数理解析研究所講究録
第775巻 1992年 167-173

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）

§0. 序

Abel多様体の準同型環は、数論的代数幾何学の重要な研究テーマの1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]）によって、ほぼ完全に調べられている。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。ここでは、その準同型環の$\mathbb{Z}$-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、そ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"によって具体化したのが、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いるが、（1989 [6]）本質的には、T. Ibukiyamaのものを書きかえたに過ぎず、具体的に書き下す、ここでの目標にはあたらない。また、冗長になるので、証明は全て省略する。（cf. [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, $\mathcal{O}_D$ の類数を次数にもつ, $\mathbb{Z}$-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 $\mathbb{F}_p$ 上定義された楕円曲線, $\mathrm{End}(E)$ 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, $\mathbb{F}_p$-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。ここで, 次を得る。(c.f. N. Elkies [2])

Lemma 1

$\overline{P_D}(X) = 0$ が, $\overline{\mathbb{F}_p}$ において, $j(E)$ を根にもつならば, 埋め込み, $\mathcal{O}_D \hookrightarrow \mathrm{End}(E)$ が存在する。

Lemma 2

埋め込み, $\mathcal{O}_D \hookrightarrow \mathrm{End}(E)$ が存在するとき, $\mathcal{O}_D$ を含むある虚2次の order $\mathcal{O}_{D_0}$ が存在して, $\overline{P_{D_0}}(X) = 0$ が, $\overline{\mathbb{F}_p}$ において, $j(E)$ 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 によって. 有限体上定義された楕円曲線の準同型環は. その j-不変量のみを用いて調べることが出来る。

§2. Π-basis の決定.

p を. 2, 3 と異なる素数とし. E を $\mathbb{F}_p$ 上定義された supersingular 楕円曲線, $\mathrm{End}(E)$ をその準同型環とする。supersingular 楕円曲線は. $\mathbb{F}_p$ 又は $\mathbb{F}_{p^2}$ 上定義されたものに高同型となることが知られている。本質的に. $\mathbb{F}_p$ 又は $\mathbb{F}_{p^2}$ 上定義されたもののみを考えればよい。ここでは. 最も簡単な. $\mathbb{F}_p$ 上定義されたもののみを扱う。

次の Theorem が知られている。

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

$0 < -D_0 \leq \frac{4}{15}p$ なる虚2次の order の判別式 D_0 で. $\overline{P_{D_0}}(j(E)) = 0$ を満たすものが存在する。

E に対して. 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4元数環. $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ は. 次の様に表わせる。

Proposition 3

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

ただし．$\pi^2=-p$．$\beta^2=D_0$．$\pi\beta=-\beta\pi$ を満たす。

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

Proposition 4

(i) $D_0\equiv 1 \pmod 4$ のとき．

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

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

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

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

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

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

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

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

ただし．$$\alpha:=\begin{cases}\dfrac{\pi+\beta/2}{2} & (\text{if } D_0\equiv 4 \pmod 8)\\ \dfrac{1+\pi+\beta/2}{2} & (\text{if } D_0\equiv 0 \pmod 8)\end{cases}$$

Remark

1. Proposition 3 の同型は．$\mathbb{Q}$ 上の正定値4元数環として

の同型で. Proposition 4 の同型は. 環としての同型を. 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. $E(\mathbb{F}_p)$ で. 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。ところが. 整数 s を正確に決めなければならない。その $\mathbb{Z}$-basis の形から. s の符号を取り換えても. 環としては同型で. 更に (i) では β が. (ii) (iii) では $\beta/2$ が. $\mathrm{End}(E)$ に属することから. (i) では modulo D_0 で. (ii) (iii) では modulo $D/2$ で決めれば充分である。一方. 実際に s を定めるためには. (i) では $\frac{\pi-s}{D_0}\beta$ が E の準同型として実現される様に計算すればよいが. それには. $E[D_0]$ を求め. そこでの π や β の作用を計算しなければならない。具体的な例でも, どこでも. この様な計算は. 実行不可能である。これを打開したのが. 主結果である. 次の Theorem である。

Theorem 5

(i) 次を満たす. $D_1 \equiv 0, 1 \pmod 4$ が. 唯一存在する。

$$\frac{4P}{-D_0} \le -D_1 < \frac{4P}{-D_0} + \frac{-D_0}{4}, \quad D_1 \neq D_0$$

$$P_{D_1}(j(E)) = 0$$

(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)
$$s_1 := \begin{cases} \frac{t}{2} & (\text{if } t : \text{even}) \\ \frac{D_0 + t}{2} & (\text{if } t : \text{odd}) \end{cases}$$

とおくとき、s_1 は整数で、Proposition 4 の整数 s は、

$$s \equiv \pm s_1 \begin{cases} \pmod{D_0} & (\text{if } D_0 \equiv 1 \pmod 4) \\ \pmod{p\ell} & (\text{if } D_0 \equiv 0 \pmod 4) \end{cases}$$

とみたす。

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

先に述べたことから、Theorem 5 のもとで、Proposition 4 の整数 s が、決定する。従って、Proposition 4 と Theorem 5 により、$\mathrm{End}(E)$ 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 楕円曲線についても、類多項式を用いて、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、p とのみ分岐する正定値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

かれているが、代表を与えるだけなら、条件 $P_D(x)=0$ を全て取り除いて、判別式の組 (D_0, D_1) を取れば、それから、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. Kaneko : 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環 : 大阪大学修士論文 (1991)

[6] D.R. Dorman : Global Orders in Definite Quaternion Algebras as Endomorphism Rings for Reduced CM Elliptic Curves : in Number Theory. J-M. Deconinck & C. Levesque (ed.) (1989) 108-116.