暗号と楕円曲線

松本　眞[1]

平成 31 年 1 月 29 日

[1]広島大学理学部数学科 m-mat@math.sci.hiroshima-u.ac.jp

目 次

第1章　通信

インターネット通信を念頭におく。

1.1　暗号

1.1.1　イントロダクション

Alice は Bob にメッセージを伝えたいとする。

定義 1.1.1. 暗号（鍵なし）とは、平文 (plain text) の集合と呼ばれる集合 P、暗号化文 (ciphered text) の集合と呼ばれる集合 C、暗号化関数 (encrypting function) と呼ばれる写像 $e : P \to C$、復号化関数 (decrypting function) と呼ばれる写像 $d : C \to P$ で、任意の $m \in P$ に対して $d(e(m)) = m$ となるものである。

Alice は P, C, e を計算できる計算機を持ち、Bob は P, C, d を計算できる計算機を持つ。

Alice がメッセージ $m \in P$ を送りたいとする。Alice は $e(m)$ を危険な通信路（第三者 Oscar が盗聴できる通信路）を用いて Bob に送る。Bob はもらった $e(m)$ に対して $f(e(m))$ を計算することで元の m を知ることができる。Oscar は $e(m)$ を知ることができるが、そこから m を推測することは必ずしもできない。安全な暗号を作るには、推測が困難なように e を設計する必要がある。

定義 1.1.2. N を自然数とする。$\mathbb{Z}/N := \{0, 1, \ldots, N-1\}$ と置く。$\mathbb{Z}/N$ における和、差、積はすべて $\bmod N$ で（すなわち、いちいち N で割った余りをとって）計算することで、$\mathbb{Z}/N$ の元を与える。これにより、$\mathbb{Z}/N$ は単位元をもつ可換環となる。N が素数 p であるとき、$\mathbb{Z}/p$ は体となる。

例 1.1.3. (Caesar 暗号) アルファベット 26 文字を $\mathbb{Z}/26 = \{0, 1, \ldots, 25\}$ と順番に一対一対応させる。そして $P = C = \mathbb{Z}/26$ とし、$e(m) := m + 3$, $d(m) := m - 3$ とおく。$d(e(m)) = m$ なので、これは暗号である。

実際には、メッセージはアルファベットからなる列 $m_1, m_2, \ldots$ である。この場合、Alice は $e(m_1), e(m_2), \ldots$ を暗号化文として Bob に送る。Bob はそれぞれの元に d を施して復号する。

Oscar は、$e(m_1), e_(m_2), \ldots$ に対し、$k = 0, 1, 2, \ldots, 25$ について $e(m_1) - k, e(m_2) - k, \ldots$ を計算する。アルファベットに直したとき、意味の通る文になっていれば、その k が正しい「カギ」であることがわかる。この場合は $k = 3$ である。こうして、Caesar 暗号は容易に破られる。

さて、世界には沢山の人がインターネットなどで通信している。それらの人が同じアルゴリズム（あるいはプログラム）で暗号化通信をできれば、便利である。（というより、通信した

い二人がいるごとに、e, d をまったく別の方法で作るということは非現実的である。）そこで、鍵の集合 K というものを考えて、$k \in K$ ごとに $e_k : P \to C$, $d_k : C \to P$ で暗号となっているものを考えるのがふつうである。このとき、通信したい二人は K の元 k を一つとり、e_k と d_k で上述のような暗号化通信を行う。

定義 1.1.4. 暗号（鍵あり）

平文の集合 P、暗号文の集合 C、鍵の集合と言われる K があり、各 $k \in K$ に対し $e_k : P \to C$, $e_k : C \to P$ が上の意味で暗号となっているとき、共有鍵暗号という。

1.1.2 Diffie-Hellman 鍵共有

A さんと B さんが直接会ったりせずに、C さんに見られている通信路を使って鍵を共有することはできないか？

⇒ Diffie Hellman 鍵共有　(1976, 最初に提案された公開鍵暗号)

G を離散ログ問題を解くのが難しい群 (G の元 h と g から $g^n = h$ なる自然数 n を計算するのに宇宙の寿命以上の時間がかかるような群) とする。

以下、簡単のため、G は位数が素数 p の巡回群とする。

1. $a \in G$ を決めて、a, G をみんなに公開する。
2. A さんは $n \in \mathbb{Z}/p$ をでたらめに選ぶ (だれにも教えず記録しておく)
3. B さんは $m \in \mathbb{Z}/p$ をでたらめに選ぶ (だれにも教えず記録しておく)
4. A さんは、a^n を計算して通信路で B さんに送る
5. B さんは、a^m を計算して通信路で A さんに送る
6. A さんは、受け取った数を n 乗して結果を鍵とする
7. B さんは、受け取った数を m 乗して結果を鍵とする

事実：ある種の G では、p が大きいとき、$a \in G$ に対して a^n を計算することは計算機を使えば容易だが、a と a^n が与えられて n を求めることは計算が著しく難しい (離散対数問題 discrete log problem という)。有限体上の楕円曲線の有理点のなす群はこのような性質を持つと思われている（一部例外除く)。

1. C さんが見られる情報：a, a^n, a^m, G
2. A さんだけが持っている情報 n
3. B さんだけが持っている情報 m
4. B さんが送ってきたものを n 乗すれば A さんは $(a^m)^n$ を得る
5. A さんが送ってきたものを m 乗すれば B さんは $(a^n)^m$ を得る

G では $(a^m)^n = (a^n)^m$。これにより、A さんと B さんが秘密の共有鍵をもつことができる。(これを暗号の鍵として使う)。

注意 1.1.5. a, a^n, a^m, G から a^{nm} を求める問題を DH 問題という。離散対数がもとまれば解ける。DH 問題から離散対数問題がとけるかは未解決。

レポート問題 1. 上の「G では $(a^m)^n = (a^n)^m$」を示せ。
一般に、a が半群の元なら $(a^m)^n = (a^n)^m$ となることを証明せよ。
結合法則が成り立たない場合には、これが成立しない例があることを示せ。

1.1.3 どのような群が暗号に使えるか

$\rho : G \to \mathrm{Aut}(X)$, X が小さい集合だと、軌道を調べて DLP がとけてしまう。
有望なのは $G = \mathbb{F}_p^\times$ p 素数、2^{1024} 以上 $G = \mathbb{F}_q^\times$ $q \geq 2^{1024}$
一番ポピュラーなのが G を有限体上の楕円曲線の有理点のなす群とするものである。（楕円曲線暗号）G の位数は $\geq 2^{250}$ （電子カードなどでは、使えるメモリが限られているので後者が有利）

1.2 楕円曲線

1.2.1 イントロダクション

K 体
K 上の楕円曲線 E とは、K 上の種数 1 の非特異 proper 代数曲線で、$E(K)$ が指定されているもの。
(Hartshorn)
この定義を説明するのは大変。初等的な言葉で述べられることを述べる。

1.2.2 Weierstrass Equations

K 上の Weierstrass equation とは $y^2 = x^3 + Ax + B$, $A, B \in K$ ただし $4A^3 + 27B^2 \neq 0$ のこと。これは elliptic curve E を与える。
条件は、式の右辺が重根をもたないことと同値。
$K \subset L$ 拡大体のとき、$E(L)$ とは上の L における解の集合に、∞ という元を付け加えたもの。これが群の台集合になる。
一般化 Weierstrass equations: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ 標数 2,3 でないときは Weierstrass equation にできる。

1.2.3 K=$\mathbb{R}$ の場合

$y^2 = x^3 - x$, $y^2 = x^3 + 1$
∞ は y 軸にそって∞にある点（あとで説明）∞ を通る直線とは、$x = c$。

1.2.4　群演算

K 体 Weierstrass equation において、$\infty \in E(L)$ を 0 元とし、$E(L)$ の点 P_1, P_2, P_3 が一直線上にあるとき、$P_1 + P_2 + P_3 = 0$ となるよう演算 $+$ を定義する。

P の y 座標の符号を反転したものが $-P$ となる。

(x_1, y_1), (x_2, y_2) を座標とすると

$P_1 \neq P_2$ の場合、P_1, P_2 を含む直線 L をもとめる。傾き $m = \frac{y_2 - y_1}{x_2 - x_1}$

$x_2 = x_1$ のとき：L は ∞ を含む。$P_1 + P_2 + 0 = 0$ より $P_1 + P_2 = 0$.

そうでないとき：$y = m(x - x_1) + y_1$.

代入すると $0 = x^3 - m^2x^2 + \cdots$

根と係数の関係から

$x = m^2 - x_1 - x_2$。

$y = m(x - x_1) + y_1$ (L 上にのる。)

$(x, -y)$ が $P_1 + P_2$ である。

$P_1 = P_2$ のときは、「接線」を引く。実数体以外一般の体では、$y^2 = x^3 + Ax + B$ と $y = m(x - x_1) + y_1$ が $(x - x_1)$ で重根をもつように m を定める。

y を消去して

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

この式の左辺引く右辺が $(x - x_1)^2$ で割り切れればよい。$(x - x_1)^2$ で割った余りを考えると

$$2my_1(x - x_1) + y_1^2 - x^3 - Ax - B$$

$y_1^2 = x_1^3 - Ax_1 - B$ を代入して

$$2my_1(x - x_1) + (x_1^3 - x^3) + A(x_1 - x)$$

これは $(x - x_1)$ で割り切れて商が $2my_1 - (x^2 + xx_1 + x_1^2) - A$ これがもう一度 $(x - x_1)$ で割り切れる必要十分条件は $2my_1 - 3x_1^2 - A = 0$.

$y_1 = 0$ のとき、$3x_1^2 + A \neq 0$ である。これは、$x^3 + Ax + B$ が x_1 を根に持つが重解をもたないことから従う。(一般の体で、多項式 $f(x)$ の微分が定義できる。「$f(x_1) = 0$ かつ $f'(x_1) = 0$」が $f(x)$ が $(x - x_1)^2$ で割り切れることと同値。) よってこのような m は存在しない。このとき接線は $x = x_1$。実際、$y^2 = x_1^3 + Ax_1 + B = 0$ は重根をもつ。この直線の $E(L)$ との交点は ∞ である。

$y_1 \neq 0$ のとき、$m = \frac{3x_1^2 + A}{2y_1}$ と定まる。(ただし、体の標数が 2 でないときのみ。標数 2 のときには、Weierstrass equation は特異点をもち、楕円曲線を与えない。)

m が定まれば、$x = m^2 - 2x_1$

$y = m(x - x_1) + y_1$

で $(x, -y)$ が P_3。

可換群の公理を満たすことの証明は、associativity 以外はやさしく、associativity は難しい。

まとめ

定義 1.2.1. E を Weierstrass equation $y^2 = x^3 + Ax + B$ が与える K 上の楕円曲線とする。拡大体 $K \subset L$ に対し、$E(L)$ は次の二項演算 $+$ を持つ。

$P_1, P_2 \in E(L)$ とする。$P_3 = P_1 + P_2$ を以下のように定義する。

1. いずれかが ∞ なら $P+\infty=\infty+P=P$ で定義
2. どちらも ∞ でないとき、$P_1=(x_1,y_1), P_2=(x_2,y_2)$ とおく。
3. $x_1 \neq x_2$ のとき、$m=\frac{y_2-y_1}{x_2-x_1}$ とおく。$P_3(x_3,y_3)$ とするとき、$x_3=m^2-x_1-x_2$, $y_3=m(x_1-x_3)-y_1$.
4. $x_1=x_2, y_1\neq y_2$ のとき、$P_1+P_2=\infty$.
5. $P_1=P_2$ かつ $y_1\neq 0$ のとき、$m=\frac{3x_1^2+A}{2y_1}$ とおいて
   $x_3=m^2-2x_1$
   $y_3=m(x_1-x_3)-y_1$.
6. $P_1=P_2$ かつ $y_1=0$ のとき、$P_1+P_2=\infty$.

定理 1.2.2. $(E(L),+)$ は ∞ を単位元とする可換群である。

1. $P_1+P_2=P_2+P_1$
2. $P+\infty=P$
3. P の y 座標の符号を反転させたものを P' とすると $P+P'=\infty$
4. $(P_1+P_2)+P_3=P_1+(P_2+P_3)$ (associativity)

associativity 以外の証明は自明である。associativity の証明は、定義に基づいて数式処理システムで計算することで確かめられる。

自然な証明は、$E(\overline{K})$ が $E_{\overline{K}}$ の次数 0 の因子類群 (divisor class group) と一対一対応であることを示すものであるが、ここでは触れない。

注意 1.2.3. 実は、K の標数が 2 の時には、Weierstrass equation は特異曲線となり楕円曲線を与えないし、上の計算は実行できない。

レポート問題 2. K の標数が 2 の時には、上の計算はどこで破たんするか？

レポート問題 3. $x^3+Ax+B=0$ に重根があるときには、上の計算はどこで破たんするか？

1.2.5 複素数体上の楕円曲線

$\mathbb{C}$ 上の楕円曲線 E に対し、$E(\mathbb{C})$ は二次元トーラスと位相的に同型になる。それどころか、$\mathbb{R}$ 上一次独立な $1,\tau$ ($\tau\in\mathbb{C}$) が存在して、$\mathbb{C}/<1,\tau>_{\mathbb{Z}}$ と複素多様体としても、位相群としても同型になる。可換群 A に対してその n-torsion（捻じれ）point の集合を $A[n]:=\{a \mid na=0\}$ とおくと、

$$E(\mathbb{C})[n]=\{\frac{i}{n}+\frac{j}{n}\tau \mid i,j=0,\ldots,n-1\}$$

となり、群としては $\mathbb{Z}/n\times\mathbb{Z}/n$ と同型である。ふしぎなことに、有限体でもこれに似た現象が観察される。

1.2.6　元の n 倍

$(G,+)$ を加法群とし、$n \in \mathbb{N}$, $P \in G$ とする。nP を計算するには、n を二進展開し（j 桁とする）、P, $2P$, $4P = 2P + 2P$, …, $2^jP = 2^{j-1}P + 2^{j-1}P$ と順番に計算して、二進展開に合わせて足すことで、たかだか $2\log_2(n)$ 回の G での和で計算できる。

一般に、例えば $K = \mathbb{Q}$ のとき $E(K)$ でこういう計算をするのは大変である（分母・分子が爆発的に増大する）が、$K = \mathbb{F}_p$ (あるいはより一般に $\mathbb{F}_q$) のときには、x, y 座標ともにこの有限の体の中で計算ができるためにこの問題は起きない。

1.2.7　アファイン空間と射影空間

K を代数閉体とし、n を自然数とする。$A^n(K)$ で、K^n をあらわし K 上の n 次元アファイン空間という。$A^n(K)$ の部分集合で、ある定数でない多項式の共通零点

$$Z(f) := \{(x_1, \ldots, x_n) \in K^n \mid f(x_1, \ldots, x_n)\}$$

となっているものをアファイン代数超曲面という。特に $n = 2$ のとき $Z(f)$ を「f が定義するアファイン平面代数曲線」という。

レポート問題 4. アファイン平面代数曲線は、空集合ではないことを示せ。（示せれば、無限集合であることも示せ。）

$f(x, y)$ が（$K[x, y]$ の元として）既約の時、この曲線を既約であるという。この曲線の次数は、x, y を 1 次と数えたときの $f(x, y)$ の次数で定義される。

$f(x, y)$ に対して、x による微分、y による微分が通常の多項式に対して定義されるように定義される。アファイン代数曲線 $Z(f)$ の特異点とは、この曲線上の点 (a, b) であって、$f_x(a, b) = 0$ かつ $f_y(a, b) = 0$ を満たす点である。$Z(f)$ が非特異であるとは、特異点がないことである。

$g \in K[x, y]/(f)$ は、$Z(f)$ から K への関数を与える。$K[x, y]/(f)$ を $Z(f)$ の正則関数の環という。f が既約ならばこの環は整域。その商体を $Z(f)$ の有理関数体という。

K 上の n 次元射影空間とは、商集合

$$P^n(K) := \{(x_0, x_1, \ldots, x_n) \in K^{n+1} | x_0 = x_1 = \cdots = x_n = 0 \text{ でない }\}/\sim$$

ここで $\sim$ は $(x_0, x_1, \ldots, x_n) \sim (x'_0, x'_1, \ldots, x'_n)$ を、ある $a \in K$ が存在して $(x_0, x_1, \ldots, x_n) = a(x'_0, x_1, \ldots, x'_n)$ であることとして定義される。この同値類を $[x_0 : x_1 : \cdots : x_n]$ と表記する。

$A^n(K)$ から $P^n(K)$ への単射 $(x_1, \ldots, x_n) \mapsto [1 : x_1 : \cdots : x_n]$ がある。$P^n(K)$ は $n + 1$ 個のアファイン n 次空間で覆える。

例えば、$P^1(\mathbb{C})$ は二つの $\mathbb{C}$ で覆える。リーマン球面と呼ばれる。

$P^2(K)$ は $[x : y : z]$ なる比の全体である。今、x, y, z について斉次な多項式（x, y, z を一次と数えて、どの単項式も同じ次数を持つ多項式）$F(x, y, z)$ が与えられたとする。F は定数ではないとする。このとき、$F(x, y, z) = 0$ となるような $[x : y : z]$ の集合を $Z(F) \subset P^2(K)$ と書き、平面的射影代数曲線という。F が既約のときこの曲線を既約という。$P^2(K)$ は 3 つの $A^2(K)$ で覆えるが、$Z(F)$ と $A^2(K)$ の共通部分はアファイン代数曲線である。実際、$f(x, y) = F(x, y, 1)$ とおけば $Z(f)$ がこの共通部分である。こうして得られる三つのアファイン代数曲線が非特異であるとき、$Z(F)$ は非特異であるという。

いま、n 次式 $f(x,y)$ が与えられたとき、

$$F(x,y,z) := z^n f(x/z, y/z)$$

を f の斉次化といい、平面射影曲線 $Z(F)$ をアファイン平面曲線 $Z(f)$ の射影化という。

Weierstrass equation $f(x,y) = y^2 - x^3 - Ax - B$ に対し、その斉次化 $F(x,y,z) = y^2z - x^3 - Axz^2 - Bz^3$ を考え、射影曲線 $Z(F)$ を考えると、$Z(f)$ に一点を付け加えたものになる。実際、$\{z=1\} \cap Z(F) = Z(f)$ は計算すれば確かめられ、$\{z=0\} \cap Z(F)$ は $x^3 = 0$ だから $[0:y:0] = [0:1:0]$ なる一点になる。これが前に述べた ∞ の正体である。

なお、定義も証明もしないが、次の定理が知られている。

定理 1.2.4. (Bézout) C, D を既約平面射影曲線とし、その次数を d, e とする。$C \cap D$ は有限個の点からなる。各点ごとにその重複度が定義され、$C \cap D$ を重複度をこめて数えると de となる。

Weierstrass equation は非特異 3 次曲線 E を与える。上の定理により、任意の直線は重複度を込めてちょうど 3 点で交わる。E 上二個点を定めれば、その二点を通る直線がただ一つあり、直線と E の交点は 3×1 個あるから、第 3 の点が定まる。(二点が一致するときには、E とその点で重複度 2 以上で交わる直線がただ一つ存在する。ここで、その点が非特異であるということが必要となる。) こうして、∞ を付け加えると二項演算 $+$ が得られることは Bézout の定理からほぼ従う。

特異点のあるとき : K 上のアファイン曲線 $y^2 = x^2(x-1)$ は $(0,0)$ という特異点を持つ。このとき、任意の $m \in L$ $K \subset L$ に対し、$(0,0)$ を通る直線 $y = mx$ は $(0,0)$ で重解をもつ。したがって、「接線」が一意に定まらない。

1.2.8 一般化 Weierstrass equation

標数 2 のとき、Weierstrass equation は特異点を持った。

次の事実が知られている。任意の体 K に対し、任意の楕円曲線は一般化 Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ により与えられる。∞ は $[0:1:0]$ に対応する。

K が標数 2 の時は、全ての楕円曲線は

$$y^2 + x_1y = x_1^3 + a_2x^2 + a_6$$

$(a_6 \neq 0)$ が非特異性と同値

または

$$y^2 + a_3y = x_1^3 + a_4x^1 + a_6$$

$(a_3 \neq 0)$ が非特異性と同値

のいずれかからえられる。$K \subset L$ に対し、$E(L)$ は同様の方法で加法群となる。

1.2.9　Hasse の定理

定理 1.2.5. (Hasse bound) E を $\mathbb{F}_q$ 上の楕円曲線とする。すると、$|q+1-\#E(\mathbb{F}_q)| \leq 2\sqrt{q}$ が成立する。

$\mathbb{P}^1(\mathbb{F}_q)$ の元は $q+1$ 個ある。$y^2 = f(x)$, f は x の 3 次式、と考えたとき、$f(x)$ が $\mathbb{F}_q$ で 0 以外の平方数になっているときに y は二個とれる。上の定理は、$f(x)$ が平方数になるような x は大体半分 (丁度半分なら $q+1$) で、ずれはたかだか $\sqrt{q}$ 個であるという主張である。証明は、やるかやらないか決めていない。

1.3　楕円曲線の射

1.3.1　曲線の間の射

K を代数閉体とする。$C \subset A^2(K)$ を $f(x,y) \in K[x,y]$ の零点として定義される代数曲線とする。f が既約であるとき、$K[x,y]/f$ を C 上の正則関数環という。その元 g は、$C \to K$ なる写像を与える。

$K[x,y]/(f)$ の商体を $K(C)$ とかき、C 上の有理関数体という。たとえば、$h(x,y)/g(x,y)$ は、C 上で $g(x,y) \neq 0$ となる点で定義されて K に値をとる関数となる。

そこで、このような C の部分集合が開集合となる位相を C にいれる。

1.3.2　Zariski 位相

K を代数閉体とする。$f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ をとる。共通零点

$$Z(f_1, f_2, \ldots, f_s) := \{(\alpha_1, \ldots, \alpha_n) \in K^n \mid f_1(\alpha_1, \ldots, \alpha_n) = 0, \ldots, f_s(\alpha_1, \ldots, \alpha_n) = 0, \} \subset A^n(K)$$

を A^n の代数的集合という。代数的集合の全体は「閉集合の公理」をみたす。こうして A^n に与えられた位相を Zariski 位相という。

アフィン平面代数曲線 $C \subset A^2(K)$ に、A^2 から誘導された位相を C の Zariski 位相という。

$P^2(K)$ には、$A^2(K)$ の Zariski 位相の貼り合わせ（商位相）として位相が入る。これを Zariski 位相という。射影平面代数曲線 $C \subset P^2(K)$ にも、誘導された位相として Zariski 位相が入る。

射影平面曲線 C から C' への正則射とは、台集合 C から C' への写像 f であって、C の任意の点 P について、P を含むある Zariski 開集合 U があり、f を U に制限すると正則であるもの。($x_1 = h_1(x,y)/g_1(x,y), y_1 = h_2(x,y)/g_2(x,y)$ とおいたとき、g_1, g_2 が $(x,y) \in U$ で 0 点を持たず、かつ $(x_1, y_1) \in C'$ となること。)

定義 1.3.1. 平面曲線 C の空でない Zariski 開集合から C' への正則写像を、C から C' への rational map という。

定理 1.3.2. C を既約非特異代数曲線、C' を射影代数曲線とする。このとき、C から C' への rational map は、C から C' への正則写像に一意的に伸びる。

厳密な証明には相当の準備を要する。

1. C の開集合は、有限個の点の補集合、および空集合となる。ゆえに、$f : C \to C'$ は有限個の点を除いて定義されている。

2. P を f が定義されていない点とする。C の有理関数体 $K(C)$ を考え、P において正則（分母が P で 0 にならない）有理関数がなす部分集合を O_P であらわす。

3. P が非特異であるとき、O_P は discrete valuation ring になる。すなわち、ある $t \in O_P$ が存在して、任意の 0 でない $x \in O_P$ がただ一通りに $t^n u$ $(n \in \mathbb{N})$, $u \in O_P^\times$ の形に書ける。t を P における uniformizer という。$O_P[t^{-1}] = K(C)$ となる。$K(C)^\times$ の元は、$t^n u$ $(n \in \mathbb{N})$, $u \in O_P^\times$ の形に一通りに書ける。

4. rational map $f : C \to C'$ は $(x, y) \mapsto (g_1(x, y), g_2(x, y))$、ここに $g_1, g_2 \in K(C)$ と書ける。斉次化して $[g_1 : g_2 : 1]$ と書ける。

5. $[g_1 : g_2 : 1]$ を、$K(C)$ の元の比とみる。$g_1, g_2, 1$ の分母に t^n が現れなければ、この rational map は P で定義される。分母に現れる y^{-n} の n の最大のものをとる。rational map を $[t^n g_1 : t^n g_2 : t^n]$ で定義すれば、これは C' 上の点を与える。こうして、P を含む開集合上に rational map は伸ばせる。

1.3.3 楕円曲線の準同型写像

K を体とし、E_1, E_2 を K 上の楕円曲線とする。E_1 から E_2 への K 上定義された代数射とは、$K(E_1)$ の 2 元 $R_1(x, y), R_2(x, y)$ であって、$(x, y) \in E(\overline{K})$ ならば $(R_1(x, y), R_2(x, y)) \in E_2(\overline{K})$ を満たすものをいう。(R_1, R_2) が定数 ((∞) も含む) のとき、この写像を定数写像という。

E_1 の非特異性と E_2 の射影性から、前述の定理により、R_1, R_2 のどちらかの分母が点 $P \in E_1(\overline{K})$ で 0 となる場合も、対応する $E_2(\overline{K})$ の点がただ一つ定まり、$\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ なる正則写像が定まる。

この写像が群準同型のとき、すなわち $\alpha(\infty) = \infty$, $\alpha(P + Q) = \alpha(P) + \alpha(Q)$ を考える。E_1 の全ての点を ∞ に対応させる写像を 0 と書く。0 以外の群準同型を E_1 から E_2 への同種写像 (isogeny) という。

楕円曲線 E から E 自身への準同型を自己準同型 (endomorphism) といい、$\mathrm{End}(E)$ と書く。

例 1.3.3. K の標数は 2 でないとする。$y^2 = x^3 + Ax + B$ が与える楕円曲線 E において、$P \mapsto 2P$ は $E(\overline{K}) \to E(\overline{K})$ なる自己準同型を与える。実際、$m = \frac{3x^2 + A}{2y}$ とおくと

$$R_1(x, y) = m^2 - 2x,$$

$$R_2(x, y) = m(3x - m^2) - y$$

が 2 倍を与えることを先に見た。分母が 0 になるのは $y = 0$ のときである。E を射影座標でみると $[R_1(x, y) : R_2(x, y) : 1]$ であり、$y = 0$ に伸ばそうとすると $[R_1(x, y)y^3 : R_2(x, y)y^3 : y^3]$ となる。(m の分母に y があり、$y = 0$ で $3x^2 + A \neq 0$ であるので $y^3 R_2(x, y)$ は $y = 0$ で $-m^3 y^3$ は 0 でない有限の値をとる。すなわち、$y = 0$ における比は $[0 : 1 : 0]$ となり、∞ に一致する。)

命題 1.3.4. $y^2 = x^3 + Ax + B$ が与える楕円曲線 E に置いて $K(E) = K(x)[y]/(y^2 - x^3 - Ax - B)$.

証明. アフィン曲線 y^2-x^3-Ax-B 上の正則関数の環は $K[x,y]/(y^2-x^3-Ax+B)$ である。その商体が $K(E)$ である。$K[x,y] \to K(x)[y]/(y^2-x^3-Ax+B)$ なる環準同型を考えると、カーネルが (y^2-x^3-Ax-B) となることがわかる。なぜならば、カーネルから $f(x,y)$ を持ってくると $f(x,y)$ が $K(x)[y]$ の多項式として (y^2-x^3-Ax-B) で割り切れることがわかる。すなわち $f(x,y)=g(x,y)(y^2-x^3-Ax+B)$, ここに $g(x,y)$ は $K(x)[y]$ の元。$g(x,y)$ を y の次数について整理して、係数を $K(x)$ の元と見たとき、分母をはらうことによって $h(x)g(x,y) \in K[x,y]$ とできる。すると $h(x)f(x,y) = (h(x)g(x,y))(y_2 - x^3 - Ax - B)$。$K[x,y]$ は UFD であるから $f(x,y)$ を $y_2 - x^3 - Ax - B$ が割り切る。こうして、$K(x)[y]/(y^2 - x^3 - Ax - B)$ は $K[x,y]/(y^2 - x^3 - Ax - B)$ を含むが、$y^2 - x^3 - Ax - B$ の $K(x)[y]$ における既約性より体である。どの元も（分母を払うやり方で）$K[x,y]/(y^2 - x^3 - Ax - B)$ の商として書けるので、この環の商体が $K(x)[y]/(y^2 - x^3 - Ax - B)$ となる。 □

証明が難しかったが、本質的には、次のことを示しているに過ぎない。「任意の有理式 $f(x,y)$ は、$y^2 = x^3 + Ax + B$ なる関係のもと、$\alpha(x) + \beta(x)y$」の形に書ける。まず、y^2 は x の多項式なので任意の多項式は y について 1 次にできる。任意の有理式は y について分母分子が 1 次にできる。$a, b \in K(x)$ として、$1/(ay-b) = (ay+b)/[(ay-b)(ay+b)] = (ay+b)(a^2y^2-b^2)$ とすれば分母は $K(x)$ の元とできるので、y は分子のみに現れるとしてよい。

レポート問題 5. 命題 1.3.4 の証明をキチンと述べよ（上で与えた証明はかなり省略されている）。

1.3.4　写像の次数

以下、K を体とする。その標数は 2 でないとし、E を $y^2 = x^3 + Ax + B$ によって定義された楕円曲線とする。先の命題により、endomorphism $\alpha : E \to E$ は

$$(x,y) \in E(\overline{K}) \mapsto (r_1(x) + s_1(x)y, r_2(x) + s_2(x)y)$$

の形に書けることがわかる。ここで、準同型性より $\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y)$ だから、

$$(r_1(x) - s_1(x)y, r_2(x) - s_2(x)y) = (r_1(x) + s_1(x)y, -r_2(x) - s_2(x)y)$$

が成立しなくては $s_1(x) = 0$, $r_2(x) = 0$ が従う。そこで、$s_2(x)$ を新たに $r_2(x)$ と取り直すことで、

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

と書ける。

$r_1(x) = p(x)/q(x)$ と互いに素な $K[x]$ の元の商に書いたとする。$q(x) = 0$ となる (x,y) に対し、$\alpha(x,y) = \infty$ が（射影曲線への延長で示したように）示せる。$q(x) \neq 0$ のとき、$r_2(x)$ の分母は 0 にならない。実際、$r_2(x) = s(x)/t(x)$ と既約分数式に書いたとき、

$$(r_2(x)y)^2 = r_1(x)^3 + Ar_1(x) + B$$

より

$$\frac{s(x)^2(x^3 + Ax + B)}{t(x)^2} = \frac{\text{x の多項式で } q(x) \text{ と互いに素}}{q(x)^3}$$

と書ける。両辺を $t(x)^2q(x^3)$ 倍して

$$s(x)^2(x^3+Ax+B)q(x)^3 = (\text{x の多項式で } q(x) \text{ と互いに素})t(x)^2$$

ここで、$t(x_0)=0$ となるような x_0 において、右辺は重解を持つ。左辺では、$s(x)$ は $t(x)$ と互いに素だから x_0 を根にもたない。x^3+Ax+B は根の多重度は 1。よって、$q(x)^3$ も x_0 を根にもち、$q(x_0)=0$。対偶をとって、$q(x_0)\neq 0$ ならば $t(x_0)\neq 0$ であり、$\alpha(x_0,y)$ は定義される。

定義 1.3.5. α の写像度 (degree) を、

$$\deg(\alpha) := \max\{\deg p(x), \deg q(x)\}$$

で定義する。$\alpha=0$ の時は、$\deg(0)=0$ と定義する。

注意 1.3.6. 上の定義は技巧的過ぎる。通常、二つの代数曲線 C,C' に対して、像が開集合を含むような rational map $f: C\to C'$ があると、f による引き戻し $f^*: K(C')\to K(C)$ が体の単射となる。体の拡大 $K(C)\supset f^*K(C')$ は有限次拡大となり、この拡大次数を f の次数と定義する。この定義と上の定義は一致するが、証明がやや大変である。

例 1.3.7. $K=\overline{K}$ とする。$f: C\to C'$ の写像度が d でかつ f が separable のとき、「$C(K)$ 上の一般の点で」f は $d:1$ 写像となることが知られている。

separable の定義もしないが、例として、$C=C'=A^1(K)$ とし、f を次数 1 以上の K 係数多項式とすると $f: C\to C'$ を与える。f が separable であるとは、f' が恒等的に 0 ではないことである。

K の標数が 0 なら、f は separable である。一方、標数が p のとき、x^p は微分すると恒等的に 0 になり、separable でない (inseparable という)。一般に、$g(x^p)$ の形の関数は inseparable である。

$f(x)$ が separable であるとする。このとき、$f(x)=b$ の根は、$f'(x)=0$ となるような点 (separable なので有限個) をのぞけば $\deg f$ 個ある。すなわち、「一般には」f は $\deg f:1$ の写像である。

さて、上の定義での f の写像度を見る。$f^*K[x]=K[f(x)]$ であるから、写像度は $[K[x]: K[f(x)]]$ である。ここで、$T:=f(x)$ とおき、x の $K[T]$ における最小多項式を考えると、$f(X)-T$ であることがわかる。($X=x$ のとき 0 となるし、$K(T)[X]$ 上既約であることはガウスの補題と T の一次式であることから確かめられる。) よってこの拡大次数は $\deg f$ となる。

レポート問題 6. レポート問題 6 K を体とし、$K(x)$ を有理式体とする。$p(x),q(x)$ を互いに素な $K[x]$ の元とする。$\deg(p(x))\geq 1$ とする。$p(x)/q(x)$ の K 係数有理式体 $K(p(x)/q(x))$ は $K(x)$ の部分体である。拡大次数 $[K(x): K(p(x)/q(x))]$ は $\max\{\deg p(x), \deg q(x)\}$ に一致することを示せ。

可能なら、これを用いて注意 1.3.6 を $C=E=E'$, $\alpha: E\to E$ の場合に証明せよ。

定義 1.3.8. K を体とする。$K[x]$ の互いに素な多項式 $p(x),q(x)$ に対し、$p(x)/q(x)$ の微分を

$$(p(x)/q(x))'(p'(x)q(x)-p(x)q'(x))/q(x)^2$$

で定義する。

こうして $K(x)$ の元に対して微分が定義される。この微分はライプニッツ則 $(fg)' = f'g + fg'$ を満たす。

$r(x) \in K(x)$ が separable であるとは、$r'(x)$ が有理式として 0 ではないこととして定義する。$r(x) = p(x)/q(x)$ としたとき、この定義は $p'(x), q'(x)$ のいずれかが多項式として 0 ではないことと同値となる。

定義 1.3.9. K 上の Weierstrass equation が与える楕円曲線 E に対し、endomoriphism $\alpha : E \to E$ が

$$\alpha(x, y) = (r_1(x), r_2(x)y)$$

$r_1(x) = p(x)/q(x)$ で与えらえているとする。このとき、α が separable であるとは、$r_1(x)$ が separable であると定義する。

定理 1.3.10. $K = \overline{K}$ とし、$\alpha : E \to E$ を 0 でない E の endomorphism とする。α が separable ならば、$\#(\mathrm{Ker}\alpha) = \deg(\alpha)$ が成立する。inseparable ならば、$\#(\mathrm{Ker}\alpha) < \deg(\alpha)$ が成立する。

証明. 一般に、群準同型 $\alpha : G \to H$ があったとする。α の像から $h \in H$ をとると、$\alpha(x_0) = h$ なる $x_0 \in G$ が存在する。このとき、$\alpha^{-1}(h) = x + \mathrm{Ker}\alpha$ が成立するから、$\#(\alpha^{-1}(h)) = \mathrm{Ker}\alpha$ となる。

故に、上の定理を示すには、α の像の元 h であって、α が separable な時には

$$\#(\alpha^{-1}(h)) = \deg \alpha$$

を満たすものを見つければよく、inseparable なときには

$$\#(\alpha^{-1}(h)) < \deg \alpha$$

となるものを見つければよいことになる。

$G = H = E(K)$ とおき、$h = (a, b)$ とおく。$K = \overline{K}$ より $\alpha(E(K))$ は無限集合であることをまず注意する。よって、α の像の元として、$h = (a, b)$ は ∞ でなく、$a \neq 0$, $b \neq 0$ ととれる。すると、ある $(x_0, y_0) \in E(K) \setminus \{\infty\}$ がとれて、

$$\alpha(x_0, y_0) = (r_1(x_0), r_2(x_0)y_0) = (a, b)$$

とできる。ここで、$r_1(x) = p(x)/q(x)$ と既約分数式であらわしておく。$q(x_0) = 0$ ならば $\alpha(x_0, y_0) = \infty$ であることはすでに見た。故に $q(x_0) \neq 0$ であり、$r_2(x_0)$ も有限の値を持つ。ここで、$r_2(x) = 0$ を満たす x は有限個であるから、h を取り直して、$r_2(x_0) \neq 0$ としてよい。このとき、$r_2(x_0)y_0 = b$ により、x_0 が決まれば y_0 はただ一つ定まる。よって、$r_1(x) = a$ の解の個数が $\alpha^{-1}h$ の元の個数となる。

$r_1(x) = a$ は $f(x) - aq(x) = 0$ と同値である。ここで、

$$\deg(f(x) - aq(x)) \leq \max\{\deg f(x), \deg g(x)\} = \deg \alpha$$

である。この不等号が真に $<$ となるのは、$\deg f(x) = \deg g(x)$ であるとき、かつ a が $f(x)$ の最高次の係数を $g(x)$ のそれで割った値であるときのみである。このような a はたかだか一つなので、必要なら h を取り換えて、この不等号が等号になるようにできる。

こうして、$\deg(f(x) - aq(x)) = \deg \alpha$ としてよい。さて、$f(x) - aq(x) = 0$ の解の個数が $\alpha^{-1}h$ の元の個数であった。$r_1(x)$ が separable と仮定する。すると、$f'(x)$ と $q'(x)$ のいずれ

かは 0 ではないから、$f'(x) - aq'(x) = 0$ となるような x は有限個である。それぞれの x に対して、a はただ一つにきまる。h をとりなおして、このような有限個の a を x 座標にもたないようにする。すると、$f'(x) - aq'(x) \neq 0$ $(\forall x \in K)$ である。すなわち、$f(x) - aq(x) = 0$ は重根をもたず、$\deg \alpha$ 個の相異なる根をもつ。こうして $\#\alpha^{-1}(h) = \deg(\alpha)$ となり、separable の場合の証明は終わる。

α が inseparable であるとすると、$f'(x) - aq'(x)$ は恒等的に 0 であり、$f(x) - aq(x) = 0$ は常に重根を持つ。特に、その根の個数は $\deg(\alpha)$ より真に小さい。よって inseparable の場合の証明が終わる。 □

定理 1.3.11. 上で、$\alpha : E(\overline{K}) \to E(\overline{K})$ は全射である。

証明. $\infty = \alpha(\infty)$ は α の像である。それ以外の $E(\overline{K})$ の元は (a, b) の形をしている。上の証明で、$(r_1(x_0), r_2(x_0)y_0) = (a, b)$ となる (x_0, y_0) が見つかればよい。まず $r_1(x) = p(x)/q(x) = a$ となる x が存在することを示す。いま、$p(x) - aq(x)$ が定数でなければ、その根 x_0 が存在する。y_1 として、$x_0^3 + Ax_0 + Bx_0$ の平方根のいずれかをとると $(x_0, y_1) \in E(\overline{K})$ である。$\alpha(x_0, y_1) = (r_1(x_0), r_2(x_0)y_1) = (a, b')$ である。ここで、$(a, b') \in E(\overline{K})$ だから、$b' = b$ または $b' = -b$ である。前者であれば $y_0 = y_1$ ととれば $\alpha(x_0, y_0) = (a, b)$ を満たし、後者であれば $y_0 = -y_1$ ととれば良い。

$p(x) - aq(x)$ が定数であったとする。$p(x)$ が定数であったとすると $q(x)$ も定数であり、任意の $(x, y) \in E(\overline{K})$ に対して $\alpha(x, y) = (C, \pm\sqrt{C})$ である。これは、α が $d : 1$ 写像 (d は有限) であることに反する。よって、$p(x)$ は定数でないとしてよい。$q(x)$ も定数ではない。すると、$p(x) - aq(x)$ が定数関数となるような a はたかだか一つしかない。(p と q の最高次の係数の比である。) 存在したとして、それを a_0 とする。$(a_0, \pm\sqrt{a_0})$ 以外の $E(\overline{K})$ の元 (a, b) は α の像に入る。これは無限集合であるから、$(a', b') = (a_0, \sqrt{a_0}) + (a, b) \neq (a_0, \sqrt{a_0})$ となるような (a, b) がとれる。すると、(a', b') も (a, b) も α の像にはいるから、その差である $(a_0, \sqrt{a_0})$ も像に入る。どうようにして $(a_0, -\sqrt{a_0})$ も像に入る。従って α は全射である。 □

1.3.5 Torsion Points

$n \in \mathbb{Z}$ とする。E を K 上の楕円曲線とする。$P \mapsto nP$ は、$E(\overline{K}) \to E(\overline{K})$ なる群準同型写像を与えるが、「$P + Q$ を与える式」が有理関数で書けることから、正則写像であることがわかる。すなわち、n 倍写像は E の endomorphism である。

n 倍写像の核を、E の n-torision といい、$E[n]$ であらわす。

定義 1.3.12. E を K 上の楕円曲線とする。

$$E[n] := \{P \in E(\overline{K}) \mid nP = O\}$$

を E の n-torsion point という。

例 1.3.13. K の標数が 2 でないとする。E を Weierstrass Equation が与える楕円曲線とする。$E[2]$ を考えると、$2P = O$ となる点 P の集合となる。$P = O$ はこれを満たす。$E(\overline{K})$ における 2 倍の定義から、O 以外でこれを満たす点は $y = 0$ を満たす点である。$x^3 + Ax + B =$

$(x-e_1)(x-e_2)(x-e_3)$ と因数分解すると、$(e_1,0),(e_2,0),(e_3,0)$ がこれを満たす。$E[2]$ は O を含めて 4 つの元からなる。どの元の位数も 2 または 1 であり、群としては

$$E[2] \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

となる。

定理 1.3.14. E を K 上の楕円曲線とする。n 倍写像の degree は n^2 である。
n が K の標数と互いに素なとき (標数 0 なら常にそう考える)、n 倍写像は separable であり、

$$E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$$

となる。n が K の標数で割り切れるとき、n 倍写像は inseparable である。

証明は、n 倍写像の式を具体的に計算する division polynomial を用いて与えられるが、ここでは省略する。例えば Elliptic Curves (Lawrence C. Washington) §3.2 参照。
複素数体上の楕円曲線 E に対しては、$E(\mathbb{C}) \cong S^1 \times S^1$ から上の定理は従う。有限体上でも、標数と n が互いに素なら同じ定理が従うことが興味深い。
標数が n を割り切るときには違う現象が起きる。次の定理の証明も、Washington の本の同じ部分を参照とする。

定理 1.3.15. K を標数 $p>0$ の体とし、E を K 上の楕円曲線とする。すると、$E[p]$ は $\mathbb{Z}/p$ と同型か、もしくは自明な群となる。前者のとき E を ordinary elliptic curve といい、後者のとき E を super singular elliptic curve という。

1.3.6 Frobenius map

定義 1.3.16. K を有限体 $\mathbb{F}_q$ とする。このとき、$f(x,y) \mapsto f(x,y)^q$ は $K[x,y] \to K[x,y]$ の環準同型写像を与える。これを Frobenius map といい、Fr_q であらわす。定数体 K 上では identity となる。
E が K 上定義された楕円曲線である場合、$Fr(x,y) := (x^q, y^q)$ は E から E への endomorphism を与える。これも Frobenius map という。

証明. E が K 係数多項式 $f(x,y)=0$ で与えられた曲線であるとする。この曲線上の点 (a,b) に対し、$f(a^q,b^q) = f(a,b)^q = 0$ であることが上の定義の前半で述べられたことから従う。よって、E から E への正則写像であることは従う。あとは、群準同型であることを示せばよいが、

$$(a,b)+(a',b') = (r_1(a,b,a',b'), r_2(a,b,a',b'))$$

となる 4 変数有理式 r_1, r_2 があることと、定義の前半で述べられたことが有理式においてもなりたつことから、準同型性が従う。 □

定理 1.3.17. Fr_q の写像度は q である。Fr_q は separable ではない。

証明. Washington §2 参照。 □

1.3.7 The Weil Pairing

定義 1.3.18. K を体とし、n を K の標数で割り切れない自然数とする。

$$\mu_n := \{x \in \overline{K} \mid x^n = 1\}$$

を 1 の n 乗根のなす群という。

$x^n - 1$ の微分は nx^{n-1} なので、この共通零点は (n が K で可逆元なので) 存在しない。したがって $x^n - 1 = 0$ の根に重根はなく、μ_n は n 個の相異なる元からなる。体の乗法群の有限部分群は巡回群という定理があるので、μ_n はある位数 n の元 $\zeta \in \mu_n$ により生成される。位数 n の元を、1 の原始 n 乗根という。

定義 1.3.19. K を体とし、$\overline{K}$ をその代数的閉包とする。$\mathrm{Aut}_K(\overline{K})$ で、$\sigma : \overline{K} \to \overline{K}$ なる体同型のうちで、$\sigma_{|K} = \mathrm{id}_K$ となるものの全体のなす群とする。(K の絶対ガロア群と呼ばれる群となる。)

$\sigma \in \mathrm{Aut}_K(\overline{K})$ は、群 μ_n に作用する。$x^n = 1$ ならば $\sigma(x)^n = 1$ なので $\sigma : \mu_n \to \mu_n$。これが群同型であることは、σ が体の自己同型であることから従う。

E を K 上の楕円曲線とする。各座標に作用させることで $\sigma : E(\overline{K}) \to E(\overline{K})$ なる写像が得られるが、これは群同型となる。(このことは、E の定義方程式の係数が K に含まれること、および E の群構造を与える式が K 係数有理式であることから従う。Frobenius map と同様。)

定義 1.3.20. (non-degenerating skew-symmetric pairing.) G を可換群とする。写像 $e : G \times G \to \mu_n$ が bilinear paring であるとは、

1. それぞれの変数について群準同型である、すなわち

$$e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$$

$$e(S, T_1 + T_2) = e(S, T_1)e(S, T_2)$$

が全ての S, T について成立すること。

このとき、e が non-denegerate であるとは

2. $e(S, T) = 1$ がすべての $T \in G$ について成り立てば $S = O$、かつ $e(S, T) = 1$ がすべての $S \in G$ について成り立てば $T = O$ であること。

3. さらにこのとき、e が skew-symmetric であるとは $e(S, S) = 1$ が全ての S について成り立ち、$e(S, T) = e(T, S)^{-1}$ がすべての $S, T \in G$ について成り立つこと。

レポート問題 7. $G = (\mathbb{Z}/n)^m, \mu_n$ に対して、non-degenerated skew-symmetric pairing $e : G \times G \to \mu_n$ が存在することを示せ。

定理 1.3.21. (Weil pairng.) K を体とする。E を K 上の楕円曲線とする。n を K の標数が割り切らない自然数とする。このとき、Weil pairing と呼ばれる non-degenerated skew-symmetric pairing

$$e_n : E[n] \times E[n] \to \mu_n$$

が存在し、次の性質を満たす。

4. 任意の $\sigma \in \mathrm{Aut}_K(\overline{K})$ と $S,T \in E[n]$ に対し、

$$e_n(\sigma(S),\sigma(T)) = \sigma(e_n(S,T)).$$

5. 任意の endomorphism $\alpha : E \to E$ に対し、

$$e_n(\alpha(S),\alpha(T)) = e_n(S,T)^{\deg \alpha}.$$

この定理の証明は、Washington Chapter 11 を参照。

系 1.3.22. $E[n]$ が二元 S,T で可換群として生成されるとする。このとき $e_n(S,T) = \zeta$ は 1 の原始 n 乗根である。

証明. S,T で生成されることと、S,T の位数が n で $< S > \cap < T >= \{O\}$ となることとは同値。

結論を否定すると、$d|n$ で $d < n$ なるある d により、$\zeta^d = 1$ となる。すると $e_n(S,dT) = e_n(S,T)^d = 1$ より任意の $a,b \in \mathbb{Z}$ に対し $e_n(aS+bT,dT) = 1$ となって、非退化性より $dT = O$。これは T の位数が n であることに矛盾。 □

系 1.3.23. $E[n] \subset E(K)$ ならば、$\mu_n \subset K$.

証明. $E[n] \subset E(K)$ ならば、任意の $S \in E[n]$ と任意の $\sigma \in \mathrm{Aut}_K(\overline{K})$ に対して $\sigma(S) = S$。よって特に $E[n]$ を生成する S,T に対して $\sigma(e_n(S,T)) = e_n(S,T)$. ここで $e_n(S,T) = \zeta$ は μ_n の生成元である。無限次ガロア理論の基本定理より、このことから $\zeta \in K$ が従う。従って $\mu_n \subset K$. □

たとえば、$\mu_n \subset \mathbb{Q}$ が成り立つ n は $n = 2$ のみなので、$E[n]$ の点が全て $\mathbb{Q}$ 有理点となるには $n = 2$ が必要であり、$n > 2$ では $E[n]$ の点のどれかは $\mathbb{Q}$ 有理点ではない。

定義 1.3.24. E を K 上の楕円曲線、n を K の標数が割り切らない自然数とする。このとき、$E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$ であるが、$(1,0)$, $(1,0)$ に対応する元 $S,T \in E[n]$ を基底と取ることで、$(x,y)^t \in (\mathbb{Z}/n)^2$ (縦ベクトル) と $xS+yT \in E[n]$ の対応が群同型を与える。

$E[n]$ から $E[n]$ への群準同型のなす環は、行列環 $M_2(\mathbb{Z}/n)$ と同型となる。

例えば、E の endomorphsim α は $E[n]$ の endomorphism

$$\alpha_n : E[n] \to E[n]$$

を引き起こし、上の基底が与える同型から

$$\alpha_n \in M_2(\mathbb{Z}/n)$$

と同一視される。

命題 1.3.25. E を K 上の楕円曲線、α をその自己準同型、n を K の標数が割り切らない自然数とする。このとき、

$$\det(\alpha_n) \equiv \deg(\alpha) \bmod n.$$

証明. 先の基底に関する表現行列を $\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とおく。$a, b, c, d \in \mathbb{Z}/n$. このとき、$\alpha(S) = aS + cT$, $\alpha(T) = bS + dT$ である。系 1.3.22 より、$e_n(S,T) =: \zeta$ は 1 の原始 n 乗根である。ここで、Weil pairing の性質 (定理 1.3.21 の 5. 他) より

$$\begin{aligned} \zeta^{\deg \alpha} &= e_n(S,T)^{\deg \alpha} = e_n(\alpha(S), \alpha(T)) = e_n(aS + cT, bS + dT) \\ &= e_n(S, bS + dT)^a e_n(T, bS + dT)^c = e_n(S,T)^{ad} e_n(T,S)^{bc} = e_n(S,T)^{ad-bc} \\ &= \zeta^{\det(\alpha_n)} \end{aligned}$$

である。ζ の位数は n であるから、ζ の肩に乗った数は $\bmod n$ で一致。ここから命題が従う。 □

補題 1.3.26. R を可換環とし、$A, B \in M_2(R)$ を 2 次正方行列とする。このとき、次が成り立つ。

$$\det(aA + bB) = a^2 \det(A) + b^2 \det(B) + ab(\det(A + B) - \det A - \det B)$$

証明は、A,B の各成分を変数として（8 変数、a, b も入れて 10 変数の式) を力づくで計算することで得られる。

力づくといっても、少しスマートにできる。左辺において a^2 が現れる項に着目するとその係数は $\det(A)$ となり、b^2 の係数は $\det(B)$ になることは簡単にわかる。問題は ab の係数が両辺で一致することを示すことに帰着する。

レポート問題 8. 上の補題を証明せよ。

次の命題は、Hasse bound の証明に使われる。

命題 1.3.27. E を K 上の楕円曲線、α, β を E の endomorphism、a, b を整数とする。このとき、$a\alpha + b\beta$ も E の endomorphism である。次が成り立つ。

$$\deg(a\alpha + b\beta) = a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta). \tag{1.1}$$

証明. 直前の補題から、この式 (1.1) の deg を det に、α, β を α_n, β_n に置き換えれば等式が成り立つことが従う。命題 1.3.25 を用いれば、この式 (1.1) は K の標数で割り切れない任意の自然数 n に対して $\bmod n$ すれば成立することが示せる。これは、この式の左辺と右辺の差は、いくらでも大きい n で割り切れることを意味している。差の絶対値より大きい K の標数と素な n をとることにより、(1.1) が真の等号であることが分かる。 □

1.4 Hasse bound の証明

この章では $K = \mathbb{F}_q \subset \overline{K}$ とする。$\{x \in \overline{K} | Fr_q(x) = x\} = \mathbb{F}_q$ が成立する。なぜならば、$x^q - x$ は重根を持たず、$\overline{K}$ 内に丁度 q 個の元をもち、それが左辺である。右辺が左辺に含まれることは既にみた。個数が一致しているので両辺は等しい。$Fr_{q^n} = (Fr_q)^n$ であることを注意しておく。

命題 1.4.1. E を $\mathbb{F}_q$ 上の楕円曲線とする。任意の自然数に対して、

$$E(\mathbb{F}_{q^n}) = \mathrm{Ker}(Fr_{q^n} - 1).$$

ここで、右辺は $E(\bar{})$ からそれ自身への準同型の核である。

証明. 自己準同型環を $\mathrm{End}(E(\bar{}))$ とかく。Fr_{q^n}, 1 倍はこの環の元であるから、その差 $Fr_{q^n} - 1$ も自己準同型である。$P = (x, y)$ がこの核に入ることは、$(x, y) - (x, y) = O$ と同値であり、$Fr_{q^n}(x) = x$ かつ $Fr_{q^n}(y) = y$ と同値であり、$(x, y) \in E(\mathbb{F}_{q^n})$ と同値である。 □

命題 1.4.2.

$$\#E(\mathbb{F}_q) = \deg(Fr_q - 1).$$

証明. 定理 1.3.10 により、$Fr_q - 1$ が separable であることを示せばよい。この式を定義通りに計算すると separable であることが示せる。より感覚的には、separable でないとは微分が 0 となるということであり、Fr_q の微分は K の標数が q の約数なので 0 となる。すると、$Fr_q - Id$ の微分は $-Id$ の微分となり、0 でないので separable である。 □

定理 1.4.3. (Hasse bound) E を $\mathbb{F}_q$ 上の楕円曲線とする。すると、$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$ が成立する。

証明の準備をする。

$$a := q + 1 - \#E(\mathbb{F}_q) \tag{1.2}$$

とおく。この a はあとあと使われる。

補題 1.4.4. r, s を互いに素な整数とする。このとき

$$\deg(rFr_q - s) = r^2 q + s^2 - rsa.$$

証明. 命題 1.3.27 の式 (1.1) に、$r = a$, $s = 1$, $\alpha = Fr_q$, $\beta = -1$ を代入すると

$$\deg(rFr_q - s) = r^2 \deg(Fr_q) + s^2 \deg(-1) + rs(\deg(Fr_q - 1) - \deg(Fr_q) - \deg(-1)).$$

ここで、$\deg(Fr_q) = q$ (定理 1.3.17), $\deg(-1) = 1$ (-1 倍は全単射であるから核は $\{O\}$, separable であるから定理 1.3.10 より $\deg(-1) = 1$) を代入すると、求める式を得る。 □

Hasse の bound の証明：

$$\deg(rFr_q - s) = r^2 q + s^2 - rsa$$

が任意の互いに素な r, s で成立し、かつ deg なので左辺は非負である。右辺を s^2 で割って $x := r/s$ とおくと

$$qx^2 - ax + 1$$

となり、これが任意の有理数 x について非負である。有理数は実数の中で稠密だから、この式の連続性より任意の実数 x でこの式は非負である。したがって、二次式の判別式は正ではなく $a^2 - 4q \leq 0$, $a^2 \leq 4q$, $|a| \leq 2\sqrt{q}$ となる。この不等式は Hasse の bound に他ならない。

定理 1.4.5. E を $\mathbb{F}_q$ 上の楕円曲線とし、$a := q+1-\#E(\mathbb{F}_q)$ とおくと、E の自己準同型環の中で

$$Fr_q^2 - aFr_q + q = 0$$

が成立する。

整数 k に対して

$$Fr_q^2 - kFr_q + q = 0$$

となれば、$k = a$ である。

証明. $F := Fr_q^2 - kFr_q + q$ とおく。$F \neq 0$ ならば $\mathrm{Ker}F : E(\overline{K}) \to E(\overline{K})$ は有限群である。（定理 1.3.10）そこで、この核が無限群であることを示せば $F = 0$ が示せる。n を K の標数が割らない自然数とする。$E[n]$ への Fr_q の作用の表現行列を

$$Fr_{q,n} := \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

とする。a の定義 (1.2) から次の式の最初の等号が成立する。

$$q+1-a = \#\mathrm{Ker}(Fr_q - 1) = \deg(Fr_q - 1) \equiv \det(Fr_{q,n} - I) = sv - tu - (s+t) + 1 \bmod n$$

となる。ここで、$sv - tu = \det(Fr_{q,n}) \equiv q \bmod n$ (命題 1.3.25 と定理 th:deg-of-Fr から）なので

$$\mathrm{Tr}(Fr_{q,n}) = s + v \equiv a \bmod n$$

が成立する。ケーリーハミルトンの定理から

$$(Fr_{q,n})^2 - aFr_{q,n} + qI = 0 \bmod n$$

が成立する。左辺は $E[n]$ へ 0 倍で作用する。左辺の作用は F の $E[n]$ への作用であったから、$\mathrm{Ker}F$ には $E[n]$ が含まれる。n はいくらでも大きくとれるから、$\mathrm{Ker}F$ は無限群である。したがって、最初の議論により $F = 0$ である。

定理の後半を示すため、$a \neq k$ について定理の式が成り立ったとすると $(a-k)Fr_q = 0$. これを $E(\overline{K})$ に作用させる。Fr_q は全射だったから、$(a-k)$ 倍が $E(\overline{K})$ の元を全て 0 に送ることになる。$a - k \neq 0$ ならその核は有限群なので矛盾する。よって $a = k$。 □

定理 1.4.6. E を $\mathbb{F}_q$ 上の楕円曲線とし、a を (1.2) ととる。$X^2 - aX + q$ の二根（複素数内で考える）を α, β とする。このとき任意の自然数 n に対して

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

注意：この等式により、$n = 1$ のときの $\#E(\mathbb{F}_q)$ を求めれば、$\#E(\mathbb{F}_{q^n})$ は整数係数漸化式により求まることが分かる。実際、α^n は漸化式 $s_{n+1} - as_n + qs_{n-1} = 0$ の解であり、β^n も同じ漸化式を満たすので $t_n := \alpha^n + \beta^n$ も同じ漸化式を満たす。$t_0 = 2$,$t_1 = a$ であるので、t_2 以降はこの漸化式により定まる整数となる。

証明. Fr_q は $X^2 - aX + q = 0$ なる方程式を $\mathrm{End}(E(\overline{K}))$ で満たす。Fr_q^n は $Y^2 - (\alpha^n + \beta^n)Y + q = 0$ を満たすことを示す。実際、

$$X^2 - aX + q = (X - \alpha)(X - \beta)$$

から $Y = X^n$ とおくと $Y^2 - (\alpha^n + \beta^n)Y + q^n = (Y - \alpha^n)(Y - \beta^n)$。$(X^n - \alpha^n)(X^n - \beta^n)$ は $(X - \alpha)(X - \beta) = X^2 - aX + q$ で割り切れるから、$X = Fr_q$ を代入すると 0 となる。このとき $Y = Fr_{q^n}$ となるから従って $Fr_{q^n}^2 - (\alpha^n + \beta^n)Fr_{q^n} + q^n = 0$. $K = \mathbb{F}_{q^n}$ のときの定理 1.4.5 の後半を適用すれば、この場合の a が $\alpha^n + \beta^n$ となる。a の定義 (1.2) より、

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n})$$

これより定理が従う。 □

こうして $\#E(\mathbb{F}_{q^n})$ は $n = 1$ の場合を求めればより大きな n について簡単に計算できる。この位数が巨大な素数 p を素因数に含むとき、$E(\mathbb{F}_{q^n})$ は位数 p の巡回群を部分群にもつ。その元を探索して g とし、g が生成する部分群を G として、離散ログ問題の解きにくいおおきな群を探すことができる。

レポート問題 9. (必須)

授業に関する忌憚のない意見を述べよ。

授業に出なかったひとは、すなおに出なかった理由を述べよ。

また、改善すべき点などを遠慮なく述べよ。