# 志村曲線およびその関数体類似の有理点について

新井 啓介 (東京電機大学)

**概 要**

QM アーベル曲面 (つまり有理数体上の不定符号 4 元数体の極大整環の作用する 2 次元アーベル多様体) のモジュライ空間は, 志村曲線と呼ばれる. 志村曲線の有理点の非存在に関して筆者が得た研究成果を紹介する. また, $\mathscr{D}$-elliptic sheaf や Drinfeld-Stuhler module と呼ばれるもののモジュライ空間は, 志村曲線の関数体類似になっている. 筆者が最近取り組んでいるこの関数体類似の有理点の非存在に関する研究成果についても, 併せて紹介する. 今回の主結果を用いると, ハッセ原理の反例の具体例を構成することができる. なお, 関数体類似の方の研究は, 近藤智氏と Mihran Papikian 氏との共同研究である.

## 1 序文 (ハッセ原理の反例)

本節では, ハッセ原理やその反例について具体例を挙げつつ述べる. 次の記号を用いる.

- $K$: 代数体, つまり有理数体 $\mathbb{Q}$ の有限次拡大体 (例: $K = \mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$),
- $\Omega_K$: $K$ の素点全体の集合,
- $K_v$: $K$ の $v \in \Omega_K$ での完備化.

**例 1.1.** $K = \mathbb{Q}$ とすると, $\Omega_K = \{\text{ 素数 }\} \cup \{\infty\}$ (ただし $\infty$ は無限素点と呼ばれるもの) と自然に同一視される. また

$$K_v = \begin{cases} \mathbb{Q}_p & (v = p\ (\text{素数})\ \text{のとき}), \\ \mathbb{R} & (v = \infty\ \text{のとき}) \end{cases}$$

である.

まず, 方程式

$$x^2 + y^2 + 3 = 0 \tag{1.1}$$

の解を考えよう. 次の同値が成り立つ.

$$
\begin{aligned}
&\quad \text{(1.1) が } K \text{ に解をもつ} \\
\Longleftrightarrow\ & \forall v \in \Omega_K \text{ に対して, (1.1) が } K_v \text{ に解をもつ} \\
\Longleftrightarrow\ & \text{任意の無限素点 } v \in \Omega_K \text{ および 3 を割る任意の } v \in \Omega_K \text{ に対して, (1.1) が } K_v \text{ に解をもつ} \\
\Longleftrightarrow\ & \begin{cases} \text{(i) 体の埋め込み } K \hookrightarrow \mathbb{R} \text{ が存在せず, かつ} \\ \text{(ii) } \forall v \in \Omega_K\ (v \mid 3) \text{ に対して拡大次数 } [K_v : \mathbb{Q}_3] \text{ が偶数.} \end{cases}
\end{aligned}
$$

最初の同値は, ハッセ原理 (後述) による. 2 番目の同値は, 次の補題による.

**補題 1.2** ([2, 補題 1.1])**.** (1) (1.1) は 3 以外の全ての素数 $p$ に対して $\mathbb{Q}_p$ に解をもつ.

(2) (1.1) は $\mathbb{R}$, $\mathbb{Q}_3$ に解をもたない.

**注 1.3.** (1) $K$ に解をもつ $\Longrightarrow$ $\forall v \in \Omega_K$ に対して $K_v$ に解をもつ ($K \subseteq K_v$ だから).

(2) ($K$ 係数の多項式) $= 0$ という方程式に対して,
「$\forall v \in \Omega_K$ に対して $K_v$ に解をもつ $\Longrightarrow$ $K$ にも解をもつ」
が成り立つとき, **ハッセ原理**が成り立つという.

(3) 方程式 (1.1) に関して, (任意の代数体 $K$ に対して) ハッセ原理が成り立つ (例えば [2, 第 1 節], [5, Theorem 5.3.3] を参照).

方程式 (1.1): $x^2 + y^2 + 3 = 0$ の解の有無の具体例を, 表 1 に挙げる.

表 1: $x^2 + y^2 + 3 = 0$ の $K$ における解の有無

| 解なし | 解あり |
|---|---|
| • $[K : \mathbb{Q}]$ が奇数<br>• $K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}),$<br>$\mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ | • $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ |

表 1 に関して, 次のことが言える.

- $[K : \mathbb{Q}]$ が奇数のときや $K = \mathbb{Q}(\sqrt{2})$ のときは, $K$ は $\mathbb{R}$ の部分体になる.
- 3 は $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ で完全分解し, $\mathbb{Q}(\sqrt{-1})$ で惰性し, $\mathbb{Q}(\sqrt{-3})$ で分岐する.
- 解の存在は
$$1^2 + (2\sqrt{-1})^2 + 3 = 0, \quad 0^2 + (\sqrt{-3})^2 + 3 = 0$$
のように直接確かめることもできる.

以上の考察で見たように, 方程式の代数体における解の有無という難解な問題が, **ハッセ原理が成り立つときは**比較的易しい局所的な解の有無を調べれば解けてしまう.

次に, 方程式

$$y^2 = -(x^4 + x^3 - x^2 - x + 1)(7x^4 + 23x^3 + 5x^2 - 23x + 7) \tag{1.2}$$

を考える. この方程式が $\mathbb{R}$ に解をもたないことは, 実数の 2 乗は 0 以上ということから分かる ([2, 補題 1.2] を参照). 代数体や局所体における解の有無については, 例えば次のことが分かる.

**命題 1.4.** $n \in \mathbb{Z}$ を平方因子をもたない奇数, $K = \mathbb{Q}(\sqrt{-13}, \sqrt{2n})$ とするとき, 次が成り立つ.

(1) (1.2) は $K$ に解をもたない.

(2) (1.2) は $\forall v \in \Omega_K$ に対して $K_v$ に解をもつ.

**注 1.5.** (1) 方程式 (1.2) は $K$ 上の**ハッセ原理の反例**を与える. つまり, 方程式 (1.2) は

(i) 大域的に考えると解をもたないが,

(ii) 局所的に考えると至る所で解をもつ.

(2) ハッセ原理の反例は数論的に面白い現象であり, 上の命題はハッセ原理の反例の**無限族**を与えている ($n$ が無限通りに変化するから).

ここで, 代数体と関数体の類似はよく知られている. 表 2 に $\mathbb{Q}$ と $\mathbb{F}_q(T)$ の類似をまとめる. $\mathbb{F}_q$ は, 元の個数が $q$ であるような有限体である.

表 2: $\mathbb{Q}$ と $\mathbb{F}_q(T)$ の類似

| 代数体側 | 関数体側 |
|---|---|
| $\mathbb{Q}$ | $F = \mathbb{F}_q(T)$ |
| $\mathbb{Z}$ | $A = \mathbb{F}_q[T]$ |
| 素数 $l$ | 既約モニック多項式 $f \in A \setminus \mathbb{F}_q$ |
| 無限素点 $\infty$ | $\frac{1}{T} \in F$ |
| $\mathbb{Q}_l$ | $F_f$ |
| $\mathbb{R}$ | $\mathbb{F}_q((\frac{1}{T}))$ |
| 有限次拡大 $K/\mathbb{Q}$ | 有限次拡大 $K/F$ |
| 整数環 $\mathcal{O}_K$ $(\subseteq K)$ | "整数環" $\mathcal{O}_K$ $(\subseteq K)$ |
| 楕円曲線 $E/K$ | Drinfeld module $\phi/K$ |
| QM アーベル曲面 $A/K$ | Drinfeld-Stuhler $\mathcal{O}_D$-module $\phi/K$ |
| 志村曲線 $M^B/\mathbb{Q}$ | Drinfeld-Stuhler variety $X^D/F$ |

表 2 の関数体側において, $F_f$ は $F$ の $f$ での完備化を表し, $\mathcal{O}_K = \{\, x \in K \mid x \text{ は } A \text{ 上整} \,\}$ (つまり $A$ の $K$ における整閉包) である.

## 2 志村曲線の有理点 [代数体側]

本節では, 志村曲線の代数体上の有理点の非存在に関する結果, およびハッセ原理の反例への応用について述べる. 次の記号や用語を用いる.

- $B$: $\mathbb{Q}$ 上の不定符号 4 元数体
  (特に, $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$, $B \not\cong \mathrm{M}_2(\mathbb{Q})$),

- $\mathbf{Ram}(B) := \{\, p\text{: 素数} \mid B \otimes_{\mathbb{Q}} \mathbb{Q}_p \not\cong \mathrm{M}_2(\mathbb{Q}_p) \,\}$
  (このとき $\mathbf{Ram}(B)$ は空でない有限集合で, 偶数個の元より成る),

- $\mathcal{O} = \mathcal{O}_B \subseteq B$: 極大整環を 1 つ固定
  (ここで任意の極大整環は $a\mathcal{O}a^{-1}$, $a \in B$ の形である),

- 体 $L$ 上の $\mathcal{O}_B$ による **QM アーベル曲面** $(A, i)$:

  $$\begin{cases} A\text{: } L \text{ 上の 2 次元アーベル多様体}, \\ i : \mathcal{O}_B \hookrightarrow \mathrm{End}_L(A)\text{: } i(1) = 1 \text{ を満たす環の単射準同型} \end{cases}$$

  (ただし $\mathrm{End}_L(A)$ は $A$ の $L$ 上定義された自己準同型から成る環であり, また $(A, i)$ を単に $A$ と記すこともある),

- $M^B$: $\mathcal{O}_B$ による QM アーベル曲面の粗モジュライ.

このとき $M^B$ は $\mathbb{Q}$ 上の固有スムーズ代数曲線であり, **志村曲線**と呼ばれる. $M^B$ の有理点に関して, 次の定理は基本的である.

**定理 2.1.** [15, Theorem 0]
$M^B(\mathbb{Q}) = M^B(\mathbb{R}) = \emptyset$.

**例 2.2.** $\mathbf{Ram}(B) = \{\, 2, 3 \,\}$ なら, $M^B$ の定義方程式をアファイン形で表すと, 例えば

$$(1.1)\text{: } x^2 + y^2 + 3 = 0$$

となる ([9, Theorem 1-1]). この方程式は $\mathbb{Q}$ にも $\mathbb{R}$ にも解をもたない. 実際は $M^B$ は射影曲線なので, 同次形

$$X^2 + Y^2 + 3Z^2 = 0$$

で表される. 無限遠点も含めた有理点の正確な議論は, [2] を参照.

主定理の定式化のために, 記号を導入する. 素数 $q$ に対し, $\mathcal{B}(q)$ で次を満たす $\mathbb{Q}$ 上の不定符号 4 元数体 $B$ の (同型類の) 集合を表す.

$$\begin{cases} q \neq 2 \text{ なら} \\ \qquad B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q})), \\ q = 2 \text{ なら} \\ \qquad B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1})) \quad \text{かつ} \quad B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-2}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-2})). \end{cases}$$

$\mathcal{B}(q)$ は, 標数 $q$ の有限体上の QM アーベル曲面の自己準同型環の分類と関係している. 今回の代数体側の主定理を挙げる.

**定理 2.3.** [1, Theorem 1.1]

- $\mathfrak{q}$: $O_K$ の極大イデアル, 剰余標数は $q$,
- $\mathfrak{q}$ は $q$ の上の唯一の極大イデアル,
- $f_{\mathfrak{q}} := [\kappa(\mathfrak{q}) : \mathbb{F}_q]$ は奇数 (ただし $\kappa(\mathfrak{q})$ は $\mathfrak{q}$ の剰余体),
- $B \in \mathcal{B}(q)$

とすると, 素数の**計算可能な**有限集合 $S(K, \mathfrak{q})$ があって次を満たす.

「素数 $p$ で $p \in \mathbf{Ram}(B)$, $p \notin S(K, \mathfrak{q}) \cup \{ q \}$ なるものがあれば, $M^B(K) = \emptyset$」.

**注 2.4.** (1) $[K : \mathbb{Q}] = 2$ の場合は既に知られている ([7, Theorem 6.3], [13, Theorem 1.1]).

(2) $S(K, \mathfrak{q})$ は実際は $\kappa(\mathfrak{q})$ の元の個数 $q^{f_{\mathfrak{q}}}$ と, $\mathfrak{q}$ の $K/\mathbb{Q}$ での分岐指数 $e_{\mathfrak{q}}$ に依存する.

(3) 各条件は, 具体的な計算でチェックできる $\Longrightarrow$ $M^B(K) = \emptyset$ の**具体例が作れる.**

**例 2.5.** $\mathbf{Ram}(B) = \{ 3, 13 \}$, $K = \mathbb{Q}(\sqrt{-13}, \sqrt{2n})$ (ただし $n \in \mathbb{Z}$ は平方因子をもたない奇数) とすると, $(p, q) = (13, 2)$ として定理 2.3 を適用して,

$$M^B(K) = \emptyset$$

を得る (ここで $S(K, \mathfrak{q}) = \{ 2, 3, 5, 7, 47 \}$ である). また, $M^B$ の局所体上の有理点の存在のための必要十分条件 [8, Theorems 2.5, 5.1, 5.4, 5.6] (または [7, Theorem 0]) を用いて,

$$\text{任意の } v \in \Omega_K \text{ に対して } M^B(K_v) \neq \emptyset$$

が分かる. さらに [6, Theorem 4.5] により, $M^B$ の定義方程式をアファイン形で表すと, 例えば

$$(1.2)\text{: } y^2 = -(x^4 + x^3 - x^2 - x + 1)(7x^4 + 23x^3 + 5x^2 - 23x + 7)$$

となる. これより命題 1.4 が従う. 実際は $M^B$ は射影曲線 (さらに言えば超楕円曲線) であり, 無限遠点も含めた有理点の正確な議論は, [2] を参照.

志村曲線の有理点に関する研究の動向については, [3] を参照.

# 3 Drinfeld-Stuhler variety の有理点 [関数体側]

本節では, 前節の関数体類似を述べる. すなわち, Drinfeld-Stuhler variety の関数体上の有理点の非存在に関する結果, およびハッセ原理の反例への応用について述べる. 関数体側の理論に馴染みのある読者は多くないと思われるため, まず Drinfeld module や Drinfeld-Stuhler module について簡単に説明する.

[Drinfeld module の説明]

次の記号や用語を用いる. 2 節 [代数体側] と同じ記号が違う意味に使われている場合もあるので, 注意されたい.

- $p$: 素数, $q = p^r \quad (r \in \mathbb{Z}, r \geq 1)$,
- $F = \mathbb{F}_q(T)$, $A = \mathbb{F}_q[T]$,
- $L$: $A$-field, つまり $L$ は体で, $\gamma(1) = 1$ を満たす環準同型 $\gamma : A \longrightarrow L$ が与えられているもの (例: $L = F$ で $\gamma$ は包含写像, $L = A/TA \cong \mathbb{F}_q$ で $\gamma$ は標準全射),
- $L[\tau] := \{ a_n\tau^n + \cdots + a_1\tau + a_0 \mid n \geq 0,\ a_i \in L \}$,
  演算 $\left\{\begin{array}{l} \text{和: 普通のやり方,} \\ \text{積: } \tau a = a^q\tau \ (a \in L) \end{array}\right\}$ により, $L[\tau]$ は ($L \cong \mathbb{F}_q$ の場合を除いて) **非可換環**になる,
- $\partial : L[\tau] \longrightarrow L;\ \displaystyle\sum_{i=0}^{n} a_i\tau^i \mapsto a_0$,
- $L$ 上の **Drinfeld module** とは:
  $\mathbb{F}_q$ 代数の準同型
  $$\phi : A\ (= \mathbb{F}_q[T]) \longrightarrow L[\tau];\ a \mapsto \phi_a$$
  で次を満たすもの.
  $$\begin{cases} (0)\ \phi_1 = 1, \\ (1)\ \partial \circ \phi(a) = \gamma(a) \in L \quad (\forall a \in A), \\ (2)\ \phi(A) \not\subseteq L. \end{cases}$$

**注 3.1.** (1) Drinfeld module $\phi$ は $T$ の像 $\phi_T$ によって決まる.

(2) $\phi_T = \gamma(T) + \displaystyle\sum_{i=1}^{r} a_i\tau^i \in L[\tau] \quad (r \geq 1,\ a_i \in L,\ a_r \neq 0)$
という形に表される. この $r$ は $\phi$ の**ランク**と呼ばれ, $\phi$ の「大きさ」を表す. $r$ は $\phi$ の Tate 加群のランクに等しい.

(3) $\phi$ は単射になる.

**例 3.2.** (1) $\phi_T = \gamma(T) + \tau \quad$ (ランク 1). これは Carlitz module と呼ばれ, Drinfeld module の原型とでも言うべきものである.

(2) $\phi_T = \gamma(T) + \tau + \tau^2 \quad$ (ランク 2).

先の定義によれば, Drinfeld module $\phi$ は (いくつかの条件を満たす) 環の準同型である. 実は, $\phi$ は次のような幾何的な見方をすることもできる. まず,

$$\mathbb{G}_a = \mathbb{G}_{a,L} = \operatorname{Spec} L[X]$$

には, 次のように $L$ 上の群スキームの構造が入る. $\mathbb{G}_a$ は**加法群**と呼ばれる.

- $+ : \mathbb{G}_a \times \mathbb{G}_a \longrightarrow \mathbb{G}_a$ は
  $L[X] \longrightarrow L[X] \otimes_L L[X];\ X \mapsto X \otimes 1 + 1 \otimes X$,

- $-1 : \mathbb{G}_a \longrightarrow \mathbb{G}_a$ は
  $L[X] \longrightarrow L[X];\ X \mapsto -X$,

- $0 : \operatorname{Spec} L \longrightarrow \mathbb{G}_a$ は
  $L[X] \longrightarrow L;\ X \mapsto 0$
  から定まる.

$$\operatorname{End}_L(\mathbb{G}_a) := \{\, f : \mathbb{G}_a \longrightarrow \mathbb{G}_a \mid f \text{ は } L \text{ 上の群スキームの射} \,\}$$

とおく. これは $L$ 代数になる.

**補題 3.3.** $L$ 代数として,

$$L[\tau] \cong \operatorname{End}_L(\mathbb{G}_a).$$

ここに, $\tau$ は $\mathbb{G}_a = \operatorname{Spec} L[X]$ に $\tau(X) = X^q$, $\tau(a) = a$ $(a \in L)$ として作用する.

この補題より, Drinfeld module $\phi : A \longrightarrow L[\tau]$ は

$$\phi : A \longrightarrow L[\tau] \cong \operatorname{End}_L(\mathbb{G}_a)$$

となり, **$A$ の作用する** $\mathbb{G}_a$ と思える. この作用のしかたがいろいろあり, それによって様々な Drinfeld module ができる. ($\mathbb{G}_a$ は 1 次元である. ランク 2 の場合が最も楕円曲線に性質が近い.)

[Drinfeld-Stuhler module の説明]
次の記号や用語を用いる.

- $p$: 素数, $q = p^r$ $(r \in \mathbb{Z},\ r \geq 1)$,

- $F = \mathbb{F}_q(T)$, $A = \mathbb{F}_q[T]$,

- $L$: $A$-field,

- $L[\tau] := \{\, a_n\tau^n + \cdots + a_1\tau + a_0 \mid n \geq 0,\ a_i \in L \,\}$,
  $\tau a = a^q \tau$ $(a \in L)$.

ここまでは, Drinfeld module の場合と同じである.

- $d \in \mathbb{Z}$, $d \geq 1$ を固定,

- $D$: $F$ 上の中心的単純環, $\dim_F D = d^2$
  (例: $D = \mathrm{M}_d(F)$),

- $D \otimes_F \mathbb{F}_q((\frac{1}{T})) \cong \mathrm{M}_d(\mathbb{F}_q((\frac{1}{T})))$ と仮定
  (この条件は志村曲線のときの $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$ の類似),

- $\mathbf{Ram}(D) := \{\, f \in A \setminus \mathbb{F}_q$: 既約モニック $\mid D \otimes_F F_f \not\cong \mathrm{M}_d(F_f) \,\}$,
- $\mathcal{O} = \mathcal{O}_D \subseteq D$: 極大整環, 1 つ固定,
- $L$ 上の **Drinfeld-Stuhler $\mathcal{O}_D$-module** とは:
  $\mathbb{F}_q$ 代数の単射準同型

$$\phi : \mathcal{O}_D \longrightarrow \mathrm{M}_d(L[\tau])\ (\cong \mathrm{End}_L(\mathbb{G}_a^d));\ a \mapsto \phi_a$$

で次を満たすもの.

$$\begin{cases} (0)\ \phi_1 = 1, \\ (1)\ \partial \circ \phi(a) = \begin{pmatrix} \gamma(a) & & O \\ & \ddots & \\ O & & \gamma(a) \end{pmatrix} \in \mathrm{M}_d(L) \quad (\forall a \in A \subseteq \mathcal{O}_D) \\ \qquad (\text{ここに } \partial : \mathrm{M}_d(L[\tau]) \longrightarrow \mathrm{M}_d(L);\ \sum_{i=0}^n B_i\tau^i \mapsto B_0,\ \text{ただし } B_i \in \mathrm{M}_d(L)), \\ (2)\ 0 \neq \forall b \in \mathcal{O}_D \text{ に対して}, \ker(\phi_b : \mathbb{G}_a^d \longrightarrow \mathbb{G}_a^d)\ (\subseteq \mathbb{G}_a^d) \text{ は } L \text{ 上の位数} \\ \qquad \sharp(\mathcal{O}_D/(\mathcal{O}_D \cdot b)) \text{ の有限群スキーム}. \end{cases}$$

**注 3.4.** (1) Drinfeld-Stuhler $\mathcal{O}_D$-module $\phi$ は, $\mathcal{O}_D$ の作用する $\mathbb{G}_a^d$ と思える ($\mathbb{G}_a^d$ は $d$ 次元).

(2) $d = 1$
$\Longrightarrow \mathcal{O}_D = A$, Drinfeld-Stuhler $\mathcal{O}_D$-module $\phi$ はランク 1 の Drinfeld module.

(3) $d = 2$
$\Longrightarrow \phi$ は (狭い意味で) QM アーベル曲面の類似.

(4) 正標数での局所 Langlands 対応という文脈で, $\mathscr{D}$-elliptic sheaf というものが出てきた ([10]). $\mathscr{D}$-elliptic sheaf の定義は複雑で分かりづらいように思われる. Drinfeld-Stuhler $\mathcal{O}_D$-module は $\mathscr{D}$-elliptic sheaf を分かりやすく表現し直したもの, と理解することができる.

ここで,

- $X^D$: “Drinfeld-Stuhler $\mathcal{O}_D$-module の粗モジュライ”
  (厳密には $\mathscr{D}$-elliptic sheaf の粗モジュライ)

とする. $D$ が斜体なら $X^D$ は $F$ 上の固有スムーズ代数多様体であり, **Drinfeld-Stuhler variety** と呼ばれる. また,

$$\dim X^D = d - 1$$

である. $X^D$ は志村曲線 $M^B$ の広い意味での類似である. $d = 2$ なら $\dim X^D = 1$ であり, $X^D$ は $M^B$ の狭い意味での類似である. 今回の関数体側の主定理を挙げる.

**定理 3.5.** [4, Theorem 6.10]

- $K$ は $F$ の拡大体で $[K:F]=d,\ \ D\otimes_F K\cong \mathrm{M}_d(K)$,
- $\mathfrak{n}\in A\setminus\mathbb{F}_q$: 既約モニック, $K$ で完全分岐,
- $\forall\mu\in\mathbb{F}_q^\times$ に対して $D\otimes_F F(\sqrt[d]{\mu\mathfrak{n}})\not\cong \mathrm{M}_d(F(\sqrt[d]{\mu\mathfrak{n}}))$,
- $\mathfrak{n}\notin\mathbf{Ram}(D)$,
- $\mathfrak{p}\in\mathbf{Ram}(D)$, $\mathrm{inv}_{\mathfrak{p}}(D)=\frac{1}{d}\ (\in\mathbb{Q}/\mathbb{Z}\cong\mathrm{Br}(F_{\mathfrak{p}}))$

とすると, $A\setminus\mathbb{F}_q$ の既約モニック多項式の**計算可能な**有限集合 $S(K,\mathfrak{n},\deg(\mathfrak{p}))$ があって次を満たす.
「$\mathfrak{p}\notin S(K,\mathfrak{n},\deg(\mathfrak{p}))\Longrightarrow X^D(K)=\emptyset$」.

**注 3.6.** (1) $F_{\mathfrak{p}}$ は $F$ の $\mathfrak{p}$ での完備化であり, $\mathrm{Br}(F_{\mathfrak{p}})$ は $F_{\mathfrak{p}}$ のブラウアー群であり, $\mathrm{inv}_{\mathfrak{p}}(D)$ は $D\otimes_F F_{\mathfrak{p}}$ の $\mathrm{Br}(F_{\mathfrak{p}})$ における不変量である.

(2) 仮定「$[K:F]=d,\ \ D\otimes_F K\cong\mathrm{M}_d(K)$」は弱められそうである.

(3) 仮定 $\mathfrak{p}\notin S(K,\mathfrak{n},\deg(\mathfrak{p}))$ では, 例外集合 $S(K,\mathfrak{n},\deg(\mathfrak{p}))$ が $\mathfrak{p}$ に依存する (代数体側では例外集合 $S(K,\mathfrak{q})$ は $p$ に依存しなかった). このため, 仮定を満たす $\mathfrak{p}$ は具体例を探す際に少し見つけにくくなっている. この違いが生じる原因は, 関数体は代数体とは異なり「定数拡大」(つまり $\mathbb{F}_q(T)$ に対して $\mathbb{F}_{q^n}(T)$ という拡大) をもつことにある. このために, 代数体側と関数体側では類体論を用いたガロア群の指標の計算に違いが出る.

**例 3.7.** $d=2, q=5, \mathbf{Ram}(D)=\{\,T^3+2T+4, T+2\,\}$, $K=F(\sqrt{2T(T^3+2T+4)(T+2)})$ とすると, $(\mathfrak{p},\mathfrak{n})=(T^3+2T+4,T)$ として定理 3.5 を適用して,

$$X^D(K)=\emptyset$$

を得る. また, $d=2$ の場合の $X^D$ の局所体上の有理点の存在のための必要十分条件 [11, Theorems 3.1, 4.1, 5.10] を用いて,

$$\forall v\in\Omega_K \text{ に対して } X^D(K_v)\neq\emptyset$$

が分かる. これより $K$ 上の**ハッセ原理の反例**が得られる (代数多様体に関するハッセ原理については, [16] を参照). ただし, この場合の $X^D$ の定義方程式は知られていないようである.

# 4 証明の方針

[定理 2.3 の証明の方針 (代数体側)]

$M^B$ は精モジュライではなく粗モジュライであるため, $M^B$ の $K$ 有理点は $K$ 上の QM アーベル曲面と対応するとは限らない. 実際には, 次の定理が成り立つ.

**定理 4.1** ([7, Theorem 1.1])**.** $F$ を標数 0 の体とし, $x \in M^B(F)$ とする. このとき, $x$ が $F$ 上の QM アーベル曲面 $(A, i)$ と対応するための必要十分条件は, $B \otimes_{\mathbb{Q}} F \cong \mathrm{M}_2(F)$ である.

定理 2.3 の仮定の下で $M^B(K) \neq \emptyset$ だったとして, 矛盾を導く. $x \in M^B(K)$ をとる. $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ とすると, 定理 4.1 より $x$ は $K$ 上の QM アーベル曲面 $(A, i)$ と対応する. ($B \otimes_{\mathbb{Q}} K \not\cong \mathrm{M}_2(K)$ のときは, $B \otimes_{\mathbb{Q}} L \cong \mathrm{M}_2(L)$ となるような $K$ の 2 次拡大 $L$ をとると, $x$ は $L$ 上の QM アーベル曲面 $(A, i)$ と対応する. このことを利用して証明を行うが, ここでは詳細は略す.)

$p$ を素数, $n \geq 1$ を整数として,

$$A[p^n] := \ker([p^n] : A(\overline{K}) \longrightarrow A(\overline{K})),$$

$$T_pA := \varprojlim (A[p] \longleftarrow A[p^2] \longleftarrow \cdots)$$

とする. ここに $\overline{K}$ は $K$ の代数閉包, $[p^n] : A(\overline{K}) \longrightarrow A(\overline{K})$ は (アーベル群の) $p^n$ 倍写像, $\varprojlim$ の中の各 $A[p^n] \longleftarrow A[p^{n+1}]$ は $p$ 倍写像である. すると

$$A[p] \cong \mathcal{O}/p\mathcal{O},$$

$$T_pA \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

となる. $A[p]$ は $\mathbb{F}_p$ 線形空間としては 4 次元であり, $T_pA$ は $\mathbb{Z}_p$ 加群としては自由でランク 4 である. $A[p]$ および $T_pA$ へのガロア群 $\mathrm{G}_K := \mathrm{Gal}(\overline{K}/K)$ の作用から, それぞれガロア表現

$$R : \mathrm{G}_K \longrightarrow (\mathcal{O}/p\mathcal{O})^\times,$$

$$\widetilde{R} : \mathrm{G}_K \longrightarrow (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$$

が定まる.

$p \in \mathbf{Ram}(B)$ とすると,

$$\mathcal{O}/p\mathcal{O} \cong \left\{ \begin{pmatrix} a & * \\ 0 & a^p \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}_{p^2}) \right\}, \quad (\mathcal{O}/p\mathcal{O})^\times \cong \left\{ \begin{pmatrix} a & * \\ 0 & a^p \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2}) \right\}$$

となり ([17, Chapitre II, Corollaire 1.7] または [14, 補題 3.13 の証明] を参照), $R$ の $(1,1)$ 成分から**指標** (つまり群の準同型)

$$\varrho : \mathrm{G}_K \longrightarrow \mathbb{F}_{p^2}^\times$$

が生じる. $A$ は $K$ の全ての有限素点で potentially good reduction をもち, $\mathfrak{q}$ の上での (体拡大した後の) 還元は $\kappa(\mathfrak{q})$ 上の QM アーベル曲面になる (これを $A_{\kappa(\mathfrak{q})}$ と表すこと

にする). $p \neq q$ とする. $R, \widetilde{R}$ や $\varrho$ の $\mathfrak{q}$ でのフロベニウスの像は, $A_{\kappa(\mathfrak{q})}$ のフロベニウス自己準同型の作用を通して理解できる. $\mathfrak{q}$ の一意性の仮定は, 大域類体論を用いた $\varrho$ の $\mathfrak{q}$ での計算に使われる. $\widetilde{R}$ による $\mathfrak{q}$ でのフロベニウスの像の被約トレース $a$ は整数になるが, $p \notin S(K, \mathfrak{q})$ なら $a$ は $q$ で割れる. この $p \notin S(K, \mathfrak{q})$ という条件は, $a$ や $q$ に関係した整数の間の mod $p$ の合同式を等式にするための条件である. $f_{\mathfrak{q}}$ が奇数であることと有限体上の QM アーベル曲面 $A_{\kappa(\mathfrak{q})}$ の自己準同型環の分類により, $B \notin \mathcal{B}(q)$ となり, 矛盾が生じる. ゆえに $M^B(K) = \emptyset$ が従う. $\square$

[定理 3.5 の証明の方針 (関数体側)]

大雑把な方針は代数体側と同様である. 定理 4.1 の類似として, 次の定理が成り立つ.

**定理 4.2** ([12, Theorem 6.13]). $L$ を $A$-field とし, $\ker(\gamma : A \longrightarrow L) = fA$, ただし $f \in A$ は 0 または既約モニックとなるようにとる. $f \notin \mathbf{Ram}(D)$ と仮定し, また $x \in X^D(L)$ とする. このとき, $x$ が $L$ 上の Drinfeld-Stuhler $\mathcal{O}_D$-module $\phi$ と対応するための必要十分条件は, $\mathcal{O}_D \otimes_A L \cong \mathrm{M}_d(L)$ である.

定理 3.5 の仮定の下で $X^D(K) \neq \emptyset$ だったとして, $x \in X^D(K)$ をとる.

$$\ker(\gamma : A \longrightarrow K) = \{\, 0 \,\}$$

および

$$\mathcal{O}_D \otimes_A K \cong (\mathcal{O}_D \otimes_A F) \otimes_F K \cong D \otimes_F K \cong \mathrm{M}_d(K)$$

より, 定理 4.2 から $x$ は $K$ 上の Drinfeld-Stuhler $\mathcal{O}_D$-module $\phi$ と対応する. $\mathfrak{p} \in A \setminus \mathbb{F}_q$ を既約モニックとして,

$$\phi[\mathfrak{p}] := \ker([\phi_{\mathfrak{p}}] : (K^{\mathrm{sep}})^d \longrightarrow (K^{\mathrm{sep}})^d)$$

とする. ここに $K^{\mathrm{sep}}$ は $K$ の分離閉包, $[\phi_{\mathfrak{p}}]$ は $\phi_{\mathfrak{p}} \in \mathrm{End}_K(\mathbb{G}_a^d)$ が定める群準同型である. すると

$$\phi[\mathfrak{p}] \cong \mathcal{O}/\mathfrak{p}\mathcal{O}$$

となる. $\phi[\mathfrak{p}]$ は $\mathbb{F}_{\mathfrak{p}}$ $(:= A/\mathfrak{p}A)$ 線形空間として $d^2$ 次元である. $\phi[\mathfrak{p}]$ へのガロア群 $\mathrm{G}_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ の作用から, ガロア表現

$$R : \mathrm{G}_K \longrightarrow (\mathcal{O}/\mathfrak{p}\mathcal{O})^\times$$

が定まる.

$\mathfrak{p} \in \mathbf{Ram}(D)$ とすると, $\mathrm{inv}_{\mathfrak{p}}(D) = \frac{1}{d}$ より

$$(\mathcal{O}/\mathfrak{p}\mathcal{O})^\times \cong \left\{ \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_d \\ 0 & a_1^{q^s} & a_2^{q^s} & \cdots & a_{d-1}^{q^s} \\ 0 & 0 & a_1^{q^{2s}} & \cdots & a_{d-2}^{q^{2s}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_1^{q^{(d-1)s}} \end{pmatrix} \in \mathrm{GL}_d(\mathbb{F}_{\mathfrak{p}}^{(d)}) \right\}$$

(ただし $\mathbb{F}_{\mathfrak{p}}^{(d)}$ は $\mathbb{F}_{\mathfrak{p}}$ の $d$ 次拡大体, $\sharp\mathbb{F}_{\mathfrak{p}} = q^s$) となり, $R$ の $(1,1)$ 成分から指標

$$\varrho : \mathrm{G}_K \longrightarrow (\mathbb{F}_{\mathfrak{p}}^{(d)})^{\times}$$

が生じる. $\phi$ は $K$ の全ての有限素点で potentially good reduction をもち, $\mathfrak{n}$ の上での (体拡大した後の) 還元は $\mathbb{F}_{\mathfrak{n}}$ 上の Drinfeld-Stuhler $\mathcal{O}_D$-module になる (これを $\phi_{\mathbb{F}_{\mathfrak{n}}}$ と表すことにする). $\mathfrak{n} \notin \mathbf{Ram}(D)$ とする. $\phi_{\mathbb{F}_{\mathfrak{n}}}$ のフロベニウス自己準同型の最小多項式の係数を, $\varrho$ の計算を通して調べる. ここで, $\mathfrak{n}$ が $K$ で完全分岐, $\mathfrak{p} \notin S(K, \mathfrak{n}, \deg(\mathfrak{p}))$ という仮定を用いる. $\mathfrak{n} \notin \mathbf{Ram}(D)$ のときの $\phi_{\mathbb{F}_{\mathfrak{n}}}$ の自己準同型環の分類より, ある $\mu \in \mathbb{F}_q^{\times}$ に対して $D \otimes_F F(\sqrt[d]{\mu\mathfrak{n}}) \cong \mathrm{M}_d(F(\sqrt[d]{\mu\mathfrak{n}}))$ となり, 矛盾が生じる. ゆえに $X^D(K) = \emptyset$ が従う. $\square$

モジュライの有理点問題は, 代数体側ではいろいろな研究があるが, 関数体側ではあまり開拓されていないようである. そのため, 関数体側では今後発展する余地が大いにあると思われる. なお, 講演原稿は以下のウェブアドレス上にある.

https://www.cck.dendai.ac.jp/~araik/

## 謝辞

2019 年 9 月に東北大学において第 64 回代数学シンポジウムが行われた. 本稿は, そこでの筆者の講演にもとづいて作成されたものである. 講演の機会を与えてくださった関係者の方々, 特にシンポジウム責任者の金銅誠之氏 (名古屋大学), 数論のプログラム責任者の市野篤史氏 (京都大学), 安福悠氏 (日本大学), および会場責任者の山崎隆雄氏 (東北大学) に感謝したい.

本研究は科研費 (16K17578) の助成を受けたものである.

# 参考文献

[1] K. Arai, *Non-existence of points rational over number fields on Shimura curves*, Acta Arith. **172** (2016), no. 3, 243–250.

[2] 新井 啓介, ディオファントス問題と志村曲線の有理点, 第１０回福岡数論研究集会報告集, 2017 年 1 月, 83–92.

[3] K. Arai, *A survey of rational points on Shimura curves*, Algebraic number theory and related topics 2015, RIMS Kôkyûroku Bessatsu **B72** (2018), 197–207.

[4] K. Arai, S. Kondo, M. Papikian, *Drinfeld-Stuhler modules and the Hasse principle*, preprint (https://arxiv.org/pdf/1908.08678).

[5] H. Cohen, Number theory. Vol. I. Tools and Diophantine equations, Graduate Texts in Mathematics, 239. Springer, New York, 2007.

[6] J. González, S. Molina, *The kernel of Ribet's isogeny for genus three Shimura curves*, J. Math. Soc. Japan **68** (2016), no. 2, 609–635.

[7] B. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92–114.

[8] B. Jordan, R. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. **270** (1985), no. 2, 235–248.

[9] A. Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), no. 3, 277–300.

[10] G. Laumon, M. Rapoport, U. Stuhler, *$\mathscr{D}$-elliptic sheaves and the Langlands correspondence*, Invent. Math. **113** (1993), no. 2, 217–338.

[11] M. Papikian, *Local Diophantine properties of modular curves of $\mathscr{D}$-elliptic sheaves*, J. Reine Angew. Math. **664** (2012), 115–140.

[12] M. Papikian, *Drinfeld-Stuhler modules*, Res. Math. Sci. **5** (2018), no. 4, Paper No. 40, 33 pp.

[13] V. Rotger, C. de Vera-Piquero, *Galois representations over fields of moduli and rational points on Shimura curves*, Canad. J. Math. **66** (2014), no. 5, 1167–1200.

[14] 清水英男, 保型関数 I–III, 第 2 版. 岩波書店基礎数学, 8. 代数, vii. 岩波書店, 東京, 1984.

[15] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.

[16] A. Skorobogatov, Torsors and rational points, Cambridge Tracts in Mathematics, 144, Cambridge University Press, Cambridge, 2001.

[17] M.-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Mathematics, 800, Springer, Berlin, 1980.