楕円曲線の加群構造

非線形物理学　4sp01118 小堀敏行

1　序論　楕円曲線とは何か

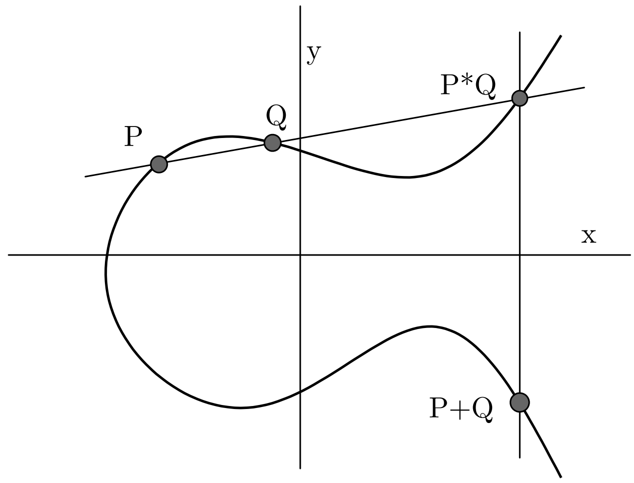
代数曲線とは「(２変数の多項式)$=0$」のことであり、その多項式の最大べき指数を代数曲線の次数という。２次の代数曲線の代表的なものに $x^2+y^2-1=0$ があり、これは単位円の方程式である。今回扱う楕円曲線とは次数が３次の代数曲線のことを言う。一般に３次曲線は $ax^3+bx^2y+cxy^2+dy^3+\cdots=0$ $(a,b,c,d,\ldots$ は定数$)$ と表せるが、任意の３次曲線は $y^2=x^3+ax^2+bx+c$ という Weierstrass の標準形に変形出来ることが知られているので、以降では、この Weierstrass の標準形を考える。また、３次多項式の全ての係数が有理数で表される曲線を有理３次曲線、曲線上の点が (x,y) 両座標ともに有理数である点を有理点と言う。

2　楕円曲線上の加法

楕円曲線上の２点の間に加法（足し算）が定義できることを以下で示す。３次曲線 C 上の３点 P,Q,O が与えられたとき、P と Q を結ぶ直線と C との交点を $P*Q$ と記すことにする。また、$P*Q$ と O を結ぶ直線と C との交点を $P+Q$ と定義すると以下に示す条件を満たすので、これは与えられた点 O を単位元とするような群とみなせる。以後は無限遠点を零元（単位元）にとる (図参照)。ある演算が足し算（加法）とみなせるための条件は４つある。

1. 零元（単位元）があること：　$P+O=P$
2. 逆元があること：　$Q+(-Q)=O$
3. 結合法則が成り立つこと：　P,Q,R を曲線C上の３点として、$(P+Q)+R=P+(Q+R)$
4. 可換であること：　$P+Q=Q+P$

有理３次曲線の場合、有理点どうしの加法はあきらかに部分群をなす。本卒業研究ではこの４つの条件が成り立つことを確認した。



3　具体例

Weierstrass 形の３次曲線上の２点 P_1+P_2 の座標を表す公式を求める。$P_1=(x_1,y_1),\ P_2=(x_2,y_2)$ とおき、P_1 と P_2 を結ぶ直線 $y=\lambda x+\nu$ が３次曲線と交わる３番目の交点を $P_1*P_2=(x_3,y_3)$ とすれば図より $P_1+P_2=(x_3,-y_3)$ となる。直線の方程式を３次曲線の方程式に代入すれば３番目の交点の座標は

$$x_3=\lambda^2-a-x_1-x_2,\ y_3=\lambda x_3+\nu$$

のように求まる。また、$2P=P+P$ の座標は上記の公式が使えないので別に求める必要がある。

具体的に公式を用いて３次曲線 $y^2=x^3+17$ 上での足し算を Risa/Asir というプログラムを使って計算した。この３次曲線には、$P_1=(4,9),P_2=(8,23)$ という有理点がある。これを足してみると $P_1+P_2=(1/4,33/8)$ という別の有理点を見つけることができた。

参考文献

楕円曲線論入門、J.H. シルヴァーマン/J. テイト　(シュプリンガー・フェアラーク東京)