四角い箱の中身

代数から
コンピュータへ

数を文字で表すようになって，人間の計算する力は一気に拡大しました。昔々，代数が誕生した頃のことです。
それから何百年かたって，私たちは再び計算の力が一気に拡大する時代を迎えます。コンピュータの誕生です。
科学技術や私たちの生活に飛躍的な進歩をもたらしたコンピュータの中には，ありとあらゆる「科学」が詰め込まれています。その中で数学は目に見えない部分，つまり論理的な部分をつかさどっています。
インターネットを見たり，メールを送ったり・・・あなたの目の前で今日も数学は懸命に活躍しているのです。

フェルマーの最終定理が証明されるまで

**350年間，誰も解くことができなかった数学の問題があります。それがフェルマーの最終定理です。
しかし，この超難問は1994年にワイルズというイギリス人によって解かれました。
そしてそのヒントを考え出したのは2人の日本人でもありました。**

フェルマーの最終定理とは？

350年以上も昔，近代整数論の始祖として活躍したフェルマーは，本の余白に次のように書き残しました。

「nが３以上の時に，方程式

$$x^n + y^n = z^n$$

を満たす自然数，x，y，zは存在しない。私はこのことの驚くべき証明を発見したが，この余白はそれを書くには狭すぎる。」

フェルマーの最終定理と呼ばれるこの言明を証明しようとして，多くの人が努力しましたが，果たせず，しかしその試みの中で新しい数学理論が次々と生まれました。

フェルマー
17世紀のフランスの数学者。
アマチュア数学者であったフェルマーは，整数論の研究以外にも，微積分学の先駆者としても知られ，またパスカルとの手紙は，確率論の先駆けとして有名です。資料提供：日本評論社

ワイルズ
フェルマーの最終定理をついに証明したのは，アンドリュー・ワイルズです。
ワイルズは，大変若い頃から，バーチとスウィグナートン・ダイヤーの予想について大きな仕事をするなど，整数論で大活躍をしてきた人です。
フェルマーの最終定理の証明では，構想を得てから長い間，屋根裏部屋にこもって研究を続けたと伝えられています。写真：PPS通信社

「ヒント」は日本人によって

1955年日光で開かれた研究集会で，出席者谷山は楕円曲線と保型関数についての一つの予想を提出しました。この予想は，後に志村によって，正確な形にされました。

1986年，フライは谷山・志村の予想を証明すれば，フェルマーの最終定理が証明されることを発見しました。

そして，ついに1994年，ワイルズによって，フェルマーの最終定理は証明されました。

ワイルズは，谷山・志村予想をフェルマーの最終定理の証明に必要な程度まで証明したのです。

谷山豊

谷山は，l 進表現，保型関数論などの数論の分野に独創的な業績を残しました。
おしくも若くして亡くなりましたが，その名前は，伝説の天才数学者として，世界中の整数論研究者の間で有名です。写真提供：日本評論社

志村五郎
志村は後にアメリカに渡り，プリンストン大学で，保型関数などの整数論の様々な分野の研究の，世界的な指導者として活躍しました。その名を冠する志村多様体は，整数論の研究の重要な対象として，現在でも盛んに研究されています。

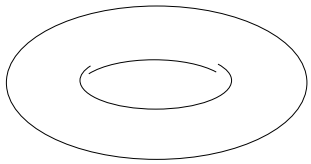
ワイルズの証明

ワイルズの証明は，$x^n + y^n = z^n$ の解（があったとして，背理法！），その解からあるやり方で決まる数 a，b について，式

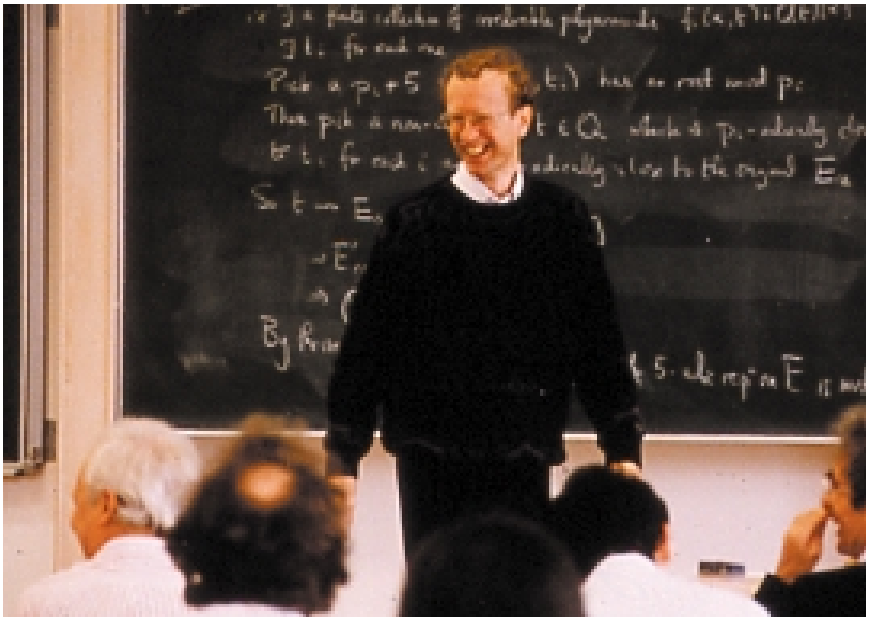
$$Y^2 = X(X-a)(X-b)$$

で表される図形を調べることでなされました。

この図形は，X，Y が複素数の範囲で考えると，図のような形をしていて，楕円曲線と呼ばれます。



楕円曲線



ガロア体と計算機

19世紀の若き天才数学者は「1+1=0」という，不思議な数学の世界を発見しました。
そしてその成果は時を超え，20世紀後半に発明されたコンピュータの中で開花することになりました。

1 + 1 = 0

1+1=0。こんな式が何かの役に立つと思う人はまずいないでしょう。

しかし，「1+1=0の数学」は，情報通信や確率シミュレーションにおいて不可欠の存在となっています。

コンピュータは情報を0,1の二値（ビット）の列にして，処理します。たとえば電子メールでアルファベットのAを送るには，00100001を送ります。

ガロア
19世紀フランスの数学者。その短い20年の生涯の中で，群，有限体（ガロア体）などの，多くの発見をして，数学の世界に革命をもたらしました。資料提供：日本評論社

$$x^5 + ax^4 + bx^3 + cx + d = 0$$

５次方程式
ガロア体は５次方程式の研究の中から発見された。

暗号化

ネットワーク上で情報を送るときには，ハッカーに情報が漏れるのを防ぐために，「暗号化」をして送信します。

暗号化をして情報を送るには，送る人と受ける人で，「合言葉」になる数字，たとえば01110011を決めておきます。そして，Aに対応する00100001を送りたいときには，合言葉の01110011を足して送るのです。

このときの足し算は，1+1=0の足し算です。

何万文字もある文書の暗号化をするには，短い合言葉では足りません。

そこで短い合言葉から長いでたらめな数の列を作ります。この列を作るところで，再び1+1=0の数学が活躍するのです。

+	0	1
0	0	1
1	1	0

2つの元からなるガロア体の足し算

×	0	1
0	0	0
1	0	1

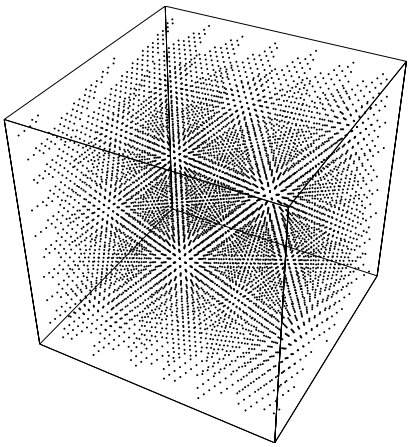
2つの元からなるガロア体のかけ算

ガロア体

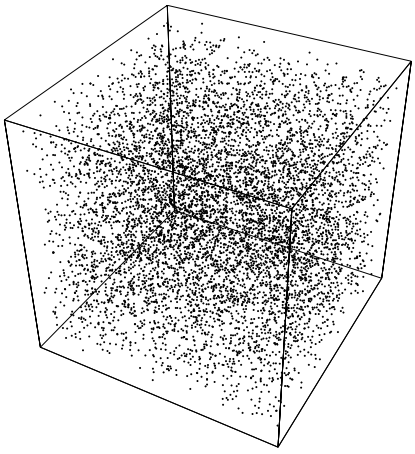
1+1=0の数学世界（ガロア体とよばれる）は，19世紀初めにガロアにより導入されました。

100年をへて，20世紀のデジタルコンピュータの発達によって，ガロア体には，思いもよらなかったような応用が見つかったのです。

それは，コンピュータの中では，1+1=0の数学世界の方が通常の数学世界よりずっと効率良く実現されるからなのです。



通常の1+1=2の計算規則を用いたC言語のプログラムrandにより生成された空間内の「ランダム」な点列
ランダムとは言い難い結晶構造が見られる。



1+1=0の数学に基づき，松本眞・西村拓士両氏が開発したメルセンヌツイスター法により生成されたランダムな点列
従来の生成法より遥かに乱数性が高く高速で，国内外で高く評価されている。

特異点解消と計算代数

人間が描く似顔絵と写真とはどこが違うでしょうか？似顔絵を描く時には，相手の特徴を捕らえて，時にはそれを思いっきり誇張して描きます。例えば八重歯だとかホクロだとか・・・。図形の「ホクロ」にあたるのが特異点です。図形の特徴が分かるためには，特異点をしっかり描かなければなりません。そのためには図形を表す式について理論的な考察をすることが大切なのです。

特異点解消の問題

多項式を使って定義される図形には，ところどころ，複雑に絡み合った特異点と呼ばれる部分があります。
方程式

$$x^2 + y^2 + z^3 = 0$$

で表される図形では，原点(0,0,0)が特異点です。

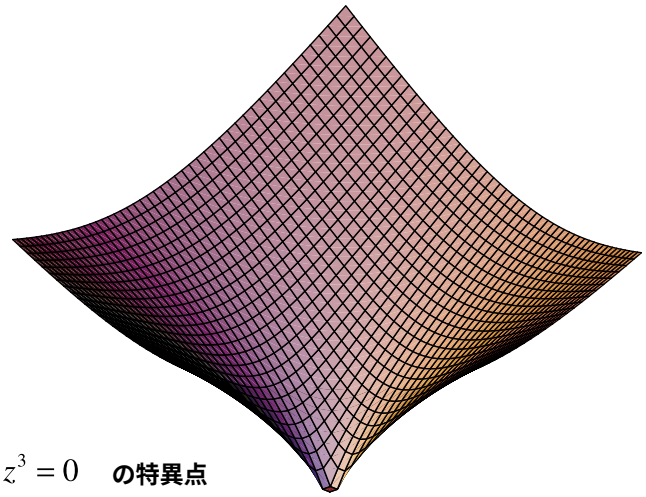
特異点があると，多項式を使って定義される図形を調べる上で，困難が起こります。

あるいは図形の持っている大切な情報が，特異点の回りのからまりの中に隠れてしまって見えづらくなります。特異点のからまりをほぐすのが特異点の解消の問題です。

下の図は数式処理ソフトでかいた，$x^2 + y^2 + z^3 = 0$ の特異点の絵です。

このような絵をコンピュータに書かせようとすると，特異点のところがなかなかきれいに書けません。

図の中で一番情報が詰まっている特異点のところを正しく理解するには，機械に任せてしまうのではなく，人間の頭で考える必要があるのです。



$x^2 + y^2 + z^3 = 0$ の特異点

廣中平祐　写真提供：日本評論社

標準基底

特異点解消の問題は，図形の次元が１，２の場合には19世紀に解決されていて，また図形の次元が３次元の場合には1944年にアメリカの数学者オスカー・ザリスキーが解決していました。

廣中平祐は1964年に発表した論文で，すべての次元の特異点の解消の問題を解決しました。

廣中の論文は，200余頁の長大なもので，証明に４重帰納法を用いる大作でした。

廣中は，特異点解消の問題を解決した論文の中で，図形を定義する方程式を調べるために，標準基底というアイデアを考えました（注）。

グレブナー基底

標準基底のアイデアは，多項式の計算をシンボリックに行う計算代数の中で再登場しました。

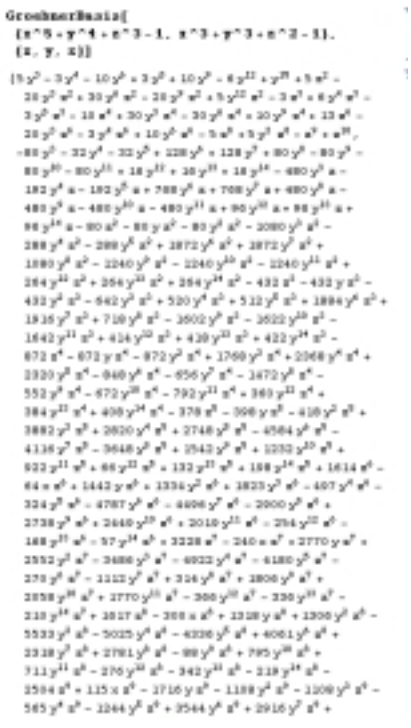
廣中より少し遅れて，ブックバーガーは廣中の標準基底と同じような概念に到達し，それをグレブナー基底と呼びました。

ブックバーガーは方程式の組を与えたとき，そのグレブナー基底を求めるやり方（アルゴリズム）を発見しました。

注：
廣中の標準基底とグレブナー基底には，局所的と大域的と言う差はがありますが，本質的なアイデアは同じです。

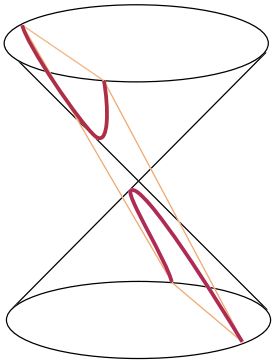
コンピュータによる発展

標準基底とその計算法は，電子計算機の発達に助けを借りて，これまで不可能だと考えられてきた，多項式のいろいろな計算を可能にしました。

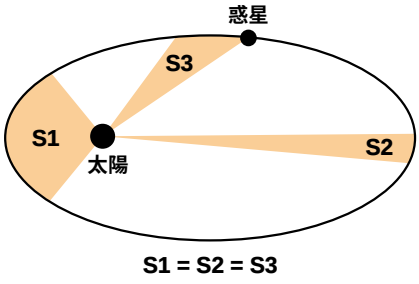


数式処理ソフト上でのグレブナー基底の計算

幾何学と理論物理学 2000年のつきあい

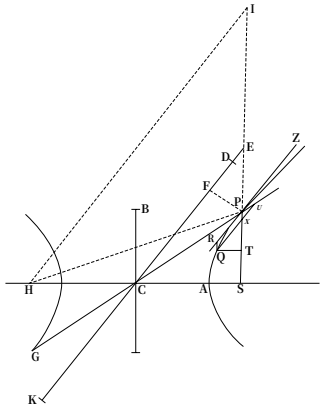


円錐曲線



ケプラーの第2法則

太陽と惑星を結ぶ線分が
一定時間に描く面積は一定である。



双曲線に沿った運動（プリンキピアより）

数学

前3世紀

ユークリッド：幾何学原論によって、論理的体系的に幾何学を記述。

前2世紀

アポロニウス：円錐曲線論（円錐曲線とは楕円、放物線、双曲線のこと）

16世紀

ケプラー：惑星の運動が円錐曲線であることを発見。

17世紀

ニュートン：ユークリッド幾何学原論のスタイルで、プリンキピア（自然哲学の数学的原理）を書き、重力理論によりケプラーの法則を説明。

18世紀から19世紀

ファラデイー・マックスウェル：場という考え方を用いて、電気力や磁力を幾何学的に説明した。

18世紀から19世紀

ガウス：曲面の幾何学。空間の曲がり方を表す量、曲率を発見。我々の住んでいる空間が曲がっているかを測量により調べようとした。

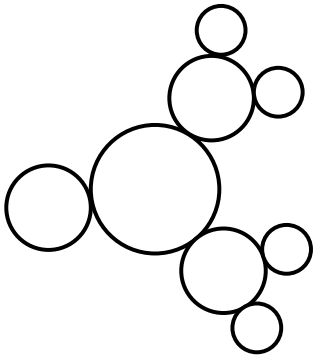
1860年代

リーマン：高次元の曲がった空間の幾何学、リーマン幾何学を創始。

$$\int_{\Sigma} g_{ij} \frac{\partial x^i}{ds^a} \frac{\partial x^j}{ds^b} h^{ab} ds^a ds^b$$

弦のエネルギー

南部の定式化をポリヤコフらが改良したものです。エネルギーから決まる運動方程式の解は，数学では調和写像と呼ばれます。



リーマン面の退化

弦理論とリーマン面

超弦理論はひもの運動で，物理現象を説明します。その数学的基礎はリーマン面で，これは，ひもが動いた跡である曲面の理論です。

リーマン面

$$\int_{\text{3角形}} \text{曲率} = \text{3角形の内角の和} - 180^\circ$$

ガウス・ボンネの定理

3角形の内角の和の，180 °からのずれが，空間の曲がり方ををあらわす。

$$ds^2 = \sum_{ij} g_{ij} dx^i dx^j$$

リーマン計量

曲がった空間で，長さや面積を定めます。

$$g^* A = g^{-1} dg + g^{-1} A g$$

ゲージ変換

素粒子物理学の標準理論は，ほとんどすべての力をゲージ理論で説明します。

$$R_{ij} = T_{ij}$$

アインシュタインの重力理論（一般相対性理論）の基本方程式

空間の曲がり方がその場所のエネルギー密度に比例するという式。

$$\int \| dA + A \wedge A \|^2 dx$$

ヤン・ミルズの汎関数

ゲージ理論の基本量であるヤン・ミルズ汎関数は，ゲージ場の曲率の2乗の積分です。

数学

19世紀末

ポアンカレ：高次元空間の大域幾何学（位相幾何学）を始める。

1910年代

アインシュタイン：重力は空間が曲がることから起きることを発見。

1920年～

ワイルやカルタンによって、ゲージ変換とか接続の概念が発見されました。

1920年代

カルサ・クライン：高い次元の空間を使う、統一場の理論を提唱。（当時は不評）。

1950年代

ヤン・ミルズ・内山：接続とゲージ変換に基づきゲージ場の理論を創始。

1960年代

ワインバーグ・サラム・グラショー：ゲージ理論によって弱い力と電磁場の統一理論を作る。

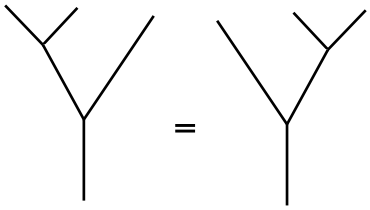
1970年代から

ゲージ理論や弦理論などで、次元の高い空間の幾何学や、大域幾何学が盛んに用いられるようになってきました。数学者の物理学への関心も、２０世紀の最後になって、再び高まってきました。

$$a \times (b \times c) = (a \times b) \times c$$

結合法則

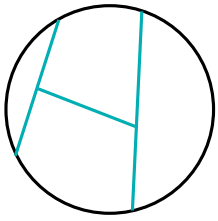
弦理論の基礎である交叉対称性は，かけ算の結合法則と関係があります。



交叉対称性

すべての力を統一する大統一理論になると期待される，超弦理論は，およそ２０世紀のありとあらゆる数学を使います。

超弦理論には２１世紀の数学が必要であろう・・・（といっている人もいます）



コード図

絡み合ったひもを研究する結び目理論と場の量子論が関わるところで登場します。