有限体上の単純 Abel 多様体と Weil number

土屋和由

本稿は 2001 年 8 月 29 日から 8 月 31 日の間に行われたワークショップ「暗号理論とそれを支える代数曲線理論」における講演「CM 法とそれを支える数論的性質」に関する報告である.

超楕円曲線暗号は, その Jacobi 多様体の有理点のなす群に関する離散対数問題を安全性の根拠においた暗号である. 安全性の保持のために, 有理点のなす群の位数を知ることが超楕円曲線暗号では重要である.

一般に有限体上の Abel 多様体に対して, その有理点のなす群の位数は Frobenius 準同型の特性多項式を用いて記述することが出来る. さらに, Frobenius 準同型の特性多項式から Weil number とよばれるある特別な性質を持つ代数的整数が定まるが, 実は Weil number に対してそれに対応する単純 Abel 多様体が決まることがわかる.

本稿では, 有理点のなす群の位数と Frobenius 準同型の特性多項式との関係に関する Weil の理論, 有限体上の単純 Abel 多様体と Weil number に関する Tate-Honda の理論に関する解説を行う.

1. 有理点の位数と Frobenius 準同型

1.1 p を素数, $q = p^r$ とする. A を体 $\mathbb{F}_q$ 上の g 次元 Abel 多様体とする. $n \in \mathbb{Z}$ に対して $A[n]$ を A の n 等分点の群とする. すなわち $A[n] = \mathrm{Ker}[[n] : A \to A]$ とする. 今, p と異なる素数 l に対して, 射影的極限 $\varprojlim_n A[l^n]$ を考える. ただし射影系は

$$\cdots \longrightarrow A[l^{n+1}] \xrightarrow{[l]} A[l^n] \xrightarrow{[l]} \cdots \xrightarrow{[l]} A[l]$$

である. このとき

$$T_l(A) = \varprojlim_n A[l^n](\overline{\mathbb{F}_q})$$

とおくと $T_l(A)$ は $\mathbb{Z}_l$ 上の加群の構造を持つ. ただし $\mathbb{Z}_l$ は l 進整数環である. $T_l(A)$ を A の l 進 Tate 加群と呼ぶ. 今, $\mathbb{Z}/l^n\mathbb{Z}$ 加群の同型 $A[l^n](\overline{\mathbb{F}_q}) \simeq (\mathbb{Z}/l^n\mathbb{Z})^{2g}$ から $\mathbb{Z}_l$ 加群の同型 $T_l(A) \simeq (\mathbb{Z}_l)^{2g}$ を得る. また $T_l(A)$ は $G = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ 加群の構造を持つ.

f を Abel 多様体 A の自己準同型 $f : A \to A \in \mathrm{End}_{\mathbb{F}_q}(A)$ とする. このとき p と異なる素数 l に対して $T_l(f) : T_l(A) \longrightarrow T_l(A)$ が定まる. $T_l(f)$ は $T_l(A)$ の $\mathbb{Z}_l$ 上の基底を定めることにより行列表現ができる.

f を Abel 多様体 A の自己準同型 $f : A \to A \in \mathrm{End}_{\mathbb{F}_q}(A)$ とする．今 f が全射であるとき f は同種（isogeny）であると呼ぶ．このとき $\mathrm{Ker}\, f$ は有限群スキームであり，その群スキームとしての位数, すなわち $\mathrm{Ker}\, f$ の座標環を $\mathbb{F}_q$ 上の加群とみたときの階数を $\deg f$ あるいは $\#\mathrm{Ker}\, f$ と記す.

命題 1.2. 同種写像 $f : A \to A \in \mathrm{End}_{\mathbb{F}_q}(A)$ に対して

$$\deg f = \det T_l(f)$$

が成立する．さらに $P(t) := \det(t - T_l(f))$ は有理整数係数の $2g$ 次モニック多項式である.

上の命題から $P(t)$ は l の取り方に依らずに f だけで決まることがわかる．そこで $P(t)$ を同種写像 f の特性多項式と呼ぶ．このとき, Weil による以下の定理が成立する.

定理 1.3. (Mumford [2], 21, Theorem 4.)
A を体 $\mathbb{F}_q$ 上の g 次元 Abel 多様体，$\xi \in \mathrm{End}_{\mathbb{F}_q}(A)$ を Abel 多様体 A の Frobenius 準同型，$P_\xi(t)$ を ξ の特性多項式，$\pi_1, \ldots, \pi_{2g}$ を特性多項式 $P_\xi(t)$ の根とする．このとき

$$(1)\ \#A(\mathbb{F}_{q^n}) = P_{\xi^n}(1) = \prod_{i=1}^{2g}(1 - \pi_i^n)$$
$$(2)\ \pi_i\overline{\pi_i} = q \quad (\ \forall i\ )$$

が成立する. ただし $P_{\xi^n}(t)$ は ξ^n の特性多項式，$\overline{\pi_i}$ は π_i の複素共役を表す.

例 1.4. $p = 7$ とする. 以下 $\mathbb{F}_7$ 上の楕円曲線 $E/\mathbb{F}_7 : y^2 = x^3 + 1$ の Frobenius 準同型 ξ の特性多項式 $P(t)$ を求める．今, 楕円曲線 E の $\mathbb{F}_7$ 有理点のなす群 $E(\mathbb{F}_7)$ は

$$E(\mathbb{F}_7) = \{(0,1), (0,6), (1,3), (1,4), (2,3), (2,4), (3,0), (4,3), (4,4), (5,0), (6,0), \infty\}$$

となる. したがって $\#E(\mathbb{F}_7) = 12$ である. 一方

$$\begin{aligned}
\mathrm{Nr}(T_l(\xi)) &= \deg(\xi) = p = 7 \\
\mathrm{Tr}(T_l(\xi)) &= 1 + \deg(\xi) - \deg(1 - \xi) \\
&= 1 + p - \#E(\mathbb{F}_7) \\
&= 1 + 7 - 12 = -4
\end{aligned}$$

が成立する．したがって, 特性多項式 $P(t)$ は

$$\begin{aligned}
P(t) &= t^2 - \mathrm{Tr}(T_l(\xi))\ t + \mathrm{Nr}(T_l(\xi)) \\
&= t^2 + 4t + 7 \\
&= (t - (-2 + \sqrt{-3}))(t - (-2 - \sqrt{-3}))
\end{aligned}$$

となる.

2. 有限体上の単純 Abel 多様体と Weil number

2.1 p を素数とする．代数的整数 π が order r の (A_0) 型であるとは，任意の π の共役 π^σ に対して

$$\pi^\sigma \overline{\pi^\sigma} = p^r$$

をみたすことをいう．同様に, ある代数体のイデアル I が order r の (A_0) 型であるとは，任意の I の共役 I^σ に対して

$$I^\sigma \overline{I^\sigma} = (p^r)$$

をみたすことをいう．(A_0) 型の代数的整数 π を総称して Weil number とよぶ.

2.2 以下, r を固定して $q = p^r$ とおく．A を体 $\mathbb{F}_q$ 上の Abel 多様体とする．A が A と 0 しか $\mathbb{F}_q$ 上の部分 Abel 多様体を持たないとき，A は $\mathbb{F}_q$ の上で単純であるという．今, 一般の Abel 多様体 A に対して Poincaré's complete reducibility theorem から A は $A_1^{n_1} \times \cdots \times A_k^{n_k}$ と同種であることがわかる． ただし, 各 A_i は互いに同種ではない単純 Abel 多様体であり，A_i と n_i は一意的に決まる．このとき Wedderburn の構造定理から

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq M(n_1, D_1) \times \cdots \times M(n_k, D_k)$$

が成立する. ただし各 D_i は $D_i = \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$ であり, Schur の補題から各 D_i は division algebra であることがわかる.

2.3 以下, 本稿の主題である単純 Abel 多様体と Weil number との対応に関する定理を述べる.

定理 2.4. (Tate [5] - Honda [1])

$$\Phi_r : \{\ \mathbb{F}_{p^r} \text{ 上の } \mathbb{F}_{p^r} \text{ 単純 Abel 多様体の } \mathbb{F}_{p^r} \text{ 同種類 }\}$$
$$\longrightarrow \{\ \text{order } r \text{ の Weil number の共役類 }\}$$

は全単射. ($\forall r > 0 \in \mathbb{Z}$)

上の定理における **(1)** well-defined 性, 単射性は Tate によって示され，**(2)** 全射性は Honda によって示された.

2.5 **(1)** well-defined 性, 単射性に関しては Tate による以下の定理およびその系

定理 2.6. (Tate [5])
k を有限体とし, $G = \mathrm{Gal}(\overline{k}/k)$ とおく． A を k 上の Abel 多様体とする. このとき単射 G 準同型

$$\mathrm{End}_k(A) \otimes \mathbb{Q}_l \longrightarrow \mathrm{End}_{\mathbb{Q}_l}(T_l(A) \otimes \mathbb{Q}_l)^G$$

は全単射である． しかも, Abel 多様体 A の Frobenius 準同型 ξ_A は $T_l(A) \otimes \mathbb{Q}_l$ に半単純に作用する.

系 2.7. (Tate [5], Main Theorem.)
k を有限体とし, $G = \mathrm{Gal}(\overline{k}/k)$ とおく． A_1, A_2 を k 上の Abel 多様体とする. このとき単射 G 準同型

$$\mathrm{Hom}_k(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(A_1), T_l(A_2))^G$$

は全単射である.

から導かれる以下の性質からわかる.

定理 2.8. A_1, A_2 を有限体 k 上の Abel 多様体, $P_{A_1}(t), P_{A_2}(t)$ をそれぞれ A_1, A_2 の Frobenius 準同型の特性多項式とする. このとき A_1 と A_2 が同種であることと, $P_{A_1}(t) = P_{A_2}(t)$ は同値である.

（証明）有限体 k 上の Abel 多様体 A_1, A_2 に対して「A_1 が A_2 の部分 Abel 多様体と同種であることと, $P_{A_1}(t) | P_{A_2}(t)$ が同値」であることを示せばよい.

今, k 準同型 $\varphi : A_1 \to A_2$ に対して, $\varphi_l : T_l(A_1) \otimes \mathbb{Q}_l \to T_l(A_2) \otimes \mathbb{Q}_l$ が定まる． l は体 k の標数と異なる素数である． 今 φ が有限 kernel を持つことと φ_l が単射であることが同値であるから, A_1 が A_2 の部分 Abel 多様体と同種であるとき, φ_l が単射であることがわかる． よって $P_{A_1}(t) | P_{A_2}(t)$ が成立する.

逆に $P_{A_1}(t) | P_{A_2}(t)$ が成立すると仮定する． このとき ξ_{A_1}, ξ_{A_2} をそれぞれ A_1, A_2 の Frobenius 準同型とすると, ξ_{A_1}, ξ_{A_2} がそれぞれ $T_l(A_1) \otimes \mathbb{Q}_l, T_l(A_2) \otimes \mathbb{Q}_l$ に半単純に作用する． よって、P_{A_1}, P_{A_2} の $\mathbb{Q}$ 上の既約分解をそれぞれ

$$P_{A_1} = {P_1}^{a_1} \cdots {P_r}^{a_r}, \quad P_{A_2} = {Q_1}^{b_1} \cdots {Q_s}^{b_s}$$

とおくと, $\mathbb{Q}_l$ 上のベクトル空間 $T_l(A_1) \otimes \mathbb{Q}_l, T_l(A_2) \otimes \mathbb{Q}_l$ はそれぞれ

$$T_l(A_1) \otimes \mathbb{Q}_l = \bigoplus_{i=1}^{r} \mathrm{Ker}\ P_i(\xi_{A_1}),$$

$$T_l(A_2) \otimes \mathbb{Q}_l = \bigoplus_{i=1}^{s} \mathrm{Ker}\ Q_i(\xi_{A_2})$$

に射影分解される. したがって $T_l(A_1)\otimes\mathbb{Q}_l$ は $T_l(A_2)\otimes\mathbb{Q}_l$ の部分空間に G 同型である. 今, $u : T_l(A_1)\otimes\mathbb{Q}_l \to T_l(A_2)\otimes\mathbb{Q}_l$ を単射 G 準同型とする. このとき, 系 2.7 から $\mathrm{Hom}_k(A_1, A_2)\otimes\mathbb{Q}$ の元 φ で $\varphi_l = u$ をみたすものが存在する. 今 u は単射であるから, φ に対応する $\mathrm{Hom}_k(A_1, A_2)$ の元は finite kernel をもつ.

定理 2.9. 有限体上の Abel 多様体 A に対して, A が単純 Abel 多様体ならば, A の Frobenius 準同型の特性多項式 $P(t)$ は有理数体 $\mathbb{Q}$ 上の既約多項式のベキである.

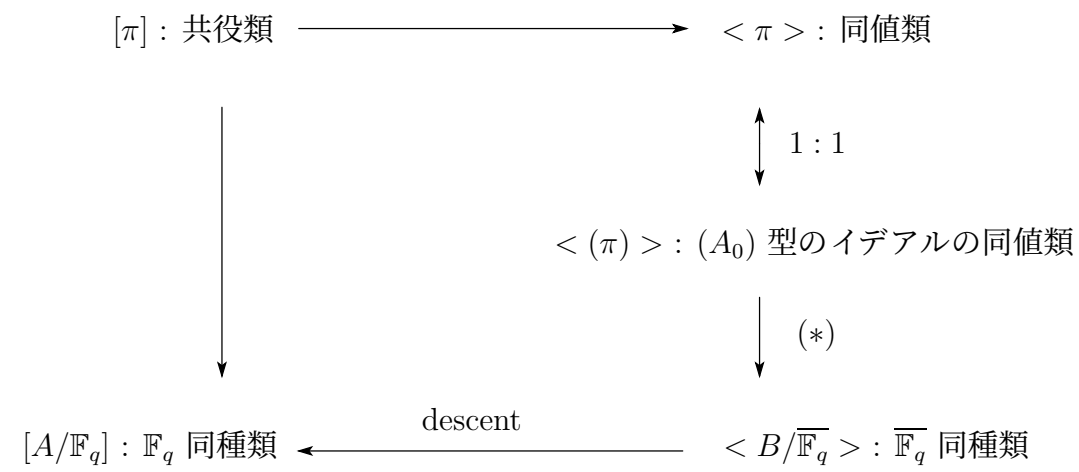
(証明) 系 2.7 から $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ の中心は $\mathbb{Q}[\xi_A]$ (ξ_A は A の Frobenius 準同型) であることがわかる. また Abel 多様体 A が単純であれば $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ は単純である. よって, 単純環の中心は可換体であるということから $\mathbb{Q}[\xi_A]$ が可換体であることが導かれる. 一方, 多項式 $Q(t)$ を $P(t)$ の互いに異なる $\mathbb{Q}$ 上の既約成分の積とすると, $\mathbb{Q}[\xi_A] \simeq \mathbb{Q}[t]/(Q(t))$ が成立する. 今 $\mathbb{Q}[\xi_A]$ は可換体であるから $Q(t)$ は $\mathbb{Q}$ 上の既約多項式である. したがって $P(t)$ は $\mathbb{Q}$ 上の既約多項式のベキであることがわかる.

注意 2.10. Abel 多様体 A が単純であっても, A の特性多項式 $P_A(t)$ が $\mathbb{Q}$ 上既約とは限らない. 今, $P_A(t) = Q(t)^e$ ($Q(t)$ は $\mathbb{Q}$ 上の既約多項式) と書けたとする. このとき $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ は $\mathbb{Q}[\xi_A]$ の上の e^2 次の division algebra である. したがって特性多項式 $P_A(t)$ が $\mathbb{Q}$ 上既約であることと $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}[\xi_A]$ であること, すなわち $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ が可換であることは同値である.

2.11 定理における **(2)** 全射性について議論する. Weil number に対して, まず代数的閉体上の単純 Abel 多様体を構成し, それを descent することによって対応する単純 Abel 多様体を構成する. そのためにまず準備を行う.

Weil number π_1, π_2 に対して, π_1 と π_2 が同値であるとは, ${\pi_1}^{\nu_1}$ が ${\pi_2}^{\nu_2}$ と共役であるような整数 $\nu_1 > 0, \nu_2 > 0 \in \mathbb{Z}$ が存在することである. π_1 と π_2 が同値であるとき $\pi_1 \sim \pi_2$ と記す. 同様に, (A_0) 型のイデアル I_1, I_2 に対して, I_1 と I_2 が同値であるとは, ${I_1}^{\nu_1}$ が ${I_2}^{\nu_2}$ と共役であるような整数 $\nu_1 > 0, \nu_2 > 0 \in \mathbb{Z}$ が存在することである. I_1 と I_2 が同値であるとき $I_1 \sim I_2$ と記す.

order r の Weil number π に対して, 対応する $\mathbb{F}_{p^r}$ 上の $\mathbb{F}_{p^r}$ 単純 Abel 多様体 A を構成する. 以下, r を固定して $q = p^r$ とおく. 構成の手順を述べる (下模式図参照). order r の Weil number π に対して, π の同値類 $<\pi>$ を考える. さらに $<\pi>$ に対応する (A_0) 型のイデアルの同値類 $<(\pi)>$ を考える (実はこの対応は 1 : 1, Honda [1], Theorem 1). そして $<(\pi)>$ に対応する $\overline{\mathbb{F}_q}$ 上の単純 Abel 多様体の $\overline{\mathbb{F}_q}$ 同種類 $<B>$ を構成し, $<B>$ を descent することによって, 求める $\mathbb{F}_q$ 上の単純 Abel 多様体の $\mathbb{F}_q$ 同種類 $[A]$ を得る.



2.12 以下構成に関して, 特に上図 $(*)$ 部分について解説する. 次に述べる補題がこの構成に関する key lemma である.

補題 2.13. (Honda [1], Theorem 2.)
ある代数体の (A_0) 型のイデアル I に対して, 以下を満たす CM 型 $(F;\{\varphi_i\})$ が存在する.

$$\textbf{条件}: \quad F \text{ は } \mathbb{Q} \text{ 上正規,} \qquad \prod_i \mathfrak{p}^{\psi_i} \sim I.$$

ただし, $\mathfrak{p}$ は p の F における素因子であり, $\psi_i = \varphi_i^{-1}$ である.

I をある代数体の (A_0) 型のイデアルとする. このとき

定理 2.14. (Shimura [4], CHAPTER III, Proposition 26.)
CM 型 $(F;\{\varphi_i\})$ に対して, $(F;\{\varphi_i\})$ を CM 型にもつ有限次代数体 K 上の Abel 多様体 (A,ι) が存在する.

から補題 2.13 の条件を満たす CM 型 $(F;\{\varphi_i\})$ をもつ代数体 K 上の Abel 多様体 (A,ι) が存在する. 今 $F^{\varphi_i} \subset K$ ($\forall i$) と仮定する. このとき

定理 2.15. (Serre-Tate [3])
代数体 K 上の Abel 多様体 (A,ι) に対して, A は potencially good reduction をもつ.

から, A は K の任意の素イデアルで good reduction をもつと仮定してよい. p の F における素因子を $\mathfrak{p}$ とし, p の K における素因子を $\mathfrak{P}$ とする. $\tilde{A} = A \mod \mathfrak{P}$ とおく. こ

のとき $\pi_0 \in F$ が存在して $\tilde{\iota}(\pi_0)$ が $\tilde{A}$ の Frobenius 準同型であり

$$(\pi_0) = \prod_i (\mathrm{Nr}_{K/F^{\varphi_i}}(\mathfrak{P}))^{\psi_i}$$

をみたす. ただし $\psi_i = \varphi_i^{-1}$ である. 一方, $\tilde{A}$ は単純 Abel 多様体のベキであり, その単純成分を B とおく. この単純 Abel 多様体 B が (A_0) 型のイデアル I に対応する単純 Abel 多様体である. 実際 ξ_B を B の Frobenius 準同型とすると

$$(\xi_B) \sim (\pi_0) = \prod_i (\mathrm{Nr}_{K/F^{\varphi_i}}(\mathfrak{P}))^{\psi_i} \sim \prod_i \mathfrak{p}^{\psi_i} \sim I$$

が成立する.

例 2.16. $\pi = -2 + \sqrt{-3}$ とおく. このとき $\pi\overline{\pi} = (-2+\sqrt{-3})(-2-\sqrt{-3}) = 7$ であるから π は $p = 7$ に関する order 1 の Weil number である. 今, π に対応する $\mathbb{F}_7$ 上の楕円曲線を E とおく. このとき $P_E(t)$ を E の Frobenius 準同型の特性多項式とすると

$$\begin{aligned} P_E(t) &= t^2 - (\pi + \overline{\pi})t + \pi\overline{\pi} \\ &= t^2 + 4t + 7 \end{aligned}$$

が成立する. したがって

$$\#E(\mathbb{F}_7) = P_E(1) = 1 + 4 + 7 = 12$$

が成立する.

今, $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-3})$ であり, $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ を $\mathbb{Q}(\sqrt{-3})$ の整数環とすると $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z} + \mathbb{Z}((1+\sqrt{-3})/2)$ である. $L = \mathbb{Z} + \mathbb{Z}((1+\sqrt{3}i)/2)$ とおくと L は $\mathbb{C}$ の格子であり, $\mathbb{C}/L$ は複素トーラスになる. ここで E' を複素トーラス $\mathbb{C}/L$ に対応する $\mathbb{C}$ 上の楕円曲線とする. このとき E' は $y^2 = x^3 + 1$ で定義されており, $\tilde{E}' = E' \bmod 7$ とおくと

$$\begin{aligned} \tilde{E}'/\mathbb{F}_7 : y^2 &= x^3 + 1, \\ \#\tilde{E}'(\mathbb{F}_7) &= 12 \end{aligned}$$

がわかる.

例 2.17. $\pi = (2 + \sqrt{3} + \sqrt{-(13 - 4\sqrt{3})})/2 = (2 + \sqrt{3} + \sqrt{-1}(2\sqrt{3} - 1))/2$ とおく. π は $t^4 - 4t + 11t^2 - 20t + 25 = (t^2 - (2+\sqrt{3})t + 5)(t^2 - (2-\sqrt{3})t + 5)$ の根である. よって, π は $p = 5$ に関する order $r = 1$ の Weil number である. 以下, (A_0) 型のイデアル $I = (\pi)$ に対して, 補題 2.13 をみたす CM 型を構成する.

今 $\mathbb{Q}(\pi)$ は $\mathbb{Q}$ 上 4 次の Galois 拡大 $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ である. このとき Galois 群は

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{-1})/\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$$

である. ただし $\sigma_1 : \sqrt{3} \mapsto -\sqrt{3}$, $\sigma_2 : \sqrt{-1} \mapsto -\sqrt{-1}$ である.

$p = 5$ の $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ における素イデアル分解は, $\mathfrak{p}_1 = (2 + \sqrt{-1}), \mathfrak{p}_2 = (2 - \sqrt{-1})$ とおくとき $(5) = \mathfrak{p}_1\mathfrak{p}_2$ である. またイデアル $I = (\pi)$ の素イデアル分解は $I = (\pi) = \mathfrak{p}_2$ である. 実際,

$$\begin{aligned}\pi = \frac{2 + \sqrt{3} + \sqrt{-1}(2\sqrt{3} - 1)}{2} &= \frac{(2 - \sqrt{-1}) + \sqrt{3}(1 + 2\sqrt{-1})}{2} \\ &= \frac{(2 - \sqrt{-1}) + \sqrt{3}\sqrt{-1}(2 - \sqrt{-1})}{2} \\ &= (2 - \sqrt{-1})\frac{1 + \sqrt{3}\sqrt{-1}}{2}\end{aligned}$$

よりわかる.

以下, CM 型 $(\mathbb{Q}(\sqrt{3}, \sqrt{-1}); \{\varphi_1, \varphi_2\})$ で $\mathfrak{p}_1^{\varphi_1^{-1}}\mathfrak{p}_1^{\varphi_2^{-1}} \sim I$ をみたすものを決定する. イデアル I の形と Galois 群 $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{-1})/\mathbb{Q})$ の形からすぐに条件をみたす φ_1, φ_2 を決定できるが, 一般論を視野に入れ構成的に考える.

今 $\mathfrak{p}_1$ に関する分解群 Z は

$$\begin{aligned}Z &= \{\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{-1})/\mathbb{Q}) \mid \mathfrak{p}_1^{\tau} = \mathfrak{p}_1\} \\ &= \{\mathrm{id}, \sigma_1\}\end{aligned}$$

である. よって $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{-1})/\mathbb{Q}) = Z\ \mathrm{id} + Z\sigma_2$ が成立する. このとき $(p), I$ の素イデアル分解はそれぞれ

$$\begin{aligned}(p) = (5) = \mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_1^e\mathfrak{p}_1^{e\sigma_2} = \mathfrak{p}_1\mathfrak{p}_1^{\sigma_2} \quad (e = 1) \\ I = (\pi) = \mathfrak{p}_2 = \mathfrak{p}_1^{\nu_1}\mathfrak{p}_1^{\nu_2\sigma_2} = \mathfrak{p}_1^{\sigma_2} \quad (\nu_1 = 0, \nu_2 = 1)\end{aligned}$$

となる. 一方 $p = 5$ の $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ における相対次数 f は $f = 2$ である. $d = f/r = 2$ とおく.

まず $d\nu_1 = 0$ 個の元を分解群 Z からえらび, その選んだ元のなす Z の部分集合を S_1 とおく. ここでは $S_1 = \emptyset$ である. 今, 埋め込み $\rho : \mathbb{Q}(\sqrt{3}, \sqrt{-1}) \to \mathbb{C}$ を複素共役とする. このとき $S_2 := Z\ \mathrm{id}\rho - S_1\rho = Z\sigma_2 - \emptyset = Z\sigma_2 = \{\sigma_2, \sigma_1\sigma_2\}$ となる. 集合 S_2 の元 $\varphi_1 = \sigma_2, \varphi_2 = \sigma_1\sigma_2$ が求める CM 型 の埋め込みである. 実際,

$$\begin{aligned}\mathfrak{p}_1^{\varphi_1^{-1}}\mathfrak{p}_1^{\varphi_2^{-1}} &= (2 + \sqrt{-1})^{\varphi_1^{-1}}(2 + \sqrt{-1})^{\varphi_2^{-1}} \\ &= (2 - \sqrt{-1})^2 \\ &= \mathfrak{p}_2^2 \\ &= I^2 \\ &\sim I\end{aligned}$$

が成立する.

2.18 最後に, order r の Weil number π に対して, 対応する $\mathbb{F}_q$ 上の Abel 多様体を構成する. $q = p^r$ とおく. このとき前節の考察により π に対して, 整数 $\nu \geq 1$ と $\mathbb{F}_{q^\nu}$ 上の単純 Abel 多様体 B で, π^ν の $\mathbb{Q}(\pi^\nu) \to \mathrm{End}_{\mathbb{F}_{q^r}}(B) \otimes \mathbb{Q}$ による像が B の Frobenius 準同型になるものが存在する. σ を $\mathbb{F}_{q^\nu}/\mathbb{F}_q$ の Frobenius 置換とする. ここで $C = B \times B^\sigma \times B^{\sigma^2} \times \cdots \times B^{\sigma^{\nu-1}}$ とおき, g を因子の入れ換えにより定まる同型射 $g : C^\sigma \to C$ とする. このとき, $\mathbb{F}_q$ 上の Abel 多様体 A_0 と $\mathbb{F}_{q^\nu}$ 上の同型射 $f : C \to A_0$ で $f^\sigma = f \circ g$ をみたすものが存在する (Weil [7], Theorem 3.). Abel 多様体 A_0 の単純成分 A が Weil number π に対応する $\mathbb{F}_q$ 上の単純 Abel 多様体である.

参考文献

[1] T. Honda, Isogeny classes of abelian varieties over finite fields, *J. Math. Soc. Japan.*, Vol. 20, Nos. 1-2, 83-95(1968)

[2] D. Mumford, *Abelian varieties*, Tata Inst. Studies in Math., Oxford University Press 1970

[3] J.-P. Serre and J. Tate, Good reduction of abelian varieties, *Ann. of Math.*, (2),88, 492-517(1968)

[4] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series 46, Princeton University Press 1998

[5] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.*, 2, 134-144(1966)

[6] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Scient. Éc. Norm. Sup.*, 4^e série, t. 2, 521-560(1969)

[7] A. Weil, The field of definition of a variety, *Amer. J. Math.*, 78, 509-524(1956)

土屋和由
中央大学大学院理工学研究科数学専攻博士後期課程 2 年
112-8551
東京都文京区春日 1-13-27
e-mail address : kazu@grad.math.chuo-u.ac.jp