楕円曲線のさまざまな側面

東京理科大学 創域理工学部 数理科学科 講師　松本（まつもと）　雄也（ゆうや）

代数学のうち代数幾何学は，代数的に定義される図形の性質を調べる分野ですが，代数学だけを使うわけではなく，数学の様々な分野と交差・連携します．本稿では代数幾何学の基本的かつ奥の深い対象である楕円曲線を軸に，いろいろな分野との関連を見ていこうと思います．

なお，本特集の吉川氏の記事では楕円曲線の整数論的側面が扱われますので，合わせてお読みいただければ幸いです．

1　R上の楕円曲線

$\mathbf{R}$ で実数全体の集合を表す．

$a,b\in\mathbf{R}$ に対し$\Delta:=-4a^3-27b^2$ とおく．以下，a,b は$\Delta\neq 0$ を満たすと仮定する．

$E(\mathbf{R}):=\{(x,y)\in\mathbf{R}^2\mid y^2=x^3+ax+b\}\cup\{\mathrm{O}\}$ とおく．ただし O は「無限遠点」であり，$\mathbf{R}^2$ の点ではなく，その外にあるものとする．このような図形を**楕円曲線**（*elliptic curve*）という．

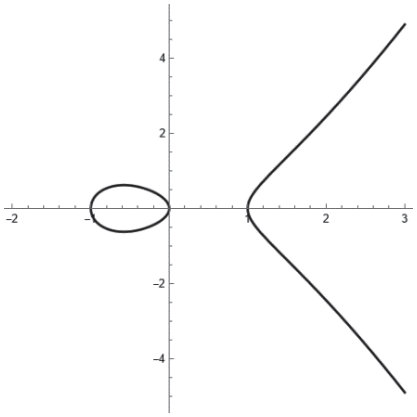
この曲線（無限遠点以外の部分）は x 軸に関し線対称であり，概形は次のいずれかになる．

- 2つの成分からなる．有界でない方の成分の $y>0$ の部分は単調増加である．（例【図 1】：$y^2=x^3-x$）
- 1つの成分からなり，$y>0$ の部分は単調増加である．（例【図 2】：$y^2=x^3+x-2$）
- 1つの成分からなり，$y>0$ の部分は単調増加ではない．（例【図 3】：$y^2=x^3-2x+2$）

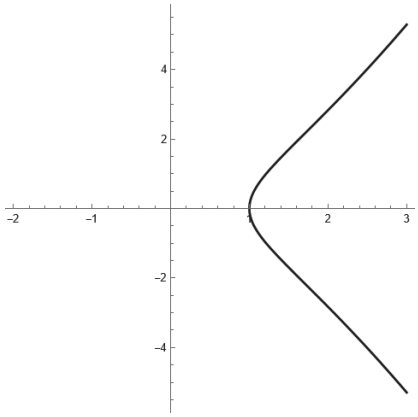
楕円曲線の著しい性質は「加法」が自然に定義されることである．$P_1,P_2\in E(\mathbf{R})$ に対し，その2点の和 $P_1\oplus P_2$ を以下のように定める．

- $P_1=(x_1,y_1),P_2=(x_2,y_2)$ が相異なる点で，2点を通る直線 L が y 軸に平行でない場合：L の方程式を $y=cx+d$ と書くと，連立方程式 $y^2=x^3+ax+b$，$y=cx+d$ から y を消去して得られる3次方程式は重複度を込めて3つの実数解 $x=x_1,x_2,x_3$ をもつ（なお，x_3 が x_1 や x_2 と一致する可能性もある）．$y_3=cx_3+d$ とおくと $(x_3,y_3)\in E(\mathbf{R})\cap L$ である．これを用いて $P_1\oplus P_2:=(x_3,-y_3)$ とする（y_3 にマイナスがついている点に注意）．
- $P_1=P_2=(x_1,y_1)$ かつ $y_1\neq 0$ の場合：L として E の P_1 における接線を考え（これは y 軸と平行にならない），以下は前項と同様にする．
- P_1 と P_2 が相異なる点で，2点を通る直線 L が y 軸に平行である場合：$P_1\oplus P_2=\mathrm{O}$ とする（第3の交点は無限遠点だと考える）．
- $P_1=P_2=(x_1,y_1)$ かつ $y_1=0$ の場合：L として E の P_1 における接線を考えると y 軸と平行になるので，前項と同様に $P_1\oplus P_2=\mathrm{O}$ とする．
- $P_1\oplus\mathrm{O}=P_1$，$\mathrm{O}\oplus P_2=P_2$，$\mathrm{O}\oplus\mathrm{O}=\mathrm{O}$ とする．

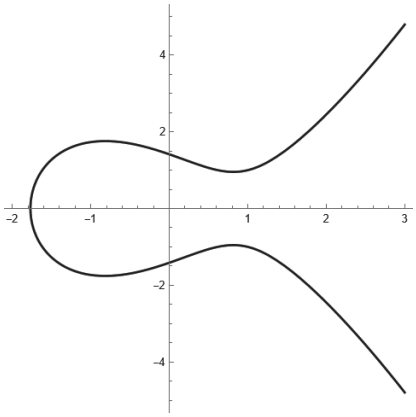
この加法は様々な性質を満たす．例えば，O は



【図 1】楕円曲線 $y^2=x^3-x$



【図 2】楕円曲線 $y^2=x^3+x-2$



【図 3】楕円曲線 $y^2=x^3-2x+2$

「ゼロ」の役割を果たし，また各元の「マイナス 1 倍」が存在する（具体的には，$P=(x,y)$ のマイナス 1 倍は $-P=(x,-y)$ である）．結合法則（$(P\oplus Q)\oplus R=P\oplus(Q\oplus R)$ が成り立つということ）の証明が実は難しいがここでは立ち入らない．$E(\mathbf{R})$ はこの加法に関して**アーベル群**（*abelian group*）をなす．

ここまでの話は，方程式の係数 a,b や点の座標 x,y として実数を考えてきたが，じつは実数でなくてもよい。より広く複素数で考えることもできるし，あるいは有理数の範囲に限定して考えることもできる．次節以降では考える領域をいろいろ変えて楕円曲線の様々な側面を見ていく．

2　Q 上の楕円曲線と有理点

Q で有理数全体の集合を表し，**Z** で整数全体の集合を表す．

$a,b\in\mathbf{Q}$ とし，前節と同様に $\Delta:=-4a^3-27b^2$ と定める．$\Delta\neq 0$ が成り立つと仮定する．

$E(\mathbf{Q}):=\{(x,y)\in\mathbf{Q}^2\mid y^2=x^3+ax+b\}\cup\{\mathrm{O}\}$ とおく．$E(\mathbf{Q})$ の点を**有理点**（*rational point*）とよぶ．前節と同じように $E(\mathbf{Q})$ の 2 点の和を定めると，和も $E(\mathbf{Q})$ の元になる．このことから $E(\mathbf{Q})$ もアーベル群になる．

以下，m 個の P の和を mP と書くことにする．

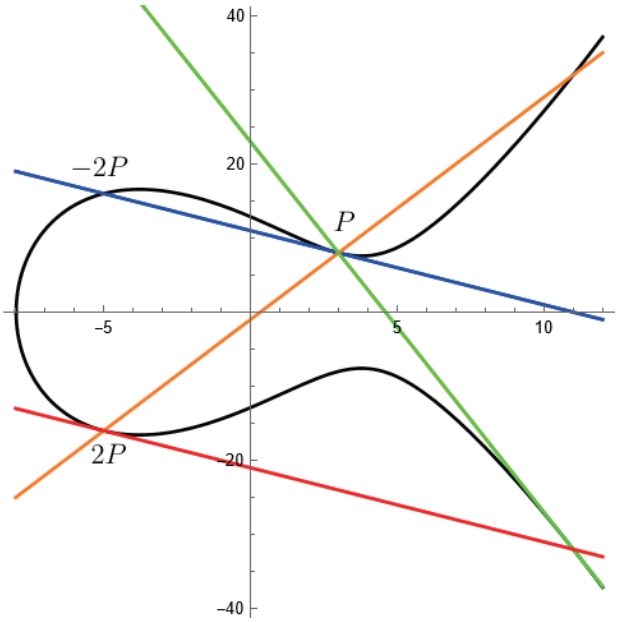
例：$y^2=x^3-43x+166$ において，$P=(3,8)$ とおくと，$2P=(-5,-16),3P=(11,-32),4P=(11,32),5P=(-5,16),6P=(3,-8)$ となり，$7P$ は O になる（**【図 4】**参照：P での接線が青い直線で，楕円曲線とのもう 1 つの交点は $-2P$ である，P と $2P$ を結ぶ直線が橙色の直線であるなど）．

ある正整数 $m\geq 1$ に対して $mP=\mathrm{O}$ となる点 $P\in E(\mathbf{Q})$ を**有限位数**（*finite order*）であるという（例えば，直前の例での P は $7P=\mathrm{O}$ を満たすので有限位数である）．そのような点について，Lutz-Nagell の定理が知られている：

定理．$a,b\in\mathbf{Z}$ で，$P=(x,y)\in E(\mathbf{Q})$ が有限位数の点ならば，$x,y\in\mathbf{Z}$ であり，y^2 は Δ の約数または 0 である．

系として，$E(\mathbf{Q})$ の有限位数の点は高々有限個であることも分かる（なぜならば，Δ の約数または 0 であることから y 座標は有限通りに絞られ，y 座標を決めると x 座標は有限通り（高々 3 通り）しかないので）．

より強い結果として，Mazur の定理によると有限位数の有理点は 16 個以下であることが知られている（ただし，証明はかなり難しい）．



【図 4】 楕円曲線 $y^2=x^3-43x+166$

以下では有限位数でない点も含めて考える．$E(\mathbf{Q})$ は無限集合である場合もあるが，次の Mordell の定理が知られている．

定理．有限個の点 $P_1,\ldots,P_n\in E(\mathbf{Q})$ が存在して次が成立する：任意の $Q\in E(\mathbf{Q})$ は，$P_1,\ldots,P_n$ から足し算（と引き算）を繰り返して作ることができる．

このことを，$E(\mathbf{Q})$ は**有限生成**（*finitely generated*）なアーベル群である，という．n の値が E によらない定数で抑えられるか，それともいくらでも大きくなりうるのかは知られていない．いくらでも大きいものが存在すると予想されていると聞いたこともあるが，限界があることを示唆する議論もあると（比較的最近）聞いたことがある．現時点での記録としては，$n\geq 28$ を必要とする例が Elkies により発見されている．

3　C 上の楕円曲線と楕円関数

$\sin\colon\mathbf{R}\to\mathbf{R}$ は周期 2π をもち $(\sin(x+2\pi)=\sin(x))$，C^∞（無限回微分可能）である．とくに連続であり，連続かつ周期的なので有界である．

C で複素数全体の集合を表す．sin の複素関数版を考える．実は，次を満たす関数 $\sin\colon\mathbf{C}\to\mathbf{C}$ がただ一つ存在することが知られている．

- 定義域を **R** に制限すると（ご存じの）正弦関数 sin に一致する．
- 各 $z\in\mathbf{C}$ に対して，h が複素数として 0 に近づく

ときの極限 $\lim_{h\to 0}\frac{\sin(z+h)-\sin z}{h}$ が存在する．この（複素数の意味での）微分ができる関数を**正則関数**（*holomorphic function*）という．

この関数も周期 2π をもつ（$\sin(z+2\pi)=\sin(z)$）が，虚数方向の周期はない．また，有界ではない．

次のような**二重周期関数**（*doubly periodic function*）$f\colon \mathbf{C}\to\mathbf{C}$ は存在するか？　という問題を考える．

・f は正則である．

・f は 1 および虚数 τ を周期にもつ．

そのような f は（連続かつ周期的なので）有界になるが，有界な正則関数は定数関数しか存在しないという複素解析学の Liouville の定理から，そのような f は定数関数しか存在しないことが分かる．

そこで，$\mathbf{C}$ 全体で定義された正則関数という条件を少し緩めることにする．τ を虚数とし，$\Lambda=\{m+n\tau\,|\,m,n\in\mathbf{Z}\}$ とおく（このような集合を**格子**（*lattice*）とよぶ）．このとき，Λ の補集合 $\mathbf{C}\setminus\Lambda$ から $\mathbf{C}$ への関数 $\wp$ で次を満たすものがただ一つ存在することが知られている．これを**ワイエルシュトラスの $\wp$ 関数**（*Weierstrass $\wp$-function*）という（「ペー関数」と読む）．

・$\wp$ は（$\mathbf{C}\setminus\Lambda$ 上の）正則関数である．

・$\wp$ は $\wp(z)=\wp(z+1)=\wp(z+\tau)$ を満たす．言い換えると，任意の $\omega\in\Lambda$ に対して $\wp(z)=\wp(z+\omega)$ を満たす．（このことを，$\wp$ は Λ を周期にもつという．）

・$\wp(z)-\frac{1}{z^2}$ は $z=0$ の近傍上の正則関数である．

最後の条件は，$\wp(z)$ が $z=0$ で 2 位の**極**（*pole*）をもつことを意味する．このことと周期性から，Λ の各点でも同様に 2 位の極をもつ．

$\wp$ のように，極以外で正則な二重周期関数を**楕円関数**（*elliptic function*）という．歴史的には，楕円の弧長を求める積分を楕円積分といい，その逆関数として楕円関数が導入された．（比較：円の弧長は逆三角関数により求められ，その逆関数である三角関数は周期関数である．）

実は $\wp$ 関数と楕円曲線には密接な関係がある．詳細は省略するが，ある（τ に依存して定まる）複素数 $g_2,g_3\in\mathbf{C}$ に対して $\wp'(z)^2=4\wp(z)^3-g_2\wp(z)-g_3=0$ が成り立つことが知られている（$\wp'$ は $\wp$ の微分）．したがって，$y^2=4x^3-g_2x-g_3$ で定まる楕円曲線を $E(\mathbf{C})$ とおくと，$(\wp(z),\wp'(z))$ は $E(\mathbf{C})$ の点になっていることが分かる．（x^3 の係数が 4 なので本稿で述べた楕円曲線の定義とは厳密には異なるが，簡単な変数変換でこの係数を消すことができるので気にしなくてよい．）

写像 $\Phi\colon\mathbf{C}\to E(\mathbf{C})$ を，$\mathbf{C}\setminus\Lambda$ の点 z は $(\wp(z),\wp'(z))$ に送り，Λ の点は $E(\mathbf{C})$ の無限遠点 O に送ることにより定める．

ここで $0,1,\tau,1+\tau$ を頂点とする平行四辺形を考え，向かい合う辺同士を張り合わせることで $\mathbf{C}/\Lambda$ という複素トーラスを作る．（より数学者好みの言い方をすれば，差が Λ の元であるような $\mathbf{C}$ の 2 元は同一視するという同値関係による商集合をとる．）$\wp$ 関数の周期性から，張り合わされる点は Φ で同じ点へ行くので，Φ は $\mathbf{C}/\Lambda$ から $E(\mathbf{C})$ への写像を定め，しかもこれは全単射（一対一対応）になる．したがって，この写像を通して複素トーラスを $\mathbf{C}$ 上の楕円曲線と同一視することができる．

この同一視を通して，複素トーラスに関する複素幾何的・複素解析的な問題を楕円曲線の代数的な問題と捉え直して考えることも，その逆もできることになり，考え方の幅が広がる．

ちなみに，トポロジー的には $\mathbf{C}/\Lambda$ は 2 次元トーラス，あるいは種数 1 の閉曲面とよばれる図形になる：これはいわゆるドーナツ型であり，いわゆる 1 人乗りの浮き輪の形でもある．

4　有限体上の楕円曲線

まず「有限体」について述べる．p を素数とする．$\mathbf{F}_p:=\{0,1,\dots,p-1\}$ とする．$\mathbf{F}_p$ の 2 元の和・差・積を，整数としての和・差・積を p で割った余りとして定める．すると 0 以外の元による割り算が（掛け算の逆演算として）定義できる．このように四則演算ができる集合のことを**体**（たい）（*field*）という．$\mathbf{Q},\mathbf{R},\mathbf{C}$ も体である．$\mathbf{F}_p$ は有限集合でもあるので**有限体**（*finite field*）という．（$\mathbf{F}_p$ についても，数学者好みの定義は，$\{0,1,\dots,p-1\}$ ではなく，$\mathbf{Z}$ の適切な同値関係による商集合（剰余環）とするものである．）

$\mathbf{F}_p$ においては $1+\cdots+1=0$（左辺は p 個の 1 の和）が成り立つ．このことを標数 p という，これに対して $\mathbf{R}$ や $\mathbf{C}$ などは標数 0 という．標数 p は一見怪しい世界に見えるが，代数幾何学の多くの部分は標数 p の場合でも標数 0 の場合と同様に展開できる．

p を素数とする．都合により $p\geq 3$ と仮定しておく．（本当は $p=2$ の場合も扱えるが，式が煩雑になるのを避ける）a,b は整数で，Δ が p で割れないものとする．

$E(\mathbf{F}_p):=\{(x,y)\in\mathbf{F}_p{}^2\,|\,-y^2+x^3+ax+b$ は p で割りきれる$\}\cup\{\mathrm{O}\}$ とおく．このような $\mathbf{F}_p$ 上の楕円曲線にも 1 節と同様に加法を定義できる．この場合直線

とは，$c,d,e\in\mathbf{F}_p$（c,d の少なくとも一方は 0 と異なる）を用いて，$L=\{(x,y)\in\mathbf{F}_p^2 \mid cx+dy+e$ は p で割りきれる$\}$ と書ける集合である．

標数 p の楕円曲線の中には，標数 0 の楕円曲線では起こらない性質をもつものがある．それらを**超特異**（*supersingular*）であるといい，そうでないものを**通常**（*ordinary*）であるという．超特異の同値な定義（特徴づけ）がいくつかある．比較的少ない前提知識で説明できるものとして次がある．

- $\mathrm{End}(E)$ を，E から E への“正則な”写像で O を O にうつすもの全体の集合とする．$\mathrm{End}(E)$ の元は合成することができる．$f,g\in\mathrm{End}(E)$ で $f\circ g\neq g\circ f$ を満たすものが存在するとき，$\mathrm{End}(E)$ は**非可換**（*non-commutative*）であるという．$\mathrm{End}(E)$ が非可換であるとき E を超特異であるという．
- $|E(\mathbf{F}_p)|-1$ が p で割りきれるとき，E を超特異であるという．
- $E(\mathbf{F}_p)$ は x,y 座標が $\mathbf{F}_p$ に属する点のみを考えているが，より大きい領域まで広げて考え，$pP=\mathrm{O}$ を満たす点 $P\neq\mathrm{O}$ が存在しないとき E を超特異であるという．

例を挙げる．$y^2=x^3-x$ が定める楕円曲線 E は（$\Delta=4$ なので）2 以外のすべての素数 p に対する $\mathbf{F}_p$ 上の楕円曲線と考えられる．p が 4 で割って 1 余る素数のときは通常であり，4 で割って 3 余る素数のときは超特異であることが知られている．ただし，通常と超特異をこのように簡単に判別できる楕円曲線はむしろ例外的である．

楕円曲線だけでなく，より高次元の（正標数の）代数多様体についても，「通常」や「超特異」などの概念が定義されることがある．私は主に正標数の超特異 K3 曲面を研究しております．

5　有限体上の楕円曲線の応用

$E(\mathbf{F}_p)$ の点およびその加法は整数だけで表現できるので，コンピュータで実装でき，数々の応用がある．

$E(\mathbf{F}_p)$ の点 P と正整数 m に対して，mP（m 個の P の和）を計算することは難しくない．一方で，2 点 P,Q が与えられたときに，$Q=mP$ を満たす正整数 m を見つけることは難しい．（一般に，アーベル群に対するこのような問題を**離散対数問題**（*discrete logarithm*）という．）このことを利用した暗号プロトコルがある．

また，2 つの楕円曲線の間に**同種**（*isogenous*）という関係が定義されるのだが，超特異楕円曲線の間の同種関係を用いた暗号プロトコルもある．

$E(\mathbf{F}_p)$ の点の和を計算する際には，「$0<n<p$ を満たす整数 n に対し，mn が p で割って 1 余る整数 m をみつける」という操作を頻繁に行うことになる（m が $\mathbf{F}_p$ における「n 分の 1」である）．これには（p と n に対して）ユークリッドの互除法を使う．p が素数ならば，p と n は互いに素でありそのような m は必ず存在する．もし p が素数でなく，p と n が互いに素でないときは，ユークリッドの互除法により最大公約数（$\neq1$）がみつかる．これを逆手にとって，素数でないことは分かっているが非自明な約数が知られていない整数 p に対して，“$E(\mathbf{F}_p)$ の点の和”をひたすら計算することで非自明な約数をみつける，という Lenstra の素因数分解アルゴリズムが知られている．

参考文献

- Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. 足立恒雄，木田雅成，小松啓一，田谷久雄（訳），楕円曲線論入門，丸善出版，2012.
- Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. 鈴木 治郎（訳），楕円曲線の数論，共立出版，2023.