情報数学

横浜国立大学助教授／工学博士
今井秀樹著

株式会社 昭晃堂

情報数学

横浜国立大学助教授／工学博士
今井秀樹著

株式会社昭晃堂

昭和57年6月20日　初版1刷発行

著者紹介

今井秀樹（いまいひでき）　工学博士

1943年　松江に生まれる
1966年　東京大学工学部電子工学科卒業
1971年　横浜国立大学講師
現　在　同大学工学部情報工学科助教授

検印省略
著者承認

情報数学

© 著作者　今井秀樹

発行者　阿井國昭
東京都新宿区矢来町48

印刷所　育英印刷深川工場
東京都江東区森下3-10-25

発行所　株式会社　**昭晃堂**

郵便番号162　東京都新宿区矢来町48
振替口座 東京3-139320番
電話(03)269-3449番(代表)

定価 3,400 円

Printed in Japan
日本書籍出版協会会員
自然科学書協会会員
工学書協会会員

(株) 松本製本所

ISBN4-7856-3034-5

まえがき

情報数学は情報工学や情報科学の基礎数学を意味するが，その内容が厳密に定義されている訳ではないし，まして情報数学という一つの学問体系が存在する訳でもない．しかし，現代社会において，情報の伝達，蓄積，処理の技術が目覚ましく発展し，それに対する需要も著しく拡大していく中で，情報数学の必要性はむしろ第一線のエンジニアの間から切実に認識されるようになってきた．もはや，従来の数学的知識では，この分野の技術の進展に対処し得なくなってきたからである．

従来の応用数学は微積分を中心としたものであり，いわば連続・無限がその主役を演じていた．ところが，情報を扱う分野においては，そのほとんどすべての領域で，ディジタル技術が確実にしかも急速に浸透し，そこに新たな主役，離散そして有限が生まれたのである．

情報数学がこの離散・有限で特徴づけられることは，大方の異論のないところであろう．本書においても，離散・有限な対象の数学的取り扱いが主要なテーマとなっている．

本書で取り上げた事項には教養課程の数学と重複する部分も少なくない．しかし，離散的立場から見るとき，それはまた異なった顔を見せてくれる．たとえば第4,5章では線形代数を論じるが，そこでは有限体上の線形代数が一つの柱となっており，教養課程の線形代数とは一味も二味も違ったものとなっているはずである．しかし，本書では，連続・無限なものでも，情報工学，情報科学への応用上極めて重要と思われる事項は敢えて取り上げた．

情報数学のもう一つの特徴は，この応用という点にある．情報数学はあくまで応用数学であり，情報工学，情報科学への応用につながるものでなければならない．端的な表現をすれば，情報数学は道具としての数学である．しかし，その道具を使いこなすためには，基礎からの十分な理解が必要であることはい

うまでもない.

本書では，対象とする読者層として主に，情報工学，情報科学，電子工学，通信工学などの専門課程の学生およびこの分野のエンジニアを考え，このような読者が情報数学を道具として十分使いこなせるようになることを目標とした．このために，羅列的な概説はできるだけ避け，応用上最も重要な事項に絞り，その基礎から応用までを丁寧に述べた．また，直観的な理解が可能となるように豊富な図と例を用いた．さらに，各章末に多数の演習問題，巻末に解答を付して自習にも適するように編集した．これらの例や問題には応用上深い意味をもつものも少なくない.

さて，情報数学の応用分野は極めて多岐にわたるから，何が応用上最も重要であるかは判断の分れるところであろう．ここでは，符号理論，ディジタル回路，ディジタル信号処理，パターン認識への応用を特に意識してテーマの取捨選択を行った．それは，これらの分野において情報数学が非常に有力な武器となり，しかもこれらの分野に関連するエンジニアが情報数学の必要性を最も切実に感じているからである．しかし，このような分野の基礎数学はまた，情報工学，情報科学の他の多くの分野に共通な基盤を与えるものでもある．たとえば，第7章の順序機械は情報工学的考え方の一つの典型を示すものといえよう.

本書は著者の講義ノートをもとに書かれたものであるが，執筆中，巻末にあげた文献を種々参考にさせて頂いた．これらの著者に敬意と謝意を表したい．また，本書執筆の機会を与えて頂いた昭晃堂阿井國昭氏，刊行にあたり大変お世話になった松野久生氏に心から感謝の意を表する次第である.

昭和 57 年 2 月

今　井　秀　樹

目　次

1 代数の基礎

2 群

3 環と体

4 線形代数 I

5 線 形 代 数 Ⅱ

6　束とブール代数

7　順序機械

1

代 数 の 基 礎

本章では，代数の基礎となることがらについて述べる．ここでは，集合，関係と関数，代数系およびこれらに関連する種々の概念の定義が中心となっている．これらは，第2章以下の各章の理論の基礎となるものであるので，十分に把握しておかねばならない．

また，本章の内容は情報数学の基礎となるばかりでなく，情報工学の様々な分野において，その直接の基礎を与える．たとえば，集合と関係は，データ構造やデータベースの理論における最も重要な概念である．

1.1 集　　合

1.1.1 集合の表現

集合（set）は数学で最も基本的な概念であるが，それを厳密に定義することは難しい．直観的にいえば，**元**または**要素**（element）と呼ばれる対象を一つの全体にまとめたものが集合である．この場合，ある対象がその集合に属するかどうかを明確に判別できることおよび二つの対象が同一かどうかを知り得ることが前提となる．

集合 A に属する元の数が有限であるとき，A を**有限集合**と呼び，そうでないとき**無限集合**という．有限集合は，その元をすべて列記することによって表すことができる．すなわち，元が $a_1, a_2, \cdots, a_n$ である有限集合 A は

$$A=\{a_1, a_2, \cdots, a_n\} \tag{1.1}$$

と表せる．このような集合の表現法を**外延的記法**という．無限集合であっても，この外延的記法に準じた表し方をすることがある．非負整数の集合を{0, 1, 2, 3, …}のように表すのはその例である．

集合を表現するもう一つの方法は，集合の元の性質を示すことである．いいかえれば，集合の元が満たすべき条件を示すことによって，集合を表すのである．ここで，Pをある性質としよう．そして，$P(x)$で“xはPという性質をもつ”ということを表すことにする．もちろん，xが具体的に決まれば，$P(x)$が正しいか（真であるか），正しくないか（偽であるか）が判定できなければならない．このとき，性質Pをもつx全体の集合を

$$\{x|P(x)\} \tag{1.2}$$

で表す．いいかえれば，$P(x)$が真となるようなxすべての集合を$\{x|P(x)\}$で表すのである．このような表現法を**内包的記法**という．なお，$P(x)$は**述語**または**命題関数**とも呼ばれる．

内包的記法においては，性質$P(x)$の対象となるxをあらかじめある種のものに制限しているのがふつうである．たとえば，xとして非負整数を考えるとか，実数を考えるとかいうように範囲を決めて論じている．いいかえれば，あらかじめxはある集合の元であると仮定しているのである．この集合を**普遍集合**と呼ぶ．

例として，$P(x)$が“$x^4=1$”である場合を考えよう．すなわち，

$$A=\{x|x^4=1\} \tag{1.3}$$

という集合を考える．これは，$x^4=1$を満たす元xすべてからなる集合である．この場合，普遍集合が非負整数全体の集合であるなら，$A=\{1\}$となるし，普遍集合が整数全体の集合なら，$A=\{1, -1\}$となる．また，普遍集合が複素数全体の集合であるなら，$A=\{1, -1, i, -i\}$となる†．このように，普遍集合として何を考えているかによって，同じ形の表現でも異なる集合を表すことに注意を要する．

さて，aが集合Aの元であることを$a\in A$と書き，そうでないとき$a\notin A$と書く．

† iは虚数単位である．すなわち，$i^2=-1$.

ここで，普遍集合をこの世の中のあらゆる集合の集合とし，

$$R=\{x \mid x \notin x\} \tag{1.4}$$

という集合を考えてみよう．すなわち，自分自身を元として含まない集合すべての集合を R とするのである．もし，$R \in R$ であれば，R は R の元の性質 $x \notin x$ を満たさないから，R に含まれない．すなわち，$R \notin R$ である．一方，$R \notin R$ とすれば，R は R の元の性質を満たすから，$R \in R$ となる．したがって，$R \in R$ と $R \notin R$ とが同等となり，矛盾を生じることになる．これをラッセル (Russel) の逆理という．これは普遍集合として余りにも大きな集合を考えたためである．ここでは，これ以上立ち入らないが，このような矛盾を避けるために，集合の定義を制限した公理的集合論が構成されている．

1.1.2 部分集合とべき集合

集合 A のすべての元が集合 B の元でもあるとき，A は B の**部分集合** (subset) であるといい，$A \subseteq B$ (または $B \supseteq A$) と書く．いいかえれば，$a \in A$ であれば常に $a \in B$ となるとき，A は B の部分集合というのである．

$A \subseteq B$ であり，かつ $B \subseteq A$ であるとき，すなわち，$a \in A$ と $a \in B$ が同等であるとき，集合 A と B は等しいといい，$A=B$ で表す．また，そうでないとき $A \neq B$ と書く．

$A \subseteq B$ であり，$A \neq B$ であるとき，A は B の**真部分集合**という．このとき，特に $A \subsetneq B$ と表すことがある．

さて，元を一つも含まない集合を定義しておくと便利である．これを**空集合** (empty set) といい，ϕ で表す．空集合はすべての集合の部分集合となる．

集合 A に対し，その部分集合全体の集合を A の**べき集合** (power set) と呼び，$\mathcal{P}(A)$ または 2^A で表す．べき集合を 2^A で表すのは，A が有限集合の場合，A の部分集合の総数が $2^{|A|}$ となるからである．ただし，$|A|$ は集合 A の元の数を表す．

ここで，集合 $A=\{a, b, c\}$ の部分集合を考えてみよう．これを表 1.1 に示す．この表の**所属表**の部分の各欄には，その行に対応する部分集合に，その列に対

応する元が含まれているとき1，そうでないとき0が記入されている．このようにして，集合 A の各部分集合は，長さが $|A|$ の0,1のパターン（すなわち，所属表の各行）と対応づけることができる．このことから，有限集合 A の部分集合の総数が $2^{|A|}$ となることが理解できよう．

表 1.1　$\{a, b, c\}$ の部分集合

部分集合	所属表		
	a	b	c
ϕ	0	0	0
$\{a\}$	1	0	0
$\{b\}$	0	1	0
$\{c\}$	0	0	1
$\{a, b\}$	1	1	0
$\{a, c\}$	1	0	1
$\{b, c\}$	0	1	1
$\{a, b, c\}$	1	1	1

1.1.3 集合の濃度

有限集合の大きさを比較するのは簡単である．その元の数を比較しさえすればよい．しかし，無限集合ではそうはいかない．そこで，**濃度**または**基数**（cardinal number）という概念が必要になる．これは，有限集合の元の個数の概念を拡張したものである．

濃度を考えるには，まず集合の間の対等という関係を定義しておかねばならない．集合 A と B があり，A のすべての元がそれぞれ B のただ一つの元に対応づけられていて，しかも，すべての B の元に対し，それに対応づけられている A のただ一つの元が存在するとき†，A と B は**対等**であるといい，$A \sim B$ で表す．

集合 A と B が対等のとき，A と B の濃度は等しいとする．また，集合 A が B の一つの部分集合と対等で，しかも A と B が対等でないとき，A の濃度は B の濃度より小さいとする．

さて，最も簡単な無限集合はすべての自然数の集合 $N=\{1, 2, 3, \cdots\}$ であろう．N と対等な集合を**可算無限集合**または単に**可算集合**という．このような集合は，要するに，そのすべての元に $1, 2, 3, \cdots$ と番号を付けられる集合なのである．この意味で**可付番集合**と呼ぶこともある．

すべての偶数の集合やすべての整数の集合が可算集合であることは明らかであろう．また，すべての有理数の集合も可算集合である．すべての有理数に番号を付けるには，たとえば有理数を次のように並べればよい（簡単のため非負

† すなわち，A から B の上への1対1の写像（全単射）が存在するとき．1.4.1項参照．

の有理数のみを並べる).

$$0, \frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{4}{2}, \frac{3}{3}, \frac{2}{4},$$
$$\frac{1}{5}, \frac{6}{1}, \frac{5}{2}, \cdots$$

ただし，この中から2/2，4/2などのように可約なものは除くとする．

ところで，すべての偶数の集合は，すべての整数の集合の真部分集合であるが，同時にこの両者には1対1の対応があり，対等である．このように，無限集合には，自分自身と対等な真部分集合が存在する．これは，無限集合と有限集合の基本的相違の一つである．

可算集合よりやや無限度の高い，すなわち濃度の大きい集合として，すべての実数の集合 $\boldsymbol{R}$ が考えられる．実際，すべての自然数の集合 $\boldsymbol{N}$ は $\boldsymbol{R}$ の部分集合であり，しかも $\boldsymbol{N}$ と $\boldsymbol{R}$ が対等でないことが次のようにして証明できる．

$\boldsymbol{N}$ と $\boldsymbol{R}$ が対等であると仮定する．このとき，すべての実数に番号が付けられるはずである．そこで，区間 $[0,1)$†の実数に番号を付け，$\{a_1, a_2, a_3, \cdots\}$ で表すものとしよう．このような区間 $[0,1)$ の実数は

$$a_i = 0.\alpha_{i1}\alpha_{i2}\alpha_{i3}\cdots \qquad (i=1,2,\cdots) \tag{1.5}$$

という形の小数で表せるはずである．ただし，α_{i1}, α_{i2}, α_{i3}, …は9以下の非負整数である．ここで，β_i $(i=1,2,\cdots)$ を $\beta_i \neq \alpha_{ii}$ となる9以下の非負整数として，

$$b = 0.\beta_1\beta_2\beta_3\cdots \tag{1.6}$$

という実数を考える．b は明らかに区間 $[0,1)$ の実数であるから，$\{a_1, a_2, a_3, \cdots\}$ に含まれねばならない．ところが，$\beta_i \neq \alpha_{ii}$ $(i=1,2,\cdots)$ であるから，どのような i に対しても，$b=a_i$ となることがなく，矛盾を生じる．したがって，$\boldsymbol{N}$ と $\boldsymbol{R}$ が対等でないことが結論される．なお，この証明においては，a_1, a_2, a_3, …の小数表現において，α_{11}, α_{22}, α_{33}, … という対角線の部分を取り出して証明を行っているので，**対角線論法**と呼ばれる．

† $[a,b)$ は $a \leq x < b$ となる実数 x 全体の集合を表す．また，$[a,b]$ は $a \leq x \leq b$，(a,b) は $a < x < b$ となる実数 x 全体の集合を表す．なお，$[a,b]$ を閉区間，(a,b) を開区間，$[a,b)$ を半開区間という．

以上では，すべての実数の集合 $\boldsymbol{R}$ を考えたが，任意の（空でない）区間に含まれる実数全体の集合は $\boldsymbol{R}$ と対等であり，非可算である．たとえば，$0 \leq x < \varepsilon$ となる実数 x 全体の集合は，ε がどんなに小さくても正の数である限り，すべての自然数の集合よりも（濃度の）大きな集合なのである．

さて，ある集合 A に対し，そのべき集合 $\mathcal{P}(A)$ は A よりも濃度が大きいことが，対角線論法を用いて証明できる．たとえば，自然数の集合 $\boldsymbol{N}$ のべき集合を作れば，実数の集合 $\boldsymbol{R}$ と対等な集合が得られる．さらに，$\boldsymbol{R}$ のべき集合を作れば，$\boldsymbol{R}$ よりも濃度の大きい集合が得られる．この集合は，ある区間で定義された実数値関数全体の集合と対等である．このようにして，べき集合を作っていくことにより，いくらでも濃度の大きい集合を作ることができる．

1.1.4 自然数の集合と数学的帰納法

前項で述べたように，無限集合として最も簡単なものはすべての自然数の集合 $\boldsymbol{N}$ であろうが，これをきちんと定義することは案外難しい．もちろん，すべての元を並べて示すわけにはいかないから，その性質を記述しなければならないのである．

自然数は，物の数を数えることから生まれたものであろう．そこで，“数える”という行為の基本的な要素として，自然数 x をその次の自然数 $x+1$ に対応づけるものを考える．これを x の**後者** (successor) といい，$\sigma(x)$ で表すことにしよう†．ペアノ (Peano) は，この後者を用い，自然数すべての集合 $\boldsymbol{N}$ を次の（1）～（5）の性質を満たすものと定義した††．

（1） $1 \in \boldsymbol{N}$

（2） $x \in \boldsymbol{N} \Longrightarrow \sigma(x) \in \boldsymbol{N}$

（3） $x \in \boldsymbol{N} \Longrightarrow \sigma(x) \neq 1$

（4） $\sigma(x) = \sigma(y) \Longrightarrow x = y$

（5） $\boldsymbol{N}$ の部分集合 S が

（i） $1 \in S$，（ii） $x \in S \Longrightarrow \sigma(x) \in S$

† σ は $\boldsymbol{N}$ から $\boldsymbol{N}$ への関数である．関数については 1.4 節参照．

†† “$\alpha \Longrightarrow \beta$ は” “α ならば β” と読む．

の両方を満たすなら，$S=N$

これらの性質は**ペアノの公理**と呼ばれる．特に（5）は数学的帰納法の原理となるものであり，数学的帰納法の公理とも呼ばれる．

ここで，**数学的帰納法**について述べておこう．$P(x)$ を自然数 x についての性質とする．このとき，次の（i），（ii）から，すべての自然数 x について $P(x)$ が真であることを結論するのが数学的帰納法である．

（i）　$P(1)$ は真である．

（ii）　任意の自然数 x について，$P(x)$ が真であれば，$P(\sigma(x))$ も真となる．

この帰納法を証明するには，$P(x)$ が真となるような自然数すべての集合を考えてみればよい．すなわち，$S=\{x|P(x)\}$ という集合を考えるのである．このとき，ペアノの公理（5）からただちに $S=N$ となることが導ける．

1.1.5 集合の演算

すでに述べたように，集合を論じる場合，あらかじめ普遍集合を設定し，その部分集合について考えるのがふつうである．ここで，普遍集合を U で表すことにしよう．

さて，集合 A に属さない元すべての集合を A の補集合といい，A^c で表す．すなわち，

$$A^c=\{x|x\notin A\} \qquad (1.7)$$

もちろん，この式の x は U の元であり，A^c も U の部分集合である．

また，集合 A,B に対し，A または B の少なくとも一方に含まれる元すべての集合を A と B の**和集合**といい，$A\cup B$ で表す．すなわち，

$$A\cup B=\{x|x\in A\vee x\in B\}^{\dagger} \qquad (1.8)$$

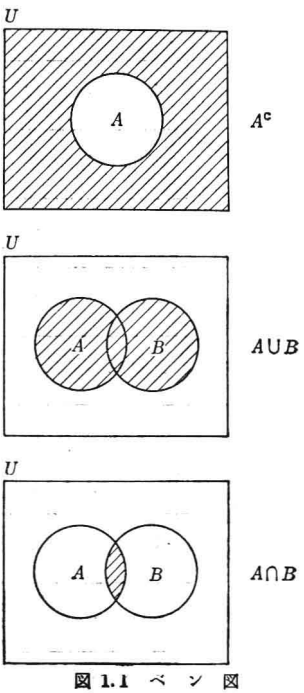

図 1.1　ベ　ン　図

† (p. 7, p. 8) "∨" は "または"，"∧" は "かつ" と読む．