

研究内容（より詳しい内容については要望があれば別ファイルをお送りします。）

工学的な応用の話題を取り上げると、 学習理論、暗号理論に数学を応用できる。 離散対数問題(DLP)には、楕円曲線を使った暗号、楕円曲線暗号が用いられている。

【イントロダクション】

方程式表示された曲面を調べるといっても、例えば曲がりぐあいを調べるなど色々な見方が存在する。しかし各所の曲がりぐあいを調べても関数表示はできるかもしれないが、感覚的な意味合いで詳細によりすぎていて「木を見て森を見ない」といったことがある。場合によってはもっとマクロな意味合いで特徴づけをして分類をしたいという願望が生まれうる。補則するなら、犯罪者の手配書を警察の人が聴聞して作り上げるように、わざわざ人の顔をデジタルに局所、1ピクセルの明るさや色合いを調べなくても、例えば釣り目だとか、耳が大きいなどといった「特異な」情報の集合で有効な成果物が得られるのと同様のことが言える。曲面上の特異点と呼ばれる対象を分析することで欲しい情報が得られるのである。

【前準備】

「代数学の基本定理」について説明する。2次方程式を思い浮かべたときに係数が実数の場合だと解の個数が変わり、判別式というツールが必要となる。こういったことが起こらないように代数的に閉じられた数の範囲で考える。この文書上では、複素数のことと考えて影響はない。重要なのは「代数学の基本定理」という定理から、複素数の範囲の係数で考えることにより、最高次の次数に応じて解の個数を考えられる。 2次方程式なら2つ、3次方程式なら3つ、といった具合である

次に変数の数は最低でも2つ以上とする。例えば $y^2 = x^3 - x$ の様な式を考える。方程式を解いて $y = \dots$ という式に変形したときに右辺側では x など(2変数なら x のみ)で構成されるやや複雑な関数が現れる。

最後の下準備、幾何的な考察を組み入れる。方程式を通る点の集合として曲線や曲面が考えられる。もちろん平行移動の変換を行えば曲線や曲面の形自体は変わることはない。曲面上で無鉄砲に点を考えると、事実だけ言えば、大きな成果は得られないので、特別な点、特異点を考える。特異点とは非線形方程式の非線形たらしめる部分であるともいっている。

特異点が(0, 0)や(0, 0, 0)など原点を通るように平行移動をして考察する。 特異点判別には定理があるのだが例をいえば $y^2 = x^3 + t^2$ だと、(0, 0, 0)が特異点になる。

【具体的な研究内容】

ここから特異点はいくら拡大しても滑らかにならない尖った点ということにしておく。(厳密にはもう少し補足が要る)

具体的な特異点の研究方法というのは尖りぐあい、特異ぐあいを減らすことから始まる。特異点解消は、一例としては、曲線が2次元上のギリシャ文字の γ (ガンマ)のような図形だとして、そこに数軸を追加して3次元上でらせん状にするようなものである。

特異点解消とは有限回の、変数への代入変換から構成される。(例： $x = XY$, $y = Y$) 1回の変換でとがりぐあいが減っていく。ここでもしも変換前と変換後で完全に同等、同質だとすると最初から変換後を考えればいいということになるが、そのような事態は発生せず不可逆変換である。つまり性質を損なって、言い方を変えるとある種の犠牲を払って変換される。事実だけ言えば、ある種の犠牲とは元の曲面にはなかった直線が余計にできるということである。この変換でできる余計なものの情報を統合して数式化する。例としてコンポーネント(Component)の頭文字をとって“ $C_0 + C_1 + 2C_2 \dots$ ”のように表す。この直線の数や図形的な交わり方で曲面の特徴づけができる。 詳細や注意点がいくつかあるが、文面では伝わりにくいので省略する。

こうして方程式およびその曲面が2つあったとして一見異なるように見えて、ある観点では同じ性質を持つ、といったことができる。これは人が編み出した方程式や曲面という理論体系に新たに分類分けをすることができるという大きな成果である。すでに似たことを述べたが大雑把に言えばたとえ曲面の全体像が分からなくてもローカルな情報（特異点の近傍）によって分類することができるといっている。

勝手気ままに方程式設定をすればいいというものでもなく高い次数ばかりで定義されたものは処理が非常に難しいので、 いくらか条件付けをした上で処理の軽いものから順に解析した。 まず曲面を、連続に変形する線が山積みになって構成されたものとして考える。 そうなると事実だけ述べれば特異点を通る有限個の曲線と、 それ以外の線に分けて考えられる。「それ以外の線」は一括してネーミングできて、事実だけ述べれば曲面の名前もそこから決定することができる。 例をあげれば、ある種の高校課程で扱わない1段階レベルの高い曲線となると楕円曲線(例えば $y^2 = x^3 - x$)がある。それぞれの変数の次数をあげるとより解析が複雑になる。

特異点解消をすることは、 要点を的確に見抜き結論をまとめ上げることにつながり、 業務ワークに活用できる。