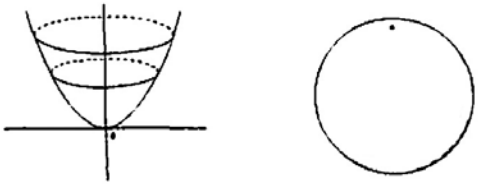
桂　利行

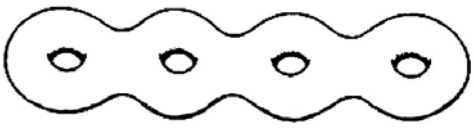
正標数の代数幾何と情報理論

代数幾何学は代数多様体という図形を研究する数学の分野である。代数多様体とは、単純化して述べれば、いくつかのn変数多項式の共通零点のなす図形であり、この図形を貼り合わせることによって一般の代数多様体が得られる。pをあるきまった素数とし、１をp個加えると０になるとき標数p、あるいは正標数であるという。正標数の世界で図形を考えれば複素数の世界で考えた時とは違う独特の現象が現れることがある。そのような現象を解明することが本研究の目的である。

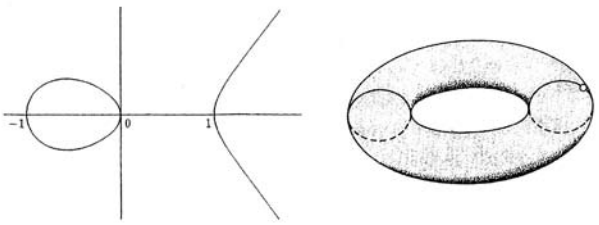
研究の対象が与えられた時、その対象を分類することはそれらをよりよく理解するために有力な方法である。代数多様体が与えられた時、独立に動きうる変数の数をその代数多様体の次元という。１次元代数多様体を代数曲線、２次元代数多様体を代数曲面という。代数多様体が滑らかで、尖ったり重なったりする点が存在しない時、非特異代数多様体という。また、無限に発散しないで閉じた代数多様体を完備代数多様体という。



ここでは、非特異で完備な代数多様体を研究の対象とし、それがどのくらい存在するか考察する。複素数を係数にする場合には、非特異完備代数曲線は、連続変形によって（位相的に）いくつか穴のあいた浮き袋のような形になるころが知られている。



この穴の数gを非特異完備代数曲線の種数という。種数は分類の重要な離散的不変量であり、種数が違えば代数曲線として異なる。種数が同じである代数多様体はどのくらい存在するのであろうか。これは連続パラメータの問題になるが、種数$g=0$のときには射影直線P^1ただ一つしか存在しない。種数$g=1$の代数曲線は楕円曲線といわれる。楕円曲線はj-不変量と呼ばれる任意の複素数を取りうる連続的不変量を持ち、j-不変量と楕円曲線が１対１に対応することが知られている。jの取りうる値全体は複素平面であるから、それをM_1とおいて楕円曲線のモジュライ空間という。種数$g\geqq 2$の代数曲線に対してもモジュライ空間M_gが存在し、種数gの代数曲線とモジュライ空間M_gの点が１対１に対応する。また、M_gは$3g-3$次元の代数多様体の構造を持つことが知られている。



２次元の場合にも離散的不変量による分類理論や、連続的不変量としての様々なモジュライ空間が構成されている。我々の研究では、アーベル曲面やK３曲面という小平不変量が０である代数曲面のモジュライ空間を取り上げ、正標数に於いて特有の部分多様体の構造を分析している。これは、１次元の場合には楕円曲線に対応する部分であり、豊かな構造を秘めている。高次元のアーベル多様体やK３曲面の一般化であるガラビ・ヤウ多様体のモジュライ空間も重要な研究対象である。

情報理論との関係については、１９８０年代はじめにGoppaによって、代数幾何符号が発見され、正標数の代数曲線の理論が誤り訂正符号の理論に用いられることが見い出された。その応用として、それまで知られていなかったVarshamov-Gilbert限界式を超えるような符号がTsfasman-Vladut-Zinkによって構成された。暗号理論に於いては、楕円曲線暗号が１９８５年にKoblitzとMüllerによって独立に発見され、現在では実用の域に達している。種数の大きな正標数の代数曲線のJacobi多様体を用いた暗号も考案されており、暗号理論で活用されている。代数幾何学とこのような領域の交流を図り、新しい知見を得ることも興味ある課題である。