P に対応するギリシア文字から作られています。ここでは、和の記号 $\sum$ と積の記号 $\prod$ に込められている意味とこれらの記号の使い方について学びます。

●積の記号

n 個の実数 $a_1, \cdots, a_n$ が与えられたとき、a_1 に a_2 を加え、得られた数 $a_1 + a_2$ に a_3 を加え $\cdots$ というように、a_1 から a_n まで順番に和をとることにより得られる実数を $\sum_{i=1}^{n} a_i$ で表わすのでした（第 6 節参照）。これと同様に、a_1 から a_n まで順番に積をとることにより得られる実数 $a_1 a_2 \cdots a_n$ を

$$\prod_{i=1}^{n} a_i$$

という記号で表わします。実数 $\prod_{i=1}^{n} a_i$ は、

$$\prod_{i=1}^{1} a_i = a_1, \quad 2 \leq k \leq n \text{ に対して } \prod_{i=1}^{k} a_i = \Big(\prod_{i=1}^{k-1} a_i\Big) a_k$$

によって帰納的に定義されています。

例 10-7 自然数 n に対して、n の階乗 $n!$ は $n! = \prod_{i=1}^{n} i$ と表わすことができる。

また、実数 a に対して、a の n 乗は $a^n = \prod_{i=1}^{n} a$ と表わすことができる。

● $\sum$ 記号・$\prod$ 記号の意味と使い方

有限集合（= 元の個数が有限個であるような集合）I の各元 i に対して、実数 a_i が 1 つ定められているとします。このとき、I のすべての元 i にわたって a_i たちの和をとることにより、1 つの実数が得られます。この実数を、記号

$$\sum_{i \in I} a_i$$

で表わします。同様に、I のすべての元 i にわたって a_i たちの積をとることにより得られる実数を、記号

$$\prod_{i \in I} a_i$$

で表わします。

演習 10-3 * $\sum_{i \in I} a_i$ や $\prod_{i \in I} a_i$ ような記号の使い方が許される根拠は何か？ 記号 $\sum_{i \in I} a_i$ と $\prod_{i \in I} a_i$ に対する上で述べた説明の不十分なところを指摘して、その根拠を述べよ。

例 10-8 m を自然数とし、$I = \{\, d \in \mathbb{N} \mid d \text{ は } m \text{ の約数} \,\}$ とおく。各 $d \in I$ に対して、1 から d までの自然数の中で d と互いに素なものの個数を $\varphi(d)$ とおくと、

$$m = \sum_{d \in I} \varphi(d)$$

が成り立つ (m を具体的に与えて確かめてみて下さい)。

有限個の実数についての和や積を書くときは、上で記したように書くことが基本ですが、誤解が生じない範囲内で、$\sum$ 記号や $\prod$ 記号の下の記述を変更することができます。例えば、例 10-8 の等式の右辺はしばしば $\sum_{d|m} \varphi(d)$ のように書かれます ($d|m$ は d が m の約数であることを表わす記号です)。ここで、よく使われる書き方を紹介しておきます。

① n を自然数とします。$I = \{1, \cdots, n\}$ のとき、和 $\sum_{i \in I} a_i$ および積 $\prod_{i \in I} a_i$ をそれぞれ

$$\sum_{1 \le i \le n} a_i \qquad \text{および} \qquad \prod_{1 \le i \le n} a_i$$

のようにも書きます。これらはそれぞれ $\sum_{i=1}^{n} a_i$, $\prod_{i=1}^{n} a_i$ と同じ実数を表わします。

例 10-9 $\displaystyle\sum_{1 \le k \le n} k^2 = \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \qquad \prod_{1 \le k \le n} k^2 = \prod_{k=1}^{n} k^2 = (n!)^2.$

② I, J を 2 つの有限集合とし、直積集合 $I \times J$ の各元 (i, j) に対して、実数 a_{ij} が 1 つ定められているとします。このとき、$I \times J$ のすべての元 (i, j) にわたる a_{ij} たちの和、および、積をそれぞれ記号

$$\sum_{(i,j) \in I \times J} a_{ij} \qquad \prod_{(i,j) \in I \times J} a_{ij}$$

によって表わします。特に、I, J が、m, n を自然数として、$I = \{1, \cdots, m\}$, $J = \{1, \cdots, n\}$ によって与えられているときは、和 $\sum_{(i,j) \in I \times J} a_{ij}$ および積 $\prod_{(i,j) \in I \times J} a_{ij}$ をそれぞれ

$$\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij} \qquad \text{および} \qquad \prod_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij}$$

のようにも書き表わします。さらに、$n = m$ の場合には

$$\sum_{1 \le i,j \le n} a_{ij} \quad \left(\text{または} \quad \sum_{i,j=1}^{n} a_{ij} \right) \qquad \text{および} \qquad \prod_{1 \le i,j \le n} a_{ij} \quad \left(\text{または} \quad \prod_{i,j=1}^{n} a_{ij} \right)$$

のように書き表わします。

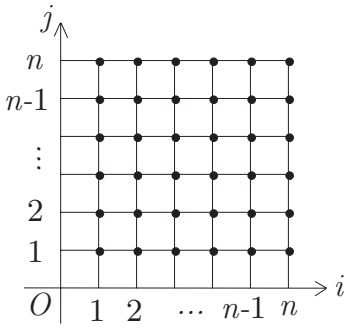
例10-10 $\displaystyle\sum_{1 \le i,j \le n} ij = \Big(\sum_{i=1}^{n} i \Big)^2 = \frac{n^2(n+1)^2}{4}, \qquad \prod_{1 \le i,j \le n} ij = \prod_{i=1}^{n} (i^n n!) = (n!)^{2n}.$

演習 10-4 *

n を自然数とする。$1 \leq i,\ j \leq n$ を満たす整数 $i,\ j$ の各組 (i,j) に対して、実数 a_{ij} が 1 つ定められているとする。等式

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

が成り立つことを右図を使って簡単に説明せよ。



③ $1 \leq i \leq j \leq n$ を満たす整数 i と j の各組 (i,j) に対して、1 つの実数 a_{ij} が定められているとします。このとき、$S := \{\ (i,j) \mid 1 \leq i \leq j \leq n\ \}$ のすべての元 (i,j) にわたる a_{ij} たちの和 $\sum\limits_{(i,j)\in S} a_{ij}$ および積 $\prod\limits_{(i,j)\in S} a_{ij}$ をそれぞれ

$$\sum_{1\leq i\leq j\leq n} a_{ij} \qquad \text{および} \qquad \prod_{1\leq i\leq j\leq n} a_{ij}$$

のようにも書き表わします。

同様に、$\{\ (i,j) \mid 1 \leq i < j \leq n\ \}$ のすべての元 (i,j) にわたる a_{ij} たちの和と積をそれぞれ

$$\sum_{1\leq i<j\leq n} a_{ij} \qquad \text{および} \qquad \prod_{1\leq i<j\leq n} a_{ij}$$

のようにも書き表わします。

例10-11 各 $i = 1, 2, \cdots, n$ に対して実数 a_i が定められているとき、

$$\Big(\sum_{i=1}^{n} a_i\Big)^2 = \sum_{i=1}^{n} a_i^2 + 2\sum_{1\leq i<j\leq n} a_i a_j,$$

$$\prod_{1\leq i<j\leq n}(a_i - a_j) = (-1)^{\frac{n(n+1)}{2}} \sum_{(i_1,\cdots,i_n)\in I} (-1)^{\varepsilon(i_1,\cdots,i_n)} a_1^{i_1}\cdots a_n^{i_n}$$

となる。但し、下の等式における I は $0, 1, \cdots, n-1$ の順列全体からなる集合であり、各 $(i_1, \cdots, i_n) \in I$ に対して $\varepsilon(i_1, \cdots, i_n)$ はその順列の転倒数を表わす、すなわち、$0 \leq a < b \leq n-1$ を満たす整数の組 (a,b) のうちで $i_a > i_b$ を満たすものの個数を表わす。

演習 10-5 $1 \leq i \leq j \leq n$ を満たす整数 i, j の各組 (i,j) に対して、実数 a_{ij} が 1 つ定められているとする。等式

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

が成り立つことを図を使って簡単に説明せよ。

演習 10-6 $n \in \mathbb{N}$ とする。和

$$\sum_{j=0}^{n}\sum_{i=j}^{n} \binom{n}{i}\binom{i}{j}$$

を求めよ。

● $\sum$ 記号と $\prod$ 記号の性質

$\sum$ 記号と $\prod$ 記号が持つ基本的な性質についてまとめておきましょう。

有限集合 I の各元 i に対して、2つの実数 $a_i,\ a'_i$ が定められているとき、

$$\text{(i)}\ \sum_{i\in I}(a_i+a'_i)=\sum_{i\in I}a_i+\sum_{i\in I}a'_i$$

$$\text{(ii)}\ \prod_{i\in I}(a_ia'_i)=\Big(\prod_{i\in I}a_i\Big)\Big(\prod_{i\in I}a'_i\Big)$$

が成り立ちます。

2 つの有限集合 I,J の直積集合 $I\times J$ の各元 (i,j) に対して、実数 a_{ij} が定められているとき、

$$\text{(iii)}\ \sum_{(i,j)\in I\times J}a_{ij}=\sum_{i\in I}\Big(\sum_{j\in J}a_{ij}\Big)=\sum_{j\in J}\Big(\sum_{i\in I}a_{ij}\Big)$$

$$\text{(iv)}\ \prod_{(i,j)\in I\times J}a_{ij}=\prod_{i\in I}\Big(\prod_{j\in J}a_{ij}\Big)=\prod_{j\in J}\Big(\prod_{i\in I}a_{ij}\Big)$$

が成り立ちます。(i) と (iii) は加法の結合法則・交換法則から、(ii) と (iv) は乗法の結合法則・交換法則から導くことができます ((iii) については演習 10-4 を参照)。

$\sum$ 記号については、加法と乗法の間の分配法則から次も成り立つことがわかります。有限集合 I の各元 i に対して実数 a_i が定められていて、有限集合 J の各元 j に対して実数 b_j が定められているとき、任意の実数 α に対して、

$$\text{(v)}\ \alpha\Big(\sum_{i\in I}a_i\Big)=\sum_{i\in I}\alpha a_i$$

$$\text{(vi)}\ \Big(\sum_{i\in I}a_i\Big)\alpha=\sum_{i\in I}a_i\alpha$$

$$\text{(vii)}\ \Big(\sum_{i\in I}a_i\Big)\Big(\sum_{j\in J}b_j\Big)=\sum_{(i,j)\in I\times J}a_ib_j$$

が成り立ちます。

演習 10-7 (v), (vii) に対応する $\prod$ に関する公式を書け ($\displaystyle\prod_{i\in I}\alpha a_i$, $\displaystyle\prod_{(i,j)\in I\times J}a_ib_j$ はどう書けるか)。

最後に 1 つ注意しておいてもらいたいことは、上で述べた $\sum$ 記号と $\prod$ 記号の諸性質を導くのに、実数の和と積に関する結合法則、交換法則、分配法則しか使っていないということです。このことから、上の文章の中の「実数」という言葉を「複素数」という言葉に置き換えても同じ等式が成り立つことがわかります。より一般に、集合 S になんらかの方法で、2つの二項演算—加法と乗法—を定義することができたとき、S に属する有限個の元についての和や積を、$\sum$ 記号や $\prod$ 記号を使って表わすことができます。このとき、S の加法と乗法が結合法則、交換法則、分配法則を満たしていれば、上で述べたような $\sum$ 記号や $\prod$ 記号の諸性質が成り立つことがわかります。いずれこのような集合 S について、詳しく触れることになるでしょう。

§11. 写像の概念

写像の概念は、数列、二項演算、有限集合を定義する際に、すでに暗黙のうちに使われています。この節では、写像の概念を明確化します。ここでの目標は、写像の定義、写像の相等、写像の合成、全単射、逆写像などの写像に関する基礎概念を理解することです。

●写像の定義

A, B を2つの空でない集合とします。A に属する各々の元に対して、B の元が1つずつ定められているとき、その対応規則を A から B への**写像** (map, mapping) といいます。f が A から B への写像であることを

$$f : A \longrightarrow B \qquad \text{または} \qquad A \xrightarrow{f} B$$

のように書き表わします。また、写像 f の下で $a \in A$ に $b \in B$ が対応することを「a は f によって b に**写される**」あるいは「f は a を b に**写す**」といい、この b を $f(a)$ と書き表わします。$f(a)$ は f による a の**像** (image) と呼ばれます。授業では、

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \cup\!\!| & & \cup\!\!| \\ a & \longmapsto & f(a) \end{array}$$

のように書き表わすこともあります。

写像 $f : A \longrightarrow B$ に対して、A を f の**定義域** (domain) または**始域**といい、B を f の**終域** (codomain) といいます。

写像のかわりに**関数** (function) という言葉も同じ意味で使われますが、関数という言葉を使うのは、終域が $\mathbb{R}$ や $\mathbb{C}$ などの数の集合である場合が多いようです。

例 11-1

(1) f を、各 $x \in \mathbb{R}$ に対して $x^2 \in \mathbb{R}$ を対応させる規則とすると、この f は $\mathbb{R}$ から $\mathbb{R}$ への写像（関数）$f : \mathbb{R} \longrightarrow \mathbb{R}$ を定める。

(2) 実数列 $\{a_n\}_{n=1}^{\infty}$ が与えられると、写像 $a : \mathbb{N} \longrightarrow \mathbb{R}$ が $a(n) := a_n$ $(n \in \mathbb{N})$ によって定まる。逆に、写像 $a : \mathbb{N} \longrightarrow \mathbb{R}$ が与えられれば、$a(1), a(2), \cdots, a(n), \cdots\cdots$ という実数列が得られる。つまり、実数列とは、$\mathbb{N}$ から $\mathbb{R}$ への写像のことである、と思って差し支えない（というより、これが数列の厳密な定義である）。

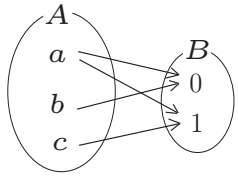
(3) 集合 S $(\neq \varnothing)$ 上の二項演算とは、$S \times S$ から S への写像のことに他ならない。

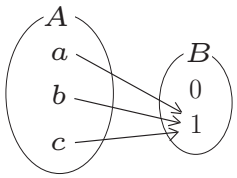
例 11-2

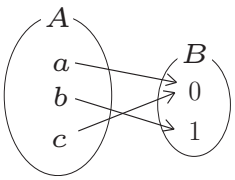
(1) A $(\neq \varnothing)$ を集合とするとき、A の各元 a に対して A の中の同じ元 a を対応させる A から A への写像を考えることができる。この写像を A 上の**恒等写像** (identity map) といい、id_A または 1_A によって書き表わす。

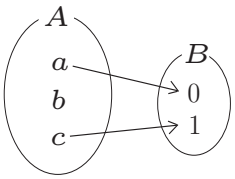
(2) A, B を2つの空でない集合とし、b_0 を B の元とするとき、A に属するどの元に対しても b_0 を対応させることによって、A から B への写像を定義することができる。このような写像を**定値写像** (constant map) という。

演習 11-1 * $A=\{a,b,c\},\ B=\{0,1\}$ とする。例えば、図 (1) は a を 0 と 1 の両方に対応させ、b を 0 に対応させ、c を 1 に対応させる規則を表わしている。この対応規則は A から B への写像と呼ぶことができるか？(2) から (4) の各図についても同様の考察をせよ。

(1)


(2)


(3)


(4)


注意：一般論を展開する際の抽象的な議論では、「$f:A\longrightarrow B$ を写像とする」のように書かれていることがよくあります。このように書かれているときは、「A に属する各々の元 a に対して、B のある元 (これを $f(a)$ で表わします) を対応させる規則が f によって (具体的に書かれてはいないけれども) 1 つ与えられている」と思う必要があります。

逆に、何か 1 つ写像を具体的に定義したいときがあります。例えば、$\mathbb{R}$ から $\mathbb{R}$ への写像を 1 つ具体的に定義したかったとしましょう。この場合には、単に「写像を $f:\mathbb{R}\longrightarrow\mathbb{R}$ と (定義) する」と書いて済ませることはできません。この状態ではまだ写像が定義できていないのです。写像を 1 つ具体的に定義するには、「写像 $f:\mathbb{R}\longrightarrow\mathbb{R}$ を $f(x)=2x-1$ によって定義する」のように、元の対応規則も書かなければなりません。

●写像の相等

2 つの写像 $f:A\longrightarrow B$ と $g:A'\longrightarrow B'$ が**等しい**とは、$A=A'$ かつ $B=B'$ であって、すべての $a\in A$ に対して $f(a)=g(a)$ となるときをいいます。このとき、$f=g$ と書き表わします。等しくないときには、$f\neq g$ と書き表わします。

例 11-3 写像 $f:\mathbb{R}\longrightarrow\mathbb{R}$ が $f(x)=x^2$ $(x\in\mathbb{R})$ によって定義されていて、写像 $g:\mathbb{Q}\longrightarrow\mathbb{R}$ が $g(x)=x^2$ $(x\in\mathbb{Q})$ によって定義されているとき、これらの定義域は等しくないので、写像としては $f\neq g$ である。

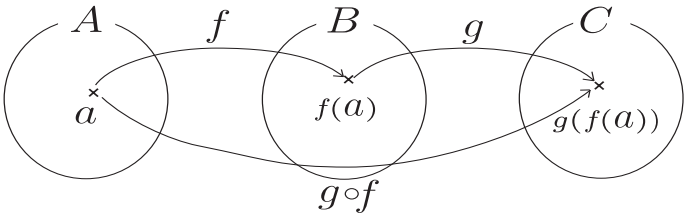
上の例のように、たとえ写像を定める 定義式が同じであっても、定義域や終域が等しくなければ、写像として等しくない ということをしっかり覚えておきましょう。

●写像の合成

写像 $f:A\longrightarrow B$ と $g:B\longrightarrow C$ が与えられたとき、元 $a\in A$ をまず f で B の元 $f(a)$ に写し、その元 $f(a)$ をさらに g で C の元 $g(f(a))$ に写すことにより、A から C への写像を定義することができます（次図参照)。このようにして得られる A から C への写像を f と g の**合成写像** (composite map) といい、$g\circ f:A\longrightarrow C$ または単に $g\circ f$ と書き表わします。つまり、$g\circ f$ とは

$$(g\circ f)(a)=g(f(a))\quad(a\in A)$$

によって定義される A から C への写像のことを言います。



例 11-4 $f : \{\bigcirc,\ \triangle,\ \square\} \longrightarrow \{$ア, イ, ウ, エ$\}$ を

$$f(\bigcirc) = \text{イ}, \quad f(\triangle) = \text{ア}, \quad f(\square) = \text{ウ}$$

によって与えられる写像とし、$g : \{$ア, イ, ウ, エ$\} \longrightarrow \{1,\ 2,\ 3\}$ を

$$g(\text{ア}) = 1, \quad g(\text{イ}) = 2, \quad g(\text{ウ}) = 2, \quad g(\text{エ}) = 3$$

によって与えられる写像とする。このとき、合成写像 $g \circ f$ は

- 定義域が $\{\bigcirc,\ \triangle,\ \square\}$、
- 終域が $\{1,\ 2,\ 3\}$ であって、
- $(g \circ f)(\bigcirc) = 2,\ (g \circ f)(\triangle) = 1,\ (g \circ f)(\square) = 2$

によって与えられる写像である。 □

演習 11-2* 関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ と関数 $g : \mathbb{R} \longrightarrow \mathbb{R}$ を次のように定義する。

$$f(x) = x^2 + 2x - 4, \qquad g(x) = 3x + 4 \quad (x \in \mathbb{R})$$

このとき、合成写像 $g \circ f$ と $f \circ g$ によって各 $x \in \mathbb{R}$ はそれぞれどのような実数に写されるか、答えよ。また、$g \circ f = f \circ g$ かそうでないかを調べよ。

補題 11-5

写像の合成に関して、次が成り立つ。

(1) 任意の写像 $f : A \longrightarrow B$ について、$f \circ \mathrm{id}_A = f$、$\mathrm{id}_B \circ f = f$.

(2) 任意の 3 つの写像 $f : A \longrightarrow B,\ g : B \longrightarrow C,\ h : C \longrightarrow D$ について、

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

(**proof**)

(1) は写像の合成、恒等写像の定義、写像の相等の定義よりただちに従う。(2) を証明する。

2 つの写像 $(h \circ g) \circ f,\ h \circ (g \circ f)$ について、どちらの定義域も A であり、どちらの終域も D である。さらに、各 $a \in A$ に対して、

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

が成り立つ、すなわち、$(h \circ g) \circ f,\ h \circ (g \circ f)$ による $a \in A$ の像が一致する。

これで、$(h \circ g) \circ f = h \circ (g \circ f)$ の証明が終わった。 □

この補題 (2) から、有限個の写像の合成において、合成をとる順番は気にしなくてよいことがわかります（定理 10-3 の証明を参照)。したがって、写像の合成を記述する際には、$h \circ g \circ f$ のように、括弧をつける必要がありません。

●単射と全射

与えられた写像がどのような写像かを調べる際に、それが単射かどうか、全射かどうかを知ることは基本的な問題です。というのは、これらの概念が逆写像 (逆関数) の存在と関連しているからです (逆写像については単射と全射を説明したあとで述べます)。

定義 11-6

$f : A \longrightarrow B$ を写像とする。

(1) f が**単射** (injection) または**1 対 1 の写像** (one-to-one mapping) であるとは、A の異なる 2 つの元が f によって B の異なる 2 つの元に写されるときをいう。すなわち、

$$\text{すべての } a,\ a' \in A \text{ について「} a \neq a' \ \Rightarrow\ f(a) \neq f(a')\text{」}$$

が成り立つときをいう。

(2) f が**全射** (surjection) または**上への写像** (onto mapping) であるとは、B に属するどの元も A に属するある元の f による像となっているときをいう。すなわち、

$$\forall\, b \in B,\ \exists\, a \in A \ \text{ s.t. } \ f(a) = b$$

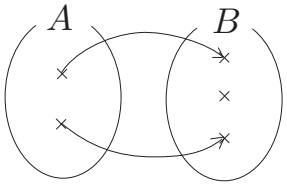
が成り立つときをいう。

(3) f が**全単射** (bijection) または**1 対 1 かつ上への写像**であるとは、f が単射でありかつ全射であるときをいう。

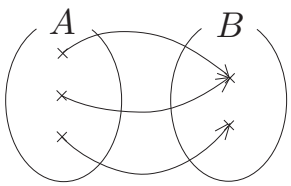
注意：写像 $f : A \longrightarrow B$ が単射であるための条件は、

$$\text{すべての } a, a' \in A \text{ について「} f(a) = f(a') \ \Rightarrow\ a = a'\text{」}$$

と同値です。したがって、写像が単射であることを証明するときには、この条件が成り立つことを確かめてもよいことになります。



単射であるが全射でない



全射であるが単射でない

例 11-7

(1) 任意の集合 $A\ (\neq \varnothing)$ に対して、恒等写像 id_A は全単射である。

(2) $f(x) = x^2\ (x \in \mathbb{R})$ によって定義される関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ は、全射でも単射でもない。実際、$f(1) = 1 = f(-1)$ となるので単射でなく、$f(x) = -1$ となる $x \in \mathbb{R}$ は存在しないから全射でない。

(3) 写像 $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ を $f(n) = 2n$ によって定義する。f は単射であるが全射でない。実際、$n \neq m$ ならば $2n \neq 2m$ なので、f は単射である。これに対して、$f(n) = 1$ となる $n \in \mathbb{Z}$ は存在しないので、f は全射でない。

演習 11-3 次の各写像について、単射であるかどうか、全射であるかどうかを調べよ。

(1) $f : [0, \pi] \longrightarrow [-1, 1],\quad f(x) = \sin x\ (x \in [0, \pi])$

(2) $g : \mathbb{R} \longrightarrow \{0, 1\},\quad g(x) = \begin{cases} 0 & (x \text{ が有理数のとき}) \\ 1 & (x \text{ が無理数のとき}) \end{cases}$

単射性、全射性、全単射性は合成をとる操作の下で保たれます。すなわち、次が成り立ちます。

補題 11-8
写像 $f : A \longrightarrow B$ と写像 $g : B \longrightarrow C$ が与えられたとき、
(1) $f,\ g$ が共に単射ならば合成写像 $g \circ f$ も単射である。
(2) $f,\ g$ が共に全射ならば合成写像 $g \circ f$ も全射である。
(3) $f,\ g$ が共に全単射ならば合成写像 $g \circ f$ も全単射である。

演習 11-4　補題 11-8 を証明せよ。

注意：補題 11-8 の逆は成立しませんが、次のことは言えます (証明は易しいので各自でつけて見て下さい)。
(1) 合成写像 $g \circ f$ が単射ならば f は単射である。
(2) 合成写像 $g \circ f$ が全射ならば g は全射である。
(3) 合成写像 $g \circ f$ が全単射ならば f は単射で g は全射である。

●逆写像

写像 $f : A \longrightarrow B$ が全単射であるとき、任意の $b \in B$ について $f(a) = b$ となる $a \in A$ は存在し（$\because f$ は全射)、かつ、そのような $a \in A$ は唯一つ（$\because f$ は単射）です。したがって、全単射 $f : A \longrightarrow B$ に対しては、各 $b \in B$ に対して $f(a) = b$ となる $a \in A$ を対応させることによって、B から A への写像を定めることができます。この写像を f の**逆写像** (inverse map) といい、$f^{-1} : B \longrightarrow A$ または単に f^{-1} によって表わします。記号 f^{-1} は「エフ インヴァース」と読みます。

逆写像の定義により、$f : A \longrightarrow B$ が全単射であるとき、$a \in A,\ b \in B$ について

$$f^{-1}(b) = a \iff b = f(a)$$

が成り立ちます。

例 11-9　次の写像 f は全単射であることを示し、その逆写像 f^{-1} を求めよ。

$$f : \mathbb{R} \longrightarrow \mathbb{R},\ f(x) = 3x + 4 \quad (x \in \mathbb{R}).$$

解；

- 単射であること：

  $x_1, x_2 \in \mathbb{R}$ が、$f(x_1) = f(x_2)$ を満たしているとき、$x_1 = x_2$ となることを示せばよい。

  $f(x_1) = f(x_2)$ ならば、$3x_1 + 4 = 3x_2 + 4$ である。この両辺に -4 を加えてから、$\frac{1}{3}$ 倍することにより、$x_1 = x_2$ が得られる。よって、f は単射である。

- 全射であること：

  $y \in \mathbb{R}$ を任意にとる。このとき、$y = f(x)$ となる $x \in \mathbb{R}$ が存在することを示せばよい。

  まず、このような x が存在したと仮定すると、x はどのようなものでなければならないかを考える。そのために、$y = f(x) = 3x + 4$ を x について解く。すると、$x = \dfrac{y-4}{3}$ となることがわかる。そこで、$y \in \mathbb{R}$ に対して $x = \dfrac{y-4}{3} \in \mathbb{R}$ を取る。すると、

$$f(x) = 3x + 4 = 3 \times \frac{y-4}{3} + 4 = y$$

となることがわかる。よって、f は全射である。

f は単射であって全射であることが示されたから、全単射である。よって、逆写像が存在する。その逆写像 f^{-1} は、f が全射になることの証明から、

$$f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}, \quad f^{-1}(y) = \frac{y-4}{3} \quad (y \in \mathbb{R})$$

であることがわかる。 □

演習 11-5* 写像 $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{2\}$ を

$$f(x) = \frac{2x-3}{x-1} \quad (x \in \mathbb{R} - \{1\})$$

によって定義する。f は全単射であることを示し、その逆写像 f^{-1} を求めよ（定義域と終域も書くこと）。

補題 11-10

写像 $f : A \longrightarrow B$ が全単射であるとき、

(1) $f^{-1} \circ f = \mathrm{id}_A$ かつ $f \circ f^{-1} = \mathrm{id}_B$ が成り立つ。

(2) $f^{-1} : B \longrightarrow A$ は全単射であり、$(f^{-1})^{-1} = f$ が成り立つ。

演習 11-6 上の補題を証明せよ。

次の定理は今後様々な場面で使われることになる、重要な定理です。

定理 11-11

写像 $f : A \longrightarrow B$ について、次の 2 つは同値である。

(i) f は全単射である。

(ii) 写像 $g : B \longrightarrow A$ であって、$g \circ f = \mathrm{id}_A$ かつ $f \circ g = \mathrm{id}_B$ を満たすものが存在する。

このとき、さらに、$g = f^{-1}$ が成り立つ。

(**proof**)

「(i) ⇒ (ii)」の証明：

f が全単射ならば、逆写像 f^{-1} が存在する。これを g とおけば、定理の条件 (ii) を満たす (補題 11-10)。

「(ii) ⇒ (i)」の証明：

恒等写像は全単射なので、演習 11-4 の下の注意から直ちに前半部分の証明が終わるが、ここではそれを用いずに、直接証明する。

定理の条件 (ii) を満たす写像 $g : B \longrightarrow A$ が存在したと仮定する。このとき、f が全単射であることを示す。

- f が単射であること：

$a,\ a' \in A$ を任意にとる。

もし、$f(a) = f(a')$ であれば、この両辺に g を作用させて、$g(f(a)) = g(f(a'))$ となる。ここで、$g \circ f = \mathrm{id}_A$ を使って、

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a') = \mathrm{id}_A(a') = a'$$

を得る。よって、f は単射である。

• f が全射であること：
$b \in B$ を任意にとる。$a = g(b)$ とおく。$a \in A$ である。
g は $f \circ g = \mathrm{id}_B$ を満たしているから、

$$f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b$$

となる。よって、f は全射である。

• 最後に条件 (ii) の g が f の逆写像 f^{-1} と等しいことを示す。
まず、g も f^{-1} も B から A の写像であることに注意する。
次に、任意に $b \in B$ をとり、$a = g(b)$ とおく。上で示したように $b = f(a)$ となるから、

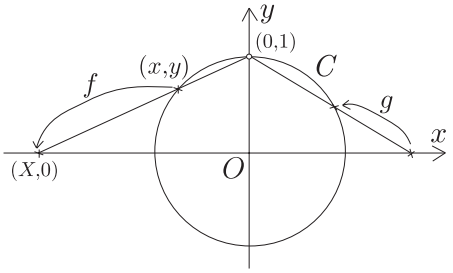
$$f^{-1}(b) = f^{-1}(f(a)) = a = g(b)$$

が成り立つ。よって、$g = f^{-1}$ である。 □

例11-12 平面における単位円周 $C = \{\ (x,y) \mid x, y \in \mathbb{R},\ x^2 + y^2 = 1\ \}$ を考える。
写像 $f : C - \{(0,1)\} \longrightarrow \mathbb{R}$ を

$$f(x,y) = \frac{x}{1-y}, \qquad (x,y) \in C - \{(0,1)\}$$

によって定義する。f は全単射である。
解；



写像 f は次のようにして作られている。点 $(x,y) \in C - \{(0,1)\}$ をとると、点 $(0,1)$ から (x,y) へ向かう半直線を引くことができる。この半直線と x-軸との交点がちょうど $(\frac{x}{1-y}, 0)$ である。
f が全単射であることを示すために、逆写像を構成しよう。
まず、任意に $x \in \mathbb{R}$ をとる。
今度は点 $(x,0)$ と $(0,1)$ を結ぶ直線

(11-1) $$l : (X,Y) = t(x,-1) + (0,1) \qquad (t \in \mathbb{R})$$

を考える。この直線と単位円周

(11-2) $$C : X^2 + Y^2 = 1$$

との交点のうち、$(0,1)$ でない方を求める。(11-1) と (11-2) を連立させてその交点を求めると、$(X,Y) = (\frac{2x}{x^2+1}, \frac{x^2-1}{x^2+1})$ であることがわかる。
以上の考察をもとに、写像 $g : \mathbb{R} \longrightarrow C - \{(0,1)\}$ を

$$g(x) = (\frac{2x}{x^2+1}, \frac{x^2-1}{x^2+1}) \qquad (x \in \mathbb{R})$$

によって定義する。このとき、

$$\begin{cases} \text{任意の } (x,y) \in C - \{(0,1)\} \text{ に対して、} (g \circ f)(x,y) = (x,y) \text{ であり、} \\ \text{任意の } x \in \mathbb{R} \text{ に対して、} (f \circ g)(x) = x \text{ であること} \end{cases}$$

が簡単に確かめられる (各自で確認して下さい)。したがって、$g \circ f = \mathrm{id}_{C-\{(0,1)\}}$, $f \circ g = \mathrm{id}_{\mathbb{R}}$ であり、f は全単射である。そして、その逆写像は上で定義した g によって与えられる。 □

演習 11-7　写像 $f : A \longrightarrow B$ と $g : B \longrightarrow C$ が共に全単射であるとき、$g \circ f$ は全単射であって、

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

が成り立つことを証明せよ。

●写像のグラフ

集合 A から集合 B への写像 $f : A \longrightarrow B$ の**グラフ** (graph) とは、直積集合 $A \times B$ の部分集合

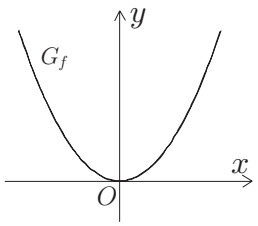
$$G_f := \{\ (a, f(a)) \mid a \in A\ \}$$

のことをいいます。

例11-13　関数 $f : \mathbb{R} \longrightarrow \mathbb{R},\ f(x) = x^2$ のグラフ G_f は

$$G_f = \{\ (a, a^2) \mid a \in \mathbb{R}\ \}$$

によって与えられる $\mathbb{R} \times \mathbb{R}$ の部分集合である。右図はこれを (x, y)-平面に図示したものである。



写像 $f : A \longrightarrow B$ のグラフ G_f は次の条件を満たしています (∃! は「一意的に存在する」ということを表わす記号だったことを思い出しましょう)。

$$\forall\, a \in A,\ \exists!\, b \in B \ \text{ s.t. } \ (a, b) \in G_f.$$

逆に、$A \times B$ の (空でない) 部分集合 G が

$$(*) \qquad \forall\, a \in A,\ \exists!\, b \in B \ \text{ s.t. } \ (a, b) \in G$$

を満たしているとします。このとき、各 $a \in A$ に対して、$(a, b) \in G$ となるような $b \in B$ を対応させることにより、写像 $f : A \longrightarrow B$ が定まります。つまり、A から B への写像を与えることと $A \times B$ の部分集合 G であって、条件 $(*)$ を満たすものを与えることとは同値になります。このことは、A から B への写像を、直積集合 $A \times B$ の $(*)$ を満たす部分集合として定義することができる、ということを示唆しています。

●有限集合

集合 S が有限集合であるとは、それを構成している元の個数が有限個である場合を呼ぶのでした（第 10 節参照)。したがって、集合 S が有限集合かどうかを調べるためには、それの属する元を $1, 2, 3, \cdots$ と数えていったとき、有限のところで終わるかどうかを見ればよいことになります。「集合 S の元の個数を数える」ことは「S から $\mathbb{N}$ への（単射な）写像を作る」ことに対応していますから、有限集合という概念は次のように捉え直すことができます。

集合 S $(\neq \varnothing)$ が**有限集合** (finite set)

$\iff$　自然数 n と全単射な写像 $f : S \longrightarrow \{1, \cdots, n\}$ が存在する

上の状況下で、n が S を構成している元の個数と対応していることに注意しましょう。

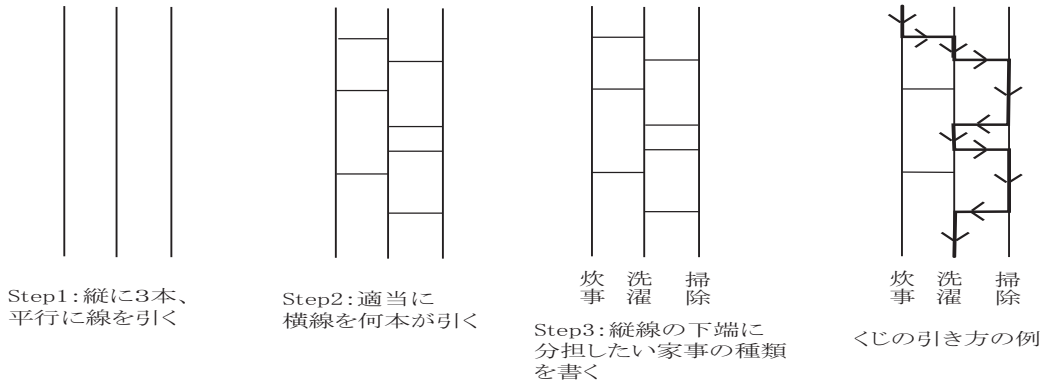
なお、上の言い換えでは空集合については何も言ってませんが、空集合 $\varnothing$ は有限集合であると約束します。

§12. 置換の概念

この節では、置換の概念をあみだくじという古来からある籤(くじ)引きの方法と対比させながら説明します。ここでの目標は、置換の積や符号の性質を知り、それらを計算できるようになることです。

●あみだくじ

よく知られている籤引きの一種にあみだくじがあります。あみだくじは次のようにして作ることができます。例えば、A 君、B 君、C 君の 3 兄弟がいて、家事の分担をあみだくじで決めることになったとします。紙を用意して、その上に縦に 3 本、平行な線を引きます。次に、みんなで勝手に 1 本目と 2 本目、2 本目と 3 本目の間に、横線をいくつか入れていきます。但し、1 本目と 2 本目の間に入れた横線と 2 本目と 3 本目の間に入れた横線が、一直線にならないようにしなければなりません。最後に、縦線の 3 つの下端に分担する家事の種類を書き入れます。これであみだくじの完成です。



あみだくじの引き方は簡単です。あみだくじの縦線の上端が籤を引く部分です。A 君、B 君、C 君の 3 人で、誰がどの上端を引くのか、最初に決めます。次に、引いた縦線の上端から下端に向かって、線に沿って進んでいきます。進んでいく途中で、横線に出会ったら、その横線をつたって隣りの縦線に移動し、再び下端に向かって進んでいきます。これを繰り返せば、最後には下端に辿りつきますが、そこに書かれている家事の種類が、その籤を引いた人の仕事となります。

ここで少し不思議に思えるのは、どの場所に横線をいれても、また、横線の数を増やしても、籤引きの結果は 3 人とも互いに異なる、つまり、出発する上端が違えば、到達する下端が違う、ということです。

●置換

n を 2 以上の自然数とします。このとき、集合 $\{1,2,\cdots,n\}$ から $\{1,2,\cdots,n\}$ への全単射な写像を n 文字の**置換** (permutation) と呼びます。n 文字の置換 σ を、次のような表として書き表わします（上段に 1 から n までの数字を並べ、下段にその置換による数字 i $(i=1,2,\cdots,n)$ の像 $\sigma(i)$ を並べて書きます)。

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

例えば、$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ と表示される置換 σ は、1 を 4 に写し、2 を 2 に写し、3 を 1 に写し、4 を 3 に写すような全単射 $\sigma : \{1,2,3,4\} \longrightarrow \{1,2,3,4\}$ を意味しています。

n 文字の置換全体からなる集合を $\mathfrak{S}_n$ という記号で表わします。($\mathfrak{S}$ は英語の S に相当するドイツ文字です。現在の教科書では、$\mathfrak{S}_n$ を S_n と書くことが多くなっていますが、ここでは古い書き方を採用しました。) $\mathfrak{S}_n$ は元の個数が $n!$ であるような有限集合です。

2つの置換 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & m \\ \sigma(1) & \sigma(2) & \cdots & \sigma(m) \end{pmatrix}$ と $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$ が**等しい**とは、

- $n = m$、かつ、
- すべての $i = 1, \cdots, n$ について $\sigma(i) = \tau(i)$

となるときをいいます (写像の相等の定義を参照)。このとき、$\sigma = \tau$ と書き表わします。

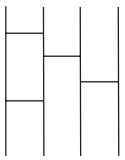
例 12-1 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ と $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ とは、置換の文字数が違っているので、等しくない。

演習 12-1 3 文字 $\{1, 2, 3\}$ の置換をすべて書き並べよ。

●あみだくじと置換との対応関係

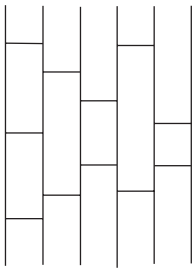
n 本 ($n \geq 2$) の縦線からなるあみだくじが 1 つ与えられたとします。そのあみだくじの左から i 番目の上端を引いたときに到達する下端が、左から a_i 番目であったとします。すると、このあみだくじによって、1 から n までの各数字 i を 1 から n までのある数字 a_i にうつす対応規則が与えられます。このようにして、n 本の縦線からなるあみだくじから、n 文字の置換 $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ が定まります。

例 12-2 右のあみだくじが定める置換は $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ である。

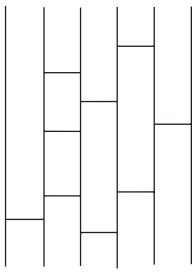


演習 12-2* 次の各あみだくじに対応する置換を求めよ。

(1)



(2)



置換の書き表わし方のバリエーション

n 文字の置換を $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ と書き表わす約束でしたが、常に「1 から n の順番で書く」というのは少し煩わしく感じることでしょう。そこで、上の数字と下の数字の組 「$\begin{smallmatrix} i \\ \sigma(i) \end{smallmatrix}$」をひと固まりとして、並べ方の順番を変えたものも同じ置換を表わすと約束します。この約束により、例えば、次の等式が成立します。

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

●置換の積

2つの n 文字の置換 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ と $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$ が与えらているとき、

$$\tau\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \cdots & \tau(\sigma(n)) \end{pmatrix}$$

という n 文字の置換 $\tau\sigma$ を考えることができます。これを τ と σ の積といいます。積 $\tau\sigma$ は合成写像 $\tau \circ \sigma : \{1, 2, \cdots, n\} \longrightarrow \{1, 2, \cdots, n\}$ のことに他なりません。

例 12-3　2つの置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ と $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ について、

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

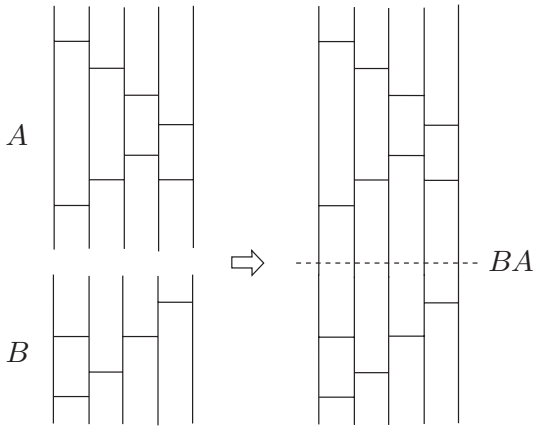
である。特に、$\sigma\tau \neq \tau\sigma$ である。

注意：置換の積の記法を上で定義したものと左右逆に書く流儀があるので、そのような本を参照するときには気をつけて下さい。上の例で示されているように、置換の積は交換法則を満たさないので、記法の約束が異なると、同じように $\tau\sigma$ と書かれていても、積をとった結果は一致しません。

演習 12-3* 次の 4 文字の置換 σ と τ の積 $\tau\sigma$ を求めよ。

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

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



置換の積はあみだくじを使って解釈することができます。n 本の縦線からなるあみだくじ A と B が与たえられたとします。このとき、A の下に B を継ぎ足すことによって、新しいあみだくじを作ることができます (左図参照)。これを BA と書いて、A と B の積と呼ぶことにします。A が定める n 文字の置換を σ とし、B が定める n 文字の置換を τ とするとき、積 BA が定める n 文字の置換は、σ と τ の積 $\tau\sigma$ になっています。

3 つの置換 $\rho, \sigma, \tau \in \mathfrak{S}_n$ について、結合法則 $(\tau\sigma)\rho = \tau(\sigma\rho)$ が成り立ちます (補題 11-5)。このことから、k 個の置換 $\sigma_1, \cdots, \sigma_k$ について、積 $\sigma_1 \cdots\cdots \sigma_k$ が括弧の付け方によらずに定まることがわかります（第 10 節参照)。

●逆置換

n 文字の置換 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ に対して、各 $\sigma(i)$ を i に写すような置換

$$\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

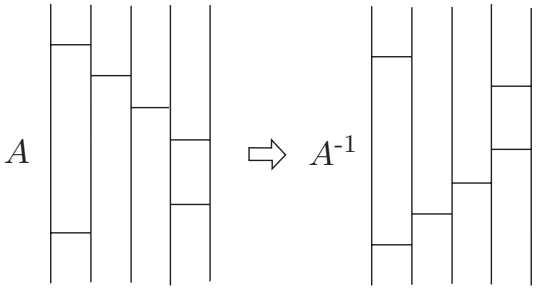
を考えることができます。この置換を σ の**逆置換** (inverse permutation) といい、記号 σ^{-1} を用いて表わします。σ の逆置換とは、σ の逆写像のことに他なりません。

例 12-4 置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ の逆置換は $\sigma^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ である。

演習 12-4* 次の各置換 σ の逆置換 σ^{-1} を求めよ。

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

逆置換はあみだくじを使って解釈することができます。n 本の縦線からなるあみだくじ A の上下を逆にして、新しいあみだくじを作ることができます (右図参照)。このあみだくじを A^{-1} と書くことにします。A が定める置換が σ であるとき、A^{-1} が定める置換は σ の逆置換 σ^{-1} になっています。



●恒等置換

1 から n までの各数字 i に対して、i 自身を対応させる n 文字の置換を $\mathfrak{S}_n$ における**恒等置換** (identity permutation) といい、記号 1_n で表わします (e で表わす流儀もあります)。

$$1_n = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

1_n は $\{1, \cdots, n\}$ 上の恒等写像のことに他なりません。前後の文脈から、数字の 1 と混乱する恐れのない場合には、1_n を 1 と書き表わします。

任意の置換 $\sigma \in \mathfrak{S}_n$ に対して、

$$\sigma 1_n = 1_n \sigma = \sigma$$
$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1_n$$

が成り立ちます (補題 11-5(1), 補題 11-10(1))。

●互換

互換 (transposition) とは、ある 2 つの数字だけを入れかえるような置換のことをいいます。すなわち、互換とは、2 以上のある自然数 n とある 2 つの数字 $i, j \in \{1, 2, \cdots, n\}$, $i \neq j$ について、

$$\begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ 1 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

(但し、点線の部分は上下同じ数字が並んでいるものとします) のように表わされる置換のことをいいます。2つの数字 i と j を入れ換える互換は $(i\ j)$ のようにも書き表わしますが、この書き方をする場合には、何文字の置換として扱っているのかを常に意識しながら、読み書きしなければなりません。

例 12-5 $\mathfrak{S}_4$ における互換 $(13), (23), (14), (12)$ の積 (合成写像) $(13)(23)(14)(12)$ はどのような置換か？

解；

$\sigma = (13)(23)(14)(12)$ とおく。この置換の下で、1 は

$$1 \overset{(12)}{\longmapsto} 2 \overset{(14)}{\longmapsto} 2 \overset{(23)}{\longmapsto} 3 \overset{(13)}{\longmapsto} 1$$

のように写される (合成をとる順番に注意)。同様に、$2, 3, 4$ はそれぞれ σ によって $2, 1, 3$ に写されることがわかる。したがって、σ は $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ という 4 文字の置換である。 □

互換というのは2つの数字だけを入れかえるような特別な置換なのですが、次の定理が示すように、互換は置換について考察する上で基本的です。

定理 12-6

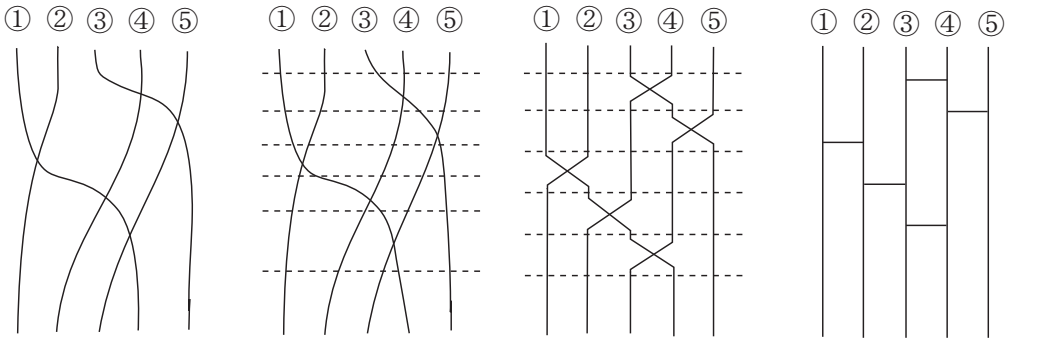
任意の置換は有限個の互換の積として書くことができる。

上の定理の厳密な証明は群論の教科書に委ねることにします。ここでは、例を見ることによりこの定理の正しさを実感してもらうことにします。

例 12-7 置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$ を互換の積で表わせ。

解；

まず、上下に 5 個の点を用意し、上側の $1, 2, 3, 4, 5$ 番目の点と下側の $4, 1, 5, 2, 3$ 番目の点をそれぞれ曲線で結び、下図のようにあみだくじを作る。



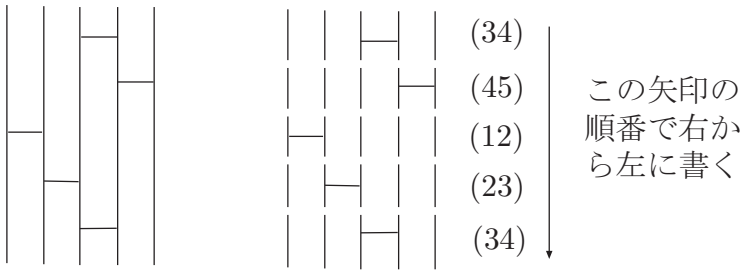
Step1：曲線で結ぶ。

Step2：各区間に曲線の交差が 1 個になるように水平線で区切る。

Step3：各区間ごとに図形を単純化する。

Step4：Step3 の交差の部分を横線でおきかえてできあがり。

このあみだくじを、次図のように、横線がちょうど一本だけあるようなあみだくじに「輪切り」にする。



置換 σ は、これらの輪切りにされたあみだくじに対応する置換を順番に掛け合わせたものに等しい。したがって、

$$\sigma = (34)(23)(12)(45)(34)$$

と表わすことができる。 □

n 文字の置換はいつでも互換の積として表わされる (定理 12-6) のですが、その表わし方には一意性はありません。

例 12-8 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$ は、上の例で見たように、$\sigma = (34)(23)(12)(45)(34)$ と表わすことができる。また、σ は、$\sigma = (35)(14)(24)$ と表わすこともできる。

演習 12-5 上の例で述べられている事実を確認せよ。つまり、等号

$$(34)(23)(12)(45)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix} = (35)(14)(24)$$

の成立を示せ。

例 12-7 では、あみだくじを利用して置換を互換の積に書く方法を紹介しました。この方法により、置換が単に互換の積でかけるということばかりでなく、隣り合う 2 つの数字を入れ替える互換の積で書くことができることがわかります。しかし、この方法を用いると、書き表わすときに用いる互換の個数は多くなりがちです。次に説明する巡回置換を用いると、その個数をずっと減らすことができます。

●巡回置換

巡回置換 (cyclic permutation) とは、ある相異なる k 個 ($k \geq 2$) の数字 $i_1, \cdots, i_k$ を

$$i_1 \longmapsto i_2,\ i_2 \longmapsto i_3,\ \cdots, i_{k-1} \longmapsto i_k,\ i_k \longmapsto i_1$$

のように写し、それ以外の数字は動かさないような置換のことをいいます。このような置換を $(i_1\ i_2\ \cdots\ i_k)$ のように表わします。例えば、$\mathfrak{S}_5$ において

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

となります。

巡回置換 $(i_1\ i_2\ \cdots\ i_k)$ に対して、k をその長さといいます。互換とは長さ 2 の巡回置換のことに他なりません。

巡回置換 $(i_1\ i_2\ \cdots\ i_k)$ は、次のようにして、互換の積に表わされます。

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-2}\ i_{k-1})(i_{k-1}\ i_k).$$

したがって、置換を巡回置換の積に書き表わすことができれば、各巡回置換を上のように互換の積で置き換えることにより、その置換を互換の積で表わすことができます。

では、どんな置換も巡回置換の積に書き表わすことはできるのでしょうか？実は、それはいつでも可能です (が、一般的な場合に証明を書くことは面倒なので省略します)。次の例を見てもらえば、そのことを実感することができるでしょう。

例 12-9 7 文字の置換

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 3 & 1 & 6 & 2 \end{pmatrix}$$

を互いに共通の文字を含まない巡回置換の積の形に表わせ。

解；

まず、σ を次々に合成していったときに、1 がどのような数字に写されていくのかを追跡する。

$$1 \overset{\sigma}{\longmapsto} 4 \overset{\sigma}{\longmapsto} 3 \overset{\sigma}{\longmapsto} 5 \overset{\sigma}{\longmapsto} 1$$

となる。次に、上の中に登場しない数字、例えば、2 について同様の考察を行なう。

$$2 \overset{\sigma}{\longmapsto} 7 \overset{\sigma}{\longmapsto} 2$$

となる。今までに登場しなかった数字は 6 のみであり、これは σ により動かされない。したがって、

$$\sigma = (7\ 2)(1\ 4\ 3\ 5)$$

のように表わされる。 □

●置換の符号

例 12-8 で見たように、n 文字の置換 σ を互換の積として表示するとき、その表わし方には一意性はないのですが、それを構成する互換の個数が偶数であるか奇数であるかは、σ によって決まっています。すなわち、次の定理が成り立ちます。

定理 12-10

置換 $\sigma \in \mathfrak{S}_n$ を次のように 2 通りの互換の積に書いたとする：

$$\sigma = \tau_1\tau_2\cdots\tau_k = \rho_1\rho_2\cdots\rho_l$$

(但し、各 $i = 1, 2, \cdots, k$ に対して τ_i は互換であり、
各 $j = 1, 2, \cdots, l$ に対して ρ_j は互換である。)

このとき、k が偶数 (resp. 奇数) ならば、l も偶数 (resp. 奇数) である。

上の定理の証明は第 17 節で与える予定です。上の定理から次の定義が意味を持ちます。

定義 12-11

置換 $\sigma \in \mathfrak{S}_n$ に対して、$\mathrm{sgn}\sigma \in \{1, -1\}$ を次のように定める。

$$\mathrm{sgn}\sigma = \begin{cases} 1 & (\sigma \text{ が偶数個の互換の積で書けるとき}) \\ -1 & (\sigma \text{ が奇数個の互換の積で書けるとき}) \end{cases}$$

$\mathrm{sgn}\sigma$ を σ の**符号** (signature) という。

演習 12-6 * 演習 12-4 の各置換 σ について、それを互換の積で表わし、その符号 $\mathrm{sgn}\sigma$ を求めよ。

定理 12-10 から、置換の符号が次の性質を持つことがわかります。

系 12-12 (置換の符号の性質)
任意の $\sigma, \tau \in \mathfrak{S}_n$ に対して、次が成り立つ。
(1) $\mathrm{sgn}(\tau\sigma) = (\mathrm{sgn}\tau)(\mathrm{sgn}\sigma)$
(2) $\mathrm{sgn}\,1_n = 1$
(3) $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}\sigma$

(**proof**)
(1) τ が k 個の互換の積で書けていて、σ が l 個の互換の積で書けていたとする。このとき、$\tau\sigma$ は $k+l$ 個の互換の積で書ける。よって、次を得る。

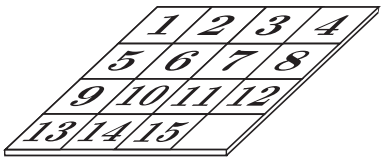
$$\mathrm{sgn}(\tau\sigma) = (-1)^{k+l} = (-1)^k(-1)^l = (\mathrm{sgn}\tau)(\mathrm{sgn}\sigma)$$

(2) $1_n = (12)(12)$ と書けることから、$\mathrm{sgn}\,1_n = 1$ とわかる。
(3) (1) と (2) より、

$$\mathrm{sgn}(\sigma^{-1})\mathrm{sgn}\sigma = \mathrm{sgn}(\sigma^{-1}\sigma) = \mathrm{sgn}\,1_n = 1$$

を得る。したがって、$\mathrm{sgn}(\sigma^{-1})$ と $\mathrm{sgn}\sigma$ は同符号である。よって、$\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}\sigma$ である。 □

演習 12-7 1 から 15 までの数字が書かれた正方形の板を、右図のように枠の中に敷き詰める。これらの板を適当に順番を変えて、配置しなおす。空いている升目の前後左右の板を移動させながら、最初の並び方（右図の状態）に戻す。これは、15 ゲームという、よく知られた遊びである。ところが、配置の仕方によっては、いくら頑張っても、最初の並び方に戻らないときがある。次の配置から出発した場合、もとの並び方に戻ることができるかどうかを調べよ。



1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

ヒント：右下隅が空いている状態から再び右下隅が空いている状態になるには、板を偶数回動かさなければならない（何故か？考えよ）。この事実と 16 文字の置換の符号とを考察せよ (空いた升目に数字の 16 が描かれていると考えて、数 $1, \cdots, 16$ の右図のような配置 A に対して、置換 $\sigma = \begin{pmatrix} 1 & \cdots & 16 \\ a_1 & \cdots & a_{16} \end{pmatrix}$ を対応させる。この配置 A に、15 ゲームのルールに従って板を 1 回動かすことは、16 文字の置換 σ に互換を一度だけ施すことに対応する)。

a_1	a_2	a_3	a_4
a_5	a_6	a_7	a_8
a_9	a_{10}	a_{11}	a_{12}
a_{13}	a_{14}	a_{15}	a_{16}

§13. 行列と線形写像

行列自体は数を長方形の形に並べた単なる表に過ぎませんが、ベクトルとの積を考えることによって、ベクトルを別のベクトルに写す（線形な）写像と考えることができます。この節では、この観点から行列について考察します。ここでの目標は、行列の積の計算に習熟すること、線形写像の幾何学的なイメージをつかむこと、そして、行列の積と線形写像の合成との関係を知ることです。この節では、$\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ とします。

§13-1 行列の積

ここでは、行列の演算の中で特に重要な積について学びます。

●行列の定義

m, n を2つの自然数とします。このとき、mn 個の (複素) 数 a_{ij} $(i = 1, \cdots, m,\ j = 1, \cdots, n)$ を、横に m 行、縦に n 列の長方形の形に並べて作られる、次のような表

$$(*) \qquad \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

のことを (m,n)-**行列** (matrix) といい、(m,n) をその行列の**サイズ** (size)、i 行 j 列に位置する数 a_{ij} をその行列の (i,j)-**成分** (component) といいます。$m = n$ のとき、(m,n)-行列を n 次**正方行列** (square matrix) といいます。

注意：1. $(*)$ の (m,n)-行列を $(a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$ のように書くこともあります。特に、$m = n$ の場合には、$(a_{ij})_{1\le i,j\le n}$ のように書いたりします。考えている行列のサイズが明白な場合は、$(a_{ij})_{i,j}$ または (a_{ij}) という簡略した書き方もよく使います。
2. 行列を表わすときに使う括弧としては $\big(\ \big)$ の他に $\big[\ \big]$ も広く使われています。
3. すべての成分が実数であるような行列を**実行列**と呼び、すべての成分が複素数であるような行列を**複素行列**と呼びます。

例 13-1 行列 $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ のサイズは $(2,3)$ である。この行列の $(2,1)$-成分は 4 である。

●行列の相等

2つの行列が等しいとは、数を並べた表として等しいことを意味します。すなわち、(m,n)-行列 A と (m',n')-行列 B が**等しい**とは、

- $m = m'$ かつ $n = n'$ であり、さらに、
- A の (i,j)-成分と B の (i,j)-成分がすべての i, j $(1 \le i \le m,\ 1 \le j \le n)$ について等しいときをいいます。

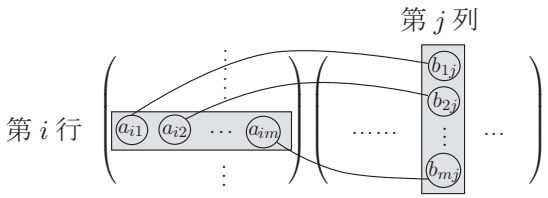
(m,n)-行列であって、どの成分も $\mathbb{K}$ の元であるようなもの全体からなる集合を $\mathrm{M}_{mn}(\mathbb{K})$ または $\mathrm{M}(m,n,\mathbb{K})$ で表わします。特に、$\mathrm{M}_{nn}(\mathbb{K})$ を $\mathrm{M}_n(\mathbb{K})$ または $\mathrm{M}(n,\mathbb{K})$ と書きます。

●行列の積

(l,m)-行列 $A=(a_{ik})_{i,k}\in \mathrm{M}_{lm}(\mathbb{K})$ と (m,n)-行列 $B=(b_{kj})_{k,j}\in \mathrm{M}_{mn}(\mathbb{K})$ に対して、(l,n)-行列

$$AB:=\Big(\sum_{k=1}^{m} a_{ik}b_{kj}\Big)_{\substack{1\le i\le l\\ 1\le j\le n}} \in \mathrm{M}_{ln}(\mathbb{K})$$

が定まります。この行列を A と B の**積** (product) といいます。



AB の第 (i,j)-成分 $\sum\limits_{k=1}^{m} a_{ik}b_{kj}$ は A の第 i 行に並ぶ数 $a_{i1},a_{i2},\cdots,a_{im}$ と B の第 j 列に並ぶ数 $b_{1j},b_{2j}\cdots,b_{mj}$ との積を順番にとっていき、それらの和をとったものになっています。

$l=m=n=3$ の場合、

$$AB=\begin{pmatrix} a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31} & a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32} & a_{11}b_{13}+a_{12}b_{23}+a_{13}b_{33}\\ a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31} & a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32} & a_{21}b_{13}+a_{22}b_{23}+a_{23}b_{33}\\ a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31} & a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32} & a_{31}b_{13}+a_{32}b_{23}+a_{33}b_{33}\end{pmatrix}$$

となります。行列の積を上のように定める理由は、13-2 節を読むとわかるでしょう。

演習 13-1 * 行列 $A=(-2\ \ \frac{1}{2}\ \ 1)$ と $B=\begin{pmatrix}-1\\2\\-3\end{pmatrix}$ について、積 AB と BA を計算せよ。

補題 13-2

(1) $I_n\in \mathrm{M}_n(\mathbb{K})$ を (i,i)-成分がすべての $i=1,\cdots,n$ について 1 で、残りの成分が 0 であるような n 次正方行列とするとき、任意の $A\in \mathrm{M}_{mn}(\mathbb{K})$ と任意の $B\in \mathrm{M}_{np}(\mathbb{K})$ に対して、

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

が成り立つ。I_n を n 次**単位行列** (unit matrix) という。

(2) $A\in \mathrm{M}_{lm}(\mathbb{K})$, $B\in \mathrm{M}_{mn}(\mathbb{K})$, $C\in \mathrm{M}_{np}(\mathbb{K})$ に対して、次が成り立つ：

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

注意：1. 行列の積については、交換法則が成り立ちません。

2. n 次単位行列 I_n を E_n で表わす流儀もあります。

演習 13-2 補題 13-2(2) を証明せよ。

●零行列

すべての成分が 0 であるような行列を**零行列** (zero matrix) と呼びます。零行列に（積が定義可能な）どのような行列を掛けても零行列です。より精密に述べると、$\mathrm{M}_{mn}(\mathbb{K})$ における零行列を O_{mn} と書くとき、任意の $A\in \mathrm{M}_{lm}(\mathbb{K})$ と任意の $B\in \mathrm{M}_{np}(\mathbb{K})$ に対して、

$$A\mathrm{O}_{mn}=\mathrm{O}_{ln},\qquad \mathrm{O}_{mn}B=\mathrm{O}_{np}$$

が成り立ちます。通常、零行列はすべて記号 O を使って書き表わします。

●逆行列

$A \in \mathrm{M}_n(\mathbb{K})$ が（$\mathrm{M}_n(\mathbb{K})$ において）**正則** (regular) である、または、**可逆** (invertible) であるとは、$AX = XA = I_n$ となる $X \in \mathrm{M}_n(\mathbb{K})$ が存在するときをいいます。このとき、X を A の**逆行列** (inverse matrix) といい、A^{-1} によって表わします。

補題 13-3

(1) $A \in \mathrm{M}_n(\mathbb{K})$ の逆行列は、それが存在すれば、ただ 1 つである。
(2) $A \in \mathrm{M}_n(\mathbb{K})$ が正則ならば、逆行列 A^{-1} も正則であり、$(A^{-1})^{-1} = A$ である。
(3) $A, B \in \mathrm{M}_n(\mathbb{K})$ が正則ならば、積 AB も正則であり、$(AB)^{-1} = B^{-1}A^{-1}$ である。

(**proof**)

(1) X の他に $Y \in \mathrm{M}_n(\mathbb{K})$ も A の逆行列であったとすれば、

$$X = XI_n = X(AY) = (XA)Y = I_nY = Y$$

となる。よって、逆行列は存在すれば、ただ 1 つである。

(2) 逆行列の定義と (1) より直ちに従う。

(3) A^{-1}, B^{-1} の定義と行列の積の結合法則により、

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$

を得る。同様にして、

$$(B^{-1}A^{-1})(AB) = I_n$$

が示される。よって、AB は正則であって、その逆行列は $B^{-1}A^{-1}$ である。 □

例 13-4 複素正方行列 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{C})$ について、

$$A：\text{正則} \iff ad - bc \neq 0$$

が成り立つ。このとき、A の逆行列は

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

によって与えられる。ここで、右辺は、行列 $\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ の各成分を $\frac{1}{ad-bc}$ 倍することによって得られる複素行列を表わしている。 □

§13-2 数ベクトル空間と線形写像

行列は、ベクトルとの積をとる操作を通じて、ベクトルをベクトルに写す写像としての側面を持っています。この節では、このような視点で行列について考えていきます。行列から定まる写像の定義域と終域は数ベクトル空間と呼ばれる集合なので、まず、数ベクトル空間の概念を導入しましょう。そのために、有限個の集合に対する直積の定義から始めます。

●有限個の集合の直積

以前、2 つの集合 A, B から直積集合 $A \times B$ を構成しました。この方法を一般化することにより、n 個の集合から直積集合を構成することができます。

$A_1, \cdots, A_n$ を n 個の空でない集合とします。このとき、各 A_i $(i = 1, \cdots, n)$ から元 a_i を 1 つずつとり、これらを並べて組 $(a_1, \cdots, a_n)$ を作ることができます。

このような 2 つの組 $(a_1, \cdots, a_n)$, $(b_1, \cdots, b_n)$ が**等しい**とは、すべての $i \in \{1, \cdots, n\}$ について $a_i = b_i$ となるときをいい、これを $(a_1, \cdots, a_n) = (b_1, \cdots, b_n)$ で表わします。

集合

$$A_1 \times \cdots \times A_n := \{\ (a_1, \cdots, a_n) \mid a_1 \in A_1, \cdots, a_n \in A_n\ \}$$

を $A_1, \cdots, A_n$ の**直積集合**または**カルテシアン積**と呼びます。

演習 13-3 直積集合 $A_1 \times \cdots \times A_n$ の 2 つの元 $(a_1, \cdots, a_n)$, $(b_1, \cdots, b_n)$ が等しくない、すなわち、$(a_1, \cdots, a_n) \neq (b_1, \cdots, b_n)$ であるとはどういう場合か。その条件を書け。

成分が $\mathbb{K}$ の元からなる (m, n) 行列の全体からなる集合 $\mathrm{M}_{mn}(\mathbb{K})$ とは、$\mathbb{K}$ の元の並べ方の違いを無視すれば、mn 個の $\mathbb{K}$ の直積集合 $\underbrace{\mathbb{K} \times \cdots \times \mathbb{K}}_{mn\ 個}$ のことに他なりません。

●数ベクトル空間

n 個の $\mathbb{K}$ の直積集合 $\overbrace{\mathbb{K} \times \cdots \times \mathbb{K}}^{n\ 個}$ を $\mathbb{K}^n$ と書き表わします：

$$\mathbb{K}^n = \{\ (a_1, \cdots, a_n) \mid a_1 \in \mathbb{K}, \cdots, a_n \in \mathbb{K}\ \}.$$

行列との積を扱うときには、元を縦に並べた方が都合がよいので、以下、

$$\mathbb{K}^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \;\middle|\; a_1 \in \mathbb{K}, \cdots, a_n \in \mathbb{K} \right\}$$

とおきます。

$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{K}^n$ に対して、

$$\mathbf{x} + \mathbf{y} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \in \mathbb{K}^n$$

を $\mathbf{x}$ と $\mathbf{y}$ の**和** (addition) といいます。

また、$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ と $t \in \mathbb{K}$ に対して、

$$t\mathbf{x} := \begin{pmatrix} tx_1 \\ \vdots \\ tx_n \end{pmatrix} \in \mathbb{K}^n$$

を $\mathbf{x}$ の t 倍、あるいは単に、**スカラー倍** (scalar multiplication) といいます。

$\mathbb{K}^n$ を単なる集合ではなく、上のような和とスカラー倍が指定されている集合と考えるとき、$\mathbb{K}^n$ を**数ベクトル空間**と呼び、その元のことを n 次元**ベクトル** (vector) といいます。ベクトル $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ の上から i 番目の元 $x_i \in \mathbb{K}$ のことを $\mathbf{x}$ の第 i 成分といいます。

例 13-5 $2\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 3\begin{pmatrix} -1 \\ 2 \\ -2 \end{pmatrix} = \begin{pmatrix} 2 \cdot 1 \\ 2 \cdot 2 \\ 2 \cdot 3 \end{pmatrix} + \begin{pmatrix} 3 \cdot (-1) \\ 3 \cdot 2 \\ 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} 2 \cdot 1 + 3 \cdot (-1) \\ 2 \cdot 2 + 3 \cdot 2 \\ 2 \cdot 3 + 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} -1 \\ 10 \\ 0 \end{pmatrix}$

ベクトルの和は結合法則と交換法則を満たします。また、和とスカラー倍との間には次の分配法則が成り立ちます：任意の $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$ と任意の $s, t \in \mathbb{K}$ に対して、

$$(s+t)\mathbf{x} = s\mathbf{x} + t\mathbf{x}, \qquad t(\mathbf{x}+\mathbf{y}) = t\mathbf{x} + t\mathbf{y}.$$

注意：1. 高校では、$\vec{\mathbf{x}}$ のように矢印をつけてベクトルを表わしていましたが、大学の教科書や授業では、矢印をつけない書き方が一般的です。
2. このプリントでは、n 次元ベクトルを、$\mathbb{K}$ の元を縦に n 個並べた組として定義しましたが、本来の定義通りに $\mathbb{K}^n$ を $\mathbb{K}$ の元を横に n 個並べた組の集合として考え、これに和とスカラー倍を

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n), \quad t(a_1, \cdots, a_n) = (ta_1, \cdots, ta_n)$$

と定めて数ベクトル空間とみなすこともあります。その元のことも n 次元ベクトルといいますが、$\mathbb{K}$ の元を横に並べているので、n 次元**行ベクトル** (row vector)、または、**横ベクトル**とも呼びます。これに対応して、$\mathbb{K}$ の元を縦に並べた組として表わされる n 次元ベクトルを n 次元**列ベクトル** (column vector)、または、**縦ベクトル**とも呼びます。

●線形写像

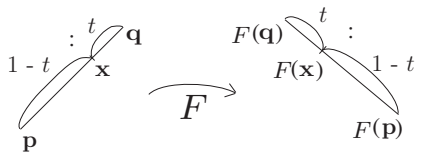
写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ が $\mathbb{K}$-**線形写像** (linear map) であるとは、次の 2 つの条件が満たされるときをいいます。

(i) すべての $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$ に対して、$F(\mathbf{x}+\mathbf{y}) = F(\mathbf{x}) + F(\mathbf{y})$.

(ii) すべての $\mathbf{x} \in \mathbb{K}^n$ とすべての $t \in \mathbb{K}$ に対して、$F(t\mathbf{x}) = tF(\mathbf{x})$.

注意：上の 2 条件の幾何学的な意味を、$\mathbb{K} = \mathbb{R}$(実数の全体), $n = 2$ の場合に考えてみましょう。

$F : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ を $\mathbb{R}$-線形写像とし、相異なる 2 つのベクトル $\mathbf{p}, \mathbf{q} \in \mathbb{R}^2$ をとります。このとき、$\mathbf{p}, \mathbf{q}$ を端点とする線分が F によってどのようなものに写されるのかを考察します。簡単のために、$F(\mathbf{p}) \neq F(\mathbf{q})$ を仮定します。$\mathbf{p}, \mathbf{q}$ を端点とする線分上の点は $t \in [0, 1]$ として $t\mathbf{p} + (1-t)\mathbf{q}$ と表わされます。これを F で写したものは、(i)(ii) の条件から、



$$F(t\mathbf{p} + (1-t)\mathbf{q}) = F(t\mathbf{p}) + F((1-t)\mathbf{q}) = tF(\mathbf{p}) + (1-t)F(\mathbf{q})$$

です。これより、線分 $\overline{\mathbf{pq}}$ を $1-t : t$ に内分する点は F により、線分 $\overline{F(\mathbf{p})F(\mathbf{q})}$ を $1-t : t$ に内分する点に写されていることがわかります。以上の考察から、大雑把に言って、線形写像とは線分の内分比を保つような写像である、と言うことができます。

例 13-6

(1) 写像 $F : \mathbb{R}^2 \longrightarrow \mathbb{R}$ を

$$F(\begin{pmatrix} x \\ y \end{pmatrix}) = x^2 + y$$

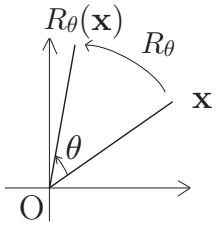
によって定義する。F は線形写像でない。

実際、$t = -1, x = 1, y = 0$ に対して、

$$F(t\begin{pmatrix} x \\ y \end{pmatrix}) = F(\begin{pmatrix} tx \\ ty \end{pmatrix}) = (tx)^2 + ty = 1 \neq -1 = t(x^2 + y) = tF(\begin{pmatrix} x \\ y \end{pmatrix})$$

となり、線形写像であるための条件 (ii) を F は満たさない。

(2) 写像 $R_\theta : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ を、原点を中心とする θ 回転とする（すなわち、R_θ は、各ベクトル $\mathbf{x} \in \mathbb{R}^2$ を原点を中心として反時計回りに角度 θ だけ回転させたベクトル $R_\theta(\mathbf{x})$ に写す写像）。幾何学的考察により、任意の $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$ と $t \in \mathbb{R}$ に対して

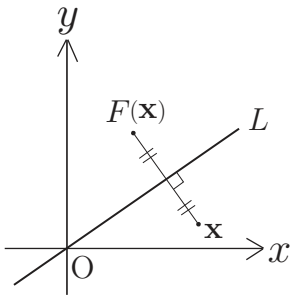


$$\begin{cases} R_\theta(\mathbf{x}+\mathbf{y}) = R_\theta(\mathbf{x}) + R_\theta(\mathbf{y}) \\ R_\theta(t\mathbf{x}) = tR_\theta(\mathbf{x}) \end{cases}$$

が成り立つことがわかるので、R_θ は $\mathbb{R}$-線形写像である。

演習 13-4 *

$\mathbb{R}^2$ を (x, y)-座標平面とみなして、方程式 $y = ax$（但し、$a \in \mathbb{R}$ は定数）によって定義される原点を通る直線 $L \subset \mathbb{R}^2$ を考える。写像 $F : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ を L に関する線対称移動とする（右図参照）。



(1) $\mathbf{x} = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$ に対して、$F(\mathbf{x})$ を求めよ。

(2) F は $\mathbb{R}$-線形写像であることを示せ。

演習 13-5 (1) $F : \mathbb{K}^l \longrightarrow \mathbb{K}^m$, $G : \mathbb{K}^m \longrightarrow \mathbb{K}^n$ がともに $\mathbb{K}$-線形写像ならば、合成写像 $G \circ F : \mathbb{K}^l \longrightarrow \mathbb{K}^n$ もまた $\mathbb{K}$-線形写像であることを証明せよ。

(2) $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ が全単射な $\mathbb{K}$-線形写像ならば、逆写像 $F^{-1} : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ も $\mathbb{K}$-線形写像であることを証明せよ。

●行列と線形写像との対応関係

行列 $A = (a_{ij})_{i,j} \in \mathrm{M}_{mn}(\mathbb{K})$ とベクトル $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ に対して、積 $A\mathbf{x} \in \mathbb{K}^m$ を

$$A\mathbf{x} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix}$$

によって定義します。これは、ベクトル $\mathbf{x}$ を $(n, 1)$-行列と考えたときの行列 A と行列 $\mathbf{x}$ の積に他なりません。この積を使って、写像 $F_A : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ を

$$F_A(\mathbf{x}) = A\mathbf{x} \quad (\mathbf{x} \in \mathbb{K}^n)$$

によって定めます。

補題 13-7

行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に対して、写像 $F_A : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ は $\mathbb{K}$-線形写像である。

(**proof**)

任意の $\mathbf{x}$, $\mathbf{y} \in \mathbb{K}^n$ と任意の $t \in \mathbb{K}$ に対して、

$$F_A(\mathbf{x}+\mathbf{y}) = A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y} = F_A(\mathbf{x}) + F_A(\mathbf{y}),$$

$$F_A(t\mathbf{x}) = A(t\mathbf{x}) = tA\mathbf{x} = tF_A(\mathbf{x})$$

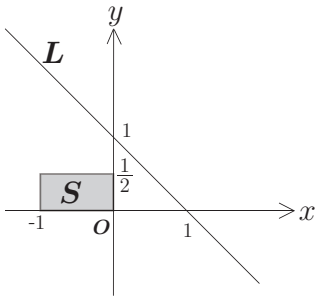
となる。よって、F_A は $\mathbb{K}$-線形である。 □

演習 13-6 *

$A = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$ とおき、線形写像 $F_A : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ を考える。

(1) 各点 $\begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix}$, $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} -1 \\ \frac{1}{2} \end{pmatrix}$ の F_A による像を求めよ。

(2) $\mathbb{R}^2$ の右図で表される部分集合 S (長方形の周および内部), L (直線) は F_A によってどのような図形に写されるか。その像 $F_A(S) = \{\, F_A(\mathbf{x}) \mid \mathbf{x} \in S \,\}$, $F_A(L) = \{\, F_A(\mathbf{x}) \mid \mathbf{x} \in L \,\}$ を (x, y)-座標平面上に図示せよ。



上では、行列から線形写像を作り出す方法を説明しました。逆に、数ベクトル空間の間の線形写像から行列を作り出すことができます。次に、このことを説明します。

命題 13-8

任意の $\mathbb{K}$-線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ に対して、$F = F_A$ となる行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ が一意的に存在する。

(**proof**)

I. A の存在：

$\mathbb{K}^n$ の n 個のベクトル

$$\mathbf{e}_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ \mathbf{e}_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix},\ \cdots, \mathbf{e}_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \quad \left(\begin{array}{l} \text{各 } \mathbf{e}_i\ (i = 1, \cdots, n) \text{ は第 } i \text{ 成分} \\ \text{だけ 1 で、残りの成分は 0 であ} \\ \text{るような } \mathbb{K}^n \text{ のベクトルを表わす} \end{array} \right)$$

を F で写し、それらを並べて行列 $A := (F(\mathbf{e}_1)\ \cdots\ F(\mathbf{e}_n)) \in \mathrm{M}_{mn}(\mathbb{K})$ を作る。

任意の $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ は、$\mathbf{x} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n$ のように n 個のベクトル $x_1\mathbf{e}_1, \cdots, x_n\mathbf{e}_n$ の和で表わすことができるから、

$$\begin{aligned} F(\mathbf{x}) &= x_1F(\mathbf{e}_1) + \cdots + x_nF(\mathbf{e}_n) \qquad (\because\ F \text{ の線形性}) \\ &= x_1A\mathbf{e}_1 + \cdots + x_nA\mathbf{e}_n \qquad (\because\ A \text{ の定義}) \\ &= x_1F_A(\mathbf{e}_1) + \cdots + x_nF_A(\mathbf{e}_n) \qquad (\because\ F_A \text{ の定義}) \\ &= F_A(x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n) \qquad (\because\ F_A \text{ の線形性}) \\ &= F_A(\mathbf{x}) \end{aligned}$$

を得る。よって、$F = F_A$ が成り立つ。

II. A の一意性：

$\mathrm{M}_{mn}(\mathbb{K})$ に属する 2 つの行列 $A = (a_{ij})_{i,j}$, $B = (b_{ij})_{i,j}$ が $F_A = F_B$ を満たしていると仮定する。このとき、$i = 1, \cdots, n$ に対して、

$$\begin{pmatrix} b_{1i} \\ \vdots \\ b_{mi} \end{pmatrix} = B\mathbf{e}_i = F_B(\mathbf{e}_i) = F_A(\mathbf{e}_i) = A\mathbf{e}_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix}$$

となる。よって、$A = B$ を得る。故に、$F = F_A$ となる $A \in \mathrm{M}_{mn}(\mathbb{K})$ は一意的である。 □

演習 13-7 * $F : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ を、原点を中心とする θ 回転とするとき (例題 13-6(2) を参照)、$F = F_A$ となる行列 $A \in \mathrm{M}_2(\mathbb{R})$ を求めよ。

●線形写像の合成と行列の積との関係

線形写像の合成はまた線形写像なので (演習 13-5(1))、行列 $A \in \mathrm{M}_{lm}(\mathbb{K})$, $B \in \mathrm{M}_{mn}(\mathbb{K})$ に対して、$F_A \circ F_B$ は線形写像です。したがって、命題 13-8 により、$F_A \circ F_B = F_C$ を満たす行列 $C \in \mathrm{M}_{ln}(\mathbb{K})$ が一意的に存在します。実は、この C は積 AB です。なぜならば、行列の積は結合法則を満たすので、任意の $\mathbf{x} \in \mathbb{K}^l$ について、

$$(F_A \circ F_B)(\mathbf{x}) = F_A(F_B(\mathbf{x})) = F_A(B\mathbf{x}) = A(B\mathbf{x}) = (AB)(\mathbf{x}) = F_{AB}(\mathbf{x})$$

となる、つまり、

$$F_A \circ F_B = F_{AB}$$

となるからです。

今述べた、線形写像の合成と行列の積との関係と命題 13-8 から、次の結果が従います。

命題 13-9

$A \in \mathrm{M}_n(\mathbb{K})$ について、

$$A\text{：正則} \iff F_A : \mathbb{K}^n \longrightarrow \mathbb{K}^n \text{ は全単射}$$

が成り立つ。このとき、F_A の逆写像は $F_{A^{-1}}$ によって与えられる：

$$F_A^{-1} = F_{A^{-1}}\ .$$

(**proof**)

A が正則であるとする。

$X = A^{-1}$ とおくと $AX = XA = I_n$ が成立するので、

$$F_A \circ F_X = F_{AX} = F_{I_n} = \mathrm{id}_{\mathbb{K}^n}, \qquad F_X \circ F_A = F_{XA} = F_{I_n} = \mathrm{id}_{\mathbb{K}^n}$$

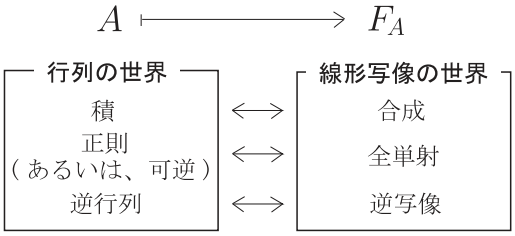
を得る。したがって、定理 11-11 より、F_A は全単射であり、$F_A^{-1} = F_X = F_{A^{-1}}$ となる。

逆に、F_A が全単射であるとすると、逆写像 F_A^{-1} が存在する。F_A^{-1} は線形写像なので (演習 13-5(2))、$F_A^{-1} = F_B$ となる行列 $B \in \mathrm{M}_n(\mathbb{K})$ が存在する (命題 13-8)。このとき、

$$F_{I_n} = \mathrm{id}_{\mathbb{K}^n} = F_A \circ F_B = F_{AB}, \qquad F_{I_n} = \mathrm{id}_{\mathbb{K}^n} = F_B \circ F_A = F_{BA}$$

となるので、$AB = BA = I_n$ であることがわかる (命題 13-8)。故に、$B = A^{-1}$ である。 □

命題 13-8 により、行列の世界と線形写像の世界を、$A \longmapsto F_A$ という対応を介して、行ったり来たりすることができるようになりました。さらに、命題 13-9 により、この対応を介して、行列に対する積、正則、逆行列といった概念と線形写像に対する合成、全単射、逆写像といった概念がきれいに対応していることがわかりました。



§14. 連続関数

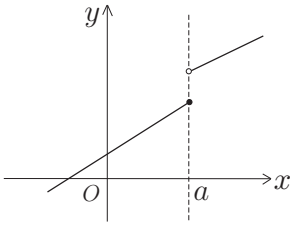
関数が連続であるとは、直感的には、そのグラフが ‘ 切れ目なく繋がっている ’ ときをいうのでした。ここではこの概念を厳密に定式化します。ここでの目標は、‘ $\varepsilon-\delta$ 式 ’ の議論を通して、関数の連続性に対する理解・認識を深めることです。

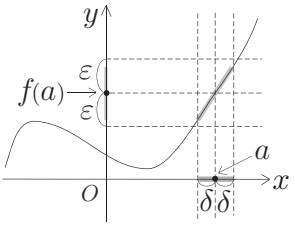
§14-1 1 変数連続関数

実数値関数 (real valued function) とは、ある集合 $S\ (\neq\varnothing)$ 上で定義された写像 $f:S\longrightarrow\mathbb{R}$ のことをいいます。特に、$S\subset\mathbb{R}$ のとき、f を 1 変数（実数値）関数といいます。この節では、1 変数関数が連続であることの定義を与え、その基本的な性質を示します。

● 1 変数実数値連続関数

右図のようなグラフを持つ関数について考えてみましょう。この関数は、点 a において値がジャンプしているので、連続ではありません。しかし、a 以外の点では、その近くでグラフは ‘ 切れ目なく繋がっている ’ ので、a 以外の点では連続と言えます。つまり、一点 a で連続でないために、右図のようなグラフを持つ関数は連続ではないわけです。逆に言えば、関数が、どのような点においても連続であれば、その関数自体が連続であると言えます。





そこで、関数 f がその定義域内の点 a で連続である、とはどういうことなのかを考察しましょう。f が点 a で連続であるとは、直感的には、「x を a に限りなく近づけていくとき、$f(x)$ が $f(a)$ に限りなく近づいていく」ことであると理解できます。このことは、「実数 $\varepsilon>0$ をいくらでも小さい値に与えても、x が a の十分近くにあれば、$|f(x)-f(a)|<\varepsilon$ が満たされる」ということであると解釈できます。さらに、「x が a の十分近くにあれば」ということは、「十分小さく実数 $\delta>0$ をとったとき、a との距離が δ よりも小さい x に対しては」ということであると解釈できます。“小さい”という概念は主観的なものなので、この言葉を削除して、文章を整理することにより、次の定義に到達することができます。

定義 14-1

集合 $S\subset\mathbb{R}$ 上で定義されている 1 変数関数 $f:S\longrightarrow\mathbb{R}$ が**点 $a\in S$ で連続** (continuous at $a\in S$) であるとは、どのような実数 $\varepsilon>0$ に対しても、次の条件 $(*)$ を満たす実数 $\delta>0$ が存在するときをいう。

$(*)$ $|x-a|<\delta$ を満たすすべての $x\in S$ について、$|f(x)-f(a)|<\varepsilon$ である。

すべての点 $a\in S$ で連続なとき、f は**連続** (continuous) であるという。

注意： 1 変数関数 $f:S\longrightarrow\mathbb{R}$ が点 $a\in S$ で連続であることを、論理記号を使って、

「$\forall\varepsilon>0,\ \exists\delta>0$ s.t. $x\in S,\ |x-a|<\delta\ \Rightarrow\ |f(x)-f(a)|<\varepsilon$」が成り立つ

のように表現します。通常、“ が成り立つ ”の部分は省略します。

例 14-2　実数 c への定数関数 $\underline{c} : \mathbb{R} \longrightarrow \mathbb{R},\ \underline{c}(x) = c\ \ (x \in \mathbb{R})$ は連続である。

(**proof**)

任意の点 $a \in \mathbb{R}$ で $\underline{c}$ が連続であることを示せばよい。

任意に $a \in \mathbb{R}$ をとる。このとき、任意の $\varepsilon > 0$ に対して、$\delta := 1$ と定める。すると、$|x - a| < \delta$ を満たすすべての $x \in \mathbb{R}$ に対して、

$$|\underline{c}(x) - \underline{c}(a)| = |c - c| = 0 < \varepsilon$$

が成り立つ。故に、$\underline{c}$ は点 a で連続である。　□

例 14-3　$f(x) = x^2\ (x \in \mathbb{R})$ によって定義される 1 変数関数 f は連続である。

(**proof**)

点 $a \in \mathbb{R}$ を任意にとる。$x \in \mathbb{R}$ に対して

$$|f(x) - f(a)| = |x^2 - a^2| = |x - a||x + a| \leq |x - a|(|x - a| + |2a|)$$

が成り立つことに注意する。さて、任意に $\varepsilon > 0$ をとり、

$$\delta := \min\Big\{1,\ \frac{\varepsilon}{1 + 2|a|}\Big\}\ > 0$$

と定める。このとき、$|x - a| < \delta$ を満たすすべての $x \in \mathbb{R}$ に対して、

$$|f(x) - f(a)| \leq |x - a|(|x - a| + 2|a|) < \delta(1 + 2|a|) \leq \varepsilon$$

となる。故に、f は点 a で連続である。したがって、f は連続である。　□

演習 14-1 * $f(x) = \frac{1}{x}\ (x \in \mathbb{R} - \{0\})$ によって定義される 1 変数関数 f は連続であることを示せ。

ヒント：$a \in \mathbb{R} - \{0\}$ に対して、「$|x - a| < \frac{|a|}{2}$ ならば、$x \neq 0$ かつ $\frac{1}{|x|} < \frac{2}{|a|}$」が成り立つことに注意して、任意の $\varepsilon > 0$ に対して、連続関数の定義における条件 $(*)$ を満たす $\delta > 0$ を探す。命題 14-4 の証明も参照。

演習 14-2 * 1 変数関数 $f : S \longrightarrow \mathbb{R}$ が連続でないとはどういうときをいうのか。その定義を、まず、論理記号 $(\forall, \exists, \Rightarrow)$ を使わずに文章で書け。次に、それを論理記号を使って書き直せ。

●連続関数の和、差、積、商

定義域が同一の集合 S であるような 2 つの実数値関数 $f : S \longrightarrow \mathbb{R},\ g : S \longrightarrow \mathbb{R}$ が与えられたとき、S を定義域とする 4 つの実数値関数 $f + g,\ f - g,\ fg,\ \frac{f}{g}$ を新たに次のようにして作ることができます（但し、4 番目の関数は、すべての $x \in S$ について $g(x) \neq 0$ のときのみ作ることができます）。

$$(f + g)(x) := f(x) + g(x) \quad (x \in S)$$
$$(f - g)(x) := f(x) - g(x) \quad (x \in S)$$
$$(fg)(x) := f(x)g(x) \quad (x \in S)$$
$$(\tfrac{f}{g})(x) := \frac{f(x)}{g(x)} \quad (x \in S)$$

この 4 つの関数を、上から順に、f と g の**和**、**差**、**積**、**商**と呼びます。

命題 14-4

2つの1変数関数 $f : S \longrightarrow \mathbb{R},\ g : S \longrightarrow \mathbb{R}$ が点 $a \in S$ で連続であるとき、

$$f+g,\ f-g,\ fg,\ \frac{f}{g}$$

はすべて点 a で連続である。但し、商を考えるときには、すべての $x \in S$ について $g(x) \neq 0$ を満たしていると仮定する。

(**proof**)

和と差については演習問題として残し、積と商について証明する。

• 積の連続性：

まず、三角不等式により、任意の $x \in S$ について

$$|(fg)(x) - (fg)(a)| \leq |f(x)||g(x) - g(a)| + |f(x) - f(a)||g(a)|$$

が成り立ち、f は点 a で連続なので、

$$\exists\, \delta_0 > 0 \ \text{ s.t. } \ x \in S,\ |x-a| < \delta_0 \ \Rightarrow\ |f(x)| < |f(a)| + 1$$

が成り立つことに注意する。

さて、任意に $\varepsilon > 0$ をとる。$\varepsilon_0 := \frac{\varepsilon}{|f(a)|+|g(a)|+1} > 0$ に対して、

$$\exists\, \delta_1 > 0 \ \text{ s.t. } \ x \in S,\ |x-a| < \delta_1 \ \Rightarrow\ |f(x) - f(a)| < \varepsilon_0$$
$$\exists\, \delta_2 > 0 \ \text{ s.t. } \ x \in S,\ |x-a| < \delta_2 \ \Rightarrow\ |g(x) - g(a)| < \varepsilon_0$$

が成り立つ。したがって、$\delta := \min\{\delta_0, \delta_1, \delta_2\}$ とおくと $\delta > 0$ であって、$|x-a| < \delta$ を満たすすべての $x \in S$ に対して、

$$\begin{aligned} |(fg)(x) - (fg)(a)| &\leq |f(x)||g(x) - g(a)| + |f(x) - f(a)||g(a)| \\ &< (|f(a)| + 1)\varepsilon_0 + \varepsilon_0|g(a)| = (|f(a)| + |g(a)| + 1)\varepsilon_0 = \varepsilon \end{aligned}$$

となる。故に、fg は点 a で連続である。

• 商の連続性：

$\frac{f}{g} = f \cdot \frac{1}{g}$ と書けることから、$\frac{1}{g}$ が点 a で連続となることを証明すればよい。まず、任意の $x \in S$ について

$$\Big|\frac{1}{g(x)} - \frac{1}{g(a)}\Big| = \frac{|g(a) - g(x)|}{|g(a)||g(x)|}$$

が成り立ち、g が点 a で連続であって、$g(a) \neq 0$ であることから、

$$\exists\, \delta_0 > 0 \ \text{ s.t. } \ x \in S,\ |x-a| < \delta_0 \ \Rightarrow\ \frac{|g(a)|}{2} \leq |g(x)|$$

が成り立つことに注意する。

さて、任意に $\varepsilon > 0$ をとる。g は点 a で連続なので、$\varepsilon_0 := \frac{|g(a)|^2\varepsilon}{2} > 0$ に対して、

$$\exists\, \delta_1 > 0 \ \text{ s.t. } \ x \in S,\ |x-a| < \delta_1 \ \Rightarrow\ |g(x) - g(a)| < \varepsilon_0$$

が成り立つ。したがって、$\delta := \min\{\delta_0, \delta_1\}$ とおくと $\delta > 0$ であって、$|x-a| < \delta$ を満たすすべての $x \in S$ に対して、

$$\Big|\frac{1}{g(x)} - \frac{1}{g(a)}\Big| = \frac{|g(a) - g(x)|}{|g(a)||g(x)|} < \frac{2\varepsilon_0}{|g(a)|^2} = \varepsilon$$

となる。故に、$\frac{1}{g}$ は点 a で連続である。 □

演習 14-3　2つの 1 変数関数 $f : S \longrightarrow \mathbb{R},\ g : S \longrightarrow \mathbb{R}$ が点 $a \in S$ で連続であるとき、$f+g$ も点 a で連続であることを示せ。

注意：1. 2つの 1 変数関数 $f : S \longrightarrow \mathbb{R},\ g : S \longrightarrow \mathbb{R}$ が点 $a \in S$ で連続であるとき、差 $f-g$ が点 $a \in S$ で連続であることは、和 $f+g$ が点 $a \in S$ で連続であることと同様にして証明することもできますが、$f-g = f+\underline{(-1)}g$ と書けることから、連続関数の和と積の連続性を使って導くこともできます。

2. 実数値関数 $f : S \longrightarrow \mathbb{R}$ と実数 c に対して、新たに実数値関数 $cf : S \longrightarrow \mathbb{R}$ を

$$(cf)(s) = cf(s) \qquad (s \in S)$$

によって定義することができます。cf を f の c 倍、または、単に、f のスカラー倍と呼びます。

f が点 $a \in S$ で連続であれば、f のスカラー倍 cf も点 a で連続になります。このことは、連続関数の定義に戻って直接証明しても易しいですが、cf が定数関数 $\underline{c}$ と f との積 $\underline{c}f$ に一致することを使って証明することもできます。

命題 14-4、恒等写像 $\mathrm{id}_{\mathbb{R}}$ の連続性、定数関数の連続性 (例 14-2) から、次が成り立つことがわかります。

例 14-5　$a_0, a_1, \cdots, a_n \in \mathbb{R}$ に対して、関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ を

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad (x \in \mathbb{R})$$

によって定義する。f は連続である。

●合成関数の連続性

2つの 1 変数関数 $f : S_1 \longrightarrow \mathbb{R},\ g : S_2 \longrightarrow \mathbb{R}$ が合成可能であるとは、すべての $x \in S_1$ について $f(x) \in S_2$ が満たされるときをいいます。このとき、関数 $g \circ f : S_1 \longrightarrow \mathbb{R}$ を

$$(g \circ f)(x) := g(f(x)) \quad (x \in S_1)$$

によって定めることができます (p.86 を参照)。この $g \circ f$ を f と g の**合成関数** (composite function) といいます。

例 14-6　$S = \{\, x \in \mathbb{R} \mid x \geq \frac{1}{2} \,\}$ 上の関数

$$h : S \longrightarrow \mathbb{R}, \quad h(x) = \sqrt{2x-1}$$

は、2つの関数

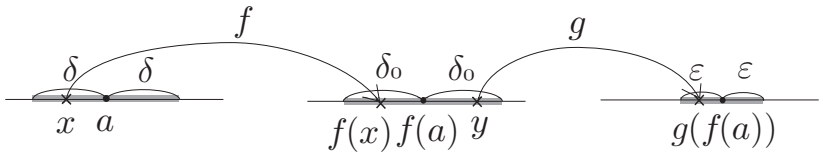
$$f : S \longrightarrow \mathbb{R},\ f(x) = 2x-1 \quad \text{と} \quad g : \{\, x \in \mathbb{R} \mid x \geq 0 \,\} \longrightarrow \mathbb{R},\ g(x) = \sqrt{x}$$

との合成関数 $g \circ f$ に等しい。

命題 14-7

合成可能な2つの 1 変数関数 $f : S_1 \longrightarrow \mathbb{R},\ g : S_2 \longrightarrow \mathbb{R}$ が与えられているとする。このとき、f が点 $a \in S_1$ で連続であり、g が点 $f(a)$ で連続であるならば、合成関数 $g \circ f$ は点 a で連続である。

(**proof**)



任意に $\varepsilon > 0$ をとる。g は点 $f(a)$ で連続なので、

$$\exists\, \delta_0 > 0 \ \text{ s.t. } \ y \in S_2,\ |y - f(a)| < \delta_0 \ \Rightarrow\ |g(y) - g(f(a))| < \varepsilon$$

が成り立つ。f は点 $a \in S_1$ で連続なので、$\delta_0 > 0$ に対して、

$$\exists\, \delta > 0 \ \text{ s.t. } \ x \in S_1,\ |x - a| < \delta \ \Rightarrow\ |f(x) - f(a)| < \delta_0$$

が成り立つ。したがって、$|x - a| < \delta$ を満たすすべての $x \in S_1$ に対して、$|f(x) - f(a)| < \delta_0$ が成り立ち、それゆえ、

$$|(g \circ f)(x) - (g \circ f)(a)| = |g(f(x)) - g(f(a))| < \varepsilon$$

となる。故に、合成関数 $g \circ f$ は点 a で連続である。 □

注意：上の命題と演習 14-1 を使って、命題 14-4 における商の連続性を再証明することができます。

演習 14-4 関数 $f : \mathbb{R} \longrightarrow \mathbb{R},\ f(x) = \begin{cases} x \sin \frac{1}{x} & (x \neq 0) \\ 0 & (x = 0) \end{cases}$ は連続であることを示せ。
(証明において sin が連続であることは使ってよい。)

●関数の連続性と数列

1 変数関数の連続性は数列を使って言い換えることができます。

定理 14-8

1 変数関数 $f : S \longrightarrow \mathbb{R}$ と点 $a \in S$ について、次の 2 つは同値である。

(i) f は点 a で連続である。

(ii) $\lim_{n\to\infty} x_n = a$ を満たす S の元からなる任意の数列 $\{x_n\}_{n=1}^{\infty}$ に対して、$\lim_{n\to\infty} f(x_n) = f(a)$ である。

(**proof**)

「(i) $\Longrightarrow$ (ii)」の証明は易しいので、演習問題として残し、「(ii) $\Longrightarrow$ (i)」を証明しよう。対偶を証明する。

f は a で連続でないとする。すると、次の条件を満たす $\varepsilon > 0$ が存在する：

$$(*) \qquad \forall\, \delta > 0,\ \exists\, x \in S \ \text{ s.t. } \ |x - a| < \delta,\ |f(x) - f(a)| \geq \varepsilon.$$

したがって、各 $n \in \mathbb{N}$ に対して $\frac{1}{n}$ を考え、$\delta = \frac{1}{n}$ に対して $(*)$ を適用することにより、$|x_n - a| < \frac{1}{n}$ かつ $|f(x_n) - f(a)| \geq \varepsilon$ を満たす $x_n \in S$ の存在がわかる。このとき、S の元からなる数列 $\{x_n\}_{n=1}^{\infty}$ は a に収束するが、数列 $\{f(x_n)\}_{n=1}^{\infty}$ は $f(a)$ に収束しない。これで「(ii) $\Longrightarrow$ (i)」の対偶が証明された。 □

注意：上の定理と命題 8-6 から命題 14-4 を再証明することができます。

演習 14-5 * 上の定理の「(i) $\Longrightarrow$ (ii)」を証明せよ。

§14-2 多変数連続関数

前節では、1 変数関数が連続であることを定義し、連続関数の性質を調べました。ここでは、その多変数版を考えます。1 変数関数が連続であることを定式化する過程で、「近づく」という概念を 2 つの実数の差の絶対値を評価することによって定量化したことを思い出しましょう。多変数関数の連続性を議論するには、1 変数の場合の絶対値に代わる「近さ」の「ものさし」を導入する必要があります。次に述べるユークリッド距離がその「ものさし」に対応する概念です。

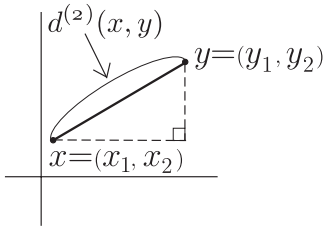
●ユークリッド距離

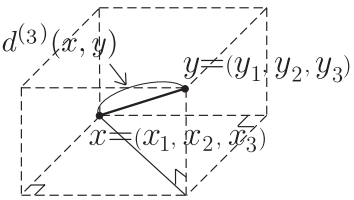
直積集合 $\mathbb{R}^n = \{\ (a_1, \cdots, a_n) \mid a_1 \in \mathbb{R}, \cdots, a_n \in \mathbb{R}\ \}$ に属する 2 つの元
$x = (x_1, \cdots, x_n),\ y = (y_1, \cdots, y_n)$ に対して、

$$d^{(n)}(x, y) := \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$$

とおき、これを x と y との**ユークリッド距離** (Euclidean distance) といいます。ユークリッド距離は**距離の公理**と呼ばれる次の 3 つの性質を満たしていることが確かめられます。

(D1) 任意の $x, y \in \mathbb{R}^n$ に対して $d^{(n)}(x, y) \geq 0$ であり、
　　$d^{(n)}(x, y) = 0$ となるのは $x = y$ のときに限る。
(D2) 任意の $x, y \in \mathbb{R}^n$ に対して $d^{(n)}(x, y) = d^{(n)}(y, x)$ である。
(D3) (**三角不等式**) 任意の $x, y, z \in \mathbb{R}^n$ に対して $d^{(n)}(x, z) \leq d^{(n)}(x, y) + d^{(n)}(y, z)$ である。





●連続写像

ユークリッド距離を使うことにより、1 変数実数値関数に対する連続の定義を多変数関数に対する連続の定義へと拡張することができます。

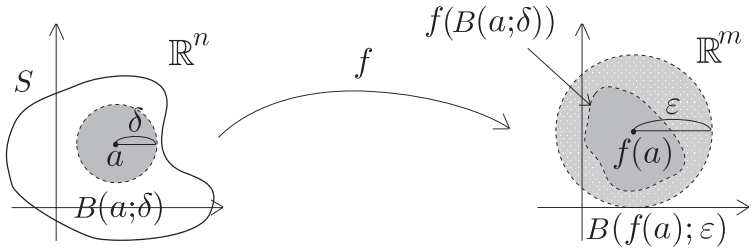
定義 14-9

集合 $S \subset \mathbb{R}^n$ 上で定義されている写像 $f : S \longrightarrow \mathbb{R}^m$ が**点** $a \in S$ **で連続** (continuous at $a \in S$) であるとは、どのような実数 $\varepsilon > 0$ に対しても、次の条件 $(*)$ を満たす実数 $\delta > 0$ が存在するときをいう。

$(*)$ $d^{(n)}(x, a) < \delta$ を満たすすべての $x \in S$ について、$d^{(m)}(f(x), f(a)) < \varepsilon$ である。

すべての点 $a \in S$ で連続なとき、f は**連続** (continuous) であるという。

注意： 上の定義の中の条件 $(*)$ は、「a との距離が δ より小さいすべての $x \in S$ について、$f(x)$ と $f(a)$ との距離は ε より小さい」ことを意味しています。言い換えれば、「a を中心とする半径 δ の開球体 $B(a; \delta) = \{\ x \in \mathbb{R}^n \mid d^{(n)}(x, a) < \delta\ \}$ と S との共通部分が、f によって、$f(a)$ を中心とする半径 ε の開球体 $B(f(a); \varepsilon) := \{\ y \in \mathbb{R}^m \mid d^{(m)}(y, f(a)) < \varepsilon\ \}$ の中に写される」ことを意味しています。



例14-10 $i=1,\cdots,n$ とし、$p_i:\mathbb{R}^n\longrightarrow\mathbb{R}$ を、各 $x=(x_1,\cdots,x_n)\in\mathbb{R}^n$ に対して、その第 i 成分 ($=x$ の左から i 番目にある実数 x_i) を対応させる写像とする：

$$p_i(x_1,\cdots,x_n)=x_i.$$

写像 p_i は連続である。p_i を $\mathbb{R}^n$ の第 i 成分への (標準) **射影** (projection) という。

(**proof**)

任意の点 $a=(a_1,\cdots,a_n)\in\mathbb{R}^n$ で連続なことを示せばよい。

任意の $\varepsilon>0$ に対して、$\delta>0$ を $\delta:=\varepsilon$ ととれば、$d^{(n)}(x,a)<\delta$ を満たすすべての $x=(x_1,\cdots,x_n)\in\mathbb{R}$ について、

$$d^{(1)}(p_i(x),p_i(a))=|x_i-a_i|\leq\sqrt{\sum_{j=1}^{n}(x_j-a_j)^2}=d^{(n)}(x,a)<\delta=\varepsilon$$

となる。よって、p_i は点 a で連続である。 □

1 変数実数値関数のときと同様にして、次を示すことができます。

命題 14-11

定義域が同一の集合 $S\subset\mathbb{R}^n$ であるような 2 つの実数値関数 $f:S\longrightarrow\mathbb{R},\ g:S\longrightarrow\mathbb{R}$ が点 $a\in S$ で連続ならば、

$$\text{和 } f+g,\ \text{差 } f-g,\ \text{積 } fg,\ \text{商 } \frac{f}{g}$$

はすべて点 a で連続である。但し、商を考えるときには、すべての $x\in S$ について $g(x)\neq0$ を満たしていると仮定する。

演習 14-6 $S_1\subset\mathbb{R}^n$ 上で定義された写像 $f:S_1\longrightarrow\mathbb{R}^m$ と $S_2\subset\mathbb{R}^m$ 上で定義された写像 $g:S_2\longrightarrow\mathbb{R}^l$ が与えられていて、この 2 つは合成可能である、すなわち、任意の $x\in S_1$ に対して $f(x)\in S_2$ が成り立っているとする。このとき、f が点 $a\in S_1$ で連続であり、g が点 $f(a)$ で連続であるならば、f と g の合成写像 $g\circ f:S_1\longrightarrow\mathbb{R}^l$ は点 a で連続であることを証明せよ。

●写像の連続性の実数値関数の連続性による言い換え

写像が連続かどうかという問題は実数値関数が連続かどうかという問題に帰着されます。

定理 14-12

$S\subset\mathbb{R}^n$ 上で定義された写像 $f:S\longrightarrow\mathbb{R}^m$ と点 $a\in S$ について、次の 2 つは同値である。

(i) f は点 a で連続である。

(ii) 各 $i=1,\cdots,m$ に対して、実数値関数

$$f_i:S\longrightarrow\mathbb{R},\quad f_i(x)=(f(x)\text{ の第 }i\text{ 成分})\qquad(x\in S)$$

は点 a で連続である。

(**proof**)
「(i) $\Longrightarrow$ (ii)」の証明：
各 $i=1,\cdots,m$ に対して、$\mathbb{R}^m$ の第 i 成分への射影を p_i とおけば、$f_i = p_i \circ f$ となっている。射影が連続であるとと演習 14-6 により、f_i は点 a で連続である。
「(ii) $\Longrightarrow$ (i)」の証明：
まず、任意の $x \in S$ に対して、

$$\begin{aligned} d^{(m)}(f(x),f(a)) &= \sqrt{\sum_{i=1}^{m}(f_i(x)-f_i(a))^2} \\ &\leq \sqrt{m}\max\{|f_1(x)-f_1(a)|,\cdots,|f_m(x)-f_m(a)|\} \end{aligned}$$

であることに注意する。
さて、任意に $\varepsilon > 0$ をとる。各 f_i は点 a で連続であるから、$\varepsilon_0 := \frac{\varepsilon}{\sqrt{m}} > 0$ に対して

$$\exists\, \delta_i > 0 \ \text{ s.t. } \ x \in S,\ d^{(n)}(x,a) < \delta_i \ \Rightarrow\ |f_i(x)-f_i(a)| < \varepsilon_0$$

となる。$\delta := \min\{\delta_1,\cdots,\delta_m\}$ とおくと、$\delta > 0$ であって、$d^{(n)}(x,a) < \delta$ を満たすすべての $x \in S$ に対して、

$$d^{(m)}(f(x),f(a)) \leq \sqrt{m}\ \max\{|f_1(x)-f_1(a)|,\cdots,|f_m(x)-f_m(a)|\} < \sqrt{m}\varepsilon_0 = \varepsilon$$

となる。故に、f は点 a で連続である。 □

上の定理を使うと、写像の連続性が定義に戻らずにわかるので便利です。最後にその例を述べて、この節を終りにしましょう。

例14-13 写像

$$f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2,\ f(x,y,z) = (y\sin(x+z), z\cos(x+y))$$

は連続であること示せ。
解；
定理 14-12 により、２つの実数値関数

$$f_1 : \mathbb{R}^3 \longrightarrow \mathbb{R},\ f_1(x,y,z) = y\sin(x+z), \quad f_2 : \mathbb{R}^3 \longrightarrow \mathbb{R},\ f_2(x,y,z) = z\cos(x+y)$$

が連続であることを調べればよい。
例えば、f_1 が連続であることは、次のようにしてわかる。
$i=1,2,3$ に対して $p_i : \mathbb{R}^3 \longrightarrow \mathbb{R}$ を第 i 成分への射影とし、$g : \mathbb{R}^3 \longrightarrow \mathbb{R}$ を

$$g(x,y,z) = \sin(x+z), \qquad (x,y,z) \in \mathbb{R}^3$$

によって定義する。$f_1 = p_2 g$ と書くことができ、さらに、$g_1 = \sin\circ(p_1+p_3)$ と書くことができる。
連続関数の和は連続であり、射影は連続であるから、p_1+p_3 は連続である。正弦関数 sin は連続なので、連続写像の合成が連続であることより、$g = \sin\circ(p_1+p_3)$ は連続である。p_2 は射影なので連続であり、連続関数の積が連続であることから、$f_1 = p_2 g$ は連続である。
同じ要領で f_2 が連続であることも証明することができる。 □

§15. 中間値の定理

中間値の定理は、有界閉区間上で定義された実数値連続関数についての３つの重要な定理のうちの１つです（残りの２つは、最大値・最小値の存在定理、一様連続性に関する定理を指します)。この節では、中間値の定理を実数の連続性に基づいて証明し、その応用として、n 乗根の存在、逆関数の連続性、指数関数の定義などを説明します。ここでの目標は、中間値の定理の重要性を、その使われ方を通して実感することです。

§15-1 中間値の定理

●中間値の定理

中間値の定理は、一言で言えば、「閉区間上で定義された連続関数 $f:[a,b]\longrightarrow\mathbb{R}$ は、$f(a)$ と $f(b)$ の間の値をすべて取る」ということを主張する定理です。

定理 15-1 (中間値の定理)

f を閉区間 $[a,b]$ 上で定義された実数値連続関数とする。

(1) $f(a)<f(b)$ のとき、次が成り立つ：

$$\gamma\in\mathbb{R},\ f(a)<\gamma<f(b)\quad\Longrightarrow\quad\exists\, c\in[a,b]\ \text{ s.t. }\ f(c)=\gamma.$$

(2) $f(b)<f(a)$ のとき、次が成り立つ：

$$\gamma\in\mathbb{R},\ f(b)<\gamma<f(a)\quad\Longrightarrow\quad\exists\, c\in[a,b]\ \text{ s.t. }\ f(c)=\gamma.$$

(**proof**)

(2) は (1) と同様に証明できるので、ここでは (1) のみ証明する。

$f(a)<\gamma<f(b)$ を満たす $\gamma\in\mathbb{R}$ を任意にとり、集合

$$A:=\{\ x\in[a,b]\mid f(x)<\gamma\ \}$$

を考える。A は $\mathbb{R}$ の空でない、上に有界な部分集合である。したがって、$\sup A$ が存在する (定理 7-9)。そこで、

$$c:=\sup A$$

とおく。$c\in[a,b]$ であって、$f(c)=\gamma$ が成り立つ。これを示す。

① $c\in[a,b]$ の証明：

$c=\sup A$ なので、A の元からなる数列 $\{x_n\}_{n=1}^{\infty}$ であって、$\lim\limits_{n\to\infty}x_n=c$ を満たすものが存在する (命題 7-10、はさみうちの原理)。各 $n\in\mathbb{N}$ について $x_n\in A\subset[a,b]$ なので、$c=\lim\limits_{n\to\infty}x_n\in[a,b]$ となる (演習 8-7)。

② $f(c)=\gamma$ の証明：

f は点 c で連続であるから、①の数列 $\{x_n\}_{n=1}^{\infty}$ について

$$f(c)=\lim_{n\to\infty}f(x_n)\le\gamma$$

が成り立つ (定理 14-8、演習 8-7)。これと $\gamma<f(b)$ により、$c\neq b$ がわかり、その結果として、任意の $n\in\mathbb{N}$ について $c<y_n$ かつ $\lim\limits_{n\to\infty}y_n=c$ を満たす $[a,b]$ 内の数列 $\{y_n\}_{n=1}^{\infty}$ が存在がわかる（例えば、$y_n=c+\frac{b-c}{n}$ とおけばよい)。c は A の上限であるから、任意の $n\in\mathbb{N}$ について $y_n\notin A$、すなわち、$f(y_n)\ge\gamma$ となる。この不等式と f の点 c での連続性により、

$$f(c)=\lim_{n\to\infty}f(y_n)\ge\gamma$$

を得る (定理 14-8、演習 8-7)。これで、$f(c)=\gamma$ が証明された。 □

演習 15-1　区間縮小法の原理 (p.54 & p.67) を使って、中間値の定理の別証明を与えよ。

ヒント：$f(a) < f(b)$ の場合、$f(a) < \gamma < f(b)$ を満たす任意の $\gamma \in \mathbb{R}$ に対して、閉区間の減少列 $[a,b] \supset [a_1,b_1] \supset [a_2,b_2] \supset \cdots\cdots$ であって、任意の $n \in \mathbb{N}$ について $f(a_n) < \gamma \leq f(b_n)$ を満たすものを以下のように帰納的に構成する。

- $f(\frac{a_{n-1}+b_{n-1}}{2}) \geq \gamma$ のとき、$a_n = a_{n-1},\ b_n = \frac{a_{n-1}+b_{n-1}}{2}$
- $f(\frac{a_{n-1}+b_{n-1}}{2}) < \gamma$ のとき、$a_n = \frac{a_{n-1}+b_{n-1}}{2},\ b_n = b_{n-1}$

演習 15-2* $n \in \mathbb{N}$, $a_1, \cdots, a_n \in \mathbb{R}$ として、関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ を

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \quad (x \in \mathbb{R})$$

によって定義する。n が奇数ならば、$f(x_0) = 0$ となる $x_0 \in \mathbb{R}$ が存在することを示せ。

ヒント：$x \neq 0$ に対して、$f(x)$ が $f(x) = x^n(\frac{a_n}{x^n} + \frac{a_{n-1}}{x^{n-1}} + \cdots + \frac{a_1}{x} + 1)$ と表わされることを使うと、数列 $\{f(k)\}_{k=1}^{\infty},\ \{f(-k)\}_{k=1}^{\infty}$ がそれぞれ $+\infty,\ -\infty$ に発散することがわかる。このことから、$f(K) > 0$ かつ $f(-K) < 0$ となる $K > 0$ の存在がわかる。閉区間 $[-K,\ K]$ 上で中間値の定理を適用する。

注意：高校数学では、どのような 3 次方程式 $x^3 + ax^2 + bx + c = 0$ (a, b, c は実定数) も実数解を持つことを、3 次関数 $f(x) = x^3 + ax^2 + bx + c$ のグラフを描いて納得せざるを得なかったのですが、ここに来て漸くこの事実に本当の意味で証明を与えることができたことになります。

●写像の像を使った中間値の定理の書き換え

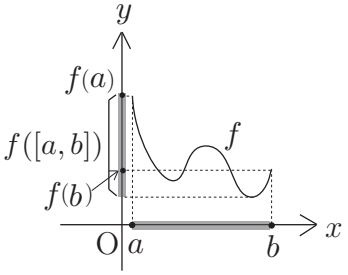
一般に、集合 A から集合 B への写像 $f : A \longrightarrow B$ と A の部分集合 S に対して、B の部分集合

$$f(S) := \{\ f(a) \mid a \in S\ \}$$

を f による S の**像** (image) といいます。特に、$f(A)$ を f の**値域** (range) と呼びます。

「像」の記号を使うと、中間値の定理を次のように簡潔に表現することができます。

定理 15-1′(中間値の定理)
f を閉区間 $[a,b]$ 上で定義された実数値連続関数とする。
(1) $f(a) < f(b)$ のとき、$[f(a), f(b)] \subset f([a,b])$ である。
(2) $f(b) < f(a)$ のとき、$[f(b), f(a)] \subset f([a,b])$ である。



● n 乗根の存在

第 14 節のユークリッド距離の定義において、**平方根** (square root) を意味する $\sqrt{\ }$ という記号を使いました。それ以前の節でも所々でこの記号を使ってきました。よく知っているように、正の実数 a の平方根 $\sqrt{a}$ とは自乗すると a になるような正の実数のことなのですが、このような実数をどんな正の実数 a に対しても考えることができるのは何故なのでしょうか。ここでは、今まで当たり前のように使って来たこの事実に、中間値の定理を使って、証明を与えましょう。

命題 15-2
自然数 n と実数 $a > 0$ に対して、$x^n = a$ となる実数 $x > 0$ が一意的に存在する。

(**proof**)

• x の存在：

$0 < a < 1$ の場合、$a = 1$ の場合、$a > 1$ の場合の 3 つに分けて示す。

① $0 < a < 1$ の場合：

関数 $f : [0,1] \longrightarrow \mathbb{R}$ を

$$f(x) = x^n - a \qquad (x \in [0,1])$$

によって定義する。f は連続である。

$f(0) = -a < 0,\ f(1) = 1 - a > 0$ であるから、中間値の定理により、$f(x) = 0$ となる $x \in [0,1]$ が存在する。この x が命題の条件を満たす実数である。

② $a = 1$ の場合：

$x = 1$ とおくと、$x^n = 1 = a$ を満たす。

③ $a > 1$ の場合：

①より、$x^n = \frac{1}{a}$ となる $x > 0$ の存在がわかる。この両辺の逆数を取って、$(\frac{1}{x})^n = a$ を得る。よって、$\frac{1}{x}$ が命題の条件を満たす実数である。

• x の一意性：

$x_1, x_2 > 0$ が $x_1^n = x_2^n = a$ を満たしていると仮定する。

もし、$x_1 \neq x_2$ ならば、$x_1 < x_2$ であるか、または、$x_2 < x_1$ である。これらの両辺は正の数なので、n 乗しても不等号の向きは変わらない。よって、$x_1^n < x_2^n$ または $x_2^n < x_1^n$ が成り立つ。しかし、いずれにしても $a < a$ が得られてしまい、矛盾が生じる。

故に、$x_1, x_2 > 0$ が $x_1^n = x_2^n = a$ を満たしていれば、$x_1 = x_2$ である。 □

命題 15-2 の x のことを a の n **乗根** (the n-th root of a) といい、$\sqrt[n]{a}$ または $a^{\frac{1}{n}}$ によって書き表わします。$\sqrt[2]{a}$ は単に $\sqrt{a}$ と書きます。

$\sqrt[n]{0} := 0$ と定めることにより、n 乗根を 0 以上のすべての実数に対して考えることができます。

●指数の有理数への拡張

0 でない任意の実数 a と任意の整数 n に対して、a の n 乗 a^n は、$n \geq 1$ のときには a を n 個掛け合わせて得られる実数を表わし、$n = 0$ のときには 1 を表わし、$n \leq -1$ のときには $\frac{1}{a}$ を $-n$ 個掛け合わせて得られる実数を表わすのでした (第 6 節, p.47 参照)。

任意の整数 n, m と 0 でない任意の実数 a, b に対して、**指数法則**

$$\text{① } a^{n+m} = a^n a^m \qquad \text{② } (a^n)^m = a^{nm} \qquad \text{③ } (ab)^n = a^n b^n$$

が成り立つことを思い出しましょう。

演習 15-3 $n, l \geq 1$ を満たす $k, l, m, n \in \mathbb{Z}$ と正の実数 a に対して、

$$\frac{m}{n} = \frac{k}{l} \quad \Rightarrow \quad (a^{\frac{1}{n}})^m = (a^{\frac{1}{l}})^k$$

次が成り立つことを示せ。

ヒント：両辺の n 乗を比較する。

上の演習問題から、有理数 r と実数 $a > 0$ に対して、実数 $a^r > 0$ が、r の分数表示 $r = \frac{m}{n}$ $(m, n \in \mathbb{Z},\ n \geq 1)$ によらずに、

$$a^r := (a^{\frac{1}{n}})^m$$

によって定まることがわかります。a^r を a の r 乗といいます。

この a^r の定義のように、数学では、表示の仕方が沢山あるもののうちの 1 つを使って、ある量や式を定義することがあります。標準的な表示を特定できない（あるいは意識的に特定しない）けれども、使った表示の仕方によらずにその量や式が定まるとき、その量や式は**矛盾なく定義されている** (well-defined) と表現します。今の場合、「a^r は矛盾なく定義されている」と言うことができます。

a^r は、その定義から、指数法則を満たすことがわかります。すなわち、任意の有理数 r, s と 0 でない任意の正の実数 a, b に対して、

$$\text{①}\ a^{r+s} = a^r a^s \qquad \text{②}\ (a^r)^s = a^{rs} \qquad \text{③}\ (ab)^r = a^r b^r$$

となることがわかります。この指数法則により、例えば、

$$(3^4)^{\frac{1}{4}} = 3^{4\cdot\frac{1}{4}} = 3^1 = 3, \qquad 2^{\frac{5}{3}} = 2^{1+\frac{2}{3}} = 2^1 2^{\frac{2}{3}} = 2(2^2)^{\frac{1}{3}} = 2\sqrt[3]{4}$$

のように計算してよいことが保証されます。

§15-2 逆関数の連続性

ここでは、中間値の定理の応用として、閉区間上で定義された連続な狭義単調関数の逆関数は連続であることを証明します。各 $x \geq 0$ に対してその n 乗根 $\sqrt[n]{x}$ を対応させる関数が連続であることは、この事実を使って証明されます。

● (狭義(きょうぎ)) 単調関数

f を $S \subset \mathbb{R}$ 上で定義された 1 変数実数値関数とします。

f が**単調増加関数** (monotone increasing function) であるとは、

$$x_1, x_2 \in S,\ x_1 \leq x_2 \quad \Rightarrow \quad f(x_1) \leq f(x_2)$$

が成り立つときをいい、f が**単調減少関数** (monotone decreasing function) であるとは、

$$x_1, x_2 \in S,\ x_1 \leq x_2 \quad \Rightarrow \quad f(x_1) \geq f(x_2)$$

が成り立つときをいいます。

f が**狭義単調増加関数** (strictly monotone increasing function) であるとは、

$$x_1, x_2 \in S,\ x_1 < x_2 \quad \Rightarrow \quad f(x_1) < f(x_2)$$

が成り立つときをいい、f が**狭義単調減少関数** (strictly monotone decreasing function) であるとは、

$$x_1, x_2 \in S,\ x_1 < x_2 \quad \Rightarrow \quad f(x_1) > f(x_2)$$

が成り立つときをいいます。

(狭義) 単調増加関数と (狭義) 単調減少関数を総称して、**(狭義) 単調関数** ((strictly) monotone function) と呼びます。

注意：教科書によっては、上で定義した狭義単調増加（減少）関数を単調増加（減少）関数と呼び、上で定義した単調増加（減少）関数を単調非減少（非増加）関数と呼んでいることがあります。読み比べるときに注意して下さい。

●1 変数実数値関数の逆関数

f を $S \subset \mathbb{R}$ 上で定義された 1 変数実数値関数とします。f が単射であるとき、任意の元 $y \in f(S)$ に対して、$y = f(x)$ となる $x \in S$ が唯一つ存在します。したがって、この場合には、関数 $f^{-1} : f(S) \longrightarrow \mathbb{R}$ を、各 $y \in f(S)$ に対して $f(x) = y$ を満たす元 $x \in S \subset \mathbb{R}$ を対応させる写像として定義することができます。この関数 f^{-1} を f の**逆関数** (inverse function) といいます。f^{-1} の値域は S になります。

例 15-3 関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ を

$$f(x) = 2x^2 + 1 \qquad (x \in \mathbb{R})$$

により定義する。f は単射でないので逆関数を持たない。

今度は $g : (-\infty, -1] \longrightarrow \mathbb{R}$ を f と同じ式によって定義される関数とする。g は単射なので逆関数を持つ。$g((-\infty, -1]) = [3, \infty)$ であるから、g の逆関数 g^{-1} は $[3, \infty)$ 上で定義されている。そして、各 $x \in [3, \infty)$ に対して $g^{-1}(x)$ は次式によって与えられる。

$$g^{-1}(x) = -\sqrt{\tfrac{x-1}{2}}.$$

●狭義単調連続関数とその逆関数の連続性

まず、次の問題を考えてみて下さい。

演習 15-4 * $S = [0, 1] \cup (2, 3]$ 上の関数 $f : S \longrightarrow \mathbb{R}$ を

$$f(x) = \begin{cases} x & (x \in [0, 1] \text{ のとき}) \\ x - 1 & (x \in (2, 3] \text{ のとき}) \end{cases}$$

によって定義する。f は単射であることに注意し、以下の問いに答えよ。

(1) f の値域 $f(S)$ はどのような集合か。具体的に書け。

(2) 逆関数 $f^{-1} : f(S) \longrightarrow \mathbb{R}$ は各 $x \in f(S)$ をどのような実数に写す関数か。$f^{-1}(x)$ を具体的に書け。

(3) f^{-1} は点 $1 \in f(S)$ で連続でないことを示せ。

上の演習問題の関数がそうであるように、単射な関数が連続であっても、その逆関数が連続であるとは限りません。しかしながら、次が成立します。

定理 15-4

閉区間 $[a, b]$ 上で定義された連続な狭義単調増加 (resp. 減少) 関数 f の逆関数 f^{-1} は、閉区間 $[f(a), f(b)]$ (resp. $[f(b), f(a)]$) 上で定義された連続な狭義単調増加 (resp. 減少) 関数である。

(**proof**)

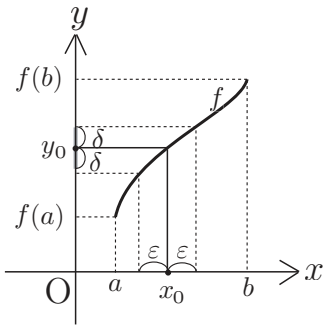
まず、狭義単調関数は単射なので、いつでも逆関数を持つことに注意する。

ここでは、f が狭義単調増加の場合を示す (狭義単調減少の場合も同様に証明することができる)。この場合には、中間値の定理により、$f([a, b]) = [f(a), f(b)]$ となることがわかる。よって、f^{-1} の定義域は閉区間 $[f(a), f(b)]$ である。

• f^{-1} の狭義単調増加性：

$y_1 < y_2$ であるような $y_1, y_2 \in f([a, b])$ を任意にとり、$x_1 = f^{-1}(y_1),\ x_2 = f^{-1}(y_2)$ とおく。f^{-1} の定義から $f(x_1) = y_1,\ f(x_2) = y_2$ である。

ここで、もし、$x_1 \geq x_2$ であったとすると、f は単調増加関数であるから、$y_1 = f(x_1) \geq f(x_2) = y_2$ となり、矛盾が生じる。よって、$x_1 < x_2$ でなければならない。故に、f^{-1} は狭義単調増加関数である。



• f^{-1} の連続性：

点 $y_0 \in f([a,b])$ を任意にとり、$x_0 = f^{-1}(y_0)$ とおく。

まず、$y_0 \neq f(a), f(b)$ のときを考える。この場合には、$(x_0 - \varepsilon_0, x_0 + \varepsilon_0) \subset [a,b]$ となる $\varepsilon_0 > 0$ が存在する。そこで、$\varepsilon_0 > \varepsilon > 0$ を満たす $\varepsilon > 0$ を任意にとり、

$$\delta := \min\{f(x_0 + \varepsilon) - y_0,\ y_0 - f(x_0 - \varepsilon)\}$$

とおく。f は狭義単調増加関数であるから、$\delta > 0$ である。このとき、$|y - y_0| < \delta$ を満たす任意の $y \in f([a,b])$ について

$$f(x_0 - \varepsilon) - y_0 \leq -\delta < y - y_0 < \delta \leq f(x_0 + \varepsilon) - y_0$$

が成り立ち、したがって、f の狭義単調増加性により、$x_0 - \varepsilon < f^{-1}(y) < x_0 + \varepsilon$、すなわち、$|f^{-1}(y) - f^{-1}(y_0)| < \varepsilon$ が成り立つことがわかる。よって、f^{-1} は $f(a), f(b)$ 以外の各点 $y_0 \in f([a,b])$ で連続である。

次に、$y_0 = f(a)$ または $y_0 = f(b)$ のときを考える。この場合には、$\frac{b-a}{2} > \varepsilon > 0$ を満たす $\varepsilon > 0$ を任意にとり、

$$\delta := \begin{cases} f(a + \varepsilon) - y_0 & (y_0 = f(a) \text{ のとき}) \\ y_0 - f(b - \varepsilon) & (y_0 = f(b) \text{ のとき}) \end{cases}$$

とおく。先ほどと同様にして、$\delta > 0$ であり、$|y - y_0| < \delta$ を満たす任意の $y \in f([a,b])$ について、$|f^{-1}(y) - f^{-1}(y_0)| < \varepsilon$ となることが示される。よって、f^{-1} は点 $f(a), f(b)$ でも連続である。以上より、f^{-1} は連続であることが示された。 □

● $\sqrt[n]{x}$ の連続性

ここでは、定理 15-4 の 1 つの応用として、次の命題を証明します。

命題 15-5

任意の $n \in \mathbb{N}$ に対して、関数 $g : [0,\infty) \longrightarrow \mathbb{R},\ \ g(x) = \sqrt[n]{x}\ \ (x \geq 0)$ は連続な狭義単調増加関数である。

(**proof**)

関数 $f : [0,\infty) \longrightarrow \mathbb{R}$ を $f(x) = x^n\ \ (x \geq 0)$ によって定めると、f は狭義単調増加関数であり、g はその逆関数である。したがって、g も狭義単調増加関数である。

g が連続であることを示すために、任意に $x_0 \in [0,\infty)$ をとり、$y_0 := \sqrt[n]{x_0}$ とおく。関数

$$f_0 : [0, y_0 + 1] \longrightarrow \mathbb{R},\ \ f_0(x) = x^n\ \ (x \in [0, y_0 + 1])$$

は閉区間上で定義された連続な狭義単調増加関数であるから、定理 15-4 により、その逆関数 $f_0^{-1} : [0, f(y_0 + 1)] \longrightarrow \mathbb{R}$ はまた連続な狭義単調増加関数となる。

$$f_0^{-1}(x) = \sqrt[n]{x} = g(x)\quad (x \in [0, f(y_0 + 1)])$$

であり、$x_0 \in [0, f(y_0 + 1))$ であるから、g は点 x_0 で連続である。 □

系 15-6

任意の $r \in \mathbb{Q}$ に対して、関数 $f : (0,\infty) \longrightarrow \mathbb{R},\ \ f(x) = x^r\ \ (x > 0)$ は連続である。

(**proof**)

$r = \frac{m}{n}$ $(m, n \in \mathbb{Z},\ n \geq 1)$ と書く。f は2つの関数

$f_1 : (0, \infty) \longrightarrow \mathbb{R}, \quad f_1(x) = \sqrt[n]{x}\ \ (x > 0)$

$f_2 : (0, \infty) \longrightarrow \mathbb{R}, \quad f_2(x) = x^m\ \ (x > 0)$

の合成である。f_1, f_2 は連続であるから、$f = f_2 \circ f_1$ も連続である。 □

演習 15-5 $a > 0$ のとき、$\lim_{n\to\infty} \sqrt[n]{a} = 1$ となることを示せ。

ヒント：$a > 1$, $a = 1$, $0 < a < 1$ の3つの場合に分けて証明する。$0 < a < 1$ の場合は逆数を考えることにより、$a > 1$ の場合に帰着される。$a > 1$ の場合には、任意の $n \in \mathbb{N}$ に対して $\sqrt[n]{a} > \sqrt[n]{1} = 1$ となるので、$\sqrt[n]{a} = 1 + b_n$ $(b_n > 0)$ とおくことができる。$a = (1 + b_n)^n \geq 1 + nb_n$ に注意して、$\lim_{n\to\infty} b_n = 0$ となることを示す。

●指数関数

15-1 節で説明したように、実数 $a > 0$ に対して、関数 $f : \mathbb{Q} \longrightarrow \mathbb{R},\ \ f(r) = a^r\ \ (r \in \mathbb{Q})$ が定まります。この関数は $\mathbb{R}$ 上の連続関数に拡張することができます。以下では、その概略を述べます（詳細は本格的な微積分学の教科書を参照して下さい)。

まず、任意の実数 x に対して、$\lim_{n\to\infty} r_n = x$ となるような**有理数列**、すなわち、各項が有理数からなる数列 $\{r_n\}_{n=1}^{\infty}$ を取ります (これが可能なことは、実数における有理数の稠密性（定理 7-3）によります)。このとき、数列 $\{a^{r_n}\}_{n=1}^{\infty}$ は収束し、かつ、その極限は $\lim_{n\to\infty} r_n = x$ となるような有理数列 $\{r_n\}_{n=1}^{\infty}$ の選び方に依らないことがわかります。このことから、$a^x \in \mathbb{R}$ を

$$a^x := \lim_{n\to\infty} a^{r_n}$$

によって矛盾なく定義することができます。

各 $x \in \mathbb{R}$ に対して $a^x \in \mathbb{R}$ を対応させる $\mathbb{R}$ から $\mathbb{R}$ への関数を $\exp_a$ と書き、a を底とする**指数関数** (exponential function) といいます。

$x \in \mathbb{Q}$ の場合には、x に収束する有理数列 $\{r_n\}_{n=1}^{\infty}$ として、$r_n = x$ $(n \in \mathbb{N})$ を取ることができるので、$\exp_a(x) = a^x$ は 15-1 節で定義された実数 a^x と一致しています。

指数関数 $\exp_a$ は次の性質を持っています。

定理 15-7 (指数関数の性質)

$a > 0$ とする。このとき、

(i) $\exp_a$ は連続であり、$\exp_a(1) = a$.

(ii) 任意の $x, y \in \mathbb{R}$ に対して $\exp_a(x + y) = \exp_a(x) \exp_a(y)$.

(iii) $a > 1$ のとき、$x < y \implies \exp_a(x) < \exp_a(y)$,
$0 < a < 1$ のとき、$x < y \implies \exp_a(y) < \exp_a(x)$.

(**proof**)

(ii) は指数関数の定義から簡単に証明できる。

(iii) を先に示す。$x < y$ となる実数 x, y を任意にとる。実数における有理数の稠密性から、$x < r < s < y$ を満たす $r, s \in \mathbb{Q}$ が存在し、さらに、$\lim_{n\to\infty} r_n = x$, $\lim_{n\to\infty} s_n = y$ となる有理数列 $\{r_n\}_{n=1}^{\infty}$, $\{s_n\}_{n=1}^{\infty}$ であって、$x < r_n < r < s < s_n < y$ $(n \in \mathbb{N})$ を満たすものが存在する。

$a > 1$ の場合には、命題 15-4 により、$a^{r_n} < a^r < a^s < a^{s_n}$ $(n \in \mathbb{N})$ であるから、

$$\exp_a(x) = a^x = \lim_{n\to\infty} a^{r_n} \leq a^r < a^s \leq \lim_{n\to\infty} a^{s_n} = a^y = \exp_a(y)$$

を得る。$0 < a < 1$ の場合も同様に証明することができる。

(i) $\exp_a(1) = a$ は指数関数の定義から直ちに従う。

$\exp_a$ が任意の $x \in \mathbb{R}$ において連続であることを示す。$\lim_{n\to\infty} x_n = x$ を満たす実数列 $\{x_n\}_{n=1}^{\infty}$ を任意にとる。$h_n = x_n - x$ $(n \in \mathbb{N})$ とおくと、$\lim_{n\to\infty} h_n = 0$ なので、

$$\forall K \in \mathbb{N},\ \exists N \in \mathbb{N}\ \text{ s.t. }\ n > N \quad \Rightarrow \quad -\tfrac{1}{K} < h_n < \tfrac{1}{K}$$

が成り立ち、さらに、(iii) を使うことにより、

$$\forall K \in \mathbb{N},\ \exists N \in \mathbb{N}\ \text{ s.t. }\ n > N \quad \Rightarrow \quad |a^{h_n} - 1| \leq |a^{\frac{1}{K}} - a^{-\frac{1}{K}}| + |a^{\frac{1}{K}} - 1|$$

が成り立つことがわかる。この事実と演習 15-5 から、$\lim_{n\to\infty} a^{h_n} = 1$ を得る (数列の極限の定義に戻って確かめよ)。さらに (ii) により、

$$\lim_{n\to\infty} a^{x_n} = \lim_{n\to\infty} (a^x a^{h_n}) = a^x \lim_{n\to\infty} a^{h_n} = a^x$$

を得る。よって、定理 14-8 により、$\exp_a$ は x において連続である。 □

性質 (i)(ii) は指数関数を特徴づけます。すなわち、次の結果が成り立ちます。

定理 15-8 (指数関数の特徴づけ)

$a > 0$ とする。関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ が連続であって、

$$f(1) = a、\text{かつ、任意の } x, y \in \mathbb{R} \text{ について } f(x+y) = f(x)f(y)$$

を満たすならば、$f = \exp_a$ である。

演習 15-6 上の定理を証明せよ。

ヒント：f, $\exp_a$ の連続性と有理数における実数の稠密性から、$\mathbb{Q}$ 上で $f = \exp_a$ となることを示せば十分である (定理 14-8 を参照)。$\mathbb{Q}$ 上で $f = \exp_a$ となること、すなわち、任意の $r \in \mathbb{Q}$ に対して $f(r) = a^r$ となることは、r が自然数、整数、有理数の場合の順で示される。

定理 15-8 から、次が導かれます。

系 15-9 (指数法則の成立)

任意の $a, b > 0,\ x, y \in \mathbb{R}$ に対して、次の指数法則が成り立つ。

$$\text{① } a^{x+y} = a^x a^y \qquad \text{② } (a^x)^y = a^{xy} \qquad \text{③ } (ab)^x = a^x b^x.$$

(**proof**)

①は指数関数の性質 (ii) から従う。

② $x \in \mathbb{R}$ を固定して、関数 $f : \mathbb{R} \longrightarrow \mathbb{R},\ \ f(y) = a^{xy}\ \ (y \in \mathbb{R})$ を考える。

これは指数関数の性質 (ii) を満たす連続関数になっている。$f(1) = a^x$ であるから、定理 15-8 により $f = \exp_{a^x}$ となり、②が成立する。

③ 今度は、関数 $g : \mathbb{R} \longrightarrow \mathbb{R},\ \ g(x) = a^x b^x\ \ (x \in \mathbb{R})$ を考える。

これは指数関数の性質 (ii) を満たす連続関数になっている。$g(1) = ab$ であるから、定理 15-8 により $g = \exp_{ab}$ となり、③が成立する。 □

§16. 複素数

複素数に関する知見は、主に 16 世紀以降— カルダノ (Cardano, 1501–1576) による 3 次方程式の解の公式や指数関数と三角関数の結びつきを記述したオイラーの公式 (1748) など—に散見されますが、その理論的基礎はガウス (Gauss, 1777–1855) によって確立されました。この節では、複素数の定義、絶対値、極形式、演算の幾何学的意味、ド・モアブルの定理などを復習します。これらの基礎概念を習得することがここでの目標です。

●複素数の定義

複素数とは、$a+bi$ $(a,b\in\mathbb{R})$ の形をした「数」のことをいいます。ここで、i は方程式 $x^2=-1$ の「解」を表わしていて、虚数単位と呼ばれます。複素数同士の計算では、多項式の計算と同じように進めて、i^2 が出て来たらそれを -1 で置き換えて計算します。例えば、$(i+2)(3i+1)$ は次のように計算します。

$$\begin{aligned}(i+2)(3i+1) &= 3i^2+(2\cdot 3+1\cdot 1)i+2\\ &= 3i^2+7i+2\\ &= 3\cdot(-1)+7i+2\\ &= 7i-1\end{aligned}$$

このように、複素数の計算原理は単純でわかりやすいものですが、複素数の定義に関しては疑問が残ります。そもそも $x^2=-1$ の「解」なるものは存在するのでしょうか？複素数に関する様々な性質を学ぶ前に、まず、複素数の定義に関するこのような疑問を解決しましょう。

実数の順序対 (a,b) 全体からなる集合 $\mathbb{R}^2$ を考え、この集合上に、二項演算 $+$ と $\times$ を次のように定義します。

$(a,b),\ (c,d)\in\mathbb{R}^2$ に対して、

$$\begin{aligned}(a,b)+(c,d) &:= (a+c,b+d)\\ (a,b)\times(c,d) &:= (ac-bd,ad+bc)\end{aligned}$$

$(a,b)\times(c,d)$ のかわりに、通常 $(a,b)\cdot(c,d)$ または $(a,b)(c,d)$ と書きます。

$\mathbb{R}^2$ を (単なる順序対の集合と考えるのではなく、) 上記の 2 つの二項演算が指定された集合と考えるとき、これを $\mathbb{C}$ という記号で表わし、その元のことを**複素数** (complex number) と呼びます。$+,\ \times$ をそれぞれ $\mathbb{C}$ における**加法**、**乗法**といいます。

演習 16-1　$\alpha=(a,b)\in\mathbb{C},\ \alpha\neq(0,0)$ に対して、$\alpha\beta=(1,0)$ となる $\beta\in\mathbb{C}$ を求めよ。

$\mathbb{C}$ における加法と乗法は、実数のときと同様に、次の性質を満たすことがわかります。

(a) 加法について次が成り立つ。

(i) **0 の存在**：$\mathbf{0}:=(0,0)$ とおくと、任意の $\alpha\in\mathbb{C}$ に対して、$\alpha+\mathbf{0}=\alpha=\mathbf{0}+\alpha$.

(ii) **結合法則**：$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ for all $\alpha,\beta,\gamma\in\mathbb{C}$.

(iii) **交換法則**：$\alpha+\beta=\beta+\alpha$ for all $\alpha,\beta\in\mathbb{C}$.

(iv) **マイナスの存在**：任意の $\alpha=(a,b)\in\mathbb{C}$ に対して、$-\alpha:=(-a,-b)\in\mathbb{C}$ を考えると、$\alpha+(-\alpha)=(-\alpha)+\alpha=\mathbf{0}$.

(b) 乗法について次が成り立つ。

(i) **1 の存在**：$\mathbf{1} := (1,0)$ とおくと、$\mathbf{1} \neq \mathbf{0}$ であって、任意の $\alpha \in \mathbb{C}$ に対して、$\mathbf{1}\cdot\alpha = \alpha = \alpha\cdot\mathbf{1}$.

(ii) **結合法則**：$(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for all $\alpha,\beta,\gamma \in \mathbb{C}$.

(iii) **交換法則**：$\alpha\beta = \beta\alpha$ for all $\alpha,\beta \in \mathbb{C}$.

(iv) **逆数の存在**：任意の $\alpha = (a,b) \in \mathbb{C},\ \alpha \neq \mathbf{0}$ に対して、$\frac{1}{\alpha} := (\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}) \in \mathbb{C}$ を考えると、$\alpha\cdot\frac{1}{\alpha} = \frac{1}{\alpha}\cdot\alpha = \mathbf{1}$.

(c) 加法と乗法の間に分配法則が成り立つ：

$\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma,\ (\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$ for all $\alpha,\beta,\gamma \in \mathbb{C}$.

複素数の減法は、任意の $\alpha,\beta \in \mathbb{C}$ に対して、

$$\alpha - \beta := \alpha + (-\beta)$$

で定義され、複素数の除法は、任意の $\alpha,\beta \in \mathbb{C},\ \beta \neq \mathbf{0}$ に対して、

$$\frac{\alpha}{\beta} = \alpha\cdot\frac{1}{\beta}$$

で定義されます。$\alpha = (a,b),\ \beta = (c,d)$ とおけば、$\alpha-\beta,\ \frac{\alpha}{\beta}$ はそれぞれ次のような複素数になります。

$$(a,b) - (c,d) = (a-c, b-d), \qquad \frac{(a,b)}{(c,d)} = \Big(\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2}\Big)$$

さてここで、$(a,0)$ という形をした複素数に注目しましょう。この形の複素数に対する和、差、積、商は

$$(a,0) \pm (b,0) = (a\pm b, 0), \quad (a,0)(b,0) = (ab,0), \quad \frac{(a,0)}{(b,0)} = \Big(\frac{a}{b}, 0\Big)$$

となることがわかります。この結果は、

$$\mathbb{R} \ni a \quad\longleftrightarrow\quad (a,0) \in \mathbb{C}$$

という対応によって、$\mathbb{C}$ の部分集合 $\{\ (a,0) \mid a \in \mathbb{R}\ \}$ と実数全体 $\mathbb{R}$ を加減乗除の演算を込めて同一視可能なことを意味しています。そこで、以下、$a \in \mathbb{R}$ に対して $(a,0) = a$ と同一視して、$\mathbb{R} \subset \mathbb{C}$ とみなすことにします。この同一視の下で、$\mathbf{0} = (0,0) = 0,\ \mathbf{1} = (1,0) = 1$ となることに注意して下さい。

次に、$(0,b)$ という形をした複素数に注目しましょう。複素数の積の定義と上で述べた同一視の約束から、

$$(0,1)(0,1) = (-1,0) = -1, \quad \text{つまり} \quad (0,1)^2 = -1$$

となります。$i := (0,1)$ とおけば、上の等式は $i^2 = -1$ と書き表わされます。さらに、任意の複素数 (a,b) は

$$(a,b) = (a,0) + (0,b) = (a,0) + (b,0)(0,1) = a + bi$$

と表わされることがわかります。i を**虚数単位** (imaginary unit) といいます。

$a+bi\ (a,b \in \mathbb{R})$ の形で、もう一度、複素数同士の加減乗除を整理しておきましょう。

$(a+bi)\pm(c+di)=(a\pm c)+(b\pm d)i$

$(a+bi)(c+di)=(ac-bd)+(bc+ad)i$

$\dfrac{a+bi}{c+di}=\dfrac{ac+bd}{c^2+d^2}+\dfrac{bc-ad}{c^2+d^2}i$ （但し、$c+di\neq 0$）

注意 1. ２つの複素数 $a+bi,\ c+di$ に対して、

$$a+bi=c+di \iff (a,b)=(c,d) \iff a=c \text{ かつ } b=d$$

が成立します (複素数の相等)。

2. 0 でない任意の複素数が逆数を持つことから、$\alpha,\beta\in\mathbb{C}$ について

$$\alpha\beta=0 \iff \alpha=0 \text{ または } \beta=0$$

となることがわかります。したがって、0 でない複素数同士の積は 0 ではありません。

●共役複素数

複素数 $\alpha=a+bi$ $(a,b\in\mathbb{R})$ に対して、複素数 $a-bi$ を α の**共役複素数** (complex conjugate number) といい、$\bar{\alpha}$ で書き表わします：

$$\bar{\alpha}=a-bi.$$

定義により、$\bar{\alpha}$ の共役複素数は α です：

$$\bar{\bar{\alpha}}=\alpha.$$

次の補題は共役をとる操作と加減乗除を行なう操作は可換なこと、つまり、共役をとってから加減乗除をしても加減乗除をしてから共役をとってもその結果得られる複素数は一緒であることを表わしています。

補題 16-1

任意の複素数 α,β に対して、

(1) $\overline{\alpha+\beta}=\bar{\alpha}+\bar{\beta}$　　(2) $\overline{\alpha-\beta}=\bar{\alpha}-\bar{\beta}$

(3) $\overline{\alpha\beta}=\bar{\alpha}\bar{\beta}$　　(4) $\overline{\left(\dfrac{\alpha}{\beta}\right)}=\dfrac{\bar{\alpha}}{\bar{\beta}}$ (但し、$\beta\neq 0$)

共役複素数を使って、実数を特徴づけることができます。

補題 16-2

複素数 α に対して、

$$\alpha\in\mathbb{R} \iff \bar{\alpha}=\alpha.$$

●実部と虚部

複素数 $\alpha=a+bi$ $(a,b\in\mathbb{R})$ に対して、a, b をそれぞれ α の**実部** (real part)、**虚部** (imarginary part) といいます。実部、虚部をそれぞれ記号で $\mathrm{Re}\alpha$, $\mathrm{Im}\alpha$ によって表わします。α の実部と虚部は、共役複素数を用いると次のように書き表わすことができます。

$$\mathrm{Re}\alpha=\frac{\alpha+\bar{\alpha}}{2},\qquad \mathrm{Im}\alpha=\frac{\alpha-\bar{\alpha}}{2i}.$$

●絶対値

複素数 $\alpha = a + bi$ $(a, b \in \mathbb{R})$ に対して、$\alpha\bar{\alpha} = a^2 + b^2$ は負でない実数です。この実数の平方根 $\sqrt{\alpha\bar{\alpha}}$ を α の**絶対値** (absolute value) といい、記号 $|\alpha|$ で表わします：

$$|\alpha| = \sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + b^2}\ .$$

定義により、任意の複素数 α に対して $|\bar{\alpha}| = |\alpha|$ が成り立ちます。

補題 16-3 (絶対値の性質)

複素数 α, β に対して、次が成り立つ。

(1) $|\alpha\beta| = |\alpha||\beta|$

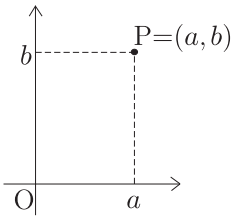
(2) $\left|\dfrac{\alpha}{\beta}\right| = \dfrac{|\alpha|}{|\beta|}$ (但し、$\beta \neq 0$)

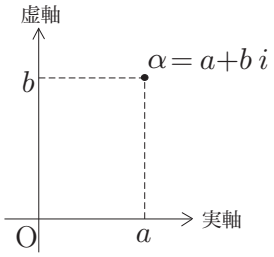
(3)(**三角不等式**) $|\alpha + \beta| \leq |\alpha| + |\beta|$

演習 16-2 上の補題の (3) を示せ。

●複素数平面

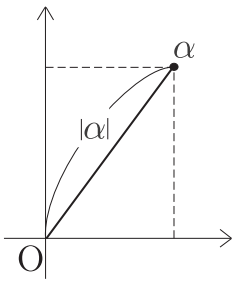
平面を 1 つ用意し、その上に直交座標系をとります（右図参照)。このとき、複素数 $\alpha = a + bi$ に対して、座標が (a, b) であるような平面上の点 P を対応させることができます。この対応によって複素数と平面上の点が 1 対 1 に対応しているので、平面上の各点に ‘ 複素数が乗っている ’ ように考えることができます。このように、複素数を図示する目的で使われる、直交座標系の与えられた平面を**複素数平面** (complex number plane) または**ガウス平面** (Gaussian plane) といいます。

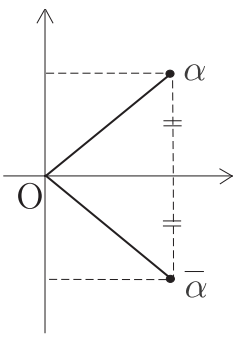




複素数平面において、第 1 座標に対応している軸（横軸）を**実軸** (real axis) といい、第 2 座標に対応している軸（縦軸）を**虚軸** (imarginary axis) といいます。今後、複素数平面上の点とそれに対応する複素数とを混同して、複素数 α と呼ぶかわりに点 α と呼んだり、左図のように書いたりします。

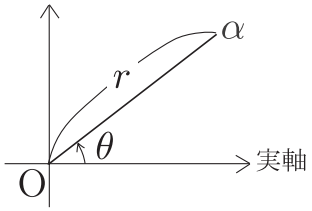
複素数 α とその共役複素数 $\bar{\alpha}$ は、複素数平面上では実軸に関して対称な位置にあり、絶対値 $|\alpha|$ は原点 O から点 α までの距離になります（下図参照)。





●極形式

0 でない複素数 α は、原点からの距離 $r = |\alpha|$ と、点 α と実軸（の正の方向）とのなす角 θ との組 (r, θ) を指定すれば定まります。組 (r, θ) を α の**極座標** (polar coordinate)、r を**動径** (radius)、θ を**偏角** (argument) といいます。通常、偏角の取り得る範囲を $[0, 2\pi)$ に限定しないため、偏角は α に対して一意的に定まりませんが、2 つ偏角の差は常に 2π の整数倍になります。α の偏角を記号 $\arg\alpha$ によって書き表わします。$\arg\alpha$ は沢山ある偏角のうちのどれか 1 つを代表していると考えます。



α $(\neq 0)$ の極座標が (r, θ) のとき、α は

$$\alpha = r(\cos\theta + i\sin\theta)$$

のように表わされます。ここで、記号

$$e^{\theta i} := \cos\theta + i\sin\theta$$

を導入すると、

$$\alpha = re^{\theta i}$$

という表示が得られます。この表示を α の**極形式** (polar form) といいます。

α $(\neq 0)$ が極形式によって $\alpha = re^{\theta i}$ $(r > 0,\ \theta \in \mathbb{R})$ と表わされるとき、$\frac{1}{\alpha}$, $\bar{\alpha}$ は $\frac{1}{\alpha} = \frac{1}{r}e^{-\theta i}$, $\bar{\alpha} = re^{-\theta i}$ のように表わされます。

演習 16-3 * 次の各複素数を極形式で表わせ。

(1) $\frac{3}{2} + \frac{3\sqrt{3}}{2}i$　　(2) $2i$　　(3) $\frac{1-i}{4}$

●複素数の和と積の幾何学的解釈

複素数同士の和や積をとる操作の下で、複素数平面上で点がどのように移動するのかを観察することにより、複素数の和と積の幾何学的な意味を知ることができます。

(1) 和

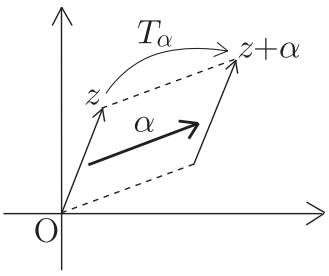
複素数 $\alpha = a + bi$ $(a, b \in \mathbb{R})$ を 1 つ固定し、複素数 z に α を加えることを考えます。$z = x + yi$ $(x, y \in \mathbb{R})$ とおくと、

$$z + \alpha = (x + a) + (y + b)i$$

となります。これより、z に α を加えることは、複素数平面上では、点 (x, y) を点 $(x+a, y+b)$ に写すことに対応していることがわかります。$(x + a, y + b)$ は位置ベクトル (x, y) をベクトル (a, b) だけ平行移動したものです。したがって、$T_\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ を、各点 $z \in \mathbb{C}$ を α だけ平行移動させる写像とすれば、

$$T_\alpha(z) = z + \alpha$$

が成り立ちます。



(2) 実数倍

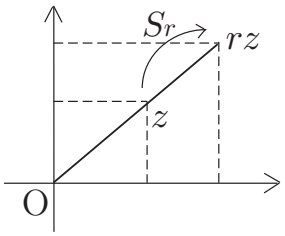
実数 r を 1 つ固定し、複素数 z を r 倍することを考えます。$z = x + yi$ $(x, y \in \mathbb{R})$ をとおくと、

$$rz = (rx) + (ry)i$$

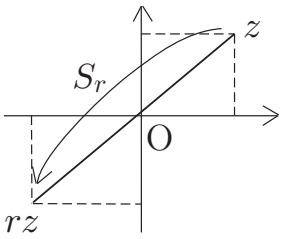
となります。これより、z を r 倍することは、複素数平面上では、点 (x, y) を点 (rx, ry) に写すことに対応していることがわかります。(rx, ry) は位置ベクトル (x, y) を r 倍に拡大したもの（注：$r < 0$ のときは、位置ベクトル (x, y) を $|r|$ 倍に拡大したのち原点に関して点対称移動したもの) です。したがって、$S_r : \mathbb{C} \longrightarrow \mathbb{C}$ を、各点 $z \in \mathbb{C}$ を r 倍に拡大させる写像とすれば、

$$S_r(z) = rz$$

が成り立ちます。



$r>0$

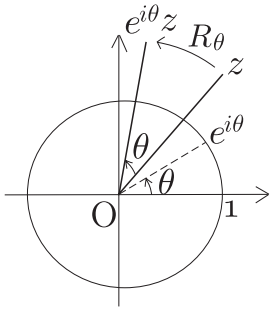


$r<0$

(3) 積

複素数 $z = x + yi$ $(x, y \in \mathbb{R})$ に複素数 $e^{\theta i} = \cos\theta + i\sin\theta$ を掛けることは、複素数平面上では、点 (x, y) を、原点を中心として反時計まわりに θ 回転した点に写すことに対応しています。これを説明します。

$R_\theta : \mathbb{C} \longrightarrow \mathbb{C}$ を、各点 $z \in \mathbb{C}$ を原点を中心に反時計まわりに $\theta \in \mathbb{R}$ だけ回転させる写像とします。このとき、幾何学的な考察から、任意の $\theta, \varphi, r \in \mathbb{R}$ と任意の $z, z_1, z_2 \in \mathbb{C}$ について、次が成立することがわかります（回転写像の性質)。



(R1) $R_{\theta+\varphi} = R_\theta \circ R_\varphi$

(R2) $R_\theta(z_1 + z_2) = R_\theta(z_1) + R_\theta(z_2)$

(R3) $R_\theta(rz) = rR_\theta(z)$

(R4) $R_\theta(1) = e^{\theta i}$

上の 4 つの性質を拠り所にして、$R_\theta(z) = e^{\theta i}z$ となることを証明します。まず、複素数 $z = x + yi$ $(x, y \in \mathbb{R})$ に対して、

$$\begin{aligned} R_{\frac{\pi}{2}}(z) &= xR_{\frac{\pi}{2}}(1) + yR_{\frac{\pi}{2}}(i) = xe^{\frac{\pi}{2}i} + yR_{\frac{\pi}{2}}(e^{\frac{\pi}{2}i}) \\ &= xi + y(R_{\frac{\pi}{2}} \circ R_{\frac{\pi}{2}})(1) = xi + yR_\pi(1) \\ &= xi + ye^{\pi i} = xi - y \\ &= iz \end{aligned}$$

となります。これより、$\theta \in \mathbb{R}$ に対して、

$$R_\theta(i) = R_\theta(e^{\frac{\pi}{2}i}) = (R_\theta \circ R_{\frac{\pi}{2}})(1) = (R_{\frac{\pi}{2}} \circ R_\theta)(1) = R_{\frac{\pi}{2}}(e^{\theta i}) = ie^{\theta i}$$

となります。以上より、

$$R_\theta(z) = xR_\theta(1) + yR_\theta(i) = xe^{\theta i} + yie^{\theta i} = e^{\theta i}z$$

が証明されました。

等式 $R_\theta(z) = e^{\theta i}z$ $(\theta \in \mathbb{R},\ z \in \mathbb{C})$ に $z = e^{\varphi i}$ を代入して (R1)(R4) を使うと、次の公式 (指数法則) が得られます。

$$e^{(\theta+\varphi)i} = e^{\theta i}e^{\varphi i} \qquad (\theta, \varphi \in \mathbb{R})$$

さらに、上式の両辺を $a + bi$ の形に書き直すと、三角関数の**加法公式**

$$\sin(\theta + \varphi) = \sin\theta\cos\varphi + \cos\theta\sin\varphi$$
$$\cos(\theta + \varphi) = \cos\theta\cos\varphi - \sin\theta\sin\varphi$$

が得られます。

●ド・モアブルの定理 (de Moivre's Theorem)

指数法則

$$e^{(\theta+\varphi)i} = e^{\theta i}e^{\varphi i} \qquad (\theta, \varphi \in \mathbb{R})$$

を繰り返し用いて、任意の実数 θ と任意の自然数 n に対して、

$$\begin{aligned} e^{(n\theta)i} &= e^{((n-1)\theta+\theta)i} = e^{(n-1)\theta i}e^{\theta i} \\ &= e^{((n-2)\theta+\theta)i}e^{\theta i} = e^{(n-2)\theta i}e^{\theta i}e^{\theta i} = e^{(n-2)\theta i}(e^{\theta i})^2 \\ &= \cdots\cdots = (e^{\theta i})^n \end{aligned}$$

となることがわかります (厳密には数学的帰納法を用います)。定義により、

$$e^{(n\theta)i} = \cos n\theta + i\sin n\theta,$$
$$(e^{\theta i})^n = (\cos\theta + i\sin\theta)^n$$

なので、次の等式が得られました。

命題 16-4 (ド・モアブルの定理)

任意の $\theta \in \mathbb{R}$ と任意の $n \in \mathbb{N}$ に対して、

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

演習 16-4　ド・モアブルの定理を使って、2 倍角の公式、3 倍角の公式を導け（すなわち、$n = 2, 3$ に対して、$\cos n\theta,\ \sin n\theta$ を $\cos\theta,\ \sin\theta$ の多項式として表わせ)。

●1 の n 乗根

自然数 n に対して、$z^n = 1$ となる複素数 z を 1 の n **乗根**といいます。n 乗すると 1 になる実数は多くても 2 個しかありません (詳しくは、n が偶数のときは 2 個、n が奇数のときは 1 個あります) が、複素数の範囲内には n 個存在します。実際、

(※)
$$1,\ e^{\frac{2\pi}{n}i},\ e^{\frac{4\pi}{n}i},\ e^{\frac{6\pi}{n}i}, \cdots, e^{\frac{2(n-1)\pi}{n}i}$$

はどれも 1 の n 乗根であり、逆に、1 の n 乗根は上のいずれかに一致することがわかります。なぜなら、z を 1 の n 乗根とすると、$|z|^n = |z^n| = 1$ ですが、$|z|$ は 0 以上の実数なので、$|z| = 1$ になります。これより、z を極形式により、

$$z = e^{\theta i} \quad (0 \leq \theta < 2\pi)$$

のように表わすことができます。指数法則により、$e^{n\theta i} = z^n = 1 = e^{i0}$ が成立するので、偏角を比較して、

$$n\theta = 2\pi k \quad (k \in \mathbb{Z})$$

つまり、

$$\theta = \frac{2\pi k}{n}$$

と書けることがわかります。$0 \leq \theta < 2\pi$ なので、整数 k は $0, 1, \cdots, n-1$ のいずれかでなければなりません。こうして、1 の n 乗根 z は $z = e^{\frac{2k\pi}{n}i}$ $(k = 0, 1, \cdots, n-1)$ のように表わされる、すなわち、(※) のいずれかに一致することが証明されました。

演習 16-5* $n = 3, 4, 6, 8$ に対して 1 の n 乗根を複素数の範囲内で求めよ。また、$n = 3, 4, 6, 8$ の各場合について、それらを複素数平面上に図示し、それらを頂点とする図形がどのような多角形になるかを答えよ。

演習 16-6 $\zeta \in \mathbb{C}$ を 1 の n 乗根とするとき、$\dfrac{1}{n}\displaystyle\sum_{k=0}^{n-1} \zeta^k$ を求めよ ($\zeta = 1$ のときとそうでないときに場合分けして計算する必要がある)。

上では 1 の n 乗根について考えましたが、より一般に、0 でない複素数 α に対して n 乗根を考えることができます。α の n **乗根**とは、$z^n = \alpha$ を満たす複素数 z のことをいいます。実数のときには、負の数の平方根 (= 2 乗根) を考えることができなかったのですが、数の範囲を複素数に広げることにより、どのような負の数についても平方根を考えることができるようになります。そればかりでなく、0 でない任意の複素数 α に対して、α の n 乗根は (複素数の範囲内に) n 個存在することがわかります。実際、α を $\alpha = re^{i\theta}$ $(r > 0,\ \theta \in \mathbb{R})$ のように極形式で表わすとき、α の n 乗根は $z_0, z_1, \cdots, z_{n-1}$ によって与えられます。但し、$k \in \mathbb{Z}$ に対して、

$$z_k = \sqrt[n]{r}\, e^{(\frac{\theta}{n} + \frac{2\pi k}{n})i}$$

とします。

注意：正の実数 a に対しては、r を有理数として、a の r 乗 a^r を定義することができました (第 15 節を参照)。そして、この「有理数乗」は次の指数法則を満たすのでした：任意の有理数 r, s と 0 でない任意の正の実数 a, b に対して、

$$\text{① } a^{r+s} = a^r a^s \qquad \text{② } (a^r)^s = a^{rs} \qquad \text{③ } (ab)^r = a^r b^r.$$

0 でない複素数 α には n 乗根が存在するので、α の有理数乗が定義され、上と同様の指数法則が成り立つのではないか、と思うかもしれません。しかし、残念ながら、上手くいきません。例えば、$(-1)^{2\cdot\frac{1}{2}} = (-1)^1 = -1$ ですが、これは $((-1)^2)^{\frac{1}{2}} = 1^{\frac{1}{2}} = 1$ に一致しません。このようなことが起きる原因は複素数の n 乗根が一つに定まらないことにあります（1 の平方根 $1^{\frac{1}{2}}$ は複素数の範囲では 2 つ存在し、$1^{\frac{1}{2}}$ はその両方を代表するためです)。

§17. 多項式

高校では文字を含んだ式のことを整式と呼ぶことが多かったかもしれませんが、大学では多項式と呼ぶ方が一般的です。この節では、多項式の定義とその演算 (和と積) について反省します。そして、差積と呼ばれる特別な多項式への置換の作用を考えることにより、第 12 節で紹介した定理 12-10 を証明します。ここでの目標は多項式の定義とその演算についての基礎を身につけることです。

この節では、$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ のいずれかとします。

§17-1 1 変数多項式

ここでは、1 変数多項式を構成的に定義して、その和と積の定義を再確認します。

● 1 変数多項式の定義

文字 X を**不定元** (indeterminate) とする $\mathbb{K}$-係数**多項式** (polynomial) とは、

$$2+X, \quad 1+(-3)X+X^2, \quad 1+(-1)X+X^2+(-1)X^3$$

のように、0 以上のある整数 d と $\mathbb{K}$ の元 $a_0, a_1, \cdots, a_d$ により

$$a_0+a_1X+a_2X^2+\cdots+a_dX^d \tag{17-1}$$

の形に表わされる‘式’のことをいいます。ここで記号 $+$ が使われていますが、この段階では $+$ は単なる形式的な記号であって、「和」の意味はありません。このことは、多項式 (17-1) は有限数列 $a_0, a_1, \cdots, a_d$ と実質的に同じものであるということを意味しています。

(17-1) の多項式を f とおくとき、$a_i \in \mathbb{K}$ $(0 \leq i \leq d)$ を多項式 f における X^i の**係数** (coefficient)、あるいは単に、係数といいます。a_0 は**定数項**とも呼ばれます。便宜上、$i > d$ を満たす任意の整数 i に対して、f における X^i の係数を 0 と定めます。このように約束することにより、f における X^i の係数が 0 以上のすべての整数 i について定義されます。

注意：1. (17-1) において $d=0$ の場合は、単に、a_0 となります。これも多項式です。このような多項式を定数多項式と呼びます。

2. 多項式 (17-1) を $\sum_{i=0}^{d} a_iX^i$ のように書くことがあります。ここで用いられている和の記号 $\sum$ も、「$+$」と同様に、形式和を表わしています。

3. (17-1) は、正確には

$$a_0X^0+a_1X^1+a_2X^2+\cdots+a_dX^d$$

のように書かれるべきものです。記号が繁雑になることを避けるために、X^0 を略し、X^1 を X と略記しています。

4. aX^i $(a \in \mathbb{K},\ 0 \leq i \in \mathbb{Z})$ という形の‘式’を**単項式** (monomial) と呼びます。多項式とは単項式 a_iX^i $(0 \leq i \leq d)$ を $+$ という記号でつなげて表わされる式のことである、と言い換えることができます。単項式 $1X^i$ を単に X^i と略記します。

5. $1-3X+X^2$ のように、多項式の表記において、単項式 a_iX^i のいくつかを「$-$」でつなげた表記も許すことにします。「$-$」でつなげた部分は $+(-a_i)X^i$ のように解釈します。例えば、$1-3X+X^2$ は $1+(-3)X+X^2$ という多項式を表わしていると読み替えます。

6. 多項式 f の不定元が X であることを強調したいときには $f(X)$ という表記を使います。この表記では X を f で写した像のように見えてしまうので、注意が必要です。多項式はあくまでも式であって、関数（写像）ではありません。

●多項式の相等

X を不定元とする２つの $\mathbb{K}$-係数多項式

$$f : a_0 + a_1X + \cdots + a_dX^d,$$
$$g : b_0 + b_1X + \cdots + b_{d'}X^{d'}$$

が**等しい**とは、0 以上のすべての整数 i について、f における X^i の係数と g における X^i の係数が等しい、すなわち、$a_i = b_i$ となるときをいいます (但し、$i > d,\ j > d'$ に対しては $a_i = 0,\ b_j = 0$ と約束します)。多項式 f, g が等しいことを $f = g$ と書き表わします。

この約束により、係数がすべて 0 であるような多項式 $0 + 0X + 0X^2 + \cdots + 0X^d$ はいずれも定数多項式 0 （つまり、$0X^0$ という多項式）に等しいことがわかります。

X を不定元とする $\mathbb{K}$-係数多項式の全体からなる集合を $\mathbb{K}[X]$ という記号で表わします：

$$\mathbb{K}[X] = \{\ a_0 + a_1X + a_2X^2 + \cdots + a_dX^d \mid a_0, a_1, a_2, \cdots, a_d \in \mathbb{K},\ d \in \mathbb{Z},\ d \geq 0\ \}.$$

●多項式の和

２つの多項式 $f, g \in \mathbb{K}[X]$ に対して、各 X^i $(i \geq 0)$ の係数の和をとって、新しい多項式 $f \boldsymbol{+} g \in \mathbb{K}[X]$ を作ることができます。この多項式 $f \boldsymbol{+} g$ を f と g の**和**といいます。

例 17-1　２つの多項式 $f = a_0 + a_1X + a_2X^2 + a_3X^3,\ g = b_0 + b_1X + b_2X^2$ に対して、
$$f \boldsymbol{+} g = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + a_3X^3\ .$$

$\mathbb{K}[X]$ における和 $\boldsymbol{+}$ は結合法則、交換法則を満たすことが簡単に確かめられます。

単項式 aX^i $(a \in \mathbb{K},\ i \geq 0)$ を $0 + 0X + \cdots + 0X^{i-1} + aX^i$ という $\mathbb{K}$-係数多項式と同一視すれば、多項式として

$$a_0 + a_1X + \cdots + a_{d-1}X^{d-1} + a_dX^d = a_0 \boldsymbol{+} a_1X \boldsymbol{+} \cdots \boldsymbol{+} a_{d-1}X^{d-1} \boldsymbol{+} a_dX^d$$

となることがわかります。これは、最初に多項式を定義するために使った記号 $+$ を後から定義した多項式の和 $\boldsymbol{+}$ と考えてよい、ということを意味しています。そこで、以後、$+$ に太字の $\boldsymbol{+}$ の意味も持たせることにして、太字の $\boldsymbol{+}$ を使わないことにします。

●多項式の積

X を不定元とする $\mathbb{K}$-係数多項式の全体 $\mathbb{K}[X]$ には、次の２条件を満たすような積（= 二項演算）が一意的に定義されます。

(i) 分配法則が成り立つ。すなわち、任意の $f, g, h \in \mathbb{K}[X]$ に対して、

$$f(g + h) = fg + fh, \quad (f + g)h = fh + gh.$$

(ii) 単項式同士の積は次で与えられる：

$$aX^i \cdot bX^j = abX^{i+j}.$$

例 17-2　2つの多項式 $f = a_0 + a_1X + a_2X^2,\ g = b_0 + b_1X + b_2X^2$ の積 fg は、上の (i) と (ii) を繰り返し用いることにより、

$$\begin{aligned} fg &= (a_0 + a_1X + a_2X^2)(b_0 + b_1X + b_2X^2) \\ &= a_0 \cdot (b_0 + b_1X + b_2X^2) + a_1X \cdot (b_0 + b_1X + b_2X^2) + a_2X^2 \cdot (b_0 + b_1X + b_2X^2) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + (a_1b_2 + a_2b_1)X^3 + a_2b_2X^4 \\ &= \sum_{k=0}^{4}(\sum_{i=0}^{k} a_ib_{k-i})X^k \end{aligned}$$

であることがわかる。但し、最後の式では $a_3 = a_4 = b_3 = b_4 = 0$ と約束している。　□

上の例と同様の計算により、一般に、2つの多項式 $f = \sum_{i=0}^{m} a_iX^i,\ g = \sum_{i=0}^{n} b_iX^i$ に対して、その積は

$$fg = (\sum_{i=0}^{m} a_iX^i)(\sum_{j=0}^{n} b_jX^j) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_ib_jX^{i+j} = \sum_{k=0}^{n+m}(\sum_{i+j=k} a_ib_j)X^k$$

によって与えられることがわかります。但し、$i > m$ に対して $a_i = 0$、$j > n$ に対して $b_j = 0$ と定め、和 $\sum_{i+j=k}$ は $i+j = k$ かつ $0 \le i \le m,\ 0 \le j \le n$ となるようなすべての整数の組 (i, j) にわたってとります。

多項式の積は交換法則、結合法則を満たすことが確かめられます。

演習 17-1* すべての自然数 n について次の等式が成り立つことを数学的帰納法を用いて証明せよ。

$$(X+1)^n = \sum_{r=0}^{n} \binom{n}{r} X^r \qquad \text{但し、} \binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

§17-2 多変数多項式

17-1 節で説明した 1 変数多項式に関する事柄は多変数の場合にそのまま拡張することができます。ここでは、まずこのことを述べてから、n 変数多項式の全体からなる集合に n 文字の置換が作用することを説明します。最後にその応用として、定理 12-10 を証明します。

●単項式

n を自然数として、n 個の異なる文字を用意します。ここでは $X_1, \cdots, X_n$ という文字を使うことにしましょう。このとき、0 以上の整数 $i_1, \cdots, i_n$ の組 $(i_1, \cdots, i_n)$ と $a \in \mathbb{K}$ に対して、次の形をした‘式’

$$aX_1^{i_1} \cdots X_n^{i_n}$$

を考えることができます。この式を $X_1, \cdots, X_n$ を不定元とする**単項式** (monomial) といい、a をその**係数**といいます。単項式 $1X_1^{i_1} \cdots X_n^{i_n}$ を単に $X_1^{i_1} \cdots X_n^{i_n}$ と書きます。

●多変数多項式の定義

n 個の異なる文字 $X_1, \cdots, X_n$ を用意します。0 以上の整数の組 $(d_1, \cdots, d_n)$ が与えられ、$0 \le i_1 \le d_1, \cdots, 0 \le i_n \le d_n$ を満たす整数 $i_1, \cdots, i_n$ の各組 $(i_1, \cdots, i_n)$ に対して $\mathbb{K}$ の元 $a_{i_1 \cdots i_n}$ が定められているとき、単項式 $a_{i_1 \cdots i_n}X_1^{i_1} \cdots X_n^{i_n}$ $(0 \le i_1 \le d_1, \cdots, 0 \le i_n \le d_n)$ たち

を記号 + で結び、1 つの ‘ 式 ’ を作ることができます。この式のことを $X_1, \cdots, X_n$ を不定元とする $\mathbb{K}$-係数**多項式**といいます。この多項式を

$$\sum_{i_1=0}^{d_1} \cdots \sum_{i_n=0}^{d_n} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n} \tag{17-2}$$

のように書き表わすこともあります。

注意：1. 具体的に多項式を書く場合には、記号が繁雑になることを避けるために、X_k^0 $(k = 1, \cdots, n)$ を省き、X_l^1 $(l = 1, \cdots, n)$ を X_l と略記します。例えば、文字 X, Y を不定元とする多項式 $a_{00}X^0Y^0 + a_{10}X^1Y^0 + a_{20}X^2Y^0 + a_{01}X^0Y^1 + a_{11}X^1Y^1 + a_{21}X^2Y$ は

$$a_{00} + a_{10}X + a_{20}X^2 + a_{01}Y + a_{11}XY + a_{21}X^2Y$$

のように書きます。
2. 1 変数多項式のときと同様に、単項式 $a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$ のいくつかを「$-$」でつなげた多項式の表記も許すことにします。「$-$」でつなげた部分は $+(-a_{i_1 \cdots i_n}) X_1^{i_1} \cdots X_n^{i_n}$ のように解釈します。例えば、多項式 $1+2X-X^2+3Y+XY-3X^2Y$ は $1+2X+(-1)X^2+3Y+XY+(-3)X^2Y$ という多項式を表わしていると読み替えます。
3. 多項式 f の不定元が $X_1, \cdots, X_n$ であることを強調したい場合には、f を $f(X_1, \cdots, X_n)$ と書き表わします。
4. 和の範囲を明記する必要がない場合には、(17-2) のような $X_1, \cdots, X_n$ を不定元とする多項式を、しばしば、

$$\sum_{i_1, \cdots, i_n} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n} \quad \text{(有限和)}$$

のように略記します。

●多項式の係数

(17-2) の多項式を f とおくとき、$a_{i_1 \cdots i_n} \in \mathbb{K}$ $(0 \leq i_1 \leq d_1, \cdots, 0 \leq i_n \leq d_n)$ を多項式 f における $X_1^{i_1} \cdots X_n^{i_n}$ の**係数**、あるいは単に、係数といいます。便宜上、$0 \leq i_1 \leq d_1, \cdots, 0 \leq i_n \leq d_n$ を満たさない整数 $i_1, \cdots, i_n$ の各組 $(i_1, \cdots, i_n)$ に対しては、f における $X_1^{i_1} \cdots X_n^{i_n}$ の係数を 0 と約束しておきます。このように約束することにより、0 以上の整数からなる任意の組 $(i_1, \cdots, i_n)$ に対して、f における $X_1^{i_1} \cdots X_n^{i_n}$ の係数が定義されます。

例 17-3 X, Y を不定元とする $\mathbb{Q}$-係数多項式

$$1 + 2X - X^2 + 3Y + XY - 3X^2Y + 5Y^2 - 4XY^2 + X^2Y^2$$

において、XY^2 の係数は -4 であり、X^3 の係数は 0 である。

●多変数多項式の相等

$X_1, \cdots, X_n$ を不定元とする 2 つの $\mathbb{K}$-係数多項式 f, g が**等しい**とは、0 以上の整数からなるすべての組 $(i_1, \cdots, i_n)$ に対して、f における $X_1^{i_1} \cdots X_n^{i_n}$ の係数と g における $X_1^{i_1} \cdots X_n^{i_n}$ の係数が等しいときをいい、このことを $f = g$ と書き表わします。

例 17-4 X, Y を不定元とする 3 つの $\mathbb{Q}$-係数多項式

$$f : 1 + 2X + X^2 + Y - XY + 9X^2Y$$
$$g : 1 + 2X + X^2 + Y - XY + 9X^2Y + 0Y^2 + 0XY^2 + 0X^2Y^2$$
$$h : 1 + 2X + X^2 + Y - XY - 9X^2Y$$

について、$f = g$ であるが、$f \neq h$ である。

$X_1, \cdots, X_n$ を不定元とする $\mathbb{K}$-係数多項式全体からなる集合を $\mathbb{K}[X_1, \cdots, X_n]$ という記号で表わします：

$$\mathbb{K}[X_1, \cdots, X_n] = \left\{ \sum_{i_1=0}^{d_1} \cdots \sum_{i_n=0}^{d_n} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n} \;\middle|\; \begin{array}{l} a_{i_1 \cdots i_n} \in \mathbb{K} \ (0 \leq i_j \leq d_j, \ j = 1, \cdots, n) \\ d_1, \cdots, d_n \in \mathbb{Z}, \ d_1, \cdots, d_n \geq 0 \end{array} \right\}.$$

●多変数多項式の和

多項式 $f, g \in \mathbb{K}[X_1, \cdots, X_n]$ に対して、各単項式ごとに係数の和をとることにより、和 $f + g \in \mathbb{K}[X_1, \cdots, X_n]$ を定義することができます。$\mathbb{K}[X_1, \cdots, X_n]$ における和は結合法則と交換法則を満たしています。1 変数の場合と同様に、単項式を多項式と自然にみなすことにより、多項式の和と多項式の定義に用いた形式和を同一視することができます。

●多変数多項式の積

$X_1, \cdots, X_n$ を変数とする $\mathbb{K}$-係数多項式の全体 $\mathbb{K}[X_1, \cdots, X_n]$ には、次の条件を満たすような積が一意的に定義されます。

(i) 分配法則が成り立つ。すなわち、任意の $f, g, h \in \mathbb{K}[X_1, \cdots, X_n]$ に対して、

$$f(g + h) = fg + fh, \quad (f + g)h = fh + gh.$$

(ii) 単項式同士の積は次で与えられる：

$$aX_1^{i_1} \cdots X_n^{i_n} \cdot bX_1^{j_1} \cdots X_n^{j_n} = abX_1^{i_1 + j_1} \cdots X_n^{i_n + j_n}.$$

演習 17-2 X, Y を変数とする 2 つの $\mathbb{K}$-係数多項式 $f = \sum_{i=0}^{3} \sum_{j=0}^{3} a_{ij} X^i Y^j$, $g = \sum_{i=0}^{3} \sum_{j=0}^{3} b_{ij} X^i Y^j$ について、積 fg における $X^i Y^j$ $(0 \leq i + j \leq 3)$ の係数を求めよ。

$\mathbb{K}[X_1, \cdots, X_n]$ の積は結合法則、交換法則を満たすことが確かめられます。したがって、実数のときと同様の意味で、多項式についても積の記号 $\prod$ を使うことができます。

例 17-5

$$\begin{aligned} \prod_{1 \leq i < j \leq 3} (X_i - X_j) &= (X_1 - X_2)(X_1 - X_3)(X_2 - X_3) \\ &= (X_1^2 - (X_2 + X_3)X_1 + X_2X_3)(X_2 - X_3) \\ &= X_1^2X_2 - X_1X_2^2 + X_2X_3^2 - X_2X_3^2 + X_3^2X_1 - X_3X_1^2 \end{aligned}$$

●多変数多項式の差

多項式 $f \in \mathbb{K}[X_1, \cdots, X_n]$ における、各 $X_1^{i_1} \cdots X_n^{i_n}$ の係数 $a_{i_1 \cdots i_n}$ を $-a_{i_1 \cdots i_n}$ で置き換えて、$\mathbb{K}$-係数多項式が得られます。この多項式を $-f$ によって表わします。任意の $f \in \mathbb{K}[X_1, \cdots, X_n]$ に対して、$f + (-f) = 0$ が成立します。$f, g \in \mathbb{K}[X_1, \cdots, X_n]$ に対して、

$$f - g := f + (-g)$$

と定義して、これを f から g を引いた**差**といいます。

例 17-6 X, Y を不定元とする $\mathbb{Q}$-係数多項式

$$f = X + 2Y + 3X^2 + 4XY + 5Y^2$$
$$g = 1 - 2X + 3Y - 4X^2 + 5XY - 6Y^2 + 7X^3$$

に対して、

$$\begin{aligned} f - g &= (X + 2Y + 3X^2 + 4XY + 5Y^2) + (-1 + 2X - 3Y + 4X^2 - 5XY + 6Y^2 - 7X^3) \\ &= -1 + 3X - Y + 7X^2 - XY + 11Y^2 - 7X^3. \end{aligned}$$

●対称式と交代式

第 12 節で定義されているように、n 文字の置換とは、全単射 $\sigma : \{1, \cdots, n\} \longrightarrow \{1, \cdots, n\}$ のことであり、これを「表」

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

で表わすのでした。例えば、1 を 4 に写し、2 を 2 に写し、3 を 1 に写し、4 を 3 に写すような 4 文字の置換を $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ と表わします。

相異なる 2 つの数字 i と j だけを入れ換える置換を互換といい、記号 $(i\ j)$ によって表わしたこと、n 文字の置換の全体からなる集合 $\mathfrak{S}_n$ 上には写像の合成によって与えられる積があったことも思い出しておきましょう。

さて、n 文字の置換 $\sigma \in \mathfrak{S}_n$ と多項式 $f = f(X_1, \cdots, X_n) \in \mathbb{K}[X_1, \cdots, X_n]$ から、新たに多項式 $\sigma f \in \mathbb{K}[X_1, \cdots, X_n]$ を次のように作ることができます。

$$\sigma f := f(X_{\sigma(1)}, \cdots, X_{\sigma(n)}).$$

より詳しく書けば、σf は、$f = \sum_{i_1, \cdots, i_n} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$（有限和）と書くとき、

$$\sigma f = \sum_{i_1, \cdots, i_n} a_{i_1 \cdots i_n} X_{\sigma(1)}^{i_1} \cdots X_{\sigma(n)}^{i_n} = \sum_{i_1, \cdots, i_n} a_{i_1 \cdots i_n} X_1^{i_{\sigma^{-1}(1)}} \cdots X_n^{i_{\sigma^{-1}(n)}}$$

によって定義される多項式です。

例 17-7 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ および多項式 $f(X_1, X_2, X_3) = 1 + X_1 X_2^2 - X_2 X_3$ に対して、

$$\sigma f(X_1, X_2, X_3) = f(X_2, X_3, X_1) = 1 + X_2 X_3^2 - X_3 X_1.$$

$X_1, \cdots, X_n$ を不定元とする $\mathbb{K}$-係数多項式の中で、対称式・交代式と呼ばれる特別な性質を持つ多項式を定義しましょう。

定義 17-8

n を 2 以上の自然数とする。

(1) 多項式 $f \in \mathbb{K}[X_1, \cdots, X_n]$ が（$X_1, \cdots, X_n$ についての）**対称式** (symmetric polynomial) であるとは、任意の互換 $\sigma \in \mathfrak{S}_n$ に対して、$\sigma f = f$ となるときをいう。

(2) 多項式 $f \in \mathbb{K}[X_1, \cdots, X_n]$ が（$X_1, \cdots, X_n$ についての）**交代式** (alternating polynomial) であるとは、任意の互換 $\sigma \in \mathfrak{S}_n$ に対して、$\sigma f = -f$ となるときをいう。

例 17-9

(1) 多項式 $X_1 + X_2,\ X_1X_2$ はいずれも X_1, X_2 についての対称式である。一方、$X_1 - X_2$ は X_1, X_2 についての交代式である。

(2) 多項式 $X_1 + X_2 + X_3,\ X_1X_2 + X_2X_3 + X_3X_1,\ X_1X_2X_3$ はすべて X_1, X_2, X_3 についての対称式である。

演習 17-3 * 多項式 $\displaystyle\prod_{1 \le i < j \le 3} (X_i - X_j)$ は X_1, X_2, X_3 についての交代式であることを示せ。

●差積

n を 2 以上の自然数とします。このとき、$\mathbb{Q}$-係数多項式

$$\Delta(X_1, \cdots, X_n) := \prod_{1 \le i < j \le n} (X_i - X_j)$$

を $X_1, \cdots, X_n$ の**差積** (difference product) といいます。

演習 17-3 の結果は次のように一般化されます。

命題 17-10

差積 $\Delta = \displaystyle\prod_{1 \le i < j \le n} (X_i - X_j)$ は $X_1, \cdots, X_n$ についての交代式である。

(**proof**)

$1 \le k < l \le n$ とし、互換 $\sigma = (k\ l)$ を考える。

集合 $S := \{X_i - X_j \mid 1 \le i < j \le n\}$ は、互いに共通部分を持たない次の 4 つの部分集合 S_1, S_2, S_3, S_4 の和集合として表わすことができる。

① X_k を含み X_l を含まないもの：

$$S_1 := \{X_k - X_j \mid k < j < l\} \cup \{X_k - X_j \mid l < j \le n\} \cup \{X_i - X_k \mid 1 \le i < k\}$$

② X_l を含み X_k を含まないもの：

$$S_2 := \{X_l - X_j \mid l < j \le n\} \cup \{X_i - X_l \mid 1 \le i < k\} \cup \{X_i - X_l \mid k < i < l\}$$

③ X_k と X_l の両方を含むもの：

$$S_3 := \{X_k - X_l\}$$

④ X_k も X_l も含まないもの：

$$S_4 := \{X_i - X_j \mid 1 \le i < j \le n,\ i, j \text{ は } k \text{ でも } l \text{ でもない}\}$$

このとき、集合 $\{X_{\sigma(i)} - X_{\sigma(j)} \mid 1 \le i < j \le n\}$ は互いに共通部分を持たない次の 4 つの部分集合 S_1', S_2', S_3', S_4' の和集合になる。

$$S_1' := \{X_l - X_j \mid k < j < l\} \cup \{X_l - X_j \mid l < j \le n\} \cup \{X_i - X_l \mid 1 \le i < k\}$$

$$S_2' := \{X_k - X_j \mid l < j \le n\} \cup \{X_i - X_k \mid 1 \le i < k\} \cup \{X_i - X_k \mid k < i < l\}$$

$$S_3' := \{X_l - X_k\}$$

$$S_4' := S_4$$

したがって、

$$\begin{aligned}\sigma\Delta &= \prod_{l<j\le n}(X_l - X_j)\cdot\prod_{1\le i<k}(X_i - X_l)\cdot\prod_{l<j\le n}(X_k - X_j)\cdot\prod_{1\le i<k}(X_i - X_k)\\ &\quad\times\underline{\prod_{k<j<l}(X_l - X_j)\cdot\prod_{k<i<l}(X_i - X_k)\cdot(X_l - X_k)}\cdot\prod_{\substack{1\le i<j\le n\\ i,j\ne k,l}}(X_i - X_j)\\ &= -\Delta\end{aligned}$$

となる。よって、差積 $\Delta = \prod_{l\le i<j\le n}(X_i - X_j)$ は $X_1, \cdots, X_n$ についての交代式である。 □

演習 17-4 上の命題の証明における最後の等号を、下線部分に注目して、証明せよ。

●定理 12-10 の証明

任意の置換 σ は有限個の互換の積で書き表わすことができますが、その書き表わし方は 1 通りではありません。しかし、書き表わすのに必要な互換の個数の偶奇は σ によって決まっている、というのが定理 12-10 の主張でした。定理 12-10 の証明には次の補題を使います。

補題 17-11

$n \ge 2$ を自然数とする。任意の多項式 $f, g \in \mathbb{K}[X_1, \cdots, X_n]$ と任意の $\sigma, \tau \in \mathfrak{S}_n$ について、次が成り立つ。

(1) $\sigma(f + g) = \sigma f + \sigma g$

(2) $\sigma(fg) = (\sigma f)(\sigma g)$

(3) $\tau(\sigma f) = (\tau\sigma)f$

補題の証明は f, g が単項式である場合に帰着されます。

演習 17-5 上の補題の (3) を示せ。

(**proof of Theorem 12-10**)

置換 $\sigma \in \mathfrak{S}_n$ を次のように互換 τ_i $(i = 1, 2, \cdots, k)$ の積と互換 ρ_j $(j = 1, 2, \cdots, l)$ の積に 2 通りの形に書く：

$$\sigma = \tau_1\tau_2\cdots\tau_k = \rho_1\rho_2\cdots\rho_l.$$

このとき、命題 17-10 と補題 17-11(3) から、差積 $\Delta = \prod_{1\le i<j\le n}(X_i - X_j)$ について、

$$\sigma\Delta = \tau_1\tau_2\cdots\tau_{k-1}(\tau_k\Delta) = -\tau_1\tau_2\cdots\tau_{k-2}(\tau_{k-1}\Delta) = \cdots\cdots = (-1)^k\Delta$$

が成立する。$\sigma = \rho_1\rho_2\cdots\rho_l$ という表示を使うと、同様にして、$\sigma\Delta = (-1)^l\Delta$ がわかる。$(-1)^k\Delta = (-1)^l\Delta$ の両辺の $X_1^{n-1}X_2^{n-2}\cdots X_{n-1}$ の係数を比較して、$(-1)^k = (-1)^l$ を得る。よって、k と l の偶奇は一致する。 □

§18. 多項式の剰余と代数学の基本定理

ここでは、多項式の剰余や根に関連する定理—除法の定理、ユークリッドの互除法、代数学の基本定理など—について学びます。この節では、$\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ とします。

●多項式の次数

多項式は整数とよく似た性質を持っています。例えば、割り算を考えることはできないけれども簡約法則が成り立ったり、商や余りを考えることができたりします。これらのことに関して重要な役割を果たすのが、次数という概念です。

0 でない多項式 $f \in \mathbb{K}[X]$ は、ある整数 $n \geq 0$ と $a_0, a_1, a_2, \cdots, a_n \in \mathbb{K},\ a_n \neq 0$ を用いて、

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

のように一意的に書き表わすことができます。このとき、f を n 次（多項）式と呼びます。また、n を f の**次数** (degree) といい、これを $\deg f$ という記号で表わします。a_n を f の**最高次係数** (leading coefficient) といいます。

注意：1. 0 の次数を便宜的に $-\infty$ と定めて、すべての整数 n について $-\infty < n$ と約束する流儀もありますが、このプリントでは未定義にしておきます。
2. $n \geq 0$ を整数とするとき、多項式 f が**高々 n 次式**であるとは、$f = 0$ であるか、または $0 \leq m \leq n$ を満たすある整数 m について f が m 次式であるときをいいます。

補題 18-1
2つの多項式 $f, g \in \mathbb{K}[X]$ がどちらも 0 でないならば、積 $fg \in \mathbb{K}[X]$ も 0 でない。さらに、次数に関して次の等式が成り立つ。

$$\deg(fg) = \deg f + \deg g.$$

残念ながら、$\mathbb{K}[X]$ は割り算に関して閉じていません (つまり、多項式を多項式で割っても一般には多項式になりません)。しかしながら、上の補題より、次の簡約法則の成立がわかります。

系 18-2 ($\mathbb{K}[X]$ における簡約法則)
3つの多項式 $f, g, h \in \mathbb{K}[X]$ について次が成り立つ。

$$fg = fh,\ f \neq 0 \quad \Rightarrow \quad g = h.$$

演習 18-1 * 補題 18-1 と系 18-2 を証明せよ（ヒント： 最高次係数に着目する）。

●除法の定理

多項式についても、整数の場合と同様に、商と余りを考えることができます。

定理 18-3 (除法の定理)
任意の多項式 $f, g \in \mathbb{K}[X],\ g \neq 0$ に対して、次の条件 (i)(ii) を満たす多項式 $q, r \in \mathbb{K}[X]$ が一意的に存在する。

(i) $f = gq + r$
(ii) $0 \leq \deg r < \deg g$ または $r = 0$

(**proof**)

証明の便宜上、$\deg 0 := -1$ と定める（この証明の中だけで通用する定義）。

I. q, r の存在の証明：

$\deg f$ に関する数学的帰納法で証明する。

① $\deg f = -1$ の場合：

$f = 0$ であるから、$q := 0,\ r = 0$ とおけばよい。

② n を 0 以上の整数とし、$\deg f < n$ を満たすすべての多項式 $f \in \mathbb{K}[X]$ について、定理は成り立つと仮定する。

$\deg f = n$ を満たす任意の多項式 $f \in \mathbb{K}[X]$ を考える。

- $\deg g > n$ のときには、$q = 0,\ r = f$ とおけばよい。
- $\deg g \leq n$ のときには、

$$f = a_0 + a_1 X + \cdots + a_n X^n \qquad (a_n \neq 0,\ a_0, a_1, \cdots, a_n \in \mathbb{K})$$

と書き、$m = \deg g$ とおいて、

$$g = b_0 + b_1 X + \cdots + b_m X^m \qquad (b_m \neq 0,\ b_0, b_1, \cdots, b_m \in \mathbb{K})$$

と書く。このとき、

$$f_1 := f - \frac{a_n}{b_m} X^{n-m} g \quad \in \ \mathbb{K}[X]$$

とおくと、$\deg f_1 < n$ となる。

帰納法の仮定から、$f_1 = q_1 g + r_1$ かつ $\deg r_1 < \deg g$ を満たす多項式 $q_1, r_1 \in \mathbb{K}[X]$ が存在する。よって、

$$q := \frac{a_n}{b_m} X^{n-m} + q_1, \qquad r := r_1$$

とおけばよい。

II. q, r の一意性の証明：

f が次のように二通りに表わされたとする。

$$f = gq + r = gq' + r', \qquad \deg r,\ \deg r' < \deg g$$

このとき、$q = q'$ かつ $r = r'$ となることを証明すればよい。まず、式変形して、

$$(*) \qquad g(q - q') = r' - r$$

を得る。ここで、$q - q' \neq 0$ と仮定すると、補題 18-1 から $r' - r = g(q - q') \neq 0$ であり、

$$\max\{\deg r,\ \deg r'\} \geq \deg(r' - r) = \deg g + \deg(q - q') \geq \deg g$$

を得る。これは、$\deg r,\ \deg r' < \deg g$ に矛盾する。よって、$q = q'$ であり、したがってまた、等式 $(*)$ より $r = r'$ である。 □

定理 18-3 において、q を、f を g で割ったときの**商** (quotient) といい、r を、f を g で割ったときの**剰余** (remainder) といいます。

例 18-4 有理係数多項式 $f = X^5 - 3X - 2,\ g = X^4 + 2X^3 + 1$ に対して、f を g で割ったときの商と剰余を求めよ。

解；

$f - qg$ の次数が $\deg g = 4$ より小さくなるような多項式 $q \in \mathbb{R}[X]$ が求まればよい。

まず、f から X^5 の項を消すために Xg を引く。次に、$f - Xg = -2X^4 - 4X - 2$ から X^4 を消すために $-2g$ を引く。すると、$f - Xg + 2g = 4X^3 - 4X$ となる。これより、$q = X - 2,\ r = 4X^3 - 4X$ とおけば、$f - qg = r,\ \deg r < \deg g$ となることがわかるから、f を g で割ったときの商と剰余はそれぞれ $q = X - 2,\ r = 4X^3 - 4X$ である。 □

●最大公約数

2つの多項式 $f, g \in \mathbb{K}[X]$ に対して、$f = gh$ となる $h \in \mathbb{K}[X]$ が存在するとき、g は f の**約数** (divisor) である、あるいは、f は g で**割り切れる** (divisible)、あるいは、f は g の**倍数** (multiple) であるといい、記号で $g|f$ と書きます。

注意：1. f が g で割り切れないことを $g \nmid f$ によって表わします。
2. $f \neq 0$ ならば $g \neq 0$ であり、$\deg g \leq \deg f$ となります。
3. 多項式なのに約数、倍数と呼ぶのは少し変な気がしますが、このような呼び方（翻訳）が定着しています。英語の“divisor”“multiple”は、それぞれ“割るもの”“何倍かされたもの”という意味であり、“数”に限らず使うことができます。

例 18-5 有理数係数多項式 $f = 2X^4 + 2X^3 - X^2 + X - 1$ は、$\mathbb{Q}[X]$ において、$f = (2X^2 + 1)(X^2 + X - 1)$ と書けるので、$2X^2 + 1$ は f の約数である。また、$f = (X^2 + \frac{1}{2})(2X^2 + 2X - 2)$ とも書けるので、$X^2 + \frac{1}{2}$ も f の約数である。

上の例からわかるように、一般に、$g \in \mathbb{K}[X]$ が $f \in \mathbb{K}[X]$ の約数であれば、g に 0 でない定数 $a \in \mathbb{K}$ を掛けて得られる多項式 ag もまた f の約数になります。通常、多項式の約数・倍数を考える際には、0 でない定数倍の違いは無視します。

定理 18-6

n 個の多項式 $f_1, \cdots, f_n \in \mathbb{K}[X],\ f_1 \neq 0$ に対して、次の条件 (i)(ii) を満たす多項式 $d \in \mathbb{K}[X]$ が定数倍を除いて一意的に存在する。

(i) $d|f_i\ \ (i = 1, \cdots, n)$.

(ii) $d'|f_i\ \ (i = 1, \cdots, n)$ を満たす任意の $d' \in \mathbb{K}[X]$ について $\deg d' \leq \deg d$.

また、このような多項式 d は $\mathbb{K}[X]$ の部分集合

$$\{\ a_1 f_1 + \cdots + a_n f_n \mid a_1, \cdots, a_n \in \mathbb{K}[X]\ \}$$

の中の 0 でない次数最小の元として特徴づけられる。

条件 (i)(ii) を満たす多項式 d の中で最高次の係数が 1 のものを $f_1, \cdots, f_n$ の**最大公約数** (the greatest common divisor) という。

(**proof**)

ここでは $n = 2$ の場合に証明する（一般の場合も全く同様に証明できる）。

以下、$f = f_1,\ g = f_2$ とおく。

I. d の存在の証明：

$$I := \{\ af + bg \mid a, b \in \mathbb{K}[X]\ \}$$

とおく。$0 \neq f \in I$ であるから、I は 0 でない元を含む。したがって、I の中に、0 でない多項式 d_0 であって、次数最小のものが存在する（自然数の整列性）。この d_0 が (i)(ii) を満たすことを示す。

(i) 任意の $h \in I$ に対して $d_0|h$ となる ことから従う。詳細は演習問題とする (演習 18-2)。

(ii) $d' \in \mathbb{K}[X]$ が $d'|f$ かつ $d'|g$ を満たしているとする。すると、任意の $a, b \in \mathbb{K}[X]$ に対して、$d'|(af + bg)$ となる。したがって、任意の $h \in I$ に対して、$d'|h$ となる。$d_0 \in I$ だから、$d'|d_0$ を得る。特に、$\deg d' \leq \deg d_0$ を得る。

Ⅱ. d の一意性の証明：

条件 (i)(ii) を満たす $d \in \mathbb{K}[X]$ は、Ⅰの証明の中の d_0 と定数倍を除いて一致することを示せばよい。まず、d が (i) の条件を満たすことと Ⅰ(ii) の証明より、$d|d_0$ を得る。よって、

$$(*) \qquad d_0 = dq \quad (q \in \mathbb{K}[X])$$

と書くことができる。一方、d, d_0 は条件 (i)(ii) を満たすから、

$$(**) \qquad \deg d = \deg d_0$$

が成り立つ。$(*)(**)$ により、$q \in \mathbb{K}$ でなければならない（$d_0 \neq 0$ より $q \neq 0$ に注意）。

Ⅲ. (i)(ii) を満たす多項式が I の中の 0 でない次数最小の元として特徴づけられること：

I の中の 0 でない次数最小の元が (i)(ii) を満たすことは、Ⅰの中で証明されている。逆に、(i)(ii) を満たす多項式 d をとると、Ⅱの証明から、$d_0 = dq$ $(q \in \mathbb{K} - \{0\})$ となる。よって、$d = q^{-1}d_0 \in I$ であり、d は I の中の 0 でない次数最小の元（のうちの 1 つ）である。 □

注意：1. 条件 (i)(ii) を満たす多項式 d のことを $f_1, \cdots, f_n$ の最大公約数と呼ぶ方が一般的ですが、このプリントでは一意性を重視して、最高次の係数が 1 のものだけを最大公約数と呼ぶことにしました。

2. $d \in \mathbb{K}[X]$ を $f_1, \cdots, f_n$ の最大公約数とするとき、d は $d'|f_i$ $(i = 1, \cdots, n)$ を満たす任意の $d' \in \mathbb{K}[X]$ によって割り切れます。

3. $f_1, \cdots, f_n$ の最大公約数を $\gcd(f_1, \cdots, f_n)$ または、単に、$(f_1, \cdots, f_n)$ で表わします。

演習 18-2　上の定理の証明中の下線部分を証明せよ。

ヒント：h を d_0 で割った余りが 0 となることを示す。

0 でない多項式 $f_1, \cdots, f_n \in \mathbb{K}[X]$ の最大公約数が 1 のとき、$f_1, \cdots, f_n$ は**互いに素** (relatively prime) であるといいます。定理 18-6 により、$f_1, \cdots, f_n$ が互いに素ならば、

$$a_1 f_1 + \cdots + a_n f_n = 1$$

を満たす多項式 $a_1, \cdots, a_n \in \mathbb{K}[X]$ が存在します。

●ユークリッドの互除法

最大公約数はユークリッドの互除法を用いて求められます。

命題 18-7

0 でない多項式 $f, g \in \mathbb{K}[X]$ を、ある $q, r \in \mathbb{K}[X]$ を用いて $f = gq + r$ $(0 \leq \deg r < \deg g$ または $r = 0)$ と書くとき、次が成り立つ：

$$\gcd(f, g) = \gcd(g, r).$$

(**proof**)

f と g の最大公約数を d とおき、g と r の最大公約数を d_1 とおく。

$d|f$ かつ $d|g$ より、$d|(f-gq)$、すなわち、$d|r$ を得る。よって、$d|d_1$ を得る (定理 18-6 の証明の下注意 2 参照)。逆に、$d_1|g$ かつ $d_1|r$ より、$d_1|(gq+r)$、すなわち、$d_1|f$ を得る。よって、$d_1|d$ を得る。

以上より、$d|d_1$ かつ $d_1|d$ が得られたから、$d=cd_1 \ \ (c\in\mathbb{K}-\{0\})$ と書ける。d, d_1 の最高次係数は 1 だから $c=1$、すなわち、$d=d_1$ を得る。 □

命題 18-7 を $\deg f \geq \deg g$ の場合に適用することにより、f と g の最大公約数を求める問題が、より次数の小さい多項式 g と r の最大公約数を求める問題に帰着されることがわかります。したがって、命題 18-7 を繰り返し適用していけば、最後には割り切れる状態になり、最大公約数が求まります。このようにして最大公約数を求めるアルゴリズムを**ユークリッドの互除法** (Euclidean algorithm) といいます。

例 18-8 $f=X^5-3X-2,\ g=X^4+2X^3+1\in\mathbb{R}[X]$ の最大公約数を求めよ。

解；

$$\begin{aligned} f &= (X-2)g+4X^3-4X \\ g &= (\tfrac{1}{4}X+\tfrac{1}{2})(4X^3-4X)+X^2+2X+1 \\ 4X^3-4X &= (4X-8)(X^2+2X+1)+12X-8 \\ X^2+2X+1 &= (\tfrac{1}{12}X+\tfrac{2}{9})(12X-8)+\tfrac{25}{9} \end{aligned}$$

より、f と g の最大公約数は

$$\gcd(f,g)=\gcd(g,4X^3-4X)=\cdots=\gcd(12X-8,\frac{25}{9})=1$$

である。 □

演習 18-3* $f=X^4-12X^2-13X-12,\ g=X^3-4X^2-9X+36,\ h=X^3+2X^2-2X+3\in\mathbb{Q}[X]$ の最大公約数をユークリッドの互除法により求めよ。

ヒント：任意の $f,g,h\in\mathbb{K}[X]$ について、$\gcd(f,g,h)=\gcd(\gcd(f,g),h)$ が成り立つ。

●代入

$\mathbb{K}'$ は $\mathbb{Q},\mathbb{R},\mathbb{C}$ のうちのどれかであって、$\mathbb{K}\subset\mathbb{K}'$ を満たすものとします。このとき、多項式 $f=a_0+a_1X+\cdots+a_nX^n\in\mathbb{K}[X]$ と $\alpha\in\mathbb{K}'$ から、$\mathbb{K}'$ の元

$$f(\alpha):=a_0+a_1\alpha+\cdots+a_n\alpha^n$$

を作ることを f に α を**代入する** (substitute) といいます。

例 18-9 $\mathbb{K}=\mathbb{R},\ \mathbb{K}'=\mathbb{C}$ のときを考える。実数係数の多項式 $f(X)=X^2-3X-2\in\mathbb{R}[X]$ に複素数 $\alpha=1+i$ を代入すると、複素数

$$f(1+i)=(1+i)^2-3(1+i)-2=-i-5$$

が得られる。

$\alpha \in \mathbb{K}'$ を代入する操作を表わす写像

$$\varphi_\alpha : \mathbb{K}[X] \longrightarrow \mathbb{K}', \quad \varphi_\alpha(f) = f(\alpha) \quad (f \in \mathbb{K}[X])$$

は次の性質を持っています：任意の $f, g \in \mathbb{K}[X]$ について、

$$\text{(i) } \varphi_\alpha(f+g) = \varphi_\alpha(f) + \varphi_\alpha(g) \qquad \text{(ii) } \varphi_\alpha(fg) = \varphi_\alpha(f)\varphi_\alpha(g) \qquad \text{(iii) } \varphi_\alpha(1) = 1$$

多項式 $f \in \mathbb{K}[X]$ に対して $f(\alpha) = 0$ となる $\alpha \in \mathbb{K}'$ を f の $\mathbb{K}'$ における**根**(こん)(root) といいます。

例18-10 有理数係数の多項式 $f(X) = X^2 - 2 \in \mathbb{Q}[X]$ を考える。このとき、$f(\alpha) = 0$ となる有理数 α は存在しないので、$f(X) = X^2 - 2$ は $\mathbb{Q}$ において根を持たない。しかし、$f(\pm\sqrt{2}) = 0$ なので、$f(X)$ は $\mathbb{R}$ において根 $\pm\sqrt{2}$ を持つ。

演習 18-4* $\alpha \in \mathbb{C}$ が多項式 $f \in \mathbb{R}[X]$ の根ならば、共役複素数 $\bar{\alpha}$ も f の根であることを示せ。

●因数定理

次の補題 (因数定理) は、定数でない多項式 $f \in \mathbb{K}[X]$ が $\mathbb{K}$ 内に根 α を持てば、f は $\mathbb{K}[X]$ において $X - \alpha$ で割り切れるということを主張しています。

補題 18-11 (因数定理)

$\deg f \geq 1$ の多項式 $f(X) \in \mathbb{K}[X]$ と $\alpha \in \mathbb{K}$ について、次が成り立つ。

$$f(\alpha) = 0 \quad \Rightarrow \quad \exists\, q(X) \in \mathbb{K}[X] \ \text{ s.t. } \ f(X) = (X - \alpha)q(X)$$

(**proof**)

除法の定理より、$f(X) = (X - \alpha)q(X) + r$ を満たす $q(X) \in \mathbb{K}[X]$ と $r \in \mathbb{K}$ が存在する。$f(\alpha) = 0$ であるから、$r = 0$ とわかる。 □

系 18-12

自然数 n に対して、n 次多項式 $f \in \mathbb{K}[X]$ の $\mathbb{K}$ における根の個数は n 個以下である。

(**proof**)

n に関する数学的帰納法で証明する。

I. $n = 1$ のとき

$\mathbb{K}$-係数の 1 次多項式 f は $f = a + bX$ $(a, b \in \mathbb{K},\ b \neq 0)$ の形をしている。$b \neq 0$ より、f は $\mathbb{K}$ において唯一の根 $\alpha = -\frac{a}{b}$ を持つ。よって、1 次多項式について系の主張が成り立つ。

II. $n \in \mathbb{N}$ とし、$\mathbb{K}$-係数の任意の n 次多項式の $\mathbb{K}$ における根の個数は n 個以下であると仮定する。

$f \in \mathbb{K}[X]$ を $(n+1)$ 次多項式とする。

もし、f が $\mathbb{K}$ 内に根を持たないならば、f の $\mathbb{K}$ における根の個数は 0 個以下であり、系の主張は成立する。そこで、f が $\mathbb{K}$ 内に根を持つ場合を考える。α を f の $\mathbb{K}$ における根とする。すると、因数定理 (定理 18-11) により、f は

$$f = (X - \alpha)g \qquad (g \in \mathbb{K}[X])$$

と表わされる。補題 18-1 により $\deg g = n$ であるから、g に対して帰納法の仮定を適用して、g の $\mathbb{K}$ における根の個数は n 個以下であることがわかる。

$\beta \in \mathbb{K}$ を f の根とすると、

$$0 = f(\beta) = (\beta - \alpha)g(\beta)$$

となるので、$\beta - \alpha = 0$ または $g(\beta) = 0$ でなければならない。つまり、f の $\mathbb{K}$ における根は α かまたは g の $\mathbb{K}$ における根のいずれかでなければならない。これは、f の $\mathbb{K}$ における根の個数は $n+1$ 個以下であることを意味する。これで、任意の $(n+1)$ 次多項式についても $\mathbb{K}$ における根の個数は $n+1$ 個以下であることがわかり、帰納法が完成した。 □

系 18-12 により、n 次式 $f, g \in \mathbb{K}[X]$ が $\mathbb{K}$ に属する相異なる $n+1$ 個の元 $\alpha_0, \alpha_1, \cdots, \alpha_n$ に対して、$f(\alpha_i) = g(\alpha_i)$ $(i = 0, 1, \cdots, n)$ を満たすならば、多項式として $f = g$ であることがわかります。つまり、n 次式は相異なる $n+1$ 個の値によって決まってしまうのです。$n+1$ の元 $\beta_0, \beta_1, \cdots, \beta_n \in \mathbb{K}$ が与えられたとき、$f(\alpha_i) = \beta_i$ $(i = 0, 1, \cdots, n)$ を満たす n 次以下の多項式 $f \in \mathbb{K}[X]$ は具体的に次の式で与えられます。この式を**ラグランジュの補間式** (Lagrange's interpolation polynomial) と呼びます。

$$f := \beta_0 \frac{f_0(X)}{f_0(\alpha_0)} + \beta_1 \frac{f_1(X)}{f_1(\alpha_1)} + \cdots + \beta_n \frac{f_n(X)}{f_n(\alpha_n)}.$$

但し、各 $i = 0, 1, \cdots, n$ に対して $f_i(X) \in \mathbb{K}[X]$ は $\prod_{j=0}^{n}(X - \alpha_j)$ から因子 $X - \alpha_i$ を削除して得られる n 次式 $f_i(X) = \frac{\prod_{j=0}^{n}(X-\alpha_j)}{X-\alpha_i}$ を表わします。

演習 18-5 3 次の実数係数多項式 f であって、$f(1) = 1,\ f(2) = \sqrt{2},\ f(3) = \sqrt{3},\ f(4) = 2$ を満たすものを 1 つ求めよ。

●代数学の基本定理

$\mathbb{R}$ 係数の多項式は $\mathbb{R}$ 内に根を持つとは限りませんが、$\mathbb{C}$ 内には根を持ちます。より一般に、$\mathbb{C}$ 係数の多項式は $\mathbb{C}$ 内に必ず根を持ちます (例 18-10 の事実と比較して下さい)。この事実は、ガウスによって厳密に証明されて以後、代数学の基本定理として広く知られるようになりました。

定理 18-13 (代数学の基本定理)
$\deg f \geq 1$ の多項式 $f \in \mathbb{C}[X]$ は $\mathbb{C}$ において少なくとも 1 つの根を持つ。

代数学の基本定理の証明にはいくつかの方法が知られています。そのいずれもかなりの準備を必要としますので、ここで完全な証明を与えることは出来ませんが、回転数を用いた証明の概略を述べておきましょう。

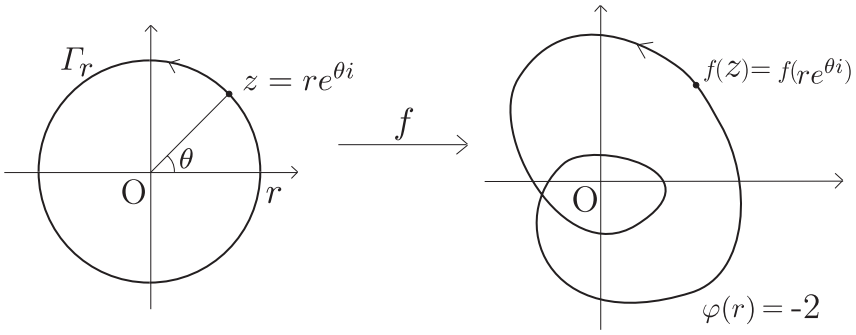
(**outline of the proof**)

背理法による。

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \qquad (a_i \in \mathbb{C},\ i = 0, 1, \cdots, n-1)$$

とおき、$f(\alpha) = 0$ を満たす $\alpha \in \mathbb{C}$ が存在しないと仮定する。

$z \in \mathbb{C}$ が原点中心半径 r の円周 Γ_r 上を反時計回りに一周するとき、$\frac{f(z)}{|f(z)|}$ が単位円周上を正味回転する回数を $\varphi(r)$ とおく（反時計回りを $+1$、時計回りを -1 と数える)。

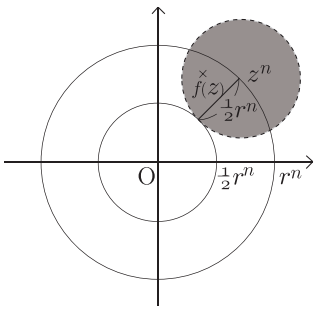


各 $z \in \mathbb{C}$ に対して $f(z) \in \mathbb{C}$ を対応させる関数は連続なので、関数 $\varphi : (0, \infty) \longrightarrow \mathbb{R}$ は連続である。(この事実は回転数を厳密に定義しなければ証明することができないので、ここでは半径 r を少しだけ変化させても回転数 $\varphi(r)$ が大きく変化しそうにないことを直感的に感じとってもらうしかない)。しかし、関数 φ の値は整数なので、中間値の定理 (定理 15-1) により、すべての $r > 0$ で $\varphi(r)$ は一定でなければならない。

(i) $r \geq \max\{1, 2(|a_{n-1}| + \cdots + |a_0|)\}$ のとき、Γ_r 上の点 $z \in \mathbb{C}$ について

$$\begin{aligned} |f(z) - z^n| &\leq |a_{n-1}|r^{n-1} + \cdots + |a_1|r + |a_0| \\ &\leq (|a_{n-1}| + \cdots + |a_1| + |a_0|)r^{n-1} \\ &\leq \frac{r^n}{2} \end{aligned}$$

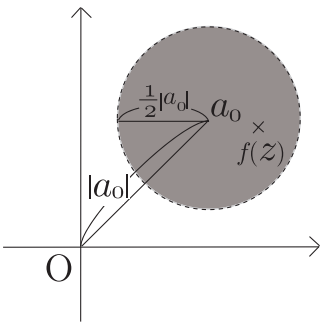
が成り立つ。z が Γ_r 上を反時計回りに一周するとき、z^n は原点のまわりを n 周する ($\because z = re^{\theta i}$ のとき $z^n = r^n e^{n\theta i}$) ので、$f(z)$ もそれにつれられて n 周する (右図参照)。したがって、r が十分大きいとき $\varphi(r) = n$ でなければならない。



(ii) $r \leq \min\{1, \frac{|a_0|}{2(1+|a_{n-1}|+\cdots+|a_1|)}\}$ のとき、Γ_r 上の点 $z \in \mathbb{C}$ について

$$\begin{aligned} |f(z) - a_0| &\leq r(r^{n-1} + |a_{n-1}|r^{n-2} + \cdots + |a_1|) \\ &\leq r(1 + |a_{n-1}| + \cdots + |a_1|) \\ &\leq \frac{|a_0|}{2} \end{aligned}$$

が成り立つので、z が Γ_r 上を反時計回りに一周するとき、$f(z)$ は原点のまわりを 0 周する (右図参照)。したがって、r が十分小さいとき、$\varphi(r) = 0$ でなければならない。



(i)(ii) は φ が定数関数でなければいけないことに矛盾する。よって、背理法の仮定は誤りであり、$f(\alpha) = 0$ を満たす $\alpha \in \mathbb{C}$ が存在する。 □

代数学の基本定理と因数定理を繰り返し用いることにより、定数でない n 次多項式 $f(X) \in \mathbb{C}[X]$ は

$$f(X) = a(X - \alpha_1) \cdots (X - \alpha_n) \qquad (a, \alpha_1, \cdots, \alpha_n \in \mathbb{C})$$

のように 1 次式の積に因数分解されることがわかります。

§19. ガウスの消去法と行列の基本変形

ガウスの消去法は連立一次方程式を解くための有用なアルゴリズムです。そのアイデアは、行列に対する基本変形という形になって、逆行列や標準形を求めるときに威力を発揮します。ここでは、逆行列や標準形の具体的な計算を通して、ガウスの消去法の有用性を実感してもらいます。そして、行列に基本変形を施す操作が、基本的な 3 種類の行列の掛け算として実現されることを学びます。この節では、$\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ とします。

§19-1 ガウスの消去法

この節では、連立一次方程式を解くための有用なアルゴリズムとして知られるガウスの消去法について説明します。後半では、そのアイデアを行列に適用し、正則行列の逆行列が単純な計算の繰り返しによって求められることを説明します。

●連立一次方程式の係数行列

$a_{ij}, b_i \in \mathbb{K}$ $(i = 1, \cdots, m,\ j = 1, \cdots, n)$ を定数とし、$x_1 \cdots, x_n$ を未知数とする連立一次方程式

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

を考えます。この連立一次方程式は行列とベクトルの積を使って、

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

のように表わすことができます。ここで、

$$A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \qquad \mathbf{x} := \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \qquad \mathbf{b} := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

です。A を連立一次方程式 $(*)$ の**係数行列** (coefficient matrix) といいます。また、行列 $(A\ \mathbf{b})$ を**拡大係数行列**といいます。$(A\ \mathbf{b})$ を $(A \mid \mathbf{b})$ と書くこともあります。

次の 3 つは、連立一次方程式を（$\mathbb{K}$ の範囲内で）解くときの基本操作です。

- 1 つの式の両辺に 0 でない数 $a \in \mathbb{K}$ を掛ける。
- 2 つの式を入れ替える (例えば、第 i 式と第 j 式を入れ替える)。
- ある式の a 倍（$a \in \mathbb{K}$）を別の式に加える。

ある連立一次方程式にこれらの基本操作を施すと、新たに連立一次方程式が得られますが、逆に、今得られた連立一次方程式に上記の基本操作を施こせば元の連立一次方程式を復元できることに注意しましょう。このことは、最初に与えらた連立一次方程式を解くことと、その連立一次方程式に上記 3 種類の基本操作を施して得られる連立一次方程式を解くことが“同値”であることを意味しています。

最初に与えらた連立一次方程式 を解く
$\xrightarrow{\text{基本操作を施す}}$
$\xleftarrow{\text{基本操作を施す}}$
新たに得られた連立一次方程式 を解く

例 19-1 連立一次方程式 $\begin{cases} 2x+3y-z=1 \\ x-2y+3z=2 \\ 4x-y+z=0 \end{cases}$ の第 1 式の -2 倍を第 3 式に加えると、

連立一次方程式

$$\begin{cases} 2x+3y-z=1 \\ x-2y+3z=2 \\ -7y+3z=-2 \end{cases}$$

が得られる。逆に、この連立一次方程式の第 1 式を 2 倍して第 3 式に加えると元の連立一次方程式が復活する。 □

上記 3 種類の操作を連立一次方程式に施すことは、(拡大) 係数行列に次の 3 種類の変形を施すことに対応しています。

(Row1) ある行に 0 でない数 $a \in \mathbb{K}$ を (一斉に) 掛ける。
(Row2) 2 つの行を入れ替える (例えば、第 i 行と第 j 行を入れ替える)。
(Row3) ある行の a 倍 ($a \in \mathbb{K}$) を他の行に加える。

これら 3 種類の変形を行列に対する**行基本変形** (elementary row operation) といいます。

●ガウスの消去法

連立一次方程式を解くための最も有効な方法に**ガウスの消去法** (Gaussian elimination) または**掃出し法** (row reduction) と呼ばれるものがあります。ガウスの消去法を一般の連立一次方程式に対して説明すると複雑になるので、ここでは、$a_{ij}, b_i \in \mathbb{K}$ $(i,j=1,2,3)$ を定数とし、x,y,z を未知数とする連立一次方程式

$$\begin{cases} a_{11}x+a_{12}y+a_{13}z=b_1 \\ a_{21}x+a_{22}y+a_{23}z=b_2 \\ a_{31}x+a_{32}y+a_{33}z=b_3 \end{cases}$$

の場合に説明します。ガウスの消去法は前進部分と後退代入の 2 つの部分からなります。

I. **前進部分**：$a_{11} \neq 0$ であるとします。このとき、第 1 式の $-\frac{a_{21}}{a_{11}}$ 倍を第 2 式に加え、第 1 式の $-\frac{a_{31}}{a_{11}}$ 倍を第 3 式に加えて、連立一次方程式

$$\begin{cases} a_{11}x+a_{12}y+a_{13}z=b_1 \\ a'_{22}y+a'_{23}z=b'_2 \\ a'_{32}y+a'_{33}z=b'_3 \end{cases} \qquad \left(\begin{array}{l} \text{但し、} \\ a'_{ij}=a_{ij}-\dfrac{a_{i1}}{a_{11}}a_{1j} \\ b'_i=b_i-\dfrac{a_{i1}}{a_{11}}b_1 \quad (i,j=2,3) \end{array} \right)$$

が得られます。与えられた連立方程式を解くことは、この連立方程式を解くことと同じです。次に、$a'_{22} \neq 0$ ならば、第 2 式の $-\frac{a'_{32}}{a'_{22}}$ 倍を第 3 式に加えて、連立一次方程式

$$\begin{cases} a_{11}x+a_{12}y+a_{13}z=b_1 \\ a'_{22}y+a'_{23}z=b'_2 \\ a''_{33}z=b''_3 \end{cases} \qquad \left(\begin{array}{l} \text{但し、} \\ a''_{33}=a_{33}-\dfrac{a'_{32}}{a'_{22}}a'_{23} \\ b''_3=b_3-\dfrac{a'_{32}}{a'_{22}}b'_2 \end{array} \right)$$

が得られます。連立方程式を解くことは、この連立方程式を解くことと同じです。

Ⅱ. **後退代入**：もし、$a''_{33} \neq 0$ ならば、最後の連立方程式は次のようにして解くことができます。まず、第 3 式から、

$$z = \frac{b''_3}{a''_{33}}$$

がわかります。これを第 2 式（を変形したもの）

$$y = \frac{b'_2 - a'_{23}z}{a'_{22}}$$

に代入して y を求めることができます。さらに、得られた z と y の値を第 1 式（を変形したもの）

$$x = \frac{b_1 - a_{12}y - a_{13}z}{a_{11}}$$

に代入して、x を求めることができます。こうして、z, y, x の順に解を求めることができます。

注意：上で述べた方法によって、いつでも連立一次方程式が解けるわけではありません。例えば、$a_{11} = 0$ のときは、上のアルゴリズムを適用することができません。しかし、$a_{i1} \neq 0$ となる i が存在するときには、第 1 式と第 i 式を交換して、上のアルゴリズムを適用することができます。このことを**枢軸の選択**といい、選ばれた a_{i1} を**枢軸** (pivot) といいます。数値計算を行う場合には、丸め誤差を小さくするために、a_{11} の値が小さいときには枢軸の選択を行う必要があります。

演習 19-1 * 次の連立一次方程式をガウスの消去法によって解け（連立一次方程式の変形の過程は、拡大係数行列の変形によって記述してよい）。

$$\begin{cases} x + y + z + 3w = -1 \\ x + 2y + 3z + w = -2 \\ x + 3y + z + 2w = 2 \\ x + 4y + 2z + w = 1 \end{cases}$$

演習 19-2 3 次実正方行列 $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ に対して、$A = LU$ となる次の形をした実正方行列 L と U を求めよ。

$$L = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

一般に、3 次正方行列 $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ を上の形をした行列 L と U の積として書くには、L と U をどのように定めればよいか。そのアルゴリズムを書け。但し、u_{11}, u_{22}, u_{33} はいずれも 0 でないとする。

●逆行列の求め方

行列の行基本変形を繰り返し用いて、逆行列を求めることができます。

定理 19-2

正則行列 $A \in \mathrm{M}_n(\mathbb{K})$ の右側に n 次単位行列 I_n を付け加えて、$(n, 2n)$-行列 $(A \mid I_n)$ を作る。この行列に 3 種類の行基本変形 (Row1)(Row2)(Row3) を有限回施して、$(I_n \mid X)$ という形の行列が得られたとする。このとき、X は A の逆行列である。

(**proof**)

$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ldots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix}$ を A の逆行列とする。$\mathbf{x}_1 = \begin{pmatrix} x_{11} \\ \vdots \\ x_{n1} \end{pmatrix}, \cdots, \mathbf{x}_n = \begin{pmatrix} x_{1n} \\ \vdots \\ x_{nn} \end{pmatrix}$ とおくと、$AX = I_n$ より、$(A\mathbf{x}_1 \ \cdots A\mathbf{x}_n) = (\mathbf{e}_1 \ \cdots \ \mathbf{e}_n)$ が成り立つ。但し、

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

とおいた。これより、A の逆行列 X は連立一次方程式 $A\mathbf{x}_j = \mathbf{e}_j$ の解 $\mathbf{x}_j$ を並べることによって得られることがわかる。連立一次方程式 $A\mathbf{x}_j = \mathbf{e}_j$ を解くには、拡大係数行列 $(A \mid \mathbf{e}_j)$ を考えて、これに 3 種類の行基本変形を繰り返して、$(I_n \mid *)$ の形にすればよい（$*$ はある縦ベクトルを表わす)。この縦ベクトル $*$ が連立一次方程式 $A\mathbf{x}_j = \mathbf{e}_j$ の解 $\mathbf{x}_j$ である。したがって、$(n, 2n)$-行列 $(A \mid \mathbf{e}_1 \ \cdots \ \mathbf{e}_n)$ に 3 種類の行基本変形を繰り返して、$(I_n \mid * \cdots *)$ の形にできれば、この行列の第 $n+1$ 列目以降からなる n 次正方行列は A の逆行列であることがわかる。 □

例 19-3 行列 $A = \begin{pmatrix} 1 & 2 & 5 \\ 1 & 4 & 7 \\ 0 & 4 & 3 \end{pmatrix} \in \mathrm{M}_3(\mathbb{Q})$ が正則ならば、その逆行列を求めよ。

解；

$(3, 6)$-行列 $(A \mid I_3)$ に行基本変形を施して、$(I_3 \mid *)$ という形の行列に変形する。

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 1 & 4 & 7 & 0 & 1 & 0 \\ 0 & 4 & 3 & 0 & 0 & 1 \end{array}\right) \xrightarrow{②+①\times(-1)} \left(\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 2 & -1 & 1 & 0 \\ 0 & 4 & 3 & 0 & 0 & 1 \end{array}\right) \xrightarrow{③+②\times(-2)}$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 2 & -1 & 1 & 0 \\ 0 & 0 & -1 & 2 & -2 & 1 \end{array}\right) \xrightarrow{③\times(-1)} \left(\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 2 & -1 & 1 & 0 \\ 0 & 0 & 1 & -2 & 2 & -1 \end{array}\right) \xrightarrow[②+③\times(-2)]{①+③\times(-5)}$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 11 & -10 & 5 \\ 0 & 2 & 0 & 3 & -3 & 2 \\ 0 & 0 & 1 & -2 & 2 & -1 \end{array}\right) \xrightarrow{②\times\frac{1}{2}} \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 11 & -10 & 5 \\ 0 & 1 & 0 & \frac{3}{2} & -\frac{3}{2} & 1 \\ 0 & 0 & 1 & -2 & 2 & -1 \end{array}\right) \xrightarrow{①+②\times(-2)}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 8 & -7 & 3 \\ 0 & 1 & 0 & \frac{3}{2} & -\frac{3}{2} & 1 \\ 0 & 0 & 1 & -2 & 2 & -1 \end{array}\right)$$

（ ⓙ+ ⓘ× a は第 j 行に第 i 行の a 倍を加える操作を表わし、ⓘ× a は第 i 行を a 倍する操作を表わす。 ）

したがって、A は正則であって、その逆行列は、$A^{-1} = \begin{pmatrix} 8 & -7 & 3 \\ \frac{3}{2} & -\frac{3}{2} & 1 \\ -2 & 2 & -1 \end{pmatrix}$ である。 □

演習 19-3* 行列 $\begin{pmatrix} 1 & 2 & -3 \\ 2 & 5 & -2 \\ 3 & 6 & -4 \end{pmatrix} \in \mathrm{M}_3(\mathbb{Q})$ が正則ならばその逆行列を求めよ。

§19-2 行列の標準形

今までは行に関する基本変形のみを考えてきました。ここでは、列に関する同様の変形も考えて、行列を標準形にすることを考えます。

●行列の階数標準形

行列の**列基本変形** (elementary column operation) とは、行列に対する次の 3 種類の操作のことをいいます。

(Column1) ある列に 0 でない数 $a \in \mathbb{K}$ を（一斉に）掛ける。
(Column2) 2 つの列を入れ替える (例えば、第 i 列と第 j 列を入れ替える)。
(Column3) ある列の a 倍 ($a \in \mathbb{K}$) を他の列に加える。

ここでは、行基本変形ばかりでなく列基本変形も施すと、どのような行列も (階数) 標準形と呼ばれる簡単な行列にすることができることを証明します。

定理 19-4

任意の行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に、行基本変形および列基本変形を有限回施すことによって、次の形の行列に変形することができる：

$$F_{m,n}(r) = \begin{pmatrix} I_r & \mathrm{O} \\ \mathrm{O} & \mathrm{O} \end{pmatrix} = \begin{pmatrix} \overbrace{\begin{matrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{matrix}}^{r} & \overbrace{\mathrm{O}}^{n-r} \\ \mathrm{O} & \mathrm{O} \end{pmatrix} \begin{matrix} \} r \\ \} m-r \end{matrix}$$

ここで、$0 \leq r \leq \min\{m, n\}$ であり、O は零行列を表わす。$F_{m,n}(r)$ を A の**階数標準形** (rank normal form)、または単に、**標準形**という。

(**proof**)

行列の行数 m に関する数学的帰納法で証明する。しかし、帰納法の第 1 段、すなわち、$m = 1$ のときに定理の主張が成り立つことの証明は、以下で述べることに本質的に含まれているので、省略する。また、$n = 1$ のときも同様の理由で証明することができるから、以下では、$m, n > 1$ であるとし、行数が $m-1$ であるような行列については定理の結果が成り立つと仮定して、行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ について定理の主張が成り立つことを証明する。

$A = \mathrm{O}$ のときはすでに標準形になっているから、$A \neq \mathrm{O}$ の場合を考えればよい。この場合、A の $(1,1)$-成分が 0 であれば、行と列の入れ替えを行って、$(1,1)$-成分が 0 でないようにすることができる。この行列に対して、(ガウスの消去法の前進部分と同様に) 第 1 行の定数倍を残りの行に加える変形を行って、次の形をした行列が得られる。

$$\begin{pmatrix} a & * & \cdots & * \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix} \quad (a \neq 0)$$

帰納法の仮定から、A' は有限回の行基本変形と列基本変形によって、$F_{m-1,n-1}(r')$ に変形される。A' を標準形 $F_{m-1,n-1}(r')$ に変形するときに行った同じ行基本変形と列基本変形を A に

施すことにより、A は次の形をした行列に変形されることがわ
かる。

$$\begin{pmatrix} a & b_2 & \cdots & b_n \\ 0 & & & \\ \vdots & & F_{m-1,n-1}(r') & \\ 0 & & & \end{pmatrix} \quad (a \neq 0)$$

$i = 2, \cdots, n$ にわたってこの行列の第 1 列の $-\frac{b_i}{a}$ 倍を第 i 列に加えていき、最後に第 1 列を $\frac{1}{a}$ 倍すれば、$F_{m,n}(r'+1)$ が得られるから、A もまた有限回の行基本変形と列基本変形により、標準形に変形される。 □

注意：定理 19-4 における r は、実は、途中の行基本変形と列基本変形の仕方によらずに定まっています。その証明と r の意味については第 21 節で説明します。

演習 19-4　3 次正方行列の標準形として、どのようなものが考えられるか。そのすべてを書き並べよ。

例 19-5　行列 $A = \begin{pmatrix} 0 & 2 & 4 & 2 \\ 1 & 2 & 3 & 1 \\ -2 & -1 & 0 & 1 \end{pmatrix}$ に基本変形を有限回施して、階数標準形にせよ。

解；

途中までは行基本変形で (ガウスの消去法を使い) 変形し、最後に列基本変形を行う。

$$A \xrightarrow{\text{①と②の入れ替え}} \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 4 & 2 \\ -2 & -1 & 0 & 1 \end{pmatrix} \xrightarrow{\text{③+①×2}} \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 4 & 2 \\ 0 & 3 & 6 & 3 \end{pmatrix}$$

$$\xrightarrow{\text{③+②×}(-\frac{3}{2})} \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 4 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{②×}\frac{1}{2}} \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow[\text{他の列に加える}]{\text{第 1 列の定数倍を}}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow[\text{他の列に加える}]{\text{第 2 列の定数倍を}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \square$$

●基本行列

行列に対する行基本変形、列基本変形という操作は、行列の積を使って説明することができます。まず、次の問題を考えてみて下さい。

演習 19-5 * 行列 $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix} \in \mathrm{M}_{34}(\mathbb{K})$ に対して、行列 A' を以下のように定めるとき、$A' = PA$ となる正則行列 P を求めよ。 但し、$t \in \mathbb{K}$, $t \neq 0$ とする。

(1) $A' =$ (A の第 2 行を t 倍したもの)

(2) $A' =$ (A の第 1 行と第 2 行を入れ換えたもの)

(3) $A' =$ (A の第 1 行の t 倍を第 3 行に加えたもの)

天下り的ですが、$t \in \mathbb{K}$, $t \neq 0$, $i \neq j$ として、次の 3 つの m 次正方行列を考えます（但し、点線部分には 1 が並び、空白の部分はすべて 0 が並んでいるとします)。

- 単位行列 I_m の (i,i)-成分を t で置き換えて得られる行列 $P_m(i;t)$

$$P_m(i;t) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & \mathrm{O} & & \\ & & 1 & & & & \\ & & & t & & & \\ & & & & 1 & & \\ & \mathrm{O} & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \quad \cdots\cdots \text{ 第 } i \text{ 行目}$$

- 単位行列 I_m の第 i 行と第 j 行を交換して得られる行列 $Q_m(i,j)$

$$Q_m(i,j) = \left(\begin{array}{ccc|ccc} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \hline & & & 0 & & 1 & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \\ & & & 1 & & & 0 \\ \hline & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{array}\right) \begin{array}{l} \\ \\ \\ \\ \cdots\cdots \text{ 第 } i \text{ 行目} \\ \\ \\ \\ \cdots\cdots \text{ 第 } j \text{ 行目} \\ \\ \\ \end{array}$$

- 単位行列 I_m の (j,i)-成分を t で置き換えて得られる行列 $R_m(i,j;t)$

$$R_m(i,j;t) = \left(\begin{array}{ccc|ccc} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \hline & & & 1 & & 0 & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \\ & & & t & & & 1 \\ \hline & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{array}\right) \begin{array}{l} \\ \\ \\ \\ \cdots\cdots \text{ 第 } i \text{ 行目} \\ \\ \\ \\ \cdots\cdots \text{ 第 } j \text{ 行目} \\ \\ \\ \end{array}$$

行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に左から $P_m(i;t)$, $Q_m(i,j)$, $R_m(i,j;t)$ を掛けることは、それぞれ、第 i 行を t 倍する変形、第 i 行と第 j 行を交換する変形、第 i 行の t 倍を第 j 行に加える変形を A に施すことに対応しています。

演習 19-6 * 行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に右から $P_n(i;t)$, $Q_n(i,j)$, $R_n(i,j;t)$ を掛けることは、それぞれ A にどのような変形を施すことに対応しているか？答えよ。

正方行列 $P_n(i;t)$, $Q_n(i,j)$, $R_n(i,j;t)$（但し、$t \in \mathbb{K}$, $t \neq 0$, $i \neq j$）を総称して、$\mathrm{M}_n(\mathbb{K})$ における**基本行列** (fundamental matrix) といいます。基本行列は正則です。実際、

$$P_n(i;t)P_n(i;t^{-1}) = P_n(i;t^{-1})P_n(i;t) = I_n,$$
$$Q_n(i,j)Q_n(i,j) = I_n,$$
$$R_n(i,j;t)R_n(i,j;-t) = R_n(i,j;-t)R_n(i,j;t) = I_n$$

となることが簡単に確認できるので、基本行列 $P_n(i;t)$, $Q_n(i,j)$, $R_n(i,j;t)$ はそれぞれ基本行列 $P_n(i;t^{-1})$, $Q_n(i,j)$, $R_n(i,j;-t)$ を逆行列として持つからです。正則行列の積は正則なので (補題 13-3(3))、以上の考察と定理 19-4 から次の定理が得られます。

定理 19-6

任意の行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に対して、$PAQ = F_{m,n}(r)$ となる 0 以上の整数 r と正則行列 $P \in \mathrm{M}_m(\mathbb{K})$ と正則行列 $Q \in \mathrm{M}_n(\mathbb{K})$ が存在する。

例 19-7 実 $(2,3)$-行列 $A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & -6 \end{pmatrix}$ について、PAQ が標準形となるような実正則行列 P と Q を求めよ。また、その標準形を求めよ。

解；

$$A \xrightarrow{②+①\times 4} \begin{pmatrix} 1 & -2 & 3 \\ 0 & -3 & 6 \end{pmatrix} \xrightarrow{②\times(-\frac{1}{3})} \begin{pmatrix} 1 & -2 & 3 \\ 0 & 1 & -2 \end{pmatrix}$$

$$\xrightarrow[③+①\times(-3)]{②+①\times 2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \end{pmatrix} \xrightarrow{③+②\times 2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\left(\begin{array}{l} \textcircled{j}+\textcircled{i}\times a \text{ , } \boxed{j}+\boxed{i}\times a \text{ はそれぞれ第 } j \text{ 行に第 } i \text{ 行の } a \text{ 倍を} \\ \text{加える操作、第 } j \text{ 列に第 } i \text{ 列の } a \text{ 倍を加える操作を表わす。} \end{array} \right)$$

なので、

$$P = \begin{pmatrix} 1 & 0 \\ 0 & -\frac{1}{3} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\frac{4}{3} & -\frac{1}{3} \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

と定めると $P \in \mathrm{M}_2(\mathbb{R})$, $Q \in \mathrm{M}_3(\mathbb{R})$ は正則であって $PAQ = F_{2,3}(2)$ となることがわかる。 □

演習 19-7 実行列 $A = \begin{pmatrix} 2 & 3 & 2 \\ 1 & 6 & 4 \\ 3 & 1 & 2 \\ 4 & 10 & 7 \end{pmatrix}$ について、PAQ が標準形となるような実正則行列 P と Q を求めよ。また、その標準形を求めよ。

§20. ベクトルの線形独立性

ここでは、連立一次方程式の解全体からなる集合を題材にして、部分空間、基底、線形独立、次元などの線形代数学の主要な概念を導入します。これらの概念を習得することがここでの目標です。この節では、$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ のいずれかとします。

●零ベクトルとベクトルの差

第 13 節で導入された数ベクトル空間 $\mathbb{K}^n$ について復習しましょう。

$\mathbb{K}^n$ は $\mathbb{K}$ の元を n 個縦に並べたもの全体からなる集合でした：

$$\mathbb{K}^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \;\middle|\; a_1 \in \mathbb{K}, \cdots, a_n \in \mathbb{K} \right\}$$

$\mathbb{K}^n$ に次のような和 $+$ と定数倍 $\cdot$ が指定されているとき、これを数ベクトル空間と呼び、$\mathbb{K}^n$ の元のことを n 次元ベクトルと呼ぶのでした：$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{K}^n$ および $t \in \mathbb{K}$ に対して、

$$\mathbf{x} + \mathbf{y} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}, \qquad t\mathbf{x} = \begin{pmatrix} tx_1 \\ \vdots \\ tx_n \end{pmatrix}.$$

$\mathbb{K}^n$ における零ベクトルとベクトルの差を定義しましょう。$\mathbb{K}^n$ における**零ベクトル** (zero vector) とは、成分がすべて 0 であるような $\mathbb{K}^n$ のベクトル $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ のことをいいます。零ベクトルを $\mathbf{0}$ によって表わします。零ベクトル $\mathbf{0}$ は、任意の $\mathbf{x} \in \mathbb{K}^n$ に対して $\mathbf{x} + \mathbf{0} = \mathbf{x} = \mathbf{0} + \mathbf{x}$ を満たす $\mathbb{K}^n$ のベクトルとして特徴づけられます。

ベクトル $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ に対して、

$$-\mathbf{x} := (-1)\mathbf{x} = \begin{pmatrix} -x_1 \\ \vdots \\ -x_n \end{pmatrix}$$

と定めます。$\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$ が成立します。また、$\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$ に対して、

$$\mathbf{x} - \mathbf{y} := \mathbf{x} + (-\mathbf{y})$$

と定め、これを $\mathbf{x}$ から $\mathbf{y}$ を引いた**差**といいます。

●連立一次方程式の解集合の構造

ここでは、連立一次方程式が解を持つ場合に、その解全体のなす集合の構造について考察します。

例 20-1 連立一次方程式 $\begin{cases} x + y + z + w = 1 \\ x + 2y - w = 0 \\ x + 2y + 2z = 2 \end{cases}$ の実数解 $\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$ のなす集合を求めよ。

解；

ガウスの消去法で解を求める。拡大係数行列を行基本変形して、

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & -1 & 0 \\ 1 & 2 & 2 & 0 & 2 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & -2 & -1 \\ 0 & 1 & 1 & -1 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & -2 & -1 \\ 0 & 0 & 2 & 1 & 2 \end{array}\right)$$

を得る。与えられた連立一次方程式を解くことは、連立一次方程式

$$\begin{cases} x+y+z+w=1 \\ y-z-2w=-1 \\ 2z+w=2 \end{cases}$$

を解くことと同じである。まず、3 番目の式から、$z=t$ $(t\in\mathbb{R})$ とおいて、$w=-2t+2$ が得られる。これを 2 番目の式に代入して $y=-1+z+2w=-1+t+2(-2t+2)=-3t+3$ が得られる。最後に 1 番目の式に代入して $x=1-y-z-w=1-(-3t+3)-t-(-2t+2)=4t-4$ が得られる。したがって、求める実数解の集合は、

$$\left\{ \begin{pmatrix} 4t-4 \\ -3t+3 \\ t \\ -2t+2 \end{pmatrix} \;\middle|\; t\in\mathbb{R} \right\} = \left\{ t\begin{pmatrix} 4 \\ -3 \\ 1 \\ -2 \end{pmatrix} + \begin{pmatrix} -4 \\ 3 \\ 0 \\ 2 \end{pmatrix} \;\middle|\; t\in\mathbb{R} \right\}$$

である。 □

演習 20-1 * 連立一次方程式 $\begin{cases} 2x-y-z+2w=5 \\ x-2y+z+w=1 \\ 3x-8y+5z+3w=1 \end{cases}$ の実数解 $\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$ のなす集合を求めよ。

例 20-1 の連立一次方程式において、$\mathbf{x}_0=\begin{pmatrix} -4 \\ 3 \\ 0 \\ 2 \end{pmatrix}$ は 1 つの解であり ($\because t=0$ の場合を考える)、“パラメータを含む部分” $t\begin{pmatrix} 4 \\ -3 \\ 1 \\ -2 \end{pmatrix}$ $(t\in\mathbb{R})$ は右辺をすべて 0 に変えて得られる連立一次方程式

(★)
$$\begin{cases} x+y+z+w=0 \\ x+2y\qquad -w=0 \\ x+2y+2z\qquad =0 \end{cases}$$

の解になっています。したがって、例 20-1 の連立一次方程式の任意の実数解は

$$(\text{連立一次方程式 (★) の実数解})+\mathbf{x}_0$$

という形をしていることがわかります。この現象は一般の連立一次方程式で成り立ちます。すなわち、

命題 20-2

行列 $A\in \mathrm{M}_{mn}(\mathbb{K})$ とベクトル $\mathbf{b}\in\mathbb{K}^m$ に対して、連立一次方程式 $A\mathbf{x}=\mathbf{b}$ が解 $\mathbf{x}_0\in\mathbb{K}^n$ を持つと仮定する。このとき、連立一次方程式 $A\mathbf{x}=\mathbf{b}$ の任意の解 $\mathbf{x}\in\mathbb{K}^n$ は

$$(\text{連立一次方程式 } A\mathbf{x}=\mathbf{0} \text{ の } \mathbb{K}^n \text{ における解})+\mathbf{x}_0$$

で与えられる。

(**proof**)

• 連立一次方程式 $A\mathbf{x}=\mathbf{b}$ の解 $\mathbf{x}_1\in\mathbb{K}^n$ が連立一次方程式 $A\mathbf{x}=\mathbf{0}$ の解 $\mathbf{x}\in\mathbb{K}^n$ によって $\mathbf{x}_1=\mathbf{x}+\mathbf{x}_0$ と表わされること：

$\mathbf{x}_1$ は連立一次方程式 $A\mathbf{x}=\mathbf{b}$ の解なので、$A\mathbf{x}_1=\mathbf{b}$ を満たす。仮定により、$A\mathbf{x}_0=\mathbf{b}$ も満たされているから、

$$A(\mathbf{x}_1-\mathbf{x}_0)=A\mathbf{x}_1-A\mathbf{x}_0=\mathbf{b}-\mathbf{b}=\mathbf{0}$$

を得る。よって、$\mathbf{x}=\mathbf{x}_1-\mathbf{x}_0$ とおくと、$\mathbf{x}\in\mathbb{K}^n$ であり、$A\mathbf{x}=\mathbf{0}$ が満たされる。

• $\mathbf{x}\in\mathbb{K}^n$ を連立一次方程式 $A\mathbf{x}=\mathbf{0}$ の解としたとき、$\mathbf{x}+\mathbf{x}_0$ が連立一次方程式 $A\mathbf{x}=\mathbf{b}$ の解になること：

$A\mathbf{x}=\mathbf{0},\ A\mathbf{x}_0=\mathbf{b}$ より、

$$A(\mathbf{x}+\mathbf{x}_0)=A\mathbf{x}+A\mathbf{x}_0=\mathbf{b}+\mathbf{0}=\mathbf{b}$$

となる。よって、$\mathbf{x}+\mathbf{x}_0\in\mathbb{K}^n$ は連立一次方程式 $A\mathbf{x}=\mathbf{b}$ の解である。 □

上の命題により、連立一次方程式 $A\mathbf{x}=\mathbf{b}$ の解の集合の研究は、連立一次方程式 $A\mathbf{x}=\mathbf{0}$ の解の集合の研究に帰着されることがわかります。

●部分空間

連立一次方程式 $A\mathbf{x}=\mathbf{0}$ の解の集合はベクトルの和とスカラー倍に関して閉じています。この性質を持つ数ベクトル空間の部分集合には次のような名前がつけられています。

定義 20-3

数ベクトル空間 $\mathbb{K}^n$ の部分集合 V が次の 3 つの条件を満たすとき、V は $\mathbb{K}^n$ の**部分空間** (subspace) であるという。

(0) $\mathbf{0}\in V$ である。

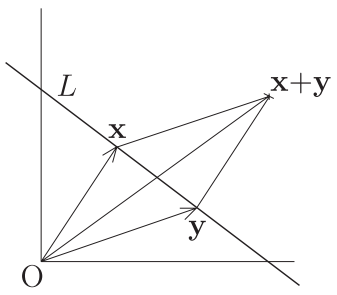
(i) すべての $\mathbf{x},\ \mathbf{y}\in V$ に対して $\mathbf{x}+\mathbf{y}\in V$ である。

(ii) すべての $\mathbf{x}\in V$ とすべての $t\in\mathbb{K}$ について $t\mathbf{x}\in V$ である。

注意：上の条件 (i)(ii) を満たすような部分集合 $V\subset\mathbb{K}^n$ について、条件 (0) が成り立つことと V が空集合でないこととは同値です。実際、V が条件 (i)(ii) を満たす $\mathbb{K}^n$ の空でない部分集合であれば、V は零ベクトル $\mathbf{0}\in\mathbb{K}^n$ を含むことが次のようにしてわかります。まず、$V\neq\varnothing$ なので、V には少なくとも 1 つの元 $\mathbf{x}$ が存在します。条件 (ii) から $-\mathbf{x}\in V$ となります。次に、$\mathbf{x},\ -\mathbf{x}\in V$ に対して条件 (i) を使って、$\mathbf{0}=\mathbf{x}+(-\mathbf{x})\in V$ がわかります。

例 20-4

(1) 平面 $\mathbb{R}^2$ 内の原点を通る直線 L は、$\mathbf{p}=\begin{pmatrix}a\\b\end{pmatrix}$ をその方向ベクトルとすると $L=\{\ t\mathbf{p}\mid t\in\mathbb{R}\ \}$ と表わすことができるので、$\mathbb{R}^2$ の部分空間である。これに対し、原点を通らない直線 L は部分空間でない (右図参照)。同様に、3 次元空間 $\mathbb{R}^3$ 内の原点を通る直線は $\mathbb{R}^3$ の部分空間であるが、原点を通らない直線は部分空間でない。



(2) 空間 $\mathbb{R}^3$ 内の原点を通る平面 H は2つの平行でないベクトル $\mathbf{p}=\begin{pmatrix}a_1\\b_1\\c_1\end{pmatrix}$, $\mathbf{q}=\begin{pmatrix}a_2\\b_2\\c_2\end{pmatrix}$ を用いて、$H=\{\ t\mathbf{p}+s\mathbf{q}\mid t,\ s\in\mathbb{R}\ \}$ と表わすことができるので、$\mathbb{R}^3$ の部分空間である。これに対し、原点を通らない平面は部分空間でない。
(3) 数ベクトル空間 $\mathbb{R}^n$ 自身は $\mathbb{R}^n$ の部分空間である。また、零ベクトル $\mathbf{0}$ のみからなる $\mathbb{R}^n$ の部分集合 $\{\mathbf{0}\}$ は $\mathbb{R}^n$ の部分空間である。

例 20-5 $A\in \mathrm{M}_{mn}(\mathbb{K})$ に対して、$V=\{\ \mathbf{x}\in\mathbb{K}^n\mid A\mathbf{x}=\mathbf{0}\ \}$ は $\mathbb{K}^n$ の部分空間である。

(**proof**)

(0) 零ベクトル $\mathbf{0}\in\mathbb{K}^n$ は確かに連立一次方程式 $A\mathbf{x}=\mathbf{0}$ の解なので、$\mathbf{0}\in V$ である。

(i) 任意の $\mathbf{x},\mathbf{y}\in V$ に対して

$$A(\mathbf{x}+\mathbf{y})=A\mathbf{x}+A\mathbf{y}=\mathbf{0}+\mathbf{0}=\mathbf{0}$$

となるので、$\mathbf{x}+\mathbf{y}\in V$ である。

(ii) 任意の $\mathbf{x}\in V$ と任意の $t\in\mathbb{K}$ に対して、

$$A(t\mathbf{x})=tA\mathbf{x}=t\mathbf{0}=\mathbf{0}$$

となるので、$t\mathbf{x}\in V$ である。

以上より、V は $\mathbb{K}^n$ の部分空間である。 □

演習 20-2 V,W を $\mathbb{K}^n$ の2つの部分空間とする。$V\cap W$ もまた $\mathbb{K}^n$ の部分空間であることを示せ。また、$V\cup W$ は $\mathbb{K}^n$ の部分空間になるか？

ヒント：後半については、$\mathbb{K}=\mathbb{R},\ n=2$ で考えてみよ。

●線形結合

$\mathbf{v}_1,\cdots,\mathbf{v}_d$ を $\mathbb{K}^n$ に属する d 個のベクトルとします。ベクトル $\mathbf{x}\in\mathbb{K}^n$ が $\mathbf{v}_1,\cdots,\mathbf{v}_d$ の $\mathbb{K}$-**線形結合** (linear combination) であるとは、$\mathbf{x}$ が、ある $t_1,\cdots,t_d\in\mathbb{K}$ により、

$$\mathbf{x}=t_1\mathbf{v}_1+\cdots+t_d\mathbf{v}_d$$

と表わされるときをいいます。$\mathbf{v}_1,\cdots,\mathbf{v}_d$ の $\mathbb{K}$-線形結合の全体からなる集合

$$\mathrm{Span}_{\mathbb{K}}\{\mathbf{v}_1,\cdots,\mathbf{v}_d\}:=\{\ t_1\mathbf{v}_1+\cdots+t_d\mathbf{v}_d\mid t_1,\cdots,t_d\in\mathbb{K}\ \}$$

は $\mathbb{K}^n$ の部分空間になります。これを $\mathbf{v}_1,\cdots,\mathbf{v}_d$ によって**張られる部分空間**といいます。

●基底

V を数ベクトル空間 $\mathbb{K}^n$ の部分空間とし、$\mathbf{v}_1,\cdots,\mathbf{v}_d$ を V に属する相異なる d 個のベクトルとします。V の部分集合 $\{\mathbf{v}_1,\cdots,\mathbf{v}_d\}$ が V の**基底** (basis) であるとは、すべての元 $\mathbf{x}\in V$ が

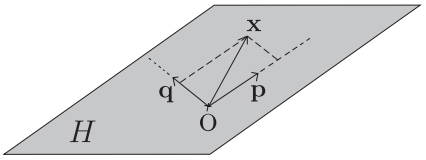
$$\mathbf{x}=t_1\mathbf{v}_1+\cdots+t_d\mathbf{v}_d\qquad(t_1,\ \cdots,t_d\in\mathbb{K})$$

のように書き表わされ、かつ、その書き表わされ方が一意的であるときをいいます。

例 20-6

(1) 平面 $\mathbb{R}^2$ 内の原点を通る直線 L について (これは数ベクトル空間 $\mathbb{R}^2$ の部分空間であった)、$\mathbf{0}$ でない L 上のベクトル (つまり、L の方向ベクトル) $\mathbf{p}$ を 1 つとると、L 上のすべての点 $\mathbf{x}$ は $\mathbf{x} = t\mathbf{p}$ $(t \in \mathbb{R})$ のように $\mathbf{p}$ のスカラー倍として表される。しかも、L 上の点 $\mathbf{x}$ が異なる実数 $t,\ t'$ によって $\mathbf{x} = t\mathbf{p},\ \mathbf{x} = t'\mathbf{p}$ のように 2 通りに書き表わされることはないので、L 上の点 $\mathbf{x}$ を $\mathbf{x} = t\mathbf{p}$ $(t \in \mathbb{R})$ のように表わす書き表わし方は一意的である。したがって、$\{\mathbf{p}\}$ は L の基底である。

(2) 同様に、$\mathbb{R}^3$ 内の原点を通る平面 H について、H 上の平行でない 2 つのベクトル $\mathbf{p}$ と $\mathbf{q}$ をとると、H 上のすべての点 $\mathbf{x}$ は $\mathbf{x} = s\mathbf{p} + t\mathbf{q}$ $(s,\ t \in \mathbb{R})$ のように $\mathbf{p}$ と $\mathbf{q}$ の一次結合として一意的に表されることがわかる。したがって、$\{\mathbf{p}, \mathbf{q}\}$ は H の基底である。



(3) $\mathbb{K}^n$ の n 個のベクトル $\mathbf{e}_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $\mathbf{e}_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, $\cdots, \mathbf{e}_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ からなる集合は $\mathbb{K}^n$ の基底である。実際、任意のベクトル $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ は

$$\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n$$

のようにただ一通りに書き表わされる。基底 $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ を $\mathbb{K}^n$ の**標準基底** (standard basis) という。

約束：今後、「$\{\mathbf{v}_1, \cdots, \mathbf{v}_d\}$ を V の基底とする」などと書くことがありますが、このように書かれているときには、d 個のベクトル $\mathbf{v}_1, \cdots, \mathbf{v}_d$ は相異なると約束します。

基底であるための条件は次の 2 つの条件に分解することができます。

定義 20-7

V を数ベクトル空間 $\mathbb{K}^n$ の部分空間とし、$\mathbf{v}_1, \cdots, \mathbf{v}_d$ を $\mathbb{K}^n$ に属するベクトルとする。

(1) $\mathbf{v}_1, \cdots, \mathbf{v}_d$ が $\mathbb{K}$ 上**線形独立** (linearly independent) であるとは、次の条件が成り立つときをいう：

任意の $t_1, \cdots, t_d \in \mathbb{K}$ について「$t_1\mathbf{v}_1 + \cdots + t_d\mathbf{v}_d = \mathbf{0} \ \Rightarrow \ t_1 = \cdots = t_d = 0$」.

(2) $\mathbf{v}_1, \cdots, \mathbf{v}_d$ が V を**張る** (span) とは、次の 2 つの条件が成り立つときをいう。

(i) $\mathbf{v}_1, \cdots, \mathbf{v}_d \in V$.

(ii) $\forall \mathbf{x} \in V,\ \exists t_1, \cdots, t_d \in \mathbb{K}$ s.t. $\mathbf{x} = t_1\mathbf{v}_1 + \cdots + t_d\mathbf{v}_d$.

注意：1. 線形独立という言葉の代わりに **一次独立**という言葉もよく使われます。

2. (2) の 2 条件は 1 つの等式 $\mathrm{Span}_{\mathbb{K}}\{\mathbf{v}_1, \cdots, \mathbf{v}_d\} = V$ で表わすことができます。

3. $\mathbf{v}_1, \cdots, \mathbf{v}_d$ の中に零ベクトル $\mathbf{0}$ が含まれているとき、これらのベクトルは線形独立ではありません。これは、例えば、$\mathbf{v}_1 = \mathbf{0}$ のとき、$1 \cdot \mathbf{v}_1 + 0 \cdot \mathbf{v}_2 + \cdots + 0 \cdot \mathbf{v}_d = \mathbf{0}$ が成り立つことからわかります。同様に、$\mathbf{v}_1, \cdots, \mathbf{v}_d$ の中に同じものが含まれていても線形独立にはなりません。

補題 20-8

V を数ベクトル空間 $\mathbb{K}^n$ の部分空間とする。$\mathbb{K}^n$ に属する d 個のベクトル $\mathbf{v}_1, \cdots, \mathbf{v}_d$ からなる集合が V の基底であるための必要十分条件は、$\mathbf{v}_1, \cdots, \mathbf{v}_d$ が $\mathbb{K}$ 上線形独立であって、かつ、V を張ることである。

(**proof**)

$\{\mathbf{v}_1, \cdots, \mathbf{v}_d\}$ が V の基底であるとする。$\mathbf{0} \in V$ であるから、

$$\mathbf{0} = t_1\mathbf{v}_1 + \cdots + t_d\mathbf{v}_d \quad (t_1, \cdots, t_d \in \mathbb{K})$$

と書くことができる。一方、

$$\mathbf{0} = 0 \cdot \mathbf{v}_1 + \cdots + 0 \cdot \mathbf{v}_d$$

とも書ける。書き表わし方の一意性から $t_1 = \cdots = t_d = 0$ でなければならない。よって、$\mathbf{v}_1, \cdots, \mathbf{v}_d$ は線形独立である。$\mathbf{v}_1, \cdots, \mathbf{v}_d$ が V を張ることは、基底の定義から直ちに従う。

次に、逆が成り立つことを示す。$\mathbf{v}_1, \cdots, \mathbf{v}_d$ が $\mathbb{K}$ 上線形独立であって、かつ、V を張ると仮定する。$\mathbf{v}_1, \cdots, \mathbf{v}_d$ が V を張ることから、任意の $\mathbf{x} \in V$ は

$$(*) \qquad \mathbf{x} = t_1\mathbf{v}_1 + \cdots + t_d\mathbf{v}_d \quad (t_1, \cdots, t_d \in \mathbb{K})$$

と書くことができる。この表わし方がただ一通りであることを示せばよい。

$$\mathbf{x} = s_1\mathbf{v}_1 + \cdots + s_d\mathbf{v}_d \quad (s_1, \cdots, s_d \in \mathbb{K})$$

とも書けたとする。このとき、

$$(t_1 - s_1)\mathbf{v}_1 + \cdots + (t_d - s_d)\mathbf{v}_d = \mathbf{x} - \mathbf{x} = \mathbf{0}$$

となる。$\mathbf{v}_1, \cdots, \mathbf{v}_d$ は線形独立であるから、$t_1 - s_1 = 0, \cdots, t_d - s_d = 0$ を得る。故に、$t_1 = s_1, \cdots, t_d = s_d$ であり、$\mathbf{x}$ を $(*)$ のように書く書き表わし方は一意的である。 □

例 20-9 2つのベクトル $\mathbf{v}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $\mathbf{v}_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ からなる集合は $\mathbb{R}^2$ の基底か。

解；

まず、$\mathbf{v}_1, \mathbf{v}_2$ が $\mathbb{R}$ 上線形独立であるかどうかを調べる。そのためには、

$$(\sharp) \qquad x\mathbf{v}_1 + y\mathbf{v}_2 = \mathbf{0} \quad (x, y \in \mathbb{R})$$

とおいて、これが $x = y = 0$ 以外に実数解をもつかどうかを調べればよい。$\mathbf{v}_1, \mathbf{v}_2$ を横に並べて行列 $A = (\mathbf{v}_1\ \mathbf{v}_2)$ を作り、$\mathbf{x} = \begin{pmatrix} x \\ y \end{pmatrix}$ とおくと、$(\sharp)$ は $A\mathbf{x} = \mathbf{0}$ という連立一次方程式になる。これを（ガウスの消去法で）解くと、$x = y = 0$ であることがわかる（計算略）。したがって、$\mathbf{v}_1, \mathbf{v}_2$ は $\mathbb{R}$ 上線形独立である。

次に、$\mathbf{v}_1, \mathbf{v}_2$ が $\mathbb{R}^2$ を張るかどうかを調べる。そのためには、任意のベクトル $\mathbf{v} \in \mathbb{R}^2$ に対して、

$$(\natural) \qquad \mathbf{v} = x\mathbf{v}_1 + y\mathbf{v}_2$$

となる $x, y \in \mathbb{R}$ が存在するかどうかを調べればよい。$\mathbf{v} = \begin{pmatrix} a \\ b \end{pmatrix}$ とおくと、$(\natural)$ は $\begin{pmatrix} a \\ b \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix}$ という連立一次方程式になる。この連立一次方程式は解 $x = 2a - b, y = -a + b$ を持つことがわかる。よって、$\mathbf{v} = (2a - b)\mathbf{v}_1 + (-a + b)\mathbf{v}_2$ と書ける。したがって、$\mathbf{v}_1, \mathbf{v}_2$ は $\mathbb{R}^2$ を張る。

以上より、$\{\mathbf{v}_1, \mathbf{v}_2\}$ は $\mathbb{R}^2$ の基底である。 □

演習 20-3 * $\left\{ \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \right\}$ は $\mathbb{R}^3$ の基底かどうかを調べよ。

●基底の存在

ここでは、零ベクトルだけからなる部分空間 $\{\mathbf{0}\}$ を除くすべての部分空間に対して、基底が存在することを証明します。

補題 20-10

数ベクトル空間 $\mathbb{K}^n$ の任意の $(n+1)$ 個のベクトルは $\mathbb{K}$ 上線形独立でない。

(**proof**)

$(n+1)$ 個のベクトル $\mathbf{v}_1, \cdots, \mathbf{v}_{n+1} \in \mathbb{K}^n$ を任意にとり、$(n, n+1)$-行列 $A := (\mathbf{v}_1 \ \cdots \ \mathbf{v}_{n+1}) \in \mathrm{M}_{n,n+1}(\mathbb{K})$ を考える。定理 19-6 より、$PAQ = F_{n,n+1}(r)$ を満たす正則行列 $P \in \mathrm{M}_n(\mathbb{K})$, $Q \in \mathrm{M}_{n+1}(\mathbb{K})$ と整数 r $(0 \leq r \leq n)$ が存在する。

今、第 $(n+1)$-成分のみ 1 で、他の成分はすべて 0 であるようなベクトル $\mathbf{e}_{n+1} \in \mathbb{K}^{n+1}$ に対して、$F_{n,n+1}(r)\mathbf{e}_{n+1} = \mathbf{0}$ が成り立つ。このとき、$\mathbf{x} := Q\mathbf{e}_{n+1} \in \mathbb{K}^{n+1}$ は Q が正則であることから零ベクトルではなく、かつ、$A\mathbf{x} = P^{-1}F_{n,n+1}(r)\mathbf{e}_{n+1} = \mathbf{0}$ を満たす。したがって、$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_{n+1} \end{pmatrix}$ のように成分表示すれば、$x_1, \cdots, x_{n+1}$ は同時には 0 ではなく、かつ、$x_1\mathbf{v}_1 + \cdots + x_{n+1}\mathbf{v}_{n+1} = \mathbf{0}$ を満たす。これは、$\mathbf{v}_1, \cdots, \mathbf{v}_{n+1}$ が $\mathbb{K}$ 上線形独立でないことを意味している。 □

補題 20-11

V を数ベクトル空間 $\mathbb{K}^n$ の部分空間、$\mathbf{v}_1, \cdots, \mathbf{v}_k$ を V の $\mathbb{K}$ 上線形独立なベクトルとする。$\mathbf{v}_1, \cdots, \mathbf{v}_k$ が V を張らないならば、$\mathbf{v}_1, \cdots, \mathbf{v}_k, \mathbf{v}$ が $\mathbb{K}$ 上線形独立となるような $\mathbf{v} \in V$ が存在する。

(**proof**)

$\mathbf{v}_1, \cdots, \mathbf{v}_k$ によって張られる $\mathbb{K}^n$ の部分空間

$$W := \{\ t_1\mathbf{v}_1 + \cdots + t_k\mathbf{v}_k \ \mid t_1, \cdots, t_k \in \mathbb{K}\}$$

を考える。$W \subset V$ であるが、$\mathbf{v}_1, \cdots, \mathbf{v}_k$ は V を張らないので、$W \neq V$ である。したがって、V に属するベクトル $\mathbf{v}$ であって、W には属さないものが存在する。このとき、$\mathbf{v}_1, \cdots, \mathbf{v}_k, \mathbf{v}$ は $\mathbb{K}$ 上線形独立である。 □

演習 20-4 上の証明の中の下線部分が成り立つことを詳しく説明せよ。

定理 20-12

数ベクトル空間 $\mathbb{K}^n$ の $\{\mathbf{0}\}$ でないすべての部分空間には基底が存在する。

(**proof**)

$V \subset \mathbb{K}^n$ を $\{\mathbf{0}\}$ でない部分空間とする。V の線形独立な有限個のベクトルであって、V を張るものは存在しないと仮定して矛盾を導く。

まず、$\mathbf{v}_1 \in V$, $\mathbf{v}_1 \neq \mathbf{0}$ を任意に 1 つとる。$\mathbf{v}_1$ は線形独立である。仮定により、$\mathbf{v}_1$ は V を張らない。よって、$\mathbf{v}_1, \mathbf{v}_2$ が線形独立となるような $\mathbf{v}_2 \in V$ が存在する (補題 20-11)。再び仮定

により、$\mathbf{v}_1, \mathbf{v}_2$ は V を張らない。よって、$\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ が線形独立となるような $\mathbf{v}_3 \in V$ が存在する。以下、同様に考えて、V に属する $(n+1)$ 個の線形独立なベクトル $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{n+1}$ の存在がわかる。これは、補題 20-10 に矛盾する。 □

●次元

ここでは、$\mathbb{K}^n$ の部分空間に対して次元という概念が定まることを証明します。

定理 20-13
V を数ベクトル空間 $\mathbb{K}^n$ の部分空間とする。$\{\mathbf{v}_1, \cdots, \mathbf{v}_d\}$, $\{\mathbf{w}_1, \cdots, \mathbf{w}_m\}$ がどちらも V の基底であれば、$d = m$ である。すなわち、V の基底を構成しているベクトルの個数は基底によらずに一定である。この個数 d のことを V の**次元** (dimension) といい、$\dim_{\mathbb{K}} V$ または $\dim V$ という記号で表わす。

(**proof**)

$\{\mathbf{w}_1, \cdots, \mathbf{w}_m\}$ は V の基底であるから、各 $\mathbf{v}_j$ を

$$\mathbf{v}_j = a_{1j}\mathbf{w}_1 + \cdots + a_{mj}\mathbf{w}_m \qquad (a_{1j}, \cdots, a_{mj} \in \mathbb{K})$$

のように書くことができる。j を 1 から d まで動かすと d 個の等式が得られるが、これらの等式は、$A := (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le d}} \in \mathrm{M}_{md}(\mathbb{K})$ と定めると、

$$(\mathbf{v}_1 \ \cdots \ \mathbf{v}_d) = (\mathbf{w}_1 \ \cdots \ \mathbf{w}_m)A$$

と表わすことができる。同様に、$\{\mathbf{v}_1, \cdots, \mathbf{v}_d\}$ は V の基底であるから、

$$(\mathbf{w}_1 \ \cdots \ \mathbf{w}_m) = (\mathbf{v}_1 \ \cdots \ \mathbf{v}_d)B$$

を満たす行列 $B \in \mathrm{M}_{dm}(\mathbb{K})$ が存在する。互いに代入して、

$$(\mathbf{v}_1 \ \cdots \ \mathbf{v}_d) = (\mathbf{v}_1 \ \cdots \ \mathbf{v}_d)BA, \qquad (\mathbf{w}_1 \ \cdots \ \mathbf{w}_m) = (\mathbf{w}_1 \ \cdots \ \mathbf{w}_m)AB$$

が得られる。前者の等式から $BA = I_d$ が得られ、後者の等式から $AB = I_m$ が得られる (下の演習 20-5 による)。

$\mathbf{a}_j \in \mathbb{K}^m$ $(j = 1, \cdots, d)$ を A の第 j 列を取り出して作ったベクトルとすると、$BA = I_d$ より、$\mathbf{a}_1, \cdots, \mathbf{a}_d$ は線形独立である ($\because \mathbf{x} \in \mathbb{K}^d$ が $A\mathbf{x} = \mathbf{0}$ を満たしていたとすると、この両辺に左から B を掛けて $\mathbf{x} = \mathbf{0}$ を得る)。よって、補題 20-10 により、$d \le m$ を得る。同様にして、$AB = I_m$ から $m \le d$ が導かれるので、$d = m$ となることがわかる。 □

演習 20-5 V を数ベクトル空間 $\mathbb{K}^n$ の部分空間とし、$\{\mathbf{v}_1, \cdots, \mathbf{v}_d\}$ を V の基底とする。このとき、行列 $A, B \in \mathrm{M}_{dm}(\mathbb{K})$ について、次式が成り立つことを示せ。

$$(\mathbf{v}_1 \ \cdots \ \mathbf{v}_d)A = (\mathbf{v}_1 \ \cdots \ \mathbf{v}_d)B \quad \Rightarrow \quad A = B.$$

ヒント：A, B を成分で書いて、$(\mathbf{v}_1 \ \cdots \ \mathbf{v}_d)A = (\mathbf{v}_1 \ \cdots \ \mathbf{v}_d)B$ の第 j 列を比較する。

例20-14 $\mathbb{K}^n$ の基底として、標準基底 $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ があるので、$\dim \mathbb{K}^n = n$ である。また、$\mathbb{K}^n$ の部分空間 $\{\mathbf{0}\}$ には基底が存在しないので、$\dim\{\mathbf{0}\} = 0$ である。

演習 20-6 * 行列 $A = \begin{pmatrix} 1 & 1 & 3 & 2 \\ 3 & 1 & 9 & 0 \\ -3 & -1 & -10 & 5 \end{pmatrix} \in \mathrm{M}_{34}(\mathbb{R})$ に対して、

$\mathbb{R}^4$ の部分空間 $V = \{\, \mathbf{x} \in \mathbb{R}^4 \mid A\mathbf{x} = \mathbf{0} \,\}$ の基底を 1 組求めよ。また、$\dim V$ を求めよ。

§21. 行列の階数と線形写像

第 19 節において、基本変形を施すとどんな (m,n)-行列 A も $F_{mn}(r)=\begin{pmatrix} I_r & \mathrm{O} \\ \mathrm{O} & \mathrm{O} \end{pmatrix}$ という形の標準形にすることができることを学びました。標準形に現れる r は A の列ベクトルの線形独立性と密接に関連していて、A の階数と呼ばれています。ここでの目標は、階数の意味とその重要性を様々な角度から知ることです。この節では、$\mathbb{K}=\mathbb{Q},\mathbb{R},\mathbb{C}$ とします。

●線形写像の核と像

$\mathbb{K}$-線形写像とは、写像 $F:\mathbb{K}^n\longrightarrow\mathbb{K}^m$ であって、次の 2 つの条件が満たされるものをいうのでした (詳しくは第 13 節を参照してください)：

(i) すべての $\mathbf{x},\mathbf{y}\in\mathbb{K}^n$ に対して、$F(\mathbf{x}+\mathbf{y})=F(\mathbf{x})+F(\mathbf{y})$.

(ii) すべての $\mathbf{x}\in\mathbb{K}^n$ とすべての $t\in\mathbb{K}$ に対して、$F(t\mathbf{x})=tF(\mathbf{x})$.

$\mathbb{K}$-線形写像 $F:\mathbb{K}^n\longrightarrow\mathbb{K}^m$ に対して、

$$\mathrm{Ker}\,F:=\{\,\mathbf{x}\in\mathbb{K}^n\mid F(\mathbf{x})=\mathbf{0}\,\},\qquad \mathrm{Im}\,F:=F(\mathbb{K}^n)=\{\,F(\mathbf{x})\mid\mathbf{x}\in\mathbb{K}^n\,\}$$

をそれぞれ F の**核** (kernel)、**像** (image) と呼びます。

例 21-1 (m,n)-行列 $A=(a_{ij})\in\mathrm{M}_{mn}(\mathbb{K})$ が与えられると、n 次元ベクトル $\mathbf{x}=\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\in\mathbb{K}^n$ を m 次元ベクトル

$$A\mathbf{x}=\begin{pmatrix} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n \\ \vdots \\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n \end{pmatrix}\in\mathbb{K}^m$$

に写すような $\mathbb{K}$-線形写像

$$F_A:\mathbb{K}^n\longrightarrow\mathbb{K}^m$$

が定まる (補題 13-7)。この線形写像 $F_A:\mathbb{K}^n\longrightarrow\mathbb{K}^m$ の核と像はそれぞれ次のようになる：

$$\mathrm{Ker}\,F_A=\{\,\mathbf{x}\in\mathbb{K}^n\mid A\mathbf{x}=\mathbf{0}\,\},$$
$$\mathrm{Im}\,F_A=\mathrm{Span}_{\mathbb{K}}\{\,\mathbf{a}_1,\cdots,\mathbf{a}_n\,\}=\{\,t_1\mathbf{a}_1+\cdots+t_n\mathbf{a}_n\mid t_1,\ \cdots,t_n\in\mathbb{K}\,\}$$

但し、$\mathbf{a}_j$ $(j=1,\cdots,n)$ は A の第 j 列ベクトルである：$\mathbf{a}_j=\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$.

(**proof**)

$\mathrm{Ker}\,F_A$ については、核の定義をそのまま書いたに過ぎない。$\mathrm{Im}\,F_A$ について示す。

$\{\mathbf{e}_1,\ \cdots,\mathbf{e}_n\}$ を $\mathbb{K}^n$ の標準基底とすると、任意のベクトル $\mathbf{x}\in\mathbb{K}^n$ は

$$\mathbf{x}=t_1\mathbf{e}_1+\cdots+t_n\mathbf{e}_n\quad(t_1,\ \cdots,t_n\in\mathbb{K})$$

のように表わされる。このとき、F_A の線形性と $F_A(\mathbf{e}_j)=A\mathbf{e}_j=\mathbf{a}_j$ $(j=1,\cdots,n)$ から

$$F_A(\mathbf{x})=t_1F_A(\mathbf{e}_1)+\cdots+t_nF_A(\mathbf{e}_n)=t_1\mathbf{a}_1+\cdots+t_n\mathbf{a}_n$$

となる。よって、

$$\mathrm{Im}\,F_A=\{\,F_A(\mathbf{x})\mid\mathbf{x}\in\mathbb{K}^n\,\}=\{\,t_1\mathbf{a}_1+\cdots+t_n\mathbf{a}_n\mid t_1,\ \cdots,t_n\in\mathbb{K}\,\}$$

と表わされる。 □

補題 21-2

$\mathbb{K}$-線形写像 $F:\mathbb{K}^n \longrightarrow \mathbb{K}^m$ に対して、$\mathrm{Ker}\,F$ および $\mathrm{Im}\,F$ はそれぞれ $\mathbb{K}^n$ および $\mathbb{K}^m$ の部分空間である。

(**proof**)

命題 13-8、例 20-5、例 21-1 を使うと補題は直ちに示されるが、ここでは定義に基づく直接的な証明を与える。

$\mathrm{Im}\,F$ が $\mathbb{K}^m$ の部分空間であることを示す（$\mathrm{Ker}\,F$ については演習問題とする）。

まず、$\mathbf{0} \in \mathrm{Im}\,F$ を示す。F の線形性と $\mathbf{0}+\mathbf{0}=\mathbf{0}$ により、

$$F(\mathbf{0}) = F(\mathbf{0}+\mathbf{0}) = F(\mathbf{0}) + F(\mathbf{0})$$

となるので、この両辺に $-F(\mathbf{0})$ を加えることにより、$\mathbf{0} = F(\mathbf{0})$ が得られる。よって、$\mathbf{0} \in \mathrm{Im}\,F$ がわかった。

次に、任意の $\mathbf{x}', \mathbf{y}' \in \mathrm{Im}\,F$ と任意の $t \in \mathbb{K}$ に対して、$\mathbf{x}'+\mathbf{y}',\ t\mathbf{x}' \in \mathrm{Im}\,F$ となることを示す。$\mathbf{x}', \mathbf{y}' \in \mathrm{Im}\,F$ なので、$\mathbf{x}' = F(\mathbf{x}),\ \mathbf{y}' = F(\mathbf{y})$（$\mathbf{x},\ \mathbf{y} \in \mathbb{K}^n$）と書き表わすことができる。このとき、$F$ の線形性から

$$\mathbf{x}'+\mathbf{y}' = F(\mathbf{x})+F(\mathbf{y}) = F(\mathbf{x}+\mathbf{y}) \in \mathrm{Im}\,F, \quad t\mathbf{x}' = tF(\mathbf{x}) = F(t\mathbf{x}) \in \mathrm{Im}\,F$$

を得る。以上より、$\mathrm{Im}\,F$ は $\mathbb{K}^m$ の部分空間であることが示された。 □

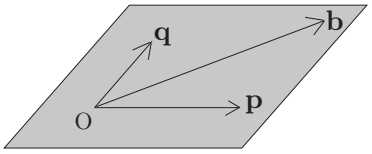
演習 21-1　$\mathbb{K}$-線形写像 $F:\mathbb{K}^n \longrightarrow \mathbb{K}^m$ に対して、$\mathrm{Ker}\,F$ は $\mathbb{K}^n$ の部分空間であることを証明せよ。

●連立一次方程式の解の存在条件

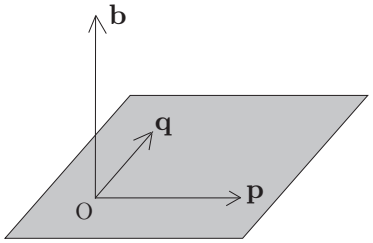
連立一次方程式 $A\mathbf{x} = \mathbf{b}$ ($A \in \mathrm{M}_{mn}(\mathbb{K}),\ \mathbf{b} \in \mathbb{K}^m$) を考えます。$\mathbf{x}$ が $\mathbb{K}^n$ 内を自由に動き回ると、それにつれられて $A\mathbf{x}$ は $\mathrm{Im}\,F_A \subset \mathbb{K}^m$ 内を動きます。この部分集合の中に $\mathbf{b}$ が入れば連立一次方程式 $A\mathbf{x} = \mathbf{b}$ には解がありますが、入らなければ解はありません。この考察と例題 21-1 から、連立一次方程式の解の存在に関する次のような理論的な判定条件が得らます。

命題 21-3

$A \in \mathrm{M}_{mn}(\mathbb{K}),\ \mathbf{b} \in \mathbb{K}^m$ とする。このとき、連立一次方程式 $A\mathbf{x} = \mathbf{b}$ が $\mathbb{K}^n$ 内に解を持つための必要十分条件は、$\mathbf{b}$ が A の列ベクトル $\mathbf{a}_1, \cdots, \mathbf{a}_n$ の $\mathbb{K}$-線形結合であること、すなわち、次のように書けることである：$\mathbf{b} = t_1\mathbf{a}_1 + \cdots + t_n\mathbf{a}_n \quad (t_1, \cdots, t_n \in \mathbb{K})$.



$A=(\mathbf{p}\ \mathbf{q})$ を係数行列とする連立一次方程式 $A\mathbf{x}=\mathbf{b}$ は解を持つ



$A=(\mathbf{p}\ \mathbf{q})$ を係数行列とする連立一次方程式 $A\mathbf{x}=\mathbf{b}$ は解を持たない

●行列の階数

定理 19-4 により、行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に行基本変形と列基本変形を有限回施すことによって、$F_{m,n}(r) = \begin{pmatrix} I_r & \mathrm{O} \\ \mathrm{O} & \mathrm{O} \end{pmatrix}$ という形の行列にすることができます。ここでは、このようにして得られる整数 r が途中の変形の仕方に依らずに定まることを証明します。

定理 21-4

行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に行基本変形と列基本変形を有限回施して、標準形 $F_{m,n}(r)$ $(0 \leq r \leq \min\{m,n\})$ が得られたとする。このとき、

$$r = \dim(\mathrm{Im}\, F_A) = (A \text{ の列ベクトルの中の } \mathbb{K} \text{ 上線形独立なものの最大個数})$$

が成り立つ。但し、$F_A : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ は A から定まる線形写像を表わす。r を A の**階数** (rank) といい、これを $\mathrm{rank}\, A$ で表わす。

定理を証明するために、補題を 1 つ準備します。

補題 21-5

$F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ を単射な $\mathbb{K}$-線形写像とする。$\mathbb{K}^n$ のベクトル $\mathbf{v}_1, \cdots, \mathbf{v}_k$ が $\mathbb{K}$ 上線形独立ならば、$F(\mathbf{v}_1), \cdots, F(\mathbf{v}_k)$ も $\mathbb{K}$ 上線形独立である。

(**proof**)

$t_1, \cdots, t_k \in \mathbb{K}$ が

$$(*) \qquad t_1 F(\mathbf{v}_1) + \cdots + t_k F(\mathbf{v}_k) = \mathbf{0}$$

を満たすとする。F の線形性により、$t_1 F(\mathbf{v}_1) + \cdots + t_k F(\mathbf{v}_k) = F(t_1\mathbf{v}_1 + \cdots + t_k\mathbf{v}_k)$ であり、一方、$F(\mathbf{0}) = \mathbf{0}$ である (演習 21-1) から、等式 $(*)$ は

$$F(t_1\mathbf{v}_1 + \cdots + t_k\mathbf{v}_k) = F(\mathbf{0})$$

と同値である。F は単射であるから、

$$t_1\mathbf{v}_1 + \cdots + t_k\mathbf{v}_k = \mathbf{0}$$

を得る。$\mathbf{v}_1, \cdots, \mathbf{v}_k$ は $\mathbb{K}$ 上線形独立なので、$t_1 = \cdots = t_k = 0$ でなければならない。故に、$F(\mathbf{v}_1), \cdots, F(\mathbf{v}_k)$ は $\mathbb{K}$ 上線形独立である。 □

注意：上の補題から、

行基本変形では線形独立な列ベクトルの場所は変わらない

という事実が従います。詳しく説明しましょう。行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ に行基本変形を施して、行列 $B \in \mathrm{M}_{mn}(\mathbb{K})$ が得られたとします。すると、ある正則行列 $P \in \mathrm{M}_n(\mathbb{K})$ が存在して、$B = PA$ となります。このとき、A の第 j 列ベクトル $\mathbf{a}_j$ と B の第 j 列ベクトル $\mathbf{b}_j$ の間には $\mathbf{b}_j = P\mathbf{a}_j = F_P(\mathbf{a}_j)$ という関係が成り立ちます。F_P は単射な $\mathbb{K}$-線形写像なので (命題 13-9)、上の補題により、

A の列ベクトル $\mathbf{a}_{i_1}, \cdots, \mathbf{a}_{i_k}$ が線形独立ならば、B の列ベクトル $\mathbf{b}_{i_1}, \cdots, \mathbf{b}_{i_k}$ も線形独立

になることがわかります。

(**proof of Theorem 21-4**)

I. $r = \dim(\mathrm{Im}\, F_A)$ の証明：

定理 19-6 より、ある正則行列 $P \in \mathrm{M}_m(\mathbb{K})$, $Q \in \mathrm{M}_n(\mathbb{K})$ が存在して $PAQ = F_{m,n}(r)$ となる。F_P, F_Q は全単射である（命題 13-9）から、

$$\mathrm{Im}\, F_A = \mathrm{Im}(F_A \circ F_Q) = \mathrm{Im}(F_P^{-1} \circ F_P \circ F_A \circ F_Q) = \mathrm{Im}(F_{P^{-1}} \circ F_{PAQ})$$

が成り立つ。ここで、

$$F_{PAQ}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = PAQ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = F_{m,n}(r) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1\mathbf{e}_1 + \cdots + x_r\mathbf{e}_r$$

より、

$$\begin{aligned} \mathrm{Im}\, F_A &= \{\ (F_{P^{-1}} \circ F_{PAQ})(\mathbf{x}) \mid \mathbf{x} \in \mathbb{K}^n\ \} \\ &= \{\ F_{P^{-1}}(F_{PAQ}(\mathbf{x})) \mid \mathbf{x} \in \mathbb{K}^n\} \\ &= \{\ F_{P^{-1}}(x_1\mathbf{e}_1 + \cdots + x_r\mathbf{e}_r) \mid x_1,\ \cdots, x_r \in \mathbb{K}\ \} \\ &= \{\ x_1P^{-1}\mathbf{e}_1 + \cdots + x_rP^{-1}\mathbf{e}_r \mid x_1,\ \cdots, x_r \in \mathbb{K}\ \} \end{aligned}$$

となる。よって、$\{P^{-1}\mathbf{e}_1,\ \cdots,\ P^{-1}\mathbf{e}_r\}$ は $\mathrm{Im}\, F_A$ を張る。また、$\mathbb{K}^m$ の r 個のベクトル $\mathbf{e}_1, \cdots, \mathbf{e}_r$ は $\mathbb{K}$-上線形独立であり、P^{-1} は正則行列であるから、$\{P^{-1}\mathbf{e}_1,\ \cdots,\ P^{-1}\mathbf{e}_r\}$ は $\mathbb{K}$-上線形独立である (補題 21-5)。以上より、$\{P^{-1}\mathbf{e}_1,\ \cdots,\ P^{-1}\mathbf{e}_r\}$ は $\mathrm{Im}\, F_A$ の基底である。よって、$\dim(\mathrm{Im}\, F_A) = r$ が示された。

Ⅱ.$\dim(\mathrm{Im}\, F_A) = (A$ の列ベクトルの中の線形独立なものの最大個数$)$ の証明：

A の列ベクトルの中で線形独立なものの最大個数を s とおく。$\mathrm{Im}\, F_A$ は A の列の入れ替えで変わらないから、A の最初の s 個の列ベクトル $\mathbf{a}_1, \cdots, \mathbf{a}_s$ が線形独立であるとしても一般性を失わない。このとき、A の第 s 列目以降の列ベクトル $\mathbf{a}_j$ $(s+1 \leq j \leq n)$ は

$$\mathbf{a}_j = t_1\mathbf{a}_1 + \cdots + t_s\mathbf{a}_s \qquad (t_1,\ \cdots, t_s \in \mathbb{K}) \qquad \cdots\cdots\cdots\cdots (※)$$

のように書ける (演習 21-2)。

線形写像 F_A の像 $\mathrm{Im}\, F_A$ は A の列ベクトル $\mathbf{a}_1, \cdots, \mathbf{a}_n$ によって張られる (例 21-1) ので、(※) から $\{\mathbf{a}_1, \cdots, \mathbf{a}_s\}$ は $\mathrm{Im}\, F_A$ を張る線形独立なベクトルの集合、すなわち、基底になっていることがわかる。これより、Ⅱ は証明された。 □

演習 21-2　上の定理の証明中の (※) が成り立つことを証明せよ。

演習 21-3　$a \in \mathbb{R}$ とする。4 次元実ベクトル $\begin{pmatrix} 1 \\ 1 \\ 0 \\ a \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \\ a \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ a \\ 1-a \\ a \end{pmatrix}$ が $\mathbb{R}$ 上線形独立になるための a に関する必要十分条件を求めよ。

例 21-6　4 つのベクトル $\mathbf{a}_1 = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}$, $\mathbf{a}_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$, $\mathbf{a}_3 = \begin{pmatrix} -2 \\ 0 \\ -2 \end{pmatrix}$, $\mathbf{a}_4 = \begin{pmatrix} -1 \\ 4 \\ -2 \end{pmatrix}$ によって張られる $\mathbb{R}^3$ の部分空間 V の次元と 1 組の基底を求めよ。

解；

定義により

$$V = \{\ t_1\mathbf{a}_1 + t_2\mathbf{a}_2 + t_3\mathbf{a}_3 + t_4\mathbf{a}_4 \mid t_1,\ t_2,\ t_3,\ t_4 \in \mathbb{R}\ \}$$

である。$A = (\mathbf{a}_1\ \mathbf{a}_2\ \mathbf{a}_3\ \mathbf{a}_4)$ とおくとき、V は線形写像 $F_A : \mathbb{R}^4 \longrightarrow \mathbb{R}^3$, $F_A(\mathbf{x}) = A\mathbf{x}$ の像 $\mathrm{Im}\, F_A$ と一致する。定理 21-4 から $\mathrm{rank}\, A = \dim(\mathrm{Im}\, F_A) = \dim V$ なので、V の次元を求

めるには $\operatorname{rank} A$ を計算すればよい。基本変形によって、

$$A \xrightarrow{(\sharp 1)} \begin{pmatrix} 1 & 2 & -2 & -1 \\ 0 & -3 & 4 & 6 \\ 0 & 6 & -8 & -5 \end{pmatrix} \xrightarrow{(\sharp 2)} \begin{pmatrix} 1 & 2 & -2 & -1 \\ 0 & -3 & 4 & 6 \\ 0 & 0 & 0 & 7 \end{pmatrix}$$

$$\xrightarrow{(\sharp 3)} \underbrace{\begin{pmatrix} 1 & 2 & -1 & -2 \\ 0 & -3 & 6 & 4 \\ 0 & 0 & 7 & 0 \end{pmatrix}} \xrightarrow{(\sharp 4)} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = F_{3,4}(3)$$

であるから $\dim V = \operatorname{rank} A = 3$ とわかる。

次に、V の基底を求めよう。定理21-4の証明から (あるいは、下の定理21-7から) $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4$ の中の $\mathbb{R}$ 上線形独立な3つのベクトルからなる集合が V の基底である。

波線のついている行列を $B = (\mathbf{b}_1\ \mathbf{b}_2\ \mathbf{b}_3\ \mathbf{b}_4)$ とおく。$\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ は $\mathbb{R}$ 上線形独立であることが簡単にわかる。$(\sharp 3)$ では第3列と第4列の入れ換えを行っているから、$(\sharp 3)$ を施す直前の行列 $C = (\mathbf{c}_1\ \mathbf{c}_2\ \mathbf{c}_3\ \mathbf{c}_4)$ において $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4$ は $\mathbb{R}$ 上線形独立である。行基本変形では線形独立な列ベクトルの場所は変わらない (補題21-5の下の注意参照) から、$(\sharp 1)$, $(\sharp 2)$ の前後では線形独立な列ベクトルの場所は変わらない。したがって、$\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_4$ は $\mathbb{R}$ 上線形独立である。よって、$\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_4\}$ は V の基底である。 □

演習 21-4* $\begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix}$ によって張られる $\mathbb{R}^3$ の部分空間 V の次元とその1組の基底を求めよ。

●定理 21-4 の応用

部分空間 $V \subset \mathbb{K}^n$ の基底とは、

① $\mathbb{K}$ 上線形独立であり、　② V を張る

ような $\mathbb{K}^n$ のベクトルからなる集合のことでした。したがって、$\mathbb{K}^n$ の部分集合が V の基底であるかどうかを知るには、①と②の両方が成り立つかどうかを確認する必要があります。しかしながら、例21-6のように V の次元 $\dim V$ があらかじめわかるときには、例えば、$\dim V = d$ であるときには、d 個の元からなる V の部分集合 $\{\mathbf{a}_1, \cdots, \mathbf{a}_d\}$ が V の基底であることを示すには、①か②のどちらか一方のみ示せば十分です。すなわち、次が成り立ちます。

定理 21-7

V を数ベクトル空間 $\mathbb{K}^n$ の部分空間とする。$\dim V = d$ であるとき、V に属する d 個のベクトル $\mathbf{a}_1, \cdots, \mathbf{a}_d$ について、次の3つは互いに同値である。

① $\{\mathbf{a}_1, \cdots, \mathbf{a}_d\}$ は V の基底である。
② $\mathbf{a}_1, \cdots, \mathbf{a}_d$ は $\mathbb{K}$ 上線形独立である。
③ $\mathbf{a}_1, \cdots, \mathbf{a}_d$ は V を張る。

(**proof**)

②と③が同値であることを証明すれば十分である。

- 「② $\Longrightarrow$ ③」の証明：

$\dim V = d$ なので、d 個の元からなる V の基底 $\{\mathbf{v}_1, \cdots, \mathbf{v}_d\}$ が存在する。このとき、写像 $F : V \longrightarrow \mathbb{K}^d$ を

$$F(t_1\mathbf{v}_1 + \cdots + t_d\mathbf{v}_d) = \begin{pmatrix} t_1 \\ \vdots \\ t_d \end{pmatrix}$$

によって定義することができる。F は全単射な $\mathbb{K}$-線形写像である。$\mathbb{K}^d$ に属する $(d+1)$ 個のベクトルは $\mathbb{K}$ 上線形独立でない（補題 20-10）ので、F を通して、V に属する $(d+1)$ 個のベクトルも $\mathbb{K}$ 上線形独立でないことがわかる。よって、任意の $\mathbf{v} \in V$ に対して、$\mathbf{a}_1, \cdots, \mathbf{a}_d, \mathbf{v}$ は $\mathbb{K}$ 上線形独立でない。仮定により、$\mathbf{a}_1, \cdots, \mathbf{a}_d$ は $\mathbb{K}$ 上線形独立なので、演習 21-2 と同様の考察により、

$$\mathbf{v} = t_1\mathbf{a}_1 + \cdots + t_d\mathbf{a}_d \quad (t_1, \cdots, t_d \in \mathbb{K})$$

と書き表わせることがわかる。故に、$\mathbf{a}_1, \cdots, \mathbf{a}_d$ は V を張る。

- 「③ $\Longrightarrow$ ②」の証明：

$A := (\mathbf{a}_1 \ \cdots \ \mathbf{a}_d) \in \mathrm{M}_{nd}(\mathbb{K})$ とおくと、V は線形写像 $F_A : \mathbb{K}^d \longrightarrow \mathbb{K}^n$ の像 $\mathrm{Im}\, F_A$ に一致する。定理 21-4 により、$d = \dim V = \mathrm{Im}\, F_A$ は A の列ベクトルの中の線形独立なものの最大個数なので、$\mathbf{a}_1, \cdots, \mathbf{a}_d$ は $\mathbb{K}$ 上線形独立でなければならない。 □

●連立一次方程式の非自明な解の存在条件

$A \in \mathrm{M}_{mn}(\mathbb{K})$ を係数行列とする連立一次方程式 $A\mathbf{x} = \mathbf{0}$ は常に $\mathbf{x} = \mathbf{0}$ を解に持ちます。この解を**自明な解**といいます。定理 21-4 の系として次の結果が得られます。

系 21-8

$A \in \mathrm{M}_{mn}(\mathbb{K})$ とし、$\mathrm{rank}\, A = r$ とおく。このとき、連立一次方程式 $A\mathbf{x} = \mathbf{0}$ が自明でない解 $\mathbf{x} \in \mathbb{K}^n$ を持つための必要十分条件は、$r < n$ となることである。したがって、特に、$m < n$ ならば、常に、連立一次方程式 $A\mathbf{x} = \mathbf{0}$ は自明でない解を $\mathbb{K}^n$ 内に持つ。

(**proof**)

A の列ベクトルを $\mathbf{a}_1, \cdots, \mathbf{a}_n$ とおくと、定理 21-3 により、次が成り立つ。

$$\begin{aligned} r < n &\iff \mathbf{a}_1, \cdots, \mathbf{a}_n \text{ は } \mathbb{K} \text{ 上線形独立でない。} \\ &\iff t_1\mathbf{a}_1 + \cdots + t_n\mathbf{a}_n = \mathbf{0} \text{ となる } \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \neq \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in \mathbb{K}^n \text{ が存在する} \\ &\iff A\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = \mathbf{0} \text{ となる } \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \neq \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in \mathbb{K}^n \text{ が存在する} \\ &\iff \text{連立一次方程式 } A\mathbf{x} = \mathbf{0} \text{ は自明でない解を } \mathbb{K}^n \text{ 内に持つ。} \ \square \end{aligned}$$

●線形写像の行列表示

第 13 節において、線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ から行列 が定まることを学びました (命題 13-8)。この行列 A は $\mathbb{K}^n$ のベクトル

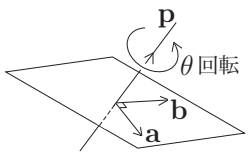
$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ \cdots, \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

の F による像を並べることにより与えられるのでした：$A = (F(\mathbf{e}_1)\ F(\mathbf{e}_2)\ \cdots\ F(\mathbf{e}_n))$. ここでは、この作り方を一般化します。線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ と $\mathbb{K}^n$, $\mathbb{K}^m$ の基底が指定されたときに、行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ を作る方法を説明します。

まず、次の問題を考えてみて下さい。

演習 21-5 * $\mathbf{p} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix} \in \mathbb{R}^3$ とおく。$\mathbb{R}$-線形写像 $F : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ を直線 $L = \{t\mathbf{p} \mid t \in \mathbb{R}\}$ を軸とする θ 回転とする。但し、回転の方向は、原点から $\mathbf{p}$ へ向かって右ネジが進むときの回転の方向と一致するものとする。

(1) $\mathbf{a} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\\0\end{pmatrix}$, $\mathbf{b} = \frac{1}{\sqrt{6}}\begin{pmatrix}1\\1\\-2\end{pmatrix}$ とおくとき、$\{\mathbf{a}, \mathbf{b}, \mathbf{p}\}$ は $\mathbb{R}^3$ の基底であることを示せ。



(2) $F(\mathbf{a})$, $F(\mathbf{b})$, $F(\mathbf{p})$ のそれぞれを $\mathbf{a}, \mathbf{b}, \mathbf{p}$ の $\mathbb{R}$-線形結合で表せ。

線形写像の行列表示を定義するためには、順序基底の概念が必要です。

数ベクトル空間 $\mathbb{K}^n$ の**順序基底** (ordered basis) とは、$\mathbb{K}^n$ の基底 $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ の要素に順番を付けたもののことをいいます。順序基底は基底の要素の組 $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ によって表わします。

$\mathbb{K}^n$ の順序基底 $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ と $\mathbb{K}^m$ の順序基底 $(\mathbf{w}_1, \cdots, \mathbf{w}_m)$ が与えられると、$\mathbb{K}$-線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ から行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ を以下のようにして定めることができます。まず、各ベクトル $F(\mathbf{v}_j)$ $(j = 1, \cdots, n)$ を $\mathbf{w}_1, \cdots, \mathbf{w}_m$ の線形結合として

$$F(\mathbf{v}_j) = a_{1j}\mathbf{w}_1 + \cdots + a_{mj}\mathbf{w}_m \quad (a_{ij} \in \mathbb{K})$$

のように書き表わします ($\{\mathbf{w}_1, \cdots, \mathbf{w}_m\}$ は $\mathbb{K}^m$ の基底なので、$a_{1j}, \cdots, a_{mj}$ は $\mathbf{v}_j$ に対して一意的に定まることに注意して下さい)。ここに現われた mn 個の $\mathbb{K}$ の元 a_{ij} を並べて、行列

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

を作ります。この A を $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ と $(\mathbf{w}_1, \cdots, \mathbf{w}_m)$ に関する F の**行列表示**といいます。F の行列表示は、

$$(F(\mathbf{v}_1)\ \cdots\ F(\mathbf{v}_n)) = (\mathbf{w}_1\ \cdots\ \mathbf{w}_m)A$$

を満たす行列 $A \in \mathrm{M}_{mn}(\mathbb{K})$ として特徴づけられます。

注意：1. $\mathbb{K}^n$ の標準順序基底とは、$\mathbb{K}^n$ の n 個のベクトル

$$\mathbf{e}_1 := \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},\ \mathbf{e}_2 := \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix},\ \cdots, \mathbf{e}_n := \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix} \quad \left(\begin{array}{l}\text{各 } \mathbf{e}_i\ (i = 1, \cdots, n) \text{ は第 } i \text{ 成分}\\ \text{だけ 1 で、残りの成分は 0 であ}\\ \text{るような } \mathbb{K}^n \text{ のベクトルを表わす}\end{array}\right)$$

を並べて得られる順序基底 $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ のことをいいます。$\mathbb{K}^n$ の標準順序基底と $\mathbb{K}^m$ の標準順序基底に関する $\mathbb{K}$-線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ の行列表示は、$A = (F(\mathbf{e}_1)\ \cdots\ F(\mathbf{e}_n))$ によって与えられます。したがって、標準順序基底に関する F の行列表示は命題 13-8 の証明で与えられているものと一致します。

2. $m = n$ の場合、$(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ と $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ に関する F の行列表示のことを、単に、$(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ に関する F の行列表示といいます。

3. 多くの教科書では、順序基底のことを単に基底と呼んでいますが、線形写像の行列表示が基底の要素の並べ方にも依存することを強調するために、このプリントでは、敢えて、順序基底という言葉を使いました。

演習 21-6 * 演習 21-5 の $\mathbb{R}$-線形写像 $F : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ とその (1) で与えられた基底 $\{\mathbf{a}, \mathbf{b}, \mathbf{p}\}$ を考える。
(1) 順序基底 $(\mathbf{a}, \mathbf{b}, \mathbf{p})$ に関する F の行列表示を求めよ。
(2) 標準順序基底 $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ に関する F の行列表示を求めよ。

ヒント：(2) については、まず、$\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ のそれぞれが $\mathbf{a}, \mathbf{b}, \mathbf{p}$ の $\mathbb{R}$-線形結合としてどのように表わされるのか、計算する。次に、演習 21-5(2) を使って $F(\mathbf{e}_1), F(\mathbf{e}_2), F(\mathbf{e}_3)$ を計算する。

定理 21-9
$\mathbb{K}$-線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ は、$\mathbb{K}^n$ の順序基底と $\mathbb{K}^m$ の順序基底を適当に選んで行列表示すると標準形 $F_{m,n}(r)$ になる。但し、$r = \dim(\mathrm{Im}\, F)$ である。

(**proof**)
$(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ を $\mathbb{K}^n$ の標準順序基底とし、$(\mathbf{e}'_1, \cdots, \mathbf{e}'_m)$ を $\mathbb{K}^m$ の標準順序基底とする。これら 2 つの順序基底に関する F の行列表示を A とおくと $F = F_A$ となる。定理 19-6 から、$PAQ = F_{m,n}(r)$ となる正則行列 $P \in \mathrm{M}_m(\mathbb{K})$, $Q \in \mathrm{M}_n(\mathbb{K})$ と整数 r が存在する。定理 21-4(の証明) により、$r = \dim(\mathrm{Im}\, F_A) = \dim(\mathrm{Im}\, F)$ である。

$\mathbf{v}_1 := Q\mathbf{e}_1, \cdots, \mathbf{v}_n := Q\mathbf{e}_n$ とおくと、Q は正則であるから $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ は $\mathbb{K}^n$ の基底になる (補題 21-5 と定理 21-7)。同様に、$\mathbf{w}_1 := P^{-1}\mathbf{e}'_1, \cdots, \mathbf{w}_m := P^{-1}\mathbf{e}'_m$ とおくと、P は正則である (したがって、P^{-1} も正則である) から、$\{\mathbf{w}_1, \cdots, \mathbf{w}_m\}$ は $\mathbb{K}^m$ の基底になる。このとき、$\mathbb{K}^n$ の順序基底 $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ と $\mathbb{K}^m$ の順序基底 $(\mathbf{w}_1, \cdots, \mathbf{w}_m)$ に関する線形写像 $F = F_A$ の行列表示は PAQ である。実際、$PAQ = (b_{ij})$ とおくと、$j = 1, \cdots, n$ に対して

$$\begin{aligned} F_A(\mathbf{v}_j) = A\mathbf{v}_j = AQ\mathbf{e}_j = P^{-1}PAQ\mathbf{e}_j \\ = P^{-1}\begin{pmatrix} b_{1j} \\ \vdots \\ b_{mj} \end{pmatrix} = P^{-1}(b_{1j}\mathbf{e}'_1 + \cdots + b_{mj}\mathbf{e}'_m) \\ = b_{1j}P^{-1}\mathbf{e}'_1 + \cdots + b_{mj}P^{-1}\mathbf{e}'_m \\ = b_{1j}\mathbf{w}_1 + \cdots + b_{mj}\mathbf{w}_m \end{aligned}$$

となる。 □

注意：定理 21-9 は、定義域と終域の順序基底をうまく選んで座標変換すれば、線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ は最初の r 成分への射影と思えることを主張しています。一般の m, n についての線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ の標準化の問題はこれで解決したといえます。次に問題になるのは、$m = n$ の場合です。この場合には、定義域と終域の順序基底として同じものをとり、線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ の行列表示を考えることができます。残念ながら今度は、定理 21-9 のような単純なことは成立しません。しかしながら、「同じ順序基底をとる」という制限をつけることにより、線形写像 $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ についてのより深い情報を引き出すことができます。この問題は固有値問題と関連して、理論的側面と応用的側面の両方から重要です。

§22. 定積分

この節は、数列の極限や関数の連続性の定義で用いた方法と似た方法で、関数の定積分を定義し、その基本的性質を導きます。最後に、閉区間上で定義された任意の連続関数は定積分可能であることを証明します。ここでの目標は定積分の定義を‘$\varepsilon-\delta$ 論法’に基づいて理解することです。

§22-1 定積分の定義とその基本的性質

ここでは、関数の定積分の定義を‘$\varepsilon-\delta$ 式’に与えて、その定義に基づいて定積分の諸性質を導きます。

●閉区間の分割

閉区間 $[a,b]$ の**分割** (division into subintervals) とは、閉区間の有限列 $I_1,\cdots,I_n$ であって、次の 4 つの条件を満たすものをいいます。

①任意の $i=1,\cdots,n-1$ に対して、$I_i\cap I_{i+1}$ は 1 点からなる集合である。
②任意の $i,j=1,\cdots,n-1,\ j-i\geq 2$ に対して、$I_i\cap I_j=\varnothing$ である。
③$I_1\cup\cdots\cup I_n=[a,b]$.
④$a\in I_1,\ b\in I_n$.

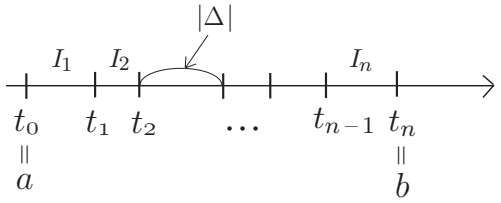
$I_i\cap I_{i+1}=\{t_i\}$ $(i=1,\cdots,n-1)$ であるような $[a,b]$ の分割 Δ を

$$\Delta : a=t_0<t_1<\cdots<t_{n-1}<t_n=b$$

と書き表わします。$[a,b]$ の分割 $\Delta : a=t_0<t_1<\cdots<t_{n-1}<t_n=b$ に対して、

$$|\Delta|:=\max\{t_1-t_0,\cdots,t_{n-1}-t_n\}$$

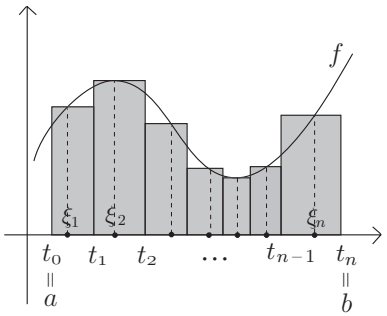
を分割 Δ の**細かさ** (mesh) と呼び、各 t_i $(i=0,1,\cdots,n)$ を分割 Δ の**分点**と呼びます。



●定積分の定義

f を閉区間 $[a,b]$ を定義域に含む 1 変数実数値関数とします。$[a,b]$ の分割 $\Delta : a=t_0<t_1<\cdots<t_{n-1}<t_n=b$ と、各区間 $[t_{i-1},t_i]$ から任意に一点 ξ_i を取って作った $\xi=(\xi_1,\cdots,\xi_n)\in\mathbb{R}^n$ に対して、実数 $S_{\Delta,\xi}(f)$ を次式で定めます：

$$S_{\Delta,\xi}(f):=\sum_{i=1}^{n}f(\xi_i)(t_i-t_{i-1}).$$



定義 22-1

関数 $f:S\longrightarrow\mathbb{R}$ の定義域 $S\subset\mathbb{R}$ は閉区間 $[a,b]$ を含んでいるとする。
$\gamma\in\mathbb{R}$ が関数 f の $[a,b]$ 上での**定積分** (definite integral) であるとは、任意の $\varepsilon>0$ に対して、次の条件 $(*)$ を満たす $\delta>0$ が存在するときをいう：

(∗) $|\Delta| < \delta$ を満たす任意の分割 $\Delta : a = t_0 < t_1 < \cdots < t_n = b$ と $\xi_i \in [t_{i-1}, t_i]$ $(i = 1, \cdots, n)$ を満たす任意の $\xi = (\xi_1, \cdots, \xi_n) \in \mathbb{R}^n$ に対して、$|S_{\Delta,\xi}(f) - \gamma| < \varepsilon$.

上のような γ が存在するとき、関数 f は $[a, b]$ 上で (リーマン) **積分可能** (integrable in the sense of Riemann) であるといい、γ を $\int_a^b f(t)dt$ によって表わす：$\gamma = \int_a^b f(t)dt$.

注意：定積分を表記するときに変数 t を用いましたが、この変数を t ではなく別の文字に変えても構いません。例えば、

$$\int_a^b f(t)dt = \int_a^b f(x)dx = \int_a^b f(\theta)d\theta.$$

演習 22-1　$r \in \mathbb{R}$ への定数関数 f について、閉区間 $[a, b]$ 上での定積分を定義に基づいて求めよ。

●定積分の性質

定積分は線形性 (次の補題の (1)) と単調性 (次の補題の (2)) を持ちます。

補題 22-2

f, g を閉区間 $[a, b]$ 上で積分可能な 2 つの実数値関数とする。このとき、

(1) (i) 和 $f + g$ は $[a, b]$ 上で積分可能であって、

$$\int_a^b (f + g)(x)dx = \int_a^b f(x)dx + \int_a^b g(x)dx.$$

(ii) $\alpha \in \mathbb{R}$ に対して、αf は $[a, b]$ 上で積分可能であって、

$$\int_a^b (\alpha f)(x)dx = \alpha \int_a^b f(x)dx.$$

(2) 任意の $x \in [a, b]$ に対して $f(x) \geq g(x)$ ならば、

$$\int_a^b f(x)dx \geq \int_a^b g(x)dx.$$

(**proof**)

(1) を演習問題として残し、(2) を証明しよう。

$h(x) := f(x) - g(x)$ $(x \in [a, b])$ によって関数 $h : [a, b] \longrightarrow \mathbb{R}$ を定めると、任意の $x \in [a, b]$ に対して $h(x) \geq 0$ が成り立ち、(1) により h は $[a, b]$ 上で積分可能である。(1) によって、$\gamma := \int_a^b h(x)dx \geq 0$ となることを証明すればよい。

背理法で示す。$\gamma < 0$ であると仮定する。h は $[a, b]$ 上で積分可能であるから、$\varepsilon := -\gamma > 0$ に対して、定義 22-1 の条件 (∗) を満たす $\delta > 0$ が存在する。したがって、$|\Delta| < \delta$ を満たす $[a, b]$ の分割 $\Delta : a = t_0 < t_1 < \cdots < t_n = b$ を 1 つ取って $\xi = (t_1, \cdots, t_n) \in \mathbb{R}^n$ を考えると、$S_{\Delta,\xi}(h) < \gamma + \varepsilon = 0$ が成り立つ。一方、$h(t_i) \geq 0$ $(i = 1, \cdots, n)$ であるから、$S_{\Delta,\xi}(h) = \sum_{i=1}^{n} h(t_i)(t_i - t_{i-1}) \geq 0$ である。ここに矛盾が生じた。故に、$\gamma \geq 0$ である。　□

演習 22-2* 上の補題 (1)(i) を証明せよ。

●有界な関数

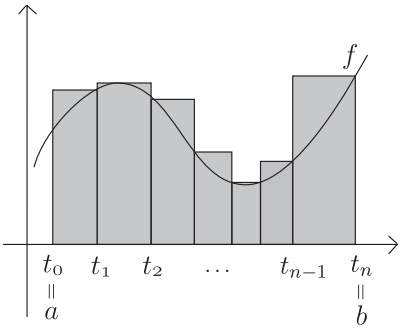
実数値関数 $f : S \longrightarrow \mathbb{R}$ が**有界** (bounded) であるとは、f の値域 $f(S) = \{\ f(s) \mid s \in S\ \}$ が $\mathbb{R}$ の有界な部分集合であるときをいいます。

●過剰和と不足和

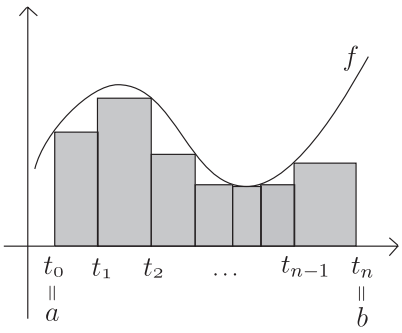
$f:[a,b]\longrightarrow\mathbb{R}$ を有界な関数とし、$[a,b]$ の分割 $\Delta: a=t_0<t_1<\cdots<t_n=b$ を考えます。各 $i=1,\cdots,n$ に対して、$M_i:=\sup f([t_{i-1},t_i]),\ m_i:=\inf f([t_{i-1},t_i])$ と定めて、

$$S_\Delta(f):=\sum_{i=1}^{n}M_i(t_i-t_{i-1}),\qquad s_\Delta(f):=\sum_{i=1}^{n}m_i(t_i-t_{i-1})$$

とおきます。$S_\Delta(f), s_\Delta(f)$ をそれぞれ分割 Δ に関する f の**過剰和**、**不足和**といいます。



過剰和 $S_\Delta(f)$



不足和 $s_\Delta(f)$

$M:=\sup f([a,b]),\ m:=\inf f([a,b])$ とおくと、

$$m(b-a)\le s_\Delta(f)\le S_\Delta(f)\le M(b-a)$$

が成り立つので、集合 $\{\ S_\Delta(f)\mid\Delta$ は $[a,b]$ の分割 $\}$, $\{\ s_\Delta(f)\mid\Delta$ は $[a,b]$ の分割 $\}$ はそれぞれ下に有界、上に有界です。したがって、

$$S(f):=\inf\{\ S_\Delta(f)\mid\Delta\text{ は }[a,b]\text{ の分割}\},\quad s(f):=\sup\{\ s_\Delta(f)\mid\Delta\text{ は }[a,b]\text{ の分割}\}$$

の存在がわかります (定理 7-9)。

●分割の細分

閉区間 $[a,b]$ の分割 $\Delta: a=t_0<t_1<\cdots<t_n=b$ とその分点でない $c\in[a,b]$ をとります。このとき、$t_{i-1}<c<t_i$ を満たす $i\in\{1,\cdots,n\}$ が一意的に存在するので、$[a,b]$ の新しい分割

$$\Delta[c]: a=t_0<\cdots<t_{i-1}<c<t_i<\cdots<t_n=b$$

を作ることができます。この $\Delta[c]$ を Δ の初等細分と呼ぶことにします。

$[a,b]$ の分割 Δ' が Δ の**細分** (subdivision) であるとは、Δ から出発して、次々と初等細分を有限回施して、Δ' が得られるときをいいます。

演習 22-3 * $f:[a,b]\longrightarrow\mathbb{R}$ を有界な関数とする。$[a,b]$ の分割 Δ とその細分 Δ' に対して、

$$s_\Delta(f)\le s_{\Delta'}(f),\qquad S_{\Delta'}(f)\le S_\Delta(f)$$

が成り立つことを示せ。

演習 22-4 有界な関数 $f:[a,b]\longrightarrow\mathbb{R}$ に対して、$s(f)\le S(f)$ が成り立つことを示せ。

ヒント：$[a,b]$ の任意の分割 Δ_1,Δ_2 に対して、$s_{\Delta_1}(f)\le S_{\Delta_2}(f)$ が成り立つことを示せばよい。Δ_1,Δ_2 の両方の分点を合わせて得られる分割 Δ_3 を考えることによりこれを示す。

●ダルブー (Darboux, 1842–1917) の定理

ダルブーの定理は連続関数の積分可能性の証明で鍵となる重要な定理です。

定理 22-3 (ダルブーの定理)

$f : [a,b] \longrightarrow \mathbb{R}$ を有界な関数とするとき、次が成り立つ。

(1) $\forall \varepsilon > 0,\ \exists \delta > 0$ s.t. $\Delta : [a,b]$ の分割, $|\Delta| < \delta \ \Rightarrow\ S_\Delta(f) - S(f) < \varepsilon$.

(2) $\forall \varepsilon > 0,\ \exists \delta > 0$ s.t. $\Delta : [a,b]$ の分割, $|\Delta| < \delta \ \Rightarrow\ s(f) - s_\Delta(f) < \varepsilon$.

(**proof**)

(1) も (2) も同様の方法で証明できるので、ここでは (1) のみ証明する。

$\varepsilon > 0$ を任意にとる。このとき、$S(f)$ の定義から、次が成り立つ。

$$\exists\, \Delta_0 : a = x_0 < x_1 < \cdots < x_N = b : [a,b] \text{ の分割 s.t. } S_{\Delta_0}(f) < S(f) + \tfrac{\varepsilon}{2}.$$

$[a,b]$ の分割 $\Delta : a = t_0 < t_1 < \cdots < t_n = b$ であって、$|\Delta| < \min\{x_1 - x_0, \cdots, x_N - x_{N-1}\}$ を満たすものを考える。各 $[t_{i-1}, t_i]$ には、Δ_0 の分点は高々 1 つしか属さないから、

$$I := \{\ i \in \{1, \cdots, n\} \mid (t_{i-1}, t_i] \text{ は } \Delta_0 \text{ の分点を含む }\}$$

はちょうど N 個の元からなる。

Δ と Δ_0 の分点を合わせて得られる $[a,b]$ の分割を Δ' とおき、$S_\Delta(f) - S_{\Delta'}(f)$ を評価する。$i = 1, \cdots, n$ に対して $M_i = \sup f([t_{i-1}, t_i])$ と定める。また、$i \in I$ に対しては、区間 $(t_{i-1}, t_i]$ に属する Δ_0 の分点を x_{p_i} とおき、$M_{i1} = \sup f([t_{i-1}, x_{p_i}]),\ M_{i2} = \sup f([x_{p_i}, t_i])$ と定める。このとき、$J := \{1, \cdots, n\} - I$ とおくと

$$S_\Delta(f) = \sum_{i \in I} M_i(t_i - t_{i-1}) + \sum_{j \in J} M_j(t_j - t_{j-1})$$

$$S_{\Delta'}(f) = \sum_{i \in I} (M_{i1}(x_{p_i} - t_{i-1}) + M_{i2}(t_i - x_{p_i})) + \sum_{j \in J} M_j(t_j - t_{j-1})$$

が成り立つ。$M := \sup f([a,b]),\ m = \inf f([a,b])$ とおくと、各 $i \in I$ に対して

$$M_i(t_i - t_{i-1}) - (M_{i1}(x_{p_i} - t_{i-1}) + M_{i2}(t_i - x_{p_i})) \le (M - m)(t_i - t_{i-1}) \le (M - m)|\Delta|$$

となるので、$S_\Delta(f) - S_{\Delta'}(f) \le (M - m)|\Delta|N$ を得る。そこで、実数 $\delta > 0$ を

$$\delta := \min\{\ \tfrac{\varepsilon}{2(M-m)N},\ \min\{x_1 - x_0, \cdots, x_N - x_{N-1}\}\}$$

と定める。$|\Delta| < \delta$ を満たす任意の分割 $\Delta : a = t_0 < t_1 < \cdots < t_n = b$ に対して、Δ と Δ_0 の分点を合わせて得られる $[a,b]$ の分割 Δ' は $S_{\Delta'} \le S_{\Delta_0}$ を満たすから (演習 22-3)、

$$\begin{aligned} S_\Delta(f) - S(f) &= (S_\Delta(f) - S_{\Delta'}(f)) + (S_{\Delta'}(f) - S_{\Delta_0}(f)) + (S_{\Delta_0}(f) - S(f)) \\ &\le (S_\Delta(f) - S_{\Delta'}(f)) + (S_{\Delta_0}(f) - S(f)) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \end{aligned}$$

を得る。これで (1) は証明された。 □

系 22-4

$f : [a,b] \longrightarrow \mathbb{R}$ を有界な関数とするとき、次が成り立つ：

$$f \text{ は積分可能である } \iff\ S(f) = s(f)$$

(**proof**)
「$\Longrightarrow$」の証明：$\gamma = \int_a^b f(t)dt$ とおく。

任意に $\varepsilon > 0$ をとると、次の条件を満たす $\delta > 0$ が存在する：

$|\Delta| < \delta$ を満たすすべての $[a,b]$ の分割 $\Delta : a = t_0 < t_1 < \cdots < t_n = b$ とすべての $\xi_i \in [t_{i-1}, t_i]$ $(i = 1, \cdots, n)$ について、$|S_{\Delta,(\xi_1,\cdots,\xi_n)}(f) - \gamma| < \frac{\varepsilon}{3}$.

今、$[a,b]$ の分割 $\Delta_0 : a = t_0 < \cdots < t_n = b$ であって、$|\Delta_0| < \delta$ かつ $S_{\Delta_0}(f) < S(f) + \frac{\varepsilon}{3}$ を満たすものを 1 つ取る (注：このような Δ_0 の存在は $S(f)$ の定義と演習 22-3 からわかる)。$M_i = \sup f([t_{i-1}, t_i])$ $(i = 1, \cdots, n)$ とおき、$\xi_i \in [t_{i-1}, t_i]$ を $M_i - \frac{\varepsilon}{3(b-a)} < f(\xi_i)$ を満たすように選ぶ。このとき、

$$|S_{\Delta_0}(f) - S_{\Delta_0,\xi}(f)| = \sum_{i=1}^{n}(M_i - f(\xi_i))(t_i - t_{i-1}) \leq \sum_{i=1}^{n} \frac{\varepsilon}{3(b-a)}(t_i - t_{i-1}) = \frac{\varepsilon}{3}$$

が成り立つ。但し、$\xi = (\xi_1, \cdots, \xi_n)$ とおいた。よって、

$$|S(f) - \gamma| \leq |S(f) - S_{\Delta_0}(f)| + |S_{\Delta_0}(f) - S_{\Delta_0,\xi}(f)| + |S_{\Delta_0,\xi}(f) - \gamma| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon$$

となり、$S(f) = \gamma$ が示された。同様にして $s(f) = \gamma$ が示されるので、$S(f) = s(f)$ を得る。
「$\Longleftarrow$」の証明：$\gamma = S(f) = s(f)$ とおき、$\varepsilon > 0$ を任意にとる。このとき、

$$\exists\, \delta_1 > 0 \ \text{ s.t. } \ \Delta : [a,b] \text{ の分割}, \ |\Delta| < \delta_1 \ \Rightarrow \ S_\Delta(f) - S(f) < \varepsilon$$

$$\exists\, \delta_2 > 0 \ \text{ s.t. } \ \Delta : [a,b] \text{ の分割}, \ |\Delta| < \delta_2 \ \Rightarrow \ s(f) - s_\Delta(f) < \varepsilon$$

が成り立つ (定理 22-3)。$\delta = \min\{\delta_1, \delta_2\}$ とおくと、$|\Delta| < \delta$ を満たす $[a,b]$ の任意の分割 $\Delta : a = t_0 < \cdots < t_n = b$ と任意の $\xi_i \in [t_{i-1}, t_i]$ $(i = 1, \cdots, n)$ に対して、

$$-\varepsilon < s_\Delta(f) - s(f) = s_\Delta(f) - \gamma \leq S_{\Delta,(\xi_1,\cdots,\xi_n)}(f) - \gamma \leq S_\Delta(f) - \gamma = S_\Delta(f) - S(f) < \varepsilon$$

となる。故に、f は $[a,b]$ 上で積分可能である。 □

演習 22-5 関数 $f : [0,1] \longrightarrow \mathbb{R}$ を $f(x) = \begin{cases} 1 & (x \text{ が有理数のとき}) \\ 0 & (x \text{ が無理数のとき}) \end{cases}$ によって定義する。f は積分不可能であることを示せ。

●区間の分割に関する定積分の加法性

定積分は、積分区間を分割すると、分割されたそれぞれの区間上での定積分の和になります。

補題 22-5

有界な関数 $f : [a,b] \longrightarrow \mathbb{R}$ と、$a < c < b$ を満たす任意の実数 c に対して、

f は $[a,b]$ 上で積分可能 $\iff$ f は $[a,c]$ 上で積分可能、かつ、$[c,b]$ 上で積分可能

が成り立つ。このとき、さらに、次の等式が成り立つ。

$$(*) \qquad \int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx$$

(**proof**)

f の定義域を $[a,c]$, $[c,b]$ に制限した関数をそれぞれ f_1, f_2 とおく。

- 「$\Longrightarrow$」の証明：

$[a,b]$ の任意の分割 Δ に対して、c を分点に付け加えて得られる $[a,b]$ の分割を Δ' とおく。さらに、Δ' を $[a,c]$ の分割 Δ_1 と $[c,b]$ の分割 Δ_2 の２つに分ける：$\Delta = \Delta_1 \cup \Delta_2,\ \Delta_1 \cap \Delta_2 = \{c\}$. このとき、

$$s_\Delta(f) \le s_{\Delta'}(f) = s_{\Delta_1}(f_1) + s_{\Delta_2}(f_2) \le s(f_1) + s(f_2)$$

であるから、

$$s(f) = \sup\{\ s_\Delta(f) \mid \Delta \text{ は } [a,b] \text{ の分割}\ \} \le s(f_1) + s(f_2)$$

がわかる。同様にして、

$$S(f_1) + S(f_2) \le \inf\{\ S_\Delta(f) \mid \Delta \text{ は } [a,b] \text{ の分割}\ \} = S(f)$$

がわかる。よって、

$$s(f) \le s(f_1) + s(f_2) \le S(f_1) + S(f_2) \le S(f)$$

を得る。ここで $S(f) = s(f)$ (仮定と系 22-4) と $s(f_1) \le S(f_1),\ s(f_2) \le S(f_2)$ を使って、$s(f_1) = S(f_1),\ s(f_2) = S(f_2)$ が得られる。よって、f は $[a,c],\ [c,b]$ 上で積分可能であり、等式 $(*)$ が成り立つ。

- 「$\Longleftarrow$」の証明：

$[a,c],\ [c,b]$ の任意の分割をそれぞれ Δ_1, Δ_2 として、それらを合わせて $[a,b]$ の分割 Δ を作る。すると、

$$s_{\Delta_1}(f_1) + s_{\Delta_2}(f_2) = s_\Delta(f) \le s(f), \quad S(f) \le S_\Delta(f) = S_{\Delta_1}(f_1) + S_{\Delta_2}(f_2)$$

が成り立つ。したがって、

$$s(f_1) + s(f_2) \le s(f), \qquad S(f) \le S(f_1) + S(f_2)$$

である。一般に $s(f) \le S(f)$ であるが、仮定により $s(f_1) = S(f_1),\ s(f_2) = S(f_2)$ なので、上の不等式から $s(f) = S(f)$ でなければならない。よって、f は $[a,b]$ 上で積分可能である。 □

閉区間 $[a,b] \subset S$ 上で積分可能な関数 $f : S \longrightarrow \mathbb{R}$ に対して、

$$\int_b^a f(t)dt = -\int_a^b f(t)dt$$

と定めます。また、任意の実数 a に対して

$$\int_a^a f(t)dt = 0$$

と定めます。このとき、補題 22-5 の等式 $(*)$ は $(a,b,c$ の大小関係に無関係に) すべての実数 a,b,c について成り立つことがわかります。

§22-2 連続関数の定積分可能性

この節では、連続関数は閉区間上で積分可能であることを証明します。証明には、閉区間上で定義された連続関数についての２つの定理—最大値・最小値の存在定理と一様連続性の定理—を使いますので、それらを最初に説明します。

●関数の最大値と最小値

集合 S 上で定義された実数値関数 $f : S \longrightarrow \mathbb{R}$ に対して、値域 $f(S) = \{\ f(s) \mid s \in S\ \}$ に最大元が存在するとき、f は**最大値** (maximal value) を持つといい、最大元 $\max f(S)$ を f の

最大値と呼びます。同様に、$f(S)$ に最小元が存在するとき、f は**最小値** (minimal value) を持つといい、最小元 $\min f(S)$ を f の最小値と呼びます。

例 22-6 関数 $f:\mathbb{R}\longrightarrow\mathbb{R},\ f(x)=2x$ は最大値も最小値も持たないが、任意の閉区間 $[a,b]$ に対して、関数 $g:[a,b]\longrightarrow\mathbb{R},\ g(x)=2x$ は最大値 $2b$ と最小値 $2a$ を持つ。

●最大値・最小値の存在定理

最大値や最小値を持たない関数は沢山ありますが、次が成り立ちます。

定理 22-7

閉区間 $[a,b]$ 上で定義された実数値連続関数 f は (必ず) 最大値と最小値を持つ。

この定理から、閉区間上で定義された連続関数 $f:[a,b]\longrightarrow\mathbb{R}$ は有界であることがわかります。定理 22-7 の証明は最後にまわします。

●関数の一様連続性

集合 $S\subset\mathbb{R}$ 上で定義された関数 $f:S\longrightarrow\mathbb{R}$ が連続であるとは、任意の点 $a\in S$ で連続であるときをいい、f が点 $a\in S$ で連続であるとは、任意の $\varepsilon>0$ に対して次の条件を満たす $\delta>0$ が存在するときをいうのでした (第 14 節参照)：

(Conti) $$x\in S,\ |x-a|<\delta\ \Rightarrow\ |f(x)-f(a)|<\varepsilon.$$

一般に、上の条件を満たす正の実数 δ は ε の選び方に依存するばかりでなく、点 a にも依存します。一様連続とは条件 (Conti) を満たす $\delta>0$ が点 $a\in S$ によらずに一定にとることができるときをいいます。

定義 22-8

集合 $S\subset\mathbb{R}$ 上で定義された関数 $f:S\longrightarrow\mathbb{R}$ が**一様連続** (uniformly continuous) であるとは、任意の $\varepsilon>0$ に対して次の条件を満たす $\delta>0$ が存在するときをいう：

(UniConti) $$x,x'\in S,\ |x-x'|<\delta\ \Rightarrow\ |f(x)-f(x')|<\varepsilon.$$

注意：定義により、一様連続関数は連続です。しかし、逆は成立しません (下の例 (2) を参照)。

例 22-9 $0\le a<1$ とし、関数 $f_a:(a,1]\longrightarrow\mathbb{R},\ f_a(x)=\frac{1}{x}\ \ (x\in(a,1])$ を考える。

(1) $a>0$ のとき f_a は一様連続である。

(2) f_0 は一様連続ではない。

(**proof**)

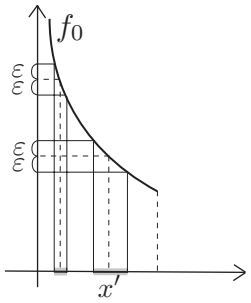
(1) 任意に $\varepsilon>0$ をとり、$\delta:=a^2\varepsilon$ とおく。$a>0$ より、$\delta>0$ である。

$|x-x'|<\delta$ を満たす $x,x'\in(a,1]$ を任意にとる。すると、

$$|f_a(x)-f_a(x')|=\Big|\frac{1}{x}-\frac{1}{x'}\Big|=\frac{|x'-x|}{|x||x'|}<\frac{1}{a^2}|x-x'|<\frac{1}{a^2}\delta=\varepsilon$$

が成り立つ。故に、f_a は一様連続である。

(2)



x' を限りなく 0 に近づけていくとき、$\delta_{x'} > 0$ を
「$|x - x'| < \delta_{x'} \quad \Rightarrow \quad |f(x) - f(x')| < \varepsilon$」
を満たすようにとるためには、$\delta_{x'}$ を際限なく
小さくしていく必要がある。

$x, x' \in (0,1]$ に対して、$\eta := x' - x$ とおくと、

$$|f_0(x) - f_0(x')| = \left|\frac{1}{x} - \frac{1}{x'}\right| = \frac{|x' - x|}{|x||x'|} = \frac{|\eta|}{|x||x + \eta|} \geq \frac{|\eta|}{|x|(|x| + |\eta|)}$$

が成り立つ。これを踏まえて、実数 η を $0 < \eta \leq \frac{1}{2}$ を満たすように取り、$x, x' \in (0,1]$ が $x' = 2\eta,\ x = \eta$ のときを考える。すると、$|f_0(x) - f_0(x')| \geq \frac{1}{2\eta} \geq 1$ となる。したがって、関数 f_0 は一様連続ではない。 □

演習 22-6 * 上の証明の下線部分を $\varepsilon - \delta$ 式の議論を使って説明せよ。

定理 22-10
閉区間 $[a,b]$ 上で定義された実数値連続関数 f は一様連続である。

この定理から、閉区間上で定義された関数に対しては、連続であることと一様連続であることとは同値になることがわかります。定理 22-10 の証明は最後にまわします。

●連続関数の定積分可能性

以上の準備の下で、次の定理を証明することができます。

定理 22-11
連続関数 $f : [a,b] \longrightarrow \mathbb{R}$ は $[a,b]$ 上で積分可能である。

(**proof**)

$\varepsilon > 0$ を任意にとると、f は一様連続である (定理 22-10) から、

$$\exists\, \delta > 0 \ \text{ s.t. } \ x, x' \in S,\ |x - x'| < \delta \ \Rightarrow\ |f(x) - f(x')| < \frac{\varepsilon}{2}$$

が成り立つ。$|\Delta| < \delta$ を満たす $[a,b]$ の任意の分割 $\Delta : a_0 = t_0 < t_1 < \cdots < t_n = b$ を考える。各 $i = 1, \cdots, n$ に対して、$M_i := \max f([t_{i-1}, t_i]),\ m_i := \min f([t_{i-1}, t_i])$ とおき、$f(c_i) = M_i,\ f(d_i) = m_i$ となる $c_i, d_i \in [t_{i-1}, t_i]$ をとる (定理 22-7)。すると、$|c_i - t_i| \leq |t_{i-1} - t_i| < \delta,\ |d_i - t_i| \leq |t_{i-1} - t_i| < \delta$ が成り立つので、

$$M_i - m_i = |f(c_i) - f(d_i)| \leq |f(c_i) - f(t_i)| + |f(t_i) - f(d_i)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

を得る。これより、

$$S(f) - s(f) \leq S_\Delta(f) - s_\Delta(f) = \sum_{i=1}^{n} (M_i - m_i)(t_{i-1} - t_i) < \sum_{i=1}^{n} \varepsilon(t_{i-1} - t_i) = \varepsilon(b - a)$$

が導かれるが、これは、$S(f) - s(f) = 0$、すなわち、$S(f) = s(f)$ を意味する。故に、系 22-4 により、f は $[a,b]$ 上で積分可能である (定理 22-7 により f は有界であることに注意)。 □

●定理 22-7 の証明

証明は次の２つの部分に分けて行う。

① $f([a,b])$ は有界である。

② $\sup f([a,b]) = \max f([a,b])$, $\inf f([a,b]) = \min f([a,b])$.

①の証明：背理法で示す。

$f([a,b])$ が有界でなかったと仮定する。このとき、$f([a,\frac{a+b}{2}])$ と $f([\frac{a+b}{2},b])$ のうち、少なくとも一方は有界でない。そこで、実数 a_1, b_1 を

$$\begin{cases} f([a,\frac{a+b}{2}]) \text{ が有界でないとき} & a_1 := a,\ b_1 := \frac{a+b}{2}, \\ f([a,\frac{a+b}{2}]) \text{ が有界なとき} & a_1 := \frac{a+b}{2},\ b_1 := b \end{cases}$$

と定める。すると、$a \le a_1 < b_1 \le b$ であって、$f([a_1,b_1])$ は有界でない。次に、$[a_1,b_1]$ を真ん中で分けて、$f([a_1,\frac{a_1+b_1}{2}])$ と $f([\frac{a_1+b_1}{2},b_1])$ を考える。この２つのうち、少なくとも一方は有界でない。そこで、実数 a_2, b_2 を

$$\begin{cases} f([a_1,\frac{a_1+b_1}{2}]) \text{ が有界でないとき} & a_2 := a_1,\ b_2 := \frac{a_1+b_1}{2}, \\ f([a_1,\frac{a_1+b_1}{2}]) \text{ が有界なとき} & a_2 := \frac{a_1+b_1}{2},\ b_2 := b_1 \end{cases}$$

と定める。すると、$a_1 \le a_2 < b_2 \le b_1$ であって、$f([a_2,b_2])$ は有界でない。以下、同様の操作を続けると、閉区間の減少列 $[a,b] \supset [a_1,b_1] \supset [a_2,b_2] \supset \cdots\cdots$ であって、条件

$$\text{「各 } n \in \mathbb{N} \text{ に対して、} f([a_n,b_n]) \text{ は有界でない、かつ、} b_n - a_n = \tfrac{b-a}{2^n}\text{」}$$

を満たすものが得られる。よって、区間縮小法の原理 (定理 8-10) より、すべての $[a_n,b_n]$ $(n = 1,2,3,\cdots)$ に共通に含まれる実数 c が唯一存在し、その実数 c は $c = \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ によって与えられる。f は点 $c \in [a,b]$ で連続であるから、

$$\exists\, \delta > 0 \ \text{ s.t. } \ x \in [a,b],\ |c-x| < \delta \ \Rightarrow\ |f(c) - f(x)| < 1$$

が成り立つ。$c = \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ なので、$[a_N,b_N] \subset [c-\delta, c+\delta]$ となる $N \in \mathbb{N}$ が存在する。この N について、$f([a_N,b_N]) \subset f([c-\delta,c+\delta]) \subset [f(c)-1, f(c)+1]$ が成り立つが、これは、$f([a_N,b_N])$ が有界でないことに矛盾する。こうして、①は証明された。

②の証明：①により $f([a,b])$ は空でない、上に有界な $\mathbb{R}$ の部分集合であることがわかるので、$\sup f([a,b])$ が存在する (定理 7-9)。$\sup f([a,b]) = \max f([a,b])$ を示すには、$\alpha := \sup f([a,b]) \in f([a,b])$ を証明すればよい。

$\alpha \notin f([a,b])$ であると仮定すると、任意の $x \in [a,b]$ に対して、$\alpha - f(x) \neq 0$ となる。したがって、関数

$$g : [a,b] \longrightarrow \mathbb{R}, \quad g(x) = \frac{1}{\alpha - f(x)} \quad (x \in [a,b])$$

を考えることができる。g は連続である（命題 14-4）から、①により、$g([a,b])$ は有界でなければならない。一方、上限の特徴づけ (命題 7-10) により、

$$\forall n \in \mathbb{N},\ \exists\, x_n \in [a,b] \ \text{ s.t. } \ \alpha - \frac{1}{n} < f(x_n)$$

が成り立つ。したがって、任意の $n \in \mathbb{N}$ について $g(x_n) > n$ となるが、これは $g([a,b])$ が有界であることに反する。故に、$\alpha \in f([a,b])$ となることが示された。

同様にして、$\inf f([a,b]) = \min f([a,b])$ を証明することができる。 □

●定理 22-10 の証明

定理 22-10 の証明のために、関数の振幅という概念を使います。

f を閉区間 $[a,b]$ 上で定義された有界な実数値関数とします。このとき、閉区間 $[a_0,b_0]\subset[a,b]$ に対して、

$$\mathcal{O}(f|_{[a_0,b_0]}) := \sup f([a_0,b_0]) - \inf f([a_0,b_0])$$

と定め、$[a_0,b_0]$ における f の**振幅** (oscillation) といいます。

補題 22-12

f を閉区間 $[a,b]$ 上で定義された実数値連続関数とする。このとき、任意の実数 $\varepsilon>0$ に対して、閉区間 $[a,b]$ の分割 $\Delta : a_0=t_0<t_1<\cdots<t_n=b$ であって、条件

(※)　　「すべての $i=1,\cdots,n$ に対して $\mathcal{O}(f|_{[t_{i-1},t_i]})<\varepsilon$ 」

を満たすものが存在する。

(**proof**)

背理法で示す。つまり、ある実数 $\varepsilon_0>0$ を取ると、どのような分割 $\Delta : a_0=t_0<t_1<\cdots<t_n=b$ についても条件 (※) は成り立たないと仮定して矛盾を導く。

閉区間 $[c,d]\subset[a,b]$ に対して、次の条件 (♯) を考える：

(♯)　$\forall\, n\in\mathbb{N},\ \forall\,\Delta : c=t_0<t_1<\cdots<t_n=d$：$[c,d]$ の分割,

$$\exists\, i\in\{1,\cdots,n\}\ \text{ s.t. }\ \mathcal{O}(f|_{[t_{i-1},t_i]})\geq\varepsilon_0.$$

背理法の仮定により、$[a,b]$ 自身は (♯) を満たすので、$[a,\frac{a+b}{2}]$, $[\frac{a+b}{2},b]$ の少なくとも一方は、(♯) を満たす。(♯) を満たす方の閉区間を $[a_1,b_1]$ とおく。すると、$[a_1,\frac{a_1+b_1}{2}]$, $[\frac{a_1+b_1}{2},b_1]$ の少なくとも一方は、(♯) を満たす。(♯) を満たす方の閉区間を $[a_2,b_2]$ とおく。以下同様に繰り返すと、(♯) を満たす閉区間の減少列 $[a,b]\supset[a_1,b_1]\supset[a_2,b_2]\supset\cdots\cdots$ であって、$b_n-a_n=\frac{b-a}{2^n}$ $(n\in\mathbb{N})$ を満たすものが得られる。よって、区間縮小法の原理 (定理 8-10) より、すべての $[a_n,b_n]$ $(n=1,2,3,\cdots)$ に共通に含まれる実数 c が唯一存在し、その実数 c は $c=\lim\limits_{n\to\infty}a_n=\lim\limits_{n\to\infty}b_n$ によって与えられる。f は点 $c\in[a,b]$ で連続であるから、$\frac{\varepsilon_0}{3}>0$ に対して、

$$\exists\,\delta>0\ \text{ s.t. }\ x\in[a,b],\ |c-x|<\delta\ \Rightarrow\ |f(c)-f(x)|<\tfrac{\varepsilon_0}{3}$$

が成り立つ。$c=\lim\limits_{n\to\infty}a_n=\lim\limits_{n\to\infty}b_n$ なので、$[a_N,b_N]\subset[c-\delta,c+\delta]$ となる $N\in\mathbb{N}$ が存在する。この N について、$f([a_N,b_N])\subset f([c-\delta,c+\delta])\subset[f(c)-\frac{\varepsilon_0}{3},f(c)+\frac{\varepsilon_0}{3}]$ が成り立つので、$\mathcal{O}(f|_{[a_N,b_N]})\leq\frac{2\varepsilon_0}{3}<\varepsilon_0$ となる。ところが、$[a_N,b_N]$ は (♯) を満たしているので、$\mathcal{O}(f|_{[a_N,b_N]})\geq\varepsilon_0$ でなければならない。ここに矛盾が生じ、補題は証明された。　□

(**proof of Theorem 22-10**)

実数 $\varepsilon>0$ を任意にとる。補題 22-12 により、$[a,b]$ の分割 $\Delta : a_0=t_0<t_1<\cdots<t_n=b$ であって、

「すべての $i=1,\cdots,n$ に対して $\mathcal{O}(f|_{[t_{i-1},t_i]})<\frac{\varepsilon}{2}$」

を満たすものが存在する。

$\delta:=\min\{t_1-t_0,\ \cdots,t_{n-1}-t_n\}$ とおく。$|x-x'|<\delta$ を満たす任意の $x,x'\in[a,b]$ に対して、$x,x'\in[t_{i-1},t_i]\cup[t_i,t_{i+1}]$ となる $i\in\{1,\cdots,n-1\}$ が存在する ($\because\ \delta$ の定め方から x と x' の間には Δ の分点は高々 1 つしか存在し得ない)。このとき、

$$|f(x)-f(x')|\leq|f(x)-f(t_i)|+|f(t_i)-f(x')|<\tfrac{\varepsilon}{2}+\tfrac{\varepsilon}{2}=\varepsilon$$

となる。よって、f は一様連続である。　□

§23. 微分

ここでは、関数の微分を‘$\varepsilon-\delta$’式に定義して、合成関数の微分法、平均値の定理、逆関数定理などの微分に関する基本的な定理を証明します。指数関数が微分可能であることを証明することが最終目標です。

§23-1 微分に関する基本的な定理

関数 f の点 a での微分 (係数) とは、大雑把に言えば、x を a に「限りなく近づけたとき」の比 $\frac{f(x)-f(a)}{x-a}$ の極限のことをいいます。関数の極限は、定義域に「沢山穴が空いていると」x を a に近づける仕方によって値が変わってしまうことがあります。このようなことが起こらないようにするために、定義域が開集合であるような関数に対してのみ微分を考えます。

●$\mathbb{R}$ の開集合

$\mathbb{R}$ の部分集合 U が**開集合** (open set) であるとは、

$$\forall\, a \in U,\ \exists\, \delta > 0 \ \text{ s.t. } \ (a-\delta, a+\delta) \subset U$$

が成り立つときをいいます。$\mathbb{R}$ の開集合であって、かつ、区間であるものを**開区間** (open interval) と呼びます。例えば、$\mathbb{R}$ 自身や $a<b$ を満たす実数 a, b に対する $(a,b) = \{\, x \in \mathbb{R} \mid a < x < b \,\}$, $(-\infty, a)$, (a, ∞) などはすべて開区間です。$\mathbb{R}$ の開集合ではあるけれども開区間でないものの例としては、$\mathbb{R} - \{0\}$, $(-4,-1) \cup (1,3)$ や空集合 $\varnothing$ などが挙げられます。

●微分の定義

1 変数実数値関数の微分を定義しましょう。

定義 23-1

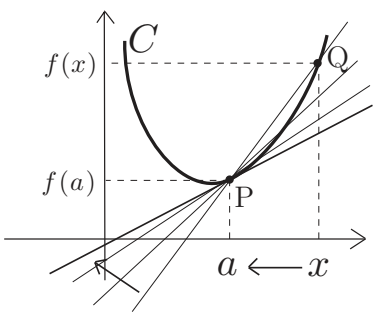
$\mathbb{R}$ の開集合 U を定義域とする関数 $f : U \longrightarrow \mathbb{R}$ が点 $a \in U$ で**微分可能** (differentiable) であるとは、次を満たす $\alpha \in \mathbb{R}$ が存在するときをいう：

$$\forall\, \varepsilon > 0,\ \exists\, \delta > 0 \ \text{ s.t. } \ x \in U,\ 0 < |x-a| < \delta \ \Rightarrow\ \left| \frac{f(x)-f(a)}{x-a} - \alpha \right| < \varepsilon.$$

α を f の a における**微分係数** (differential coefficient) といい、$f'(a)$ や $\dfrac{df}{dx}(a)$ などによって表わす。すべての $a \in U$ で f が微分可能なとき、f は**微分可能**であるといい、各 $a \in U$ に対して微分係数 $f'(a)$ を対応させる関数 $f' : U \longrightarrow \mathbb{R}$ を f の**導関数** (derivative) という。

注意：1. 連続関数の定義域は“何でもよかった”のですが、微分可能な関数の定義域は、冒頭で述べたように、開集合でなければならないことに注意しましょう。定義域を開集合に限定したことにより、f の a における微分係数 α は (存在すれば) 一意的であることが保証されます。

2. 関数 f の定義域 U から点 a をとって固定し、さらに、a に十分近い点 $x \in U$ を任意にとります。このとき、平面上の点 $\mathrm{P}(a, f(a))$ と点 $\mathrm{Q}(x, f(x))$ を結ぶ直線の傾きは $\frac{f(x)-f(a)}{x-a}$ により与えられます。“よい状況”の下では、x を a に「限りなく近づけて」いくと、Q は P に「限りなく近づいて」いき、P と Q を結ぶ直線はまた点 P で曲線 $C(x) = (x, f(x))$ に接する直線、すなわち、P における C の接線に「限りなく近づいて」いき



ます。このような考察から、f の a における微分係数は、幾何学的には、この接線の傾きを表わしていると考えられます。

3. 記号 $\frac{df}{dx}(a)$ に使われている文字 x は f の定義域 U 内を動く“変数”を表わしています。したがって、記号 $\frac{df}{dx}(a)$ を使う前に、本来は「U 内を動く変数を x という記号で表わす」という断わり書きが必要です。この約束事を書く煩わしさを避けるため、微積分学の多くの教科書では、(定義域内を動く変数を x で表わすという約束を込めて) 関数 $f(x)$ という書き方をしています。U 内を動く変数とは、厳密には U 上の恒等写像 id_U のことです。

演習 23-1 * 関数 $f:\mathbb{R}\longrightarrow\mathbb{R},\ f(x)=\begin{cases} x\sin\frac{1}{x} & (x\neq 0)\\ 0 & (x=0)\end{cases}$ は微分可能でないことを示せ。

●関数の微分と連続性

次の言い換えは (抽象的な議論において) 関数が微分可能であること証明する際に便利です。

補題 23-2

f を開集合 $U\subset\mathbb{R}$ 上で定義された実数値関数とし、$a\in U$ とする。次の 2 つは同値である。

① f は点 a で微分可能である。

② 次の 2 条件を満たす関数 $\rho_f:U\longrightarrow\mathbb{R}$ が存在する：

(i) 任意の $x\in U$ に対して $f(x)=\rho_f(x)(x-a)+f(a)$ である。

(ii) ρ_f は点 a で連続である。

このとき、f の a における微分係数は $\rho_f(a)$ によって与えられる。

(**proof**)

「① $\Longrightarrow$ ②」の証明：

関数 $\rho_f:U\longrightarrow\mathbb{R}$ を

$$\rho_f(x)=\begin{cases}\dfrac{f(x)-f(a)}{x-a} & (x\neq a\ \text{のとき})\\ f'(a) & (x=a\ \text{のとき})\end{cases}$$

によって定める。この ρ_f は②を満たす。

「② $\Longrightarrow$ ①」の証明：

関数 $\rho_f:U\longrightarrow\mathbb{R}$ は②の条件を満たしているとする。任意に $\varepsilon>0$ をとる。ρ_f は点 a で連続であるから、次の条件を満たす $\delta>0$ が存在する：

$$x\in U,\ |x-a|<\delta\ \Rightarrow\ |\rho_f(x)-\rho_f(a)|<\varepsilon.$$

(i) により、$x\neq a$ のとき $\rho_f(x)=\frac{f(x)-f(a)}{x-a}$ と書けるから、

$$x\in U,\ 0<|x-a|<\delta\ \Rightarrow\ \left|\frac{f(x)-f(a)}{x-a}-\rho_f(a)\right|<\varepsilon$$

が成り立つ。したがって、f は a で微分可能であって $\rho_f(a)=f'(a)$ である。 □

演習 23-2 上の証明の下線部分を確かめよ。

注意：上の補題②によって、(点 $a\in U$ で) 微分可能な関数は (点 $a\in U$ で) 連続である ことがわかります。しかしながら、この 逆は成立しません(演習 14-4、演習 23-1 を参照)。

●関数の和、差、積、商の微分

微分可能な関数の和、差、積、商はまた微分可能で、その導関数は最初に与えられた関数の導関数を使って書くことができます。詳しくは次の補題のようになります。

補題 23-3

f, g を同じ開集合 $U \subset \mathbb{R}$ 上で定義された実数値関数とし、点 $a \in U$ で微分可能であるとする。このとき、$f+g,\ f-g,\ fg,\ \frac{f}{g}$ はすべて点 a で微分可能であり、それらの微分係数は次で与えられる（但し、商を考えるときには、すべての $x \in U$ について $g(x) \neq 0$ であることを仮定する）：

$$(f+g)'(a) = f'(a) + g'(a), \qquad (f-g)'(a) = f'(a) - g'(a)$$

$$(fg)'(a) = f'(a)g(a) + f(a)g'(a), \qquad \Big(\frac{f}{g}\Big)'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{g(a)^2}$$

(**proof**)

どれも補題 23-2 を使って簡単に証明することができる。ここでは商について証明しよう。まず、f, g は点 a で微分可能であるから、補題 23-2 により、次の条件を満たす点 a で連続な関数 $\rho_f : U \longrightarrow \mathbb{R}$, $\rho_g : U \longrightarrow \mathbb{R}$ が存在する：任意の $x \in U$ に対して

$$f(x) = \rho_f(x)(x-a) + f(a), \quad g(x) = \rho_g(x)(x-a) + g(a).$$

このとき、任意の $x \in U$ に対して

$$\Big(\frac{f}{g}\Big)(x) = \frac{\rho_f(x)(x-a) + f(a)}{\rho_g(x)(x-a) + g(a)} = \frac{g(a)\rho_f(x) - f(a)\rho_g(x)}{g(a)(\rho_g(x)(x-a) + g(a))}(x-a) + \frac{f(a)}{g(a)}$$

と書ける。関数

$$\rho : U \longrightarrow \mathbb{R}, \quad \rho(x) = \frac{g(a)\rho_f(x) - f(a)\rho_g(x)}{g(a)(\rho_g(x)(x-a) + g(a))} \quad (x \in U)$$

は点 a で連続であるから、$\frac{f}{g}$ は点 a で微分可能であって、その微分係数は次式で与えられる：

$$\Big(\frac{f}{g}\Big)'(a) = \rho(a) = \frac{f'(a)g(a) - f(a)g'(a)}{g(a)^2}. \qquad \square$$

演習 23-3 * 上の補題の積について証明せよ。

例 23-4 $n \in \mathbb{N}$ に対して、関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^n$ $(x \in \mathbb{R})$ は微分可能であって、その導関数は $f'(x) = nx^{n-1}$ $(x \in \mathbb{R})$ によって与えられる（積の微分公式を使って帰納法で示すことができる）。

●合成関数の微分法

微分可能な関数の合成関数はまた微分可能になります。

補題 23-5

U, V を $\mathbb{R}$ の開集合とする。関数 $f : U \longrightarrow \mathbb{R}$ と関数 $g : V \longrightarrow \mathbb{R}$ は $f(U) \subset V$ を満たしているとする。f が点 $a \in U$ で微分可能で、g が点 $f(a) \in V$ で微分可能であるとき、合成関数 $g \circ f$ は点 a で微分可能であって、次が成り立つ：

$$(g \circ f)'(a) = g'(f(a))f'(a).$$

(**proof**)

点 a で連続な関数 $\rho_f : U \longrightarrow \mathbb{R}$ と点 $f(a)$ で連続な関数 $\rho_g : V \longrightarrow \mathbb{R}$ が存在して、

$$\forall\, x \in U,\ f(x) = \rho_f(x)(x-a) + f(a),$$
$$\forall\, y \in V,\ g(y) = \rho_g(y)(y-f(a)) + g(f(a))$$

が成り立つ (補題 23-2)。したがって、任意に $x \in U$ をとると、

$$g(f(x)) = \rho_g(f(x))(f(x)-f(a)) + g(f(a)) = \rho_g(f(x))\rho_f(x)(x-a) + (g\circ f)(a)$$

が成り立つ。ここで、

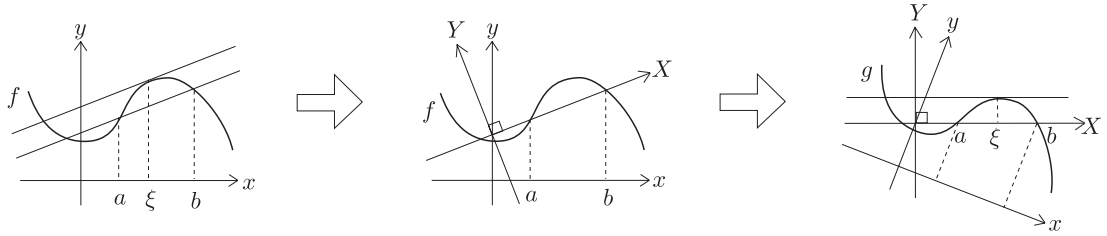
$$\rho(x) = \rho_g(f(x))\rho_f(x) \qquad (x \in U)$$

によって定義される関数 $\rho : U \longrightarrow \mathbb{R}$ は点 a で連続であるから、$g \circ f$ は a で微分可能であって、その微分係数は次式で与えられる：

$$(g\circ f)'(a) = \rho(a) = \rho_g(f(a))\rho_f(a) = g'(f(a))f'(a). \qquad \square$$

●平均値の定理 (mean value theorem)

平均値の定理は、微分可能な関数 f の定義域内の 2 点 a, b $(a < b)$ に対して平面上の 2 点 $(a, f(a))$ と $(b, f(b))$ を結ぶ直線を考えると、f のグラフが表わす曲線 C に、その直線と同じ傾きを持つ接線を引くことができる、ということを主張する定理です。座標軸を適当に取り替えると、$f(a) = f(b) = 0$ とすることができますが、この場合の平均値の定理は、曲線 C に x 軸と水平な接線を引くことができるという主張になります。f の極大点や極小点を与える点では曲線 C の接線は x 軸と水平なので、定理の主張の正しさを実感することができます。



定理 23-6 (平均値の定理)

f を $[a, b]$ 上で定義された連続な実数値関数とする。f が (a, b) 上で微分可能ならば、

$$\frac{f(b)-f(a)}{b-a} = f'(\xi)$$

を満たす $\xi \in (a, b)$ が存在する。

(**proof**)

$g : [a, b] \longrightarrow \mathbb{R}$ を

$$g(x) = \frac{f(b)-f(a)}{b-a}(x-a) + f(a) - f(x) \quad (x \in [a, b])$$

によって定める。$g'(\xi) = 0$ となる $\xi \in (a, b)$ の存在を示せば定理の証明は終わる。

g は連続であるから、$M := \max g([a, b]),\ m := \min g([a, b])$ が存在する (定理 22-7)。

(i) $M = m$ の場合：

g は $[a, b]$ 上で定数関数になる。よって、任意の $x \in (a, b)$ に対して $g'(x) = 0$ となる。特に、$\xi = \frac{a+b}{2}$ に対して $g'(\xi) = 0$ が成り立つ。

(ii) $M > m$ かつ $M > g(a)$ の場合：

$M = g(\xi)$ $(\xi \in [a,b])$ とおく。$M > g(a) = 0 = g(b)$ であるから、$\xi \in (a,b)$ である。補題 23-2 により、ξ で連続な関数 $\rho_g : (a,b) \longrightarrow \mathbb{R}$ であって、すべての $x \in (a,b)$ に対して $g(x) = \rho_g(x)(x-a) + g(\xi)$ を満たすものが存在する。$M = g(\xi)$ は g の最大値なので、

$$\xi < x < b \ \Rightarrow\ \frac{g(x)-g(\xi)}{x-\xi} \leq 0, \qquad a < x < \xi \ \Rightarrow\ \frac{g(x)-g(\xi)}{x-\xi} \geq 0$$

が成り立つ。よって、開区間 (ξ, b) の元 $x_n = \frac{b-\xi}{n} + \xi$ $(n \in \mathbb{N})$ からなる数列 $\{x_n\}_{n=1}^{\infty}$ に対して

$$g'(\xi) = \rho_g(\xi) = \rho_g(\lim_{n\to\infty} x_n) = \lim_{n\to\infty} \rho_g(x_n) \leq 0$$

となり（左から 3 番目の等号は ρ_g の ξ における連続性による）、開区間 (a, ξ) の元 $y_n = -\frac{\xi-a}{n} + \xi$ $(n \in \mathbb{N})$ からなる数列 $\{y_n\}_{n=1}^{\infty}$ に対して

$$g'(\xi) = \rho_g(\xi) = \rho_g(\lim_{n\to\infty} y_n) = \lim_{n\to\infty} \rho_g(y_n) \geq 0$$

となる。故に、$g'(\xi) = 0$ が示された。

(iii) $M > m$ かつ $M = g(a)$ の場合：

$g(a) > m$ より、(ii) と同様にして $g'(\xi) = 0$ となる $\xi \in (a,b)$ の存在を示すことができる。 □

平均値の定理から直ちに次の系が導かれます。

系 23-7

f を開区間 I 上で定義された微分可能な実数値関数とする。すべての $a \in I$ について $f'(a) > 0$ (resp. $f'(a) < 0$) ならば、f は狭義単調増加関数 (resp. 狭義単調減少関数) である。

●逆関数定理

微分可能な関数 f がその定義域内の点 a において 0 でない微分係数を持てば、a を含むある小さい開区間において f は逆関数を持ち、その逆関数は $f(a)$ で微分可能になります。これは**逆関数定理**と呼ばれる、応用範囲の広い重要な定理です。ここでは、この定理の「簡易版」を述べ、それを証明します。

定理 23-8 (逆関数定理)

f を開区間 I 上で定義された微分可能な関数であるとし、すべての点 $a \in I$ において $f'(a) > 0$ であると仮定する。このとき、$f(I)$ は開区間であり、f の逆関数 $f^{-1} : f(I) \longrightarrow \mathbb{R}$ は微分可能である。さらに、点 $b = f(a)$ における微分係数は次式で与えられる：

$$(f^{-1})'(b) = \frac{1}{f'(a)}.$$

(**proof**)

すべての点 $a \in I$ において $f'(a) > 0$ であるので、f は狭義単調増加関数になる (系 23-7)。よって、逆関数 f^{-1} が存在する。また、中間値の定理を使うと、$f(I)$ が開区間 (= 開集合、かつ、区間) であることがわかり、さらに、定理 15-4 により、f^{-1} は連続であることがわかる。

f^{-1} が任意の点 $b \in f(I)$ において微分可能であることを示す。$a = f^{-1}(b) \in I$ とおく。f は点 $a \in I$ で微分可能なので、補題 23-2 により、a で連続な関数 $\rho_f : I \longrightarrow \mathbb{R}$ であって、すべての $x \in I$ に対して

$$(*) \qquad f(x) = \rho_f(x)(x-a) + f(a)$$

を満たすものが存在する。ここで、$\rho_f(a) = f'(a) > 0$ であり、$x \neq a$ であるような $x \in I$ に対しても $\rho_f(x) = \frac{f(x)-f(a)}{x-a} > 0$ であるから、すべての $x \in I$ に対して、$\rho_f(x) > 0$ となる。$(*)$ により、任意の $y \in f(I)$ に対して、

$$y = f(f^{-1}(y)) = \rho_f(f^{-1}(y))(f^{-1}(y) - a) + f(a) = \rho_f(f^{-1}(y))(f^{-1}(y) - f^{-1}(b)) + b$$

であるが、$\rho_f(f^{-1}(y)) > 0$ であるから、上式は

$$f^{-1}(y) - f^{-1}(b) = \frac{1}{\rho_f(f^{-1}(y))}(y - b)$$

と書き換えることができる。f^{-1} は連続であり、ρ_f は点 a において連続であるから、$\rho(y) = \frac{1}{\rho_f(f^{-1}(y))}$ $(y \in f(I))$ によって定義される関数 $\rho : f(I) \longrightarrow \mathbb{R}$ は $b = f^{-1}(a)$ において連続である。したがって、f^{-1} は点 b で微分可能であり、その微分係数は次で与えられる。

$$(f^{-1})'(b) = \frac{1}{\rho_f(f^{-1}(b))} = \frac{1}{\rho_f(a)} = \frac{1}{f'(a)}.$$ □

注意：f^{-1} の微分可能性が最初にわかっているときには、合成関数の微分法を使って、$(f \circ f^{-1})(x) = x$ の両辺を微分することによって、定理の公式を導くことができます。

§23-2 指数関数の微分可能性

第 15 節では、$\mathbb{Q}$ 上で指数関数を定義し、それを拡張する形で $\mathbb{R}$ 上の指数関数を定義しました。ここでは、無限級数を使った、指数関数のもう 1 つの定義を紹介します。

●絶対収束級数

無限級数 $\sum_{n=1}^{\infty} a_n$ が**絶対収束**する (absolutely converge) とは、級数 $\sum_{n=1}^{\infty} |a_n|$ が収束するときをいいます。

補題 23-9
無限級数 $\sum_{n=1}^{\infty} a_n$ が絶対収束するならば、その級数自体も収束する。

(**proof**)
各 $k \in \mathbb{N}$ に対して、

$$a_k^+ = \frac{|a_k| + a_k}{2}, \quad a_k^- = \frac{|a_k| - a_k}{2}$$

とおくと、$0 \leq a_k^+ \leq |a_k|, 0 \leq a_k^- \leq |a_k|$ が成り立つ。これらの不等式と数列 $\left\{\sum_{k=1}^{n} |a_k|\right\}_{n=1}^{\infty}$ が上に有界であること ($\because$ 仮定による) から、数列 $\left\{\sum_{k=1}^{n} a_k^+\right\}_{n=1}^{\infty}, \left\{\sum_{k=1}^{n} a_k^-\right\}_{n=1}^{\infty}$ は上に有界な単調増加数列である。したがって、無限級数 $\sum_{n=1}^{\infty} a_n^+, \sum_{n=1}^{\infty} a_n^-$ は収束し、差 $\sum_{n=1}^{\infty} a_n^+ - \sum_{n=1}^{\infty} a_n^- = \sum_{n=1}^{\infty} a_n$ も収束する。 □

例 23-10 任意の $x \in \mathbb{R}$ に対して、無限級数 $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ は絶対収束する。したがって、無限級数 $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ 自身も収束する。その和を e^x で表わす。
(**proof**)

$b_n = \sum_{k=0}^{n} \frac{|x|^k}{k!}$ $(n \in \mathbb{N})$ とおく。$N > |x|$ となる自然数 N を 1 つ固定する。このとき、$n > N$ を満たす任意の $n \in \mathbb{N}$ に対して

$$b_n = b_N + \sum_{k=N+1}^{n} \frac{|x|^k}{k!} \leq b_N + \sum_{k=N+1}^{n} \frac{|x|^k}{N!N^{k-N}} = b_N + \frac{N^N}{N!} \sum_{k=N+1}^{n} \Big(\frac{|x|}{N}\Big)^k$$

$$= b_N + \frac{N^N}{N!}\Big(\frac{|x|}{N}\Big)^{N+1} \frac{1 - \Big(\frac{|x|}{N}\Big)^{n-N}}{1 - \frac{|x|}{N}} \leq b_N + \frac{N^N}{N!} \frac{1}{1 - \frac{|x|}{N}}$$

となるので、数列 $\{b_n\}_{n=1}^{\infty}$ は上に有界である。また、数列 $\{b_n\}_{n=1}^{\infty}$ は単調増加列である。よって、$\{b_n\}_{n=1}^{\infty}$ は収束する。 □

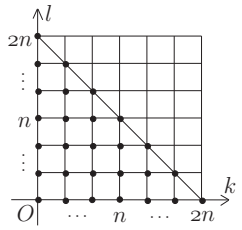
補題 23-11

任意の $x, y \in \mathbb{R}$ について $e^{x+y} = e^x e^y$ が成り立つ。

(**proof**)

e^x, e^y, e^{x+y} を定める無限級数の第 n 部分和をそれぞれ s_n, t_n, u_n とおく。

$$u_{2n} = \sum_{m=0}^{2n} \frac{(x+y)^m}{m!} = \sum_{m=0}^{2n} \sum_{k=0}^{m} \frac{x^k y^{m-k}}{k!(m-k)!} = \sum_{(k,l)\in J} \frac{x^k y^l}{k!l!}$$



となる。但し、$J = \{\ (k,l) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq k, l \leq 2n,\ k + l \leq 2n\ \}$ である。したがって、

$$|s_{2n}t_{2n} - u_{2n}| = \Big| \sum_{0 \leq k,l \leq 2n} \frac{x^k y^l}{k!l!} - \sum_{(k,l)\in J} \frac{x^k y^l}{k!l!} \Big|$$

$$\leq \sum_{k=0}^{2n} \frac{|x|^k}{k!} \sum_{l=n+1}^{2n} \frac{|y|^l}{l!} + \sum_{k=n+1}^{2n} \frac{|x|^k}{k!} \sum_{l=0}^{2n} \frac{|y|^l}{l!} \leq e^{|x|} \sum_{l=n+1}^{2n} \frac{|y|^l}{l!} + \sum_{k=n+1}^{2n} \frac{|x|^k}{k!} e^{|y|}$$

を得る。ここで、$z \in \mathbb{R}$ に対して、

$$\sum_{l=n+1}^{2n} \frac{|z|^l}{l!} \leq e^{|z|} - \sum_{l=0}^{n} \frac{|z|^l}{l!} \ \to 0 \ \ (n \to \infty)$$

であるから、

$$\lim_{n\to\infty} (s_{2n}t_{2n} - u_{2n}) = 0$$

を得る。一般に、数列 $\{a_n\}_{n=1}^{\infty}$ が $\alpha \in \mathbb{R}$ に収束するとき、その偶数番目を取り出して作られる数列 $\{a_{2n}\}_{n=1}^{\infty}$ も同じ値 α に収束するから、

$$\lim_{n\to\infty} s_{2n} = e^x, \qquad \lim_{n\to\infty} t_{2n} = e^y, \qquad \lim_{n\to\infty} u_{2n} = e^{x+y}$$

が成り立つ。したがって、次の等式を得る：

$$0 = \lim_{n\to\infty} (s_{2n}t_{2n} - u_{2n}) = \lim_{n\to\infty} s_{2n} \lim_{n\to\infty} t_{2n} - \lim_{n\to\infty} u_{2n} = e^x e^y - e^{x+y}. \qquad \square$$

注意：$x \geq 0$ のとき $e^x > 0$ であることは定義からすぐにわかりますが、$x < 0$ のときも $e^x > 0$ であることが、上の指数法則からわかります。

●指数関数の微分可能性

関数 $\exp : \mathbb{R} \longrightarrow \mathbb{R}$ を

$$\exp(x) = e^x \quad (x \in \mathbb{R})$$

によって定義します。

定理 23-12
関数 exp は微分可能で、$\exp' = \exp$ である。

(**proof**)

f は任意の点 $a \in \mathbb{R}$ で微分可能であることを示す。

$\varepsilon > 0$ を任意にとる。$0 < |x| < 1$ に対して、$\frac{e^x-1}{x} - 1 \leq |x|e$ である (下の演習 23-4) から、次の条件を満たす $\delta > 0$ が存在する：

$$0 < |x| < \delta \ \Rightarrow\ \left|\frac{e^x - 1}{x} - 1\right| < \frac{\varepsilon}{e^a}.$$

したがって、補題 23-11 により、$0 < |h| < \delta$ を満たすすべての $h \in \mathbb{R}$ に対して、

$$\left|\frac{e^{a+h} - e^a}{h} - e^a\right| = \left|e^a \frac{e^h - 1}{h} - e^a\right| = e^a \left|\frac{e^h - 1}{h} - 1\right| < \varepsilon$$

となる。よって、exp は点 a において微分可能であって、$\exp'(a) = \exp(a)$ となる。 □

演習 23-4 $0 < |x| < 1$ に対して、不等式 $\frac{e^x-1}{x} - 1 \leq |x|e$ が成り立つことを示せ。
ヒント：次の①と②を示せばよい。

① $x \neq 0$ のとき、$\frac{e^x - 1}{x} - 1 = \sum_{n=2}^{\infty} \frac{x^{n-1}}{n!}$　　② $|x| < 1$ のとき、$\sum_{k=2}^{n} \frac{|x|^{k-1}}{k!} \leq |x|e$

注意：補題 23-11 と定理 23-12 により、exp は第 15 節で定義した指数関数 $\exp_e$ に一致することがわかります (定理 15-8 と第 9-3 節も参照)。

●対数関数

定理 23-12 により、任意の $x \in \mathbb{R}$ に対して、$\exp'(x) = \exp(x) > 0$ となるので、exp は狭義単調増加関数です (系 23-7)。したがって、exp は微分可能な逆関数を持ちます (定理 23-8)。その逆関数を log と書き、**対数関数** (logarithmic function) といいます。log の定義域は $\exp(\mathbb{R}) = (0, \infty)$ です (例 9-2、演習 9-2)。また、逆関数定理 (定理 23-8) により、その導関数は次で与えられます：$\log'(x) = \dfrac{1}{x}$ $(x > 0)$.

●冪関数

$\alpha \in \mathbb{R}$ と $a \in (0, \infty)$ に対して、

$$a^\alpha := \exp(\alpha \log a)$$

と定めます。

$a \in \mathbb{R}$ を固定すると、各 $\alpha \in \mathbb{R}$ に a^α を対応させる関数 f_a が得られます。exp, log の性質から、f_a は連続であり、$f_a(\alpha + \beta) = f_a(\alpha) f_a(\beta)$ $(\alpha, \beta \in \mathbb{R})$ が成り立つので、f_a は第 15 節で定義した指数関数 $\exp_a$ に一致することがわかります (定理 15-8)。

一方、$\alpha \in \mathbb{R}$ を固定すると、$g(x) = x^\alpha$ $(x \in (0, \infty))$ によって関数 $g : (0, \infty) \longrightarrow \mathbb{R}$ が定義されます。この関数 g を**冪関数** (power function) といいます。exp, log は狭義単調増加関数なので、冪関数は、$\alpha > 0$ のとき狭義単調増加関数、$\alpha < 0$ のとき狭義単調減少関数になります。

演習 23-5 * 冪関数は微分可能であることを示せ。また、その導関数を求めよ。

§24. 微積分学の基本定理と広義積分

この節の前半では微積分学の基本定理を、後半では広義積分について述べます。ここでの目標は、積分と微分の相互関係を知ること、そして、広義積分の定義を理解することです。

§24-1 微積分学の基本定理

微積分学の基本定理とは、微分と積分が互いに逆操作であることを主張する定理です。この基本定理の証明には、積分に関する平均値の定理を使います。

●積分の平均値の定理

積分の平均値の定理は見かけ上前回紹介した平均値の定理と異なりますが、微積分学の基本定理を通じて、両者は本質的に同じ命題であることがわかります。

定理 24-1 (積分の平均値の定理)

f を $S \subset \mathbb{R}$ 上で定義された実数値連続関数とし、$[a,b] \subset S$ であるとする。このとき、

$$\frac{1}{b-a}\int_a^b f(x)dx = f(c)$$

を満たす $c \in [a,b]$ が存在する。

(**proof**)

f は連続なので、$[a,b]$ において最大値 M と最小値 m を持つ（定理 22-6）。

$m \leq f(x) \leq M$ が区間 $[a,b]$ 内のすべての x について成り立つから、

$$(b-a)m \leq \int_a^b f(x)dx \leq (b-a)M$$

を得る（補題 22-2、演習 22-1）。よって、$m < M$ ならば、

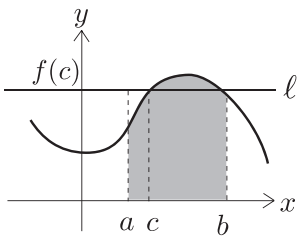
$$\frac{1}{b-a}\int_a^b f(x)dx \in [m,M] = f([a,b])$$

となり (中間値の定理)、$m = M$ ならば、

$$\frac{1}{b-a}\int_a^b f(x)dx = M = f(a)$$

となる。 □

注意：連続関数 f のグラフが右図のようになっているとき、定積分 $\int_a^b f(x)dx$ は斜線部分の面積を表わしていると考えられます。積分の平均値の定理は、グラフの‘凹凸を平均化’するように x-軸に平行な直線 ℓ をうまくとれば、斜線部分の面積は直線 ℓ と x-軸、および直線 $y=a$, $y=b$ で囲まれる長方形の面積に等しくなる、ということを主張しています。



●微積分学の基本定理 (fundamental theorem of calculus)

微分と積分は定義の仕方が全く違うにも関わらず、驚くべきことに、実は違いに逆操作になっています。ここでは、この事実を証明します。

$$f \longmapsto F(x)=\int_a^x f(t)dt \longmapsto F'=f$$
(元に戻る)

$$f \longmapsto f' \longmapsto F(x)=\int_a^x f'(t)dt=f(x)-f(a)$$
(定数項のずれを除くと元に戻る)

定理 24-2 (微積分学の基本定理)
f を開区間 I 上で定義された実数値連続関数とし、$a\in I$ を固定する。このとき、関数
$$F: I\longrightarrow \mathbb{R},\quad F(x):=\int_a^x f(t)dt \quad (x\in I)$$
は微分可能であり、その導関数 F' は f に一致する：$F'(x)=f(x)\ \ (x\in I)$.

(**proof**)
$b\in I$ を任意にとり、F が点 b で微分可能であることを示す。$x\in I,\ x\neq b$ に対して、
$$\begin{aligned}\frac{F(x)-F(b)}{x-b}&=\frac{1}{x-b}\Big(\int_a^x f(x)dx-\int_a^b f(x)dx\Big)\\&=\frac{1}{x-b}\Big(\int_a^x f(x)dx+\int_b^a f(x)dx\Big)=\frac{1}{x-b}\int_b^x f(x)dx\end{aligned}$$
なので (p.177)、積分の平均値の定理 (定理 24-1) により、次がわかる：
$$\exists\, c_x\in[\min\{x,b\},\max\{x,b\}]\ \text{ s.t. }\ \frac{F(x)-F(b)}{x-b}=\frac{1}{x-b}\int_b^x f(x)dx=f(c_x).$$
さて、任意に $\varepsilon>0$ をとる。f の連続性によって、次の条件を満たす $\delta>0$ が存在する：
$$x\in I,\ |x-b|<\delta\ \Rightarrow\ |f(x)-f(b)|<\varepsilon.$$
$0<|x-b|<\delta$ を満たす $x\in I$ を任意にとる。このとき、$|c_x-b|<\delta$ であるから
$$\Big|\frac{F(x)-F(b)}{x-b}-f(b)\Big|=|f(c_x)-f(b)|<\varepsilon$$
が成り立つ。よって、F は b で微分可能であって、$F'(b)=f(b)$ となる。 □

演習 24-1 I を開区間、$a\in I$ とし、集合 A,B を次のように定義する：
$A=\{\ f\mid f$ は I 上で定義された実数値連続関数 $\}$,
$B=\{\ F\mid F$ は I 上で定義された実数値微分可能な関数で、F' は連続、かつ、$F(a)=0\ \}$.
さらに、 2つの写像 $\Phi: A\longrightarrow B,\ \Psi: B\longrightarrow A$ を次のように定義する：
$$\Phi(f)=F\ \ (f\in A),\ \text{ 但し、}F(x)=\int_a^x f(t)dt\ \ (x\in I),$$
$$\Psi(F)=F'\ \ (F\in B).$$
このとき、Φ と Ψ は互いに他の逆写像であること ($\Psi\circ\Phi=\mathrm{id}_A,\ \Phi\circ\Psi=\mathrm{id}_B$) を示せ。

●原始関数

開区間 I 上で定義された実数値関数 f の**原始関数** (primitive function) とは、微分可能な関数 $F: I\longrightarrow\mathbb{R}$ であって、$F'=f$ を満たすもののことをいいます。F_1,F_2 が f の2つの原始関数ならば、平均値の定理（定理 23-6）により、F_1-F_2 は定数関数になります。定理 24-2 の系として次が得られます。

系 24-3

f を開区間 I 上で定義された実数値連続関数とし、F をその原始関数とする。このとき、任意の $a, b \in I$ に対して

$$\int_a^b f(t)dt = F(b) - F(a).$$

注意：1. 定理 24-2 により、f が連続ならばその原始関数が存在します。
2. 積分の計算では、$F(b) - F(a)$ をしばしば記号 $[F(x)]_a^b$ で表わします。

演習 24-2　上の系を証明せよ。

f の原始関数、つまり、微分すると f になる関数が求められると、系 24-3 の等式を使って、定積分を計算することができます。

例 24-4　$\alpha \in \mathbb{R}$, $a, b > 0$ に対して、次が成り立つ（演習 23-5、系 24-3）。

$$\int_a^b x^\alpha dx = \begin{cases} \frac{1}{\alpha+1}(b^{\alpha+1} - a^{\alpha+1}) & (\alpha \neq -1 \text{ のとき}) \\ \log\left(\frac{b}{a}\right) & (\alpha = -1 \text{ のとき}) \end{cases}$$

演習 24-3 * $a > 0$, $x \in \mathbb{R}$ とする。等式

$$\int_0^x \frac{1}{\sqrt{t^2 + a}} dt = \log(x + \sqrt{x^2 + a}) - \frac{1}{2}\log a$$

が成り立つことを示せ。

系 24-3 の公式を、関数の積と合成関数に対して適用する (補題 23-3、補題 23-5) ことにより、高校で習った部分積分公式と置換積分公式を導くことができます。

系 24-5

(1) (**部分積分法**) f, g を開区間 I 上で定義された実数値関数とし、f は連続、g は微分可能で、その導関数 g' は連続であるとする。F を f の原始関数とするとき、任意の $a, b \in I$ に対して、次の公式が成り立つ：

$$\int_a^b (fg)(x)dx = [F(x)g(x)]_a^b - \int_a^b (Fg')(x)dx.$$

(2) (**置換積分法**) f, φ をそれぞれ開区間 I, J 上で定義された実数値関数とし、f は連続、φ は微分可能で、その導関数 φ' は連続であり、$\varphi(J) \subset I$ であるとする。このとき、任意の $a, b \in J$ に対して、次の公式が成り立つ：

$$\int_{\varphi(a)}^{\varphi(b)} f(x)dx = \int_a^b f(\varphi(t))\varphi'(t)dt.$$

§24-2 広義積分

これまで扱ってきた定積分は、ある閉区間 $[a, b]$ 上で定義された有界な関数についてのものでした。ここでは、閉区間 $[a, b]$ の端点 a または b では値が定義されない関数（有界でない関数）の積分を考えます。このような有界でない関数や積分区間が有界でない関数の積分のことを広義積分といいます。重要な関数や興味深い実数の多くは広義積分の形で与えられます。

●右側極限と左側極限

例えば、半開閉区間 $(a,b]=\{\,x\in\mathbb{R}\mid a<x\le b\,\}$ 上で定義された関数 f の $(a,b]$ 上での積分を考えたいときには、a に十分近い点 $x\in(a,b]$ から b までの定積分 $F(x)=\int_x^b f(t)dt$ を考えて、x を a に近づけていったときに $F(x)$ の値がどう変化するのかを観察します。x は数直線上で見て a の右側から近づけていくことになるので、f の $(a,b]$ 上での積分（広義積分）を定義するためには、関数の右側極限の概念が必要になります。

定義 24-6

f を $S\subset\mathbb{R}$ 上で定義された実数値関数とする。

(1) f が点 $a\in\mathbb{R}$ において**右側極限を持つ**とは、$(a,a+\delta_0)\subset S$ となる実数 $\delta_0>0$ が存在し、かつ、次の条件を満たす $\alpha\in\mathbb{R}$ が存在するときをいう：

$$\forall\,\varepsilon>0,\ \exists\,\delta>0\ \text{ s.t. }\ x\in S,\ 0<x-a<\delta\ \Rightarrow\ |f(x)-\alpha|<\varepsilon.$$

α を f の a における**右側極限** (right-side limit) といい、$\lim_{x\to a+0}f(x)$ で表わす：$\alpha=\lim_{x\to a+0}f(x)$.

(2) f が点 $b\in\mathbb{R}$ において**左側極限を持つ**とは、$(b-\delta_0,b)\subset S$ となる実数 $\delta_0>0$ が存在し、かつ、次の条件を満たす $\beta\in\mathbb{R}$ が存在するときをいう：

$$\forall\,\varepsilon>0,\ \exists\,\delta>0\ \text{ s.t. }\ x\in S,\ 0<b-x<\delta\ \Rightarrow\ |f(x)-\beta|<\varepsilon.$$

β を f の b における**左側極限** (left-side limit) といい、$\lim_{x\to b-0}f(x)$ で表わす：$\beta=\lim_{x\to b-0}f(x)$.

注意：1. (1) の条件を満たす α と (2) の条件を満たす β は一意的です。

2. $a\in S$ であり、かつ、f が点 a で連続ならば、f は a において右側極限を持ち、$\lim_{x\to a+0}f(x)=f(a)$ となります。左側極限についても同様のことが成り立ちます。

3. $\lim_{x\to a+0}f(x)$, $\lim_{x\to b-0}f(x)$ における文字 x は別の文字に変えることができます。

4. $\lim_{x\to 0+0}f(x)$, $\lim_{x\to 0-0}f(x)$ をそれぞれ $\lim_{x\to+0}f(x)$, $\lim_{x\to-0}f(x)$ と書きます。

右側極限の存在を示すときには、次の定理が有効です。

定理 24-7

開区間 (a,b) 上で定義された実数値関数 f について、次の 3 つは互いに同値である。

(i) f は点 a において右側極限を持つ。

(ii) 次の条件を満たす $\alpha\in\mathbb{R}$ が存在する：

a に収束する (a,b) 内の任意の数列 $\{x_n\}_{n=1}^{\infty}$ に対して、$\lim_{n\to\infty}f(x_n)=\alpha$ である。

(iii) $\forall\,\varepsilon>0,\ \exists\,\delta>0\ \text{ s.t. }\ x,x'\in(a,b),\ x-a<\delta,\ x'-a<\delta\ \Rightarrow\ |f(x)-f(x')|<\varepsilon.$

(**proof**)

「(ii) ⇒ (i) ⇒ (iii) ⇒ (ii)」の順番で示すが、「(ii) ⇒ (i)」と「(i) ⇒ (iii)」の証明は演習問題として残し (演習 24-4)、「(iii) ⇒ (ii)」を証明する。証明を次の 3 段階に分ける。

① ある $c\in(a,b)$ が存在して、$f((a,c])$ は有界である。

② 各 $n\in\mathbb{N}$ に対して、

$$a_n:=a+\frac{c-a}{n}\in(a,c],\quad y_n:=\sup f((a,a_n])$$

とおく。数列 $\{y_n\}_{n=1}^{\infty}$ は下に有界な単調減少列である。したがって、$\alpha:=\lim_{n\to\infty}y_n$ が存在する。

③ a に収束する (a,b) 内の任意の数列 $\{x_n\}_{n=1}^{\infty}$ に対して、$\lim_{n\to\infty} f(x_n)=\alpha$ である。

①の証明：

仮定により、

$$「x,x'\in(a,b),\ x-a<\delta_0,\ x'-a<\delta_0\ \Rightarrow\ |f(x)-f(x')|<1」$$

を満たす $2(b-a)>\delta_0>0$ が存在する。このとき、

$$c:=a+\frac{\delta_0}{2}\in(a,b)$$

は $c-a<\delta_0$ を満たす。よって、任意の $x\in(a,c]$ に対して $x-a<c-a<\delta_0$ であり、$|f(x)-f(c)|<1$ が成り立つ。これは、$f((a,c])\subset(f(c)-1,f(c)+1)$ となることを意味するので、$f((a,c])$ は有界である。

②の証明：

$m>n$ ならば $a_n>a_m$ なので $f((a,a_n])\supset f((a,a_m])$ である。したがって、

$$y_n=\sup f((a,a_n])\geq\sup f((a,a_m])=y_m$$

となり、$\{y_n\}_{n=1}^{\infty}$ は単調減少数列である。また、任意の $n\in\mathbb{N}$ に対して、

$$y_n=\sup f((a,a_n])\geq\inf f((a,a_n])\geq\inf f((a,c])$$

となるから、$\{y_n\}_{n=1}^{\infty}$ は下に有界である。よって、$\lim_{n\to\infty} y_n$ が存在する。この値を α とおく。

③の証明：

$\lim_{n\to\infty} x_n=a$ を満たす (a,b) 内の数列 $\{x_n\}_{n=1}^{\infty}$ および $\varepsilon>0$ を任意にとる。各 $n\in\mathbb{N}$ に対して、$y_n=\sup f((a,a_n])$ であるから、

$$\exists\, x_n'\in(a,a_n]\ \text{ s.t. }\ y_n-\frac{1}{n}<f(x_n')\leq y_n$$

が成り立つ。はさみうちの原理により、数列 $\{f(x_n')\}_{n=1}^{\infty}$ は α に収束することがわかるので、

$$\exists\, N_1\in\mathbb{N}\ \text{ s.t. }\ n>N_1\ \Rightarrow\ |f(x_n')-\alpha|<\frac{\varepsilon}{2}$$

が成り立つ。一方、仮定により、次が成り立つ：

$$\exists\,\delta>0\ \text{ s.t. }\ x,x'\in(a,b),\ x-a<\delta,\ x'-a<\delta\ \Rightarrow\ |f(x)-f(x')|<\frac{\varepsilon}{2}.$$

各 $n\in\mathbb{N}$ に対して $x_n'\in(a,a_n]=(a,a+\frac{c-a}{n}]$ ゆえ、$\lim_{n\to\infty} x_n'=a$ である。よって、

$$\exists\, N_2\in\mathbb{N}\ \text{ s.t. }\ n>N_2\ \Rightarrow\ |x_n'-a|<\delta$$

が成り立つ。このとき、$\lim_{n\to\infty} x_n=a$ より、次が成り立つ：

$$\exists\, N_3\in\mathbb{N}\ \text{ s.t. }\ n>N_3\ \Rightarrow\ |x_n-a|<\delta.$$

そこで、$N=\max\{N_1,N_2,N_3\}$ とおくと、$n>N$ を満たすすべての $n\in\mathbb{N}$ に対して、

$$|f(x_n)-\alpha|\leq|f(x_n)-f(x_n')|+|f(x_n')-\alpha|<\frac{\varepsilon}{2}+\frac{\varepsilon}{2}=\varepsilon$$

となる。よって、$\lim_{n\to\infty} f(x_n)=\alpha$ となり、③も示された。 □

演習 24-4　上の定理の「(ii) ⇒ (i)」と「(i) ⇒ (iii)」が成り立つことを示せ。

ヒント：前者は対偶を証明するとよい (定理 14-8 の証明と同様)。

例 24-8 $\alpha > 0$ のとき、$\lim_{x \to +0} x^{\alpha} = 0$ となる。

(**proof**)

$\{x_n\}_{n=1}^{\infty}$ を 0 に収束するような $(0, \infty)$ 内の任意の数列とする。任意に $\varepsilon > 0$ をとると、「$n > N \ \Rightarrow \ x_n < \varepsilon^{\frac{1}{\alpha}}$」を満たす $N \in \mathbb{N}$ が存在する。

$\alpha > 0$ なので、冪関数 $x \longmapsto x^{\alpha}$ は $x > 0$ 上で単調増加関数である。したがって、

$$「n > N \text{ を満たすすべての } n \in \mathbb{N} \text{ について } x_n^{\alpha} < (\varepsilon^{\frac{1}{\alpha}})^{\alpha} = \varepsilon」$$

が成り立つ (p.190 を参照)。これは、$\{x_n^{\alpha}\}_{n=1}^{\infty}$ が 0 に収束することを意味する。したがって、$\lim_{x \to +0} x^{\alpha} = 0$ である (定理 24-7)。 □

●半開閉区間上での広義積分

連続関数 $f : [a, b) \longrightarrow \mathbb{R}$ に対して、左側極限 $\lim_{x \to b-0} \int_a^x f(t)dt$ が存在するとき、f は $[a, b)$ 上で**広義積分可能**であるといい、その極限を $\int_a^b f(t)dt$ によって書き表わします：

$$\int_a^b f(t)dt = \lim_{x \to b-0} \int_a^x f(t)dt.$$

同様に、連続関数 $f : (a, b] \longrightarrow \mathbb{R}$ に対して、右側極限 $\lim_{x \to a+0} \int_x^b f(t)dt$ が存在するとき、f は $(a, b]$ 上で広義積分可能であるといい、その極限を $\int_a^b f(t)dt$ によって書き表わします：

$$\int_a^b f(t)dt = \lim_{x \to a+0} \int_x^b f(t)dt.$$

注意：1. 左側極限や右側極限が存在するしないに関わらず、$\int_a^b f(t)dt$ という記号を使い、これを**広義積分** (improper integral) と呼ぶことがあります。この場合、左側極限 $\lim_{x \to b-0} \int_a^x f(t)dt$ が存在するとき、この広義積分は**収束する**といいます。同様に、右側極限 $\lim_{x \to a+0} \int_x^b f(t)dt$ が存在するとき、この広義積分は収束するといいます。

2. 連続関数 $f : [a, b] \longrightarrow \mathbb{R}$ に対しては $F(x) = \int_a^x f(t)dt \ \ (x \in [a, b])$ によって定義される関数 F は連続になる (定理 24-2) ので、左側極限 $\lim_{x \to b-0} \int_a^x f(t)dt$ と右側極限 $\lim_{x \to a+0} \int_x^b f(t)dt$ はともに存在して、その値は定積分 $\int_a^b f(t)dt$ に一致します。したがって、広義積分は定積分の拡張概念になっています。

補題 24-9

(1) $f : [a, b) \longrightarrow \mathbb{R}$ が $[a, b]$ で広義積分可能なとき、任意の実数 $c \in [a, b)$ に対して f は $[c, b)$ 上で広義積分可能で、次の等式が成り立つ：

$$\int_a^b f(t)dt = \int_a^c f(t)dt + \int_c^b f(t)dt.$$

(2) $f : (a, b] \longrightarrow \mathbb{R}$ が $[a, b]$ で広義積分可能なとき、任意の実数 $c \in (a, b]$ に対して f は $(a, c]$ 上で広義積分可能で、次の等式が成り立つ：

$$\int_a^b f(t)dt = \int_a^c f(t)dt + \int_c^b f(t)dt.$$

(**proof**)

(1) も (2) も証明は同様なので、ここでは (1) を証明する。

$\beta := \lim_{x\to b-0}\int_a^x f(t)dt$ とおき、任意に $\varepsilon > 0$ をとる。このとき、

$$\exists\,\delta > 0 \ \text{ s.t. } \ b - x < \delta,\ x \in [a,b) \ \Rightarrow\ \left|\int_a^x f(t)dt - \beta\right| < \varepsilon$$

が成り立つ。したがって、区間の分割に関する定積分の加法性 (補題 22-5) により

$$b - x < \delta,\ x \in [c,b) \ \Rightarrow\ \left|\int_c^x f(t)dt - \left(\beta - \int_a^c f(t)dt\right)\right| = \left|\int_a^x f(t)dt - \beta\right| < \varepsilon$$

を得る。これより、f は $[c,b)$ 上で広義積分可能であって、次の等式が成り立つ：

$$\lim_{x\to b-0}\int_c^x f(t)dt = \beta - \int_a^c f(t)dt. \qquad \square$$

●広義積分可能性の判定条件

半開閉区間上で定義された連続関数が広義積分可能かどうかを知る際には、次の定理が役に立ちます。

定理 24-10

$a < b$ を満たす実数 a, b に対して、次が成り立つ。

(1) 次の条件を満たす連続関数 $f : [a,b) \longrightarrow \mathbb{R}$ は $[a,b)$ 上で広義積分可能である。

$$\exists\, C > 0,\ \exists\,\alpha > 0 \ \text{ s.t. } \ \forall\, x \in [a,b),\ \ |f(x)| < C(b-x)^{\alpha-1}.$$

(2) 次の条件を満たす連続関数 $f : (a,b] \longrightarrow \mathbb{R}$ は $(a,b]$ 上で広義積分可能である。

$$\exists\, C > 0,\ \exists\,\alpha > 0 \ \text{ s.t. } \ \forall\, x \in (a,b],\ \ |f(x)| < C(x-a)^{\alpha-1}.$$

(**proof**)

ここでは (1) のみ示す ((2) も同じ方法で証明される)。

$$F(x) := \int_a^x f(t)dt \quad (x \in [a,b))$$

によって定義される $[a,b)$ 上の関数 F が定理 24-7 の条件 (iii) を満たすことを示せばよい。

まず、任意の $x_1, x_2 \in [a,b),\ x_1 \le x_2$ に対して、次が成り立つことに注意しよう：。

$$\begin{aligned}
|F(x_2) - F(x_1)| &= \left|\int_{x_1}^{x_2} f(t)dt\right| \le \int_{x_1}^{x_2}|f(t)|dt \quad (\text{補題 22-2(2) を } -|f| \le f \le |f| \text{ に適用}) \\
&\le C\int_{x_1}^{x_2}(b-t)^{\alpha-1}dt = C\Big[-\tfrac{1}{\alpha}(b-t)^{\alpha}\Big]_{x_1}^{x_2} \\
&= \tfrac{C}{\alpha}((b-x_1)^{\alpha} - (b-x_2)^{\alpha}).
\end{aligned}$$

さて、任意に $\varepsilon > 0$ をとる。$\alpha > 0$ なので、例 24-8 により、次の条件を満たす $\delta > 0$ が存在する：

$$x_1, x_2 \in (-\infty, b),\ b - x_1 < \delta,\ b - x_2 < \delta \ \Rightarrow\ |(b-x_2)^{\alpha} - (b-x_1)^{\alpha}| < \frac{\varepsilon^{\alpha}}{C}.$$

故に、$b - x_1 < \delta,\ b - x_2 < \delta$ を満たすすべての $x_1, x_2 \in [a,b)$ について、

$$|F(x_2) - F(x_1)| \le \frac{C}{\alpha}|(b-x_2)^{\alpha} - (b-x_1)^{\alpha}| < \varepsilon$$

が成り立つ。定理 24-7 により、左側極限 $\lim_{x\to b-0} F(x)$ が存在する。よって、f は $[a,b)$ 上で広義積分可能である。 □

●制限写像

集合 A から集合 B への写像 $f : A \longrightarrow B$ と A の空でない部分集合 A' が与えられたとします。このとき、A' から B への写像 $f|_{A'} : A' \longrightarrow B$ を

$$f|_{A'}(x) = f(x) \quad (x \in A')$$

によって定義することができます。この写像を f の A' への**制限** (restriction) といいます。

$S \subset \mathbb{R}$ 上で定義された関数 $f : S \longrightarrow \mathbb{R}$ が連続ならば、S の任意の部分集合 S' $(\neq \varnothing)$ について、制限 $f|_{S'}$ は連続です。また、開集合 U 上で定義された関数 $f : U \longrightarrow \mathbb{R}$ が微分可能ならば、U に含まれる任意の開集合 U' $(\neq \varnothing)$ について、制限 $f|_{U'}$ は微分可能です。

●開区間上での広義積分

連続関数 $f : (a,b) \longrightarrow \mathbb{R}$ が (a,b) で**広義積分可能**であるとは、任意の $c \in (a,b)$ に対して、$f|_{[c,b)} : [c,b) \longrightarrow \mathbb{R}$ と $f|_{(a,c]} : (a,c] \longrightarrow \mathbb{R}$ がそれぞれ $[c,b)$ と $(a,c]$ において広義積分可能なときをいいます（注：補題 24-9 により、“任意の $c \in (a,b)$” を “ある $c \in (a,b)$” に置き換えることができます)。このとき、補題 24-9 により、和

$$\int_a^c f(t)dt + \int_c^b f(t)dt$$

は $c \in (a,b)$ の選び方によりません。この値を $\int_a^b f(t)dt$ によって書き表わします。

例24-11 関数 $f : (-1,1) \longrightarrow \mathbb{R}$ を $f(x) = \dfrac{1}{\sqrt{1-x^2}}$ $(x \in (-1,1))$ によって定義する。

f は $(-1,1)$ 上で広義積分可能である。

(**proof**)

$f|_{[0,1)}$, $f|_{(-1,0]}$ がそれぞれ $[0,1]$, $[-1,0]$ 上で広義積分可能であることを示せばよい。

$$\forall\, x \in [0,1), \quad |f(x)| = (1+x)^{-\frac{1}{2}}(1-x)^{-\frac{1}{2}} \leq (1-x)^{-\frac{1}{2}}$$

が成り立つから、$f|_{[0,1)}$ は $[0,1)$ 上で広義積分可能である (定理 24-10)。同様に、

$$\forall\, x \in (-1,0], \quad |f(x)| = (1+x)^{-\frac{1}{2}}(1-x)^{-\frac{1}{2}} \leq (1+x)^{-\frac{1}{2}}$$

が成り立つから、$f|_{(-1,0]}$ は $(-1,0]$ 上で広義積分可能である。よって、示された。 □

演習 24-5* 任意の実数 $p, q > 0$ に対して、広義積分 $B(p,q) = \int_0^1 x^{p-1}(1-x)^{q-1}dx$ は収束することを示せ。

ヒント：p, q のそれぞれが 1 より大きい場合と 1 以下の場合に分けて考察する。

注意：２変数関数 $B(p,q)$ $(p,q>0)$ は**ベータ関数** (beta function) と呼ばれる重要な関数です。$x^p(1-x)^{q-1} = (1-x)^{p+q-1}\left(\frac{x}{1-x}\right)^p$ と書いて、部分積分公式を適用すると、漸化式 $B(p+1,q) = \frac{p}{p+q}B(p,q)$ を導くことができます。これより、p, q が自然数のとき、$B(p,q) = \frac{(p+q-1)!}{(p-1)!(q-1)!}$ であることがわかります（二項係数によく似ていますね)。

§25. 曲線の長さ

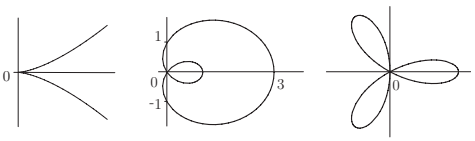
ここでは、曲線の長さを厳密に定義し、その積分公式を導きます。さらに、それを用いて、円周率、正弦関数、余弦関数を厳密に定義します。ここでの目標は、曲線の長さの扱いを通して、定積分、微分、上限、収束などの解析学の諸概念に対する理解を深めることです。この節では、行列との積を考えないので、$\mathbb{R}^n = \{(a_1, \cdots, a_n) \mid a_1 \in \mathbb{R}, \cdots, a_n \in \mathbb{R}\}$ と考え、これを和 $(x_1, \cdots, x_n)+(y_1, \cdots, y_n) = (x_1+y_1, \cdots, x_n+y_n)$ とスカラー倍 $t(x_1, \cdots, x_n) = (tx_1, \cdots, tx_n)$ を備えた数ベクトル空間として扱います。

●曲線

区間 I から $\mathbb{R}^n$ への連続写像を**パラメータつき曲線** (parametrized curve) といいます。

例 25-1 パラメータつき曲線の例

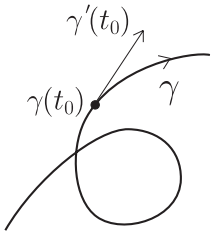
(1) $\gamma(t) = (t^2,\ t^3)\ \ (t \in \mathbb{R})$
(2) $\gamma(t) = (\cos t + \cos 2t + 1,\ \sin t + \sin 2t)\ \ (t \in \mathbb{R})$
(3) $\gamma(t) = (\cos t + \cos 2t,\ -\sin t + \sin 2t)\ \ (t \in \mathbb{R})$
(4) $\gamma(t) = (e^{-t}\cos t,\ e^{-t}\sin t)\ \ (t \in \mathbb{R})$



左から (1)(2)(3) の曲線の像

● C^1-級曲線

$\mathbb{R}$ の開集合 U 上で定義された関数 $f : U \longrightarrow \mathbb{R}$ が **C^1-級** (C^1-class) であるとは、f が微分可能であって、かつ、その導関数 f' が連続なときをいいます。



パラメータつき曲線 $\gamma : I \longrightarrow \mathbb{R}^n$ が **C^1-級**であるとは、I が開区間であって、$\gamma(t) = (\gamma_1(t), \cdots, \gamma_n(t))\ \ (t \in I)$ によって定まる n 個の 1 変数関数 $\gamma_i : I \longrightarrow \mathbb{R}\ \ (i = 1, \cdots, n)$ がどれも C^1-級であるときをいいます。このとき、$\gamma' : I \longrightarrow \mathbb{R}^n$ を $\gamma'(t) = (\gamma_1'(t), \cdots, \gamma_n'(t))\ (t \in I)$ によって定義します。各 $t_0 \in I$ に対して、$\gamma'(t_0)$ を (時刻) t_0 における γ の**速度ベクトル** (velocity vector) あるいは**接ベクトル** (tangent vector) と呼びます。

例 25-2 例 25-1 のパラメータつき曲線はすべて C^1-級である。例えば、パラメータつき曲線 $\gamma : \mathbb{R} \longrightarrow \mathbb{R}^2,\ \gamma(t) = (t^2,\ t^3)$ の t_0 における速度ベクトルは $\gamma'(t_0) = (2t_0,\ 3t_0^2)$ である。

●ベクトルの長さ

$\mathbb{R}^n$ に属する元 $x = (x_1, \cdots, x_n)$ に対して、

$$\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2} = \sqrt{x_1^2 + \cdots + x_n^2}$$

と定め、これを x の**長さ** (norm) といいます。各 $x \in \mathbb{R}^n$ にその長さ $\|x\|$ を対応させる関数 $\|\cdot\| : \mathbb{R}^n \longrightarrow \mathbb{R}$ は連続です。

演習 25-1 任意の $x, y \in \mathbb{R}^n$ に対して、$\|x + y\| \leq \|x\| + \|y\|$ が成り立つことを示せ。

注意：1. 任意の $x=(x_1,\cdots,x_n)\in\mathbb{R}^n$ は $x=(x_1,0,\cdots,0)+\cdots+(0,\cdots,0,x_n)$ と書くことができるので、演習問題の不等式から不等式

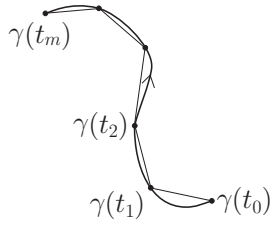
$$\|x\|\le|x_1|+\cdots+|x_n|$$

が従います。
2. $\mathbb{R}^n$ のユークリッド距離 $d^{(n)}$ (p.114) は $d^{(n)}(x,y)=\|x-y\|$ $(x,y\in\mathbb{R}^n)$ と表わされるので、演習問題の不等式から三角不等式

$$d^{(n)}(x,z)\le d^{(n)}(x,y)+d^{(n)}(y,z)$$

が従います。

●パラメータつき曲線の長さ



$\gamma:[a,b]\longrightarrow\mathbb{R}^n$ をパラメータつき曲線とし、$\Delta: a=t_0<t_1<\cdots<t_m=b$ を $[a,b]$ の分割とします。このとき、

$$\ell_\Delta(\gamma):=\sum_{i=1}^{m}\|\gamma(t_i)-\gamma(t_{i-1})\|$$

と定めます。$[a,b]$ の分割 Δ' が Δ の細分ならば、$\ell_\Delta(\gamma)\le\ell_{\Delta'}(\gamma)$ が成り立ちます (演習 25-1)。$\mathbb{R}$ の部分集合 $\{\,\ell_\Delta(\gamma)\mid\Delta$ は $[a,b]$ の分割$\,\}$ に上限が存在するとき、γ は**長さ有限** (finite length) であるといいます。その上限を $\ell(\gamma)$ と書き、γ の**長さ** (length) といいます。

演習 25-1 の下の注意 1 の不等式を使って、次の補題を証明することができます。

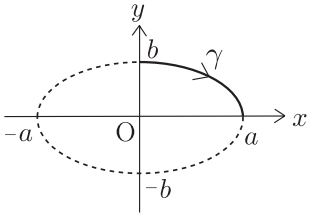
補題 25-3
$\gamma:[a,b]\longrightarrow\mathbb{R}^n$ をパラメータつき曲線とし、関数 $\gamma_i:[a,b]\longrightarrow\mathbb{R}$ $(i=1,\cdots,n)$ を $\gamma(t)=(\gamma_1(t),\cdots,\gamma_n(t))$ $(t\in[a,b])$ によって定義する。このとき、各 γ_i が単調関数ならば、γ は長さ有限である。

演習 25-2 上の補題を証明せよ。

例 25-4 $a\ge b>0$ として、パラメータつき曲線 $\gamma:[0,a]\longrightarrow\mathbb{R}^2$ を

$$\gamma(t)=\Big(t,\ \frac{b}{a}\sqrt{a^2-t^2}\Big)\qquad(t\in[0,a])$$

によって定義する。補題 25-3 により、γ の長さ有限である。γ は方程式 $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$ によって表わされる楕円の“ 4 分の 1 ”弧を表わしている。



補題 22-4 の証明と同様の方法で次の補題を証明することができます。

補題 25-5
$\gamma:[a,b]\longrightarrow\mathbb{R}^n$ をパラメータつき曲線とし、$c\in(a,b)$ とするとき、

$$\gamma\text{ は長さ有限}\iff\gamma|_{[a,c]},\ \gamma|_{[c,b]}\text{ は長さ有限}$$

が成り立つ。さらに、γ が長さ有限のとき、次の等式が成り立つ：

$$\ell(\gamma)=\ell(\gamma|_{[a,c]})+\ell(\gamma|_{[c,b]}).$$

●曲線の長さに関するダルブーの定理

閉区間 $[a,b]$ の分割 $\Delta : a = t_0 < t_1 < \cdots < t_m = b$ に対して、記号 $|\Delta|$ は実数

$$|\Delta| = \max\{\ t_1 - t_0, \cdots, t_m - t_{m-1}\ \}$$

を表わすのでした。定積分に関するダルブーの定理と同様に、次が成り立ちます。

定理 25-6

$\gamma : [a,b] \longrightarrow \mathbb{R}^n$ を長さ有限なパラメータつき曲線とする。このとき、次が成り立つ。

$$\forall\, \varepsilon > 0,\ \exists\, \delta > 0\ \text{ s.t. }\ \Delta : [a,b]\ \text{の分割},\ |\Delta| < \delta\ \Rightarrow\ \ell(\gamma) - \ell_\Delta(\gamma) < \varepsilon.$$

(**proof**)

$\varepsilon > 0$ を任意にとる。$\ell(\gamma)$ の定義から、

$$\exists\, \Delta_0 : a = x_0 < x_1 < \cdots < x_N = b : [a,b]\ \text{の分割}\ \text{ s.t. }\ \ell(\gamma) - \frac{\varepsilon}{2} < \ell_{\Delta_0}(\gamma)$$

が成り立つ。一方、関数 $\gamma_i\ \ (i = 1, \cdots, n)$ を

$$\gamma(t) = (\gamma_1(t), \cdots, \gamma_n(t)) \qquad (t \in [a,b])$$

によって定める。各 γ_i は閉区間上の連続関数であるから一様連続である。よって、次の条件を満たす $\delta_i > 0$ が存在する：

$$t, s \in [a,b],\ |s-t| < \delta_i\ \Rightarrow\ |\gamma_i(t) - \gamma_i(s)| < \frac{\varepsilon}{4nN}.$$

そこで、$\delta_0 := \min\{\delta_1, \cdots, \delta_n\}$ と定めると、次が成り立つ (演習 25-1 の下の注意参照)：

$$t, s \in [a,b],\ |s-t| < \delta_0\ \Rightarrow\ \|\gamma(t) - \gamma(s)\| < \frac{\varepsilon}{4N}.$$

$\delta := \min\{\delta_0,\ \min\{\ x_1 - x_0, \cdots, x_N - x_{N-1}\ \}\}$ と定め、$[a,b]$ の分割 $\Delta : a = t_0 < t_1 < \cdots < t_m = b$ であって、$|\Delta| < \delta$ を満たすものを任意にとる。各 $[t_{i-1}, t_i]$ には、Δ_0 の分点は高々 1 つしか属さないから、

$$I := \{\ i \in \{1, \cdots, m\} \mid (t_{i-1}, t_i]\ \text{は}\ \Delta_0\ \text{の分点を含む}\ \}$$

はちょうど N 個の元からなる。Δ と Δ_0 の分点を合わせて得られる $[a,b]$ の分割を Δ' とおき、各区間 $(t_{i-1}, t_i]$ に属する Δ_0 の分点を x_{p_i} とおく。このとき、

$$\|\gamma(x_{p_i}) - \gamma(t_{i-1})\| + \|\gamma(t_i) - \gamma(x_{p_i})\| \le \frac{\varepsilon}{4N} + \frac{\varepsilon}{4N} = \frac{\varepsilon}{2N}$$

が成り立つので、

$$\ell_{\Delta'}(\gamma) - \ell_\Delta(\gamma) \le \sum_{i \in I} (\|\gamma(x_{p_i}) - \gamma(t_{i-1})\| + \|\gamma(t_i) - \gamma(x_{p_i})\|) \le \sum_{i \in I} \frac{\varepsilon}{2N} = \frac{\varepsilon}{2}$$

を得る。$\ell_{\Delta_0}(\gamma) \le \ell_{\Delta'}(\gamma)$ を用いて、次の不等式を得る：

$$\begin{aligned}
\ell(\gamma) - \ell_\Delta(\gamma) &= (\ell(\gamma) - \ell_{\Delta_0}(\gamma)) + (\ell_{\Delta_0}(\gamma) - \ell_{\Delta'}(\gamma)) + (\ell_{\Delta'}(\gamma) - \ell_\Delta(\gamma)) \\
&\le (\ell(\gamma) - \ell_{\Delta_0}(\gamma)) + (\ell_{\Delta'}(\gamma) - \ell_\Delta(\gamma)) \\
&< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\
&= \varepsilon. \qquad\qquad \square
\end{aligned}$$

系 25-7

$\gamma : [a,b] \longrightarrow \mathbb{R}^n$ を長さ有限なパラメータつき曲線とする。このとき、

$$\ell(\gamma) = \lim_{t \to b-0} \ell(\gamma|_{[a,t]}) = \lim_{t \to a+0} \ell(\gamma|_{[t,b]}).$$

(**proof**)

$\ell(\gamma) = \lim_{t \to b-0} \ell(\gamma|_{[a,t]})$ を示す ($\ell(\gamma) = \lim_{t \to a+0} \ell(\gamma|_{[t,b]})$ の証明も同様)。

任意に $\varepsilon > 0$ をとる。定理 25-6 により、次の条件を満たす $\delta_1 > 0$ が存在する：

$$|\Delta| < \delta_1 \text{ を満たす } [a,b] \text{ のすべての分割 } \Delta \text{ について、} \ell(\gamma) - \ell_\Delta(\gamma) < \frac{\varepsilon}{2}.$$

また、$\gamma : [a,b] \longrightarrow \mathbb{R}^n$ は点 b で連続であるから、次が成り立つ：

$$\exists\, \delta_2 > 0 \ \text{ s.t. } \ t \in [a,b],\ |t-b| < \delta_2 \ \Rightarrow\ \|\gamma(t) - \gamma(b)\| < \frac{\varepsilon}{2}.$$

そこで、$\delta = \min\{\delta_1, \delta_2\}$ とおき、$b - t < \delta$ をみたす $t \in [a,b]$ を任意にとる。$|\Delta_0| < \delta$ を満たす $[a,t]$ の分割 Δ_0 を 1 つ取り、Δ_0 と $[t,b]$ を合わせて $[a,b]$ の分割 Δ を作ると、

$$\ell_{\Delta_0}(\gamma|_{[a,t]}) + \|\gamma(b) - \gamma(t)\| = \ell_\Delta(\gamma) > \ell(\gamma) - \frac{\varepsilon}{2}$$

であるから、

$$\ell(\gamma) - \ell(\gamma|_{[a,t]}) \le \ell(\gamma) - \ell_{\Delta_0}(\gamma|_{[a,t]}) < \frac{\varepsilon}{2} + \|\gamma(b) - \gamma(t)\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

となる。これは、$\ell(\gamma) = \lim_{t \to b-0} \ell(\gamma|_{[a,t]})$ を意味する。 □

● C^1-級パラメータつき曲線の長さ

パラメータつき曲線が C^1-級のときには、その長さを積分によって表わすことができます。

定理 25-8

$\gamma : I \longrightarrow \mathbb{R}^n$ を C^1-級パラメータつき曲線とする。このとき、任意の $a, b \in I,\ a < b$ に対して、$\gamma|_{[a,b]}$ は長さ有限であり、その長さは次式で与えられる。

$$\ell(\gamma|_{[a,b]}) = \int_a^b \|\gamma'(s)\| ds.$$

(**proof**)

関数 $\gamma_i : I \longrightarrow \mathbb{R}\ \ (i = 1, \cdots, n)$ を $\gamma(t) = (\gamma_1(t), \cdots \gamma_n(t))\ \ (t \in I)$ によって定義する。

$\Delta : a = t_0 < t_1 < \cdots < t_m = b$ を $[a,b]$ の分割とする。各 $i = 1, \cdots, n$ と各 $j = 1, \cdots, m$ に対して、平均値の定理 (定理 23-6) から

$$(\sharp) \qquad \gamma_i(t_j) - \gamma_i(t_{j-1}) = \gamma_i'(c_{ij})(t_j - t_{j-1})$$

となる $c_{ij} \in (t_{j-1}, t_j)$ が存在する。よって、

$$(*) \qquad \ell_\Delta(\gamma|_{[a,b]}) = \sum_{j=1}^m \sqrt{\sum_{i=1}^n \gamma_i'(c_{ij})^2 (t_j - t_{j-1})^2} = \sum_{j=1}^m \sqrt{\sum_{i=1}^n \gamma_i'(c_{ij})^2}\,(t_j - t_{j-1})$$

が成り立つ。$\gamma_i'^2$ は $[a,b]$ 上で連続である ($\because \gamma$ は C^1-級) から、$[a,b]$ で最大値 M_i を持つ (定理 22-7)。このとき、$(*)$ によって、次の不等式を得る：

$$\ell_\Delta(\gamma|_{[a,b]}) \le \sum_{j=1}^m \sqrt{\sum_{i=1}^n M_i}\,(t_j - t_{j-1}) = \sqrt{\sum_{i=1}^n M_i}\,(b-a).$$

故に、$\{\ \ell_\Delta(\gamma)\mid \Delta$ は $[a,b]$ の分割 $\}$ は上に有界であり、$\gamma|_{[a,b]}$ は長さ有限である。

次に $\ell(\gamma|_{[a,b]})$ の公式を求めるために、任意に $\varepsilon>0$ をとる。$M:=M_1+\cdots+M_n+1$ とおく。関数

$$f:[0,M]\longrightarrow\mathbb{R},\quad f(x)=\sqrt{x}\qquad(x\in[0,M])$$

は一様連続である (定理 22-10) から、次の条件を満たす $\xi>0$ が存在する：

$$x,y\in[0,M],\ |x-y|<\xi\ \Rightarrow\ |\sqrt{x}-\sqrt{y}\,|<\frac{\varepsilon}{3(b-a)}.$$

また、各 $i=1,\cdots,n$ について $\gamma_i'^2$ は連続であるから、閉区間 $[a,b]$ 上で一様連続である。したがって、次の条件を満たす $\delta_i>0$ が存在する：

$$t,s\in[a,b],\ |t-s|<\delta_i\ \Rightarrow\ |\gamma_i'(t)^2-\gamma_i'(s)^2|<\frac{\xi}{n}.$$

さて、$\delta_0:=\min\{\delta_1,\cdots,\delta_n\}>0$ とおき、$|\Delta|<\delta_0$ をみたす $[a,b]$ の任意の分割 $\Delta:a=t_0<t_1<\cdots<t_m=b$ を考える。この分割 Δ について (♯) のような $c_{ij}\in(t_{j-1},t_j)$ を各 i,j について取ると、$|t_j-c_{ij}|\le|t_j-t_{j-1}|<\delta_0$ となるので、

$$|\gamma_i'(t_j)^2-\gamma_i'(c_{ij})^2|<\frac{\xi}{n}$$

が成り立つ。したがって、不等式

$$\Big|\sum_{i=1}^n\gamma_i'(t_j)^2-\sum_{i=1}^n\gamma_i'(c_{ij})^2\Big|\le\sum_{i=1}^n\Big|\gamma_i'(t_j)^2-\gamma_i'(c_{ij})^2\Big|<\xi$$

を得る。$\displaystyle\sum_{i=1}^n\gamma_i'(t_j)^2,\ \sum_{i=1}^n\gamma_i'(c_{ij})^2\in[0,M]$ より、

$$\Big|\sqrt{\sum_{i=1}^n\gamma_i'(t_j)^2}-\sqrt{\sum_{i=1}^n\gamma_i'(c_{ij})^2}\,\Big|<\frac{\varepsilon}{3(b-a)}$$

がわかる。よって、関数 $\|\gamma'\|:[a,b]\longrightarrow\mathbb{R}$ を $t\longmapsto\|\gamma'(t)\|\ \ (t\in[a,b])$ によって定めると、$(*)$ により、

$$\big|S_{\Delta,(t_1,\cdots,t_m)}(\|\gamma'\|)-\ell_\Delta(\gamma|_{[a,b]})\big|\le\sum_{j=1}^m\left|\sqrt{\sum_{i=1}^n\gamma_i'(t_j)^2}-\sqrt{\sum_{i=1}^n\gamma_i'(c_{ij})^2}\,\right|(t_j-t_{j-1})<\frac{\varepsilon}{3}$$

が成り立つ。$\|\gamma'\|$ は $[a,b]$ 上で積分可能である ($\because$ $\|\gamma'\|$ は連続) から、次のような $\delta_0'>0$ が存在する：

$$\begin{gathered}|\Delta|<\delta_0'\text{ を満たす任意の分割 }\Delta:a=t_0<t_1<\cdots<t_m=b\text{ と}\\ \text{任意の }\xi_j\in[t_{j-1},t_j]\ \ (j=1,\cdots,m)\text{ に対して、}\\ \Big|S_{\Delta,(\xi_1,\cdots,\xi_m)}(\|\gamma'\|)-\int_a^b\|\gamma'(t)\|dt\,\Big|<\frac{\varepsilon}{3}.\end{gathered}$$

また、定理 25-6 により、次のような $\delta_0''>0$ が存在する：

$$|\Delta|<\delta_0''\text{ を満たす }[a,b]\text{ の任意の分割 }\Delta\text{ について、}\ell(\gamma|_{[a,b]})-\ell_\Delta(\gamma|_{[a,b]})\le\frac{\varepsilon}{3}.$$

故に、$\delta := \min\{\delta_0, \delta_0', \delta_0''\}$ とおき、$|\Delta| < \delta$ を満たす $[a,b]$ の分割 $\Delta : a = t_0 < t_1 < \cdots < t_m = b$ を 1 つ取ってくると、

$$\begin{aligned}\left|\int_a^b \|\gamma'(t)\|dt - \ell(\gamma|_{[a,b]})\right| &\leq \left|\int_a^b \|\gamma'(t)\|dt - S_{\Delta,(t_1,\cdots,t_m)}(\|\gamma'\|)\right| \\ &\quad + \left|S_{\Delta,(t_1,\cdots,t_m)}(\|\gamma'\|) - \ell_\Delta(\gamma|_{[a,b]})\right| \\ &\quad + \left|\ell_\Delta(\gamma|_{[a,b]}) - \ell(\gamma|_{[a,b]})\right| \\ &\leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon\end{aligned}$$

となる。これは、$\ell(\gamma|_{[a,b]}) = \displaystyle\int_a^b \|\gamma'(s)\|ds$ となることを意味する。 □

演習 25-3 * 例 25-1(1) と (4) のパラメータつき曲線 γ について、$\gamma|_{[-2,2]}$ の長さを求めよ。
ヒント：(1) $a > 0$ を定数とし、$t\sqrt{t^2+a} = at/\sqrt{t^2+a} + t^2 \cdot t/\sqrt{t^2+a}$ の両辺を積分 (右辺第２項に部分積分法を適用) して、関数 $f(t) = t\sqrt{t^2+a}$ $(t \in \mathbb{R})$ の原始関数を求める。

●円周率

$a \geq b > 0$ として、パラメータつき曲線 $\gamma : [-a,a] \longrightarrow \mathbb{R}^2$ を

$$\gamma(t) = \left(t,\ \frac{b}{a}\sqrt{a^2-t^2}\right) \qquad (t \in [-a,a])$$

によって定義します (例 25-4 参照)。γ は $(-a,a)$ の各点 t で微分可能であり、$\gamma'(t) = (1, -\frac{bt}{a\sqrt{a^2-t^2}})$ となるので、補題 25-5、系 25-7、定理 25-8 により、その長さは、

$$\ell(\gamma) = \ell(\gamma|_{[-a,0]}) + \ell(\gamma|_{[0,a]}) = \lim_{x\to -a+0} \ell(\gamma|_{[x,0]}) + \lim_{x\to a-0} \ell(\gamma|_{[0,x]})$$

$$= \lim_{x\to -a+0} \int_x^0 \|\gamma'(t)\|dt + \lim_{x\to a-0} \int_0^x \|\gamma'(t)\|dt = \int_{-a}^a \sqrt{\frac{(b^2-a^2)t^2+a^4}{a^2(a^2-t^2)}}dt$$

で与えられます。この広義積分は楕円積分と呼ばれる、重要な研究対象の 1 つです。$a = b = 1$ のとき、この広義積分の値は**円周率** π に他なりません：

$$\pi = \int_{-1}^1 \frac{1}{\sqrt{1-t^2}}dt.$$

●正弦関数と余弦関数

すでに何回か登場していますが、ここでは、正弦関数と余弦関数の定義を反省します。関数 $\phi : [-1,1] \longrightarrow \mathbb{R}$ を

$$\phi(x) = \begin{cases} \displaystyle\int_x^1 \frac{1}{\sqrt{1-t^2}}dt & (x \in (-1,1) \text{ のとき}) \\ 0 & (x = 1 \text{ のとき}) \\ \pi & (x = -1 \text{ のとき}) \end{cases}$$

によって定義します。定義から ϕ は連続です。また、微積分学の基本定理により、ϕ は $(-1,1)$ 上で微分可能であり、その導関数は次式によって与えられます：

$$\phi'(t) = \frac{-1}{\sqrt{1-t^2}} \quad (t \in (-1,1)).$$

演習 25-4 * $\phi(0)=\frac{\pi}{2},\ \phi(\frac{1}{\sqrt{2}})=\frac{\pi}{4},\ \phi(-\frac{1}{\sqrt{2}})=\frac{3\pi}{4}$ であることを示せ。
ヒント：$\phi(0)=\frac{\pi}{2}$ を示すには、$s:(-1,0]\longrightarrow[0,1),\ s(t)=-t$ という変数変換を考えよ。$\phi(\frac{1}{\sqrt{2}})=\frac{\pi}{4}$ を示すには、$s:[\frac{1}{\sqrt{2}},1)\longrightarrow[0,\frac{1}{\sqrt{2}}),\ s(t)=\frac{t-\sqrt{1-t^2}}{\sqrt{2}}$ という変数変換を考えよ。

ϕ は狭義単調減少関数なので狭義単調減少な逆関数を持ちます。その逆関数を $c:[0,\pi]\longrightarrow[-1,1]\subset\mathbb{R}$ で表わすことにします。逆関数定理 (定理 23-8) から c は $(0,\pi)$ で微分可能であり、任意の $\theta\in(0,\pi)$ に対して

$$c'(\theta)=\frac{1}{\phi'(c(\theta))}=-\sqrt{1-c(\theta)^2}$$

となることがわかります。また、$c(\frac{\pi}{2})=0$ であり、かつ、c は狭義単調減少関数なので、$\theta\in[0,\pi]$ に対して、次が成り立ちます：

$$\begin{cases} c(\theta)>0 & \Longleftrightarrow\ \theta\in[0,\frac{\pi}{2}) \\ c(\theta)=0 & \Longleftrightarrow\ \theta=\frac{\pi}{2} \\ c(\theta)<0 & \Longleftrightarrow\ \theta\in(\frac{\pi}{2},\pi]. \end{cases}$$

$s:[0,\pi]\longrightarrow\mathbb{R}$ を $s(\theta)=\sqrt{1-c(\theta)^2}$ によって定義します。s も $(0,\pi)$ で微分可能であって、$s'(\theta)=c(\theta)$ となることが確かめられます。

補題 25-9
(1) 任意の $\theta\in[0,\frac{\pi}{2}]$ に対して、$c(\theta)=s(\theta+\frac{\pi}{2})=s(\frac{\pi}{2}-\theta)$ が成り立つ。
(2) 任意の $\theta\in[\frac{\pi}{2},\pi]$ に対して、$c(\theta)=-s(\theta-\frac{\pi}{2})=-s(\frac{3\pi}{2}-\theta)$ が成り立つ。

(**proof**)
任意の $\theta\in[0,\frac{\pi}{2}]$ に対して、$c(\theta)=s(\theta+\frac{\pi}{2})$ となることを示す。そのためには、$f(\theta):=\phi(s(\theta+\frac{\pi}{2}))$ に対して、$f(\theta)=\theta\ (\theta\in[0,\frac{\pi}{2}])\ \cdots\cdots(*)$ となることを示せばよい。まず、

$$f(\frac{\pi}{4})=\phi(s(\frac{3\pi}{4}))=\phi(\sqrt{1-c(\frac{3\pi}{4})^2})=\phi(\frac{1}{\sqrt{2}})=\frac{\pi}{4}$$

である (演習 25-4)。また、f は $(0,\frac{\pi}{2})$ の各点において微分可能であり、

$$f'(\theta)=\phi'(s(\theta+\frac{\pi}{2}))s'(\theta+\frac{\pi}{2})=\frac{-1}{\sqrt{1-s(\theta+\frac{\pi}{2})^2}}c(\theta+\frac{\pi}{2})=1$$

である。したがって、任意の $\theta\in(0,\frac{\pi}{2})$ に対して、$f(\theta)=\theta$ を得る（原始関数の一意性)。f は $[0,\frac{\pi}{2}]$ において連続であるから、

$$f(0)=\lim_{\theta\to+0}f(\theta)=0,\qquad f(\frac{\pi}{2})=\lim_{\theta\to\frac{\pi}{2}-0}f(\theta)=\frac{\pi}{2}$$

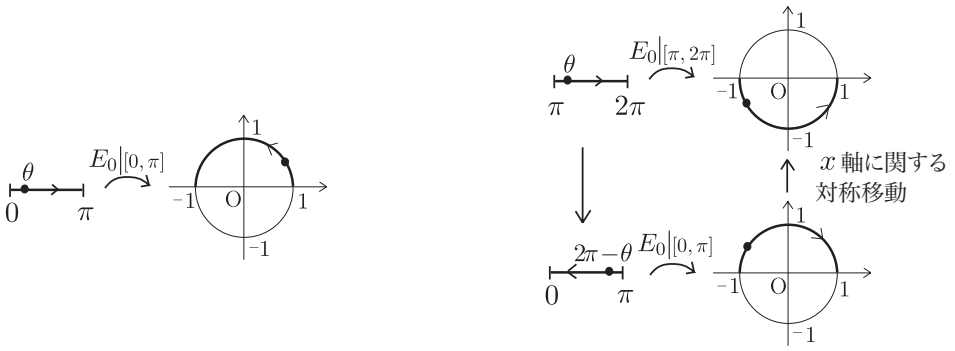
となる。これで、$(*)$ が証明された。残りの三つの等式も同様にして証明することができる。 □

曲線 $E_0:[0,2\pi]\longrightarrow\mathbb{R}^2$ を

$$E_0(\theta)=\begin{cases}(c(\theta),\ s(\theta)) & (\theta\in[0,\pi]\text{ のとき}) \\ (c(2\pi-\theta),\ -s(2\pi-\theta)) & (\theta\in[\pi,2\pi]\text{ のとき})\end{cases}$$

によって定義します ($\theta=\pi$ を上の式に代入しても下の式に代入しても同じ値になることに注意しましょう)。さらに、各整数 n に対して $E_n:[2n\pi,2(n+1)\pi]\longrightarrow\mathbb{R}^2$ を次式で定義します。

$$E_n(\theta)=E_0(\theta-2n\pi)\qquad(\theta\in[2n\pi,2(n+1)\pi]).$$



$E_{n-1}(2n\pi) = (1,0) = E_n(2n\pi)$ なので、$E_n : [2n\pi, 2(n+1)\pi] \longrightarrow \mathbb{R}^2$ たちを“すべての $n \in \mathbb{Z}$ にわたって継なぎ合わせる”ことにより、曲線 $\mathrm{Exp} : \mathbb{R} \longrightarrow \mathbb{R}^2$ を構成することができます：各 $\theta \in \mathbb{R}$ に対して、$\theta \in [2n\pi, 2(n+1)\pi]$ となる $n \in \mathbb{Z}$ をとり、

$$\mathrm{Exp}(\theta) := E_n(\theta).$$

2つの関数 $\cos : \mathbb{R} \longrightarrow \mathbb{R}$ と $\sin : \mathbb{R} \longrightarrow \mathbb{R}$ を

$$\mathrm{Exp}(\theta) = (\cos\theta, \sin\theta) \quad (\theta \in \mathbb{R})$$

により定め、それぞれ**余弦関数** (cosine function)、**正弦関数** (sine function) といいます。

定理 25-10 (余弦関数と正弦関数の性質)

(1) 任意の $\theta \in \mathbb{R}$ について $\sin^2\theta + \cos^2\theta = 1,\ \sin(\theta+2\pi) = \sin\theta,\ \cos(\theta+2\pi) = \cos\theta.$

(2) $\begin{cases} \sin\theta = 0 & \Longleftrightarrow\ \theta = n\pi \quad (n \in \mathbb{Z}) \\ \cos\theta = 0 & \Longleftrightarrow\ \theta = n\pi + \frac{\pi}{2} \quad (n \in \mathbb{Z}) \end{cases}$

(3) sin は $[-\frac{\pi}{2}, \frac{\pi}{2}]$ において狭義単調増加し、cos は $[0,\pi]$ において狭義単調減少する。

(4) sin および cos は微分可能で、$\sin' = \cos,\ \cos' = -\sin$ である。

(**proof**)

(1)(2)(3) については簡単に証明できるから、ここでは、(4) について示そう。

E_0 が π を除くすべての $\theta \in (0, 2\pi)$ において微分可能なことはすぐにわかる。したがって、Exp は $n\pi$ $(n \in \mathbb{Z})$ を除くすべての $\theta \in \mathbb{R}$ において微分可能である。また、$\theta \in (0,\pi)$ に対して $s'(\theta) = c(\theta),\ c'(\theta) = -s(\theta)$ となることから、$n\pi$ $(n \in \mathbb{Z})$ を除くすべての $\theta \in \mathbb{R}$ について、$\sin'\theta = \cos\theta,\ \cos'\theta = -\sin\theta$ であることがわかる。

次に、曲線 $\gamma : [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow \mathbb{R}^2$ と $\delta : [\frac{\pi}{2}, \frac{3\pi}{2}] \longrightarrow \mathbb{R}^2$ をそれぞれ

$$\gamma(\theta) = \big(s\big(\tfrac{\pi}{2} - \theta\big),\ c\big(\tfrac{\pi}{2} - \theta\big)\big) \qquad (\theta \in [-\tfrac{\pi}{2}, \tfrac{\pi}{2}]),$$

$$\delta(\theta) = \big(-s\big(\theta - \tfrac{\pi}{2}\big),\ c\big(\theta - \tfrac{\pi}{2}\big)\big) \qquad (\theta \in [\tfrac{\pi}{2}, \tfrac{3\pi}{2}])$$

によって定義する。$\gamma,\ \delta$ はそれぞれ $0,\ \pi$ で微分可能であり、補題 25-9 により、

$$(\natural) \qquad \mathrm{Exp}(\theta) = \begin{cases} \gamma(\theta - 2m\pi) & (\theta \in [-\frac{\pi}{2} + 2m\pi,\ \frac{\pi}{2} + 2m\pi] \text{ のとき}), \\ \delta(\theta - 2m\pi) & (\theta \in [\frac{\pi}{2} + 2m\pi,\ \frac{3\pi}{2} + 2m\pi] \text{ のとき}) \end{cases}$$

が任意の $m \in \mathbb{Z}$ について成立する。この表示から、Exp は $n\pi$ $(n \in \mathbb{Z})$ においても微分可能であり、$\sin' n\pi = \cos n\pi,\ \cos' n\pi = -\sin n\pi$ であることがわかる。 □

演習 25-5 上の定理の証明における $(\natural)$ 以降の部分を詳しく検証せよ。

§26. 合同式

自然数 m で割った余りが等しい２つの整数は、m を法として合同であると呼ばれます。等号 (=) の代わりに、合同 (≡) を使って記述された整数係数の代数方程式を合同式といいます。ここでは、まず、ユークリッドの互除法について説明します (多項式の場合に以前説明したことを、整数について説明しなおします)。次に、合同式の概念を導入し、１次の合同方程式の解の存在条件、および、その解法を説明します。ここでの目標は、合同式の性質を理解し、計算を通じてその扱い方に慣れることです。

§26-1 ユークリッドの互除法

ユークリッドの互除法は、最大公約数を求めるための強力なアルゴリズムです。

●約数と倍数

２つの整数 $a\ (\neq 0),\ b$ に対して、$b = qa$ となる $q \in \mathbb{Z}$ が存在するとき、b は a の倍数である、あるいは、a は b の約数である、あるいは、b は a で割り切れる、あるいは、a は b を割り切ると呼ぶのでした。このことを、記号 $a|b$ で表わします。

整数 $a\ (\neq 0), b\ (\neq 0), c, d, m, n$ に対して、次が成り立ちます。

(i) $a|b,\ b|c\ \Rightarrow\ a|c$

(ii) $a|b,\ b|a\ \Rightarrow\ a = \pm b$

(iii) $a|c,\ b|d\ \Rightarrow\ ab|cd$

(iv) $a|c,\ a|d\ \Rightarrow\ a|(mc + nd)$

1 は任意の整数の約数であり、0 は任意の整数の倍数です。自然数の整列性により、0 でない整数 b に対して、その約数は有限個しかありません。

$a|b$ でないことを $a \nmid b$ で表わします。

例 26-1　$2|4$ であるが、$3 \nmid 4$ である。

●最大公約数

$a_1, \cdots, a_n$ を n 個の整数とし、$a_1 \neq 0$ であるとします。このとき、$d|a_i\ \ (i = 1, \cdots, n)$ を満たす整数 d を $a_1, \cdots, a_n$ の**公約数** (common divisor) といいます。$a_1, \cdots, a_n$ の正の公約数の中で、最大のものを $a_1, \cdots, a_n$ の**最大公約数**といいます。$a_1, \cdots, a_n$ の最大公約数を $\gcd(a_1, \cdots, a_n)$ または、単に、$(a_1, \cdots, a_n)$ で表わします。

定理 26-2

n 個の整数 $a_1, \cdots, a_n\ \ (a_1 \neq 0)$ の最大公約数は、$\mathbb{Z}$ の部分集合

$$\{\ x_1a_1 + \cdots + x_na_n \mid x_1, \cdots, x_n \in \mathbb{Z}\ \}$$

に属する正の整数の中で最小の元として特徴づけられる。

(**proof**)

ここでは $n = 2$ の場合に証明する（一般の場合も全く同様に証明できる)。

以下、$a = a_1,\ b = a_2$ とし、

$$I := \{\ xa + yb \mid x, y \in \mathbb{Z}\ \}$$

とおく。$0 \neq \pm a \in I$ であるから、I は 0 でない正の整数を含む。したがって、I に属する最小の正の整数 d_0 が存在する（自然数の整列性）。この d_0 が a, b の最大公約数に一致することを示す。そのためには、a, b の最大公約数を d とおき、$d \geq d_0$ かつ $d_0 \geq d$ となることを示せばよい。

(i) $d_0 \geq d$ の証明：

$d|a,\ d|b$ より、任意の $x, y \in \mathbb{Z}$ に対して、$d|(xa + yb)$、すなわち、任意の $h \in I$ に対して $d|h$ となる。$d_0 \in I$ なので、特に、$d|d_0$ が成り立つ。これより、$d_0 \geq d$ を得る。

(ii) $d \geq d_0$ の証明：

$d_0 \in I$ の選び方により、$d_0|a$ かつ $d_0|b$ が成り立つ。

$\because$)

$a = qd_0 + r\ (q, r \in \mathbb{Z},\ 0 \leq r < d_0)$ と書き表わすと、$d_0 \in I$ なので、ある $x, y \in \mathbb{Z}$ により d_0 は $d_0 = xa + yb$ のように表わされる。すると、

$$r = a - qd_0 = (1 - qx)a + (-qy)b \ \in \ I$$

となる。d_0 の選び方から $r = 0$ でなければならない。よって、$d_0|a$ が示された。同様にして、$d_0|b$ を示すことができる。 □

d_0 は a, b の公約数であることがわかったから、$d \geq d_0$ を得る。

(i)(ii) により、$d = d_0$ が証明された。 □

演習 26-1 n 個の整数 $a_1, \cdots, a_n\ \ (a_1 \neq 0)$ の最大公約数は、$a_1, \cdots, a_n$ の任意の公約数によって割り切れることを証明せよ。

0 でない n 個の整数 $a_1, \cdots, a_n$ の最大公約数が 1 のとき、$a_1, \cdots, a_n$ は**互いに素** (relatively prime) であるといいます。定理 26-2 の系として、直ちに、次が得られます。

系 26-3

n 個の整数 $a_1, \cdots, a_n\ \ (a_1 \neq 0)$ の最大公約数を d とするとき、

$$a_1x_1 + \cdots + a_nx_n = d$$

を満たす $x_1, \cdots, x_n \in \mathbb{Z}$ が存在する。特に、$a_1, \cdots, a_n$ が互いに素ならば、

$$a_1x_1 + \cdots + a_nx_n = 1$$

を満たす $x_1, \cdots, x_n \in \mathbb{Z}$ が存在する。

上の系の応用として、次が得られます。

系 26-4

整数 $a, b, s, t\ (a \neq 0, b \neq 0)$ について、次が成り立つ。

(1) $a|st,\ \gcd(a, s) = 1 \quad \Rightarrow \quad a|t.$

(2) $a|s,\ b|s,\ \gcd(a, b) = 1 \quad \Rightarrow \quad ab|s.$

(**proof**)
(1) 系 26-3 により、$ax + sy = 1$ を満たす整数 x, y が存在する。この両辺に t を掛けて、$tax + tsy = t$ となる。仮定 $a|st$ により、$a|(tax + tsy)$ となるから、$a|t$ が示された。
(2) $a|s$ より、$s = aa'$ $(a' \in \mathbb{Z})$ と書くことができる。$b|a'$ を示せばよい。
$\gcd(a, b) = 1$ なので、

$$ua + vb = 1$$

となる $u, v \in \mathbb{Z}$ が存在する (系 26-3)。この両辺に a' を掛けると、

$$us + va'b = uaa' + vba' = a'$$

となる。$b|s$ であるから、$b|(us + va'b)$ である。よって、$b|a'$ が示された。 □

●ユークリッドの互除法

最大公約数はユークリッドの互除法を用いて求めることができます。

命題 26-5
0 でない 2 つの整数 a, b を、ある $q, r \in \mathbb{Z}$ を用いて $a = qb + r$ $(0 \leq r < b)$ と書くとき、

$$\gcd(a, b) = \gcd(b, r)$$

が成り立つ。

(**proof**)
$d = \gcd(a, b)$, $d_1 = \gcd(b, r)$ とおく。
$d|a$ かつ $d|b$ より、$d|(a - qb)$、すなわち、$d|r$ を得る。よって、$d|d_1$ を得る (演習 26-1)。
逆に、$d_1|b$ かつ $d_1|r$ より、$d_1|(qb + r)$、すなわち、$d_1|a$ を得る。よって、$d_1|d$ を得る。
$d|d_1$ かつ $d_1|d$ より、$d = \pm d_1$ が導かれるが、$d, d_1 > 0$ だから $d = d_1$ とわかる。 □

命題 26-5 を $a \geq b$ の場合に適用することにより、a と b の最大公約数を求める問題が、より小さい整数 b と r の最大公約数を求める問題に帰着されることがわかります。したがって、命題 26-5 を繰り返し適用していけば、最後には割り切れる状態になり、最大公約数が求まります。このようにして最大公約数を求めるアルゴリズムを**ユークリッドの互除法**といいます。

●不定方程式

ユークリッドの互除法を使うと、a, b の最大公約数 d が求められるばかりでなく、$ax + by = d$ を満たす $x, y \in \mathbb{Z}$ も求めることができます。

例 26-6 $d := \gcd(123, 33)$ および $123x + 33y = d$ を満たす整数 x, y を 1 組求めよ。
解；

$$\begin{aligned} 123 &= 3 \cdot 33 + 24, \\ 33 &= 1 \cdot 24 + 9, \\ 24 &= 2 \cdot 9 + 6, \\ 9 &= 1 \cdot 6 + 3, \\ 6 &= 2 \cdot 3 \end{aligned}$$

となるから、ユークリッドの互除法により、$d = \gcd(6, 3) = 3$ とわかる。

また、上の計算過程から

$$24 = 123 - 3\cdot 33 = 1\cdot 123 - 3\cdot 33,$$
$$9 = 33 - 1\cdot 24 = 33 - (1\cdot 123 - 3\cdot 33) = -1\cdot 123 + 4\cdot 33,$$
$$6 = 24 - 2\cdot 9 = (1\cdot 123 - 3\cdot 33) - 2\cdot(-1\cdot 123 + 4\cdot 33) = 3\cdot 123 - 11\cdot 33,$$
$$3 = 9 - 1\cdot 6 = (-1\cdot 123 + 4\cdot 33) - 1\cdot(3\cdot 123 - 11\cdot 33) = -4\cdot 123 + 15\cdot 33$$

を得る。最後の等式から、$123x + 33y = 3$ を満たす整数の 1 組として $(x, y) = (-4, 15)$ が見つかる。 □

演習 26-2* $d := \gcd(15640, 1037)$ および $15640x + 1037y = d$ となる整数 x, y を 1 組求めよ。

一般に、0 でない 2 つの整数 a, b および整数 k に対して、$aX + bY = k$ という形の X, Y についての方程式を**不定方程式** (indeterminate equation) といいます。k が $d = \gcd(a, b)$ の倍数のとき、系 26-3 によって、不定方程式 $aX + bY = k$ は必ず整数解を持ちます。そして、不定方程式 $aX + bY = d$ の 1 つの整数解から、次の命題のようにして、不定方程式 $aX + bY = k$ のすべての整数解を求めることができます。

命題 26-7

a, b を 0 でない整数とし、k を $d = \gcd(a, b)$ の倍数とする。このとき、不定方程式 $aX + bY = k$ は解を持つ。さらに、$(X, Y) = (x_0, y_0)$ を不定方程式 $aX + bY = d$ の 1 つの整数解とすると、不定方程式 $aX + bY = k$ のすべての整数解は

$$(X, Y) = \left(\frac{k}{d}x_0 + \frac{b}{d}t,\ \frac{k}{d}y_0 - \frac{a}{d}t\right), \qquad t \in \mathbb{Z}$$

によって与えられる。

(**proof**)

• 不定方程式 $aX + bY = k$ が解を持つこと：

系 26-3 により、不定方程式 $aX + bY = d$ は整数解を持つ。その整数解を $(X, Y) = (x_0, y_0)$ とすると、

$$ax_0 + by_0 = d \tag{$\diamond$}$$

が成り立つ。一方、k は d の倍数なので、$k = dm$ となる整数 m が存在する。($\diamond$) の両辺を m 倍すると

$$a(x_0 m) + b(y_0 m) = dm = k$$

となるので、不定方程式 $aX + bY = k$ は整数解 $(X, Y) = (x_0 m, y_0 m)$ を持つ。

• 不定方程式 $aX + bY = k$ のすべての整数解を求めること：

$(X, Y) = (x, y)$ を不定方程式 $aX + bY = k$ の整数解とすると、$ax + by = k$ が満たされる。2 つの等式

$$\begin{cases} ax + by = k, \\ a(x_0 m) + b(y_0 m) = k \end{cases}$$

の各辺を引いて、

$$a(x - x_0 m) + b(y - y_0 m) = 0 \tag{$\star$}$$

を得る。$d = \gcd(a, b)$ であるから、互いに素な整数 a', b' を使って、

$$a = da', \quad b = db'$$

と表わすことができる。このとき、$(\star)$ の両辺を d で割り、後ろの項を移項すると、

$$a'(x - x_0 m) = b'(y_0 m - y)$$

が得られる。これより、$a' | b'(y_0 m - y)$ がわかるが、$\gcd(a', b') = 1$ なので、$a' | (y_0 m - y)$ である (系 26-4(1))。よって、

$$y_0 m - y = ta' \qquad (t \in \mathbb{Z})$$

とおくことができる。これを $a'(x - x_0 m) = b'(y_0 m - y)$ に代入し、両辺を a' で割って、

$$x - x_0 m = b't$$

が得られる。こうして、$(X, Y) = (x, y)$ が不定方程式 $aX + bY = k$ の整数解であれば、

$$(x, y) = (x_0 m + tb',\ y_0 m - ta') = \left(\frac{k}{d}x_0 + \frac{b}{d}t,\ \frac{k}{d}y_0 - \frac{a}{d}t\right), \quad t \in \mathbb{Z}$$

と表わされることがわかった。逆に、上の形をした整数の組が不定方程式 $aX + bY = k$ の解になっていることは容易に確かめられる。 □

例 26-8 不定方程式 $20X + 9Y = 2$ の整数解をすべて求めよ。

解；

2 は $\gcd(20, 9) = 1$ の倍数であるから、不定方程式 $20X + 9Y = 2$ は整数解を持つ。

(ユークリッドの互除法を用いて、) 不定方程式 $20X + 9Y = 1$ の 1 つの解を求めると、$(X, Y) = (-4, 9)$ であることがわかる (計算略)。したがって、命題 26-7 により、不定方程式 $20X + 9Y = 2$ の整数解は

$$(X, Y) = (2 \cdot (-4) + 9t,\ 2 \cdot 9 - 20t) = (-8 + 9t,\ 18 - 20t), \qquad t \in \mathbb{Z}$$

によって与えられる。 □

§26-2 合同式

ここでは、等号 $=$ の拡張概念である合同 $\equiv$ の概念を導入します。合同 $\equiv$ の基本的な性質を調べたのち、1 次の合同方程式の解の存在条件と解の求め方を学びます。

●整数に対する合同の概念

m を自然数とします。2 つの整数 a, b について、$a - b$ が m の倍数であるとき、すなわち、$a - b = qm$ となる整数 q が存在するとき、

$$a \equiv b \pmod{m}$$

と書いて、a は b に m **を法として合同** (congruent modulo m) であるといいます。$\bmod m$ は「モジュロ m」または「モード m」などと読みます。a が b に m を法として合同でないことを $a \not\equiv b \pmod{m}$ と書き表わします。

例 26-9 $100 \equiv 0 \pmod{2}$ であるが、$100 \not\equiv 0 \pmod{3}$ である。

注意：整数 $a, b \in \mathbb{Z}$ に対して、$a = b$ とは a が b に「0 を法として合同である」ということと思うことができます。このように、「$\equiv \pmod m$」は等号の概念を拡張したものと捉えることができます。

●合同式の基本的性質

“$\equiv \pmod m$”は、以下の 3 つの補題で述べるような性質を持っています。

補題 26-10

$m \in \mathbb{N}$ とする。$a, b, c \in \mathbb{Z}$ に対して、次が成り立つ。

(i) (反射律) $a \equiv a \pmod m$

(ii) (対称律) $a \equiv b \pmod m \quad \Rightarrow \quad b \equiv a \pmod m$

(iii) (推移律) $a \equiv b \pmod m,\ b \equiv c \pmod m \quad \Rightarrow \quad a \equiv c \pmod m$

(**proof**)

(i) $a - a = 0$ は m の倍数であるから、$a \equiv a \pmod m$ が成り立つ。

(ii) $a \equiv b \pmod m$ であると仮定すると、$a - b = qm$ となる $q \in \mathbb{Z}$ が存在する。このとき、$b - a = -qm = (-q)m$ と書けて、$-q \in \mathbb{Z}$ であるから、$b \equiv a \pmod m$ となる。

(iii) $a \equiv b \pmod m$ かつ $b \equiv c \pmod m$ と仮定する。すると、

$$a - b = q_1 m, \quad b - c = q_2 m$$

となる $q_1, q_2 \in \mathbb{Z}$ が存在する。このとき、

$$a - c = (a - b) + (b - c) = q_1 m + q_2 m = (q_1 + q_2)m$$

と書けて、$q_1 + q_2 \in \mathbb{Z}$ であるから $a \equiv c \pmod m$ となる。 □

補題 26-11

$m \in \mathbb{N}$ とし、$a, b, a', b' \in \mathbb{Z}$ は、

$$a \equiv a' \pmod m \ \text{ かつ } \ b \equiv b' \pmod m$$

を満たしているとする。このとき、次が成り立つ。

(i) $a + b \equiv a' + b' \pmod m$

(ii) $a - b \equiv a' - b' \pmod m$

(iii) $ab \equiv a'b' \pmod m$

(**proof**)

ここでは (i) だけを示し、残りは演習問題とする。

$a \equiv a' \pmod m,\ b \equiv b' \pmod m$ なので、

$$a - a' = q_1 m, \qquad b - b' = q_2 m$$

となる $q_1, q_2 \in \mathbb{Z}$ が存在する。このとき、

$$(a + b) - (a' + b') = (a - a') + (b - b') = (q_1 + q_2)m$$

と書けるが、$q_1 + q_2 \in \mathbb{Z}$ であるから、$a + b \equiv a' + b' \pmod m$ が成り立つ。 □

演習 26-3 * 上の補題の (ii)(iii) を証明せよ。

演習 26-4　$11\times13\times19\times23+29\times31\times37$ を 7 で割ったときの余りを求めよ。

補題 26-12

$m\in\mathbb{N},\ a,b,c\in\mathbb{Z}$ とする。$\gcd(c,m)=1$ のとき、次が成り立つ。

$$ca\equiv cb\pmod m\quad\Rightarrow\quad a\equiv b\pmod m.$$

(**proof**)

$ca\equiv cb\pmod m$ であるとすると、$m|(ca-cb)$ となる。$\gcd(c,m)=1$ なので、系 26-4 により、$m|(a-b)$ となる。故に、$a\equiv b\pmod m$ が成り立つ。　□

●1 次の合同方程式

m を 2 以上の整数とし、X を不定元とする整数係数の 1 次多項式

$$aX+b\quad(\text{但し、}m\nmid a)$$

を考えます。整数 x が $ax+b\equiv0\pmod m$ を満たすとき、x は**合同方程式** $aX+b\equiv0\pmod m$ の解である、あるいは、合同方程式 $aX\equiv-b\pmod m$ の解である、といいます。

整数 x が合同方程式 $aX+b\equiv0\pmod m$ の解であるとき、$x\equiv x'\pmod m$ を満たすすべての整数 x' も合同方程式 $aX+b\equiv0\pmod m$ の解になります。合同方程式 $aX+b\equiv0\pmod m$ の解を、m を法としてすべて求めることを、合同方程式 $aX+b\equiv0\pmod m$ を解くといいます。m が小さい場合には、下の例にあるように、$x=0,1,2,\cdots,m-1$ を代入して、与えられた合同式が満たされるかどうかを調べることにより、合同方程式を解くことができます。

例26-13　合同方程式 $4X\equiv2\pmod6$ を解け。

解；

$x=0,1,2,3,4,5$ の中で、$4x\equiv2\pmod6$ を満たすものを求めればよい。

計算により、$x=2,5$ は $4x\equiv2\pmod6$ を満たし、$x=0,1,3,4$ は $4x\equiv2\pmod6$ を満たさないことがわかる。よって、解は、2 と 5 である。　□

●合同方程式の解の存在条件

m を法とする合同方程式 $aX\equiv b\pmod m$ に解があるかないかは、$x=0,1,2,\cdots,m-1$ を代入して調べなくても、次の定理を使って直ちに知ることができます。

定理 26-14

m を 2 以上の整数、a を $m\nmid a$ を満たす整数、b を任意の整数とし、$d=\gcd(a,m)$ とおく。このとき、合同方程式 $aX\equiv b\pmod m$ の解が存在するための必要十分条件は $d|b$ である。

(**proof**)

I. 合同方程式 $aX\equiv b\pmod m$ は解を持つと仮定する。

$x\in\mathbb{Z}$ をその解とすると、$b=ax+qm$ となる $q\in\mathbb{Z}$ が存在する。

d は a と m の最大公約数だから、$d|a$ かつ $d|m$ であり、したがって、$d|(ax+qm)$ となる。これで、$d|b$ が示された。

Ⅱ. $d|b$ であると仮定し、$b=cd$ $(c\in\mathbb{Z})$ と書く。

系 26-3 により、$ax+my=d$ を満たす $x,y\in\mathbb{Z}$ が存在する。両辺を c 倍して、

$$cax+cmy=cd=b$$

を得る。よって、

$$a(cx) \equiv b \pmod{m}$$

となるので、合同方程式 $aX \equiv b \pmod{m}$ は解 $cx \in \mathbb{Z}$ を持つ。 □

上の定理から次の系が導かれます (この系は系 26-3 を使って直接導くこともできます)。

系 26-15
m を 2 以上の整数、a を任意の整数とするとき、次が成り立つ。

$$ax \equiv 1 \pmod{m} \text{ となる } x \in \mathbb{Z} \text{ が存在する} \iff \gcd(a, m) = 1.$$

演習 26-5 * 合同方程式 $36X \equiv 32 \pmod{100}$ は解を持つか。持つ場合にはその解も求めよ。

●中国式剰余定理 (Chinese remainder theorem)

次の定理の原形が、古代中国において暦の作成に使われていたそうです。

定理 26-16 (中国式剰余定理)
$m_1, m_2, \cdots, m_n$ を互いに素な 2 以上の整数、$a_1, a_2, \cdots, a_n$ を任意の整数とする。このとき、連立 1 次合同方程式

$$\begin{cases} X \equiv a_1 \pmod{m_1} \\ X \equiv a_2 \pmod{m_2} \\ \quad \cdots\cdots \\ X \equiv a_n \pmod{m_n} \end{cases}$$

の解が、$m = m_1 m_2 \cdots m_n$ を法としてただ 1 つ存在する。

(**proof**)

I. 解の存在：

各 $i = 1, \cdots, n$ に対して、$M_i \in \mathbb{Z}$ を $m = m_i M_i$ によって定める。$m_1, \cdots, m_n$ は互いに素であるから、m_i と M_i も互いに素である。よって、$x_i M_i \equiv 1 \pmod{m_i}$ を満たす $x_i \in \mathbb{Z}$ が存在する (系 26-15)。そこで、

$$x = a_1 x_1 M_1 + a_2 x_2 M_2 + \cdots + a_n x_n M_n$$

とおく。この x は与えられた連立 1 次合同方程式の解である。実際、$i \in \{1, \cdots, n\}$ を任意にとると、$j \neq i$ なる $j \in \{1, \cdots, n\}$ については $M_j \equiv 0 \pmod{m_i}$ であるから、x は

$$x \equiv a_i x_i M_i \equiv a_i \pmod{m_i}$$

を満たすことがわかる。

II. 解の一意性：

$x, x' \in \mathbb{Z}$ が与えられた連立 1 次合同方程式の 2 つの解であるとすると、すべての $i = 1, \cdots, n$ に対して $x \equiv a_i \equiv x' \pmod{m_i}$ となる。$m_1, \cdots, m_n$ は互いに素であるから、$x \equiv x' \pmod{m}$ となる (系 26-4(2))。このことは、x と x' が m を法として同じ解であることを意味する。 □

演習 26-6 3 で割ると 2 余り、5 で割ると 3 余り、7 で割ると 5 余る正の整数の中で最小のものを求めよ。

§27. 同値関係

日常使われる言葉“関係”は数学では専門用語として使われます。例えば、等号 $=$、不等号 $\leq$、合同 $\equiv \pmod m$ は“関係”の一種です。ここでは、“関係”の中の“同値関係”という概念について説明します。同値関係で結ばれているもの同士を“同じもの”とみなすことにより、同値類や商集合の概念が得られます。ここでの目標は、同値関係、同値類、商集合の概念を理解し、その扱い方に慣れることです。

§27-1 同値関係

集合 X 上の関係とは、X の2元 x, y について、$x \sim y$ であるか、$x \sim y$ でないかのどちらか一方が成り立つような“$\sim$ のこと”をいいます。特に大切な性質を持つ関係として、同値関係と順序関係がありますが、ここでは、同値関係のみを考察します。

●関係

X を空でない集合とします。直積集合 $X \times X$ の部分集合 R を X 上の**二項関係** (binary relation)、あるいは、単に、**関係**といいます。$x, y \in X$ が $(x, y) \in R$ を満たすとき、x と y の間に関係 R が成立するといい、xRy のように書き表わします。

例 27-1 (1) $\{\, (x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x \leq y \,\}$ は $\mathbb{Q}$ 上の1つの関係である。この関係を $\mathbb{Q}$ 上の大小関係という。
(2) m を自然数とする。$\{\, (x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod m \,\}$ は $\mathbb{Z}$ 上の1つの関係である。この関係を $\mathbb{Z}$ 上の m を法とする合同関係という。

集合 X 上に関係を定義したいときは、次の例のような書き方をよくします。

例 27-2 $\mathbb{R}$ 上の関係 R を、$x, y \in \mathbb{R}$ に対して、

$$xRy \overset{\text{def}}{\iff} x - y \in \mathbb{Z}$$

によって定義する。

この例の場合、$R = \{\, (x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{Z} \,\}$ という $\mathbb{R}$ 上の関係を考えていることになります。

●同値関係

空でない集合 X 上の関係 R が次の3条件を満たすとき、R は X 上の**同値関係** (equivalence relation) であるといいます。

(i) (**反射律**) 任意の $x \in X$ に対して、xRx である。
(ii) (**対称律**) 任意の $x, y \in X$ について、「xRy ならば yRx」である。
(iii) (**推移律**) 任意の $x, y, z \in X$ について、「「xRy かつ yRz」ならば xRz」である。

上では同値関係を、記号 R で表わしましたが、これより以後は慣例に従い、記号 $\sim$ を主に使います。

例 27-3

(1) $\mathbb{Q}$ 上の大小関係 $\leq$ (例 27-1(1)) は、同値関係ではない。なぜならば、$1 \leq 2$ であるのに $2 \leq 1$ ではないからである (対称律を満たさない)。

(2) m を自然数とする。$\mathbb{Z}$ 上の m を法とする合同関係 $\equiv \pmod m$ (例 27-1(2)) は、補題 26-10 により、$\mathbb{Z}$ 上の同値関係である。

(3) $\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ のいずれかとして、すべての成分が $\mathbb{K}$ の元からなる (m,n)-行列の全体 $\mathrm{M}_{mn}(\mathbb{K})$ を考える。$\mathrm{M}_{mn}(\mathbb{K})$ 上に関係 $\sim$ を、$A, B \in \mathrm{M}_{mn}(\mathbb{K})$ に対して、

$$A \sim B \overset{\text{def}}{\iff} B = PAQ \text{ となる正則行列 } P \in \mathrm{M}_m(\mathbb{K}) \text{ と正則行列 } Q \in \mathrm{M}_n(\mathbb{K}) \text{ が存在する}$$

によって定義する。$\sim$ は $\mathrm{M}_{mn}(\mathbb{K})$ 上の同値関係である。

演習 27-1 * $X := \mathbb{Z} \times (\mathbb{Z} - \{0\})$ 上に関係 $\sim$ を、$(a,x), (b,y) \in X$ について

$$(a,x) \sim (b,y) \overset{\text{def}}{\iff} ay = bx$$

によって定義する。$\sim$ は X 上の同値関係であることを示せ。

●同値類

空でない集合 X 上に同値関係 $\sim$ が与えられているとします。このとき、各 $a \in X$ に対して、X の部分集合 $[a]$ を

$$[a] := \{x \in X \mid x \sim a\}$$

によって定め、これを $\sim$ に関する a の**同値類** (equivalence class) といいます。X の部分集合 C が $\sim$ に関する同値類であるとは、ある $a \in X$ によって $C = [a]$ と表わされるときをいいます。このような a を同値類 C の**代表元** (representative) といいます。

例 27-4 2 を法とする合同関係 $\equiv \pmod 2$ を考える。$\mathbb{Z}$ の部分集合

$$C := \{2n \mid n \in \mathbb{Z}\}, \qquad D := \{2n+1 \mid n \in \mathbb{Z}\}$$

は、それぞれ、$C = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 2\} = [0]$, $D = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 2\} = [1]$ と書けるので、$\equiv \pmod 2$ に関する同値類である。0 や 2 は C の代表元であり、1 や -1 は D の代表元である。

同値類については、次の定理が基本的です。この定理は、X を同値類に分割するとき、同値類同士には共通部分がないか、または、共通部分があったとすれば完全に一致してしまうということを主張しています。

定理 27-5

X を空でない集合、$\sim$ をその上の同値関係とする。$x, y \in X$ について、次の 3 つは同値である。

① $x \sim y$　　② $[x] \cap [y] \neq \varnothing$　　③ $[x] = [y]$

(**proof**)

「③ ⇒ ② ⇒ ① ⇒ ③」の順番で示す。

③ ⇒ ②：反射律により $x \in [x]$ であるから、$[x] = [y]$ ならば $x \in [x] \cap [y]$ である。よって、$[x] \cap [y] \neq \varnothing$ である。

② ⇒ ①：$[x] \cap [y] \neq \varnothing$ なので、元 $z \in [x] \cap [y]$ が存在する。$z \in [x]$ より $z \sim x$ であり、対称律により、$x \sim z$ である。一方、$z \in [y]$ より $z \sim y$ である。したがって、$x \sim z$ かつ $z \sim y$ が成り立つ。ここで推移律を使うと、$x \sim y$ がいえる。

① ⇒ ③：この証明は演習問題として残しておく。 □

演習 27-2 * 上の定理の「① ⇒ ③」を証明せよ。

●商集合

X を空でない集合とし、$\sim$ を X 上の同値関係とします。このとき、X の同値類全体からなる集合を $X/\sim$ によって書き表わし、これを $\sim$ による X の**商集合** (quotient set) 、または、**剰余集合** (residue set) といいます：

$$X/\sim = \{\ [a] \mid a \in X\ \}.$$

例 27-6 m を 2 以上の自然数とし、$\mathbb{Z}$ 上の同値関係 $\sim$ を合同関係 $\equiv \pmod m$ によって定義する。商集合 $\mathbb{Z}/\sim$ を $\mathbb{Z}/m\mathbb{Z}$ と書く（著者によっては、$\mathbb{Z}_m$ や $\mathbb{Z}/(m)$ という記号が使われる）。また、各 $a \in \mathbb{Z}$ に対して、$\sim$ に関する a の同値類を $[a]_m$ と書くことにする：

$$[a]_m = \{\ x \in \mathbb{Z} \mid x \equiv a \pmod m\ \}.$$

このとき、次が成り立つ：

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \cdots, [m-1]_m\}.$$

(**proof**)

$\{[0]_m, [1]_m, \cdots, [m-1]_m\} \subset \mathbb{Z}/m\mathbb{Z}$ は商集合の定義から明らかである。

$\mathbb{Z}/m\mathbb{Z} \subset \{[0]_m, [1]_m, \cdots, [m-1]_m\}$ を示す。

$C \in \mathbb{Z}/m\mathbb{Z}$ を任意にとる。すると、$C = [a]_m$ $(a \in \mathbb{Z})$ と書くことができる。除法の原理から、$a = qm + r$ $(0 \leq r < m)$ を満たす $q, r \in \mathbb{Z}$ が存在する。このとき、$a \equiv r \pmod m$ となるから、$[a]_m = [r]_m$ が成り立つ (定理 27-5)。よって、$C = [r]_m \in \{[0]_m, [1]_m, \cdots, [m-1]_m\}$ が示された。 □

演習 27-3 例 27-3(3) で与えられている $\mathrm{M}_{mn}(\mathbb{K})$) 上の同値関係 $\sim$ を考える。商集合 $\mathrm{M}_{mn}(\mathbb{K})/\sim$ は有限集合であることを示せ。また、その元の個数を求めよ。

●部分集合族

集合 X の冪集合 $\mathcal{P}(X) = \{\ X$ の部分集合全体 $\}$ の空でない部分集合を X の部分集合族と呼ぶのでした (p.42 参照)。つまり、X の部分集合族とは、X の部分集合を要素とするような空でない集合のことです。例えば、閉区間 $[-\frac{1}{n}, \frac{1}{n}]$ を要素とする集合 $\{[-\frac{1}{n}, \frac{1}{n}] \mid n \in \mathbb{N}\}$ は $\mathbb{R}$ の部分集合族です。また、$\sim$ を集合 X $(\neq \varnothing)$ 上の同値関係とするとき、商集合 $X/\sim$ は X の部分集合族です。

$\mathcal{S}$ を X の部分集合族とするとき、和集合 $\bigcup_{A\in\mathcal{S}} A$ が

$$\bigcup_{A\in\mathcal{S}} A = \{\, x\in X \mid \exists A\in\mathcal{S} \ \text{ s.t. } \ x\in A \,\}$$

によって定義されたことを思い出しておきましょう。

●類別

$\sim$ を空でない集合 X 上の同値関係とすると、同値関係の定義と定理 27-5 により、

❶ $\forall x\in X,\ \exists C\in X/\!\sim \ \text{ s.t. } \ x\in C.$
❷ $C,C'\in X/\!\sim,\ C\neq C' \ \Rightarrow \ C\cap C'=\varnothing.$
❸ $\forall C\in X/\!\sim,\ C\neq\varnothing.$

が成り立ちます。このことから、X は、互いに交わらない空でない部分集合たちの和集合として次のように表わされることがわかります：

$$X=\bigcup_{C\in X/\sim} C.$$

X をこのような和集合に分割することを、X を**類別**するといいます。

例 27-7 m を 2 以上の自然数とするとき、次が成り立つ：
(1) $\mathbb{Z}=[0]_m\cup[1]_m\cup\cdots\cup[m-1]_m$.
(2) $i,j\in\mathbb{Z},\ 0\le i<m,\ 0\le j<m,\ i\neq j$ に対して、$[i]_m\cap[j]_m=\varnothing$.
(**proof**)
(1) $\mathbb{Z}/m\mathbb{Z}$ は、$\mathbb{Z}$ 上の m を法とする合同関係 $\equiv \pmod m$ による商集合であり、例 27-6 により、

$$\mathbb{Z}/m\mathbb{Z}=\{[0]_m,[1]_m,\cdots,[m-1]_m\}$$

である。したがって、

$$\mathbb{Z} \ = \bigcup_{C\in\mathbb{Z}/m\mathbb{Z}} C = [0]_m\cup[1]_m\cup\cdots\cup[m-1]_m$$

となる。
(2) $i,j\in\mathbb{Z}$ が $[i]_m\cap[j]_m\neq\varnothing$ を満たしているとする。定理 27-5 より、$i\equiv j \pmod m$ となる。この合同式は、$0\le i<m,\ 0\le j<m$ の場合には、$i=j$ と同値である。 □

§27-2 整数の合同に関する剰余集合の構造

2 以上の自然数 m と $a\in\mathbb{Z}$ に対して、$\mathbb{Z}$ の部分集合

$$[a]_m=\{\, x\in\mathbb{Z}\mid x\equiv a \pmod m \,\}$$

を m による a の**剰余類** (residue class) といいます (例 27-6)。ここでは、剰余集合 $\mathbb{Z}/m\mathbb{Z}=\{[a]_m\mid a\in\mathbb{Z}\}$ に、和と積を定義し、その性質を調べます。

●整数の剰余集合における和と積

任意の $C,D\in\mathbb{Z}/m\mathbb{Z}$ に対して、$C=[a]_m,\ D=[b]_m$ となる代表元 $a,b\in\mathbb{Z}$ をとり、

$$C+D:=[a+b]_m, \qquad CD:=[ab]_m$$

によって定めます。$C+D$ と CD はどちらも C, D の代表元の選び方によらずに定まっています。実際、$C=[a']_m,\ D=[b']_m$ でもあったとすると、定理 27-5 により $a \equiv a' \pmod m$, $b \equiv b' \pmod m$ となります。ここで、補題 26-8 を使うと、

$$a+b \equiv a'+b' \pmod m, \qquad ab \equiv a'b' \pmod m$$

であることがわかるので、再び定理 27-5 により、$[a+b]_m=[a'+b']_m,\ [ab]_m=[a'b']_m$ が得られます。こうして、任意の $C, D \in \mathbb{Z}/m\mathbb{Z}$ に対して、$C+D \in \mathbb{Z}/m\mathbb{Z}$ と $CD \in \mathbb{Z}/m\mathbb{Z}$ が、**矛盾なく定義されている** (well-defined) ことがわかりました。$C+D,\ CD$ をそれぞれ C と D の**和、積**といいます。

例 27-8 $[0]_2+[0]_2=[1]_2+[1]_2=[0]_2$,
$[0]_2+[1]_2=[1]_2+[0]_2=[1]_2$,
$[0]_2[0]_2=[0]_2[1]_2=[1]_2[0]_2=[0]_2$,
$[1]_2[1]_2=[1]_2$
であるから、$\bar{0}=[0]_2,\ \bar{1}=[1]_2$ とおき、和の表と積の表を作ると次のようになる。

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

但し、左の表は、$\bar{a}, \bar{b}$ をそれぞれ各表の縦、横に並ぶ $\mathbb{Z}/2\mathbb{Z}$ の元とするとき、縦と横の交わる部分に $\bar{a}+\bar{b},\ \bar{a}\,\bar{b}$ を書き入れて作られている。

演習 27-4 $\bar{0}=[0]_4,\ \bar{1}=[1]_4,\ \bar{2}=[2]_4,\ \bar{3}=[3]_4$ とおき、$\mathbb{Z}/4\mathbb{Z}$ における和と積の表を作成せよ。

● $\mathbb{Z}/m\mathbb{Z}$ の和と積の性質

$\mathbb{Z}/m\mathbb{Z}$ の和 (加法)、積 (乗法) は $\mathbb{Z}$ の和、積と同様の性質を持っています。

(a) 加法について次が成り立つ。任意の $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/m\mathbb{Z}$ に対して、
- (i) **0 の存在**：$\bar{0} := [0]_m$ と定めると、$\bar{a}+\bar{0}=\bar{a}=\bar{0}+\bar{a}$.
- (ii) **結合法則**：$(\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c})$.
- (iii) **交換法則**：$\bar{a}+\bar{b}=\bar{b}+\bar{a}$.
- (iv) **マイナスの存在**：$\bar{a}$ の代表元を $a \in \mathbb{Z}$ として、$-\bar{a}=[-a]_m \in \mathbb{Z}/m\mathbb{Z}$ と定めると、$\bar{a}+(-\bar{a})=(-\bar{a})+\bar{a}=\bar{0}$.

(b) 乗法について次が成り立つ。任意の $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/m\mathbb{Z}$ に対して、
- (i) **1 の存在**：$\bar{1}=[1]_m$ と定めると、$\bar{1} \neq \bar{0}$ であって、$\bar{1}\cdot\bar{a}=\bar{a}=\bar{a}\cdot\bar{1}$.
- (ii) **結合法則**：$(\bar{a}\bar{b})\bar{c}=\bar{a}(\bar{b}\bar{c})$.
- (iii) **交換法則**：$\bar{a}\bar{b}=\bar{b}\bar{a}$.

(c) 加法と乗法の間に**分配法則**が成り立つ：任意の $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/m\mathbb{Z}$ に対して、

$$\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c},\ (\bar{a}+\bar{b})\bar{c}=\bar{a}\bar{c}+\bar{b}\bar{c}.$$

注意：1. (a-iv) において、$\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ のマイナス元 $-\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ を、$\bar{a}$ の代表元 a を 1 つとって、$-\bar{a}=[-a]_m$ として定めました。この $-\bar{a}$ は、補題 26-11 により、$\bar{a}$ の代表元 a の選び方に関係なく定まっています。

2. $\mathbb{Z}$ における積は、**簡約法則**「$c \neq 0,\ ac=bc \ \Rightarrow\ a=b$」を満たしていますが、$\mathbb{Z}/m\mathbb{Z}$ における積はこれを満たすとは限りません。例えば、$\mathbb{Z}/4\mathbb{Z}$ においては、$[2]_4 \neq \bar{0}$ ですが、

$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4 = [0]_4 \cdot [2]_4$ であり、簡約法則が成り立ちません (演習 27-4)。実は、$\mathbb{Z}/m\mathbb{Z}$ における積が簡約法則を満たすような m は素数に限ります (命題 27-9)。

● $\mathbb{Z}/m\mathbb{Z}$ の可逆元

$\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ に対して、$\bar{a}\bar{x} = \bar{1}$ となる $\bar{x} \in \mathbb{Z}/m\mathbb{Z}$ が存在するとき、$\bar{a}$ は ($\mathbb{Z}/m\mathbb{Z}$ の乗法に関する) **可逆元** (invertible element)、あるいは、**単元** (unit) であるといいます。また、この $\bar{x}$ を $\bar{a}$ の (乗法に関する) **逆元** (inverse element) といいます。

$\mathbb{Z}/m\mathbb{Z}$ のどのような元が可逆元になるのかは、次の命題のようにして、簡単に知ることができます。

命題 27-9

m を 2 以上の整数とする。$\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ とし、$a \in \mathbb{Z}$ をその代表元（すなわち、$\bar{a} = [a]_m$）とするとき、次が成り立つ：

$$\bar{a}\bar{x} = \bar{1} \text{ となる } \bar{x} \in \mathbb{Z}/m\mathbb{Z} \text{ が存在する} \iff \gcd(a, m) = 1.$$

(**proof**)

系 26-15 により、

$$\gcd(a, m) = 1 \iff ax \equiv 1 \pmod{m} \text{ となる } x \in \mathbb{Z} \text{ が存在する}$$

が成り立つ。$ax \equiv 1 \pmod{m}$ となる $x \in \mathbb{Z}$ が存在することと $[a]_m[x]_m = \bar{1}$ となる $x \in \mathbb{Z}$ が存在することとは同値であるから、命題の主張が成立する。 □

上の命題から、p が素数のとき、$\bar{0}$ でない任意の $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ に逆元が存在することがわかります。

演習 27-5 * $\mathbb{Z}/10\mathbb{Z}$ における可逆元をすべて求めよ。また、各可逆元の逆元を求めよ。

§27-3 有理数の構成

同値類の概念を使って、整数から有理数を厳密に構成することができます。この節では、その構成方法について説明します。

●有理数の構成方法および和と積の定義

演習 27-1 において、$X := \mathbb{Z} \times (\mathbb{Z} - \{0\})$ 上の次のような同値関係 $\sim$ を考えました：

$$(a, x) \sim (b, y) \iff ay = bx.$$

この同値関係 $\sim$ に関する $(a, x) \in X$ の同値類を $[a, x]$ と書き、商集合 $X/\sim = \{\, [a, x] \mid (a, x) \in X \,\}$ を $Q(\mathbb{Z})$ と書くことにします。

$Q(\mathbb{Z})$ の 2 元 $[a, x],\ [b, y]$ に対して、$[a, x] + [b, y]$ と $[a, x] \cdot [b, y]$ を次のように定めます。

(※) $$[a, x] + [b, y] = [ay + bx, xy], \qquad [a, x] \cdot [b, y] = [ab, xy].$$

演習 27-6 $[a, x],\ [b, y] \in Q(\mathbb{Z})$ に対して、$[a, x] + [b, y]$ と $[a, x] \cdot [b, y]$ は、代表元の選び方によらずに、矛盾なく定義されていることを示せ。

上で定められた $Q(\mathbb{Z})$ における和 $[a,x]+[b,y]$ と積 $[a,x]\cdot[b,y]$ は次の性質を持つことが簡単に確かめられます。ここで注目すべきことは、$Q(\mathbb{Z})$ の 0 でない任意の元は (積に関して) 逆元を持つ、ということです (下の (b-iv) 参照)。

$Q(\mathbb{Z})$ の和と積の性質

(a) 加法について次が成り立つ。任意の $r,s,t\in Q(\mathbb{Z})$ に対して、
  (i) **0の存在**：$\mathbf{0}:=[0,1]$ と定めると、$r+\mathbf{0}=r=\mathbf{0}+r$.
  (ii) **結合法則**：$(r+s)+t=r+(s+t)$.
  (iii) **交換法則**：$r+s=s+r$.
  (iv) **マイナスの存在**：$r=[a,x]$ $(a,x\in\mathbb{Z},\ x\neq 0)$ に対して、$-r=[-a,x]\in Q(\mathbb{Z})$ と定めると、$r+(-r)=(-r)+r=\mathbf{0}$.

(b) 乗法について次が成り立つ。任意の $r,s,t\in Q(\mathbb{Z})$ に対して、
  (i) **1の存在**：$\mathbf{1}=[1,1]$ と定めると、$\mathbf{1}\neq\mathbf{0}$ であって、$\mathbf{1}\cdot r=r=r\cdot\mathbf{1}$.
  (ii) **結合法則**：$(rs)t=r(st)$.
  (iii) **交換法則**：$rs=sr$.
  (iv) **逆元の存在**：$r=[a,x]\in Q(\mathbb{Z})$ が $\mathbf{0}$ でなければ、$r^{-1}=[x,a]\in Q(\mathbb{Z})$ を考えることができ ($\because [a,x]\neq\mathbf{0}$ より $a\neq 0$ なので $[x,a]\in Q(\mathbb{Z})$ を考えることができる)、
  $$rr^{-1}=\mathbf{1}=r^{-1}r.$$

(c) 加法と乗法の間に**分配法則**が成り立つ：任意の $r,s,t\in Q(\mathbb{Z})$ に対して、
  $$r(s+t)=rs+rt,\quad (r+s)t=rt+st.$$

さて、$[a,x]\in Q(\mathbb{Z})$ を $\frac{a}{x}$ という「分数」の形で改めて書き表わし、等式 (※) を書き直すと、

$$\frac{a}{x}+\frac{b}{y}=\frac{ay+bx}{xy},\qquad \frac{a}{x}\cdot\frac{b}{y}=\frac{ab}{xy}$$

となります。これは今まで使ってきた有理数に対する和、積と同じ式です。ここに、分数の意味が明確となり、さらに、有理数に対する和と積は商集合 $Q(\mathbb{Z})$ 上の矛盾なく定義された演算として定式化されることがわかりました。

●有理数の大小関係

有理数の構成的な定義および和と積の定義は上で説明しました。有理数に対しては、和と積の他に大小関係を考えることができます。$\mathbb{Q}$ 上の大小関係に相当する $Q(\mathbb{Z})$ 上の関係はどのようにして定義されるのでしょうか。

$Q(\mathbb{Z})$ 上の関係 $\leq$ を

$Q(\mathbb{Z})\ni r=[a,x],s=[b,y]$ (但し、$x>0,\ y>0$) に対して、

(♯)
$$r\leq s\quad\overset{\text{def}}{\Longleftrightarrow}\quad ay\leq bx.$$

によって定義します。まず、この関係 $\leq$ は矛盾なく定義されていることを見ておきましょう。$r=[a',x'],\ s=[b',y']$ (但し、$x'>0,\ y'>0$) とも書けているとします。すると、

$$\begin{aligned}(a'y')xy &= (a'x)yy' = (ax')yy' \\ &= (ay)x'y' \leq (bx)x'y' \quad (\because\ x', y' > 0,\ ay \leq bx) \\ &= xx'(by') = xx'(b'y) \\ &= (b'x')xy\end{aligned}$$

となります。$x, y > 0$ なので、上の不等式から $a'y' \leq b'x'$ が従います。これで、$Q(\mathbb{Z})$ 上に関係 $\leq$ が、(♯) のようにして矛盾なく定義されることがわかりました。

$Q(\mathbb{Z})$ 上の、今定義された関係 $\leq$ は次の性質を持つことが確かめられます。

$Q(\mathbb{Z})$ 上の関係 $\leq$ の性質

任意の $r, s, t \in Q(\mathbb{Z})$ に対して、次が成り立つ。

- $r \leq s$ または $s \leq r$.
- **推移性**：$r \leq s,\ s \leq t \implies r \leq t$.
- 加法、乗法と $\leq$ との間に
  (i) $r \leq s \iff r + t \leq s + t$.
  (ii) $0 \leq t$ のとき、$r \leq s \iff rt \leq st$.

以上で、有理数同士の計算を行う際に使ってきたすべての規則や法則が、商集合 $Q(\mathbb{Z})$ を舞台として実現されることがわかりました。

●「$\mathbb{Z} \subset \mathbb{Q}$」の意味

私たちは「$\mathbb{Z} \subset \mathbb{Q}$」という事実を「知っていて」、有理数の計算の際にしばしば使ってきました。「整数は有理数の一部である」というこの事実は、有理数の構成的な定義からは「当たり前」のことではありません。そこで、「$\mathbb{Z} \subset \mathbb{Q}$」の正確な意味について説明しておきます。

各 $a \in \mathbb{Z}$ に対して $[a, 1] \in Q(\mathbb{Z})$ を対応させる写像

$$j : \mathbb{Z} \longrightarrow Q(\mathbb{Z})$$

を考えます。この写像は単射になっています。なぜならば、$a, b \in \mathbb{Z}$ に対して、$[a, 1] = [b, 1]$ であったとすると、$a = a \cdot 1 = b \cdot 1 = b$ となるからです。そこで、この単射 j を通して $\mathbb{Z} \subset Q(\mathbb{Z})$ とみなすことにします。すなわち、$a \in \mathbb{Z}$ を $[a, 1] \in Q(\mathbb{Z})$ と同一視して、

$$a = [a, 1]$$

と約束するのです。$a, b \in \mathbb{Z}$ に対して

- $[a, 1] + [b, 1] = [a + b, 1]$
- $[a, 1][b, 1] = [ab, 1]$
- $a \leq b \iff [a, 1] \leq [b, 1]$

が成立するので、$Q(\mathbb{Z})$ における和、積、大小関係を $\mathbb{Z}$ の上に制限して考えると、それらは $\mathbb{Z}$ にもともとあった和、積、大小関係と一致していることがわかります。このことは、$\mathbb{Z}$ が単に $Q(\mathbb{Z})$ の部分集合とみなされ得るだけでなく、和と積の演算、大小関係を込めて $\mathbb{Z} \subset Q(\mathbb{Z})$ であることを意味します。j によって $\mathbb{Z}$ における $0,\ 1$ が $Q(\mathbb{Z})$ における $\mathbf{0},\ \mathbf{1}$ にそれぞれ写されることにも注意しましょう。

§28. 体

体とは、加減乗除を（0 で割ることを除いて）“自由に”行えるような集合のことをいいます。体の典型的な例として、$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ があります。この節の前半では、体の定義、体の例、順序関係、順序体について説明します。後半では、基本列の概念を導入し、有理数列の基本列を使って、実数体 $\mathbb{R}$ を構成する方法（カントールの構成法）について紹介します。

§28-1 環（かん）と体（たい）

ここでは、環と体の定義と例、および、その基本的な性質について述べます。

●環と体の定義

集合 $R(\neq \varnothing)$ 上に、**和** (または**加法**) と呼ばれる二項演算 $+$ と、**積** (または**乗法**) と呼ばれる二項演算 $\cdot$ が定義されていて、以下の条件を満たすとき、R を**可換環** (commutative ring) といいます。

(a) (i) **零元の存在**：次の条件を満たす元 $0_R \in R$ が存在する：任意の $a \in R$ に対して、$a + 0_R = a = 0_R + a$.

(ii) **結合法則**：任意の $a, b, c \in R$ に対して、$(a + b) + c = a + (b + c)$.

(iii) **交換法則**：任意の $a, b \in R$ に対して、$a + b = b + a$.

(iv) **マイナスの存在**：任意の $a \in R$ に対して、次の条件を満たす元 $x \in R$ が存在する：$a + x = x + a = 0_R$.（但し、0_R は (a-i) と同じ R の元である。）

(b) (i) **単位元の存在**：次の条件を満たす元 $(0_R \neq)\ 1_R \in R$ が存在する：任意の $a \in R$ に対して、$a \cdot 1_R = a = 1_R \cdot a$.

(ii) **結合法則**：任意の $a, b, c \in R$ に対して、$(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii) **交換法則**：任意の $a, b \in R$ に対して、$a \cdot b = b \cdot a$.

(c) **分配法則**：任意の $a, b, c \in R$ に対して、

$$a \cdot (b + c) = a \cdot b + a \cdot c,\ (a + b) \cdot c = a \cdot c + b \cdot c.$$

上記の 8 つの条件に加えて、さらに、次の条件も満たすとき、R を**体** (field) といいます。

(b) (iv) **逆元の存在**：任意の $(0_R \neq)\ a \in R$ に対して、次の条件を満たす元 $x \in R$ が存在する：$a \cdot x = x \cdot a = 1_R$.（但し、$1_R$ は (b-i) と同じ R の元である。）

注意：1. 可換環とは、正確には、組 $(R, +, \cdot)$ のことを指します。

2.“R を可換環とする”という言い方をすることがあります。この場合には、集合 R 上に、上の条件を満たす和 $+$ と積 $\cdot$ が 1 組指定されていると考えます。

3. 積 $a \cdot b$ をしばしば ab で表わします。

4. 加法の結合法則から、n 個の元 $a_1, a_2, \cdots, a_n \in R$ に対して、R の元 $a_1 + a_2 + \cdots + a_n$ が括弧の付け方によらずに定まります (定理 10-3)。同様に、乗法の結合法則から、R の元 $a_1 \cdot a_2 \cdot \cdots \cdot a_n$ が括弧の付け方によらずに定まります。特に、$a_1 = \cdots = a_n = a$ のとき、$a_1 + a_2 + \cdots + a_n$ を na と書き、$a_1 a_2 \cdot \cdots \cdot a_n$ を a^n と書きます。

5. 二項演算 $+$ と $\cdot$ が、(b-iii)(b-iv) を除くすべての条件を満たすとき、単に、**環** (ring) といいます。体は可換環であり、可換環は環です。つまり、「体 $\Rightarrow$ 可換環 $\Rightarrow$ 環」が成り立ちます。

6. (a-i) の性質を持つ元 0_R を R の**零元** (zero element) といい、(b-i) の性質を持つ元 1_R を R の**単位元** (identity element) といいます。環 R において、零元、単位元はそれぞれ 1 つづつしかありません。

7. 誤解の恐れのないときには、R の零元 0_R、単位元 1_R を、それぞれ、$0, 1$ と書きます。

●環の例—整数環、多項式環、行列環—

環の典型例を挙げます。

例 28-1 整数全体からなる集合 $\mathbb{Z}$ は、いつも使っている和と積に関して可換環である。この可換環を (有理) **整数環** (integer ring) という。$2 \in \mathbb{Z}$ の逆元が ($\mathbb{Z}$ の中に) 存在しないので、整数環 $\mathbb{Z}$ は体ではない。一方、有理数全体からなる集合 $\mathbb{Q}$、実数全体からなる集合 $\mathbb{R}$、複素数全体からなる集合 $\mathbb{C}$ は、いつも使っている和と積に関して体である。これらの体を、順番に、**有理数体** (rational number field)、**実数体** (real number field)、**複素数体** (complex number field) という。

演習 28-1 * 実数体 $\mathbb{R}$ の部分集合

$$\mathbb{Q}(\sqrt{2}\,) = \{\ a + b\sqrt{2} \mid a, b \in \mathbb{Q}\ \}$$

に対して和と積を定義し、それらに関して $\mathbb{Q}(\sqrt{2}\,)$ が体になることを確かめよ。

例 28-2 R を可換環（例えば、$R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$）とするとき、$R$ 係数の 1 変数多項式全体からなる集合

$$R[X] = \{\ a_0 + a_1X + a_2X^2 + \cdots + a_dX^d \mid a_0, a_1, a_2, \cdots, a_d \in R,\ d \in \mathbb{Z},\ d \geq 0\ \}$$

は、多項式の（いつもの）和と積に関して、可換環になる。この環を R 係数の 1 変数**多項式環** (polynomial ring) という。X の逆元が $R[X]$ の中に存在しないので、$R[X]$ は体ではない。より一般に、R 係数の n 変数多項式全体からなる集合 $R[X_1, \cdots, X_n]$ も、（いつもの）和と積に関して、可換環になる。この環を R 係数の n 変数多項式環という。

例 28-3 R を可換環とし、R の元を成分とする n 次正方行列の全体 $\mathrm{M}_n(R)$ を考える。$\mathrm{M}_n(R)$ は、$A = (a_{ij}),\ B = (b_{ij}) \in \mathrm{M}_n(R)$ について、和 $A + B$ と積 AB を

$$A + B = (a_{ij} + b_{ij}), \quad AB = (\sum_{k=1}^{n} a_{ik}b_{kj})$$

と定めると環になる。この環を R 係数の n 次**行列環** (matrix ring) という。$n > 1$ のとき、$\mathrm{M}_n(R)$ は可換環ではない。

●有限体

前節において、m を 2 以上の自然数として、剰余集合 $\mathbb{Z}/m\mathbb{Z} = \{\ [a]_m \mid a \in \mathbb{Z}\ \} = \{[0]_m, [1]_m, \cdots, [m-1]_m\}$ 上に和と積を導入して、その性質について考察しました。ここで、$a \in \mathbb{Z}$ に対して、

$$[a]_m = \{\ x \in \mathbb{Z} \mid x \equiv a \pmod{m}\ \}$$

であり、和と積はそれぞれ次のように定義されました：

$$[a]_m + [b]_m = [a+b]_m, \qquad [a]_m \cdot [b]_m := [ab]_m.$$

前節で観察したように、これらの和と積に関して、剰余集合 $\mathbb{Z}/m\mathbb{Z}$ は可換環になります。この環を m を法とする**剰余類環** (residue class ring) といいます。命題 27-9 により、環 $\mathbb{Z}/m\mathbb{Z}$ が体であるための必要十分条件は、m が素数であることです。素数 p に対して、体 $\mathbb{Z}/p\mathbb{Z}$ を p を法とする**剰余類体** (residue class field)、あるいは、位数 p の**有限体** (finite field) といいます。

●差 (減法) と商 (除法) の定義

環 R における減法と除法はそれぞれ加法と乗法の逆演算として定義されます。

補題 28-4

R を環とし、$a \in R$ とする。このとき、
(1) $a + x = x + a = 0$ を満たす $x \in R$ が一意的に存在する。この x を $-a$ で表わす。
(2) $a \cdot x = x \cdot a = 1$ を満たす $x \in R$ は一意的である。このような x が存在するとき、この x を a^{-1} で表わす。

(**proof**)

(1) も (2) も同じように証明できるので、(1) のみ示す。

(1) の条件を満たす x の存在は、環の定義 (a-iv) で保証されているから、一意性を示せばよい。$y \in R$ も x と同じ条件を満たしているとする。このとき、

$$x = 0 + x = (y + a) + x = y + (a + x) = y + 0 = y$$

となる。よって、$a + x = x + a = 0$ を満たす $x \in R$ は一意的である。 □

演習 28-2 R を環とする。以下の等式が成り立つことを確認せよ。
(1) $a, b \in R$ に対して、

① $0a = 0 = a0$　　② $-(-a) = a$　　③ $(-a)b = -ab$　　④ $(-a)(-b) = ab$.

(2) $a, b \in R$ が逆元を持つとき、

① $(a^{-1})^{-1} = a$　　② $(ab)^{-1} = b^{-1}a^{-1}$.

環 R の任意の 2 元 a, b に対して、

$$a - b := a + (-b)$$

と定義し、a から b を引いた**差**といいます。また、R が体のとき、$a \in R$ と $(0 \neq)\ b \in R$ に対して、

$$\frac{a}{b} := ab^{-1}$$

と定義し、a を b で割った**商**といいます。

§28-2 順序関係と体

順序関係は、実数に対する不等号や集合の間の含む・含まれるという関係が持つ性質を抽象化して得られる概念です。

●順序関係

空でない集合 X 上の関係 O が次の 3 つの条件を満たすとき、O は**順序関係** (order relation) である、または、**順序** (order) であるといいます。

(i) (**反射律**) 任意の $x \in X$ に対して、xOx である。
(ii) (**反対称律**) 任意の $x, y \in X$ に対して、「「xOy かつ yOx」ならば $x = y$」である。
(iii) (**推移律**) 任意の $x, y, z \in X$ に対して、「「xOy かつ yOz」ならば xOz」である。

上では順序関係を、記号 O を使って表わしましたが、これより以後は慣例に従い、記号 $\leq$ を主に使います。$a, b \in X$ に対して、$b \leq a$ のことを $a \geq b$ とも書きます。また、$b \leq a$ かつ $b \neq a$ であることを $b < a$ または $a > b$ で表わします。

例 28-5 (1) $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ において、いつも使っている不等号 $\leq$ を考えると、これは X の順序である。この順序を X 上の大小関係という。
(2) S を集合として、$\mathcal{P}(S) = \{\ S$ の部分集合全体 $\}$ を考える。$\mathcal{P}(S)$ 上の関係 $\leq$ を次のように定義する。$A, B \in \mathcal{P}(S)$ に対して、

$$A \leq B \iff A \subset B.$$

関係 $\leq$ は $\mathcal{P}(S)$ 上の順序である。この順序を**包含関係**による順序という。

演習 28-3 * $X = \mathbb{R} \times \mathbb{R}$ 上の関係 $\preceq$ を、$(a_1, a_2), (b_1, b_2) \in X$ に対して、

$$(a_1, a_2) \preceq (b_1, b_2) \iff 「a_1 < b_1」 \text{ または } 「a_1 = b_1 \text{ かつ } a_2 \leq b_2」$$

と定義する。但し、$\leq$ は $\mathbb{R}$ の大小関係である。$\preceq$ は X 上の順序であることを示せ。

●全順序

集合 X $(\neq \varnothing)$ 上の順序 $\leq$ が、条件

「任意の $x, y \in X$ に対して、$x \leq y$ または $y \leq x$ である」

を満たすとき、X 上の**全順序** (total order) であるといいます。

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ 上の大小関係や演習 28-3 の $\mathbb{R} \times \mathbb{R}$ 上の順序 $\preceq$ は全順序ですが、例 28-5(2) の $\mathcal{P}(S)$ 上の順序 $\subset$ は、S の元の個数が 2 個以上のとき、全順序ではありません。

●順序集合

順序が指定された集合のことを**順序集合** (ordered set) といいます。順序集合を、集合 X $(\neq \varnothing)$ とその上の順序 $\leq$ との組 $(X, \leq)$ によって表わします。$\leq$ が全順序のとき、順序集合 $(X, \leq)$ を**全順序集合** (totally ordered set) といいます。

順序集合の部分集合に対して、実数の場合と同様にして、最大元、最小元、上に有界、下に有界、上限、下限等の概念が定義されます。

●順序体

体 $K = (K, +, \cdot)$ 上に全順序 $\leq$ が与えられているとします。次の 2 条件が満たされるとき、組 $(K, +, \cdot, \leq)$ は**順序体** (ordered field) であるといいます。

(OF1) 任意の $x, y, z \in K$ に対して、「$x \leq y$ ならば $x + z \leq y + z$」である。
(OF2) 任意の $x, y, z \in K$ に対して、「「$x \leq y$ かつ $0 \leq z$」ならば $xz \leq yz$」である。

例えば、有理数体 $\mathbb{Q}$、実数体 $\mathbb{R}$ は通常の和と積、大小関係に関して順序体になります。一方、複素数体 $\mathbb{C}$ にいかなる全順序を導入しても順序体にはならないことが知られています。

実数体 $\mathbb{R}$ は、順序体 $(K,+,\cdot,\leq)$ であって、次の互いに同値な条件 (**連続性の公理**) のいずれかを満たすものとして“特徴づけられます”。

- (i) $a,b\in K,\ a,b>0$ に対して、$a<nb$ となる自然数 n が存在し、かつ、
  (ii) K における閉区間の任意の減少列 $I_1\supset I_2\supset\cdots$ に対して、$\bigcap_{n=1}^{\infty} I_n\neq\varnothing$.
- K の空でない上に有界な部分集合は上限を持つ。
- K の元からなる上に有界な単調増加数列は収束する。
- K の空でない 2 つの部分集合 A,B が $K=A\cup B$ かつ任意の $a\in A$ と任意の $b\in B$ に対して $a<b$ を満たすならば、A に最大元が存在するか、B に最小元が存在する。

§28-3 実数の完備性とその構成

ここでは、実数体の 1 つの特徴である、完備性について説明します。さらに、この条件を使って、実数体を有理数体から構成する方法を説明します。

●基本列

実数列 $\{a_n\}_{n=1}^{\infty}$ が**基本列** (fundamental sequence) である、または、**コーシー列** (Cauchy sequence) であるとは、

$$\forall\,\varepsilon>0,\ \exists\,N\in\mathbb{N}\ \text{ s.t. }\ n,m>N\ \Rightarrow\ |a_n-a_m|<\varepsilon$$

が成り立つときをいいます。基本列を考える利点は、数列の極限が何であるかを知らなくても、収束するかしないかを判断することができる点にあります (詳しくは次の命題を参照)。

命題 28-6 (実数の完備性)
実数列 $\{a_n\}_{n=1}^{\infty}$ について、

$$\{a_n\}_{n=1}^{\infty}\text{ はある実数に収束する}\quad\Longleftrightarrow\quad\{a_n\}_{n=1}^{\infty}\text{ は基本列である}$$

(**proof**)

収束する実数列が基本列であることはすぐにわかる (後の演習 28-4) ので、逆が成立することを示す。$\{a_n\}_{n=1}^{\infty}$ は基本列であるとする。$\{a_n\}_{n=1}^{\infty}$ は有界である。

$\because$)

$\{a_n\}_{n=1}^{\infty}$ は基本列なので、

$$n,m>N\ \Rightarrow\ |a_n-a_m|<1$$

を満たす $N\in\mathbb{N}$ が存在する。このとき、$n>N$ を満たすすべての $n\in\mathbb{N}$ に対して、$|a_n|<|a_{N+1}|+1$ となるから、

$$K:=\max\{|a_1|,|a_2|,\cdots,|a_N|,|a_{N+1}|+1\}$$

とおけば、すべての $n\in\mathbb{N}$ に対して $|a_n|<K$ が成り立つ。 □

各 $n\in\mathbb{N}$ に対して、$x_n,y_n\in\mathbb{R}$ を

$$x_n:=\inf\{\ a_k\mid k\in\mathbb{N},\ k\geq n\ \},\qquad y_n:=\sup\{\ a_k\mid k\in\mathbb{N},\ k\geq n\ \}$$

によって定義する。$x_n\leq y_n$ であり、$\{x_n\}_{n=1}^{\infty}$ は単調増加数列、$\{y_n\}_{n=1}^{\infty}$ は単調減少数列である。そこで、$I_n:=[x_n,y_n+\frac{1}{n}]$ とおき、閉区間の減少列 $I_1\supset I_2\supset\cdots$ に区間縮小法の原理を適用する。すると、実数 $\alpha\in\bigcap_{n=1}^{\infty} I_n$ の存在がわかる。

さて、任意に $\varepsilon > 0$ をとる。$\{a_n\}_{n=1}^{\infty}$ は基本列であるから、

$$\exists N \in \mathbb{N} \ \text{ s.t. } \ m, n > N \ \Rightarrow \ |a_m - a_n| < \frac{\varepsilon}{3}$$

が成り立つ。また、上限、下限の定義から、$n > N$ を満たす任意の $n \in \mathbb{N}$ に対して、

$$n < \ \exists m_1 \in \mathbb{N} \ \text{ s.t. } \ a_{m_1} < x_n + \frac{\varepsilon}{3},$$

$$n < \ \exists m_2 \in \mathbb{N} \ \text{ s.t. } \ a_{m_2} > y_n - \frac{\varepsilon}{3}$$

が成り立つ。したがって、$n > N$ を満たすすべての $n \in \mathbb{N}$ に対して、

$$y_n - x_n < (a_{m_2} + \frac{\varepsilon}{3}) + (-a_{m_1} + \frac{\varepsilon}{3}) \leq \frac{2\varepsilon}{3} + |a_{m_1} - a_{m_2}| < \varepsilon$$

が成り立つ。これとアルキメデスの公理から、

$$\lim_{n\to\infty} (y_n + \tfrac{1}{n} - x_n) = 0$$

がわかる。この事実と、任意の $n \in \mathbb{N}$ について $x_n \leq \alpha \leq y_n + \frac{1}{n}$ であることから、

$$I_M = [x_M, \ y_M + \tfrac{1}{M}] \subset (\alpha - \varepsilon, \alpha + \varepsilon)$$

を満たす $M \in \mathbb{N}$ の存在がわかる。したがって、$m > M$ を満たすすべての $m \in \mathbb{N}$ に対して、$a_m \in I_M \subset (\alpha - \varepsilon, \alpha + \varepsilon)$ となる。これは、$\{a_n\}_{n=1}^{\infty}$ が α に収束することを意味する。 □

演習 28-4 収束する実数列は基本列であることを示せ。

実は、アルキメデス性 (= 任意の $a, b > 0$ に対して $a < nb$ となる $n \in \mathbb{N}$ が存在する) と完備性 (= 基本列は収束する) の 2 つを合わせた条件は、連続性の公理と同値です。

●実数体の構成

$\mathbb{R}$ において $\mathbb{Q}$ は稠密であった、すなわち、任意の実数 α に対して、$\lim_{n\to\infty} a_n = \alpha$ となるような有理数列 $\{a_n\}_{n=1}^{\infty}$ が存在したことを思い出しましょう (定理 7-3)。この事実を逆手にとって、有理数列から実数体を構成することができます。

$\mathbb{Q}^+$ を正の有理数全体からなる集合とします。有理数列 $\{a_n\}_{n=1}^{\infty}$ であって、条件

$$\forall r \in \mathbb{Q}^+, \ \exists N \in \mathbb{N} \ \text{ s.t. } \ m, n > N \ \Rightarrow \ |a_m - a_n| < r$$

を満たすもの全体からなる集合 $\mathcal{C}$ を考えます。$\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty} \in \mathcal{C}$ に対して有理数列 $\{a_n + b_n\}_{n=1}^{\infty}, \{a_n b_n\}_{n=1}^{\infty}$ は再び $\mathcal{C}$ に属すことから、$\mathcal{C}$ は次のように定義される和 $+$ と積 $\cdot$

$$\{a_n\}_{n=1}^{\infty} + \{b_n\}_{n=1}^{\infty} := \{a_n + b_n\}_{n=1}^{\infty}, \qquad \{a_n\}_{n=1}^{\infty} \cdot \{b_n\}_{n=1}^{\infty} := \{a_n b_n\}_{n=1}^{\infty}$$

に関して可換環になることがわかります。$\mathcal{C}$ 上に関係 $\sim$ を

$$\{a_n\}_{n=1}^{\infty} \sim \{b_n\}_{n=1}^{\infty} \iff \forall r \in \mathbb{Q}^+, \ \exists N \in \mathbb{N} \ \text{ s.t. } \ n > N \ \Rightarrow \ |a_n - b_n| < r$$

によって定義します。関係 $\sim$ は $\mathcal{C}$ 上の同値関係であることがわかります。そして、$\mathcal{C}$ 上の和と積は商集合 $R := \mathcal{C}/\sim$ 上の和と積を誘導することがわかります。すなわち、2 元 $\alpha = [\{a_n\}_{n=1}^{\infty}], \ \beta = [\{b_n\}_{n=1}^{\infty}] \in R$ に対して、和 $+$ と積 $\cdot$ を

$$\alpha + \beta = [\{a_n + b_n\}_{n=1}^{\infty}], \qquad \alpha \cdot \beta = [\{a_n b_n\}_{n=1}^{\infty}]$$

によって定義することができます (演習 28-5)。

演習 28-5 * 上の $+$ と $\cdot$ の定め方で、R 上に二項演算が矛盾なく定義されることを確かめよ。

上で定義した R の和と積に関して R は可換環になります。R における零元 0_R は $0,0,0,\cdots\cdots$ という有理数列の同値類であり、単位元 1_R は $1,1,1,\cdots\cdots$ という有理数列の同値類です。また、$\alpha=[\{a_n\}_{n=1}^{\infty}]\in R$ に対するマイナス元 $-\alpha$ は、$-\alpha=[\{-a_n\}_{n=1}^{\infty}]$ によって与えられます。さらに、任意の $(0_R\neq)\ \alpha\in R$ に対して逆元が存在することがわかるので、可換環 R は体になります。実際、$\alpha=[\{a_n\}_{n=1}^{\infty}]$ と表わすと、$\alpha\neq 0_R$ より条件

$$\forall\, n\in\mathbb{N},\ \exists\,\tilde{n}>n\ \ \text{s.t.}\ \ |a_{\tilde{n}}|\geq r$$

を満たす $r\in\mathbb{Q}^+$ が存在し、$\{a_n\}_{n=1}^{\infty}\in\mathcal{C}$ より、$r/2\in\mathbb{Q}^+$ に対して条件

$$m,n>N_1\quad\Rightarrow\quad |a_m|-|a_n|\leq|a_m-a_n|<\tfrac{r}{2}$$

を満たす $N_1\in\mathbb{N}$ が存在します。この 2 つの事実から、$N:=\max\{N_1,\tilde{N_1}\}\in\mathbb{N}$ とおくと

$$n>N\ \Rightarrow\ |a_n|>\tfrac{r}{2}$$

が導かれるので、有理数列 $\{a_{n+N}^{-1}\}_{n=1}^{\infty}$ を考えることができ、この有理数列は $\mathcal{C}$ に属していることがわかります。$\alpha=[\{a_{n+N}\}_{n=1}^{\infty}]$ とも書けるので、$\{a_{n+N}^{-1}\}_{n=1}^{\infty}$ は α の逆元になっています。

次に、R 上の次のように定義される関係 $\leq$ を考えます。

$$[\{a_n\}_{n=1}^{\infty}]\leq[\{b_n\}_{n=1}^{\infty}]\quad\Longleftrightarrow\quad\begin{array}{l}\text{「}[\{a_n\}_{n=1}^{\infty}]=[\{b_n\}_{n=1}^{\infty}]\text{」または}\\ \text{「}\exists\, r\in\mathbb{Q}^+,\ \exists\, N\in\mathbb{N}\ \ \text{s.t.}\ \ n>N\ \Rightarrow\ r<b_n-a_n\text{」}.\end{array}$$

演習 28-6 R 上のこの関係 $\leq$ は矛盾なく定義されていて、R に全順序を定めることを示せ。

定理 28-7 (実数体の構成)
上のように定義される $(R,+,\cdot,\leq)$ は順序体になり、アルキメデスの公理と完備性を満たす。

(**proof**)

$(R,+,\cdot,\leq)$ が順序体の条件 (OF1)(OF2) を満たすことをみるのは易しいので、各自の演習問題として残す。ここでは、$(R,+,\cdot,\leq)$ がアルキメデスの公理と完備性を満たすことを示す。

• $(R,+,\cdot,\leq)$ がアルキメデスの公理を満たすこと：

$\alpha,\beta\in R$ を任意にとり、$\alpha=[\{a_n\}_{n=1}^{\infty}],\ \beta=[\{b_n\}_{n=1}^{\infty}]$ $(\{a_n\}_{n=1}^{\infty},\{b_n\}_{n=1}^{\infty}\in\mathcal{C})$ と書く。$\mathcal{C}$ の定義から、$1\in\mathbb{Q}^+$ に対して

$$\exists\, N_1\in\mathbb{N}\ \ \text{s.t.}\ \ n,m>N_1\ \Rightarrow\ |a_n-a_m|<1,$$
$$\exists\, N_2\in\mathbb{N}\ \ \text{s.t.}\ \ n,m>N_2\ \Rightarrow\ |b_n-b_m|<1$$

が成り立つ。そこで、$N:=\max\{N_1,N_2\}+1$ とおくと、

$$n>N\quad\Longrightarrow\quad -1-a_N<-a_n,\ -1+b_N<b_n$$

となることがわかる。$\mathbb{Q}$ はアルキメデスの公理を満たす (p.54) から、有理数 $-1-a_N,\ -1+b_N$ に対して $-1-a_N<n_0(-1+b_N)$ となる $n_0\in\mathbb{N}$ の存在がわかる。したがって、$n>N$ なる任意の $n\in\mathbb{N}$ に対して

$$n_0b_n-a_n>n_0(-1+b_N)-1-a_N>0$$

となる。これは $n_0\beta > \alpha$ を意味する。

• $(R, +, \cdot, \leq)$ が完備であること：

$\{\alpha_n\}_{n=1}^{\infty}$ を R の基本列とする。各 $n \in \mathbb{N}$ に対して $\alpha_n = [\{a_{nk}\}_{k=1}^{\infty}]$ となる $\{a_{nk}\}_{k=1}^{\infty} \in \mathcal{C}$ を 1 つずつとる。$\{a_{nk}\}_{k=1}^{\infty} \in \mathcal{C}$ より

$$\exists K \in \mathbb{N} \ \text{ s.t. } \ k, l > K \quad \Rightarrow \quad |a_{nk} - a_{nl}| < \tfrac{1}{n}$$

が成り立つ。そこで、

$$k(n) := \min\{\ K \in \mathbb{N} \mid k, l > K \quad \Rightarrow \quad |a_{nk} - a_{nl}| < \tfrac{1}{n}\ \} + 1$$

とおく。$\{a_{n,k(n)}\}_{n=1}^{\infty} \in \mathcal{C}$ であり、$\lim_{n\to\infty} \alpha_n = [\{a_{n,k(n)}\}_{n=1}^{\infty}]$ となることを示そう。

$r \in \mathbb{Q}^+$ を任意にとり、$\frac{r}{3}, \frac{r}{3}, \frac{r}{3}, \cdots\cdots$ という有理数列 $\boldsymbol{r}'$ を考える。$\boldsymbol{r}' \in \mathcal{C}$ なので $[\boldsymbol{r}'] \in R$ が定まり、$[\boldsymbol{r}'] > 0$ である。$\{\alpha_n\}_{n=1}^{\infty}$ は基本列なので、

$$\exists N \in \mathbb{N} \ \text{ s.t. } \ m, n > N \quad \Rightarrow \quad |\alpha_m - \alpha_n| < [\boldsymbol{r}']$$

が成り立つ。$\mathbb{Q}^+$ はアルキメデスの公理を満たすので、$\frac{1}{N_0} < \frac{r}{3}$ を満たす $N_0 \in \mathbb{N}$ が存在する。

さて、$m, n > \max\{N, N_0\}$ を満たす $m, n \in \mathbb{N}$ を任意にとる。$|\alpha_m - \alpha_n| < [\boldsymbol{r}']$ であるから、R における $\leq$ の定義により

$$\exists K_0 \in \mathbb{N} \ \text{ s.t. } \ k > K_0 \quad \Rightarrow \quad |a_{mk} - a_{nk}| < \tfrac{r}{3}$$

となることがわかる。このとき、$k = \max\{K_0 + 1, k(m), k(n)\} \in \mathbb{N}$ とすれば

$$\begin{aligned} |a_{m,k(m)} - a_{n,k(n)}| &\leq |a_{m,k(m)} - a_{mk}| + |a_{mk} - a_{nk}| + |a_{nk} - a_{n,k(n)}| \\ &< \tfrac{1}{m} + \tfrac{r}{3} + \tfrac{1}{n} < \tfrac{2}{N_0} + \tfrac{r}{3} < \tfrac{2r}{3} + \tfrac{r}{3} = r \end{aligned}$$

となる。したがって、$\{a_{n,k(n)}\}_{n=1}^{\infty} \in \mathcal{C}$ が示された。

次に、$\alpha := [\{a_{n,k(n)}\}_{n=1}^{\infty}]$ とおき、$\lim_{n\to\infty} \alpha_n = \alpha$ となることを示す。$\varepsilon > 0$ なる $\varepsilon \in R$ を任意にとる。$\varepsilon = [\{r_n\}_{n=1}^{\infty}]$ $(\{r_n\}_{n=1}^{\infty} \in \mathcal{C})$ と書くと、$\varepsilon > 0$ より

$$\exists r_\varepsilon \in \mathbb{Q}^+, \ \exists N_\varepsilon \in \mathbb{N} \ \text{ s.t. } \ n > N_\varepsilon \quad \Rightarrow \quad r_\varepsilon < r_n$$

となる。$r = r_\varepsilon$ の場合に先程のような $\boldsymbol{r}' \in \mathcal{C}$ や $N, N_0 \in \mathbb{N}$ を考える。$n > \max\{N, N_0\}$ を満たす $n \in \mathbb{N}$ を任意にとる。このとき、

$$(※) \qquad i > \max\{k(n), N_0, N_\varepsilon\} \quad \Rightarrow \quad |a_{ni} - a_{i,k(i)}| < r_i$$

となる。実際、$i > \max\{k(n), N_0, N_\varepsilon\}$ を満たす任意の $i \in \mathbb{N}$ に対して、先程と同様の理由で、

$$\exists K_0 \in \mathbb{N} \ \text{ s.t. } \ k > K_0 \quad \Rightarrow \quad |a_{ik} - a_{nk}| < \tfrac{r}{3}$$

となることがわかる。このとき、$l = \max\{K_0 + 1, k(i), k(n)\} \in \mathbb{N}$ とすれば、

$$|a_{ni} - a_{i,k(i)}| \leq |a_{ni} - a_{nl}| + |a_{nl} - a_{il}| + |a_{il} - a_{i,k(i)}| < \tfrac{1}{n} + \tfrac{r}{3} + \tfrac{1}{i} < \tfrac{2}{N_0} + \tfrac{r}{3} < \tfrac{2r}{3} + \tfrac{r}{3} = r$$

となる。$r = r_\varepsilon < r_i$ $(\because\ i > N_\varepsilon)$ なので、(※) が証明された。

(※) は $|\alpha_n - \alpha| < \varepsilon$ と同値であるから、$\lim_{n\to\infty} \alpha_n = \alpha$ が示された。 □

最後に、有理数 q を、$q, q, q, \cdots\cdots$ という有理数列 $\boldsymbol{q} \in \mathcal{C}$ の同値類と同一視することにより、(順序体として) $\mathbb{Q} \subset R$ とみなすことできることを注意しておきます。

§29. 抽象ベクトル空間

ここでは、第 13 節において導入された数ベクトル空間に関する概念の一般化を扱います。数ベクトル空間と (抽象) ベクトル空間との大きな違いは、数ベクトル空間には「標準的な座標」が先天的に与えられているのに対して、(抽象) ベクトル空間にはそれがない（つまり、始めに座標が与えられていない）という点です。ここでの目標は、多くの例に接しながら、(抽象) ベクトル空間の概念の重要性を実感することです。

●ベクトル空間の定義

K を体とします。集合 $V(\neq \varnothing)$ に対して、**和** (または**加法**) と呼ばれる二項演算 $+ : V \times V \longrightarrow V, (u, v) \longmapsto u+v$ と、**スカラー倍** (または**作用**) と呼ばれる写像 $\cdot : K \times V \longrightarrow V, (t, v) \longmapsto t \cdot v$ が定義されていて、以下の条件を満たすとき、V を K 上の**ベクトル空間** (vector space) または**線形空間** (linear space) といいます。

(a) (i) 次の条件を満たす元 $0_V \in V$ が存在する：
　　任意の $v \in V$ に対して、$v + 0_V = v = 0_V + v$.
　(ii) 任意の $u, v, w \in V$ に対して $(u + v) + w = u + (v + w)$.
　(iii) 任意の $u, v \in V$ に対して $u + v = v + u$.
　(iv) 任意の $v \in V$ に対して次の条件を満たす元 $x \in V$ が存在する：
　　$v + x = x + v = 0_V$（但し、0_V は (a-i) と同じ V の元）.

(b) (i) 任意の $v \in V$ に対して $1 \cdot v = v$（但し、1 は K の単位元）.
　(ii) 任意の $s, t \in K$ と任意の $v \in V$ に対して $(st) \cdot v = s \cdot (t \cdot v)$.
　(iii) 任意の $s, t \in K$ と任意の $v \in V$ に対して $(s + t) \cdot v = s \cdot v + t \cdot v$.
　(iv) 任意の $t \in K$ と任意の $u, v \in V$ に対して $t \cdot (u + v) = t \cdot u + t \cdot v$.

注意：1. 体 K 上のベクトル空間とは、正確には、組 $(V, +, \cdot)$ のことを指します。V の元のことをベクトル空間 $(V, +, \cdot)$ の**ベクトル**、または、**点**といいます。
2. “V を体 K 上のベクトル空間とする”という言い方をすることがあります。この場合には、集合 V 上に、上の条件を満たす和 $+$ とスカラー倍 $\cdot$ が 1 組指定されていると考えます。
3. スカラー倍 $t \cdot v$ $(t \in K,\ v \in V)$ を tv のようにも表わします。
4. (a-ii) から、n 個のベクトル $v_1, v_2, \cdots, v_n \in V$ に対して、和 $v_1 + v_2 + \cdots + v_n \in V$ が括弧の付け方によらずに定まります (定理 10-3)。特に、$v_1 = \cdots = v_n = v$ のとき、$v_1 + v_2 + \cdots + v_n$ を nv と書きます。
5. (a-i) の性質を持つ元 0_V は一意的です。これを V における**零ベクトル**といいます。誤解の恐れのないときには、零ベクトル 0_V を、単に、0 と書きます。
6. 補題 28-4(1) と全く同様に、(a-iv) を満たす $x \in V$ は一意的であることがわかります。この x を $-v$ と書きます。このとき、演習 28-2(1) と同様にして、$v \in V,\ t \in K$ に対して、

① $0_K \cdot v = 0_V$　　①′ $t \cdot 0_V = 0_V$　　② $-(-v) = v$　　③ $(-t)v = -tv$　　④ $(-t)(-v) = tv$

が成り立つことがわかります。特に、③と (b-i) から $(-1)v = -v$ が得られます。
7. $u, v \in V$ に対して、$u - v := u + (-v)$ と定義して、u から v を引いた**差**といいます。

●ベクトル空間の例

ベクトル空間の典型的な例を 5 つ列挙します。

例 29-1 体 K を n 個直積して得られる集合

$$K^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \;\middle|\; a_1 \in K, \cdots, a_n \in K \right\}$$

を考え、和とスカラー倍を次のように定義する：$\mathbf{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in K^n,\ t \in K$ に対して、

$$\mathbf{a} + \mathbf{b} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}, \qquad t\mathbf{a} = \begin{pmatrix} ta_1 \\ \vdots \\ ta_n \end{pmatrix}.$$

この和とスカラー倍に関して K^n は K 上のベクトル空間になる。

例 29-2 K を体とし、$m, n \in \mathbb{N}$ とする。K の元を成分とする (m,n)-行列全体からなる集合 $\mathrm{M}_{mn}(K)$ は、次のように定義される和とスカラー倍に関して、K 上のベクトル空間になる：$A = (a_{ij}),\ B = (b_{ij}) \in \mathrm{M}_{m,n}(K),\ t \in K$ に対して、

$$A + B = (a_{ij} + b_{ij}), \quad tA = (ta_{ij}).$$

例 29-3 K を体とする。K-係数の 1 変数多項式全体からなる集合

$$K[X] = \left\{ \sum_{i=0}^{d} a_i X^i \mid a_0, a_1, \cdots, a_d \in K,\ d \in \mathbb{Z},\ d \geq 0 \right\}$$

は、いつもの和とスカラー倍

$$\sum_{i=0}^{d} a_i X^i + \sum_{i=0}^{d'} b_i X^i = \sum_{i=0}^{\max\{d,d'\}} (a_i + b_i) X^i, \quad t \sum_{i=0}^{d} a_i X^i = \sum_{i=0}^{d} (ta_i) X^i \quad (t, a_i, b_i \in K)$$

に関して、K 上のベクトル空間になる。

例 29-4 K を体とし、K の元からなる列 $\{a_n\}_{n=1}^{\infty}$ 全体からなる集合 $\mathrm{Seq}(K)$ を考える。$\mathrm{Seq}(K)$ は、次のように定義される和とスカラー倍に関して、K 上のベクトル空間になる：$\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty} \in \mathrm{Seq}(K),\ t \in K$ に対して、

$$\{a_n\}_{n=1}^{\infty} + \{b_n\}_{n=1}^{\infty} = \{a_n + b_n\}_{n=1}^{\infty}, \quad t\{a_n\}_{n=1}^{\infty} = \{ta_n\}_{n=1}^{\infty}.$$

演習 29-1 * 例 29-1 から例 29-4 までの各ベクトル空間 V について、零ベクトルと $v \in V$ に対する $-v$ を書け。

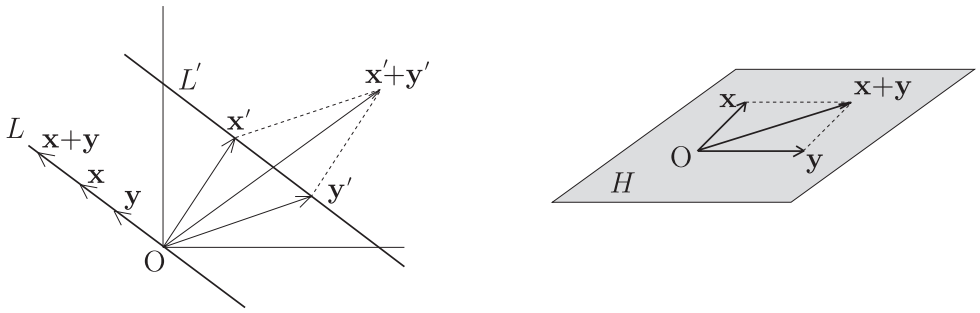
例 29-5 K を体とし、S を空でない集合とする。S から K への写像全体からなる集合を $\mathrm{Map}(S, K)$ と書くことにする。$\mathrm{Map}(S, K)$ は、次のように定義される和とスカラー倍に関して、K 上のベクトル空間になる：$f, g \in \mathrm{Map}(S, K),\ t \in K$ に対して、

$$(f + g)(s) = f(s) + g(s), \quad (tf)(s) = tf(s) \quad (s \in S).$$

演習 29-2 例 29-5 の主張を確かめよ。

●部分空間

体 K 上のベクトル空間 V が与えられているとし、V の部分集合 W を考えます。V には和 $+$ とスカラー倍 $\cdot$ が指定されているので、W の2元 w, w' に対して和 $w+w'$ を考えたり、W の元 w と K の元 t に対してスカラー倍 tw を考えたりすることができます。残念ながら、一般的には、これらは W の中に留まっていません (下図右の L' を参照)。しかし、もし、すべての $w, w' \in W$ に対して $w+w' \in W$ であり、すべての $w \in W$ とすべての $t \in K$ に対して $tw \in W$ であれば、W は V の中で「閉じた空間」を作っていることになります。このような性質を持つベクトル空間の部分集合のことを部分空間と呼びます。正確な定義は以下の通りです。



定義 29-6

$(V, +, \cdot)$ を体 K 上のベクトル空間とし、W を V の部分集合とする。W が $(V, +, \cdot)$ の**部分(ベクトル) 空間**であるとは、以下の3つの条件が成り立つときをいう。

(0) $0_V \in W$.

(i) 任意の $w, w' \in W$ に対して、$w+w' \in W$.

(ii) 任意の $w \in W$ と任意の $t \in K$ に対して、$tw \in W$.

注意： W がベクトル空間 $(V, +, \cdot)$ の部分空間のとき、V の和 $+ : V \times V \longrightarrow V$ とスカラー倍 $\cdot : K \times V \longrightarrow V$ を、それぞれ $W \times W$, $K \times W$ に制限して、

$$+_W : W \times W \longrightarrow W, \qquad (w, w') \longmapsto w + w'$$
$$\cdot_W : K \times W \longrightarrow W, \qquad (t, w) \longmapsto tw$$

という、2つの写像を考えることができます。このとき、組 $(W, +_W, \cdot_W)$ は K 上のベクトル空間になります。部分空間をベクトル空間として扱うときは、特別の断わり書きがない限り、この方法によります。

数ベクトル空間の部分空間の例は、例 20-4、例 21-2 などで、すでにいくつも見てきましたので、ここでは、それ以外の例を挙げておきます。

例 29-7 K を体として、n 次正方行列全体が作るベクトル空間 $\mathrm{M}_n(K)$ を考える (例 29-2 参照)。$A \in \mathrm{M}_n(K)$ に対して (i, j)-成分が A の (j, i)-成分であるような行列を ${}^tA$ と書く。$\mathrm{M}_n(K)$ の部分集合

$$\mathrm{Sym}_n(K) = \{\ A \in \mathrm{M}_n(K) \mid {}^tA = A\ \},$$
$$\mathrm{Alt}_n(K) = \{\ A \in \mathrm{M}_n(K) \mid {}^tA = -A\ \}$$

はどちらも $\mathrm{M}_n(K)$ の部分空間である ($\mathrm{Sym}_n(K)$, $\mathrm{Alt}_n(K)$ の元はそれぞれ**対称行列** (symmetric matrix)、**交代行列** (alternating matrix) と呼ばれる)。

例 29-8　$K=\mathbb{R}$ として、例 29-4 のベクトル空間 $\mathrm{Seq}(\mathbb{R})$ を考える。$\mathrm{Seq}(\mathbb{R})$ の部分集合

$$W=\{\ \{a_n\}_{n=1}^{\infty}\in \mathrm{Seq}(\mathbb{R})\mid \{a_n\}_{n=1}^{\infty}\text{ は収束する}\ \}$$

は $\mathrm{Seq}(\mathbb{R})$ の部分空間である (命題 8-6)。

例 29-9　$K=S=\mathbb{R}$ として、例 29-5 のベクトル空間 $\mathrm{Map}(\mathbb{R},\mathbb{R})$ を考える。 $\mathrm{Map}(\mathbb{R},\mathbb{R})$ の部分集合

$$W_1:=\{\ f\in \mathrm{Map}(\mathbb{R},\mathbb{R})\mid f\text{ は連続である}\ \},$$
$$W_2:=\{\ f\in \mathrm{Map}(\mathbb{R},\mathbb{R})\mid f\text{ は積分可能である}\ \},$$
$$W_3:=\{\ f\in \mathrm{Map}(\mathbb{R},\mathbb{R})\mid f\text{ は微分可能である}\ \}$$

は、どれも $\mathrm{Map}(\mathbb{R},\mathbb{R})$ の部分空間である (命題 14-4、補題 22-2(1)、補題 23-3)。

●線形結合と線形独立

V を体 K 上のベクトル空間とし、$v_1,\cdots,v_k\in V$ とします。ベクトル $v\in V$ が、

$$v=t_1v_1+\cdots+t_kv_k\qquad (t_1,\cdots,t_k\in K)$$

のように表わされるとき、v は $v_1,\cdots,v_k$ の K-**線形結合**であるといいます。

定義 29-10

V を体 K 上のベクトル空間とする。

(1) V に属する k 個のベクトル $v_1,\cdots,v_k$ が K 上**線形独立**である、あるいは、K 上**1 次独立**であるとは、次の条件が成り立つときをいう：

任意の $t_1,\cdots,t_k\in K$ について「$t_1v_1+\cdots+t_kv_k=0\ \Rightarrow\ t_1=\cdots=t_k=0$」.

このとき、V の部分集合 $\{v_1,\cdots,v_k\}$ を V の**線形独立系**と呼ぶ。

(2) V の部分集合 $\mathcal{L}$ が V の**線形独立系**であるとは、$\mathcal{L}$ のすべての有限部分集合が V の線形独立系であるときをいう。

例29-11　K を体とする。このとき、K-係数の 1 変数多項式全体のなすベクトル空間 $K[X]$ (例 29-3) において $\mathcal{L}=\{1,X,X^2,X^3,\cdots\cdots\}$ は K 上線形独立である。

(**proof**)

$\mathcal{L}$ の有限部分集合 $\mathcal{S}$ $(\neq\varnothing)$ を任意にとる。$\mathcal{S}$ が $K[X]$ の線形独立系であることを示せばよい。

$$\mathcal{S}=\{X^{i_1},\ X^{i_2},\ \cdots,\ X^{i_k}\}\qquad (0\le i_1<i_2<\cdots<i_k)$$

とおくことができる。$t_1,t_2,\cdots,t_k\in K$ として

$$t_1X^{i_1}+t_2X^{i_2}+\cdots+t_kX^{i_k}=0$$

とおく。このとき、多項式の相等の定義から、

$$t_1=t_2=\cdots=t_k=0$$

を得る。よって、$\mathcal{S}$ は $K[X]$ の線形独立系である。　□

演習 29-3 $\{\sin x, \sin 2x, \sin 3x, \cdots\cdots\}$ は、$\mathbb{R}$ 上のベクトル空間 $\mathrm{Map}(\mathbb{R},\mathbb{R})$ の線形独立系であることを示せ (ヒント：$\displaystyle\int_0^{2\pi} \sin mx \sin nx dx$ を計算する)。

●基底

体 K 上のベクトル空間 V の部分集合 $\mathcal{B}$ が、次の 2 条件を満たすとき、V の**基底**であると呼ばれます。

① $\mathcal{B}$ は V の線形独立系である。

② $\mathcal{B}$ は V を K 上**張る**。すなわち、任意の $v \in V$ に対して、$\mathcal{B}$ に属する有限個のベクトル $v_1, \cdots, v_n$ が存在して、v はそれらの K-線形結合である。

例29-12 K を体、n を自然数とし、例 29-1 のベクトル空間 K^n を考える。

K^n の n 個のベクトル

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

からなる集合は K^n の基底である。

例29-13 K を体とする。このとき、K の元を成分とする (m,n)-行列全体のなすベクトル空間 $\mathrm{M}_{mn}(K)$ (例 29-2) を考える。$1 \leq i \leq m,\ 1 \leq j \leq n$ を満たす自然数の組 (i,j) に対して、$E_{ij} \in \mathrm{M}_{mn}(K)$ を (i,j)-成分のみ 1 で、残りの成分はすべて 0 であるような行列とする。このとき、$\{\ E_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n\ \}$ は $\mathrm{M}_{mn}(K)$ の基底である。

例29-14 K を体とし、$\mathrm{M}_n(K)$ の部分空間 $\mathrm{Sym}_n(K),\ \mathrm{Alt}_n(K)$ を考える (例 29-7 を参照)。

$1 \leq i < j \leq n$ なる自然数 i, j に対して

$$S_{ij} := E_{ij} + E_{ji}, \qquad A_{ij} := E_{ij} - E_{ji}$$

とおく。但し、$1 \leq k, l \leq n$ を満たす自然数の組 (k,l) に対して、$E_{kl} \in \mathrm{M}_n(K)$ は (k,l)-成分のみ 1 で、残りの成分はすべて 0 であるような行列を表わす。このとき、

$$\{\ S_{ij} \mid 1 \leq i < j \leq n\ \} \cup \{\ E_{ii} \mid 1 \leq i \leq n\ \}, \qquad \{\ A_{ij} \mid 1 \leq i < j \leq n\ \}$$

はそれぞれ $\mathrm{Sym}_n(K),\ \mathrm{Alt}_n(K)$ の基底である。

例29-15 K を体とする。このとき、K-係数の 1 変数多項式全体のなすベクトル空間 $K[X]$ (例 29-3) において $\{1, X, X^2, X^3, \cdots\cdots\}$ は $K[X]$ の基底である。

例 29-4 や例 29-8、例 29-9 で挙げられているベクトル空間については簡単に基底を求めることはできませんが、存在することは証明されています。より一般に、零ベクトルだけからなるベクトル空間 $\{0\}$ を除く、すべてのベクトル空間には基底が存在することが知られています。

基底の定義から次の補題が直ちに証明されます。

補題 29-16

V を体 K 上のベクトル空間とする。$\{v_1, \cdots, v_n\}$ が V の基底であるとき、

$$F\left(\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}\right) = t_1 v_1 + \cdots + t_n v_n \qquad \left(\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in K^n\right)$$

によって定義される写像 $F : K^n \longrightarrow V$ は K-**線形同型写像**である。すなわち、F は全単射であって、かつ、次の２条件が成り立つ。

① 任意の $\mathbf{a}, \mathbf{b} \in K^n$ に対して、$F(\mathbf{a}+\mathbf{b}) = F(\mathbf{a}) + F(\mathbf{b})$ である。

② 任意の $\mathbf{a} \in K^n$ と任意の $t \in K$ に対して、$F(t\mathbf{a}) = tF(\mathbf{a})$ である。

注意：この補題は、n 個のベクトルからなる基底が存在するような K 上のベクトル空間 V を数ベクトル空間 K^n とみなすことができる、ということを主張しています。しかしながら、$V = K^n$ とみなすためには、V の基底を１つ指定する必要があるということに注意しましょう。F は V の基底の選び方に依存しているので、基底を取り替えると同一視 $V = K^n$ の仕方も変わります。

●次元

V を体 K 上のベクトル空間とします。有限個の元からなる基底が V の中に存在するとき、V は**有限次元** (finite dimensional) であるといい、そうでないとき、**無限次元** (infinite dimensional) であるといいます。有限次元ベクトル空間の典型例として、数ベクトル空間 K^n や例 29-2 のベクトル空間 $\mathrm{M}_{mn}(K)$ があり、無限次元ベクトル空間の典型例として、例 29-3、例 29-4 のベクトル空間 $K[X]$, $\mathrm{Seq}(K)$ があります。

定理 29-17

V を体 K 上の有限次元ベクトル空間とする。このとき、次が成り立つ。

(1) V の任意の線形独立系は有限集合である。

(2) $\mathcal{B}_1$ と $\mathcal{B}_2$ が V の基底のとき、$\mathcal{B}_1$ に属する元の個数と $\mathcal{B}_2$ に属する元の個数は等しい。

V の基底に属する元の個数を V の**次元**といい、$\dim_K V$ または単に $\dim V$ という記号で表わす。

(**proof**)

(1) V は有限次元なので、有限個の元からなる基底 $\mathcal{B}$ が存在する。$\mathcal{B}$ に属する元の個数を n とおけば、K-線形同型写像 $F : K^n \longrightarrow V$ が存在する (補題 29-16)。

さて、$\mathcal{L}$ を V の線形独立系とすると、$F^{-1}(\mathcal{L})$ は K^n の線形独立系となる (補題 21-5)。K^n の $(n+1)$ 個のベクトルは K 上線形独立でない (補題 20-10) から、$F^{-1}(\mathcal{L})$ は有限集合でなければならない。F は全単射なので、$\mathcal{L}$ も有限集合でなければならない。

(2) $\mathcal{B}_1$, $\mathcal{B}_2$ を V の２つの基底とすると、(1) により、$\mathcal{B}_1$, $\mathcal{B}_2$ は有限集合である。$\mathcal{B}_1$, $\mathcal{B}_2$ に属する元の個数をそれぞれ m, n とおけば、補題 29-16 により、K-線形同型写像 $F : K^m \longrightarrow V$, $G : K^n \longrightarrow V$ が存在する。このとき、合成 $G^{-1} \circ F : K^m \longrightarrow K^n$ も K-線形同型写像であるから、数ベクトル空間（の部分空間）に対する次元（定理 20-13）を比較して、

$$m = \dim K^m = \dim(G^{-1} \circ F)(K^m) = \dim K^n = n$$

を得る。 □

演習 29-4* 漸化式 $a_{n+3} + 2a_{n+2} - a_{n+1} + a_n = 0$ $(n = 1, 2, 3, \cdots)$ を満たす実数列 $\{a_n\}_{n=1}^{\infty}$ の全体からなる集合を W とおく。

(1) W は 例 29-4 のベクトル空間 $\mathrm{Seq}(\mathbb{R})$ の部分空間であることを示せ。

(2) W の一組の基底を求めよ。

(3) W の次元を求めよ。

●三角関数の加法公式

第 16 節では、幾何学的考察に基づいて、三角関数の加法公式を導きました (p.131)。ここでは、定理 25-10 に書かれている $\cos, \sin$ の性質と定理 29-17 を使って、加法公式を導きましょう。

命題 29-18

次の 2 条件を満たす関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ 全体からなる集合を W とおく：

(i) f は C^2-級である。すなわち、f は 2 回微分可能であって、その第 2 次導関数 $f'' := (f')'$ は連続である。

(ii) $f'' = -f$.

このとき、W は $\mathbb{R}$ 上のベクトル空間 $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ の 2 次元部分空間であり、$\{\cos, \sin\}$ はその 1 組の基底である。

(**proof**)

W が $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ の部分空間であることはすぐに確かめられる。$\{\cos, \sin\}$ が W の基底であることを示す。

• $\{\cos, \sin\}$ が $\mathbb{R}$ 上線形独立であること：

$$a \sin + b \cos = 0 \qquad (a, b \in \mathbb{R})$$

とおくと、任意の $x \in \mathbb{R}$ に対して

$$a \sin x + b \cos x = (a \sin + b \cos)(x) = 0(x) = 0$$

となる。この等式において、$x = 0$ の場合と $x = \frac{\pi}{2}$ の場合を考えて定理 25-10(2) を適用することにより、$b = 0,\ a = 0$ を得る。故に、$\sin,\ \cos$ は $\mathbb{R}$ 上線形独立である。

• $\{\cos, \sin\}$ が W を張ること：

まず、定理 25-10(4) から $\sin,\ \cos \in W$ である。

次に、任意の $f \in W$ が $\sin,\ \cos$ の $\mathbb{R}$-線形結合で表わされることを示す。$f(0) = a,\ f'(0) = b$ とおき、

$$g(x) = a \cos x + b \sin x - f(x) \qquad (x \in \mathbb{R})$$

によって定義される関数 $g : \mathbb{R} \longrightarrow \mathbb{R}$ を考える。$g \in W$ であって、$g(0) = g'(0) = 0$ を満たしていることがわかる。実は $g = 0$ となる。実際、$g'' = -g$ から、

$$(g^2 + g'^2)' = 2gg' + 2g'g'' = 2gg' - 2g'g = 0$$

となるので、平均値の定理 (定理 23-6) により、$g^2 + g'^2$ は定数関数である。したがって、任意の $x \in \mathbb{R}$ に対して

$$g(x)^2 + g'(x)^2 = (g^2 + g'^2)(x) = (g^2 + g'^2)(0) = g^2(0) + g'^2(0) = 0$$

となる。$g(x), g'(x) \in \mathbb{R}$ であるから、上式が成り立つためには、$g(x) = g'(x) = 0$ でなければならない。これで、$g = 0$ が証明され、$f = a \cos + b \sin$ と表わされることがわかった。

以上で、W は $\{\cos, \sin\}$ を基底に持つことが示された。 □

上の命題から $\sin,\ \cos$ の加法公式を導くことができます (例えば、$\sin$ の加法公式を導くには、$\varphi \in \mathbb{R}$ を固定し、$f(x) = \sin(x + \varphi)\ \ (x \in \mathbb{R})$ によって定義される関数 f を考えます)。

系 29-19 (三角関数の加法公式)
sin, cos は、任意の $\theta, \varphi \in \mathbb{R}$ に対して、次の等式を満足する。

$$\begin{cases} \sin(\theta+\varphi) = \sin\theta\cos\varphi + \cos\theta\sin\varphi \\ \cos(\theta+\varphi) = \cos\theta\cos\varphi - \sin\theta\sin\varphi \end{cases}$$

演習 29-5 上の系を証明せよ。

●幾何ベクトル

高校では、ベクトルを“矢印のついた線分 (= 有向線分)”で表わし、平行移動でぴったりと重なる有向線分を同じベクトルとして扱いました。そして、ベクトルに対して和をとったり、スカラー倍したりするときには、ベクトル (を表わす有向線分) の“始点”を都合よい位置に動かして計算することができました。このようなことが許される理由は何なのでしょうか。考えてみると不思議ですね。ここでは、このことを現代数学流に説明してみましょう。

K を体とし、n 次元数ベクトル空間 K^n を考えます。任意の $\mathbf{p}, \mathbf{q} \in K^n$ に対して、写像

$$\gamma_{\mathbf{p},\mathbf{q}} : [0,1] \longrightarrow K^n, \qquad \gamma_{\mathbf{p},\mathbf{q}}(t) = (1-t)\mathbf{p} + t\mathbf{q} \quad (t \in [0,1])$$

を $\mathbf{p}$ から $\mathbf{q}$ への**有向線分**といいます。

K^n の有向線分全体からなる集合を $\mathcal{L}$ とおきます：$\mathcal{L} = \{\gamma_{\mathbf{p},\mathbf{q}} \mid \mathbf{p}, \mathbf{q} \in K^n\}$.

$\gamma, \delta \in \mathcal{L},\ k \in K$ に対して、$\gamma+\delta : [0,1] \longrightarrow K^n,\ k\gamma : [0,1] \longrightarrow K^n$ をそれぞれ

$$(\gamma+\delta)(t) = \gamma(t) + \delta(t), \qquad (k\gamma)(t) = k\gamma(t) \qquad (t \in [0,1])$$

と定めると、$\gamma+\delta,\ k\gamma \in \mathcal{L}$ であることがわかり、さらに、$\mathcal{L}$ はこれらの和とスカラー倍に関して、K 上のベクトル空間になることがわかります。

この $\mathcal{L}$ は‘大きすぎる’ので、次のような同値関係 $\sim$ を導入して、商集合 $\mathcal{L}/\sim$ を考えます：$\gamma, \delta \in \mathcal{L}$ に対して

$$\gamma \sim \delta \iff^{\text{def}} \exists\, \mathbf{a} \in K^n \ \text{ s.t. } \forall\, t \in [0,1],\ \delta(t) = \gamma(t) + \mathbf{a}.$$

商集合 $\mathcal{L}/\sim$ を V_n とおくとき、次が成立します。

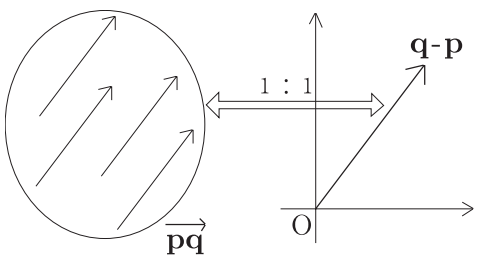
命題 29-20
(1) V_n には次のようにして和とスカラー倍が定義され、これらに関して、V_n は K 上のベクトル空間になる：$\gamma, \delta \in \mathcal{L},\ k \in K$ に対して、

$$[\gamma] + [\delta] = [\gamma+\delta], \qquad k[\gamma] = [k\gamma].$$

(2) $F(\mathbf{p}) = [\gamma_{\mathbf{0},\mathbf{p}}]$ $(\mathbf{p} \in K^n)$ によって定義される写像 $F : K^n \longrightarrow V_n$ は K-線形同型写像である。但し、$\mathbf{0}$ は K^n の零ベクトルを表わす。

演習 29-6 上の命題を証明せよ。

以上から、(高校で習う)“矢印”ベクトルとは、同値類 $\overrightarrow{\mathbf{pq}} := [\gamma_{\mathbf{p},\mathbf{q}}]$ のことであるとわかりました。そして、“矢印”ベクトルと位置ベクトルの関係が、上の命題の中の線形同型写像 F によって与えられることもわかりました。



§30. 濃度

数学では、集合の‘元の個数’を濃度と呼びます。集合には、その元の個数を数え上げることのできる有限集合と、それができない無限集合があります。無限集合にも、すべての元を番号付けられる可算（無限）集合とそれのできない非可算（無限）集合があります。ここでの目標は、$\mathbb{Q}$ が可算（無限）集合であり、$\mathbb{R}$ が非可算（無限）集合であることの証明方法を知ることです。

§30-1 有限集合と濃度

‘もの’の個数を数えるときに 1 個、2 個、3 個 $\cdots$ のように自然数を使います。ここでは、‘n 個’という概念について反省をしましょう。この節では、$n \in \mathbb{N}$ に対して、1 から n までの自然数全体からなる集合を $N(n)$ で表わすことにします：

$$N(n) := \{1, 2, \cdots, n\}.$$

任意の $a \in N(n)$ について $a \leq n$ であり、$n+1 \notin N(n)$ であることに注意しましょう。

●有限集合と無限集合

集合 A が**有限集合** (finite set) であるとは、

(i) A は空集合である、または、(ii) $n \in \mathbb{N}$ および全単射 $f : A \longrightarrow N(n)$ が存在する

のうちのいずれかが成り立つときをいいます(p.92 参照)。有限集合でない集合を**無限集合** (infinite set) といいます。定義により、空集合 $\varnothing$ や $\{a\}, \{a, b\}, \{a, b, c\}$ 等は有限集合です。

●有限集合の濃度

空でない有限集合 A に対して、その定義から、自然数 n と全単射 $f : A \longrightarrow N(n)$ が存在します。そこで、この n のことを‘A に属する元の個数’と定義したいのですが、1 つ問題があります。それは、このような n は A に対して唯一通りに定まるか？という問題です。すなわち、n とは別の自然数 m に対して、全単射 $g : A \longrightarrow N(m)$ が存在することはないのか？ということです。このようなことがない、ということを保証するためには、次の補題が必要です。

補題 30-1

n を自然数とし、A を $N(n)$ の空でない部分集合とする。このとき、全単射 $f : A \longrightarrow N(n)$ が存在するならば、$A = N(n)$ である。

(**proof**)

すべての自然数 n について

$P(n)$：全単射 $f : A \longrightarrow N(n)$ が存在するような $\varnothing \neq A \subset N(n)$ は $A = N(n)$ に限る

が成り立つことを数学的帰納法で証明する。

I. $P(1)$ が成立すること：

$N(1) = \{1\}$ の空でない部分集合は $N(1)$ のみであるから、命題 $P(1)$ は成立する。

II. $n \in \mathbb{N}$ について $P(n)$ が成り立っていると仮定する。A を $N(n+1)$ の空でない部分集合とし、全単射 $f : A \longrightarrow N(n+1)$ が存在すると仮定する。

$n+1 \in A$ である。

$\because$)

もし、$n+1 \notin A$ と仮定すると、$A \subset N(n)$ である。f は全射なので、$f(a) = n+1$ となる $a \in A$ が存在する。

写像 $g : A - \{a\} \longrightarrow N(n)$ を

$$g(x) = f(x) \qquad (x \in A - \{a\})$$

によって定める。g は全単射であり、$A - \{a\} \subset N(n)$ であるから、帰納法の仮定により、$A - \{a\} = N(n)$ が成り立つ。故に、$a \notin N(n)$ である。このことと $a \in A \subset N(n+1)$ を合わせて $a = n+1$ が得られるが、これは仮定 $n+1 \notin A$ に矛盾する。 □

上のように $f(a) = n+1$ となる $a \in A$ をとり、全単射 $g : A - \{a\} \longrightarrow N(n)$ を定める。また、写像 $h : A - \{n+1\} \longrightarrow A - \{a\}$ を次のように定める。

Case1：$a = n+1$ のとき、$h = \mathrm{id}_{A-\{n+1\}}$.

Case2：$a \neq n+1$ のとき、各 $x \in A - \{n+1\}$ に対して

$$h(x) = \begin{cases} n+1 & (x = a \text{ のとき}) \\ x & (x \neq a \text{ のとき}). \end{cases}$$

h は全単射なので、$g \circ h : A - \{n+1\} \longrightarrow N(n)$ も全単射である。$A - \{n+1\} \subset N(n)$ であるから、帰納法の仮定により、$A - \{n+1\} = N(n)$ を得る。これより、

$$A = (A - \{n+1\}) \cup \{n+1\} = N(n) \cup \{n+1\} = N(n+1)$$

が示され、帰納法の証明が完成した。 □

補題 30-1 から重要な２つの系が得られます。

系 30-2

$\mathbb{N}$ は無限集合である。

(**proof**)

$\mathbb{N}$ が有限集合であったと仮定すると、ある自然数 n と全単射 $f : \mathbb{N} \longrightarrow N(n)$ が存在する。$A := f(N(n+1))$ とおくと、f を $N(n+1)$ に制限することにより、全単射 $g : N(n+1) \longrightarrow A$ が得られる。その逆写像 $g^{-1} : A \longrightarrow N(n+1)$ も全単射であり、また、$A \subset N(n) \subset N(n+1)$ であるから、補題 30-1 により、$A = N(n+1)$ でなければならない。これは $N(n) = N(n+1)$ を導くので、矛盾が生じる。よって、$\mathbb{N}$ は有限集合ではない、すなわち、無限集合である。 □

系 30-3

集合 A に対して、２つの自然数 m, n と２つの全単射 $f : A \longrightarrow N(m),\ g : A \longrightarrow N(n)$ が存在したと仮定する。このとき、$m = n$ である。

(**proof**)

$\mathbb{N}$ における通常の大小関係 $\leq$ は全順序であるから、$m \leq n$ または $n \leq m$ のいずれかが成り立つ。一般性を失うことなく、$m \leq n$ であると仮定してよい。このとき、$N(m) \subset N(n)$ となる。また、仮定により、$g \circ f^{-1} : N(m) \longrightarrow N(n)$ は全単射である。したがって、補題 30-1 により、$N(m) = N(n)$ でなければならない。特に、$n \in N(n) = N(m)$ であり、その結果、$n \leq m$ を得る。これで、$m = n$ が示された。 □

系 30-3 により、次の定義が意味を持ちます。

定義 30-4
有限集合 A に対して、以下のように定義される 0 以上の整数 $\sharp A$ を A の**濃度** (power) または**基数** (cardinal number) または A に属する元の個数という。
$A = \varnothing$ のとき：$\sharp A = 0$ と定める。
$A \neq \varnothing$ のとき：有限集合の定義により、自然数 n と全単射 $f : A \longrightarrow N(n)$ が存在する。この n を $\sharp A$ と定める。

注意：$\sharp A$ の代わりに $|A|$ や $\mathrm{card}A$ という記号が使われることもあります。また、$\sharp A = n$ であるような有限集合を ‘ (ちょうど) n 個の元からなる集合 ’ ということがあります。

●有限集合の部分集合
有限集合の部分集合は有限集合になります。ここでは、この当たり前の事実を証明しましょう。その証明を記述するのに便利な言葉と記号を導入しておきます。

定義 30-5
集合 A の部分集合 B が A に等しくないとき、B は A の**真部分集合** (proper subset) であるといい、記号で $B \subsetneqq A$ あるいは $A \supsetneqq B$ と書き表わす。

注意：p.23 でも注意しましたが、集合 B が集合 A の部分集合であることを $B \subseteq A$ あるいは $A \supseteq B$ と記す本もあります（このプリントでは これを $B \subset A$ あるいは $A \supset B$ によって表わしています)。このような記法を採用する本では、$\subset$, $\supset$ は真部分集合の意味で用いられることが多いようです。他の本を参照するときに注意して下さい。

定理 30-6
A を有限集合とする。このとき、
(1) A の任意の部分集合 B は有限集合であり、$\sharp B \leq \sharp A$ である。
(2) $B \subset A$ かつ $\sharp B = \sharp A$ ならば $B = A$ である。

(**proof**)
すべての自然数 n に対して、

$$P(n)：N(n) \text{ の任意の真部分集合 } A \text{ は有限集合であり、} \sharp A < n$$

が成り立つことを数学的帰納法で証明すれば十分である。
I. $P(1)$ が成り立つこと：
$N(1) = \{1\}$ の真部分集合は $\varnothing$ のみである。これは有限集合であり、その濃度は $0\ (< 1)$ である。
II. $n \in \mathbb{N}$ とし、$P(n)$ が成り立っていると仮定する。$A \subsetneqq N(n+1)$ とする。
Case1 $n+1 \notin A$ の場合：
$A \subset N(n)$ となるので、帰納法の仮定により、A は有限集合であり、$\sharp A \leq n < n+1$ である。
Case2 $n+1 \in A$ の場合：
$A \neq N(n+1)$ より、$m \notin A$ となる $m \in N(n+1)$ が存在する。写像 $\sigma : N(n+1) \longrightarrow N(n+1)$ を m と $n+1$ の互換とする。このとき、$n+1 \notin \sigma(A) \subset N(n+1)$ となるから、Case1 により、

$\sigma(A)$ は有限集合であり、$\sharp\sigma(A) \leq n < n+1$ である。$\sigma|_A : A \longrightarrow \sigma(A)$ は全単射であるから、A もまた有限集合であり、$\sharp A = \sharp\sigma(A) < n+1$ がわかる。

これで、$P(n+1)$ も成立することがわかった。 □

演習 30-1 A, B が有限集合ならば、$A \cup B$ も有限集合であり、$\sharp(A \cup B) = \sharp A + \sharp B - \sharp(A \cap B)$ が成り立つことを示せ。

ヒント：① $A \cap B = \varnothing$ のとき $\sharp(A \cup B) = \sharp A + \sharp B$ となること、および、② $B \subset A$ のとき $\sharp(A - B) = \sharp A - \sharp B$ となることを示せばよい。

演習 30-1 の結果を応用して次の命題を証明することができます。

命題 30-7

A, B が有限集合ならば、直積集合 $A \times B$ も有限集合であって、$\sharp(A \times B) = \sharp A \times \sharp B$ である。

(**proof**)

$\sharp A = m$ とおき、$A = \{a_1, \cdots, a_m\}$ とおく。また、各 $i = 1, \cdots, m$ に対して、

$$X_i := \{a_1, a_2, \cdots, a_i\} \times B$$

とおく。すると、$X_m = A \times B$ であり、$i = 1, \cdots, m-1$ に対して

$$(\diamondsuit) \qquad X_{i+1} = X_i \cup (\{a_{i+1}\} \times B), \qquad X_i \cap (\{a_{i+1}\} \times B) = \varnothing$$

が成り立つ。

X_i $(i = 1, \cdots, m)$ は有限集合であり、$\sharp X_i = i \times \sharp B$ となることを数学的帰納法で証明する。

I. $X_1 = \{a_1\} \times B$ と B との間に全単射が存在するから、X_1 は有限集合であり、$\sharp X_1 = \sharp B$ が成り立つ。

Ⅱ. $1 \leq i \leq m-1$ とし、X_i は有限集合であり、$\sharp X_i = i \times \sharp B$ であるとする。このとき、$(\diamondsuit)$ と演習 30-1 により、X_{i+1} は有限集合であり、

$$\sharp X_{i+1} = \sharp X_i + \sharp(\{a_{i+1}\} \times B) = i \times \sharp B + \sharp B = (i+1) \times \sharp B$$

となることがわかる。

以上で帰納法が完成した。よって、$X_m = A \times B$ は有限集合であり、$\sharp X_m = m \times \sharp B = \sharp A \times \sharp B$ である。 □

●有限集合の間の写像の全単射性

次の命題が成り立つことは直感によく合致していて、当然のように思えることでしょう。

命題 30-8

空でない有限集合 A から有限集合 B への写像 $f : A \longrightarrow B$ について、次が成り立つ。

(1) f が単射ならば、$\sharp A \leq \sharp B$ である。

(2) f が全射ならば、$\sharp B \leq \sharp A$ である。

(**proof**)

$m = \sharp A,\ n = \sharp B$ とおく。全単射 $g : A \longrightarrow N(m),\ h : B \longrightarrow N(n)$ が存在する。

(1) f が単射なので、

$$k := h \circ f \circ g^{-1} : N(m) \longrightarrow N(n)$$

は単射である。$C := k(N(m))$ とおくと、k は $N(m)$ から C への全単射と思える。このとき、その逆写像 $k^{-1} : C \longrightarrow N(m)$ は全単射である。

もし、$n < m$ であったと仮定すると、$C \subset N(n) \subset N(m)$ となるから、補題 30-1 により、$C = N(m)$ を得る。これは $N(n) = N(m)$ を導く。特に、$m \in N(m) = N(n)$ より、$m \leq n$ が得られて、矛盾が生じる。したがって、$m \leq n$ でなければならない。

(2) f が全射なので、

$$k = h \circ f \circ g^{-1} : N(m) \longrightarrow N(n)$$

は全射である。したがって、各 $b \in N(n)$ に対して、$\{\ x \in N(m) \mid k(x) = b\ \}$ は空集合でない。よって、

$$j(b) := \min\{\ x \in N(m) \mid k(x) = b\ \}$$

が存在する (自然数の整列性)。このとき、写像 $j : N(n) \longrightarrow N(m)$ は単射であるから、(1) により、$n \leq m$ を得る。 □

上の命題の証明と同様の手法で次の命題を証明することができます。

命題 30-9

A, B を $\sharp A = \sharp B$ であるような空でない有限集合とする。写像 $f : A \longrightarrow B$ について、

$$f \text{ が単射} \iff f \text{ が全射}$$

が成り立つ。

演習 30-2　命題 30-9 を証明せよ。

§30-2 無限集合と濃度

無限集合は、大別すると、元に番号をつけることのできる集合とそうでない集合に分けられます。ここでは、$\mathbb{Q}$ が前者に帰属し、$\mathbb{R}$ が後者に帰属することを証明します。

●濃度が等しい集合

２つの集合 A と B がともに空集合であるか、または、全単射 $f : A \longrightarrow B$ が存在するとき、A は B と**濃度が等しい** (equipotent)、または、**対等**であるといいます。これを $A \sim B$ で表わします。

補題 30-10

集合 A, B, C について次が成り立つ。

(i) $A \sim A$

(ii) $A \sim B \ \Rightarrow\ B \sim A$

(iii) $A \sim B,\ B \sim C \ \Rightarrow\ A \sim C$

演習 30-3　補題 30-10 を証明せよ。

例 30-11　(1) $\mathbb{R}$ と区間 $(-1,1)$ の濃度は等しい。
(2) 区間 $(0,1)$ と区間 $(0,1]$ の濃度は等しい。
(**proof**)
(1) 写像 $f:(-1,1)\longrightarrow\mathbb{R}$ を

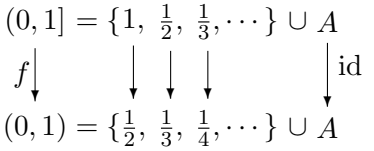
$$f(x)=\frac{x}{1-|x|}\qquad(x\in(-1,1))$$

によって定義する。f は全単射である。実際、f は

$$g:\mathbb{R}\longrightarrow(-1,1),\quad g(x)=\frac{x}{1+|x|}\qquad(x\in\mathbb{R})$$

を逆写像として持つ。
(2) $A=(0,1]-\{\frac{1}{n}\mid n\in\mathbb{N}\}$ とおき、
写像 $f:(0,1]\longrightarrow(0,1)$ を

$$f(x)=\begin{cases}\frac{1}{n+1} & (x=\frac{1}{n},\ n\in\mathbb{N}\text{ のとき})\\ x & (x\in A\text{ のとき})\end{cases}$$



によって定義する（右図参照）。容易に確かめられるように、f は全単射である。　□

注意：(2) と同じ証明方法で、$(0,1)$, $[0,1)$, $[0,1]$ の濃度はすべて等しいことがわかります。このことと次の演習 30-4 から、任意の区間は $\mathbb{R}$ と同じ濃度を持つことがわかります。

演習 30-4* 開区間 (a,b) と $(-1,1)$ の濃度は等しいことを示せ。

●可算集合

集合 A が**可算** (countable) であるとは、自然数全体からなる集合 $\mathbb{N}=\{1,2,3,\cdots\}$ と濃度が等しいときをいいます。このとき、A を**可算集合**といいます。定義により、$\mathbb{N}$ は可算集合です。

例 30-12　$\mathbb{Z}$ は可算集合である。なぜならば、全単射 $f:\mathbb{Z}\longrightarrow\mathbb{N}$ を作ることができるからである。実際、f を

$$f(0)=1,\ f(n)=2n,\ f(-n)=2n+1\quad(n\in\mathbb{N})$$

によって定義すればよい。

演習 30-5* 偶数全体からなる集合 $2\mathbb{Z}=\{\cdots,-4,-2,0,2,4,\cdots\}$ は可算であることを示せ。

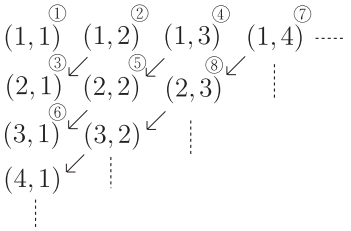
●$\mathbb{Q}$ の可算性

可算集合については次の定理が基本的です。

定理 30-13
(1) 集合 A, B が可算ならば、直積集合 $A\times B$ も可算である。
(2) 可算集合の部分集合は有限または可算である。

(**proof**)

(1) $A = B = \mathbb{N}$ の場合に証明すれば十分である。



$\mathbb{N}\times\mathbb{N}$ の元は右のように番号づけることができる。したがって、$\mathbb{N}\times\mathbb{N}$ は可算集合である。実際、全単射 $f : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ が次式によって与えられる。

$$f(m,n) = \frac{(m+n-1)(m+n-2)}{2} + m \quad (m,n \in \mathbb{N}).$$

(2) $\mathbb{N}$ の任意の無限部分集合 A が可算集合であることを示せば十分である。A が無限集合であることと自然数の整列性を使って、A の元からなる数列 $a_1, a_2, a_3, \cdots$ を次のように帰納的に定義することができる。

$$a_1 := \min A, \quad a_k := \min(A - \{a_1, \cdots, a_{k-1}\}) \qquad (k = 2, 3, 4, \cdots).$$

このとき、$A = \{a_1, a_2, a_3, \cdots\}$ が成り立つ。実際、もし、$A \neq \{a_1, a_2, \cdots\}$ であると仮定すると、$m \notin \{a_1, a_2, \cdots\}$ となる $m \in A$ が存在する。特に、$m \notin \{a_1, a_2, \cdots, a_m\}$、すなわち、$m \in A - \{a_1, \cdots, a_m\}$ である。よって、$m + 1 \leq a_{m+1} \leq m$ を得る (1 番目の不等号は $\{a_n\}_{n=1}^{\infty}$ が自然数の狭義単調増加数列であることから、2 番目の不等号は a_{m+1} の定め方から従う)。これは矛盾である。これで、$A = \{a_1, a_2, a_3, \cdots\}$ が示されたので、全単射 $f : \mathbb{N} \longrightarrow A,\ f(n) = a_n\ (n \in \mathbb{N})$ が得られた。 □

系 30-14

$\mathbb{Q}$ は可算集合である。

演習 30-6 * 上の系を示せ。

ヒント：まず、正の有理数全体 $\mathbb{Q}^+$ が可算集合であることを示す。任意の有理数は既約分数の形に一意的に表わされることを使う。

● $\mathbb{R}$ の非可算性

可算でない無限集合は**非可算** (uncountable) であると呼ばれます。

定理 30-15

$\mathbb{R}$ は非可算集合である。

(**proof**)

背理法で証明する。$\mathbb{R}$ が可算集合であると仮定すると、例 30-11(1)、演習 30-4、補題 30-10 により、$(0,1)$ も可算集合である。よって、全単射 $f : \mathbb{N} \longrightarrow (0,1)$ が存在する。各 $n \in \mathbb{N}$ に対して、$f(n) \in (0,1)$ を

$$(*) \qquad f(n) = 0.a_{n1}a_{n2}a_{n3}\cdots\cdots \quad (a_{nj} \in \{0, 1, \cdots, 9\})$$

のように無限 10 進小数で表わすことにする。但し、$\frac{1}{2} = 0.50000\cdots\cdots = 0.49999\cdots\cdots$ のように 2 通りの 10 進小数表示を持つ実数に対しては、ある位から先は 0 が無限に続く表示を用いることにする。このように決めておくと、$(0,1)$ に属する任意の実数は $(*)$ のような無限 10 進小数の形に一意的に書き表わすことができる (命題 9-9)。

$$
\begin{array}{l}
f(1) = 0.\, a_{11}\, a_{12}\, a_{13} \cdots\cdots\, a_{1n} \cdots\cdots \\
f(2) = 0.\, a_{21}\, a_{22}\, a_{23} \cdots\cdots\, a_{2n} \cdots\cdots \\
f(3) = 0.\, a_{31}\, a_{32}\, a_{33} \cdots\cdots\, a_{3n} \cdots\cdots \\
\quad\vdots \qquad\quad \vdots \qquad\quad \ddots \qquad\quad \vdots \\
f(n) = 0.\, a_{n1}\, a_{n2}\, a_{n3} \cdots\cdots\, a_{nn} \cdots\cdots \\
\quad\vdots \qquad\quad \vdots \qquad\qquad\qquad\quad \vdots
\end{array}
$$

今、上の表の小数点以下の“対角線部分”$a_{11}, a_{22}, a_{33}, \cdots$ に着目して、各 $n \in \mathbb{N}$ に対して、b_n を

$$
b_n = \begin{cases} 2 & (a_{nn} = 1 \text{ のとき}) \\ 1 & (a_{nn} \neq 1 \text{ のとき}) \end{cases}
$$

と定め、$0.b_1b_2b_3 \cdots\cdots b_n \cdots\cdots$ という無限 10 進小数表示を持つ実数を x とおく。$x \in (0,1)$ である。一方、任意の $n \in \mathbb{N}$ について $b_n \neq a_{nn}$ であるから、$x \neq f(n)$ である。これは f が全射であることに反する。故に、$\mathbb{R}$ は可算集合ではない。 □

注意：1. 上の証明法はカントールが発明した方法で、**対角線論法**と呼ばれています。
2. $\mathbb{Q}$ は可算集合なのに $\mathbb{R}$ は非可算集合なので、有理数よりも無理数のほうが‘はるかに多く’存在することがわかります。

●ベルンシュタインの定理と $\mathbb{C}$ の濃度

集合 A, B について、A から B への単射と B から A への単射が存在するとき、$A \sim B$ となることが知られています (**ベルンシュタインの定理**)。これを使うと次の定理を証明することができます。

定理 30-16

$\mathbb{R}$ と $\mathbb{C}$ の濃度は等しい。

(**proof**)

$\mathbb{R} \sim (0,1)$, $\mathbb{C} = \mathbb{R} \times \mathbb{R} \sim (0,1) \times (0,1)$ なので、$(0,1) \sim (0,1) \times (0,1)$ を示せばよい。

$(0,1)$ から $(0,1) \times (0,1)$ への単射として写像

$$
f : (0,1) \longrightarrow (0,1) \times (0,1), \qquad f(a) = (a, a) \quad (a \in (0,1))
$$

が考えられる。一方、$(0,1) \times (0,1)$ から $(0,1)$ への単射として次のように定義される写像 $g : (0,1) \times (0,1) \longrightarrow (0,1)$ が考えられる：$a, b \in (0,1)$ に対して、無限 10 進小数表示

$$
a = 0.a_1a_2a_3 \cdots, \qquad b = 0.b_1b_2b_3 \cdots
$$

を考え、$0.a_1b_1a_2b_2a_3b_3 \cdots$ という無限 10 進小数で表示される実数を $g(a,b)$ と定める。但し、a, b が 2 通りの無限 10 進小数表示を持つ場合には、ある位から先はすべて 0 が続くような表示を用いることにする。無限 10 進小数表示 $0.a_1b_1a_2b_2a_3b_3 \cdots$ においてある位から先がすべて 9 になることはないので、g は確かに単射である。

以上から、ベルンシュタインの定理により、$(0,1) \sim (0,1) \times (0,1)$ とわかる。 □

注意：集合 A から集合 B への単射は存在するけれども全単射は存在しないとき、B の濃度は A の濃度よりも大きいといいます。上の定理を見ると、$\mathbb{R}$ の濃度よりも大きい濃度を持つ集合は存在しないような印象を持つかもしれませんが、そうではありません。任意の集合 A に対して、その冪集合 $\mathcal{P}(A)$ の濃度は常に A の濃度よりも大きいことを証明することができます。

§31. 選択公理

選択公理とは、空でない集合からなる族 $\{A_\lambda\}_{\lambda\in\Lambda}$ が与えられたときに、すべての $\lambda\in\Lambda$ について集合 A_λ から一斉に元を取り出すことができる、ということを主張する命題です。この選択公理は現代数学のほとんどの分野で使われています。気がつかなかったかも知れませんが、実は、私たちはすでに暗黙のうちにこの公理を使っています。ここでは、選択公理を使っているということを意識しながら、そのような箇所をもう一度証明しなおしてみましょう。

●添字づけられた集合族

空でない集合 Λ の各元 λ に対して、集合 A_λ が 1 つづつ定められているとき、それらの“集まり”を $\{A_\lambda\}_{\lambda\in\Lambda}$ という記号で表わし、Λ を**添字集合** (index set) とする集合族といいます。ここで 1 つ注意してもらいたいことは、(実) 数列 $\{a_n\}_{n=1}^{\infty}$ と集合 $\{a_n \mid n\in\mathbb{N}\}$ を区別したように、$\{A_\lambda\}_{\lambda\in\Lambda}$ は $\{A_\lambda \mid \lambda\in\Lambda\}$ とは違うということです。$\{A_\lambda\}_{\lambda\in\Lambda}$ と書く場合には、集合の集まりというだけではなく、「各 $\lambda\in\Lambda$ に対して集合 A_λ を対応させる規則」も指定されています。

Λ を添字集合とする集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ に対して、集合 $\bigcap\limits_{\lambda\in\Lambda} A_\lambda$, $\bigcup\limits_{\lambda\in\Lambda} A_\lambda$ を

$$\bigcap_{\lambda\in\Lambda} A_\lambda := \{\ x \mid \forall\,\lambda\in\Lambda,\ x\in A_\lambda\ \}$$
$$\bigcup_{\lambda\in\Lambda} A_\lambda := \{\ x \mid \exists\,\lambda\in\Lambda\ \text{ s.t. }\ x\in A_\lambda\ \}$$

によって定めることができます。

もし、すべての A_λ がある固定された集合 X の部分集合であれば、定理 5-7 と同様に、**ド・モルガンの法則**

$$X-\bigcap_{\lambda\in\Lambda} A_\lambda=\bigcup_{\lambda\in\Lambda}(X-A_\lambda),\qquad X-\bigcup_{\lambda\in\Lambda} A_\lambda=\bigcap_{\lambda\in\Lambda}(X-A_\lambda)$$

が成り立ちます。

演習 31-1 $\Lambda=\{\lambda\in\mathbb{Q}\mid 1\le\lambda\le\sqrt{2}\}$ のとき、$\bigcap\limits_{\lambda\in\Lambda}[\lambda,1+\lambda]$ と $\bigcup\limits_{\lambda\in\Lambda}[\lambda,1+\lambda]$ を求めよ。

●無限個の集合に対する直積集合

直積集合の定義は選択公理と密接に関連しています。ここで、直積集合の概念について反省しておきましょう。

2 つの集合 A, B の直積集合 $A\times B$ とは、$a\in A$ と $b\in B$ の順序対 (a,b) の全体からなる集合のことでした：

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

ここで、2 つの順序対 (a,b) と (a',b') が等しい、すなわち、$(a,b)=(a',b')$ であるとは、$a=a'$ かつ $b=b'$ となるときを言うのでした。

順序対 (a,b) および直積集合 $A\times B$ の類似は、$\Lambda(\neq\varnothing)$ を添字集合とする集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ に対して考えることができます。まず、各 $\lambda\in\Lambda$ について A_λ の元 a_λ が 1 つづつ指定されて

いる“組”$(a_\lambda)_{\lambda\in\Lambda}$ を考えます。このような2つの“組”$(a_\lambda)_{\lambda\in\Lambda}, (a'_\lambda)_{\lambda\in\Lambda}$ が等しいとは、すべての $\lambda\in\Lambda$ について $a_\lambda = a'_\lambda$ となるときである、と定めます。すなわち、

$$(a_\lambda)_{\lambda\in\Lambda} = (a'_\lambda)_{\lambda\in\Lambda} \iff \forall\,\lambda\in\Lambda,\ \ a_\lambda = a'_\lambda$$

と定義します。このとき、集合

$$\prod_{\lambda\in\Lambda} A_\lambda = \{(a_\lambda)_{\lambda\in\Lambda} \mid a_\lambda \in A_\lambda\ \ (\lambda\in\Lambda)\}$$

を集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ の**直積**といいます。

注意：1.「各 $\lambda\in\Lambda$ について A_λ の元 a_λ が1つづつ指定されている“組”$(a_\lambda)_{\lambda\in\Lambda}$」とは、厳密に言えば、$f(\lambda) = a_\lambda$ $(\lambda\in\Lambda)$ によって定義される写像 $f:\Lambda\longrightarrow \bigcup_{\lambda\in\Lambda} A_\lambda$ のことに他なりません。したがって、

$$\prod_{\lambda\in\Lambda} A_\lambda = \{\ f:\Lambda\longrightarrow \bigcup_{\lambda\in\Lambda} A_\lambda \mid \forall\,\lambda\in\Lambda,\ f(\lambda)\in A_\lambda\ \}$$

と書き表わすことができます。これが直積集合の正確な定義です。
2. A を集合とします。$\Lambda(\neq\varnothing)$ を添字集合とする集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ が、任意の $\lambda\in\Lambda$ について $A_\lambda = A$ を満たすとき、直積集合 $\prod_{\lambda\in\Lambda} A_\lambda$ のことを A^Λ と書きます：

$$A^\Lambda = \{\text{ 写像 } f:\Lambda\longrightarrow A \text{ の全体 }\}.$$

演習 31-2　空でない2つの集合 A, B に対して、集合 $A\times B = \{\ (a,b)\mid a\in A,\ b\in B\ \}$ と集合 $\{\ f:\{1,2\}\longrightarrow A\cup B \mid f(1)\in A,\ f(2)\in B\ \}$ との間に全単射が存在することを示せ。

●集合論の逆理

集合とは「“もの”の集まりであって、その集まりがどのような“もの”からなるかが客観的に規定されているもののこと」をいいました（第3節参照）。このように素朴に集合を定義してしまうと、少し困った状況が生じます。それは**逆理** (paradox) の存在です。ここで、その代表例として、**ラッセルの逆理**を紹介しておきます。

例 31-1 (Russel の逆理)　$\mathcal{A} := \{\ A \mid A \text{ は } A\notin A \text{ を満たす集合}\ \}$ については、$\mathcal{A}\in\mathcal{A}$ も $\mathcal{A}\notin\mathcal{A}$ もどちらも成り立たない。

(**proof**)

もし、$\mathcal{A}\in\mathcal{A}$ であったと仮定する。すると、$\mathcal{A}$ は $\{\ A\mid A \text{ は } A\notin A \text{ を満たす集合}\ \}$ の元であるから、$\mathcal{A}\notin\mathcal{A}$ を満たしていなければならない。これは、$\mathcal{A}\in\mathcal{A}$ としていたことに矛盾する。

今度は、$\mathcal{A}\notin\mathcal{A}$ であったと仮定する。すると、$\mathcal{A}$ の定義によって、$\mathcal{A}\in\mathcal{A}$ となり、やはり矛盾が生じてしまう。　□

私達が通常扱っている集合はすべて自分自身を要素に持ちませんから、例 31-1 の $\mathcal{A}$ は“かなり大きな集合”であることがわかります。このような“巨大な集合”を排除することにより、逆理が起こりそうにない集合論を構築しようという動きが20世紀初頭に現れ、ツェルメロ、フレンケル、スコーレム、フォン・ノイマンらにより公理的集合論が提唱されました。公理的集

合論では、集合と呼ぶべき対象が自然数の集合などの良く知られた集合から以下の操作を有限回施して得られるものに限定されます（詳しくは集合論の教科書を参照して下さい)。

- 集合 A, B から直積集合 $A \times B$ を作ること
- 集合 A から冪集合 $\mathcal{P}(A)$ を作ること
- 集合 Λ の各元 λ に対して、集合 A_λ を対応させる規則が与えられたとき、集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ を作ること
- 集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ から和集合 $\bigcup_{\lambda\in\Lambda} A_\lambda$ を作ること
- 集合 A と、A を定義域とする命題関数 $P(x)$ が与えられたとき、$P(x)$ が真であるような A の元全体からなる部分集合を作ること（例えば、集合 A, B から差集合 $A - B$ を作ることや集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ から共通部分 $\bigcap_{\lambda\in\Lambda} A_\lambda$ を作ることがこれに含まれます）

注意：集合 A から B への写像全体 $\mathrm{Map}(A, B)$ は上の意味で集合になります。何故ならば、$\mathrm{Map}(A, B)$ は冪集合 $\mathcal{P}(A\times B)$ の部分集合 G であって、条件「$\forall\, a \in A,\ \exists!\, b \in B$ s.t. $(a, b) \in G$」を満たすもの全体とみなせるからです (次の演習問題を参照)。

演習 31-3　A, B を (空でない) 2 つの集合とする。A から B への写像全体からなる集合を $\mathrm{Map}(A, B)$ とおき、$A \times B$ の次の条件を満たす (空でない) 部分集合 G 全体からなる集合を $\mathrm{Graph}(A, B)$ とおく：$\forall\, a \in A,\ \exists!\, b \in B$ s.t. $(a, b) \in G$.

このとき、$\mathrm{Map}(A, B)$ と $\mathrm{Graph}(A, B)$ の間に全単射が存在することを示せ。

ヒント：$f \in \mathrm{Map}(A, B)$ に対して、f のグラフ $G_f := \{\, (a, f(a)) \mid a \in A\} \subset A \times B$ を考えよ。

●選択公理

2 つの集合 A, B について、

$$A \neq \varnothing \ \text{ かつ } \ B \neq \varnothing \ \ \Longrightarrow \ \ A \times B \neq \varnothing$$

が成り立つことは、$A \times B$ の定義から直ちに従います。より一般に、n 個の集合 $A_1, \cdots, A_n$ について、

$$\forall\, i \in \{1, \cdots, n\}, \ \ A_i \neq \varnothing \ \ \Longrightarrow \ \ A_1 \times \cdots \times A_n \neq \varnothing$$

が成り立つことがわかります。では、無限集合 Λ を添字集合とする集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ について同様のことがいえるのでしょうか。ツェルメロはこの問題の重要性を認識し、**選択公理** (axiom of choice) と呼ばれる次の主張を、集合論における 1 つの公理として提出しました (1904 年)。

選択公理

$\Lambda(\neq \varnothing)$ を添字集合とする任意の集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ に対して、

$$\forall\, \lambda \in \Lambda,\ A_\lambda \neq \varnothing \ \ \Longrightarrow \ \ \prod_{\lambda\in\Lambda} A_\lambda \neq \varnothing.$$

選択公理の内容がわかりにくいかもしれませんので、少し説明を加えておきます。各 $\lambda \in \Lambda$ について $A_\lambda \neq \varnothing$ であれば、A_λ に元が少なくとも 1 つ存在します。そこで、各 $\lambda \in \Lambda$ について A_λ から元を 1 つずつとり、それを a_λ とおきます。このとき、これらを“並べて”$\prod_{\lambda\in\Lambda} A_\lambda$ の元 $(a_\lambda)_{\lambda\in\Lambda}$ を作ることができるので、$\prod_{\lambda\in\Lambda} A_\lambda \neq \varnothing$ が証明できるように思えます。しかし、これは正しくないのです。問題点は、各 A_λ から元 a_λ をどのような方法で取り出せばよいのか

一般には全くわからない、ということにあります。Λ が無限集合であって、与えられた集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ が (得体の知れない) 様々な (条件によって定義された) 集合からなる場合、その 1 つ 1 つから（順番に）元を取り出して $(a_\lambda)_{\lambda\in\Lambda}$ のような組を作ることは、一般には不可能です。つまり、各 $\lambda\in\Lambda$ について A_λ から一斉に元を取り出さなければ、直積 $\prod_{\lambda\in\Lambda} A_\lambda$ の元を与えることはできないのです。そこで、“一斉に取り出せる”ということを公理で保証しようというわけです。

注意：選択公理がいつでも必要になるわけではありません。添字集合が有限集合であれば、先に述べたように、選択公理は定理です。また、各 A_λ が（他の元と区別のつく）特別な元を備えていれば、選択公理を使うことなく、$\prod_{\lambda\in\Lambda} A_\lambda \neq \varnothing$ が示されます。例えば、各 A_λ が体 K 上のベクトル空間である場合には、A_λ には零ベクトル 0_{A_λ} という特別な元があるので、写像 $f:\Lambda\longrightarrow \bigcup_{\lambda\in\Lambda} A_\lambda$ を $f(\lambda)=0_{A_\lambda}$ $(\lambda\in\Lambda)$ によって定義することができます。この f は $\prod_{\lambda\in\Lambda} A_\lambda$ の元であり、したがって、$\prod_{\lambda\in\Lambda} A_\lambda \neq \varnothing$ がわかります。

●選択公理を使って得られる結果

ここでは、選択公理を使って得られる結果をいくつか紹介します。次の命題の (2)「① ⇒ ②」の証明に選択公理が必要になります。

命題 31-2

(1) 写像 $f:X\longrightarrow Y$ について、次は同値である。

① f は単射である。

② 写像 $r:Y\longrightarrow X$ であって、$r\circ f=\mathrm{id}_X$ となるものが存在する。

(2) 写像 $f:X\longrightarrow Y$ について、次は同値である。

① f は全射である。

② 写像 $s:Y\longrightarrow X$ であって、$f\circ s=\mathrm{id}_Y$ となるものが存在する。

(**proof**)

一般に、写像 $f:X\longrightarrow Y$ と $g:Y\longrightarrow X$ について $g\circ f=\mathrm{id}_X$ であるならば、g は全射であり、f は単射になる（これは演習問題とする。演習 31-4）から、(1)(2) の「② ⇒ ①」が成り立つ。

(1)「① ⇒ ②」の証明：

f が単射であるとすると、f の終域 Y を $f(X)$ に制限することにより得られる写像

$$f':X\longrightarrow f(X),\quad f'(x)=f(x)\qquad (x\in X)$$

は全単射である。

$x_0\in X$ を任意にとり 1 つ固定する。このとき、写像 $r:Y\longrightarrow X$ を

$$r(y)=\begin{cases}(f')^{-1}(y) & (y\in f(X)\text{ のとき})\\ x_0 & (y\in Y-f(X)\text{ のとき})\end{cases}$$

によって定義する。この r は $r\circ f=\mathrm{id}_X$ を満たす。

(2)「① ⇒ ②」の証明：

f が全射であるとすると、任意の $y \in Y$ に対して、

$$f^{-1}(\{y\}) := \{x \in X \mid f(x) = y\}$$

は空集合ではない。選択公理により、

$$\prod_{y \in Y} f^{-1}(\{y\}) \neq \varnothing$$

であるから、元 $a \in \prod_{y \in Y} f^{-1}(\{y\})$ が存在する。a は写像 $a : Y \longrightarrow \bigcup_{y \in Y} f^{-1}(\{y\})$ であって、すべての $y \in Y$ について $a(y) \in f^{-1}(\{y\}) \subset X$ を満たす。そこで、$s : Y \longrightarrow X$ を

$$s(y) = a(y) \qquad (y \in Y)$$

によって定めると、$f \circ s = \mathrm{id}_Y$ が成り立つ。 □

注意：(1)②の r は全射であり、(2)②の s は単射です (演習 31-4)。このことから、集合 X, Y について

$$「X \text{ から } Y \text{ へ単射が存在する} \iff Y \text{ から } X \text{ へ全射が存在する}」$$

が成立することがわかります。

演習 31-4 写像 $f : X \longrightarrow Y$ と $g : Y \longrightarrow X$ について、

$$g \circ f = \mathrm{id}_X \text{ ならば「} g \text{ は全射であり、かつ、} f \text{ は単射である」}$$

ことを示せ。

以前、数ベクトル空間 K^n の $\{\mathbf{0}\}$ でないすべての部分空間には基底が存在するという定理 (定理 20-12) を証明しましたが、その証明には暗黙のうちに選択公理が使われています。

例 31-3 数ベクトル空間 K^n の $\{\mathbf{0}\}$ でないすべての部分空間には基底が存在する。

(**proof**)

$V \subset K^n$ を $\{\mathbf{0}\}$ でない部分空間とする。V の線形独立な有限部分集合 L であって、V を張るものは存在しないと仮定して矛盾を導く。

まず、

$$\mathcal{L} = \{\ L \subset V \mid L \text{ は有限集合、かつ、} V \text{ の線形独立系}\ \}$$

とおき、各 $L \in \mathcal{L}$ に対して、V の部分集合

$$V_L := \{\ v \in V \mid L \cup \{v\} \text{ は } V \text{ の線形独立系}\ \}$$

を考える。仮定により、$V_L \neq \varnothing$ である (補題 20-12) から、選択公理により、写像

$$f : \mathcal{L} \longrightarrow \bigcup_{L \in \mathcal{L}} V_L \subset V$$

であって、

$$\text{すべての } L \in \mathcal{L} \text{ について } f(L) \in V_L$$

を満たすものが存在する。

$L_0 := \varnothing \in \mathcal{L}$ に対して $\mathbf{v}_1 := f(L_0)$ とおくと、$\{\mathbf{v}_1\} = L_0 \cup \{\mathbf{v}_1\}$ は V の線形独立系である。次に、$L_1 := \{\mathbf{v}_1\} \in \mathcal{L}$ に対して $\mathbf{v}_2 := f(L_1)$ とおくと、$\{\mathbf{v}_1, \mathbf{v}_2\} = L_1 \cup \{\mathbf{v}_2\}$

は V の線形独立系である。以下、同様に (厳密には数学的帰納法を用いて)、$\mathcal{L}$ 内の増大列 $L_0 \subset L_1 \subset L_2 \subset \cdots$ であって、$\sharp L_k = k$ $(k \in \mathbb{N})$ となるものの存在がわかる。特に、L_{n+1} は $(n+1)$ 個のベクトルからなる V の線形独立系である。しかしながら、これは、数ベクトル空間 K^n の任意の $(n+1)$ 個のベクトルは K 上線形独立でないこと (補題 20-10) に矛盾する。 □

演習 31-5 以前、1 変数関数 $f : S \longrightarrow \mathbb{R}$ と点 $a \in S$ について、次の 2 つが同値であることを証明した (定理 14-8)：

(i) f は点 a で連続である。

(ii) $\lim_{n\to\infty} x_n = a$ を満たす S の元からなる任意の数列 $\{x_n\}_{n=1}^{\infty}$ に対して、$\lim_{n\to\infty} f(x_n) = f(a)$ である。

この定理の「(ii) $\Rightarrow$ (i)」の証明は以下のようであった。

f は a で連続でないと仮定する。すると、次の条件を満たす $\varepsilon > 0$ が存在する：

$$(*) \qquad \forall\, \delta > 0,\ \exists\, x \in S \ \text{ s.t. } \ |x - a| < \delta,\ |f(x) - f(a)| \geq \varepsilon.$$

したがって、各 $n \in \mathbb{N}$ に対して $\frac{1}{n}$ を考え、$\delta = \frac{1}{n}$ に対して $(*)$ を適用することにより、$|x_n - a| < \frac{1}{n}$ かつ $|f(x_n) - f(a)| \geq \varepsilon$ を満たす $x_n \in S$ の存在がわかる。このとき、S の元からなる数列 $\{x_n\}_{n=1}^{\infty}$ は a に収束するが、数列 $\{f(x_n)\}_{n=1}^{\infty}$ は $f(a)$ に収束しない。これで「(ii) $\Longrightarrow$ (i)」の対偶が証明された。 □

上の証明を選択公理を明示した証明に書き換えよ。

● Zorn の補題

選択公理と「同値」な命題に **Zorn の補題** (Zorn's lemma) があります。Zorn の補題を説明するために順序集合における極大元という概念を導入します。

定義 31-4

$(X, \leq)$ を順序集合とする。$a \in X$ が順序集合 $(X, \leq)$ の **極大元** (maximal element) であるとは、

$$x \in X,\ a \leq x \quad \Longrightarrow \quad x = a$$

となるときをいう。

極大元は最大元とは異なり、複数存在する可能性があります。例えば、$A = \{1, 2, 3, 4\}$ の冪集合 $\mathcal{P}(A)$ の部分集合

$$X = \{\varnothing,\ \{1\},\ \{2, 4\},\ \{1, 2, 4\},\ \{3\},\ \{1, 3\}\}$$

を考えます。X に包含関係による順序を与えて、X を順序集合とみなします。このとき、$\{1, 2, 4\}$ および $\{1, 3\}$ はどちらも順序集合 X の極大元です。

準備が整いましたので、Zorn の補題を述べることにしましょう。

Zorn の補題

順序集合 X $(\neq \varnothing)$ において、空でない任意の全順序部分集合が X の中に上界を持つならば、X には少なくとも 1 つ極大元が存在する。

Zorn の補題は、X がある冪集合（の部分集合）上の包含関係を順序とする集合の場合によく使われます。例えば、体 K 上の $\{0\}$ でない任意のベクトル空間 V に基底が存在することは、以下の手順で示されます。

Step1. $\mathcal{S} = \{$ K 上一次独立な V の部分集合の全体 $\}$ とおくと、$\mathcal{S} \neq \varnothing$ である。

Step2. $\mathcal{S}$ を包含関係による順序集合とみなす。$\mathcal{S}$ の空でない全順序部分集合 $\mathcal{O}$ について、$\bigcup_{B\in\mathcal{O}} B$ は $\mathcal{S}$ に属する。

Step3. $\mathcal{S}$ に極大元が存在する (Zorn の補題を用いる)。

Step4. $\mathcal{S}$ の極大元 $\mathfrak{B}$ は V の K 上の基底である。

演習 31-6　体 K 上の $\{0\}$ でない任意のベクトル空間 V には基底が存在することを示せ。

ヒント：Step4 は、$v \in V$ がどのような有限個 $x_1, \cdots, x_r \in \mathfrak{B}$ についても

$$v = a_1x_1 + a_2x_2 + \cdots + a_rx_r \quad (a_i \in K,\ i = 1, \cdots, r)$$

のように書けないならば、$\mathfrak{B} \subsetneqq \mathfrak{B} \cup \{v\}$ かつ $\mathfrak{B} \cup \{v\} \in \mathcal{S}$ が成り立つこと（演習 20-4 参照）から従う。

上の演習問題により、無限次元ベクトル空間にも基底が存在することがわかります。例えば、$\mathbb{R}$ 上で定義された実数値関数全体のなすベクトル空間 $\mathrm{Map}(\mathbb{R}, \mathbb{R})$、実数列のなすベクトル空間 $\mathrm{Seq}(\mathbb{R})$、$\mathbb{R}$ を自然な方法で $\mathbb{Q}$ 上のベクトル空間とみなしたもの（$\mathbb{Q}$ の $\mathbb{R}$ への作用は実数の積を使って定義します）にも (具体的には求められないけれども) 基底が存在します。

注意：$\mathbb{R}$ が $\mathbb{Q}$ 上のベクトル空間として無限次元であることは以下のように示されます。

$\mathbb{R}$ の $\mathbb{Q}$ 上のある基底 $\mathfrak{B}$ が有限個の元 $x_1, \cdots, x_r$ からなると仮定します。すると、全単射 $\mathbb{R} \longrightarrow \mathbb{Q}^r$ が存在します (但し、$\mathbb{Q}^r$ は $\mathbb{Q}$ の r 個の直積です)。これより、$\mathbb{R}$ と $\mathbb{Q}^r$ の濃度は等しくなければなりませんが、これはあり得ません。何故ならば、$\mathbb{Q}^r$ は可算 ($\because$ 可算集合の有限個の直積は可算、$\mathbb{Q}$ は可算) である一方で、$\mathbb{R}$ は非可算だからです。

●整列可能性定理と選択公理

順序集合 X が**整列集合** (well-ordered set) であるとは、任意の空でない部分集合が最小元を持つときをいいます。例えば、任意の有限全順序集合や自然数全体 $\mathbb{N}$ は整列集合です。任意の集合は、順序を適当に定めることにより、整列集合にすることができる（**整列可能性定理**）ことが知られています。

注意：整列集合は全順序集合です。何故ならば、相異なる任意の $x, y \in X$ に対して、$\{x, y\}$ は最小元を持つので、x が最小元であるとすると $x < y$ が成り立つからです。

Zorn の補題が選択公理と「同値」であることは述べましたが、整列可能性定理も実は選択公理と「同値」であることが知られています。すなわち、次の 3 つは互いに同値な命題です。

(i) (**選択公理**) $\Lambda(\neq \varnothing)$ を添字集合とする任意の集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ に対して、
$$\forall\, \lambda \in \Lambda,\ A_\lambda \neq \varnothing \implies \prod_{\lambda\in\Lambda} A_\lambda \neq \varnothing.$$

(ii) (**Zorn の補題**) 順序集合 X $(\neq \varnothing)$ において、空でない任意の全順序部分集合が X の中に上界を持つならば、X には少なくとも 1 つ極大元が存在する。

(iii) (**整列可能性定理**) 任意の集合は、順序を適当に定めることにより、整列集合にすることができる。

このように命題を並べてみると、選択公理が決して「当たり前なことではない」ことがよくわかりますね。

– お し ま い –

参考文献

[1] H. アントン『やさしい線形代数』, 山下純一・訳, 現代数学社, 1979.
[2] 伊吹山知義「誰でもわかる数学の基礎」, 2002 年度大阪大学理学部数学科 I-2a,b 演習教材.
[3] 彌永昌吉 『数の体系（上・下)』(岩波新書), 岩波書店, 1972, 1978.
[4] 彌永昌吉 『集合と位相 I』(岩波講座基礎数学), 岩波書店, 1976.
[5] 内田伏一『集合と位相』(数学シリーズ), 裳華房, 1896.
[6] 宇野利雄『微分積分学 Ⅲ』(基礎数学講座 9-A）, 共立出版, 1956.
[7] H.-D. エビングハウス, H. ヘルメス, F. ヒルツェブルフ, M. ケッヒャー, K. マインツァー, J. ノイキルヒ, A. プレステル, R. レンメルト・共著『数（上)』, 成木勇夫・訳, シュプリンガーフェアラーク東京, 1991.
[8] 片山孝次『整数論入門』, 実教出版, 1975.
[9] 片山孝次『代数学入門』(基礎数学叢書 3), 新曜社, 1981.
[10] M・ケッヒャー『数論的古典解析—歴史を訪ねて』, 長岡昇勇・訳, シュプリンガー・フェアラーク東京, 1996.
[11] 小林昭七『なっとくするオイラーとフェルマー』, 講談社, 2003.
[12] 酒井孝一『複素数とその関数』(数学ワンポイント双書) 共立出版, 1980.
[13] 酒井榮一『数』(現代数学レクチャーズ A-8), 培風館, 1986.
[14] System5「理論体系ＣＬＣ」 数学セミナー 1985 年 12 月号, 日本評論社, p.73–76.
[15] 鈴木晋一『集合と位相への入門—ユークリッド空間の位相—』（ライブラリ新数学体系 E1）, サイエンス社, 2003.
[16] G. ストラング『線形代数とその応用』, 山口昌哉・監訳, 井上昭・訳, 産業図書, 1978.
[17] 赤攝也『集合論入門』(新数学シリーズ 1), 培風館, 1959.
[18] 竹内外史『集合とはなにか』(ブルーバックス B298), 講談社, 1976.
[19] 田島一郎『解析入門』(岩波全書), 岩波書店, 1981.
[20] 田島一郎『イプシロン・デルタ』(数学ワンポイント双書 20), 共立出版, 1978.
[21] 田島一郎『整数』(数学ワンポイント双書 10), 共立出版, 1977.
[22] 田中一之、鈴木登志雄・共著『数学のロジックと集合論』, 培風館, 2003.
[23] G. チャートランド、A. D. ポリメニ、P. チャン『証明の楽しみ・基礎編–数学を使いこなす練習をしよう–』, 鈴木治郎・訳, ピアソン・エデュケーション, 2004.
[24] リュディガー・ティーレ『証明のすすめ–数学の証明–』, 金井省二・訳, 森北出版, 1990.
[25] 寺坂英孝『初等幾何学　第２版』(岩波全書), 岩波書店, 1973.
[26] 中内伸光『ろんりの練習帳』, 共立出版, 2002.
[27] 中島匠一『代数と数論の基礎』(21 世紀の数学９), 共立出版, 2000.
[28] 日本大学文理学部数学科・編『数学基礎セミナー』, 日本評論社, 2003.
[29] 野崎昭弘「数学的帰納法–核心を眼で見てとらえよう–」数学セミナー, 1975 年 3 月号.（数学セミナーリーディングス『数の世界』数学セミナー増刊, 1982 に所収）
[30] E. ハイラー、G. ヴァンナー『解析教程（下)』, 蟹江幸博・訳, シュプリンガーフェアラーク東京, 1997.
[31] ピーター・M・ヒギンズ『数学がわかる楽しみ』, 吉永良正・訳, 青土社, 2003.
[32] 一松信『複素数と複素数平面』(新数学入門シリーズ３) 森北出版, 1993.
[33] 廣瀬健『数学・基礎の基礎』, 難波完爾・校閲, 海鳴社, 1996.
[34] 細井勉『イプシロン・デルタを理解するために』(数セミ・ブックス３), 日本評論社, 1982.
[35] 本橋信義『新しい論理序説』（すうがくぶっくす 16）, 朝倉書店, 1997.
[36] 増田真郎『応用のための代数系入門』（サイエンスライブラリ 23）, サイエンス社, 1981.
[37] 松村英之『集合論入門』(基礎数学シリーズ５), 朝倉書店, 1966.
[38] 三村征雄『微分積分学 I』(岩波全書), 岩波書店, 1970.
[39] 宮島静雄『微分積分学Ｉ一変数の微分積分—』, 共立出版, 2003.
[40] Ｓ・ラング『解析入門 I, Ⅱ 増補版』, 松坂和夫・片山孝次・訳, 岩波書店, 1968.
[41] S. リプシュッツ『線形代数（上)』(マグロウヒル大学演習シリーズ) 加藤明史・訳, マグロウヒル, 1986.
[42] 数学セミナー増刊『100 人の数学者–ギリシャから現代まで–』, 日本評論社, 1971.
[43] 数学セミナー増刊『数学 100 の発見』, 日本評論社, 1972.

索　引

さ行

た行

な行

は行

ま行

や行

ら行

わ行