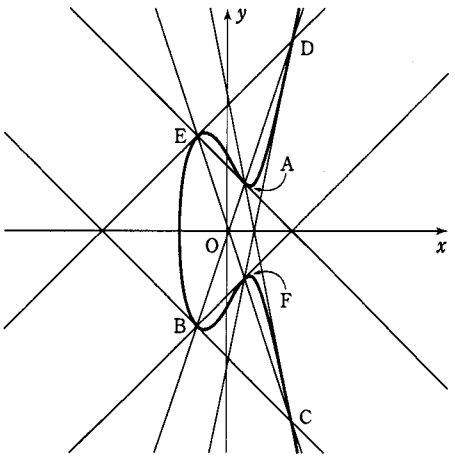
楕円曲線上のある群について

石濱（いしはま）　文武（ふみたけ）



§1　楕円曲線上の有理点・整点

曲線　　$y^2=x^3+ax^2+bx+c$

は楕円曲線（3次曲線）とよばれます．2次曲線の楕円ではありません．楕円の弧長を計算するときに現われるのが名称の由来です．

例えば，本稿で扱う楕円曲線 $y^2=x^3-43x+166$ のグラフは上の図のようになります．

x，y がともに有理数であるとき，点 $(x,\ y)$ を有理点といい，x，y がともに整数であるとき，点 $(x,\ y)$ を整点といいます．

整点 $(3,\ 8)$ が上記の楕円曲線上にあることを確かめてください．他に曲線上の整点をみつけることができるでしょうか．

本稿では，上記の楕円曲線上のある整点の集合がある演算に関して閉じていることを示します．

§2　楕円曲線上の演算（加法）

曲線 $C:y^2=x^3+ax^2+bx+c$（a，b，c は整数）上の有理点 P，Q（ただし，P，Q が x 軸に関して対称である場合を除く）に対して C 上の点 P+Q を次のように定義します．

> 直線 PQ（PとQが一致するときはPにおける C の接線）と曲線 C との共有点 R（これを P＊Qで表す）と x 軸に関して対称な点を P＋Qとする．

このとき，P+Q が C 上の有理点であることが次のようにして示されます．同時に定義の妥当性（well-defined）も示されます．

［i］　PとQが異なる点の場合

$P(x_1,\ y_1)$，$Q(x_2,\ y_2)$ とおくと直線 PQ の傾き m は　　$m=(y_2-y_1)/(x_2-x_1)$

より，m は有理数になり直線 PQ の方程式を

$$y=mx+n$$

とおくと　　$n=y_1-mx_1$

より，n も有理数になります．

直線 PQ の方程式と曲線 C の方程式を連立させて，y を消去すれば

$$x^3+ax^2+bx+c-(mx+n)^2=0$$
$$x^3-(m^2-a)x^2+(b-2mn)x+c-n^2=0$$

この x の3次方程式の解のうち2つは x_1，x_2 だから，残りの解を x_3（P＊Q の x 座標）とおけば，解と係数との関係により，

$$x_1+x_2+x_3=m^2-a$$
$$x_3=m^2-a-x_1-x_2$$

となって，x_3 は有理数になります．

P＊Q の y 座標は P＊Q が直線 PQ 上にあることから　　mx_3+n

で，有理数になり，P＊Q は有理点になります．

曲線 C は x 軸に関して対称だから，P＊Q を x 軸に関して対称に移動した点 P+Q も曲線 C 上の有理点になります．

［ii］　PとQが一致する場合

$y^2=x^3+ax^2+bx+c$ の両辺を x で微分して

$$2yy'=3x^2+2ax+b$$
$$y'=(3x^2+2ax+b)/2y$$

したがって，$P(x_1, y_1)$ (ただし $y_1 \neq 0$) とおくと，
P における接線の傾き m は

$$m=(3x_1^2+2ax_1+b)/2y_1$$

となり，m は有理数になります．

以下，[i] と同様にして，P＊P の x 座標は

$$m^2-a-2x_1$$

となって，P+P は曲線 C 上の有理点になります．

なお，このとき P+P=2P とし，一般に，

$$(n+1)P=nP+P \quad (n=1, 2, 3, \cdots\cdots)$$

と nP を定義します．

§3 具体例

§1で示した楕円曲線 $K: y^2=x^3-43x+166$ について§2で定義した加法を適用します．記号は§2と同様とします．($a=0$, $b=-43$, $c=166$, P=A)

K 上の有理点 A(3, 8) について

接線の傾きは　$m=-1$,
接線の方程式は　$y=-x+11$,
A＊A の座標は　(−5, 16)

となるので　2A(−5, −16)

となります．この点を B(−5, −16) とします．

同様にして，§2で示された式を使って計算すると (A+B)(11, −32) となり，この点を C(11, −32) とします．さらに，

A+C=D とおくと　D(11, 32),
A+D=E とおくと　E(−5, 16),
A+E=F とおくと　F(3, −8)

となって，A と F は x 軸に関して対称になります．

この他に新たな点は生成されません．例えば，B+C=E, B+D=F です．

以上の結果に基づいて，グラフを描くと冒頭の図のようになります．

§4 楕円曲線 K 上の有限群

§3で示された通り，K 上の整点の集合

$$S=\{A, B, C, D, E, F\}$$

は「S の 2 点を通る直線 (2 点が一致するときは接線) と K との共有点は S に属する」という性質をもっています．ただし，2 点が x 軸に関して対称である場合 (x 軸上にある場合を含む) を除いています．

この例外を解消するために

無限遠点○

を導入します．

2 点が x 軸に関して対称である場合は 2 点を通る直線 (x 軸上にある場合は接線) は y 軸に平行になるが，この直線は曲線 K と無限遠点○と交わるとする．

このようにすると，K 上の整点の集合

$$G=\{○, A, B, C, D, E, F\}$$

は§2で定義した加法に関して群 (有限可換群) になります．§3でみた通り，この群は A を生成元とする巡回群になります．すなわち

2A=B, 3A=C, 4A=D, 5A=E,
6A=F, 7A=○

となります．また A の位数は 7 であるといいます．B〜F の位数もすべて 7 になります．

また，各元の逆元については

−○=○, −A=F, −B=E, −C=D,
−D=C, −E=B, −F=A

となります．

§5 おわりに

楕円曲線論は豊富な内容を含んでいます．

> 非特異な 3 次曲線に有理点があれば，有理点全体は有限生成の群をなす[Mordell]．
>
> 整数係数非特異 3 次曲線の有限位数の有理点は整点である[Nagell-Lutz]．
>
> 整数係数非特異 3 次曲線上の整点は有限個である[Siegel]．

また，フェルマーの大定理

「方程式 $x^n+y^n=z^n$ ($n \geqq 3$, n は整数)
は自然数解をもたない」

の証明には楕円曲線論が使われています．暗号学では大きな整数の素因数分解に楕円曲線法[Lenstra のアルゴリズム]が使われます．

〈参　考　文　献〉

[1] シルヴァーマン／テイト (足立恒雄他訳)，楕円曲線論入門，シュプリンガー・フェアラーク東京㈱，1997.
原題：*Rational Points on Elliptic Curves*, 1992.
[2] 足立恒雄，フェルマーの大定理が解けた！，講談社ブルーバックス B-1074，1995.

(神奈川県立湘南高等学校)