

素体上定義された supersingular 楕円曲線の準同型環について

阪大理学部 小川 裕之 (Hiroyuki Ogawa)

### 要約

Abel 多様体の準同型環は、数論的代幾何学の重要な研究テーマの一つである。最も単純な、1次元 Abel 多様体 (楕円曲線) に関するものは、M. Deuring (1941 [1]) にて、ほぼ完全に調べられていた。彼は、supersingular 楕円曲線の準同型環が、4元数環の maximal order であることを示している。これは、この準同型環の  $\mathbb{Z}$ -basis を与える。T. Ibukiyama は、4元数環の maximal order の  $\mathbb{Z}$ -basis の研究 (1982 [3]) において、このことが可能であると注意している。彼の方針を、“類多項式” にて、具体化したのが、以下に述べる内容である。なお、D. R. Dorman も、準同型環の決定をしており、(1989 [6]) 本質的には、T. Ibukiyama のものを表すかたちで述べた。具体的に書き下す。これは、この目標にはあたらない。また、見長があるので、証明は全て省略する。(c.f. [5])

### §1. 類多項式 (Class polynomials)

$D \equiv 0, 1 \pmod{4}$ ,  $D < 0$  なる整数  $D$  を取り,  $\mathcal{O}_D$  を判別式  $D$  の虚2次の order とする. ( $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\frac{D+\sqrt{D}}{2}$ )

$$P_D(x) := \prod_E (x - j(E))$$

ただし, 積は,  $\mathcal{O}_D$  を準同型環にもつ,  $\mathbb{C}$  上定義された楕円曲線の  $\mathbb{C}$ -同型類の代表を動く.  $j(E)$  は, 楕円曲線  $E$  の  $j$ -不変量とする.

虚数乗法論により,  $P_D(x)$  は,  $\mathcal{O}_D$  の類数  $h$  次数にもつ,  $\mathbb{Z}$ -係数, monic, 既約多項式であることが知られている. この  $P_D(x)$  を, 判別式  $D$  に属する類多項式と呼ぶ.

$p$  を素数とし,  $E$  を  $\overline{\mathbb{F}_p}$  上定義された楕円曲線,  $\text{Emd}(E)$  を  $E$  の準同型環とする.  $\mathbb{Z}$ -係数の多項式  $P_D(x)$  の各係数を, modulo  $p$  でみることにより,  $\overline{\mathbb{F}_p}$ -係数または  $\overline{\mathbb{F}_p}$ -係数の多項式を持つ. これを  $\overline{P}_D(x)$  と書く.  $\equiv \equiv$  で, 次を得る. (c.f. N. Elkies [2])

#### Lemma 1

$\overline{P}_D(x) = 0$  が,  $\overline{\mathbb{F}_p}$  においいて,  $j(E)$  を根にもつならば,

埋め込み,  $\mathcal{O}_D \hookrightarrow \text{Emd}(E)$  が存在する.

#### Lemma 2

埋め込み,  $\mathcal{O}_D \hookrightarrow \text{Emd}(E)$  が存在するとき,  $\mathcal{O}_D$  を含むある虚2次の order  $\mathcal{O}_0$  が存在して,  $\overline{P}_{D_0}(x) = 0$  が,  $\overline{\mathbb{F}_p}$  においいて,  $j(E)$  を根にもつ.

Lemma 1 は、楕円曲線の reduction を用いて示される。

Lemma 2 は、Deuring's Lifting Theorem を、類多項式を用いて書き変えたものである。これら2つの Lemmas に  $F_0$  を、有限体上で定義された楕円曲線の準同型環は、その  $j$ -不変量の  $j$  を用いて調べる事が出来る。

### §2. $\mathbb{Z}$ -basis の決定

中を、2.3 と異なる素数とし、 $E$  を  $\mathbb{F}_p$  上で定義された supersingular 楕円曲線、 $\text{End}(E)$  をその準同型環とする。supersingular 楕円曲線は、 $\mathbb{F}_p$  より  $\mathbb{F}_{p^2}$  上で定義されたものに  $\mathbb{F}_p$  同型となる事が知られてゐる。本質的に、 $\mathbb{F}_p$  より  $\mathbb{F}_{p^2}$  上で定義されたもののみを考へればよい。こゝでは、最も簡単な  $\mathbb{F}_p$  上で定義されたもののみを扱う。

次の Theorem が知られてゐる。

Theorem (M. Kaneko (1989 [4]))

$0 < -D_0 \leq \frac{4}{\sqrt{3}}\sqrt{p}$  なる虚二次の order の判別式  $D_0$  对し、

$\overline{\mathbb{P}}_{D_0}(\mathcal{J}(E)) = 0$  を満たすものが存在する。

$E$  に対し、この Theorem で得られる判別式  $D_0$  を取り、以下固定する。 $\mathbb{Q}$  上の正定値  $K$  元数環  $\text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$  は、次の様に表示される。

Proposition 3

$$\text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} + \mathbb{Q}\pi + \mathbb{Q}\beta + \mathbb{Q}\pi\beta$$

$$f = f^{-1}, \quad \pi^2 = -p, \quad \beta^2 = D_0, \quad \pi\beta = -\beta\pi \quad \text{を満足する。}$$

M. Deuring の結果から、 $\text{End}(E)$  は、上の 4 元数環の maximal order である。その  $\mathbb{Z}$ -basis は、次  $v$  与えられる。

Proposition 4

(i)  $D_0 \equiv 1 \pmod{4}$  のとき、

$$\exists s \in \mathbb{Z} \text{ s.t. } s^2 + p \equiv 0 \pmod{D_0}$$

$$\text{End}(E) \cong \mathbb{Z} + \mathbb{Z} \frac{1+s\beta}{2} + \mathbb{Z} \pi \frac{1+s\beta}{2} + \mathbb{Z} \frac{\pi-s}{D_0} \beta$$

(ii)  $D_0 \equiv 0 \pmod{4}$ ,  $E[2] \subset E(\mathbb{F}_p)$  のとき、

$$\exists s \in \mathbb{Z} \text{ s.t. } s^2 + p \equiv 0 \pmod{D_0}$$

$$\text{End}(E) \cong \mathbb{Z} + \mathbb{Z} \frac{1+\pi}{2} + \mathbb{Z} \frac{\beta}{2} + \mathbb{Z} \frac{\pi-s}{D_0} \beta$$

(iii)  $D_0 \equiv 0 \pmod{4}$ ,  $E[2] \not\subset E(\mathbb{F}_p)$  のとき、

$$\exists s \in \mathbb{Z} \text{ s.t. } s^2 + p - \frac{D_0}{4} \equiv 0 \pmod{D_0}$$

$$\text{End}(E) \cong \mathbb{Z} + \mathbb{Z} \alpha + \mathbb{Z} \frac{\beta}{2} + \mathbb{Z} \frac{\pi + \frac{\beta}{2} - s}{D_0} \beta$$

$$f = f^{-1}, \quad \alpha := \begin{cases} \frac{\pi + \frac{\beta}{2}}{2} & (\text{if } D_0 \equiv 4 \pmod{8}) \\ \frac{1 + \pi + \frac{\beta}{2}}{2} & (\text{if } D_0 \equiv 0 \pmod{8}) \end{cases}$$

Remark

I. Proposition 3 の同型は、 $\mathbb{Q}$  上の正定値 4 元数環と  $\mathbb{C}^2$

の同型  $\Sigma$ . Proposition 4 の同型は, 環としての同型  $\Sigma$ . 意味する。

2. 整数  $n$  に対して,  $E$  の  $n$ -等分点の全体を  $E[n]$  と表す。

また,  $E(\mathbb{F}_p)$  を,  $E$  の  $\mathbb{F}_p$ -有理点の全体を表す。

さて, Proposition 4 で,  $\mathbb{Z}$ -basis の形が一応決定した。と = 3 が, 整数  $\nu$  を正確に決めなければならぬ。この  $\mathbb{Z}$ -basis の形から,  $\nu$  の符号を取り換えても, 環としての同型で, 更に (i) では  $\beta$  が, (ii) (iii) では  $\beta/2$  が,  $\text{End}(E)$  に属する = とから, (i) では modulo  $D_0$  で, (ii) (iii) では modulo  $D_0/2$  で決めれば充分である。一才, 実際には  $\nu$  を定めるためには, (i) では  $\frac{\pi-\beta}{D_0}\beta$  が  $E$  の準同型として実現される様に計算すればよいが, これには,  $E[D_0]$  を求め,  $\Sigma = \Sigma$  の  $\pi$  や  $\beta$  の作用を計算しなければならぬ。具体的な例でも,  $\Sigma$  としても,  $\Sigma$  の様な計算は, 実行不可能である。これを打開したのが, 本結果である。次の Theorem である。

### Theorem 5

(1)  $\Sigma$  を  $\mathbb{F}_p$  上で,  $D_1 \equiv 0, 1 \pmod{4}$  が, 唯一存在する。

$$\frac{4p}{-D_0} \leq -D_1 < \frac{4p}{-D_0} + \frac{-D_0}{4}, \quad D_1 \neq D_0$$

$$\overline{D_1}(\#(E)) = 0$$

(2) 整数  $t$  で、次を満たすものが存在する。

$$D_0 D_1 = 4p + t^2.$$

$$(3) \quad \mathfrak{N}_1 := \begin{cases} \frac{t}{2} & (\text{if } t = \text{even}) \\ \frac{D_0 + t}{2} & (\text{if } t = \text{odd}) \end{cases}$$

と置くとき、 $\mathfrak{N}_1$  は整数で、Proposition 4 の整数  $\mathfrak{N}$  は、

$$\mathfrak{N} \equiv \pm \mathfrak{N}_1 \begin{cases} \pmod{D_0} & (\text{if } D_0 \equiv 1 \pmod{4}) \\ \pmod{D_0/2} & (\text{if } D_0 \equiv 0 \pmod{4}) \end{cases}$$

と取れる。

$$(4) \quad \mathbb{F}[2] \subset \mathbb{F}(\mathbb{F}_p) \iff D_0 \equiv D_1 \equiv 0 \pmod{4}$$

先に述べたことから、Theorem 5 の (3) で、Proposition 4 の整数  $\mathfrak{N}$  が、決定する。従って、Proposition 4 と Theorem 5 (1) = (F) より、 $\text{End}(E)$  の  $\mathbb{Z}$ -basis が、完全に決定された。

### §3. 補足

$\mathbb{F}_p$  上定義された supersingular 楕円曲線に、このようにも、類数項式を用いて、準同型環の  $\mathbb{Z}$ -basis を決めることが出来ると思われる。残念ながら、それは出来ていない。

§2 で得られたことから、直ちに、 $\mathbb{F}$  と  $\mathbb{Q}$  の中間にある正定値 4 元数環の、ある種の maximal orders の環同型類の代表を、 $\mathbb{Z}$ -basis の形で与えることが出来る。楕円曲線を用いて書

かれ2113か。代表を千えるだけ存す。条件  $\overline{P_D(x)} = 0$  を全2  
取り除く。判別式の組  $(D_0, D_1)$  を取れば。と。か。max.  
orders の同型類の代表が構成される。

### 参考文献

- [1] M. Deuring : Die Typen der Multiplikatorenringe  
elliptischer Funktionenkörper : Abh. Math. Sem. Hamburg  
14 (1941) 197-272
- [2] N. Elkies : The Existence of Infinitely Many  
Supersingular Primes for Every Elliptic Curve over  $\mathbb{Q}$   
: Invent. Math. 89 (1987) 561-567
- [3] T. Ibukiyama : On Maximal Orders of Division Quaternion  
Algebras over the Rational Number Fields with Certain  
Optimal Embeddings : Nagoya Math. J. 88 (1982) 181-195
- [4] M. Kameko : Supersingular  $j$ -invariants as Singular  
Moduli mod  $p$  : Osaka J. Math. 26 (1989) 849-855
- [5] H. Ogawa : 超特異楕円曲線の準同型類 : 大阪大学修工  
論文 (1991)
- [6] D.R. Dorman : Global Orders in Definite Quaternion Algebras as  
Endomorphism Rings for Reduced CM Elliptic Curves : in Number  
Theory. J.-M. DeKoninck & C. Levesgue (ed.) (1989) 108-116.