数 理 基 礎 論

担 当 ： 杉 田 公 生

目 次

第1章　数の話

1.1　数学の歴史概略

1.1.1　古代の数学

数学の意味の取り方にもよるが、文明が発達していたということは，(1) 経済基盤である農業における耕地や灌漑の管理，暦、天文観測 (エジプトのような四季のない国では、雨は突然の洪水となって襲ってくるので天文観測は重要な仕事である)，(2) 政府維持のための徴税システム，(3) 都市を形成する城壁、神殿、宮殿、水道などの大規模建築，(4) 通商、などにおいて規模の違いはあっても数学の役割は現代におけるものと大きな違いはなかってであろうから、実用的な意味の数学は紀元前 3 千年前には既に完成されていたとしてもよい。それを裏付ける資料が少ないのであるが。

エジプトの数学に関しては，幸いにパピルスに残された資料があり，分数，１次方程式，主な図形の面積・体積の計算などが知られていたが、論証の概念はなかったようである。分数の考え方も現在とは違っていた。

メソポタミヤの数学に関しては多くの資料があり、現在でも新資料が見つかっているが，多くの天文観測の資料も残されている。内容的には 2 次方程式の根の公式も知られていた。$\sqrt{2}$ の正しい近似計算方法も知られていたようである。円周率も 360 進法の分数を用いて相当の桁まで計算されていた。論証の概念は知られていたという意見もあるが肯定的な資料は知られていないようである。

1.1.2　ギリシャの数学

ギリシャ思想に対しては、19 世紀西ヨーロッパ的偏見という面はあっても、「論理に基づく知識の体系化」を、数学をモデルとして成し遂げたことは間違いのないことである。

(1) タレス (前 624?–前 546?) は最古の記録のある数学者。タレスに続く、ミレトス学派と呼ばれた人々は、「ものの根元 (アルケー) は何であるか」という問いを発して、各々説を唱えたという云う意味で、アリストテレスは哲学の祖とした。
(2) ピタゴラス (前 572?–前 492?) の宗教学園では「万物は数なり」を表題に掲げていて、幾何、数論、音楽、天文などの学科を mathema(学ぶべきもの) と呼んで学んだ。この表題を「数は一切の形あるものの原理である」(ラッセルの解釈) と考えると、 タレス以来の根本原理問題への一つの解であることが云えるし、比較を数で表現するという数の役割を発見したともいえる。
(3) エレア学派 (ゼノン:前 490?–前 429?) は「· · · である。」という命題の証明に「· · · でないとすれば、· · · に反する」という論法を発見したということで、“背理法” の祖とされている。このような論法を発見したゼノンをアリストテレスは “弁証法” の祖とも呼んでいる。また、エレア派は “アキレスと亀” の

ようなパラドックス的命題を多数唱えたということで “詭弁法” の祖ともいわれる。なお、“アキレスと亀” の命題はアリストテレスが現代的な感覚で否定しているが、無限と有限の対比という根本的な解決は日常感覚からは離れたところで議論する必要があることを示している。

(4) プラトン (前 427–前 347) 学派のアカデミヤの門には「幾何学を知らざる者は、この門を潜るべからず」という額が掲げられていたという。数学を含む学問一般の方法論と数学の構成や無理数論も展開。ここでは “mathema(ta)” が “数学” の固有の意味に用いられるようになり、一般思想から独立して行く。

(5) ユークリッド (伝記不明，前 3 世紀のヘレニズム文明の人) の “原本” 13 巻による数学を体系的に集大成。特に、幾何学に関する所謂ユークリッド幾何学の体系は、後世の学問の論理的な体系の見本にもなっている。

1.1.3　インドの数学

インドは古代文明発祥の地の一つであり、現代の数学にも大きな影響を残している。古代インドではバラモン教の影響下にあって、計算の学問という言葉が古い経典にも現れている。ギリシャ幾何学のような論理幾何学は発達しなかったようだが、0 の発見、10 進記数法、代数学が発展しており、無限大・無限小の概念はインド数学に起源があるという説もある。仏教に「ガンジスの砂の数だけガンジスがあり、その砂の数だけの倉にある金銀より、悟りは尊い」という教えがあるそうで、「1, 2, 3 . . . 無限大 (沢山)」という 1 次元に並べた無限大よりも無限大の捕らえ方が壮大である。0 の使用は紀元前 200 年頃からで、現在世界中で使用されている算用数字や記数法はインドの数字が基になっている。数に関する考え方は、現在の考え方と同じだったようである。代数学では記号による計算が用いられていた。

1.1.4　アラビアの数学

7 世紀に興ったイスラム教の歴代の教王達の中には「聖なる知」(コーランの教え) を導くものとして「世俗知」の学問を奨励した人達がいた。ギリシャ数学やインド数学はここで合流し，沢山の教本が作成され、インドから伝わった代数学を発展させた。これらのものが近代ヨーロッパへ受け継がれていった。筆算法や小数点もアラビアから伝わったと云われている。現在の算用数字をアラビア数字というのはこれらの理由からである。

理論的な面ではギリシャ数学の幾何学において確立された証明という考えを代数学にも導入し、等式の移項や両辺から同じものを引いても等式が保たれるという代数的操作の正しさを証明している。これらの操作を表すアラビア語 *al–jabr* がなまって、現在の代数学を意味する algebra に受け継がれている。

1.1.5　中国と日本の数学

古代中国では，一番古い漢字の亀甲文字は数字でないかといわれている。計算方法も “算木” や “九九” も伝説時代に遡ると思われるように “数” はかなり重要な役割を持っていたが、ギリシャ数学のように体系的な数学は生まれなかった。北京紫禁城宮殿の正面には、度量衡の基準単位になる枡と物差しが掲げられている。秦から漢 (前 2 世紀–6 世紀) にかけて、算経十書と呼ばれる教科書が整えられ、漢、唐、宋の官吏登

用試験 (科挙) に用いられた。中でも「九章算術」が重要で，分数、方程、正負の数の演算規則や日常生活での基本的数学知識が説明されている。この時代には円周率として $3.1415927 > \pi > 3.1415926$ や $\frac{22}{7}, \frac{355}{113}$ が知られていたという記録がある。宋、元の時代 (10–14 世紀) にはアラビア文明と接触があり、中国固有の算木を変数の代わりに用いた代数 “天元術” が朱世傑の「算学啓蒙」(1295) に表されている。「算学啓蒙」は単に、計算術の教科書であるだけでなく，数、式、関係の重要性が述べられており，関孝和たちによる現代的な数学の理念の発見の源になっているが、この思想はヨーロッパにおいてはデカルトの思想の基にもなったのではないかと推測されている。宗・元の文明はこの他にもヨーロッパ文明に影響を与えており，バッハの「平均率」の発想の基もこの時代にあることが知られている。明以降、新生ヨーロッパの文明が伝わり、17 世紀にユークリッドの「原本」の訳本が生まれた。geometry を幾何と呼ぶにはこの時に始まる。幾何は geo の音訳で、function を函数と訳したのと同じである。

日本では、「九章算術」は天平時代 (724–749) には伝わっていたようで,「万葉集」(–759?) に九九を使った駄洒落の歌が載っている。(三五十五夜の月、四四が十六匹の類)。算盤は室町時代後期に算木と共に伝わったようである。江戸時代までに天元術も「算学啓蒙」などの書物と共に日本に伝わり、日本独自の記号代数 (天鳳) を発展させている。吉田光由の「塵劫記」(1627 年初版) が当時のベストセラーとなり、現代我々が使用している数の数え方はこの本によっている。関孝和 (1642?–1708)、建部兄弟 (兄賢弘 1664–1739)、久留島義太は “和算” の源になった思想を興した。関孝和らの数学は連立方程式に行列式を世界で初めて導入したなど、当時の世界のレベルより進んだところがあったが、国際的な交流から取り残され論証や体系にまで発展せず，江戸時代末期には芸道のレベルに留まってしまった。

1.1.6 近代の数学

17 世紀の数学 ヨーロッパでは，13 世紀末にルネッサンスが興って近代が始まるが，技術が進歩して学問が興るのは 16 世紀末から 17 世紀になってからである。アラビアの数学がヨーロッパに伝わったのは 12 世紀，中国で発明された紙の製法が伝わったのは 14 世紀である。

この時代に重要なことは，デカルトの「方法叙説」(1637) の付録「幾何学」で述べられている考え方で、数、変数、式の導入と、現象を方程式で表現する大切さをヨーロッパで初めて提唱した。このことは単にデカルトが図形を式で表す “解析幾何学” を提唱したことに止まらず、ギリシャの数学の軛から離脱して現代に続く数理科学の基礎概念の提唱者であることをも意味している。式の変形を使って方程式を扱う考えは、中国の天元術から学んだと言われている。デカルトに続くガリレオの実証主義、パスカル (確率論，数学的帰納法)，ニュートン–ライプニッツ (微分積分法)，等の功績により、自然科学などの合理主義の分野における数学を範疇とする思想と成果へと繋り、神の教えから解き放たれた新生ヨーロッパの誕生とそれに続く近世西欧の繁栄をもたらす基になった。欧米では数学は民主主義の精神的基盤思想として教えられている。

18 世紀の数学 文化史上は啓蒙期と言われる時代である。オイラー，ラプラス，フーリエなどの大数学者がいたが，学問的には，前世紀の方法論をそのまま踏襲していた。

オイラーの所には色々なタイプの数理問題が持ち込まれて、オイラーはそれらを数学の問題として定着させ、多くの定理を得ている。オイラー自身は恐らく自覚していなかったであろうが、当時の数学研究センターにような役割を担ったことになり，現在でも多くの数学の問題が、彼に繋がっている。

19 世紀の数学　19 世紀の数学は，ガウス (数論，代数学)，コーシー (解析学)，等の大数学者を初め色々な分野で，新発見と新しい数学の開拓が続いた。ギリシャ時代の数学で発見された無理数を含む実数論が確立されたのはコーシーの功績である。

ところで、数学者は 17 世紀には思想家であって、本人もそのように行動した。専門の数学者が職業として認められようになったのは 19 世紀になってからである。それでも、ガウスの職業は天文台長であったし、研究対象は数理科学全体に及んでいる。

19 世紀半ばにリーマン (数論，幾何学)，ワイエルシュ トラス (解析学) の登場で，新しい視点からの数学が始まった。これはヒルベルトらに受け継がれ，数学基礎論を生じさせた。

19 世紀後半になり，分岐に重ねて細分化され，一方で隔離された分野の理論が交錯するようになった数学を，統一的に見ることを目的として学会活動が興ったのもこの時期からである。

コワレフスカヤという最初の女流数学者が生まれたのもこの時代である。

1.2　自然数と有理数

数学とは数・式・図形・パターン・関係・構造に関する自然科学である。この講義では、これまで説明した歴史を背景にして,「数」を中心にして考えてみよう。図形については最後の章に少し触れている。

1.2.1　自然数と素数

動物にも 5 つ位までの数の区別がつくらしいといわれている。人間の大人でも直感で判別できる数は 5 つ位までである。人が数の感覚を身につけるのは、幼児が言葉を使いだす頃であろう。

数には、個数を数える、順序を数える、大きさを比較する (何倍)、などの役割があるが、数の初めは**自然数**である。自然数は、$1, 2, 3, \ldots$ のように「次の数」という考えで作られていると考えるのが自然である。数だけではものの区別の目印に使えるであろうが、数学にならない。計算を伴って初めて数学になる。計算とは、何らかの操作により数を関連づけことである。自然数には、足し算と掛け算という計算がある。

足し算は「2 つの篭がある。一方にはリンゴが 5 個あり、他方には 3 個ある。1 つの篭にまとめると幾つ」というように「寄せ算」の考えと、「A さんは 5 番目である。A さんから 3 番先は誰」というように「足し算」の考えが合わさったものである。日本では幸いにこの区別は強調されないようである。言い換えると、自然数は 1 と足し算でできていることになる。

もう一方の基本的な計算である掛け算は、「1 箱に 15 個のリンゴが入っている箱が 12 箱あるとき、リンゴの総数は幾つか」という計算は $15 + 15 + \cdots + 15$ のように足し算を 12 回繰り返すことになるが、これを 15×12 と表し、「掛け算の九九」という暗算法を学校で教わって、計算を高速にしている。即ち,「同じ数の足し算の繰り返し」という考えが基になっている。

掛け算の立場で自然数を作るにはどれくらいの数が必要であろうか。1 の掛け算だけでは 1 しかできないから 2 が必要である。1 と 2 だけでは 2 の冪数しかできないから、3 が必要である。これを続けるのに用語を定義する。自然数 a, b があるとき、他の自然数 c があって $a = b \times c$ と表せるとき、a は b の**倍数**、b は a の**約数**または**因数**であるという。このときに a は c の倍数でもあり、c は a の約数または因数である。

定義 1　$p \geqq 2$ の自然数 p が 1 と p 以外の約数を持たないとき**素数**という。素数でない整数は**合成数**という。

p が素数かどうかを判定する方法に次のような基本的アルゴリズムがある。

1. 2 から p まで (実際は $\sqrt{p}$ まで) の数で割ってみる。最後まで割れなければ素数である。
2. **(エラトステネスの篩)** 2 から p までの番号を書いたカードを用意し、まず、その中で 2 を残し、他の 2 の倍数の番号のカードを除く。次に、残ったカードの中で最小数 (今の場合は 3) を取り、そのカードを残し、その数の倍数のカードを除く。これを最後の (実際は $\sqrt{p}$ の) 番号まで繰り返し、残った数が p 以下の素数である。

最初の方法は数が大きくなると、大変な時間がかかる。エラトステネスの方法は現在でも高速な方法である。素数を作る多項式を求めるという問題もあるが、未解決である。素数がどれ位あるかということは基本的な問題である。

定理 1 素数は無限個存在する。

証明 背理法で証明する。素数が有限個であるとし，それを小さい方から $p_1, p_2, \ldots, p_n$ とする。これ以外の数は合成数であるから，特に p_n より大きい数は合成数である。合成数は因数分解を続ける、これらの素数のどれかで割り切れなければいけない。今、$q = p_1 p_2 \ldots p_n + 1$ とすると、 q は p_n より大きいから合成数である. ところが、$p_1, p_2, \ldots, p_n$ のどれで割っても割り切れない。よって矛盾となる。

記号 n 以下の素数の個数を $\pi(n)$ と表す。

定理 2 (素数分布の定理) n が大きいとき次の近似式が成り立つ。

$$\pi(n) \approx \frac{n}{\log n}$$

$\pi(100) = 25, \pi(1000) = 168, \pi(10^6) = 78498, \pi(10^{12}) = 37607912018, \pi(10^{15}) \approx \dfrac{10^{15}}{\log 10^{15}} = 2.8953 \times 10^{13}$

一方、合成数の場合は $q = rs$ $(1 < r, s < q)$ と因数分解したとき r, s が合成数ならば、それらの因数分解を続けて、因子が素数になるまで因数分解を続けることができる。最後に得られた式は

$$q = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} \ (p_1, p_2, \ldots, p_m \text{は素数})$$

の形になる。この最後の式を**素因数分解**という。素数の定義から次の重要な定理が成り立つ。

定理 3 (素因数分解一意性定理) 素因数分解は一通りしかできない。

素因数分解の定理を使った定理をあげよう。次の性質は無理数の発見の所で使う。

補題 1 n 個の自然数 $\{a_1, a_2, \ldots, a_n\}$ の積 $a_1 a_2 \ldots a_n$ が素数 p で割り切れるならば，この数の内の少なくとも 1 つは p で割り切れる。

証明 p の約数は $1, p$ しかないのだから，p の約数を 2 つ以上の整数に分けることはできない。

補題 2 m, n を自然数，p を素数とする。n が p の倍数であることと，n^m が p の倍数であることは同値である。

証明　上の補題から明らか。

特に，n が 2 の倍数であることと n^2 が 2 の倍数であることは同値である。

素因数分解の定理の応用をもう 1 つ取り上げる。3 : 4 : 5 の辺の比を持つ三角形は直角三角形であることは良く知られている。この整数比をピタゴラス比ということにして，これ以外のピタゴラス比を考えよう。

定理 4 任意の既約なピタゴラス比 $a : b : c$ $(a^2+b^2 = c^2)$ は，$a = m^2-n^2, b = 2m^2n^2, c = m^2+n^2$ $(n, m$ は互いに素の正数) で与えられる。

証明　$(m^2 + n^2)^2 = (m^2 - n^2)^2 + (2m^2n^2)^2$ より，a, b, c がピタゴラス比であることは明らか。

逆に，a, b, c が $a^2 + b^2 = c^2$ を満たす整数とする。$c \neq 1$ であるから $c = m' + n'$ $(m', n' > 0)$ とおける。$c^2 = (m' + n')^2 = m'^2 + 2m'n' + n'^2 = (m' - n')^2 + 4mn'$. 従って、$a = m' - n', c = m' + n'$ とおくと $b^2 = 4m'n'$ が平方数 (二乗数) になればよい。$4 = 2^2$ であるから $m'n'$ に注目して、これを素因数分解して素因数の 1 つを p とする。p は $m'n'$ の中に偶数個なければならないが、m', n' 共に p の倍数であるとすると $c = m' + n', a = m' - n'$ も p の倍数になり既約性に反することになるので，p の偶数べきは m', n' のどちらかに一方に全部含まれなければならない。従って，m', n' 共に平方数となり、しかも互いに素である。$m' = m^2, n' = n^2$ と改めておけば、$b = 2m^2n^2$ となり定理を得る。

1.2.2　有理数

自然数には足し算と掛け算の 2 つの基本演算があった。足し算の逆算法が引き算である。しかし、引き算を用いる計算には 2 つの異なる意味の問題がある。「ここに 10 個のリンゴがある。これから 3 個取ると何個になるか」という問題と、「ここに 7 個のリンゴがある。何個足せば 10 個になるか」という問題がある。最初の例では直接的に「“現在数 − 取り去る数 = 結果″ だから $10 - 3 = 7$ で答えは 7」となる。このとき $(10 - 3) + 3 = 7 + 3 = 10$ であるから「引いた数を加えると元の数になる」という引き算の重要な性質に注意しよう。後者の例では「“加える分 = 合計 − 現在の分” だから引き算をして $10 - 7 = 3$，よって答えは 3」と問題を考え直す必要がある。後者の例では，他に $7 + 1 = 8, 8 + 1 = 9, 9 + 1 = 10$ で 3 個足したから答えは 3 個という考えがある。即ち、$7 + \square = 10$ の $\square$ を求めている。どちらの計算でも「引き算は足し算の逆算法」であることを示している。アメリカで買い物をすると，お釣りは次ぎのように計算してくれる。\$ 22.75 の買い物に \$ 20 札 2 枚を出したとすると，店員は，レシートをおいて,「22.75」，¢25 コインを足して「23」，\$ 1 札を 2 枚足して「24, 25」，\$ 5 札を足して「30」，\$ 10 札を足して「40, Thank you.」と素早く計算してくれる。この計算は後者の方法と同じ考えである。即ち，$22.75 + \square = 40$ の $\square$ を求めている。後者の考えによれば「ここに 7 個のリンゴがある。何個足せば 5 個になるか」という問題の場合に「引き算ができない」という答えより，$7 + \square = 5$ を考えて「2 個引けば良い」という答えが妥当であることが分かるであろう。このようにして $n + \square = 0$, $(n = 1, 2, 3, \dots)$ の答えとして**負の整数** $-1, -2, -3, \dots$ が導入される。自然数、0、負の整数を合わせた数を**整数**という。この結果から「負の数を足せば，それは引き算になる」ことが分かる。負の数を引くとどうなるであろうか。$7 - (-4) = \square$ の両辺に (-4) を加えると、引き算の性質から $\square + (-4) = 7$ と同じである。-4 を加えることは 4 を引くことと同じであったから，$\square = 11 = 7 + 4$。したがって、「負の数を引くことは符号を変えて加えることと同じである」ことが分

かり，整数同士の加減算の計算法が分かった。同時に，整数同士の加減算では新しい数を作らなくても答えが求まることも分かった。

掛け算の逆算法が割り算である。「180 個のリンゴを 12 箱に均等に分けるには、1 箱に何個ずつ入れれば良いか」という問題は「$180 \div 12 = 15$ で答えは 15 個」と教わる。ここで分けたリンゴを集め直すと元に戻る。式では $(180 \div 12) \times 12 = 15 \times 12 = 180$、即ち「割った数を掛けると元の数に戻る」。割り算を使わずに答えを求めてみよう。各箱に 1 個ずつ入れて 12 個、2 個ずつ入れて 24 個、...、15 個ずつ入れて 180 個だから、答えは 15 個と求められる。この計算は $12 \times \square = 180$ の $\square$ を求めている。どちらの意味にしても「割り算は掛け算の逆算法である」ことが分かる。しかし、いつもこのように答えが求まるとは限らない。「10 個のリンゴを 3 人で均等に分けると、1 人当たり何個になるか」という場合は、1 人当たり 3 個では 1 個余り、4 個ではリンゴが不足する。即ち、 $10 = 3 \times 3 + 1$ という関係が成り立っている。一般的に、2 つの自然数 a, b に対して $a = b \times q + r \quad (0 \leqq r < b)$ を満たす非負の自然数の組 (q, r) が唯 1 組あり、q を**商**、r を**余り**または**剰余**という。このように、掛け算が足し算の繰り返しであることに対応して「割り算は引き算の繰り返し」という見方もできる。$r = 0$ のときは「a は b で割り切れる」ことになり、自然数の範囲で答えが求まるが、割り切れない場合はどうすれば均等に分けられるであろうか。この問題の場合は、残りの 1 個を 3 等分して、それぞれが 3 個と、その 1 切れを取ればよい。分割したものを初めの 1 個と区別するために $\frac{1}{3}$ と表して、**分数**の考えと記号が導入される。この問題は初めから 10 個のリンゴを全部 3 等分して、それぞれが 10 切れを取っても同じだから、答えを $\frac{10}{3}$ と表すこともできる。ここで分けたものを集めなおすと、式にすると $10 \div 3 \times 3 = \frac{10}{3} \times 3 = 10$ となるから、割り算の性質が分数にも受け継がれていることが分かる。分数の割り算はどうなるであろう。$\frac{3}{4} \div \frac{5}{7} = \square$ は、割り算の性質から $\square \times \frac{5}{7} = \frac{3}{4}$ と同じである。従って、両辺に 7 を掛けて 5 で割ると $\square = \frac{3}{4} \times \frac{7}{5}$ であるから,「分数の割り算は割る数の分母と分子を入れ替えて掛ければよい」という計算方法が得られた。同時に分数同士の乗除算でも新しい数を作らなくても答えが求まることも分かった。

以上をまとめると負の整数，分数，負の分数を一緒にした数を**有理数**と呼ぶことにして，有理数だけで四則計算が完結している (数学用語では**閉じている**) ことが分かった。

さらに，比較を表すという数の役目の視点から有理数の性質を調べて見よう。直線上に基準点を取り**原点**とする。通常はその右側に点を取り**単位点**とし、原点と単位点の長さを単位長としよう。原点、単位点に $0, 1$ を対応させ、原点より右側、単位長の 2 倍、3 倍、... の点に $2, 3, \ldots$ に対応させる。このとき、足し算に対応する点の移動を考えれば，足した数だけ右へ移動，また、引き算に対応する点の移動を考えれば，引いた数だけ左へ移動することに対応している。従って，引き算の意味を考えれば、$-n = 0 - n$ であるから、原点から単位長左の点が -1、単位長 2 倍の点が $-2, \ldots$ と順に、負の数に対応している。分数は単位長の分数倍の点を対応させれば、直線上の点と有理数の対応ができる。このように直線上の点に数を割り当てた直線を**数直線**と呼ぶ。また、直線上の点に対応する数をその点の**座標**という。

数直線上に 2 つの有理数 $\frac{b}{a}, \frac{d}{c}$ に対応する点を取り，その和を 2 で割った数 $(\frac{b}{a} + \frac{d}{c})/2$ は中点の座標であり，しかも有理数である。したがって，もし数直線の点に隙間があれば，中点を取って埋めていくことにより数直線上の点はすべて有理数で表されるはずである。即ち，

予想 1 有理数の特徴と期待

(1) 有理数の四則計算の結果は有理数になる。(ただし、0 で割ることは除く)
(2) 2 つの有理数の中間点を求めると有理数であるから，有理数のみで直線上の点すべてが表される。

ギリシャ時代の数学では，有理数に関するこれらの性質は良く知られていたことで，ピタゴラス学派のように調和という考えでは、有理数は理想的な数だったはずである。例えば，円周率なども分数で表す努力をしている。例えば、$\left(\frac{4}{3}\right)^4$，$\frac{22}{7}$，$\frac{355}{113}$ などの近似値の計算は、小数点表記法を知らなかった時代には、大変な努力を要したはずである。

1.2.3　身の回りにある計算 (1–四則計算)

日常生活で計算がどのように利用されているかを見てみよう。加減算は買い物をすれば、必ず使用される。複雑なものはバランスシートの計算 (複式簿記) で、負の数も使用される。

掛け算は足し算の繰り返しであると説明したが、掛け算を使わなければ解けない問題に「縦 8 cm、横 7 cm の長方形の面積は何 cm^2 か」というのがある。図形の面積 (cm^2) は、その図形に含まれる 1 cm×1cm の正方形の量を表すで、縦横 1cm 刻みで直線を引いて、そこにできる升目を数えればよいから、計算は確かに繰り返しになるのであるが、リンゴ箱のリンゴの数を数えることとは根本的に異なる計算である。即ち、リンゴ箱のリンゴを数える場合は、リンゴも箱も何の変化も起きないが、面積の場合は 2 つの直線から長方形という新しいものが出現する、文字通り “次元” の異なる問題になる。また、次元の変化を用いると分数の掛け算 $\frac{5}{7}\times\frac{4}{9}=\frac{5\times4}{7\times9}$ も直感的に理解されるであろう。物理学では、“速度 × 時間 = 距離”、“距離 × 力 = 仕事”、“電流 × 電圧 = 電力”、など得られた量に自立した物理的に意味のある “物理量” が沢山あり、それが物理学理解の基礎にもなっているし、近代ヨーロッパ思想の発展につながっていく。

両方のタイプの計算に共通するものがあって、掛け算により数の表す意味が変わるということを一緒に考える必要があることである。日本の初等教育ではこの点の配慮が足りないと云われている。足し算では「5 個のリンゴと 3 個のリンゴを合わせると何個になるか」というときに 5 個＋3 個 = 8 個 のように同じ意味の数を足して、同じ意味の数を求めているので、特に気を使わなくても問題は起きないであろう。一方、掛け算では単位を考えずに計算にだけ注目すると、「1 箱に 15 個リンゴの入った箱が 0 箱ある。リンゴは全部で何個か」という問題に、$0\times0=0$ と考える小学生がいる。単位をつけて表せば、15 個/箱 × 12 箱 = 180 個 と掛け算による単位の変換も分かり、0 箱の場合も 15 個/箱 × 0 箱 = 0 個 と表すことが必然であることが理解できるであろう。さらに、単位を併せて考えれば、数と計算の表す意味を説明することができる。「1 分に 100 m 進めるとき、5 分間にどれだけ進めるか」という問題は 100 m/分 × 5 分 = 500 m と計算されるが、負の時間を過去への遡り、正の距離を前進、負の距離を後退と解釈すると、2 分前には 100 m/分 × (−2) 分 = −200 m で 200 m 後ろにいたことになり、毎分 100 m 後退しているなら、2 分後に (−100) m/分 × 2 分 = −200 m で 200 m 後退し、3 分前には (−100) m/分 × (−3) 分 = 300 m で 300 m 前にいたことが云える。この例は、「マイナス × マイナス = プラス」という “数学者の独善” のようにいわれることも、足し算で負の数が赤字を表すことと同じように、実生活の現象の表現を数と式で表しているに過ぎないことを示している。

専門の数学では、“作用素 × 要素 = 要素” のように、領域 (考察対象) の要素を他の領域の要素に変換することを表したり、“変換 × 変換 = 変換” のように、変換の合成を考えたりするときにも掛け算という言葉を用いている。

1.3 実数

1.3.1 無理数の発見

有理数の世界は、非常に明快で理想の世界だったのであるが、「等積問題」の 1 つである「与えられた正方形の面積を 2 倍にする正方形を求める」という問題で面倒が起きた。「対角辺を 1 辺とする」という解が図で求まるが，有理数で完結していたはずの世界ではこの数の存在はまことに困ることであった。

定理 5 平方が 2 である有理数は存在しない。

証明 背理法による。平方が 2 である有理数が存在するとして，それを $\frac{p}{q}$ とする。このとき p, q は共通因子のない整数としておく。
$\left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2} = 2$ より $p^2 = 2q^2$ ，即ち，p の平方は 2 の倍数である。したがって，補題 2 より p は 2 の倍数となるから $p = 2p'$ となる整数 p' が存在する。これを代入して， $p^2 = 4(p')^2 = 2q^2$，即ち，q^2 も 2 の倍数となる。したがって，q も 2 の倍数になり p, q は共に 2 という共通因子を持つことになるから，仮定に反する。

背理法を考えないと証明が完結しないことにも注意しよう。なお、定規とコンパスで「立方体を 2 倍にする 1 辺を求める」「任意の角を 3 等分する」「円と同じ面積の正方形を求める」 という問題はギリシャ数学の難問と呼ばれている。

1.3.2 有理数と無理数，代数的数と超越数

その後，無理数はさらに 2 つの種類に分類されることが分かった。

定義 2 有理数で表せない数を**無理数**という。また，整数係数の方程式の解となる数を**代数的数**，そうでない数を**超越数**という。

有理数は 1 次方程式の解となるから代数的数である。$\sqrt{2}$ などは代数的数である。5 次以上の方程式の解は冪根で表せないものがあるという定理によれば、冪根で表せない代数的数が無限にある。例えば，$z^7 = 1$ の解は冪根で表せない。円周率 π やネピアの数 e は超越数である。π や e の他に超越数がどれ位沢山あるかを考えるには「集合」の考えを必要とする。

1.3.3 実数の公理

歴史のところで説明したように，実数について詳しいことが理論的に説明できるようになったのは，コーシーの貢献である。しかし，現在においても，実数の捕らえ方は実数を数直線上の点に対応させるなどして実数の持つべき性質を考えて，極限の考えに基づいた公理系を満たすあるものと考えられている。沢山の公理系が考えられていて，それらが互いに同値であることは証明されているが，自然数から整数や有理数と構成したように，既知のものから分り易い方法で実数を構成するという方法は現在でも知られていない。理論的には次に説明する方法で問題はないのであるが，高等学校で微積分が始まったときに急に難しくなったように感じたとしたら理由があったのである。また，実用上も問題があり，例えば，計算機では実数を計算する方法がない。その結果，実は計算機には極限値の計算ができないのである。

公理 1 実数は次の公理系を満たす。

(1) 最大の自然数はない。 (アルキメデスの公理)
(2) 有界な単調数列は収束する。 (連続の公理)

(2) と同値なものとして例えば,「減少区間列は共通点を持つ」,「有界集合は上限と下限を持つ」,「デデキントの切断」などがある。

この公理で,「収束」や「極限」という考えは新しい考えなので，詳しく説明をする。$\frac{1}{3} = 0.\dot{3}$ という等式に関しては疑問を唱える人はいない。同じように $\frac{1}{9} = 0.\dot{1},\ \frac{2}{9} = 0.\dot{2}, \ldots, \frac{8}{9} = 0.\dot{8}$ が左辺の割り算をして得られる。ところが、この続きは $\frac{9}{9} = 1$ で分数はなくなってしまう。このことからも $1 = 0.\dot{9}$ という等式になると納得できない人が沢山出てくる。$0.\dot{9}$ は $\sqrt{2}$ とは違って、複素数と同様に日常世界から既に数学の中に踏み込んでいて、数学的な解釈が必要であることを認識しなければならない。

始めに考えなければならないことは「2 つの数は同じか違うかどちらかしかない」ということで，どちらの式でも等式が成り立たないというのなら，$0.\dot{3}$ と $\frac{1}{3}, 0.\dot{9}$ と 1 に隙間がなければならない。隙間は正の数である。ところが， $\frac{1}{3}$ の場合は、商が 3、余りが 1 といういつまでも続く計算があることを認めた上でその状態を表したのが $0.\dot{3}$ であると習ったはずである。すなわち、$0.333\ldots$ は続ければ $\frac{1}{3}$ に限りなく近づけることを暗黙の内に認めている。$0.\dot{9}$ の場合も 1 と $0.999\ldots$ の差は限りなく 0 に近づけることができるから、この 2 つの等式は同じ考えで成り立つことを認める方が合理的であると考えるのが数学の考えである。次に「等式の左右を入れ替えても等式になる」という等式の基本的性質に注目しよう。$0.\dot{3} = \frac{1}{3}$ というように左右を入れ替えて見ると $0.\dot{3}$ という式に、1 を 3 で割った結果ということから離れて正面から向き合わねばならないことに気がつくであろう。すなわち、$0.\dot{3}$ の数学的な定義を求められる。一番合理的な定義は無限級数として扱うということになり、それによれば $0.\dot{3} = \frac{1}{3},\ 0.\dot{9} = 1$ が言える。副産物として $0.\dot{1} \times 2 = 0.\dot{2}$ などが分数を経由しなくても成り立つことが言えるが、それからも $0.\dot{9} = 0.\dot{1} \times 9 = \frac{1}{9} \times 9 = 1$ がいえる。また、$x^2 = 2$ である数の存在は数直線のモデルから明らかであろうが、この x に対して、数列 $1, 1.4, 1.41, \ldots$ と考えると、分数で表せないある数 x に限りなく近づくことも理解できるであろう。ここでは、自然に無限大や無限小の考えが必要になり、この考えが認められないとすると、ゼノンの “アキレスと亀” のパラドックを認めざるを得ない。

このように $0.\dot{9} = 1$ と同じような状況が起きたときに、ある数に確実に近づくことを保証したのが、連続の公理である。この公理系から得られる**ネピアの数**という重要な極限値を説明する。

補題 3 (2 項定理)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad \text{ここで} \qquad \binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{(n-k+1)\ldots(n-1)n}{k!}$$

定理 6

$\lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n$ が存在する。

証明 $a_n = \left(1+\dfrac{1}{n}\right)^n$ をおく。初めに $a_n < a_{n+1}$ を示す。

$$\begin{aligned}
a_n &= \sum_{k=0}^{n}\binom{n}{k}\left(\frac{1}{n}\right)^k = \sum_{k=0}^{n}\frac{n(n-1)(n-2)\dots(n-k+1)}{k!}\frac{1}{n^k}\\
&= \sum_{k=0}^{n}\frac{1}{k!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\dots\left(1-\frac{k-1}{n}\right)\\
&\leqq \sum_{k=0}^{n}\frac{1}{k!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\dots\left(1-\frac{k-1}{n+1}\right)\\
&< \sum_{k=0}^{n+1}\frac{1}{k!}\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\dots\left(1-\frac{k-1}{n+1}\right) = a_{n+1}
\end{aligned}$$

次に a_n の有界性を示す。

$$a_n \leqq \sum_{k=0}^{n}\frac{1}{k!} \leqq 1+\sum_{k=1}^{n}\left(\frac{1}{2}\right)^{k-1} = 1+\frac{1-1/2^n}{1-1/2} \leqq 3$$

以上で a_n が単調増加で上に有界であることがわかった。従って，公理により極限値が存在する。その値を e とおいたが、この段階では e が有理数であるか，代数的数であるか，既知の数で表せるかわからないが，数の存在は確定されたことになる。

1.3.4 身の回りの計算 (2–冪乗算)

同じ数の足し算の繰り返しが掛け算であったが，同じ数の掛け算の繰り返し計算は冪乗 (べきじょう) または累乗と呼ばれる。$3\times3\times3\times3\times3$ を 3^5 と表す。一般に a を n 回掛けたものを a^n と表す。冪乗を使った計算は身の回りには、非常に沢山ある。日本では江戸時代から “ネズミ算” や “曽呂利新左衛門” の話で知られている計算があるが、預貯金の複利計算、人口増加、経済成長の問題も長期に見た場合累乗の計算になり、その計算の重要性も江戸時代の経済論に取り上げられている。“ねずみ講” が犯罪である理由も冪乗の計算をしてみれば明らかである。その他、用紙の規格も冪乗で定められている。現在日本で使用されている文書用紙には A、B、２つの系列があるが、どちらの系列も半分に折ったときに元の形と相似形になるように縦横比が定められている。この条件を満たす縦横比を求めて見よう。短辺を x、長辺を y とすると、半分に折ると短辺が $y/2$、長辺が x になる。相似の条件から $x:y = y/2:x$、即ち，$x^2 = y^2/2$、従って、$x:y = 1:\sqrt{2}$ となる。A 系列は国際規格 (ISO 規格) で，基準の A0 サイズは面積が $1\mathrm{m}^2$ と定められている。従って，短辺を l とすると、長辺は $\sqrt{2}l$ であるから、この四角形の面積が 1 となるために $\sqrt{2}l^2 = 1$、即ち，短辺は $l = 1/\sqrt[4]{2} =\fallingdotseq 0.84089\mathrm{m}$、長辺は $\sqrt{2}l = \sqrt[4]{2} \fallingdotseq 1.1892\mathrm{m}$ である。また、相似図形の辺の比は面積比の 2 乗根であるから $1/\sqrt{2}$、A4 版の短辺は $0.84089/(\sqrt{2})^4 = 0.84089/4 = 0.2104$, 長辺は $1.1892/4 = 0.2973\mathrm{m}$ である。B シリーズは江戸時代からある奉書紙 (B4 相当) が元になっている。冪乗の計算を利用するために基準の版指数が 1 でなく 0 であることにも注意して欲しい。

自然現象を記述する単位 (指数) にも、地震のエネルギーの大きさを表すマグニチュード、放射性物質の半減期、星の等級など冪乗に基づいたものがあり、音楽の音階の周波数の変化なども冪乗の系列になっている。例えば，地震のマグニチュードは 1 大きければ $31 \fallingdotseq \sqrt{1000}$ 倍のエネルギー、2 大きければ

$\sqrt{1000} \times \sqrt{1000} = 1000$ 倍のエネルギーになるように定められている。マグネチュードが 0.1 大きくなると $(\sqrt{1000})^{0.1} \fallingdotseq (2^5)^{0.1} = \sqrt{2} = 1.41$ 倍、0.2 大きくなると 2 倍エネルギーが強いことになる。放射線を出すラジューム、ウラニュームなどは放射線を出して他の原子に変化し、最終的にはどちらも鉛になって放射線が出なくなり、安定する。これを崩壊というが、放射性を出す原子の個数が崩壊しながら減少して行き、放射性を出す原子の残りの個数が始めの個数の半分になるまでかかる時間を半減期という。ウラニューム、ラジュームの半減期はそれぞれ、45 億年、1600 年であり、我々の宇宙が生まれてから 140 億年経っているというが、ウラニュームは宇宙創世時の原子がまだ　$\left(\frac{1}{2}\right)^3 = \frac{1}{8}$ 残っていて、太陽系が生まれて 45 億年経っているといわれているので、そのときのウラニュームは、まだ半分残っていることになる。炭素 14 などの放射性原子を使って同じ原理で絶対時間を測定する方法がある。星の等級はその明るさを表すが “こと座ベガ” を 0 等星として 1 等級増えると明るさが $1/\sqrt[5]{100} \fallingdotseq 1/2.512$ になるように定められている。負の等級になると反対に明るくなる。満月は -12.6 等級、太陽は -26.7 等級なので、太陽は満月の約 $2.512^{26.7-12.6} = 2.512^{14.1} \fallingdotseq 430000$ 倍明るいことになる。音階では半音毎に同じ割合で上昇するとすると半音 12 回で 1 オクターブ上がることになるから、半音上昇すると約 5.9%(正確には $\sqrt[12]{2}$) 周波数が上昇する。最も、これに忠実に調律すると、ドとミの比が $\sqrt[12]{2}^4 \fallingdotseq 1.2599$、ドとソの比が $\sqrt[12]{2}^7 \fallingdotseq 1.4983$ で有理数比でないから共鳴しないことになるが。このように冪乗の考えは我々の感覚に合った考えである。その他、ロープやケーブルの太さ、電子部品の E 系列規格も冪乗の考えで定められていて、無駄が出ないようになっている。

冪乗計算では $a^n \times a^m = a^{n+m}, (a^n)^m = a^{m \times n}$ の公式が掛け算の回数を計算して得られる。これらを**指数法則**といい、重要な式である。この法則に基づいて指数を自然数から整数、有理数と拡大して、$a^0 = 1,\ a^{-1} = 1/a,\ a^{1/n} = \sqrt[n]{a}$ などが定められる。冪乗の逆が対数である。$2 = 10^x$ 満たす x を $\log_{10} 2$ と表すが，指数と対数は三角関数と同じように数学や実生活にとって基本的な量である。

1.4　複素数

1.4.1　虚数の発見

次に複素数について説明しよう。方程式　$x^2 = -1$　の解は「ない」で実用上は問題が起きない。面積を負にするという問題はどこからも出てこないからである。したがって，初めから数学者が理論的に複素数を考えたのではない。実際に歴史上でも，メソポタミアの数学では現在我々が学ぶ 2 次方程式の解法が知られていたが、負の数の平方根は初めから議論の対象になっていない。インド数学でも同様である。このことは，負の数や分数が初めから日常生活に密着して考えられたことと本質的に同じである。ところが，次のような例が現れて，複素数の存在を認めないと矛盾が解決できなくなった。

初めに，3 次方程式　$x^3 = 3px + 2q$　の解が　$x = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}}$　であることを注意する。(詳しくは後で説明する)　所で，$x^3 - 7x + 6 = (x-1)(x-2)(x+3) = 0$　の解は $1, 2, -3$ であるが，定理に代入すると $p = 7/3,\ q = -3$ なので、根号の部分が $\sqrt{(-3)^2 - (7/3)^3} = \sqrt{9 - 343/27} = \sqrt{-100/27}$ となり，実数を拡張した数を考えないと解が存在しないことになり矛盾を生じる。

1.4.2 複素数の定義と計算

実数を拡張した数を考えるとは，実数の計算と同じ計算規則を持っていて、実数を含むものでなければならない。多項式の扱い (記号計算法) を理解していれば、記号 i を使った 1 次多項式に $i^2=-1$ という規則を追加した数という考えは容易に理解できるものである。この数を**複素数**と名付けた。即ち、複素数は $a+ib$ $(a,b:$ 実数, $i^2=-1)$ と表され，多項式として計算することを定めた数である。ib は**虚数**と呼ばれる。多項式の分数式は有理式であるが、複素数の分数の場合は $(a+ib)(a-ib)=a^2+b^2$ が実数であるから，分母の**共役複素数**(虚数部の符号を変えた数) を分母分子に掛けると分数の i が消えて、複素数の分数も i の 1 次式であることが分かる。したがって、四則計算に関してこれ以上の数の拡張の必要はない。更に，分母に関して「$a^2+b^2=0 \Leftrightarrow a=0$ かつ $b=0$」であるから、0 で割ることは複素数でもできない。

ガウス (1777–1855) は実数が直線の点に対応させられるならば，複素数は 2 つの実数を独立に扱っているので，複素数 $\alpha=a+ib$ と平面の点 (a,b) を対応させた。この対応で

$$(a+ib)+(c+id)=(a+c)+i(b+d)$$

であるから、複素数の加減は原点、点 (a,b)、点 (c,d)、点 $(a+c,b+d)$ の 4 点平行四辺形の作図 (ベクトルの和) に対応している。オイラー (1707–1783) は平面の極座標系を用いて，複素数を $\alpha=r(\cos\theta+i\sin\theta)$ と表した。通常の複素数の表示は $\alpha=a+ib$ であるから，$a=r\cos\theta, b=r\sin\theta$ の関係にある。この表記法により、掛け算に関しては，次の式が成立する。

$$\alpha\times\beta=r(\cos\phi+i\sin\phi)\times s(\cos\theta+i\sin\theta)=rs(\cos(\phi+\theta)+i\sin(\phi+\theta))$$

この式から，原点，1 ，α， β， $\alpha\beta$ に対する点を，それぞれ O， E， A， B， C とすると，三角形 OEA と三角形 OBC は相似になり，複素数の乗除は相似変換に対応することが分かる。応用として、「複数 α に対応する点を原点の回りに 90° 回転させた点は $i\alpha$ に対応する」などが言える。複素数の計算は、平面上の幾何的な説明ができることから、実数の場合よりも分かりやすいことがある。複素数を領域とする解析学は「(複素) 関数論」と呼ばれる。次の定理はこれらの性質を利用した面白い定理である。

補題 4 (ド・モアブル) $\alpha^n=r^n(\cos n\theta+i\sin n\theta)$

次の定理は複素数に関する最も重要な性質である。

定理 7 (代数学の基本定理) 複素係数の方程式の解は複素数である。

略証　任意の複素係数の方程式をとる。この方程式を n 次として

$$f(z)=a_0+a_1z+\cdots+a_{n-1}z^{n-1}+a_nz^n=0 \quad (a_n\neq 0)$$

とおく。$a_0=0$ ならば $z=0$ は $f(z)=0$ の解であるから，$a_0\neq 0$ とする。式を変形して

$$f(z)=z^n\left(a_n+a_{n-1}\frac{1}{z}+\cdots+a_0\frac{1}{z^n}\right)$$

このとき $\max\{a_{n-1},\ldots,a_0\}=A,\ |z|=M>1$ とおくと

$$\left|a_{n-1}\frac{1}{z}+\cdots+a_0\frac{1}{z^n}\right|\leqq|a_{n-1}|\frac{1}{|z|}+\cdots+|a_0|\frac{1}{|z|^n}\leqq n\frac{A}{M}$$

であるから $|z|$ が十分大きいと，この値は 0 にいくらでも近づく。

したがって，z が原点中心の十分に大きい円周上を一回転すると，ド・モアブルの公式から方程式の値は原点の廻りを n 回まわる。一方，$a_0 \neq 0$ であるから，$z = 0$ のときは原点から離れた所にある。従って，$|z|$ が大きいところから 0 へ連続的に縮小すると，$f(z)$ はどこかで原点を通過しなければならない。そのときに $f(z) = 0$ になる。即ち，方程式の解になる。

1.4.3　究極の数

有理数が四則計算に関して終点であり、実数が有理数の極限に関する終点であるように，複素数は代数方程式という点では，終点である。複素数を人工的に拡大して新しい数ができないかと考えたくなるが，複素数はこの点でも終点である。

複素数は 2 次の代数拡大と 2 次元のベクトルとしての拡大という 2 つの面を持っている。代数学の基本定理より，実数よりの 3 次以上の拡大，複素数よりの 2 次以上の拡大はない。ベクトルとしての奇数次元拡大もない。ベクトルとしての 4 次元拡大 (エルミートの四元数) というものができたが，そこでは，掛け算が掛ける順序により結果が変わるという重大な欠点があり，普通の数としては利用できないが、コンピュータグラフィックスや物理学ではエルミートの四元数を使うと計算が便利になる面があるので利用されている分野がある。

これ以上複雑なものは行列で扱う方が分かり易いし、掛け算の結合法則も成立しなくなる。更に、整数は直線上に等間隔に取った点と言うイメージがあるが、代数曲線上に取った点で、和・差・積・商が自然に定義されるものという拡張があり、暗号理論などの応用領域がある。素数や整数に関する理論は「整数論」または「数論」と呼ばれていて、「数学の女王」などとも称される分野である。

第2章　数学の論理と計算機械

2.1　数学の定理と証明

2.1.1　定理の形式

定理は数学的内容の提示であるが，その提示の仕方にも幾つかのパターンがある。それらの概要を説明する。

公式　高等学校までの数学の内容というと，殆どの人が数学を誤解しているように，計算のための「公式」である。公式は「何々を求めよ」式の問題に対する解の計算式を提示したもので，2 次方程式の解の公式のようにパラメータの値を代入して計算すれば、解が得られるので分かりやすい。

存在定理　公式と反対の極にあるといってよいものが「存在定理」である。存在定理では，代数学の基本定理で見られるように，求めるものがどういう条件下で存在するかを示したものであるが，それを求める具体的な方法は、全ての定理が示しているものではない。証明の道筋に解を求める方法が示されている場合もあるが，そういう例ばかりではない。例えば，ピタゴラスの定理 (三平方の定理) の証明方法は 100 通り以上知られているそうであるが、どの証明にも 3 : 4 : 5 以外の整数解の作り方を扱っている証明はない。第 1 章の定理 1 で説明した内容は、直角三角形とは関係がないことを理解しよう。また、代数学の基本定理の証明方法も 100 通り以上知られているそうであるが，解の求め方を具体的に書いたものはない。このことが代数学を難しくしている理由の一つである。一方で、“Fermat の最終定理” は逆に解が無いことを示しているし、“Galois 理論” と呼ばれる 5 次以上の方程式については解の公式がないという定理もある。

高等学校で習う範囲にもこれに類した定理がある。微分積分の基本定理は次の定義と定理からなっている。

定義 3 関数 f に対し，$F' = f$ をみたす関数 F を f の原始関数という。

定理 8 (微分積分の基本定理) 関数 f の原始関数の一つを F とすれば,

$$\int_a^b f\ dx = F(b) - F(a)$$

が成り立つ

この定理では定積分の計算方法を示しているが，肝心の原始関数の求め方は何処にも書いてない。実際，楕円積分といって楕円の長さを求めようとして，従来の枠 (初等解析関数) に入らない関数が発見されたという歴史がある。

アルゴリズム　公式は式に数値を代入して計算するだけであるが、2 次方程式の解の公式のように、判別式で場合分けをしなければならないものをある。さらに、存在定理と違って解は必ず求められるが、解の式がないという場合がある。例えば、1 次の連立方程式の場合、一意解の場合、解なしの場合、無限個の場合と厳密には分ける必要があるが、これは係数を見ただけでは分からない。ただし、一意解の場合は関孝和達が発見した公式がある。このように、公式と存在定理の中間に「アルゴリズム」または「算法」といい，解を求める手続きを示した定理がある。アルゴリズムは存在証明と違い，ある手順に従っていけば、必ず解が求まるか解がないことを保証した定理であるが、公式のように何かの式に代入すればすぐ解が求まるというものでもない。

代表的なアルゴリズムである**ユークリッドの互除法**と呼ばれるアルゴリズムを紹介する。2 つの整数の最大公約数を求めるのために与えられた数をある式に代入すれば最大公約数が求まるという公式はない。
一番簡単に思える方法は、素因数分解をして両方の指数の最小値を指数とする数が最大公約数であるが，これもアルゴリズムの一種であるが，この方法では素数を知っていなくてはならず、しかも非常に時間がかかることが知られている。しかし、次のようにすれば素因数分解ができなくても簡単に求まる。しかも非常に高速であることも知られている。

定理 9 2 つの自然数を a, b (ただし $a > b$) とする。a を b で割った余りを r_1 とする。r_1 は b で割った余りであるから $r_1 < b$ である。即ち，r_1 は b より確実に 1 以上小さい。次に b を r_1 で割った余りを r_2 とする。$r_2 < r_1$ であるから，r_2 は b より確実に 2 以上小さい。次に r_1 を r_2 で割った余りを r_3 とおく。これを続けると，各 1 回の計算で得られる余りは確実に 1 以上小さくなるので，有限回の計算をすれば，必ず余りが 0 になる。即ち，割り切れる。ここで,「最後に割った数が最大公約数である」。

証明　最初の計算の商を q_1 とおくと $a = b \cdot q_1 + r_1$，次の計算の商を q_2 とおくと $b = r_1 \cdot q_2 + r_2$，最後に r_n を r_{n-1} で割って割り切れたとして，その商を q_n とおくと $r_{n-1} = r_n \cdot q_n$ となる。この 1 つ前の計算は，商を q_{n-1} とすると $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$ である。

この式で，r_{n-1} は r_n で割り切れることから r_{n-2} も r_n で割り切れる。その一つ前へ戻って r_{n-3} も r_n で割り切れる。どんどん戻って r_1 も r_n で割り切れ，b も r_n で割り切れ，最後に a も r_n で割り切れる。したがって，r_n は a, b の公約数である。

次に，a, b の任意の公約数を d とおく。最初の式を書き換えて $r_1 = a - b \cdot q_1$ であり，a, b が d で割り切れることから，r_1 は d で割り切れる。次の式を同じように書き換えると $r_2 = b - r_1 \cdot q_2$ であるから，r_2 も d で割り切れる。これを続けて r_{n-1} も d で割り切れて r_n が d で割り切れることになる。従って，$r_n = d \cdot q$ ，よって $r_n \geqq d$ であるから，r_n は a, b の公約数で最大のものであることがわかった。

アルゴリズムの記述法

互除法を擬似プログラム言語 (meta–language) で表すと次のようになる。

```
入力： a, b
出力： a と b の最大公約数 d
アルゴリズム：(互除法)
1:{ r = a mod b （ a を b で割った余り）
2: if r <> 0 then {a = b; b = r （割り切れなかったら，入れ替え）
3:                          goto 1 行目（戻る）;}
4:   else d = b; return d （最後に割ったものが最大公約数）;
5:}
```

次の定理は，この互除法から導かれるものであるが，整数が関係した理論で良く利用するので紹介をしておく。

定理 10 2 つの自然数 a, b の最大公約数を d とする。m, n を任意の整数とすると $am + bn$ は d で割り切れる。とくに，$d = ah + bk$ をみたす整数 h, k が存在する。

証明 前半部は明らかである。

後半部は上記の互除法の証明の後半部から始める．$r_1 = a - bq_1$ を $r_1 = ah_1 + bk_1$ とおく。$r_2 = b - r_1q_2 = b - (ah_1 + bk_1)q_2 = a(-h_1)q_2 + b(1 - k_1q_2)$ これを $r_2 = ah_2 + bk_2$ とおく。以下同様にして $r_i = ah_i + bk_i \quad (i \leqq m)$ とおくと、$r_{m+1} = r_{m-1} - r_m \cdot q_{m+1} = ah_{m-1} + bk_{m-1} - (ah_m + bk_m)q_{m+1} = ah_{m+1} + bk_{m+1}$ ただし、$h_{m+1} = h_{m-1} - h_mq_{m+1},\ k_{m+1} = k_{m-1} - k_mq_{m+1}$．従って，$d = r_n$ も $r_n = ah_n + bk_n$ と表される。$h_n = h,\ k_n = k$ と置けば、定理は証明された。

公式 上の証明で示された h, k の計算式を整理しておこう。

$$h_0 = 0,\ h_1 = 1,\ h_m = h_{m-2} - h_{m-1}q_m \quad k_0 = 1,\ k_1 = -q_1,\ k_m = k_{m-2} - k_{m-1}q_m$$

求める h, k は最大公約数を r_n とするとき $h = h_n,\ k = k_n$.

例

q_1	1	112385	a	108108	b	25	q_2
		108108		106925			
q_3	3	4277	r_1	1183	r_2	1	q_4
		3549		728			
q_5	1	728	r_3	455	r_4	1	q_6
		455		273			
q_7	1	273	r_5	182	r_6	2	
		182		182			
		91	r_7	0			

$h_0 = 0, h_1 = 1, h_2 = h_0 - h_1q_2 = -25, h_3 = h_1 - h_2q_3 = 76, h_4 = h_2 - h_3q_4 = -101, h_5 = h_3 - h_4q_5 = 177,$
$h_6 = h_4 - h_5q_6 = -278, h_7 = h_5 - h_6q_7 = 455$
$k_0 = 1,\ k_1 = -q_1 = -1,\ k_2 = k_0 - k_1q_2 = 26,\ k_3 = k_1 - k_2q_3 = -79,\ k_4 = k_2 - k_3q_4 = 105,$
$k_5 = k_3 - k_4q_5 = -184, k_6 = k_4 - k_5q_6 = 289, k_7 = k_5 - k_6q_7 = -473$

従って，$\mathrm{GCD}(112385, 108108) = 91,\ 112385 \times 455 - 108108 \times 473 = 91$

注意 以上で説明したことは多項式に対しても成立する。

$q_1(x)$	1	$x^3 - 2x^2 - 5x + 6$	$a(x)$	$x^3 + 0x^2 - 7x + 6$	$b(x)$	$-\dfrac{x+1}{2}$	$q_2(x)$
		$x^3 + 0x^2 - 7x + 6$		$x^3 + 0x^2 - \ x + 0$			
$q_3(x)$	$\dfrac{x}{3}$	$-2x^2 + 2x + 0$	$r_1(x)$	$-6x + 6$	$r_2(x)$		
		$-2x^2 + x + 0$					
		0					

$h_0(x) = 0,\ h_1(x) = 1,\ h_2(x) = \dfrac{x+1}{2},\quad k_0(x) = 1,\ k_1(x) = -1,\ k_2(x) = -\dfrac{x-1}{2}$

従って、$\mathrm{GCD}(a(x), b(x)) = -6x + 6,\quad a(x)h_2(x) + b(x)k_2(x) = -6x + 6$

アルゴリズムで示される解法は，このままプログラムにできるところに特徴がある。多くの存在定理ではプログラムにできないのは，そのような存在定理では必ず連続や無限の操作が入るためであり，連続や無限の操作は計算機にできない。厳密には止まらないプログラムはアルゴリズムでないし，正しいときには停止するが，正しくないときは止まるかどうかわからないものもアルゴリズムでない。

2.1.2　証明の方法

論証・証明は数学に限らず、自分の主張の正当性を相手に納得させる大切な議論であるから，どの古代文明においても様々な研究がなされてきた。論証の道筋は「P ならば、Q である」であるが、前提・仮定の P と帰結・結論の Q を関連づける方法に関して、「演繹法」(deduction) と「帰納法」(induction) の主立った方法がある。演繹法は推論・推理ともいわれ、「三段論法」もこの論法に属す。演繹法では前提と帰結は経験などによらず、論理法則のみにより必然的に結びつけられるという点が重要な特徴である。

- 三角形の内角の和は 180° である。従って，正三角形の内角は 60° である。
- 地面が傾けば人も建物も倒れる。世界中どこへ行っても人も建物も倒れていない。従って，世界は平である。
- 指紋は個人毎に異なる。このコップの指紋は A さんのと一致した。従って，A さんはここに来たことがある。

などが、演繹法の例である。

帰納法は幾つかの特殊な事例から一般的な結論を導きだす蓋然的論法である。

- $2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 31$ は素数である。従って，p が素数のとき $2^p - 1$ は素数である。
- 五元素 (木火土金水) 説によると、物が燃えるということは火の要素が加わることである。物が燃えると軽くなる。従って，火の要素は負の重さを持っている。
- 前の人が欠伸をしたら、隣の人が欠伸をした。前にいる犬が欠伸をしたら隣の犬が欠伸をした。従って，欠伸はうつる。

などが帰納法である。帰納法には帰結が成り立たない例を挙げられて「それは特別な場合だ」とか「稀には例外がある」などという言い逃れがある。しかし、例外を更に追求して行けば、正しい結論に到達することが多い。自然科学では実験に基づいて、新しい現象や原理を発見する際に、この論法が用いられてきた。発見には少なくとも再現性が確かめられなければならない。幽霊や UFO が科学になり得ない理由でもある。演繹法ではそのような言い逃れはいえないのであるが，逆にそれを利用して、都合のいい結論だけ利用して前提を無視する議論が罷り通っている。前提が違えば，当然結論は違って来る。この基本的なことを故意に忘れたのが 2009 年に起きたアメリカ発の世界的な大不況である。

この 2 つの正当な論法以外にも人々も納得させる論法がある。ギリシャ時代でも自然現象に対してもゼウスのなせる技という説明が罷り通っていたが、稲妻に関して「空の至る所を駆け回って、稲妻の矢を投げて回るというようなことは、ゼウスの神性にそぐわない (神様のすることでない)」という議論があり、人々は稲妻は自然現象であることを認めるようになったと言われている。量子力学に関してアインシュタインが「神様はサイコロを玩ばない」といったとかの話がある。このような議論は通常は「論外の意見」とされるが、時に正しいことにたどり着くこともある。前者は正しい議論となったが、後者はアインシュタインの負けである。

2.1.3 数学の証明

数学の命題には演繹的な証明があるからこそ，数学的事実を使う際の限界と安全性が保証されている。しかし、帰納的な論法でも提示・証明しようという命題の説明に具体性を示すときに有効な例がしばしばあり、他の自然科学と同様に重要な研究のきっかけになることがある。前の節で挙げた $2^p - 1$ 型の素数はメルセンヌ素数といわれているが、具体的な素数を調べるのに良い例を与える。勿論，取り上げた例が素数であることは別に示す必要がある。このような状況は数理実験と呼ばれる。証明については「数学に王道無し」といわれるように一般論はないが，幾つかのパターンはある。

構成法 一番多い方法は「構成法」で，定理の提示するものを実際に定義から構成する方法である。ただし，どのように構成するかについては一般論はない。ユークリッド幾何の面白いところは補助線の発見であるといわれるように，工夫のし所でもある。

背理法 次に多い方法が「背理法」である。背理法の例は既に示したが，結論を否定してみて，仮定から導かれることに矛盾することを導く方法である。背理法は証明の中で得られたものが全て嘘であるということになるが，大きな定理になると，証明中に構成されたことは他にも利用されるのが普通で，そこにも数学の発展がある。

しらみつぶしの方法 適当な言葉がないが、考えられるすべての場合について命題が成り立つか成り立たないかを検証する方法で、該当する場合の数が有限個の場合にしか適応できない。この証明法のみにより「証明された」問題で有名な例は「四色問題」である。球面を任意に (国別の様に) 区分けした領域を隣接した領域は異なる色分けをするという条件で、必要な最少の色は４色であるという経験則が地図の製造現場で知られていた。それを数学的に証明しようと試みて、現在はコンピュータによりしらみつぶしに調べて４色で済むことは確かめられている。不思議なことに円環面 (トーラス) では７色で十分で、７色が必要な区分けがあることなどが他の曲面で従来の数学的方法で証明されているのであるが。

数学的帰納法 離散現象の証明に良く用いられる証明法が「数学的帰納法」である。自然数 n に関する命題 $P(n)$ がある。「幾つかの n について試してみるといつも成立する。従って，任意の n に対しても成立する。」という論法は帰納的であるが，数学ではこのような論法は証明として認められない。正しい証明は次のように，2 段階で行う。

(1) $P(1)$ が真であることを証明し，

(2) m が n より小さいとき $P(m)$ が真と仮定すれば、$P(n)$ が真であることを証明する。

第 1 段で $P(1)$ が真であることが保証されているから第 2 段で $P(2)$ は真である。すると第 2 段で $P(3)$ が真になる。等々、任意の自然数について $P(n)$ が真であることが言える。

アルゴリズムの含んだ数学的帰納法の例を示す。

定理 11 (ハノイの塔) 板の上に 3 本の棒が立っていて、大きさが全て異なる穴の開いた円盤が n 枚ある。初めにこの n 枚の円盤が 1 本の棒に大きい順に重ねておいてあるものとする。この円盤を次の規則で他の棒に移動する。

- 1 回に 1 枚だけ移動する。
- 全ての円盤は自分より小さい円盤の上にあってはならない。
- 円盤を動かす棒には制限がない。

n 枚の円盤を 1 つの棒から他の棒へ全て移動させるのに必要な最小の回数は $2^n - 1$ 回である。

証明　初めに問題の解法アルゴリズムを紹介する。

アルゴリズム

3 本の棒に印をつけて A,B,C とする。n 枚の円盤は初めに A に重ねてあるものとする。これを C へ移動する。

1. $n-1$ 枚の円盤を B へ移動する。
2. 最後の n 枚目の円盤を C へ移動する。
3. B に移動した $n-1$ 枚の円盤を C へ移動する。

移動回数の確認を数学的帰納法で証明する。

証明

$n = 1$ の場合　1 枚の円盤を移動するのに必要な移動回数は 1 回である。一方、$2^n - 1$ に $n = 1$ を代入すると $2^1 - 1 = 2 - 1 = 1$ であるから、$n = 1$ のときに定理は成立する。

$n > 1$ の場合　$n-1$ 枚の移動に必要な最小移動回数を $2^{n-1} - 1$ 回と仮定する。n 枚の円盤がある場合、上のアルゴリズムに従って、$n-1$ 枚を B へ移動し、最後の n 枚めを C へ移動し、B にある $n-1$ 枚を C へ移動する。全体で移動する回数は

$$(2^{n-1} - 1) + 1 + (2^{n-1} - 1) = 2 \times 2^{n-1} - 1 = 2^n - 1$$

であるから n の場合も定理が成立している。

従って、定理は任意の n の場合にも成立する。

2.2 数学の論理

2.2.1 公理系

論証については前節で説明したが，数学という体系はそれ自身が演繹的に組み立てられている。ギリシャ数学でゼノン学派がパラドックスや背理法のような重要な証明方法を発見し、論理の重要性が認識され、ユークリッド原本のように数学的事項が論理に基づいて体系化された。数学的事実の提示の仕方に “(「定義」) →「公理系」→「定理」→「証明」→「応用」” という一定の形式があることが確立された。ここでは，体系の前提となる公理について詳しく考えてみよう。広辞苑では，公理は「(1) おおやけの道理，(2) ある理論領域で仮定される基本前提。この場合，公理は自明な真理でなく，公理系の取り方によって定まる」とあり、全く相反する意味が並べてある。ここで、他の項目のように (1) が主で。(2) が (1) の派生という訳にはいかない。(1) も (2) も同等である。数学辞典では，公理は「理論の前提としての仮定であり，そこに現れる基本的な用語は定義されない」という広辞苑の (2) のものとしてある。「定義不要」という点にも注意しよう。即ち，公理系をみたすものは自由に定義しても良いのである。

公理系において重要なことは，(1) 列挙した公理が互いに矛盾していないという**無矛盾性**と，(2) その体系においてある公理が他の公理から導かれないという**独立性**，の検証を要することである。さらに、ある数学的対象の公理系を考え、それを満たすものが始めに考えたものしかないとき公理は**完全**であると言われるが，現在完全な公理系を持つ数学的対象は自然数位で、一般には完全性を考慮しない方がよい。

数学においても，初めは「経験で得られた対象」を無定義で設定し,「全く自明と思われる若干の命題」を，その理論の出発点とみなしていたのであるが，長い検証の結果，一番厳しい定義にたどりついた。これらのことに関して，大切な例で説明しよう。

平行線の公理と非ユークリッド幾何学　公理の「全く自明と思われる若干の命題」について、疑問が持たれるようになったのが、ユークリッド幾何学の平行線の公理に関してである。次の説明は「原本 (Stoicheia)」にあるものそのままでなく，Hilbert が再構成したものをさらに単純にしたものである。

初めに,「点」や「直線」についてはその性質をあげて定義として，次の公理系を設けた。

(1) 2 点を通る直線が，ただ一つ存在する。
(2) 線分はどこまでも延長できる。
(3) 任意の円を描ける。
(4) すべての直角は等しい。
(5) 2 本の直線が第 3 の直線と交わり，その一方の側に 2 つの角 (同傍内角）の和が 2 直角よりも小さいときは，それらの 2 直線はその側において交わる。

この公理系を見てすぐ浮かぶ考えは，5 番目の公理が複雑なことで，そのために，この公理が他の公理から導かれるのでないかという疑問がもたれ，長い間研究の対象にされた。19 世紀になって，この公理，即ち，平行線の公理を否定しても他の 4 つの公理に反しない幾何学が構成できることがわかった。

即ち，この公理は「直線外の 1 点を通ってその直線に平行な直線が，ただ一つ存在する」と同じであるが，平行線の存在しない幾何学や無限個存在する幾何学が作られた。これらの幾何は「非ユークリッド幾何学」(ガウスの命名といわれる) と総称されるが，それらは不自然なものではなく，物理学においては自然な世界であることがわかってきた。ただし，このことを理解するためには「直線とは何か」という，もう一つの基本的な問題を考えなければならないのである。

非ユークリッド幾何学が日常的であることを球面を例にして説明して見よう。地図を広げて，成田からアメリカへ飛行機で旅行することを想像して見よう。地図で見る限りは，成田を出発した飛行機はすぐ太平洋へ出て、ハワイの方へ行きそうであるが，実際は，北海道からアラスカの方へ飛ぶ。アメリカから帰って来る時も，ニューヨーク発であろうが， ロスアンゼルス発であろうが，飛行機はアラスカへ向かう。昔，アメリカとソビエトが厳しく対立していた時代，アメリカのソビエトミサイル防衛網のレーダーは北極の方を向いていた。これらの理由は，より近い方向が，そちらの方向であるからである。今度は，地図ではなく地球儀を持って来て，上に挙げた地点を糸で強く結んで見ると，それぞれの糸の線が示しているものが飛行路に近いことが分かるであろう。数学的には，球面上の 2 点と球の中心の 3 点を通る平面による切口が糸で強く結んでできる曲線と同じものである。これを**大円**という。この曲線を球面上の直線の役割をしていることは明らかであろう。所で，赤道上において 2 本の経線は赤道と直角に交わっている。しかし，経線は北極で交わる。同じことが球面上の直線 (大円) に対して成立する。即ち，球面上ではユークリッドの公理の内，(5) 平行線の公理が成立しないのである。もっというと，球面上では平行線が存在しない。

逆に，平行線が無限にあるような曲面も存在する。平面を半分にして，境界の直線も取り除く。この半平面上で境界線上に中心のある半円は，この半平面上の直線の役割を持つ。一つの半円を描き，この半円上にない点を通ってこの半円に交わらない半円は無数にある。

非ユークリッド幾何学の発見は，幾何学のみならず数学全体のあり方を大きく変え，現代数学への大転換点になったのである。

2.2.2　パラドックス

いろいろなパラドックス (逆理)　逆理、逆説 (paradox) を辞書で調べると (i) 一般の判断に反する結果を導く論説があって、その説に反論する正当な根拠が見出しがたい論説、(ii) ある命題とその否定命題が論理上同等と思われる論拠を持って主張され、その誤りが明確に主張できないときは 2 律背反 (antinomy) という、とある。広い意味では矛盾やディレンマを起こすような論法もこの中に入れて良いであろうが、パラドックスと呼ばれるには反論がすぐできないという条件が必要なようである。逆理の重要性は，既にギリシャ時代の数学において「ゼノンの逆理」から背理法が生まれるようになったことでも分かるように，単純思考の落し穴を避けるのに重要な役目を果たす時がある。

パラドックス、矛盾、ディレンマの幾つかのパターンをあげてみよう。東洋でよく知られたパラドックスは「矛盾」である。この場合は上記の「明確に」主張、反論できないという点は割り引いて考えることにする。これは韓非子に書かれた話で

> 楚の国で矛と盾を売る商人がいた。その商人がいうには「この矛は世界で一番強力な矛でどんな盾でも突き通すことができる。また，この盾は世界で一番強力な盾でどんな矛でも防ぐことができる。両方を買えば，天下無敵である」という。通りがかりの人が,「その矛で，その盾を突いたらどうなるか」と云われて答えられなかった。

という故事に基づく。大きな箱という話もある。

> 箱を作ることが好きな王女さまがいて、毎日、綺麗な箱をせっせと作りました。余り沢山箱ができたので、女王様が「その箱を全部箱にしまいなさい」といいました。王女さまは大きな箱を作って全部の箱を入れました。次の日に女王様に「女王様のいう通りにしました」といったと

> ころ、女王様はそこにある箱を指して「その箱はどうしたの」といいました。王女さまは仕方がないので、また大きな箱を作って、... はたして王女さまは女王様のいう通りにできるでしょうか。

簡単に見えるものもある。

> “クレタ人は全部嘘つきだ” とそのクレタ人はいった。

もっと簡単な例は

> 私は無人島に住んでいる。

ワニのパラドックスという話もある。

> ワニが子供を捕らえた。これを食べようとしたときに子供の母親が来て子供を助けてくれと頼んだ。ワニは日頃の悪評判に対抗して、自分が理性的な動物であることを示そうと「これから俺がしようとすることを当てたら救ってやろう」と母親にいった。母親は考えた末「あなたは私の子供を食べるでしょう」といった。母親は子供を救えるであろうか。
>
> このとき母親が「あなたは私の子供を食べないでしょう」といったらどうであろうか。

日常のパラドックス パラドックスの類いは数学以外のあらゆる所で見出すことができ，文学，演劇，落語，では主題の多くを占めている。絵画でもエッシャーの描いたものにはパラドックスを表したものが多数ある。それはパロディーと言われたりディレンマと言われたりしている。著名な例を挙げると， W.Shakespeare の “Hamlet” 中の “To be or not to be, that is a question.” とか，漱石の「草枕」の冒頭にある

> 「山路を登りながら，かう考えた。智に働けば角がたつ。情に掉させば流される。意地を通せば窮屈だ。兎角に人の世は住みにくい。住みにくさが高じると，安い所へ引き越したくなる。どこへ越しても住みにくいと悟った時，詩が生まれて，画ができる。」

などがある。芥川龍之介の「くもの糸」も宗教上のパラドックを扱ったものと言えるであろう。

詩では，谷川俊太郎の作品に “ひとくいどじんのサムサム” という詩がある。「何を食べてもお腹が一杯にならないサムサムが，手当たり次第に何でも食べたが，まだお腹が空いていて最後は自分も食べてしまった」という内容で，大きな箱や次の落語のテーマと同じ類いの発想であろう。

落語の傑作といわれる噺に「頭山」というのがある。

> 「ケチ兵衛さんは “出す” ということが大変嫌いだった。花見も人と同じにするとお金が出て行くというので，花が散ってから一人で桜の名所へ行った。お金もかからず桜桃というおまけもあったが，出すのが嫌いなので桜桃を食べた時も種を出さなかった。次の年、ケチ兵衛さんの頭に桜の木が芽生えた。その桜が見事に育って “頭山の桜” といって名所になり，近所ばかりか遠方からも見物に来るようになった。その騒ぎが余りに大きいので，ケチ兵衛さんは頭山の桜を根こそぎに抜いた。その跡に池ができた。今度は，その池が “頭が池” といって魚釣りや池に写る名月鑑賞といって名所になり，また人が集まってきて頭の上で騒いだ。気の休まらないケチ兵衛さんは “なぜ私だけこんな目に会わなければならないのだろう” と世を儚んで頭が池に身を投げた」

自然界もパラドックに満ちている。摩擦は邪魔なものであるが，摩擦が無くては釘一つ止めることができないし，前に進むこともできない。それどころか，摩擦がないとインクが紙の上などに残らないから，字が書けない。渦が続くためには流体に抵抗があってはならないが，抵抗が無いとそもそも渦ができない。渦ができないとすると音もでないので，話ができない。

パラドックスについて改めて認識する必要があるのは，このパラドックスに気付かないのかまたは作為的なのか、国家や経済の戦略に変形した形であるがしばしば用いられていることである。最初の説明した矛盾のような話があるのは，パラドックスが日常的に現れることを示唆している。例えば，経済のパラドックという問題で、経済に於けるバブル現象をパラドックスで説明しようという論が新聞の投稿欄に掲載されたことがある。投稿者はこの方面では専門家である。「バブルの中にいる当人はバブルであることが認識できないからパラドックスで、バブルは結果であって、防げない」という趣旨であったが、バブル現象は単なる投機というギャンブルの結果であり、参加している者全員が、「誰かがジョーカーを引くであろうが自分ではないし、他人がジョーカーを引いても自分には影響がない」というそもそも成立しない仮定の基に行動した結果であることを認めるべきである。2007 年に起きたアメリカの低所得者向き高利率ローンから発生した金融界の不況も、「不動産の価値がいつまでも上がり続ける」というあり得ない仮定に基づいたヘッジファンドや投資金融の失敗が原因で、ヘッジファンドは「格付け会社の指標に基づいて行動していたから自分たちの責任ではない」といっているし，格付け会社は「他人の (根拠のない) いうことを信用する方が悪い」といっている。そもそも、格付け会社は市場の要求があるから成立しているものであり、その指標が正しいというのも結果を見ていっている (ギャンブルの予想屋) にすぎないのである。その上、格付け自身が格付けして欲しい会社の依頼でなされているから「何をか言わんや」ということになる。経済では、「ギャンブルに乗らないと生きていけない世界が経済の一面であり、こちらの方が現代では避けることができないパラドックである」として一つの原理に全面的に頼った活動に警告を発するか、経済活動全体を複雑系の理論に基づいて経済活動を制御する全く異なる視点からの議論が生まれても良いはずである。根拠や検証なく「科学的な裏付け」とか「数学的手法」とかの冠語をつけた詐欺が国際的規模で堂々とまかり通っている。パラドックの議論は単なる論理学の問題でなく、実は身近にいくらでもあるのであるばかりでなく，物の両面のバランスをとるという良識や常識が求められているのである。

政治の面でも「多数決が民主主義の原理ならば、多数与党は何をしてもよいのか」というパラドックスがあるが、こちらの方は色々の議論がなされている。政治ではパラドックスとは異なる論理の落とし穴に注意を要することが起きてくる。政治では自分の主張が正しいことを示すために、何らかの論理を展開する必要が生じる。「自衛隊は世界の安全な所にしか派遣しない。従って、自衛隊のいる所は安全である」といった首相がいたが、これ程の論法は論外としても、気がつきにくい論法にも注意が必要である。政治の主要な目的は、互いに対立・矛盾する要求のバランスを取ることである。その際に、対立・矛盾した要求を前提に立って議論を進めていって、偏った結論を一見論理的に見える論法で導くということがよく見られる。論理学に「矛盾した公理系からはどのような命題も真であることが証明できる」という定理があることを注意しておこう。

2.3 数学基礎論と計算機械

2.3.1 Cantor の集合論

数学は推論に正しい論理を用いるものと考えられて、自然科学においては数学的に記述され証明されることが推論の正しいことの証明であるという考えが認められるようになった。このことは「数学は科学の言葉である」という言葉で表されることがある。ところがこの数学の証明の正しさを疑う大問題が数学自身から生じた。その契機は Cantor(1895 年) の提唱した**集合**という考え方である。まず，Cantor の考えた集合論から説明しよう。

定義 4 (Cantor) 集合とは我々の直感または思考の対象で，(1) 確定していて，(2) しかも互いに明確に区別されるもの (これを集合の元という) を (3) 1 つの全体としてまとめたものである。

(1) の確定しているとは、集合 A が定義されれば、任意の要素 a を持ってきたときに $a \in A$ または $a \notin A$ のどちらか一方が成立することで、(2) は、任意の 2 つの要素を持ってくれば、$a = b$ または $a \neq b$ のどちらか一方が、成立することで、(3) は、集合 A と B に対し、$A = B$、$A \neq B$、$A \in B$、$A \notin B$ などの議論ができることである。

2.3.2 Russel のパラドックス

集合という考えは自然なものであって、数学自身の記述法として大変強力なものである。現在の数学を集合の記号や考えなしに記述しようとすると、大変分かり難い数学になる。カントールの提唱に対して、新しいものに対する通例の非難中傷があったが、それらはカントールに取っては耐えられなかったであろうが、どちらが正当であるかは時間が経てば明らかになる。しかし、論理的に欠陥があるとなると時間委せにするわけにはいかない。ラッセル (B.Russell) はカントールの集合論対し、次のような逆理があることを発見した。

集合というものを説明する場合は，自然数の集合，実数の集合，連続関数の集合，犬の集合などは $\{n \mid n$ は自然数 $\}$，$\{x \mid x$ は実数 $\}$，$\{f \mid f$ は連続関数 $\}$，$\{x \mid x$ は犬 $\}$ などと表される。カントールの定義によればこれらの集合自身は他の集合の要素として扱うことができる。しかし、$\{$ 自然数 $\} + 1$ は 2 でも 5 でもないように、これらの例では集合自体は自然数でも，実数でも，連続関数でも，犬でもない。このような集合を “普通の集合” と呼ぶこととし，普通の集合全部を集めたものを N で表すと，N は $N = \{x$ は集合 $\mid x \notin x\}$ と表すことができる。

普通の集合の残りの集合を集めて来ると $A = \{x$ は集合 $\mid x \in x\}$ と表すことができて，N も A もカントールの定義する集合の条件に合っているので共に集合である。さて N 自身は普通の集合であろうか，そうでないか考えてみよう。

もし，N が普通の集合ならば，$N \in N$ となるが，これは $N \in A$ を意味するから $N \notin N$ となり矛盾である。反対に、$N \in A$ とすると，A は自分自身を含む集合であるから $N \in N$，これは N が普通の集合であることを意味するから， $N \notin A$ となりやはり矛盾である。

したがって，カントールの定義では自分が属する集合が決定できない集合があることになる。ラッセルのパラドックスについてはラッセル自身が大変悩まされたという。ラッセルのパラドックスの意味するところは，カントールの集合の定義は不十分であるということで，集合の考え自体を否定したものではない。現

在，基礎論では集合を矛盾なく定義するような研究が進められている。その研究では，集合の公理系に 10 個以上の条件が必要である。

2.3.3　数学基礎論

カントールの提唱した「素朴な集合論」に対する「ラッセルのパラドックス」は，カントールの集合論に重大な欠陥があることを明らかにした。一方で，この時点での数学は現在の数学と同じように集合論は数学を統一する有効な概念であることが認識されるようになってきた。そのために集合論が怪しいとなると数学の論理も怪しいという議論が起こり、それを研究する数学基礎論という分野が生まれてきた。

数学基礎論は数学自身を研究の対象にしている学問である。その主題は「数学とは如何なるものであるべきか」ということであるが，基礎論の発生初期から，ラッセル (1872-1970) の論理主義，ブラウエル (1881-1966) の直感主義，ヒルベルト (1862-1943) の形式主義等が対立した。論理主義は,「数学は論理学の 1 分科」と見る考え，直感主義は背理法を認めないで数学に「必要なものはすべて構成されるべき」という考え，ヒルベルトの形式主義は素朴な数学を公理と認めて残りを「形式的な演繹体系」で証明しようというものであった。現在の見方からすれば，これらの考えは互いに補完し合うものであってどれが欠けても数学の論理は成り立たない。

2.3.4　「Hilbert のプログラム」とアルゴリズム

ヒルベルトは「数学の論理の正しさを数学的に証明する」という内容の「ヒルベルトのプログラム」と呼ばれる試みを提唱した。これはこのままの意味で考えると「嘘つきクレタ人のパラドックス」と同じになる。そのために数学の命題を記号論理の方法で形式化し,「有限の立場」でのみの証明法を考えて数学の無矛盾性を証明しようと提案した。ここで有限の立場とは有限回の操作で実行できる事実にのみ基礎を置くということで，簡単に言えば「証明は算術計算のように有限で機械的な手続きでなければならない」ことである。

この考えに対してに対して，ゲーデルは「帰納的関数」という自然数上の基本的な関数のクラスを用いて,「証明の算術化」という概念を数学基礎論に導入した。ここで，証明の算術化というのは「実際に計算可能な」または「それを計算するアルゴリズムがある」ことを意味する。アルゴリズムという考えはライプニップが 17 世紀に初めて提唱したものであると考えることができる。彼は「論理は記号と形式 (記号列) の機械的な操作で説明できる」という考えを提唱した。この意味でライプニッツは「記号論理学」の祖とも呼ばれている。ライプニッツはさらにその操作を実現する機械を歯車などで作ろうとした。アルゴリズムの厳密な定義は次の通りである。

定義 5 ある問題を解決する (広義の) 計算方法が，(1) 有限個の記号により、(2) 有限の長さの記述で表されていて，(3) その方法を有限回繰り返せば問題が解決する，という 3 つの性質を持つとき，**アルゴリズム**という。

ゲーデルはこの証明の算術化の手法を用いて，まず「完全性定理」という定理でヒルベルトのプログラムは妥当なものであることを証明した。しかし，ゲーデルは**不完全性定理**(1931) でヒルベルトのプログラムが破綻する例を示した。それは「自然数の理論を含む形式的体系が有限の立場で与えられ，しかもそれが無矛

盾ならば，その体系の中で形式化された論法だけでは，その体系の無矛盾性は証明できない」というものである。不完全性定理の後にはアルゴリズムが残った。

2.3.5 Turing の計算機械

ゲーデルの提唱にもとづいて，実際に「計算可能」な関数の定式化が試みられた。チューリングはこの問題に対して,「チューリング機械」という仮想機械を考えた。チューリング機械は通常、区画割りされた 1 本のテープ上の記号に従って、状態とテープ上の記号を書き換えて変化する内部制御系で説明される。数学的には $M = (Q, \Sigma, \delta)$ という有限集合上の関数系で説明される。ここで、

Q: 有限集合で、その元は “状態” と呼ばれる。
Σ: 有限集合で、その元は “テープ記号” と呼ばれる。
δ: $Q \times \Sigma \longrightarrow Q \times \Sigma \times \{\text{left, right}\}$ の関数で、“推移関数” と呼ばれる。

が基本的な要素で、$\delta(p, X) = (q, Y, D)$ (D = left or right) は、「内部制御状態が p で、テープ上の記号が X のときに、状態が q に変り、テープ上の記号を Y に書き換えて、読み取りヘッドは右か左へ移動する」と解釈される。関数 δ の変数、値共に有限なので、三角関数や対数関数の関数表のように近似値を表す関数表でなく、有限の関数表で完全に記述される。チューリング機械の実行は、δ の関数表で電話の自動交換機のように完全に自動的に実行される。

チューリングは，更に，多様なチューリング機械を一つのチューリング機械でシミュレートできるということを示した (1936)。この機械を**万能チューリング機械**(universal Turing machine) と呼ぶ。万能チューリング機械の原理は、この機械の入力データとして目的の計算をするチューリング機械の設計図 (推移関数表) を計算データと同時に入力すると，その関数表にしたがって計算を実行するという考えである。この時代には如何なる計算機の影も形も存在しないことに注意して欲しい。この万能チューリング機械の入力データに用いられる設計図 (関数表) が後にプログラム (ソフトウェア) という形で実現されることになる。この万能チューリング機械の考えを現実の計算機にするには，さらに，ノイマンの貢献が必要だった。

2.4 電子計算機

2.4.1 計算道具の歴史

遺跡に出る最初の計算道具は、紀元前 500 年頃の「サラミスのアバカス」と呼ばれる大きな計算盤であり、これは算盤の先祖である。言葉の上でも現在の算盤 (abacus) は平板を意味する abacus が語源と思われ、現在の calculator は小石を意味する calcul が語源と考えられている。

0 の発明，それを使った 10 進の記数法はインド文明の発明である。これらがアラブ文明へ伝えられ，9 世紀のアル・フワリズミーの計算術の教科書によってヨーロッパに伝わったのは 12 世紀のことである。彼の名前はアルゴリズムという言葉へ変形されて伝わっているし，彼の教科書の名前がラテン語に訳されて algebra(代数) の名前が生まれた。現代の記数法がアラビア数字と呼ばれているのはこのような歴史的な由来による。この記数法が普及したのは 16 世紀になってのことと言われている。この記数法が普及するまで，(i) 法律による障害 (アラビア数字を使用した契約書は法律的に無効)，(ii) 0 の意味がヨーロッパ思想には受

け入れられなかった、ことで普及しなかったといわれている。0 に関しては 15 世紀になっても，“何もないものを何故表さなければならないのか” という文献があり，今でも “空 (虚) の思想の恐怖” というプラトン、ヘーゲル以来の思想が生きている。子供向の TV 番組「セサミストリート」で色々な場面で 0 を強調するのが、見ていていつも不思議に感じるが、これも同じ根があるのかも知れない。16 世紀になって，新興の技術や学問に携わる人々が合理的なアラビア式の記数法方法を採用して，それを使用する状況が主流になったがこの世紀ということらしい。

計算法は，計算板，指を用いる，暗算などが用いられたようであるが，現在の筆算が通常化したのは 16 世紀のことで，この時代になると紙も普及して来て，活版印刷術も発明されていた。紙は 2000 年前の中国の発明で 12 世紀にエジプト，アフリカ経由でヨーロッパに伝わった。

17 世紀に入るとガリレオ等の実証的な学問を始め現代に直接つながる文明が発展してきた。複雑になる計算に対応して計算道具の改良・発明が試みられた。ネピアが乗除算を加減算に変える対数計算法 (1612–14) を，パスカルが機械 (歯車) 式計算機 (1642–43) を発明した。ネピアの対数は「天文学者の寿命を十年延ばした」と言われるほど近似計算法としては画期的なものであった。機械式の方はライプニッツの四則計算ができるような改良 (1674) があったが計算をするのはあくまで人間であった。機械式の計算機や対数・計算尺は計算を必要とする研究所、事務所で、つい最近まで使用されていた。

2.4.2　Boole 代数と自動計算機

2 進法と基数変換

計算機で使われる 2 進法について説明する。我々は日常生活で 10 進法以外に色々な表記法を使用している。10 進法とは、$1+1+\cdots+1=1\times 10=10$、$10+10+\cdots+10=10\times 10=100$ のように同じものが 10 個集まったら、桁を 1 つ増やして表すものである。ここで、10 を使用しているのは、何かの必然性があるわけでなく、人の指が 10 本あるからといわれている。時間制度のように 60 進、24 進、12 進、365 進のようにいろいろのものが混じっているのは、物理的必然性と生活実感に基づく習慣によるものであろう。

人工的に定めるときは何進法でもよいが、計算機関係の世界では 2 進法が基本になる。2 進法は、同じものが 2 つ集まると、桁を 1 つ増やすという数え方であるので、2 進法の数え方を 1 から実行すると、

$$1,\ 1+1=10,\ 10+1=11,\ 11+1=10+(1+1)=10+10=100,\ 100+1=101,$$
$$101+1=100+(1+1)=100+10=110,\ 110+1=111,$$
$$111+1=110+(1+1)=110+10=100+(10+10)=100+100=1000,\ \ldots$$

即ち、

$$1,\ 10,\ 11,\ 100,\ 101,\ 110,\ 111,\ 1000,\ \ldots$$

となる。10 進法などと比べて、桁上がりが忙しい。

計算機の分野では、2 進法の他に、8 進法や 16 進法なども使われている。16 進法の場合、同じものが 16 集まったら桁を 1 つ増やすので、9 の次の数を 10 とは表せないから、$0,1,2,\ldots,8,9,\ a,b,c,d,e,f$ (16 個) を使っている。

表 2.1: 10 進 ⟷2 進 (整数の場合)

方法: 2 で割って余り、商を 2 で割って余り

商	余り
$M = 1235$	
$M/2 = 617$	1
308	1
154	0
77	0
38	1
19	0
9	1
4	1
2	0
1	0
0	1
答	10011010011_2
検	$1024 + 128 + 64 + 16 + 2 + 1 = 1235$

整数の場合 ある整数 M を 10 進法、3 進法、2 進法、16 進法で表したとき、各々$d_n d_{n-1} \ldots d_1 d_0$ $(d_i = 0, 1, 2 \ldots 9)$、$t_m t_{m-1} \ldots t_1 t_0$ $(t_i = 0, 1, 2)$、$b_l b_{l-1} \ldots b_1 b_0$ $(b_i = 0, 1)$、$h_r h_{r-1} \ldots h_1 h_0$ $(h_i = 0, 1, 2 \ldots, f)$ であるとすると

$$\begin{aligned} M &= d_n \times 10^n + d_{n-1} \times 10^{n-1} + \cdots + d_1 \times 10 + d_0 \\ &= t_m \times 3^m + t_{m-1} \times 3^{m-1} + \cdots + t_1 \times 3 + t_0 \\ &= b_l \times 2^l + b_{l-1} \times 2^{l-1} + \cdots + b_1 \times 2 + b_0 \\ &= h_r \times 16^r + h_{r-1} \times 16^{r-1} + \cdots + h_1 \times 16 + h_0 \end{aligned}$$

の関係にある。表示法を変えることを**基数変換**という。10 進と 2 進の基数変換を考える。10 進表示を 2 進表示に変えるには、この関係式から 2 で割った余りが、b_0、その商を 2 で割った余りが b_1 などとなる。2 進表示から 10 進表示へは、2 の巾乗を 10 進法で行って、2, 4, 8, 16, ... を掛けて合計する。表 2.1 に計算例を示す。

小数と分数の場合 小数の場合は、基数の負ベキが用いられる。10 進の 0.1 は $\frac{1}{10}$、0.01 は $\frac{1}{10^2}$ などである。従って、整数の場合と同じようにして、ある数 m を 10 進、3 進、2 進、16 進で表したとき、各々 $0.d_{-1}d_{-2}d_{-3}\ldots$ $(d_j = 0, 1, 2, \ldots, 9)$, $0.t_{-1}t_{-2}t_{-3}\ldots$ $(t_j = 0, 1, 2)$, $0.b_{-1}b_{-2}b_{-3}\ldots$ $(b_j = 0, 1)$,

表 2.2: 10 進 ⟷2 進 (小数の場合)

方法: 2 を掛けて整数部、小数部に 2 を掛けて整数部

$m = 0.3$	整数部	小数部	$m = 1/3$	整数部	小数部
$2m = 0.6$	0	0.6	$2m = 2/3$	0	2/3
1.2	1	0.2	4/3	1	1/3
0.4	0	0.4	2/3	0	2/3
0.8	0	0.8	4/3	1	1/3
1.6	1	0.6	⋮	⋮	⋮
1.2	1	0.2			
⋮	⋮	⋮			
答	$0.010011001\cdots_2$	$= 0.\dot{0}\dot{1}00\dot{1}_2$	答	$0.010101\cdots_2$	$= 0.\dot{0}\dot{1}_2$
検	初項 $= 1/4 + 1/32$	公比 $= 1/16$	検	初項 $= 1/4$	公比 $= 1/4$
	$(1/4 + 1/32)/(1 - 1/16)$	$= 3/10$		$(1/4)/(1 - 1/4)$	$= 1/3$
分数	$3 = 11_2,\ 10 = 1010_2$	$11/1010_2$	分数	$1 = 1_2,\ 3 = 11_2$	$1/11_2$

$0.h_{-1}h_{-2}h_{-3}\ldots$ $(h_j = 0, 1, 2\ldots, f)$ であれば

$$\begin{aligned} m &= d_{-1} \times \frac{1}{10} + d_{-2} \times \frac{1}{10^2} + d_{-3} \times \frac{1}{10^3} + \ldots \\ &= t_{-1} \times \frac{1}{3} + t_{-2} \times \frac{1}{3^2} + t_{-3} \times \frac{1}{3^3} + \ldots \\ &= b_{-1} \times \frac{1}{2} + b_{-2} \times \frac{1}{2^2} + b_{-3} \times \frac{1}{2^3} + \ldots \\ &= h_{-1} \times \frac{1}{16} + h_{-2} \times \frac{1}{16^2} + h_{-3} \times \frac{1}{16^3} + \ldots \end{aligned}$$

の関係にある。10 進表示を 2 進表示に変えるには、この関係式から 10 進表示の数に 2 を掛けた整数部分が b_{-1}、その小数部分に 2 を掛けた数の整数部分が b_{-2}、などとなる。基数の小さい方から大きい方へは、基数の小さい方の分数の割り算を大きい方の基数の基で行って合計する。例えば、2 進表示で $0.1_2 = \dfrac{1}{2}$, $0.01_2 = \dfrac{1}{4}$, $0.001_2 = \dfrac{1}{8}, \ldots$ であるから、10 進表示に直すには、各々の分数の 10 進の割り算をすれば良い。表 2.2 に例を示す。

小数部が始めから循環小数の場合は、循環小数のまま 2 倍の計算を行うか，分数表示にしてから例の様にすればよい。

もう一つの方法は，10 進表示の分母分子を夫々2 進表示に変換して，2 進数として割り算しても、同じ結果が得られる。2 進の割り算は商が 0 か 1 なので、簡単のようだが余りの計算が馴れないと面倒である。

ブール代数

ブール代数 (1854) とは, 集合 $\{0, 1\}$ の上に 演算を定義した代数系である。演算は有限集合上の関数であるから演算の種類も有限個になる。1 変数の関数は 4 つあるが自明なものを除くと 0 と 1 を入れ替える関数

(演算) が 1 つ残る。これを not という。2 変数の場合は 16 個あるが対称性を仮定すると 8 個、それから自明のものを除くと 6 個の関数 (演算) が残る。その中で代表的な and, or, eor(exclusive or) を次にあげる。

	not
0	1
1	0

and	0	1
0	0	0
1	0	1

or	0	1
0	0	1
1	1	1

eor	0	1
0	0	1
1	1	0

次に、2 進数表示の足し算の各ケタ毎の計算は次のようになる。計算はケタ上げを併せて表示する。

$$\begin{array}{r} 0 \\ +\ 0 \\ \hline 00 \end{array} \qquad \begin{array}{r} 0 \\ +\ 1 \\ \hline 01 \end{array} \qquad \begin{array}{r} 1 \\ +\ 0 \\ \hline 01 \end{array} \qquad \begin{array}{r} 1 \\ +\ 1 \\ \hline 10 \end{array}$$

上の結果を $x + y = c(x, y) \times 2 + s(x, y)$ と表し，ブール代数の演算表と照らし合わせて見ると

$$c(x, y) = x \text{ and } y \qquad \text{および} \qquad s(x, y) = x \text{ eor } y$$

が得られる。

以上のことは数の計算がブール代数の演算で得られることを示しただけであるが，ブール代数の演算が電気回路で実現できることになると話は少し違ってくる。即ち，計算が電気的に自動的にできることを示しているのである。実際に，スイッチを使ってブール代数の演算がシミュレートできることを説明する。スイッチが on の状態を 1，off の状態を 0 とする。スイッチを直列につないた合成回路は and と同値になる。また，スイッチを並列につないだ合成回路は or と同値になる。not 回路はリレーを使って作れる。また，スイッチを向かい合わせにして交差回路を作るとこれは eor と同値になる。このスイッチは階段の上下や長い廊下の両端で照明を on/off するのに使用されているものと同じである。

初期の頃の電気式計算機は手回し式の計算器の歯車の所を電気回路で真似た物であったようであるが，ブール代数の原理を用いた本格的な自動計算機は Stibitz(1936) が初めて開発したが，その前年に Zuse の 2 進法による自動計算機の特許申請がある。自動計算機とは,「計算データを入力するだけで，後は自動的に計算するもの」である。初めは，リレーが用いられ，ついで真空管を用いて作られ，計算速度は飛躍的に高速になった。しかし，これらの計算機では一度回路を組むと一つの計算式にしか使うことができず，計算式が変わるたびに回路を組み替えなければならなかった。回路の組み換えは，最初はスイッチと配線を組替えて，後にはパッチボードを用いて行った。

2.4.3 万能 Turing 機械と現代の計算機

近年まで，万能チューリング機械の考えを用いて開発された最初のコンピュータは、ノイマンの開発した**プログラム内蔵式計算機** (EDVAC:1947 年頃) であると言われていた。これが現在使われているコンピュータの全ての元祖である。この経緯により，今日の計算機は「ノイマン型計算機」とも呼ばれる。プログラム内蔵式の計算機は、単なる自動計算機とは原理的に違うことをはっきり認識して欲しい。しかし、最近、第 2 次世界大戦中のイギリスの情報機関の全貌が公開される様になって、チューリング自身が、プログラム式のコンピュータを開発して、ドイツ軍のエニグマ暗号の解読に使用していたことが明らかにされて、プログラム式コンピュータの始まりはこちらの機械であることが認められるようになっている。開発年は 1944 年、機械の名前はコロッサス (colossus:ギリシャ神話に出てくる巨人) で、名称通り巨大なコンピュータである。

その後，数学の理論はこのように計算機のハードウェアの研究にとどまらず，ソフトウェアの設計原理にも重要な指針を与えている。しかし,「ソフトウェアの正しさの検証」、「データから意味を読み取る」という問題解決がこの分野における重要な目標であるが，数学的定義の段階でも山ほどの未解決な難問がある。

第3章　複雑系，カオス，フラクタル

これまで，数学の構造や発展の原動力などについて，色々な例で説明してきた。しかし，これらの内容に満足しても，他の自然科学や工学等と比べて何となく不満が残る人もいるのではなかろうか。それは，多分,「数学では全てが整然としていて，しかも静的で動くところがない。数学は自然科学といっているが，自然はもっと複雑・多様で，しかも変化するものである」という感想ではないであろうか。

この章で，非線形の世界といわれる分野の一部を，解析学的に余り踏み込まない範囲で紹介しよう。上のような感想を持っている人はこれから説明する世界をどう見るであろうか。

3.1　カオス

我々の日常活動の世界は、「決定論の世界」と「非決定論の世界」に分けられると考えられる。決定論の世界は、次に起きることや将来の状況が現在の状況により決定されというのが基本である。非決定論の世界は確率論の世界で、サイコロやコイン投げの例で見られるように，現在の状態から次の状態が理論的にも予測ができない世界である。これを数学的に表すと、時間を追って起きる現象 $p_1, p_2, p_3, \ldots$ を一般に**時系列**というが，この時系列中の p_n が p_{n-1} により定まるのが決定論の世界で、定まらないのが非決定論の世界である。我々が決定論という言葉で期待する内容の中には、将来の状況が予測や推測ができるし、スタートが多少違っても将来の状況は余り違わないであろうということも含んでいる。ところが，決定論の世界でありながら，これらの期待に反するように見える世界があることに，最近注目が集まってきた。即ち，次の起きることは決定されているというのに、予測や推測ができないし、スタートが僅かでも違うと将来は全く異なる状況になるという世界が存在する。この世界は、「複雑系」と呼ばれることがある。以下で、複雑系の例を説明しよう。

定義 6 一般に数字の列 $x_1.x_2, \ldots, x_n, \ldots$ が，ある関数 $\varphi(x)$ により $x_{n+1} = \varphi(x_n)$ と決定されているとき $\varphi(x)$ の**力学系**という。この力学系で，初期値 x_0 から初めて次々と決まっていく数列 $x_1, x_2, \ldots, x_n, \ldots$ を，この力学系の**軌道**ということにする。

これらの言葉は，時間変数の微分方程式で定められる力学系から借りてきたもので，時間が連続でなく飛び飛び (離散的) にあると思えばよい。

3.1.1　パイこねの力学系

区間 $[0, 1]$ 上の関数 $\varphi(x)$ を

$$\varphi(x) = \begin{cases} 2x & (0 \leqq x \leqq 1/2) \\ 2 - 2x & (1/2 \leqq x \leqq 1) \end{cases}$$

とする。$0 \leqq x \leqq 1$ のとき $0 \leqq \varphi(x) \leqq 1$ であるから，力学系が定義される。「パイこね」の名前の由来は，パイの生地を作るときに、生地を麺棒で延ばして、その上に粉をふったりバターを塗って折り畳むという動作を繰り返す。これを 1 次元で見て、初めの生地を区間 $[0,1]$ の線分とすると，2 倍に延ばして半分に折り畳むという動作は $\varphi(x)$ により表されているからである。パイこねの目的は、生地に粉とバターが均等に混ざるようにするためであるが、$\varphi(x)$ で区間が均等に混ざって行く様子を次のように見てみよう。

この力学系の軌道 $x_0, x_1, x_2, \ldots$ に対し x_n が $0 \leqq x_n \leqq 1/2$ ならば文字 A に，$1/2 < x_n \leqq 1$ ならば文字 B に置き換えて，軌道に対し A と B の文字列を対応させる。このとき，初期値 x_0 の違いにより色々な文字列ができるが，これに関して次の定理がいえる。

定理 12 写像 $\varphi(x)$ により，区間 $(0,1)$ の点と A と B のすべての文字列の集合の間に一対一の対応がある。

この定理の要点は，

(1) 任意の文字列が一つの関数 $\varphi(x)$ と初期値により決定的に定められること。
(2) 異なった初期値から異なった文字列が得られること。
(3) 初期値が僅かに異なっていたら，得られる文字列はまったく異なったものになること。

であって，これは決定論の世界とも非決定論の世界とも異なる性質をもっている。

定理の証明は，二重の長い帰納法を使って，文字列の先頭から収束区間列を求めればよいが，詳細は省略して，周期的な幾つかの文字列について，初期値を決定する例を説明する。

例

(1) 文字列　ABABABAB...　の場合

初期値を x_0 とする。初めの文字が A であるから，$0 < x_0 < 1/2$，したがって $x_1 = 2x_0$，次の文字は B であるから，$1/2 < x_1 < 1$，したがって $x_2 = 2 - 2x_1 = 2 - 2(2x_0) = 2 - 4x_0$，この後をどうするかであるが，文字列は周期的であるから，この値が x_0 に戻れば，$x_0 \leftrightarrow x_1$ の間で繰り返しが生まれ，ABABAB... の繰り返し文字列が得られる。

したがって $2 - 4x_0 = x_0$ 即ち $x_0 = 2/5$ であればよい。

(2) 文字列　ABAABAABA...　の場合

同様に周期部分に注意すると，$x_1 = 2x_0,\ x_2 = 2 - 2x_1 = 2 - 4x_0,\ x_3 = 2x_2 = 4 - 8x_0 = x_0$ となれば，与えられた繰り返し文字列が得られる。

したがって $x_0 = 4/9$

(3) 文字列　BBABBABBA...　の場合

同様に周期部分に注意すると，
$x_1 = 2 - 2x_0,\ x_2 = 2 - 2x_1 = 2 - 2(2 - 2x_0) = -2 + 4x_0,\ x_3 = 2x_2 = -4 + 8x_0 = x_0$。

したがって $x_0 = 4/7$

これをパイこね運動で見れば、パイの生地は均等に混ざっていくから，生地の色々な点の折り畳まれる様子が、色々な文字列が一見でたらめに生じている様子で見て取れるであろう。

関数 $\varphi(x)$ は，部分的には 1 次関数であるが、全体では 1 次関数ではない。このように 1 次関数からわずかにずれているだけで、複雑な現象が生じている。

3.1.2 ロジスティックスの力学系

Malthus の人口論 17 世紀頃から人口の増加への関心が高まり，統計的な議論がなされた。このことに関して，18 世紀にマルサスが有名なエッセイで「人口は指数的に増えるが，食料の生産は直線的にしか増えないから，深刻な食糧危機が来るであろう」と書いた。このことを数学的にあらわすと，最初の年の人口を N_0、n 年後の人口を N_n、増加率を r とすると

$$N_1 = N_0 + N_0 \times r = N_0(1+r),\ N_2 = N_0(1+r)^2, \ldots,\ N_n = N_0(1+r)^n$$

となり、確に指数関数的に増加する。解析的には、次のように平均変化率の式から、微分方程式を得る。

t 年後の人口を $N(t)$ とすると、人口の平均変化率は

$$\frac{N(t+\triangle t) - N(t)}{\triangle t} = rN(t)$$

ここで、$\triangle t \to 0$ にすると

$$\frac{dN}{dt} = rN$$

この方程式は次の解を持つ。

$$N = N_0 e^{rt}$$

ただし，N_0 は初期の人口を表す。N_n の式と $N(t)$ の式は違うように見えるが、$N(t)$ の 1 次近似が N_n の式になる。

Berharst のロジスティック方程式 ところが，実験室などで昆虫の個体数の変化を調べて見ると，食料や環境に問題が無いようにしていても、個体数は指数的には増えないで，ある段階で増加率が減少することが観測される。ベルハルストは，1840 年頃，これに対して次の人口モデルを提案した。

$$\frac{dN}{dt} = r\left(1 - \frac{N}{K}\right)N = rN - \frac{r}{K}N^2$$

この式は 2 通りの意味付けが考えられる。マルサスの論旨では、増加の割合 (dN/dt) は現在の人口 (N) にのみ比例するという rN の項のみを考えたのに対し、ベルハルストは。第 2 式では増加率は人口が小さいときは増加率は r であるが、人口が増えてくると増加率は減少してきて、ある臨界量 K では人口の増加率が 0 になる、即ち、安定するというモデルを表し、第 3 式では、N の 2 次の項まで考慮したのである。この方程式は後に**ロジスティック方程式**と呼ばれるようになった。

この微分方程式は解析的に解けて，N_0 を初期値として，次の解を得る。

$$N(t) = \frac{KN_0e^{rt}}{N_0e^{rt} + K - N_0}$$

解の曲線は，想定通り初期値 N_0 が 0 に近いときは初めは指数関数的に増加し、やがて増加率が減少して臨界量 K に安定する。初期値 N_0 が大きいときは直線に近い形で増加するが、やがて増加率が減少して臨界量 K に安定するというカーブを描くので、昆虫などの動物の繁殖の実験結果とよくあっている数学モデルということができる。

変動する人口　1941 年，京都大学の昆虫学者，内田氏はマメゾウムシの増殖の研究から，上の結果とは異なる現象に取り組んでいた。マメゾウムシは成虫が卵を産むと成虫が全部死んでしまうので、世代が不連続に交代して増殖するので，上の例が適用できない。それで，世代毎の固体数を数えて見ると，アズキゾウムシの場合，増加率が多少増減しながら増加の相を経て，次に世代毎に増減を繰り返し，その増減の幅が減少して行き，最後に安定数に至るという結果が得られた。

この現象では，時間が連続的に取れないので，ベルハルストの微分方程式の結果を差分方程式にしてみる。差分方程式にするには，ある時間間隔 τ を定めて，軌道　$N(\tau), N(2\tau), N(3\tau), \ldots$ を作り，$N_n = N(n\tau)$ と $N_{n+1} = N((n+1)\tau)$ の関係式を作ればよい。今の場合は，係数を整理すると

$$N_{n+1} = \left(\frac{1}{b + cN_n}\right) N_n$$

という差分方程式が得られる。この関係式を使って，τ を定めて，初期値 N_0 から初めて軌道 $N_0, N_1, N_2, \ldots$ と追っていくと，τ をどのように設定しても，解析解の曲線に完全に乗る。ということは，時間を離散化してもマメゾウムシの現象を説明する数学モデルは，ベルハルストのモデルでないことを表している。

内田氏は，それに対して，次の数学モデルを提案した。

$$N_{n+1} = \left(\frac{1}{b + cN_n} - \sigma\right) N_n$$

この σ の意味については説明がないのであるが，このモデルはマメゾウムシの現象を見事に示した。

更に，ヨツモンマネゾウムシの場合は，安定数に至らず，世代毎に増減を永続的に繰り返すという実験結果を得たが，この場合も b, c, σ を適当に定めると，実験結果と同じグラフが得られた。

3.1.3　カオスの登場

ロバート・メイは，1973 年にこれまで知られていたロジスティック方程式を次のように微分を取る前に、別の形で差分化した。

$$\frac{N(t+\triangle t) - N(t)}{\triangle t} = rN(t) - \frac{r}{K}N(t)^2 = r\frac{(K - N(t))}{K}N(t)$$

ここで，$N(n\triangle t) = N_n$ とおいて次の関係式を得る。

$$N_{n+1} = \left((1 + r\triangle t) - \frac{r\triangle t}{K}N_n\right) N_n$$

さらに

$$x_n = \frac{r\triangle t N_n}{K(1 + r\triangle t)}, \qquad a = (1 + r\triangle t)$$

とおくと，次の式に変形できる。

$$(*) \qquad x_{n+1} = a(1 - x_n)x_n$$

ここで,

$$(**) \qquad f_a(x) = a(1 - x)x$$

とおけば，$0 < a < 4$ のとき，この放物線の高さは $a/4$ であるから，$0 < x < 1$ の各 x に対し，$0 < f_a(x) < 1$ となり，離散力学系

$$(*) \qquad x_{n+1} = f_a(x_n) \qquad (0 < x_0 < 1)$$

が $0 < x < 1$ の範囲で定義されることが分かる。この力学系の a の値による軌道を調べて見ると次のことがいえる。

$0 < a < 1$ の場合 任意の初期値 $0 < x_0 < 1$ に対し $\lim_{n\to\infty} x_n = 0$

$1 \leqq a \leqq 2$ のとき 任意の初期値 $0 < x_0 < 1$ に対し，単調に $\lim_{n\to\infty} x_n = 1 - 1/a$
ここで、$1 - 1/a$ は、直線 $y = x$ と放物線 $y = a(1 - x)x$ の交点である。

$2 < a < 3$ の場合 任意の初期値 $0 < x_0 < 1$ に対し $1-1/a < x_N$ になるまで単調増加であるが，$1-1/a < x_N$ の次は $x_{N+1} < 1 - 1/a < x_{N+2}$。 以後 $1 - 1/a$ を挟んで増減を繰り返し，$\lim_{n\to\infty} x_n = 1 - 1/a$。
ここではマメゾウムシの現象が起きている。

$3 \leqq a < 1 + \sqrt{6}$ の場合 任意の初期値 $0 < x_0 < 1$ に対し，$1 - 1/a < x_N$ までは単調増加であるが，以後 $1 - 1/a$ を挟んで周期 2 の軌道を描く。したがって，極限値はない。
ここではヨツモンマメゾウムシの場合に対応している。

$1 + \sqrt{6} \leqq a < a_c$ の場合 a_c は，あるクリティカルな値 $a_c \approx 3.57$ で，この区間はさらに分割されて，任意の初期値 $0 < x_0 < 1$ に対し，初めの区間の a のとき 4 周期の振動，次の区間の a のとき 8 周期の振動，... (いずれも 2^n の周期) という軌道を描く。

$a_c < a \leqq 4$ の場合 初期値 $0 < x_0 < 1$ の選び方により，色々な軌道を描く。様々な周期の周期運動をしたり，いかなる周期も持たない軌道を描いたりする。更に，初期値に関し，その軌道は非常にセンシティブで，僅かの違いで異なった軌道を描く。
即ち，最初に説明したパイこねに良く似た運動を起こしている。

ロバート・メイは最後の状況を「極めて複雑な軌道」の状態，あるいは「カオティック」と呼んだ。パイこねの関数 $\varphi(x)$ と $f_a(X)$ のグラフは傾向として良く似ている。

3.1.4 Lorenz の乱流の研究

上記の研究とほぼ同時に，もう一つのカオスの研究が物理現象で行われていた。

1963 年に地球物理学者ローレンツは対流の数値実験をするために，次の方程式を考えた。

この式で，X は対流の強さ，Y は対流の上昇流・下降流の温度差，Z は対流の上昇流・下降流の温度分布の差が線形分布から外れている量を表し，どれが 0 であっても対流は起きていないことを表している。

$$\frac{dX}{dt} = -\sigma X + \sigma Y, \quad \frac{dY}{dt} = -XZ + rX - Y, \quad \frac{dZ}{dt} = XY - bZ$$

σ は流体の物理定数，r, b は容器などに関するもので，定数としてよい。

ここで，方程式が変数について 2 次の項が入っていることに注意しよう。

ローレンツはこの方程式の解が r がある値以上であると，一見でたらめに見える軌道を描くのであるが，Z が取る極大値の列 $P_1, P_2, P_3, \ldots$ をとって，平面上に点の列 $(P_1, P_2), (P_2, P_3), (P_3, P_4), \ldots, (P_n, P_{n+1}), \ldots$ をプロットしてみたところ，パイこねで使った三角形が現れた。

3.1.5　カオス

1973 年にメリーランド大学数学のヨーク氏の所へ，地球物理の教授がローレンツの論文を持ち込んできた。ヨーク氏と彼の大学院生リー氏は，このような一見ランダムな現象がどういう条件のもとに起きるかを研究して，次の結果を得た。n 周期の定義から始める。

定義 7 離散力学系 $x_{n+1} = f(x_n)$ において，軌道 $x_0, x_1, x_2, \ldots$ を考える。

(1) ある n があって，$x_n = x_{n+1} = x_{n+2} = \ldots$ となるとき，x_n を**不動点**という。
(2) ある n があって，$x_n \neq x_{n+1} \neq x_{n+2} = x_n = x_{n+4} = \ldots, x_{n+3} = x_{n+1} = \ldots$ となっているとき，即ち，x_n 以降は x_n, x_{n+1} の繰り返しになっているとき x_n を 2 **周期点**という。
(3) $x_n, x_{n+1}, \ldots, x_{n+p-1}$ が全部異なって，$x_{n+p} = x_n$ のとき，即ち，x_n 以降は $x_n, x_{n+1}, \ldots, x_{n+p-1}$ の繰り返しのとき，p **周期点**という。

定理 13 (リー・ヨーク) $f(x)$ を区間 $[0, 1]$ 上の連続関数とし，次の条件をみたすとする。

区間 $[0, 1]$ に次のような 4 つの点 p, q, r, s がある。

$$s \leqq p < q < r \qquad f(p) = q,\ f(q) = r,\ f(r) = s$$

このとき，離散力学系 $x_{n+1} = f(x_n)$ に次の性質が成り立つ。

(1) 自然数 n を任意に選ぶと，n 周期の軌道を持つ初期値 $x_0 \in [0, 1]$ がある。
(2) 周期的でもなく，漸近的に周期軌道にも近づかない軌道を持つ初期値の集合は非可算集合である。

リーとヨークは，この論文の題名を「3 周期はカオスを意味する」と名づけた。

ロバート・メイとリー，ヨークの研究は独立になされたが，1974 年にロバート・メイがメリーランド大学へ偶然に来て行った彼の離散力学系の講演をリーとヨークが聞いたことを機にして，カオスの世界が公表されることになった。

カオス現象は，この他にも非線形の式の現れるところ，特に，微分方程式の解の挙動で古くから多数知られている。また，解析的に求めた解がきれいな形をしているのに，数値計算をするとどんなに精度を上げてもおかしな振る舞いをする解しか求まらない例も知られていて，カオス現象がおきていると思われる。

天気予報の長期予報が全然当たらないのも，これまで説明したカオスの世界に属するからであって，その振る舞いは「バタフライ効果」などと呼ばれている。即ち，蝶々が羽ばたいた程度の気圧の変化で，冷夏にも猛暑の夏にもなる可能性があるということを理論が示しているのである。

3.2 フラクタル

3.2.1 平面，空間を埋め尽くす曲線

直線，曲線，平面，曲面，空間，曲った空間 (というのは想像し難いであろうが，真っ直ぐ運動できない空間) を考えて，これらの共通点，違う点を考えてみよう。一つは真っ直ぐな図形と曲がった図形という分類法である。これはこれらの図形を定義する関数の違いによる分類と見ることができる。もう一つは，これらの図形の点を表すのに必要な独立したパラメータの個数という基準で分類する方法である。この独立したパラメータの個数を “次元” と呼ぶ。直線や曲線は，パラメーター 1 つの連続関数で表せるから 1 次元，平面や曲面を表すには，独立したパラメーターが 2 つの連続関数が要るから 2 次元，空間は 3 次元という考え方である。

ところが，ペアノが 1890 年に区間 $[0,1]$ から三角形全体への連続関数を作った。即ち，三角形全体を埋め尽くす連続曲線があることを示したのである。この曲線は「ペアノの曲線」と呼ばれている。ペアノの曲線により、三角形の点が $[0,1]$ の 1 つの実数で表されたことになり、パラメータの個数を次元と表すと、三角形は 1 次元ということになる。ペアノの結果を見て，ヒルベルトは簡単化して同じ性質を持つ所謂「ドラゴン曲線」を示した。このドラゴン曲線は正方形どころか立方体全部を埋め尽くすこともいえ，従来の考えでは，次元の意味が分からなくなってきた。このような曲線を「空間を埋め尽くす曲線 (space filling curve)」と呼んでいる。

3.2.2 カリフラワーは何次元？

さらに，1890 年にファン・コッホは平面を埋め尽くすところまでは行かないが部分的に 2 次元とも見えるもやもやの部分のある曲線を発表している。この曲線は今日「コッホの曲線」と呼ばれる。同じことを六角形でやると雪の結晶が現れる。同じ頃，ワイエルシュトラスは全ての点で微分不可能でかつ連続という関数を例示していた。微分は元々ニュートンが力学の説明のために導入した考えであったから，ワイエルシュトラスの考えは数学者の遊びであると見なされて，特別注目を浴びなかった。1903 年に日本の現代数学の祖とも言われる高木貞治はワイエルシュトラスの考えを具体的な目に見える関数で示した。この関数のグラフはもやもやの部分からできている曲線である。この関数は、近年「高木関数」と呼ばれるようになった。どちらの曲線も次のような特徴が見て取れる。「細かく見ると何処まで行ってもジグザグの曲線なのだが，全体を見ると何となく広がりを持った 2 次元の図形に見えるところもある」。「見えるカオス」ともいえる。前節のロジスティックスの力学系の極限軌道に関するグラフも同じ性質を持っている。

1970 年頃，マンデルブローがこれらの曲線をコンピュータで描くことによって，海岸線，川筋，山の稜線，樹木の形，シダの葉など自然に見られる複雑な曲線をシミュレートする手段として，**フラクタル**という概念を提案した。その後，コンピューターで絵を描くのが容易になって，このように，曲線なのか，2 次元図形なのか分からない図形が沢山作られるようになり，しかも簡単な原理でパラメータを変えるだけで色々な曲線が作られるようになった。

3.2.3　Hausdorff 次元

1937 年にハウスドルフとベシコビッチはペアノの曲線などの次元を説明するために新しい次元の提案をした。新しい次元によるとペアノ曲線の次元は，正に，2 次元になるのであるが，ここでは**自己相似図形**の場合の定義を示す。

定義 8 図形において，そのある部分が全体の縮小像であるとき，**自己相似**であるという。さらに，全体が自己相似な部分の和になっているときに**自己相似図形**であるという。

自己相似な図形は自然界に多数存在する。樹木，カリフラワー，シダの葉などが典型的なものである。

定義 9 自己相似図形において，全体が縮小率 r の部分図形の N 個の和になっているとすると，この図形の**ハウスドルフ次元** D は次の式で定義される。

$$1 = Nr^D \quad \text{即ち} \quad D = -\frac{\log N}{\log r}$$

例

(1) 直線の場合。線分を n 等分すると，元の線分は細分した線分を n 個集めてくればできるので，上の定義で $N = n, r = 1/n$ を代入して $D = \log n / \log n = 1$ で，直感的な次元に一致する。

(2) 平面の場合。四角形の 1 辺を n 等分すると，元の正方形は細分した正方形を n^2 個集めてくればできるので，$N = n^2, r = 1/n$ を代入して $D = \log n^2 / \log n = 2$ で，これも直感的な次元に一致する。

(3) ヒルベルトの曲線の場合。初めの曲線を $1/2$ に縮めて，4 つつなげば良いので，$D = \log 4 / \log 2 = 2$ 次元で直感的な次元に一致する。

(4) コッホ曲線の場合。自己相似比は $r = 1/3$，縮めた図形を $N = 4$ 個集めてくれば全体がつくれるので，$D = \log 4 / \log 3 = 1.26\ldots$ で直線と平面の中間の図形であることを，ハウスドルフ次元も示している。

(5) カントールの集合。カントールの集合の定義をする。まず，区間 $[0, 1]$ から真ん中の $1/3$ を取り去る。次に，残った $[0, 1/3], [2/3, 1]$ の各々からまた真ん中の $1/3$ を取り去る。これを無限回繰り返してできた図形である。各 1 回の操作で線分の長さが $2/3$ になるのだから，これを無限回繰り返すと残った図形 (集合) の長さは勿論，$\lim_{n\to\infty}(2/3)^n = 0$ なのであるが，この集合には連続の濃度の点が残っている。

何故ならば，カントールの集合は，$[0, 1]$ の点を 3 進数で表したときに，各桁の数が $0, 2$ のものだけを集めてきた集合と同じである。そこで，カントール集合の元 $a = 0.a_1a_2\ldots a_n\ldots$ に $b = 0.b_1b_2\ldots b_n\ldots$ を $a_i = 0 \Rightarrow b_i = 0,\ a_i = 2 \Rightarrow b_i = 1$ と対応させると，この対応は一対一で，b は $[0, 1]$ の元を 2 進数で表したものになっている。この集合のハウスドルフ次元は $D = \log 2 / \log 3 = 0.66\ldots$ である。

(6) シダの葉や樹木を例にしてハウスドルフを計算してみると，枝分かれが多くなって，もやもやの部分が多くなるとこの次元は 2 に近づいてくるし，枝分かれが少なくなって，隙間が多くなるとこの次元は 1 に近くなる。

このように，曲がりくねった図形をハウスドルフ次元で計ると，小数部分が出てくる。フラクタルという言葉は，本来分数を意味するフラクションからマンデルブローが考えた定義である。

3.2.4 Julia 集合と Mandelbrot 集合

これまで説明した自己相似写像を持つ図形のほかに，起源は古いし原理も特別に複雑なものでないが，複素数の世界で起きることをコンピュータで実現してみて初めてその複雑さが見られた集合がある。

ジュリア集合

代数方程式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ の解の近似値を求める方法に**ニュートン法**というのがある。

定理 14 関数 $f(x)$ は，区間 $[a, b]$ を含む開区間において，2 回微分可能で，次の条件をみたすとする。

$$(i)\quad f(a) < 0,\ f(b) > 0 \qquad (ii)\quad f'(x) > 0,\ f''(x) > 0 \quad (a \leqq x \leqq b) \quad (\text{下に凸})$$

このとき $f(x) = 0$ は区間 $[a, b]$ において，ただ 1 つの解 ξ をもつ。また数列 $\{c_n\}$ を

$$c_1 = b, \qquad c_{n+1} = c_n - \frac{f(c_n)}{f'(c_n)} \quad (n > 1) \text{ と定めると} \quad \lim_{n\to\infty} c_n = \xi \quad \text{となる。}$$

さらに，この数列は $|c_{n+2} - c_{n1}| < |c_{n+1} - c_n|^4$ が成り立つので，収束性が非常に良い。

この近似計算の漸化式を条件を無視すると，解に近づく保証はできないのであるが，これを複素数の離散力学系と見て，収束を無視して軌道を求めて見ると，非常に複雑な図形が得られた。

定義 10 複素係数の多項式を $f(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_0$ を考える。ニュートンの計算法で決まる軌道 $\{\zeta_n\}$ を考える。

$$J_f = \mathbf{C} - \{\zeta \in \mathbf{C} \mid \zeta_0 = \zeta,\ f(\lim_{n\to\infty} \zeta_n) = 0\}$$

を**ジュリア集合**という。

即ち，初期値 z_0 の軌道が，$f(z) = 0$ に吸い込まれない点の集まりをジュリア集合という。

ジュリア集合を目で見るために次のようなプログラムを書いてみよう。

(1) (i) 方程式の解を含む長方形，(ii) 小さい正数 ε，(iii) 繰り返し回数，(iv) 各繰り返し数に対して異なる色 (白黒でなくてもよい) を，設定する。
(2) $|f(z_0)| < \varepsilon$ ならば，その点に 0 番の色 (例えば，黒) を塗り，次の初期値へ移動する。
(3) 成立しないときは z_1 を計算し，$|f(z_1)| < \varepsilon$ ならば，1 番目の色を塗り，次の初期値へ移動する。
(4) 成立しないときは z_2 を計算し，$|f(z_2)| < \varepsilon$ ならば，2 番目の色を塗り，次の初期値へ移動する。
(5) これを初めに設定した回数繰り返せば，残った部分 (例えば，白) がジュリア集合の近似領域ということになる。

最終目的が本物のジュリア集合でなく，できてくる図形 (模様) が目的であるから，実際には，色の段階や試行回数等は現物を見て決めれば良い。

Mandelbrot 集合

ジュリア集合でニュートンの計算式を用いたのは，$g(z)$ を単なる多項式として，$z_{n+1} = g(z_n)$ としたのでは，$|z|$ が大きいところでは，発散してしまい (代数学の基本定理で証明した)，逆に小さい所では単調な模様にしかならないためであったが，それを逆手に取ったのがマンデルブロー集合である。

定義 11 複素平面で，複素数 μ をパラメータとする多項式 $f_\mu(z) = z^2 + \mu$ を取り，離散力学系 $z_{n+1} = f_\mu(z_n) = z_n^2 + \mu$ を考える。集合

$$\{\mu \in \mathbf{C} \mid z_0 = 0, z_{n+1} = f_\mu(z_n) \text{ で全ての自然数 } n \text{ に対し } |z_n| \text{ が有界 } \}$$

を**マンデルブロー集合**という。

即ち，$z_0 = 0$ からスタートした軌道が有界の範囲に留まっているようなパラメーター μ の集合がマンデルブロー集合である。この実に不思議な形とした集合を初めて見たのがマンデルブロー (1970 年頃) である。この図形は至る所に自己相似の図形を見出すことができる。この図形も軌道が発散していくパラメータ μ に，発散限界に応じた色を付ければ何とも形容のできない不思議な図形 (模様) が得られる。

第4章　暗号の数理

4.1　暗号

4.1.1　暗号の効用

暗号というと， スパイ， 推理小説， 海賊の宝物埋蔵金などロマンチックなことを想像してしてしまうが，実際は商取引きの最高機密である値段や収穫の情報を競争相手に知られないようにするために，歴史上も古い時代から利用されていたようである。また， 外交や戦争には暗号は必須の道具であり、国策や戦況を左右した例が歴史上多数ある。インターネットを利用して電子的に情報を交換する現代では次のように暗号の効用は情報の安全に関して我々の日常生活でも欠かせないものになっている。

(1) 情報の発信者の確認・認証 (ディジタル署名，パスワード)
(2) 第三者による通信の傍受・盗聴の阻止 (暗号文)
(3) 第三者による通信の改変の阻止 (上の 2 つを兼ねたもの)
(3) 通信相手による情報の改変の阻止 (電子的割り印，ディジタル署名)

その他，電話で「じゃんけん」をする方法 (マジックプロトコル) とか、古代文字の解読や遺伝子の情報解読も夢のある課題で，暗号解読技術の範疇に入るようであるが，暗号の専門家で古代文字の解読に成功した人はいないそうである。遺伝情報は A,G,C,T のたった 4 文字から成り立っているのであるが、遺伝情報に暗号の専門家が関係しているという話も聞かない。古代文字の解読の難しさは，その情報がないことがネックであり，一方，古代文字の解読はその情報を求めるのが目的であるから，言わば暗号のパラドックスになっている領域であるともいえる。

定義 12 暗号 (cryptography) とは通信文が第三者に見つかっても内容が知られないようにする方法を意味する。普通の文章を**平文**，暗号化した文章 (情報) を**暗号文**，暗号文を作る操作を**暗号** (encode) ということにする。また，暗号文を正当な持ち主が元の平文に戻すことを**復号** (decode) といい，盗んだ暗号文を平文に変換を試みることを**解読** (code breaking) するという。

4.1.2　暗号の方式

暗号の方式は次のように分類される。

steganography　文書を隠してしまう方法で、「あぶり出し」,「透かし」， 時代劇で良くある「襟や帯に縫い込む」等があるが，杖や筆などの持ちものに文章を掘り込んで上から蝋を埋め更に塗装をして隠すという手の込んだ方式，通信の使者の頭に入墨で通信文を書き頭髪が伸びるのも待って使者を派遣するという悠長なものもあったと言うが、暗号の第一要件である「その存在を知られないこと」に適した方法ではある。

code　コード方式は、特殊な記号一つずつに意味を定めておいて無意味に見える記号列を作り辞書により解読すると言う方式等が代表的な方法である。この方式は新しい人工言語を作ることに等しく，解読する方の立場は古代文字の解読に類するものであろう。また、ある単語に別の意味を持たせておき，その約束を知らない人には普通の文章であるが，約束を知る人には別の正しい情報が伝わる方式もコード式に分類される。第二次世界大戦末期に連合国のノルマンディ上陸作戦を知らせる暗号文を BBC 放送で大陸にいるレジスタンスにヴェルレーヌの詩「秋の日のヴィオロンのためいきの」で知らせたという話は良く知られている。これらの方法は特別な装置が不要で便利に思えるが、最も複雑なコード式にしても暗号化の対象範囲が広がればそれだけ辞書は大きくなるし秘密が洩れるチャンスが増える。解読者にコード表が渡れば暗号の機能はなくなる。極端な場合をいうと、知らない外国語はその人にとっては暗号であるが, 最近になり第二次世界大戦中のアメリカ・イギリスの諜報に関する情報が解禁になって、アメリカ・イギリスの暗号解読法や暗号法が知られるようになってきたが、日本軍がアメリカ軍の暗号を解読していたことの対策としてアメリカインディアン・ナバホ族の言葉を暗号に使っていたということが明らかにされた。これ以後, 日本側はアメリカ軍の暗号解読が不可能になったといわれている。暗号文を送る方も受ける方もナバホ族の人を使って，彼らは code talker と呼ばれていたという。

転置式　転置式は，後ろから書いたり，斜め書きにしたり、平文を折り返して混ぜたりすると意味の無い文字列が得られる。平凡社の百科事典によると，日本では神武天皇が前後倒置式の暗号を使用したという。古くは，ペロポネソス戦争 (紀元前 431– 紀元前 404) にスパルタの将軍リュサンドスは指揮杖に帯を巻いて横に文書を書き帯を解くと暗号文になるという方法 (skytale) を使ったと言う記述がある。また，戦国時代の大将たちはそれぞれ独自の転置式の暗号方式を工夫していたようである。転置式も工夫すると隠し文字に似た効果を得ることができる。

cypher　換字式とも言われ、通信文を何らかの方法で別の文字や数字に置き換えてしまう方法である。通信文の内容や長さに制限がない。実際に使われる暗号はこれらの方法の 1 つに限られることはなく、コードで作った暗号文を換字をしたり、それをさらに転置したりと、いろいろな工夫をして使用されている。

4.2　cypher 暗号

上記の分類で cypher 暗号方式を用いたことが文献に初めて現れる例がシーザーであるといわれている。彼の「ガリア戦記」の中に敵に包囲された副将キケロに「援軍を送る」という情報を暗号で書いて矢文で送って勝利を得たとある。

4.2.1　シーザーの暗号 (単一換字方式)

シーザーの暗号は平文の文字を各々3 文字シフトさせたものである。

平文	e	n	g	u	n	w	o	,	h	a	k	e	n	s	i	t	a
暗号文	h	q	j	x	q	z	r	c	k	d	n	h	q	v	l	w	d

この方式は， キーワードを用いて 1 文字毎にシフト量を変えるというさらに複雑な方法に発展した。今, キーワードを “暗号の数理 (angonosuuri)” とすると置換表は

平文	e	n	g	u	n	w	o	h	a	k	e	n	s	i	t	a
キー	a	n	g	o	n	o	s	u	u	r	i	a	n	g	o	n
暗号文	e	,	o	g	,	j	f	,	u	a	m	n	e	n	h	n

暗号文の解読法は歴史的には 9 世紀のアラビアの科学者の著書に「文字頻度による解読法」として表されているということである。この解読法を単純化して説明すると，

(1) 通常の文章では使われるアルファベットに使用頻度の偏りがある。
(2) 文節として使われる文字の並びに偏りがある。
(3) 発信人の文章の癖により単語の予想がされてしまう。
(4) 1 単語でも意味のある解読がされる (シフト量が分かる) と全文が解読されてしまう。

などの特徴を利用して解読を試みる。

例えば，英文の場合 “e” が一番よく使われる文字である，逆に “q” は殆ど使われない，“the” が一番よく使われる単語である，単文字の語が “a” などごく一部に限られる等を手がかりにして，暗号文中に一番よく現れる文字が “e” に対応しているのでないかとか，3 連続文字を “the” と推測するとかする方法である。日本語の場合は仮名で説明すると、“て、に、を、は” の助詞、“ここ、これ、...” などの代名詞が使用頻度が高い。暗号解読法を発見したアラビアの文章では “al” が一番使われる文字である。ポーの「黄金虫」、ドイル（シャーロック・ホームズ）の「踊る人形」は頻度解析をテーマにした推理小説である。

4.2.2 ビジュネル暗号 (多表方式)

次に登場した暗号法は、最後に完成した人に因んでビジュネル暗号と呼ばれる。これは、アルファベットの組 (a, b) に 1 つのアルファベット c を割り当てた表 (ビジュネル魔法陣という) を用意しておいて、平文 x、キーワード k に対し、この表を見て暗号文 y を $y = (x, k)$ とする方法で，ビジュネル魔法陣の表は、アルファベットを列毎に単純にシフトした物を用いる。暗号の要点は、使用される表とキーワード (特に長さ) である。

4.2.3 発展型 (全文スクランブル方式)

頻度分析による解読法に対抗してさらに複雑にするには，文字毎の置換ではなく全文を不規則に置換してしまえば良いという考えに至るであろう。電子的には通信文はアルファベットや漢字を数字 (コード) に直して送られるので，平文も数字の列とする。

平文：4659876424 7975213576 8905873123 8076753758 0953256897 6245687112 76083

に “鍵K：4973265841” を 10 桁ずつずらし、桁上がりを無視しながら加える。結果，次のような

暗号文：8522031265 1848478317 2878038964 2949918599 4826411638 0118842953 15715

が得られる。

復号は，鍵 K の数字の列を 10 桁ずつずらし引く。このときも，桁下がりは無視する。桁上がりや桁下がりを考えなくてよい理由は補題 5 による。または，桁上がりのない歯車式計算器を考えればよい。

この方式に関して,「送信文と同じ長さの “乱数” をキーワードにして，しかもその乱数を “一度だけ使う”(one–time pad)」なら、その暗号は絶対に破られないことが**数学的に証明される**のであるが，その実現は実用上不可能である。乱数というのは人為的には作れないからで、実際は何らかの方法で作られた疑似暗号表を使う。one–time pad は第二次世界大戦中にも使われていたそうであるが、暗号表が敵に渡ると解読されてしまう。現在は、更にキーワードの有効時間を組み合わせて使用されている。

この原理にできるだけ近く，しかも人為的なミスを防ぐため機械を用いて行うことを実現したのがドイツ軍が第 2 次世界大戦中に使用した「エニグマ」という機械である。エニグマの原型は商業用の暗号機械であったものをドイツ軍が改造して使用した。エニグマは文字列の置換を行う回転式のスイッチ盤と歯車を組み合わせたもので，歯車を操作すれば異なる乱数の系列ができるようになっている。タイプライター位の大きさでキーボードで容易に暗号が作成できる。メカニズムは十分に研究されていて理論通り使用されていたならばまず解読できないであろうと自負するだけの機械であった。

近代の暗号解読法はピンポイント式でも総当り式でもない。数学・統計・工学的理論により暗号機が生成できる文字列を調べるだけでなく言語学・社会学・民俗学により人間・民族の行動の研究から使われる言葉のパターンを知るということまで必要になる。以前は通信は主にモールス符号で行われていたが、通信手の僅かな癖でも暗号解読の手がかりになったと言われている。エニグマの場合も，実物の取得、スパイ活動による秘密の漏洩、U ボート捕獲による暗号表の入手、放棄された基地に残された暗号表、入手した暗号による偽通信など連合国側特にイギリスの総力を挙げての理論的な挑戦により人間である故に避けられないミスを手がかりに可能性をできるだけ絞り，最後は数理的な可能性を機械を使って総当たり的に調べた。その機械は**コロッサス** (ギリシャの巨人) と呼ばれていて、連合軍のノルマンディ上陸作戦の折に大活躍したと言われている。この機械はチューリングが指導して作成したもので、第二次世界大戦中の情報戦争の実態は長く秘密にされていたが、実体が明らかにされてくるにしたがって、プログラム内蔵式の電子計算機の第一号と認められるようになってきている。バベッジやチューリングというような偉人の場合は暗号解読に貢献したことが偶々知られるところとなったが、暗号関連者達の仕事の内容や名前は外部に知られてはいけないことからくる問題は，暗号解読に伴って得られる様々な理論的な成果を公表できないために優秀な研究者と研究結果が埋もれてしまうことである。

4.2.4　秘密鍵暗号の原理

これまで説明した方法はいずれもその原理を次のように抽象的に表すことができる。これを**秘密鍵方式の暗号**ということにして， その原理を抽象的に説明する。登場人物はこの種の話題の定番になっているアリス，ボブ，イヴ (ちなみに盗み聞きは英語で eavesdrop という) としよう。今，アリスがボブに手紙を送るとする。

(1) アリスとボブは secured route (安全な通信路) を通じて，同じ鍵Kを持っている。アリスとボブ以外には鍵 K の存在を知られてはいけない。この意味で秘密鍵である。
(2) アリスは平文に鍵 K を用いて暗号化し暗号文を送る。
(3) ボブは同じ鍵Kを用いて暗号文を復号し平文を得る。

秘密鍵方式では (1) 暗号文が解けることは暗号文の発信者の認証になり，(2) 仮に，暗号文が盗まれても同じ鍵 K がないと解読できない，(3) 鍵Kが無いと暗号文は作成もできないし、改変できないので，初めに説明した発信者の認証， 秘密保持， 改変防止が達成される。

4.3 公開鍵暗号

これまで説明した秘密鍵暗号方式は現代でも利用されている。色々な原理が考案されそれを複合したものが用いられていて安全であることが保証されている。AES，3DES， MD5 等の名称で使われている。ネットショッピングを経験したことのある人は “SSL” や “TLS” という用語を聞いたことがあろうが、SSL は Secured Socket Layer、TSL は Transport Layer Security の略で暗号化された安全な通信層を意味している。

しかし，情報が電子的に交換されるようになった現代では，初めに説明したように，暗号の必要性はより高まってくることになるが、秘密鍵の方式では銀行取引等の場合を想定すれば分かるように、鍵の管理自体が大変な作業になる。また、面識のない人と秘密鍵を交換する secured route の確保も問題である。これらの問題を解決する暗号の方式として「公開鍵暗号 (public key cryptography)」と呼ばれる方式が考えられた。この方式は 1974 年頃スタンフォード大学のヘルマン (Martin E. Hellman) がその弟子ディフィー (Whitefield Diffie) とマークル (Rolph Merkle) らと共同で発表したものである。

4.3.1 公開鍵暗号を使う

公開鍵暗号では 1 組の鍵 (Eo, Do) を使う。1 つの鍵 Eo は鍵の持ち主から直接か公開鍵認証機構 (日本にはまだ存在しないが PKI(public key initiative) という言葉が使われるようになってきた) などから取得する。PKI は印鑑証明のように面識のない人の公開鍵の持ち主の保証を行う機関である。もう 1 つの鍵 Do は持ち主のみが知っていてこちらは公開でない秘密鍵である。

暗号文を送る

公開鍵暗号を使って，公開鍵の持ち主に暗号文を送るときは，次のような手順になる。アリスがボブに手紙を送るとする。

(1) アリスはボブの公開鍵 Eb を，本人から直接または公開鍵認証機構などから手に入れる。
この段階で，この鍵が受取人本人であることが確認できないと，以下の手続きはすべて無意味どころか危険ですらある。
(2) アリスは送りたい平文をボブの公開鍵 Eb を用いて暗号文に変換する。
(3) イヴはアリスの暗号文を手に入れてボブの公開鍵 Eb を用いても解読できない。
(4) ボブは自分用の秘密の鍵 Db を用いて平文に復号する。

問題は、この方式ではイブがアリスに成りすましてボブに暗号文を送ることができることである。

デジタル署名

文書の発信者を保証するためにディジタル署名という方式が必要である。その手続きは次のように，暗号化とは逆の順序に鍵を使用する。ただし，前の説明の鍵 Do は鍵を開ける逆操作，即ち，かける方の鍵としても働くものとする。

(1) アリスは，自分の秘密鍵 Da により暗号文を作成するかまたは鍵をかける。
(2) ボブはアリスの公開鍵 Ea を用いて暗号文を復号する。鍵 Ea がアリス本人のものであることは，本人直接または公の鍵管理機構から確認をすることができる。

この方法では、イブもアリスの公開鍵を取得できるからアリスの暗号文を解読できる。

デジタル署名付き暗号文

ボブがアリスからのディジタル署名つきの暗号文を受け取るには上で説明した方法を組み合わせれば良い。

(1) アリスの公開鍵組みを (Ea, Da)，ボブの公開鍵組みを (Eb, Db) とする。
(2) アリスは自分の秘密鍵 Da により平文を暗号文に変換することでディジタル署名をする。
(3) アリスは更にその暗号文をボブの公開鍵 Eb で二重に暗号化する。
(4) ボブは，受け取った暗号文をまず自分の秘密鍵 Db で一度復号する。
(5) ボブは更にアリスの公開鍵 Ea で復号する。

復号の際の二重操作を逆に行うとディジタル署名の確認も復号もできないことに注意しよう。イヴは二人の公開鍵，Ea, Eb の 2 つの鍵を手に入れても解読どころか発信人の確認もできない。

4.4　数学からの準備

4.4.1　合同式と有限体

暗号の数学的説明のために使用される数学を説明する。計算機の世界は 2 章で説明した様に有限の世界なので、無限列や超越数は使用できない。しかし、数学には実数のアルキメデスの公理 (無限大の公理) を仮定しないでもよい代数系がある。

定義 13 $a \equiv b \pmod{p} \iff p|a-b$ ($a-b$ が p で割り切れる) $\iff a = b + pq$ を満たす整数 q がある
"$a \equiv b \pmod{p}$*"* を 「p を法として a と b は合同である」という。

計算例を示す。

mod 6 **の場合**

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$-1 \equiv 5 \pmod{6}$, $-2 \equiv 4 \pmod{4}$, $-3 \equiv 3 \pmod{6}$, $-4 \equiv 2 \pmod{6}$, $-5 \equiv 1 \pmod{6}$

mod 7 **の場合**

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$-1 \equiv 6 \pmod 7$, $-2 \equiv 5 \pmod 7$, $\dfrac{1}{2} \equiv 4 \pmod 7$, $\dfrac{1}{3} \equiv 5 \pmod 7$

補題 5 合同関係は等号関係と同じ働きを持っている.

(1) $a \equiv b \pmod q$ と任意の c に対して $a \pm c \equiv b \pm c \pmod q$, $a \times c \equiv b \times c \pmod p$
(2) さらに $a \equiv b \pmod p$, $c \equiv d \pmod p$ に対して $a \pm c \equiv b \pm d \pmod p$, $a \times c \equiv b \times d \pmod p$
(3) 任意の整数 a, b, k について $\quad b \equiv a + k \pmod p \iff a \equiv b - k \pmod p$

割り算に関しては等号と同じようには行かない. mod 6 の場合は $2 \times 2 \equiv 2 \times 5 \equiv 4 \pmod 6$ 等で分かるように割り算ができない. しかし, mod 7 では割り算ができている. その違いを次の補題で説明する.

補題 6 p を素数とする。$ab \equiv 0 \pmod p$ (ab が p の倍数) ならば, $a \equiv 0 \pmod p$ または $b \equiv 0 \pmod p$ が成り立つ。

証明 背理法で証明する。結論を否定すると a, b 両方が p で割り切れない。p は素数だから a, b は互いに p と素になる。したがって, $ah + pq = 1$ をみたす整数 h, q が存在するから, この式を移項して $ah = 1 - pq$, 従って $ah \equiv 1 \pmod p$。同じように b に対して $bk \equiv 1 \pmod p$ をみたす整数 k がある。この式を掛けて $(ab)(hk) \equiv 1 \pmod p$。これは仮定に反する。

定義 14

(1) $a \equiv b \pmod p$ のとき, a, b は p の同じ**剰余類**に属すという.

(2) 集合 $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$ を, p の**剰余類の代表**という,

(3) p を素数でない大きな数として, 例えば, $p = 10000$, 剰余類を考えたとき, 剰余類の代表 a に対し, $a + b \equiv 0 \pmod p$ を満たす代表 b を基数 p に対する a の**補数**という.

(4) p が素数のとき, 集合 $\mathbf{Z}_p$ に $\equiv$ の関係で加法と乗法を定義すると四則計算で完結した集合ができる。これを標数 p の**有限体**といい $\mathbf{Z}_p$ と表す。また、$\mathbf{Z}_p$ から 0 を除いた集合を $\mathbf{Z}_p^*$ と表す。

(5) p を素数として, $g \in \mathbf{Z}_p$ が $\{g, g^2, \ldots, g^{p-1}\} = \mathbf{Z}_p^*$ となるとき g を**原始根**という。原始根は複数ある。

(6) $\mathbf{Z}_p$ の原始根 g を 1 つ固定する. $a \in \mathbf{Z}_p^*$ に対し $g^t \equiv a \pmod p$ となる t を**離散対数**という。

例　$p = 29, g = 18$ として、$g, g^2, g^3, \ldots, g^{28}$ を 29 を法として並べると、$18, 5, 3, 25, 15, 9, 17, 16, 27, 22, 19, 23, 8, 28, 11, 24, 26, 4, 14, 20, 12, 13, 2, 7, 10, 6, 21, 1$ となり、18 が 29 の原始根であることが分かる。与えられた素数 p に対し、原始根の求め方も分かっていないし，離散対数も、今のところ $g, g^2, \ldots, g^{p-1}$ を全部計算してみなければならない。効率良く計算する方法が発見されてないので以下のように公開鍵暗号として利用可能である。また、原始根の冪乗列は規則がないようなので、疑似乱数にも使用されている。もっとも、こちらの方は乱数の定義に合いすぎるという欠点があるといわれている。次の定理は合同式での基本定理である。

定理 15 (フェルマー) p を素数とする。$0 < a < p$ をみたす任意の整数 a に対し

$$a^{p-1} \equiv 1 \pmod{p}$$

証明　1 から $p-1$ までの整数を並べて，$1, 2, \ldots, p-1$ とおく。a を p の倍数でない任意の数とする。補題より $a, 2, 3, \ldots, (p-1)a$ に同じ元はない。なぜならば，$ia \equiv ja \pmod{p}$ とすると，移項して $(i-j)a \equiv 0 \pmod{p}$，a は p の倍数でないので，補題より $i-j$ が p で割り切れなければならないが，$0 \leqq i-j < p$ より $i = j$ である。したがって，$a, 2a, 3a, \ldots, (p-1)a$ は p を法として考えると $1, 2, 3, \ldots, (p-1)$ を並べ変えたものである。よって，$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$。しかし，$(p-1)!$ は p で割り切れないから $a^{p-1} \equiv 1 \pmod{p}$

系 1

$$r \equiv 1 \pmod{p-1} \quad \text{ならば} \quad a^r \equiv a \pmod{p}$$

証明　$r \equiv 1 \pmod{p-1}$ は，ある整数 m により $r = 1 + m(p-1)$ と表せることと同じである。したがって，上記のフェルマーの定理から $a^r = a^{1+m(p-1)} = a(a^{p-1})^m \equiv a \pmod{p}$

4.4.2　2 の補数：計算機への応用

2 の補数は計算機で負の数と引き算の扱いに応用がある．計算機では 1 つのメモリのサイズや取り扱いの単位は 32 ビット, 64 ビットなどというように一定のサイズである．例えば，32 ビットを単位としている場合，2^{32} を表そうとすると，32 ビット分のメモリの中身はすべて 0 である．このことを利用して負の数を 2^{32} の剰余類で表す方式を採用している計算機が多くある．

数 x の 2 の補数とは，32 ビットとすると，$2^{32} - x$ のことである．引き算をせずに補数を求める方法を説明する．今，32 ビット単位のメモリの表す数を x とし，各ビット毎に 0,1 を反転させた数を $\bar{x}$ とする．x と $\bar{x}$ を各ビット毎に加えると 1 であるから $x + \bar{x} = 2^{32} - 1$，従って，$x + \bar{x} + 1 = 2^{32} \equiv 0 \pmod{2^{32}}$ が成り立つ．これから $\bar{x} + 1 \equiv -x \pmod{2^{32}}$，即ち，$x$ の各ビットを反転させて $+1$ すれば，$-x$ になるから 32 ビットあるいは 64 ビット単位で計算している場合は，負の数はいらない，従って，引き算も要らないということになる．ただし，32 ビット単位では 2^{31} を超えると正の数と負の数が表示上区別がつかなくなるので，正の数の最大値は 32 ビットマシンでは $2^{31} - 1$ として，32 ビット目が 1 の数は負の数として扱っている場合が多い．

4.5 暗号の数理

4.5.1 アフィン暗号方式

単一換字式、多表式どちらも次の合同式で表される。特に，ビジュネル暗号方式ではビジュネル摩方陣の作成は手間のかかることであるが，次の方式では簡単に計算できる．

互いに素な自然数数の組 (m,p) と任意の自然数 s を用意する。平文を a とするとき、暗号文 b を次の式で求める。

$$b \equiv ma + s \pmod{p}$$

$m = 1$ のときがシーザー暗号である。アルファベットを用いるときは $p = 26$ である。

復号は p, m が互いに素であるから $pq + mn = 1$ を満たす整数 q, n が存在する．この n を使って

$$n(b - s) \equiv a \pmod{p}$$

何故ならば，暗号文に対し始めに移項して $b - s \equiv ma \pmod{p}$、両辺に n を掛けると $n(b - s) \equiv mna \pmod{p}$、互いに素の関係式から $mn = 1 - pq$、これを代入して $n(b - s) \equiv (1 - pq)a \equiv a \pmod{p}$.

アフィン暗号方式では m, s と求めるために 2 つの文字が特定されなければならないので，一層複雑になる．更に，キーワードを使っている場合は、キーワードの長さを想定して、連立にしてすべてのアルファベットについて試してみるということを行う必要があるが，今日では解読はコンピュータのパワーの問題になる．

4.5.2 公開鍵方式

公開鍵方式成立の要件

公開鍵暗号法では復号のアルゴリズムが知られているのに暗号が成り立つ理由は,「一方向関数」と呼ばれる性質を持つ関数の存在をヘルマン達が発見したことによる．暗号で扱う関数 $y = f(x)$ は四則計算と冪乗計算のみから構成されている．しかも，合同式の計算になるから引き算・割り算・冪乗根の計算は使わない．実数を変数とする三角関数・逆三角関数・指数関数・対数関数などの超越関数では y から x を求めることは一般に不可能であるが，暗号で扱う関数は，その状況から y から x を求めるのは，特別に高級な関数を使わなくてもできそうに見えるが，実際は総当たり法以外に解法が考えられないような関数が存在する．これを一方向関数という．

公開鍵暗号の例 (エルガマル暗号)

公開鍵暗号方式の例を原始根を利用したエルガマル (El Gamal) 暗号で説明する。

1. ボブは p を大きい素数、g をその原始根、s を任意の数 (秘密鍵) とし、$h \equiv g^s \pmod{p}$ を計算して、(p, g, h) を公開鍵とする．
2. アリスは 適当な数 (アリスの秘密鍵にもなる)k を考えて、m $(m < p)$ を平文とするとき，$a \equiv g^k \pmod{p}, b \equiv mh^k \pmod{p}$ を計算して (a, b) を暗号文として送信する．

3. ボブは $a^s \pmod p$, $b/a^s \pmod p$ を求めて，$b/a^s \equiv m \pmod p$ で平文を得る．

何故ならば，$a^s \equiv (g^k)^s \equiv (g^s)^k \equiv h^k \pmod p$，従って，$b/a^s \equiv mh^k/h^k \equiv m \pmod p$. 割り算は、$\mathbf{Z}_p$ で行われるから実際は掛け算になる。

ここで，離散対数の計算が一方向関数になり，公開鍵の性質が満たされる．ただし，原始根や離散対数は一般的にも分かり難いものなので，安全性等に関して検証することが難しい．

4.5.3　RSA 体系の暗号

さらに，実用的で安全な方法を提案したのが，MIT(マサチューセッツ工科大学) のリベスト (Rivest)，シャミール (Shamir)，アドルマン (Adleman) のグループで，1977 年に提案され今日 **RSA 体系**と呼ばれている。RSA 体系はユークリッドの互除法という非常に古典的なアルゴリズムを利用したものであるが，これが実用的になるのは上の説明の要件を検証する必要がある。RSA 体系では次のプロセスで暗号文を作る。

RSA 体系のエンコード

(e1) 2 つの素数 p, q を想定する (任意)．n を $n = pq$ とおく。
(e2) 次に整数 r を $p-1$, $q-1$ と互いに素に選ぶ (任意)。
(e3) (n, r) を公開鍵とする．
(e4) この人に暗号文を送りたい人は，平文のコード列を n より短い列に区切り，その一つを m とするとき，$a \equiv m^r \pmod n$ を暗号文とする。

RSA のデコード

まず，復号用の鍵 s を次のように作る。

(k1) r は $p-1, q-1$ と互いに素であるから次の式を満たす e, f, g, h が存在する．

$$re + (p-1)f = 1 \tag{4.1}$$
$$rg + (q-1)h = 1 \tag{4.2}$$

(k2) 両式を引いて移項すると $r(e-g) = -(p-1)f + (q-1)h$.
$\mathrm{GCD}(p-1, q-1) = d$ とすると，r, d は互いに素であるから $e-g$ が d の倍数である．
したがって，$e-g$ が d の倍数であるから次の式をみたす整数 x, y が存在する．

$$e - g = x(p-1) + y(q-1)$$

(k3) この式を移項して得られた値を s と置く．

$$s = e - x(p-1) \tag{4.3}$$
$$= g + y(q-1) \tag{4.4}$$

もし，s が負だったり，大きすぎるときは $(p-1), (q-1)$ の最小公倍数で割って，余りを改めて s とおく．

復号の計算はこの鍵を使用して $b^s \pmod n$ を求めるだけである．$b^s \equiv a \pmod n$ を証明する．まず，

$$\begin{aligned} rs &= re - rx(p-1) = 1 - (p-1)f - rx(p-1) = 1 - (f - rx)(p-1) \equiv 1 \pmod{p-1} \\ rs &= rg - ry(q-1) = 1 - (q-1)h - ry(q-1) = 1 - (h - ry)(q-1) \equiv 1 \pmod{q-1} \end{aligned}$$

最初の等号は s の定義式 (4.3),(4.4)，次の等式は re に式 (4.1), (4.2) を移項した式による．次にフェルマーの小定理 15 の系 1 より

$$\begin{aligned} a^{rs} &\equiv a \pmod p \\ a^{rs} &\equiv a \pmod q \end{aligned}$$

即ち，$b^s = a^{rs} = a + pp' = a + qq'$．ここで $pp' = qq'$ で p, q は互いに素であるから p' が q の倍数，または q' が p の倍数であるから $pp' \equiv 0 \pmod n$．よって，$b^s \equiv a^{rs} \equiv a \pmod n$ となる．

RSA 暗号の安全性

これだけ理論が整然としていて，鍵の作り方と復号の仕方まで明示されているのに，この方式が何故暗号体系として成立できるのかというと，n が大きいと因数分解に天文学的な時間と費用が掛かるからである。例えば，RSA 体系で出された懸賞つきの暗号で解かれた例が唯一つある。その時の数は 129 桁の数で

1143816257 5788886766 9235779976 1466120102 1829672124 2362562561 8429357069 3524573389 7830597123 5639587050 5989907514 7599290026 879543541

全ての 2 因子の数の因数分解が困難な訳ではない。ここで提案された数も，比較的簡単に因数分解できるであろうとの予想がされていた。1994 年にアトキン達が 600 人の協力を得てスーパーコンピュータを動員して 8 ヵ月かかって因数分解した。この時の費用を人件費だけ計算すると約 50 億円になる。RSA 暗号方式の解読は因数分解の速度が問題でパワーの問題であるから，コンピュータの速度が進化してくると RSA 暗号方式の安全性が脅かされることになる．現在では 1024 ビット (2^{1024}10 進表示で約 300 桁) やより慎重を要する場合は 4096 ビットを使うよう推奨されている．

安全性の方は当分大丈夫としてこの方式の問題点は下の例でも分かる通り計算が大変なことである。この点の改良を目指して研究が続けられているが、全文をこの方式で利用することは、暗号・復号の手数という面で不利である。この方式で面識のない人と secured route として利用して秘密鍵を交換し、通信はその秘密鍵を利用した方法が効率上は有利であるともいわれている．

冪乗の高速計算法

RSA 暗号の計算には非常に大きな数の冪乗計算が必要である．いくら計算機といえども 10 進で 300 桁回も掛け算するには因数分解と変わらない位の計算をすることになる．ここで冪乗の計算に関して次のように高速な計算法が知られている．

冪乗計算

問題： x, n を入力として x^n を計算する．

アルゴリズム：

i. n を 2 の冪で展開して，$n = d_k 2^k + d_{k-1}2^{k-1} + \cdots + d_1 2 + d_0$. このとき $d_i = 0$ または 1.
ii. $x_0 = x, x_1 = x_0^2 = x^2, x_2 = x_1^2 = x^{2^2}, \ldots, x_{i+1} = x_i^2 = x^{2^{i+1}}, \ldots x_k = x_{k-1}^2 = x^{2^k}$ を求める．
iii. $x^n = x^{d_k 2^k + d_{k-1}2^{k-1} + \cdots + d_1 2 + d_0} = x_k^{d_k} \times x_{k-1}^{d_{k-1}} \times \cdots \times x_1^{d_1} \times x_0^{d_0}$
ただし，$d_i = 0$ または 1 であるから $d_i = 1$ の項のみを取って $x^n = x_k \times x_i \times x_j \times \ldots$ となる．

例　3^{3^3} を計算する．

i. $27 - 16 = 11, 11 - 8 = 3, 3 - 2 = 1$. したがって $27 = 16 + 8 + 2 + 1$.

ii. $3^1 = 3, 3^2 = 9,\ 3^4 = 9^2 = 81,\ 3^8 = 81^2 = 6561,\ 3^{16} = 6561^2 = 43046721$

iii. $3^{3^3} = 3^{16} \times 3^8 \times 3^2 \times 3^1 = 43046721 \times 6561 \times 9 \times 3 = 7625597484987$

この計算に必要な回数は，2 進展開も含め 10 回で，27 回より圧倒的に少ない．べき指数 n が大きくなるともっと差が開く．理論的にはこのアルゴリズムで必要な最大の計算回数は $3 \times \log_2 n$ 回である，例えば，$2^{20} - 1$ 乗するのに，このアルゴリズムでは 2 進展開の計算，2^n 乗の計算，最後の掛け算にそれぞれ 20 回，合計 60 回要するが，単純に掛け算すると約 100 万回行わねばならない．

RSA 暗号の例

以下に RSA 暗号の簡単な例を示す。

(e1) $p = 11, q = 13, n = 11 \times 13 = 143$
(e2) $p - 1 = 10, q - 1 = 12$ なので $r = 7$ にとる。
(e3) $(143, 7)$ が公開鍵である。
(e4) 平文を $a = 5$ とすると，暗号文は $b = a^r = 5^7 = 78125 \equiv 47 \pmod{143}$ で 47 である。

秘密鍵を求める．

(k1) $7 \times e + 10 \times f = 7 \times g + 12 \times h = 1$ をみたす整数は $e = 3, f = -2, g = 7, h = -4$.
(k2) $e - g = -4 = x \times 10 + y \times 12$ をみたす整数は $x = 2, y = -2$,
(k3) 従って，復号用の鍵は $s = e - x(p-1) = 3 - 2 \times 10 = 7 + (-2) \times 12 = -17$，ここで負の数ではべき乗の計算が面倒になるので，$10, 12$ の最小公倍数 60 で割って $s = 43$ を得る．

暗号文は $b = 47$ だったから，平文は $b^s = 47^{43}$．これを　mod 143 で求める．べき乗の計算はアルゴリズムを利用する．以下の合同式はすべて　mod 143 で行っている．

i. $43 = 32 + 8 + 2 + 1$
ii. $b^2 = 47^2 \equiv 64, b^4 \equiv 64^2 \equiv 92, b^8 \equiv 92^2 \equiv 27, b^{16} \equiv 27^2 \equiv 14, b^{32} \equiv 14^2 \equiv 53$
iii. $a = 47^{43} = b^{32} \times b^8 \times b^2 \times b^1 \equiv 53 \times 27 \times 64 \times 47 \equiv 64 \times 47 \equiv 5$

以上で元の平文 5 が得られた．

第5章　現代数学への道標

ギリシャ時代に確立された数学の体系は，ヒルベルトの公理論の思想により，再編成・洗練され現在へとつながっているのであるが，現代数学といわれるものになるためには数学の論理だけでなく，問題に対する視点を変える大きな転換点があった。その転換点となった問題を 2 つ取り上げて，それまでの数学とどう変わったのかを説明しよう。一つは方程式に関することで，もう一つは幾何学に関することである。

5.1　高次方程式

初めに高次方程式の解の公式を説明する。

5.1.1　3 次方程式の解法

3 次方程式の解法について説明する。

定理 16 (Cardano) 3 次方程式 $z^3 = 3pz + 2q$ の解は

$$\alpha = \sqrt[3]{q + \sqrt{q^2 - p^3}},\ \beta = \sqrt[3]{q - \sqrt{q^2 - p^3}} \qquad \text{とおくと}$$

$$\alpha + \beta,\ \omega\alpha + \omega^2\beta,\ \omega^2\alpha + \omega\beta \qquad \text{である。}$$

ただし，ω は $z^3 = 1$ の 1 以外の解で $\omega = \dfrac{-1 + i\sqrt{3}}{2}$.

証明　解を $z = x + y$ とおく。これをもとの方程式に代入すると

$$(x + y)^3 = 3xy(x + y) + (x^3 + y^3) = 3p(x + y) + 2q$$

であるから，$2q = x^3 + y^3,\ p = xy$ とおいてみる。
更に，$X = x^3,\ Y = y^3$ とおくと，$X + Y = 2q,\ XY = p^3$ と得る。
これを解いて，$X = q \pm \sqrt{q^2 - p^3}$ を得る。
次に $x^3 = X = q + \sqrt{q^2 - p^3}$ を解くと，$\alpha = \sqrt[3]{q + \sqrt{q^2 - p^3}}$ とおいて $x = \alpha,\ \omega\alpha,\ \omega^2\alpha$ を得る。
この結果を $y = \dfrac{p}{x}$ に代入して定理を得る。
一般の 3 次方程式 $ax^3 + bx^2 + cx + d = 0\ (a \neq 0)$ の場合は $z = x + b/(3a)$ とおくと定理の形になる。

5.1.2　4 次方程式の解法

4 次方程式の場合は次のように解く。

定理 17 (Ferrari) 4 次方程式 $z^4+pz^2+qz+r=0$ の解は次のように 2 段階で求める。
方程式　$\xi^3-p\xi^2-4r\xi+(4pr-q^2)=0$　の解の 1 つを ξ_0 とすると，次の 2 つの 2 次方程式を解いて得られる。

$$z^2\pm\sqrt{\xi_0-p}\left(z-\frac{q}{2(\xi_0-p)}\right)+\frac{\xi_0}{2}=0$$

証明　方程式を 2 次の式に因数分解できるとする。
$z^4+pz^2+qz+r=(z^2+\alpha z+\beta)(z^2-\alpha z+\gamma)$ とおくと係数に関して次の連立方程式を得る。

$$\left\{\begin{array}{rcl}\beta+\gamma-\alpha^2 &=& p\\ \alpha(\gamma-\beta) &=& q\\ \beta\gamma &=& r\end{array}\right.$$

初めの式の α^2 を右辺へ移項して　$p+\alpha^2=\xi$　とおく。
2 番目の式から　$(\beta-\gamma)^2=(\beta+\gamma)^2-4\beta\gamma=\xi^2-4r=\dfrac{q^2}{\alpha^2}=\dfrac{q^2}{\xi-p}$
この式の分母を払って　$\xi^3-p\xi^2-4r\xi+(4pr-q^2)=0$　を得る。
この方程式の解の 1 つを ξ_0 とおくと　$\alpha=\pm\sqrt{\xi_0-p},\ \beta+\gamma=\xi_0,\ \gamma-\beta=\dfrac{q}{\alpha}$ 。
$\beta,\ \gamma$ の連立方程式を解いて α を代入すれば，定理の式を得る。

一般の 4 次方程式　$ax^4+bx^3+cx^2+dx+e=0\quad(a\neq0)$　の場合は，$z=x+b/(4a)$　とおけば定理の形になる。

5.1.3　$z^n=\alpha$ の場合

定理 18 $z^n=1$　の解は

$$\omega=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}\quad\text{とおくと}\quad\omega,\ \omega^2,\ \ldots,\ \omega^n=1\quad\text{である。}$$

定理 19 $z^n=\alpha$　の解は　$\alpha=r(\cos\theta+i\sin\theta)$　とすると

$$\chi=\sqrt[n]{r}\left(\cos\frac{\theta}{n}+i\sin\frac{\theta}{n}\right)\quad\text{とおいて}\quad\chi,\ \chi\omega,\ \chi\omega^2,\ldots,\ \chi\omega^{n-1}\quad\text{である。}$$

5.1.4　一般の場合

定理 20 (Abel, Galois) n が 5 以上の整数のとき，n 次方程式を代数的に解く方法はない。

「公式は何々である」という定理の意味は分かるが,「ない」という定理は何を求めればよいのであろうか？

5.2 群

5.2.1 初めに

「群」は「ぐん」と読む。group の直訳である。全ての数学は一番基礎に集合があり，それに色々な数学的構造が入って，様々な数学ができるので，数学のどの定義も集団を表す意味を含んでいる。数学の門外漢が定義の言葉から内容を知ろうとしても，似たような名前ばかりなのでわかりにくい。更に,「正則」,「正規」,「同型」,「同値」等どの分野にも出てくるが，意味が全部違うなどというものさえある。数学の定義は単なる記号と思った方が安全である。

群という考えは基本的なものでいたる所で見つけることができるが，数学の中で意識的に使われ，それを用いて問題を解くようになったのは 19 世紀後半になってからである。それまでは運動とか変換という概念として扱われていた。

運動や変換と群との本質的な違いは，前者が関数という言葉が使われたときと同様に一つの何かについて考えているのに対して，群ではある性質を満たすもの全部をもってきて，その集団としてどういう性質を持っているかを考えるところにある。そして，個々のものの問題を集団の性質で解決しようというのが，現代数学がよく使う戦略である。

5.2.2 基本的な例

正多角形の変換群

正方形を考えよう。正方形を動かして (変換して) 元の正方形に重ねられるような運動を全て集める。この集合を H_4 と表し，正方形の**自己合同群**という。

(1) 正方形の中心を回転軸にして，$90°$, $180°$, $270°$, $360°$ 左回転させる。
(2) 正方形の中心線を軸にして，裏返す。中心線は 2 本あるので，この運動は 2 つある。
(3) 対角線を結ぶ線を軸にして，裏返す。これも対角線を結ぶ線は 2 本あるから運動は 2 つある。

ここで，任意の運動を 2 つ f, g 持ってきたとき，その合成 $g \circ f$ が上の運動のどれかになる。
例えば,「$f = 90°$左回転」して「$g =$ 中心線での裏返し」すると「$g \circ f =$ 対角線での裏返し」となる。
運動の説明のあいまいさを避けるために正方形の頂点に番号を付けておいて，運動でその頂点がどの頂点に重なるかで運動を表すこととする。

(1) $90°$ 左回転させると，頂点は $1 \to 2 \to 3 \to 4 \to 1$ の順に重なる。これを $(1,2,3,4)$ と表すことにする。
    $180°$ 回転させると，頂点は $1 \to 3 \to 1, 2 \to 4 \to 2$ の順に重なる。この場合運動する頂点の系列は 2 つであるから，$(1,3)(2,4)$ と表す。
    $270°$ 回転させると $(1,4,3,2)$ となる。この運動は，右方向へ $90°$ 回転させることと同じである。
    $360°$ 回転させると元に戻るので，結果として何もしないのと同じである。何もしない運動は数字の 0 や 1 と同じように運動全体の記述で便利なので E と表すことにする。
(2) 中心線で裏返す運動は $(1,2)(3,4)$, $(1,4)(2,3)$ の 2 つである。

(3) 対角線で裏返す運動は $(1)(3)(2,4)$, $(1,3)(2)(4)$ の 2 つである。前者の運動では $1,3$ 番の頂点は動いていない。通常はこのように動かない頂点は書かないことにする。したがって，この 2 つの運動は $(2,4)$, $(1,3)$ と表す。

この記号を使うと「90°回転して」して「中心線で裏返し」という運動は

$$(1,2)(3,4)\circ(1,2,3,4)=(1)(2,4)(3)=(2,4)$$

と計算できるから，対角線で裏返しであることが分かる。運動 E の役割は $(1,2)(3,4)\circ(1,2)(3,4)=E$ のように同じ中心線で裏返しを 2 回繰り返したら元に戻る，即ち，何もしないのと同じであることを表すのに使われる。

正則行列群

次に，一般的な例として，行列の掛け算を取り上げる。

集合は $n\times n$ の正方行列で正則なもの全体を考える。(1) 正則な行列の行列積は正則行列になる，(2) 単位行列は正則行列である，(3) 正則行列は逆行列を持つ，の性質をもつ。

この集合が正多角形の合同変換群の場合と一番異なるところは，前者は有限であるのに，こちらは無限集合である点である。

さらに，こちらの方は正則行列全体でなく，色々な条件を付けてそれをみたすもののみからできる部分群を考えることができる。

(1) 正則行列全体は $GL(n,\mathbf{R})$ (係数が実数の場合)，$GL(n,\mathbf{C})$ (係数が複素数の場合)
(2) 行列式に関しては $|AB|=|A||B|$ という性質があるので，この値が 1 の部分集合は群の性質を保つ。この部分群は $SL(n,\mathbf{R})$　または　$SL(n,\mathbf{C})$.
(3) 行列式の値が 1 のものは，係数が整数でも逆行列の係数は整数であるから，部分群を作る。この群は $SL(n,\mathbf{Z})$ と表す。
(4) 直交行列全体 $O(n)$，ユニタり行列全体 $U(n)$.

対称群

有限群で最も一般的な群は，集合 $\Omega=\{1,2,\ldots,n\}$ から Ω 自身への一対一写像全体の作る群である。この群についても，(1) 一対一写像を合成すると一対一写像になる，(2) 恒等写像は一対一写像である，(3) この場合，一対一写像は逆写像を持ち，逆写像も一対一写像になる，の性質をもつ。

この群は n **次対称群 (置換群)** と呼ばれ，S_n と表示される。

5.2.3　群の定義，準同型写像

定義 15 集合 G の任意の 2 つの元 a,b に演算 $a\circ b$ が定義されていて，次の条件を満たすとき，集合 G はこの演算に関して**群**を作るという。

(1) 任意の 3 つの元 a,b,c について $(a\circ b)\circ c=a\circ(b\circ c)$ をみたす。(結合法則)

(2) G には，任意の元 a に対し $a \circ e = e \circ a = a$ をみたす特別な元がある。(単位元の存在)
(3) G の任意の元 a に対し $a \circ g = g \circ a = e$ を満たす G の元 g が存在する。g は a に依存し，a の逆元といい，a^{-1} と表す。

定義 16 2 つの群 G, H に対し，写像 $\phi : G \to H$ が，群演算を保存するとき，即ち，G の任意の 2 つの元 a, b に対して，$\phi(a \circ b) = \phi(a) \circ' \phi(b)$ をみたすとき，ϕ を**準同型写像**という。ここで，前者の演算は G の演算で，後者のそれは H の演算である。

例 準同型の例をあげると，正多角形の自己同型群 H_4 の説明に用いた頂点に番号を付けて運動を表したのは，H_4 から $\{1,2,3,4\}$ 上の一対一写像の群 S_4 への準同型写像である。

また，正方形の頂点の座標を $(1,1), (-1,1), (-1,-1), (1,-1)$ とすると，90° 左回転で，頂点が $(1,1) \to (-1,1) \to (-1,-1) \to (1,-1) \to (1,1)$ と移るから，行列

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

に対応させる。同じようにして

$$(1,3)(2,4) \to \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (1,4,3,2) \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad (1,2)(3,4) \to \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$(1,4)(2,3) \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (2,4) \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (1,3) \to \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad E \to \text{単位行列}$$

と対応させる。この対応が準同型の性質をみたすことは確かめなければないが,
上で説明した $(1,2)(3,4) \circ (1,2,3,4) = (2,4)$ の例では

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

のように確かめることができる。

ここに登場した行列はいずれも直交行列であることに注意しておこう。

5.2.4 群の有効性

1 つの変換だけを対象にせずに集合にした理由は,

(1) ある条件を満たすもの全部を集めてくると，この集合の一部の元の合成で全体が構成できるのではないか。
(2) 各々の元は逆の元があり，変換を元に戻せる。
(3) 同じ性質をもつ部分群や部分集合がありその部分について集中的に考えれば，全体の性質が見えてくるのでないか。
(4) 準同型とは，構造が似ていることを意味している。計算しやすい群を用いて詳しく研究して，それと準同型なものの構造を類推する。

等の考えが有効に使えるからである。

5.3　ガロアの理論

5.3.1　体，自己同型，ガロア群

以下の説明に必要な基本的定義の導入から始める。

定義 17 集合に四則計算が定義されるとき，その集合を**体**という。

例

(1) $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ はそれぞれ体である。無限集合で体であるものは，必ず $\mathbf{Q}$ を含む。したがって，$\mathbf{Q}$ が最小の無限体である。
(2) 集合 $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ は体である。
(3) 集合 $\mathbf{Q}(i) = \{a + bi \mid a, b \in \mathbf{Q}\}$ は体である。

定義 18 体 K があるとき，K から K 自身への写像 ϕ で，K の加法群，乗法群の同型写像であるとき，K の自己同型群といい，$\mathcal{A}(K)$ と表す。

例

(1) $\mathbf{C}$ において，複素共役に写す写像は $\mathcal{A}(\mathbf{C})$ の元である。
(2) $\mathbf{Q}(\sqrt{2})$ において，$\phi(a + b\sqrt{2}) = a - b\sqrt{2}$ は自己同型写像である。

定義 19

(1) 2 つの集合 $E \supset F$ において，F が E の部分体 (F が E と同じ演算で閉じている) のとき，E を F の**拡大体**という。
(2) E が F の拡大体とする。$\mathcal{G}(E/F) = \{\sigma \mid \sigma \in \mathcal{A}(E) \text{ かつ } \sigma|_F = id_F\}$ を E/F の**ガロア群**という。
(3) F を体，$f(x)$ を F を係数とする多項式で，F において既約とする。$f(x) = 0$ の ($\mathbf{C}$ における) 解を付け加えてできる F の最小の拡大体 E を $f(x)$ の**分解体**という。

例

(1) $\mathbf{R}$ は $\mathbf{Q}$ の拡大体である。
(2) $\mathbf{C}$ は $\mathbf{R}$ の拡大体である。
$\mathcal{G}(\mathbf{C}/\mathbf{R})$ の自明でないものは複素共役写像である。
(3) $f(x) = x^3 - 1$ の拡大体は $\mathbf{Q}(\omega) = \{a + b\omega \mid a, b, c \in \mathbf{Q}\}$　(ただし　$\omega^3 = 1$) である。
このとき，$\mathcal{A}(\mathbf{Q}(\omega))$ の自明でないものは $\phi(a + b\omega) = a + b\omega^2 = a + b\bar{\omega}$ である。
(4) $g(x) = x^3 - 2$ の解は $\alpha, \alpha\omega, \alpha\omega^2$　$(\omega^3 = 1, \omega \neq 1, \alpha = \sqrt[3]{2})$ である。
$g(x)$ の分解体は $E = \mathbf{Q}(\alpha, \alpha\omega, \alpha\omega^2)$ であるが，$E = \mathbf{Q}(\alpha, \omega)$ となる。
$g(x)$ は $\mathbf{Q}$ 上既約多項式なので $\mathbf{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbf{Q}\}$ である。

定理 21 $f(x)$ を F を係数体とする多項式で，複素数体 $\mathbf{C}$ で因数分解したとき，重複因子がないとする。$f(x)$ の分解体を E とするとき，ガロア群 $\mathcal{G}(E/F)$ の元の個数 (位数という) は，E が F を係数体とするベクトルの次元に等しい。この定理の内容を記号で次のように表す。

$$|\mathcal{G}(E/F)| = |E : F|$$

例 $|\mathcal{G}(\mathbf{C}/\mathbf{R})|,\ |\mathcal{G}(\mathbf{Q}(i)/\mathbf{Q})|,\ |\mathcal{G}(\mathbf{Q}(\omega)/\mathbf{Q})|$ はいずれも 2 であるから，ガロア群の単位元以外の元は，複素共役だけである。

定理 22 $f(x)$ を F を係数体とする多項式とする。$f(x)=0$ がその分解体 E において n 個の異なる解をもてば，ガロア群 $\mathcal{G}(E/F)$ は n 次対称群 S_n の部分群と同型になる。特に，その位数は $n!$ の約数になる。

例 $E=\mathbf{Q}(\alpha,\omega)$ のとき

$$|\mathcal{G}(E/\mathbf{Q})|=|E:\mathbf{Q}|=|E:\mathbf{Q}(\alpha)||\mathbf{Q}(\alpha):\mathbf{Q}|=3|E:\mathbf{Q}(\alpha)|>3$$

が成り立つので，上の定理から $\mathcal{G}(E/\mathbf{Q})$ は 3 次対称群 S_3 に同型である。

5.3.2 群と方程式の解法

以上の準備をして，5 次以上の代数方程式が何故べき根で解けないかという定理を紹介する。
初めに「べき根で解ける」という意味から考える。

定義 20 F を体とする。$f(x)$ を F 係数の多項式とし，E を $f(x)$ の分解体とする。
拡大体の列 $F=B_0\subset B_1\subset\cdots\subset B_r=E$ において，$B_i=B_{i-1}(\chi_i)$ $(\chi^{n_i}=a_i\in B_{i-1})$ となるものがあるとき $f(x)=0$ は「F 上で**べき根によって可解である**」という。

定理 23 F を $\mathbf{Q}$ を含む体とし，χ を 1 の**原始** m **乗根**として，$E=F(\chi)$ とすると，$\mathcal{G}(E/F)$ はアーベル群になる。

群の方にも群を拡大していくときに，アーベル群を付け加えていく仕方があり，そのようにして作った群を**可解群**という。
S_2，S_3,S_4 と**アーベル群**(群の演算が可換のもの) は，可解群になることを注意しておく。
最後の定理は次のようになる。

定理 24 (ガロア) $f(x)$ を $\mathbf{Q}$ 係数の多項式とし，$\mathbf{Q}$ 上べき根によって可解であるための必要十分条件は，$\mathcal{G}(E/F)$ は可解群であることである。

定理 25 (アーベル・ルフィニ) 5 次以上の $\mathbf{Q}$ 係数の多項式 $f(x)$ でべき根により可解にならないものが存在する。

定理 26 方程式が平方根だけで解けるための必要十分条件はガロア群の位数が 2 のべきであることである。

5.4 色々な幾何学

図形の性質を研究する数学の分野を幾何学という。
幾何学の英語名は geometry でこの言葉の起源は「地面の測量」ということである。それに対し,「幾何学」という言葉は意味不明であるが，geometry を中国語に音訳したものといわれる。
幾何学というとユークリッド幾何学を想像されるであろうが，そこでは目で見えるものを扱っていて，ユークリッドの学派が体系を整えていたために，その体系の検証をしている内に色々な幾何学が生まれたのである。

5.4.1　ユークリッド幾何学で見ると

幾何学が近代的になったのは，座標という考えが導入されてからである。座標を用いて幾何学の問題を代数的に取り扱ったのはデカルト (1637 年) である。座標を入れて図形の性質を考える幾何学は解析幾何学とも呼ばれている。

ユークリッド幾何学の一番の特徴は移動で重ね合わせることができる図形，即ち，合同な図形を同一視して， 議論していることである。変換の立場から見ると, ユークリッド幾何学の変換は「距離を変えない」ということで特徴づけることができる。この点に注目して，解析幾何学から見たユークリッド幾何学の特徴をあげる。

(1) $L = \{(x, y) \mid ax + by + c = 0\}$ を直線と定義すると，公理系をみたす。
(2) ユークリッド幾何学の座標系では，一方の座標軸を原点で, 90° 回転させて他方の座標軸とする。したがって, 座標軸は直交していて, 両軸の単位の長さは等しい。
このことにより，2 点 $(x_1, y_)$, (x_2, y_2) の距離が $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ であることがいえる。
(3) ユークリッドの変換は, 長さを変えないことより, 直線は直線に移ることがいえる。
したがって，座標を用いるとユークリッド幾何学の変換，即ち，**合同変換**は 1 次写像になるから，行列で記述できる。
(4) 合同変換を $\mathbf{y} = A\mathbf{x}$ とすると，A は長さを保つことから，行列 A について $A^tA = {}^tAA = E$ という条件をみたすことがいえる。
特に，合同変換は一対一である。

(4) の条件をみたす行列は**直交行列**と呼ばれる。直交行列全体は，既に述べたが，群を作り直交群といい，$O(n)$ と表される。

5.4.2　2 次曲線

円錐曲線

平面曲線の中で特徴ある曲線について考えて見よう。

定義 21 2 次曲線とは $ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$ をみたす (x, y) の集合である。
次のものを固有の 2 次曲線という。

- 円　$x^2 + y^2 = a^2$
- 楕円　$\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1 \quad (a \neq b)$
- 双曲線　$\dfrac{x^2}{a^2} - \dfrac{y^2}{b^2} = 1$
- 放物線　$y = px^2$

これらの曲線は, 定義式の次数が同じであるだけでなく, 次の意味でも同じ仲間であると考えられる。

定義 22 軸が同じで, 頂点が重なった円錐を考える。 この円錐を平面で切ったとき得られる曲線を, 円錐曲線という。

問題の円錐は $x^2 + y^2 = z^2$ で与えられる。

(1) 平面を円錐の軸と直交するようにとる。例えば, $z = a$ $(a \neq 0)$ とすれば, 切口の曲線は, $x^2 + y^2 = a^2$ で 円になる。

(2) 平面を円錐の軸と平行にとる。例えば, $x = a$ $(a \neq 0)$ とすれば, 切口の曲線は, $a^2 + y^2 = z^2$ 移項して, $z^2 - y^2 = a^2$ で双曲線になる。

(3) 平面を円錐の母線に平行にとる。例えば, $x + z = 1$ とすれば, 切口の曲線は, $x^2 + y^2 = (1 - x)^2$ これを整理する $y^2 = 1 - 2x$ で放物線になる。

(4) 平面を上のいずれでもないようにしてとる。例えば, $x = 2z+1$ とすれば, 切口の曲線は, $(2z+1)^2+y^2 = z^2$ これを整理すると $3(z + 2/3)^2 + y^2 = 1/3$ で楕円になる。

この他にも, 1 本の定直線 (準線と呼ぶ) と 1 つの定点 (焦点と呼ぶ) を用意して, それらに至る距離の比が一定と言う条件で式を立てると, 比の値を変えて, 2 次曲線全てが得られる。

合同変換による分類

今度は, 2 次曲線の式を始めに考えて, 合同変換によりどのように分類されるかを考えてみよう。

定理 27 2 次曲線を合同変換で重なるものを同じとすると, 次のどれかの曲線に重なる。

- 円 $x^2 + y^2 = a^2$
- 楕円 $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1 \quad (a \neq b)$
- 双曲線 $\dfrac{x^2}{a^2} - \dfrac{y^2}{b^2} = 1$
- 放物線 $y = px^2$

また, これらの曲線は, 合同変換では互いに重ね合わせることができない。

証明 2 次曲線は次のように行列で表すことができる。

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = (x, y, 1) \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

行列 A をこの 2 次形式の係数行列という。

まず, 平行移動で 1 次の項が消せるかどうか考える。$x = X + u, y = Y + v$ を元の式に代入して X, Y の係数を求めて, 次の方程式を得る。

$$\begin{cases} au + bv + d &= 0 \\ bu + cv + e &= 0 \end{cases}$$

I. $ac - b^2 \neq 0$ の場合

この場合は, 連立方程式が解けるから平行移動で, 1 次の項が消せるから $ax^2 + 2bxy + cy^2 + f = 0$ から始める。次の定理が必要である。

定理 28 対称行列は直交行列で対角化できる。

このとき，対角成分は係数行列の固有値である。固有値の積は行列式に一致し，$ac-b^2 \neq 0$ であるから，0 は固有値にならない。そこで，固有値を α, β とし，変換の直交行列を P とおくと

$$ {}^tP \begin{pmatrix} a & b \\ b & c \end{pmatrix} P = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = D \qquad (\alpha\beta \neq 0) $$

従って，$(\xi, \eta) = (x, y)P$ とおくと，即ち，回転させると

$$ ax^2 + 2bxy + cy^2 = (x, y)A \begin{pmatrix} x \\ y \end{pmatrix} = (x, y)PD^tP \begin{pmatrix} x \\ y \end{pmatrix} = (\xi, \eta) \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \alpha\xi^2 + \beta\eta^2 $$

これより，定数部が 0 でなければ，α, β の符号にしたがって，円 ($\alpha = \beta$ の場合)，楕円 ($\alpha \neq \beta$ かつ $\alpha\beta > 0$)，双曲線 ($\alpha\beta < 0$ の場合)，に分類されてこれらが重なることはない。

II. $ac - b^2 = 0$ の場合

この場合は，初めに平行移動できないが，上で説明したように，係数行列 A の固有値の 1 つは 0 である。よって，最初に回転すると x, y のどちらかの 2 次の項はない。したがって，この場合は放物線になる。

5.4.3　アフィン幾何学で見ると

上で説明した内容から，距離を取ったらどんな幾何学ができるであろうか。

直線の部分をそのまま採用し，平行線の公理も採用する。座標系は，角度の概念がなくなったので，直交している必要はなく，更に，各座標系の単位の長さは異なっていても良い。

したがって，アフィン幾何学では移動 (変換) は (1) 直線を直線に移し，(2) 平行線は平行線に移す，したがって，(3) 一対一を保つ，という性質が成り立つ。この性質を持つ変換を**アフィン変換**という。ユークリッド幾何学の合同変換と同じように，アフィン変換で重ねることができるものを同じであると見なせば，アフィン幾何学では次のようなことが成り立つ。

(1) 三角形はすべて相等しい。
(2) 平行性は保つから，平行線どうしの線分比は保たれる。
　したがって，アフィン幾何学では，四角形は正方形，台形，それ以外の四角形の 3 種類しかない。平行辺が 2 つあれば正方形に，平行辺が 1 つならば台形に，それ以外の四角形は互いにアフィン変換で重ねあわせることができる。
(3) 一般に，相似な図形は相等しい。

2 次曲線の場合は，長さは問題にならなくなるので，$x^2 + y^2 = 1$(円と楕円)，$x^2 - y^2 = 1$(双曲線)，$y = x^2$(放物線) の 3 種類になる。

5.4.4　射影幾何学で見ると

ユークリッド幾何学やアフィン幾何学では，平行線はどこまで行っても平行線で，しかも，目盛りの間隔も不変であるから，どこまで行っても，同じ世界になる。しかし，我々の実際に目にしている世界は，平行な線路は遠くの方で一点に見える。このような世界を理論的に考えることはできないのであろうか。

仮に，直線の両端に無限遠点があるとして，この点を通常点と同じ性質を持つものとすると，どのような性質があるか考えてみよう。

(1) 1 つの直線の一方の無限遠点と反対側の無限遠点は同じでなければならない。
なぜならば，もし異なるとすると平行線はすべてその 2 つの無限遠点を通るから，2 点を通る直線が無数にあることになり，これは我々の感覚とは異なる。
(2) 交差する 2 本の直線の端の無限遠点は別の点である。
なぜならば，もし同じとすると，2 点を通って，異なる直線が無数に引けることになり，これも我々の感覚と異なる。

この結果，無限遠点は無数になければならないことがわかった。

次に，簡単にするために，無限遠点の集合は直線になると考えることにし，これを**無限遠直線**と呼んで l_∞ と表す。

定義 23 ユークリッド平面に無限直線を加えたものを**射影平面**といい，P^2 と表す。

定理 29 射影平面の一部はメビウスの帯と同相である。

次に，射影平面における変換を考える。再び，大平原に立って，遠くの方を見ているところを想像する。我々の目 (1 つに集約して) で見ると，目を中心点にして射影写像で一致するものは区別ができない。(距離は考えていない)

アフィン空間の座標のままでは，無限遠直線の表現ができない。何故なら，多くの人が誤解しているように ∞ は数字でない！それで，射影平面を 3 次元の空間に埋め込んで考えてみると，次のことがいえる。

定義 24 $P = (x, y, z)$ と $P' = (x', y', z')$ に対し，ある $k \neq 0$ があって，$x' = kx, y' = ky, z' = kz$ であるときに，P, P' は**同値**といい $P \equiv P'$ と表す。

この座標を用いると次のことがいえる。

(1) この同値類と射影平面の点とは一対一の対応が成り立ち，ユークリッド空間またはアフィン空間の点は $(x, y) \to \{(x, y, 1)$ の同値類 $\}$ で射影平面に埋め込むことができる。
(2) この対応で $l_\infty = \{(x, y, 0)$ の同値類 $\}$ となる。
(3) 射影平面の写像で，直線を直線に移す写像は $PGL(2, \mathbf{R}) = GL(3, \mathbf{R})/\{\mathbf{R}E\}$ である。

定理 30 ユークリッド平面における 2 次曲線 $ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$ は，上で述べた対応で射影平面の座標を用いると $ax^2 + cy^2 + fz^2 + 2bxy + 2eyz + 2dzx = 0$ と表される。

このユークリッド平面の固有の 2 次曲線は，$x^2 + y^2 - z^2 = 0$ だけである。即ち，射影空間では，円も双曲線も放物線も同じになってしまう。

理由を簡単に考えてみよう。アフィン幾何学のアフィン変換で，2 次曲線は $x^2+y^2 = 1, x^2-y^2 = 1, y = x^2$ のどれかに重ねることができた。これらを射影平面で考えると，$x^2 + y^2 = z^2, x^2 - y^2 = z^2, yz = x^2$ となる。最後の式は，yz–平面で $45°$ 回転させると $y^2 - z^2 = x^2$ となるから，3 曲線とも座標を入れ替えると同じになってしまう。

この定理の意味を無限遠直線との関係で説明する。まず，射影変換によると無限遠直線は目にみえる空間へ移すことができる。円が無限遠直線と離れているときは，特別のことはない。円が無限遠直線と 2 点で交わっているとき，無限遠直線を無限の方へ持っていくと，双曲線になる。円が無限遠直線と接するとき，無限遠直線を無限の方へ持っていくと，放物線になる。

5.4.5　クラインのエルランゲンプログラム

1872 年 10 月，クラインは 23 歳の若さでエルランゲン大学の教授に就任した。エルランゲン大学では，新任教授の就任に当たり自己紹介を兼ねて自分の研究分野の紹介と見識を述べる慣例があり，就任プログラムと呼ばれていた。クラインも自分の研究分野である幾何学と変換群との関係についてプログラムを書いた。結果として，クラインは色々な幾何学を変換群という視点に基づいて統一するという理論を提出した。

エルランゲンプログラムの意味をユークリッド幾何学，アフィン幾何学，射影幾何学で説明すると，それぞれの幾何学では図形を分類する原理は，それぞれの変換，合同変換，アフィン変換，射影変換であった。

クラインは，また，新しい幾何学の可能性も提案していた。それは，多様体という現代幾何学の基本領域となるべきもので，例えば，ある集合に直線を考えるには，次のものを定義する。

定義 25 集合 M 上の 2 つの点に対し実数値値をとる写像 ρ が次の性質を持つとき M 上の**距離関数**という。

(1) $\rho(x,y) \geqq 0$　ただし　$\rho(x,y) = 0 \Leftrightarrow x = y$ (正定符号性)
(2) $\rho(x,y) = \rho(y,x)$ (対称性)
(3) $\rho(x,z) \leqq \rho(x,y) + \rho(y,z)$ (三角不等式)

定義 26 集合 M 上に距離関数 ρ が定義されているとき，M の部分集合 l が「l の任意の 3 点 x,y,z に対して $\rho(x,z) = \rho(x,y) + \rho(y,z)$ が成り立つ」という性質を持つならば，l を (広義) の直線という。

距離関数 ρ は 2 点に対して直接定義しても良いし，積分などを介して定義しても良いが，その定義のもとになっているものを**計量**と呼んでいる。

クラインの考え方は，クラインの後に発見された「位相幾何学 (連続変形写像で重ねあわせができるものを同じとみなす分野)」や「代数幾何学 (複素領域の中で方程式の解曲線を研究する分野)」等にも影響を及ぼした。さらに，この原理は現在でも多くの数学の分野で何が研究されているかを分かり易く提示するのに使われている。最も数学以外にも敷延すると物理学も幾何学の一部になるのであるが。