Drinfeld-Stuhler 曲線と Hasse 原理の反例の無限族について

東京電機大学・未来科学部　新井 啓介
Keisuke Arai
School of Science and Technology for Future Life,
Tokyo Denki University

概要

Jordan は, 有理数体上の志村曲線の 2 次体上の有理点が存在しないための十分条件を与えた. 筆者はこの結果を, 一般次数の代数体上の有理点に関する結果へと拡張した. 応用として, 志村曲線のレベルを固定して代数体を動かした場合の Hasse 原理の反例の明示的な無限族を得た. さらに最近筆者は, 上記の結果の関数体類似, すなわち, Drinfeld-Stuhler 曲線のレベルを固定して関数体を動かした場合の Hasse 原理の反例の明示的な無限族を得たので, そのことについて本稿で述べる. Hasse 原理の反例の明示的な無限族は, 代数体側では 2 次体および 4 次体について得られている一方, 関数体側では 2 次体について得られている. なお, 今回の関数体側の結果は, 服部新氏, 近藤智氏, Mihran Papikian 氏との共同研究に基づく.

1　ハッセ原理とその反例

K を**大域体**とする. すなわち K は, 有理数体 $\mathbb{Q}$ の有限次拡大体 [**代数体**] か, $\mathbb{F}_p(t)$ (p は素数, $\mathbb{F}_p$ は p 元体, t は不定元) の有限次拡大体 [**関数体**] のいずれかであるとする. n を正の整数とし,

$$f = f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$$

を K 係数の n 変数多項式とする. K' を K の有限次拡大体とする.

方程式 $f = 0$ が K' 上の**ハッセ原理** (あるいは**局所大域原理**) を満たすとは, 次の 2 条件が同値であることを言う.

(1) $f=0$ が K' に解をもつ.

(2) K' の任意の素点 v に対して, $f=0$ が K'_v に解をもつ.

ここで, K'_v は K' の v での完備化である. なお, (1) $\Longrightarrow$ (2) はいつでも成り立つので, $f=0$ が K' 上のハッセ原理を満たすとは「(2) $\Longrightarrow$ (1) が成り立つこと」と言い換えることもできる.

K' 上の**ハッセ原理の反例**とは, K' 上のハッセ原理が成り立たないような方程式のことである. すなわち, $f=0$ は K' に解をもたないが, K' の任意の素点 v に対して K'_v に解をもつようなものである. 直観的な言い方をすれば, 方程式の解の有無に関して, 局所と大域で振る舞いが異なっているようなものである.

上では 1 つの方程式について論じたが, ハッセ原理やその反例は, 連立方程式についても同様に考えることができる.

簡単な例を挙げてみよう.

例 1.1 $K=\mathbb{Q}$ とし, $f=x_1^2+x_2^2+3\in\mathbb{Q}[x_1,x_2]$ を考える. 方程式 $f=0$ は実数体 $\mathbb{R}$ に解をもたない. 従って, $\mathbb{Q}$ にも解をもたない. $\mathbb{R}$ は $\mathbb{Q}$ の無限素点 ∞ による完備化なので, $f=0$ は $\mathbb{Q}$ 上のハッセ原理の反例でないことが分かる. ちなみに, 素数 p に対して, $f=0$ が p 進体 $\mathbb{Q}_p$ に解をもつための必要十分条件は, $p\neq 3$ である (初等的な証明は, [Ara17, 補題 1.1] を参照).

上記の例で見たように, 1 つの素点だけ調べるような安直な方法ではハッセ原理の反例は作れない. ハッセ原理の反例を作ることは, それほど簡単ではないことが想像していただけることと思う.

ハッセ原理の反例の概念を, スキームの有理点の文脈でも述べておこう. X を K 上のスキームとする. X が K' 上のハッセ原理の反例であるとは, $X(K')=\emptyset$, および K' の任意の素点 v に対して $X(K'_v)\neq\emptyset$ となることである. ここで, L を K' または K'_v とすると,

$$X(L)=\mathrm{Hom}_{\mathrm{Spec}\,K}(\mathrm{Spec}\,L,X)$$

である. 特に K が正標数 (関数体) のときは, $\mathrm{Spec}\,K$ 上の射を考えていることに注意する. 有理点の文脈でのハッセ原理については, 例えば [Poo17, Question 2.6.15] を参照.

本稿の目的は, 志村曲線や Drinfeld-Stuhler 曲線を用いてハッセ原理の反例を多く作る方法を紹介することである.

2　志村曲線

本節では, 志村曲線を用いて, 代数体上のハッセ原理の反例の明示的な無限族を構成する.

B を $\mathbb{Q}$ 上の不定符号 4 元数体とする．不定符号というのは, $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$ となることである．4 元数「体」としているので, $B \not\cong \mathrm{M}_2(\mathbb{Q})$ である.

$$\mathbf{Ram}(B) = \{\, p\text{: 素数} \mid B \otimes_{\mathbb{Q}} \mathbb{Q}_p \not\cong \mathrm{M}_2(\mathbb{Q}_p) \,\}$$

とおく．$B \otimes_{\mathbb{Q}} \mathbb{Q}_p \not\cong \mathrm{M}_2(\mathbb{Q}_p)$ のとき, B は p で分岐する (ramify) といい, $\mathbf{Ram}(B)$ という記号はそこからきている．B は不定符号なので $|\mathbf{Ram}(B)|$ は偶数であり, B は 4 元数体なので $\mathbf{Ram}(B) \neq \emptyset$ である．逆に, R を空でない素数の有限集合で $|R|$ が偶数であるようなものとすると, $\mathbf{Ram}(B) = R$ となるような $\mathbb{Q}$ 上の不定符号 4 元数体 B が, 同型を除いて一意に存在する ([Shimi92, 定理 3.5], [Voi21, Main Theorem 14.6.1] を参照).

B の極大整環 $\mathcal{O}_B$ を 1 つとって固定する．$\mathcal{O}_B$ は一意ではないが, 共役を除いて一意である．すなわち, B の任意の極大整環はある $x \in B$ を用いて $x^{-1}(\mathcal{O}_B)x$ と表される ([Shimi92, 定理 3.10] を参照).

S を $\mathbb{Q}$ 上のスキームとする．S 上の ($\mathcal{O}_B$ による) **QM アーベル曲面**とは,

- A: S 上の相対次元 2 のアーベルスキーム,
- $i : \mathcal{O}_B \hookrightarrow \mathrm{End}_S(A)$: 環の単射準同型で $i(1) = \mathrm{id}_A$ を満たすもの

の組 (A, i) のことである．$\mathcal{O}_B$ による QM アーベル曲面の $\mathbb{Q}$ 上の粗モジュライを M^B とする．M^B は $\mathbb{Q}$ 上の固有スムーズ代数曲線であり, **志村曲線**と呼ばれている ([Shimu67, p.58], [Voi21, §43.8] を参照).

志村曲線の有理点に関して, 次の基本的な結果が知られている.

定理 2.1（[Shimu75, Theorem 0]） $M^B(\mathbb{R}) = \emptyset$.

例 2.2　$\mathbf{Ram}(B) = \{\, 2, 3 \,\}$ のとき, M^B の定義方程式 (のアファイン形) は

$$x^2 + y^2 + 3 = 0 \tag{2.1}$$

である ([Kur79, Theorem 1-1 (1)] を参照)．この場合の定理 2.1 の直観的な解釈は, M^B を定義する方程式 (2.1) は体 $\mathbb{R}$ に解をもたない (あるいは実数解をもたない) と

いうことである．$\mathbf{Ram}(B) = \{ 2, 3 \}$ の場合の M^B の有理点と (2.1) の解の関係は, [Ara17, 例 3.2, 補題 5.1] を参照.

注意 2.3　$\mathbb{C}$ は代数閉体なので, $M^B(\mathbb{C}) \neq \emptyset$ である.

M^B の代数体上の有理点の非存在については, 次の定理が知られている．定理の中の $\mathcal{P}(K, \mathfrak{q})$ は, K と $\mathfrak{q}$ から簡単に計算できる素数の有限集合である.

定理 2.4（[Ara16, Theorem 1.1]）　K を偶数次の代数体, q を素数とし, 次の条件 (i)–(iv) を全て満たすとする.

(i) q を割る K の素イデアルがただ 1 つ存在する (それを $\mathfrak{q}$ とおく).
(ii) $\mathfrak{q}$ の剰余体 $\kappa(\mathfrak{q})$ の $\mathbb{F}_q$ 上の次数は奇数.
(iii) $\mathbf{Ram}(B) \not\subseteq \mathcal{P}(K, \mathfrak{q})$.
(iv) $q \neq 2$ のとき $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$,
$q = 2$ のとき $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))$ かつ $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-2}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-2}))$.

このとき, $M^B(K) = \emptyset$ となる.

注意 2.5　(1) 定理 2.4 は, 2 次体 K に対して, [Jor86, Theorem 6.3] ($B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ の場合), [RdV14, Theorem 1.1] ($B \otimes_{\mathbb{Q}} K \not\cong \mathrm{M}_2(K)$ も含めた場合, 弱い仮定付き) により得られている.
(2) 定理 2.4 で K が奇数次の場合は, K が実素点をもつので, 定理 2.1 により $M^B(K) = \emptyset$ である.

M^B の非アルキメデス局所体上の有理点の存在・非存在については, 次の定理が知られている.

定理 2.6（[JL85, Theorems 2.5, 5.1, 5.4, 5.6]）　p を素数とし, L を $\mathbb{Q}_p$ の有限次拡大体とする．$L/\mathbb{Q}_p$ の分岐指数を e, 剰余次数を f とする.

(1) f が偶数とすると, $M^B(L) \neq \emptyset$.
(2) f が奇数とする.
　(i) $p \notin \mathbf{Ram}(B)$ とすると, $M^B(L) = \emptyset$ は次が成り立つことと同値．$s \in \mathbb{Z}$ が $s^2 < 4p^f$ を満たし, $\alpha \in \overline{\mathbb{Q}}$ が $\alpha^2 + s\alpha + p^f = 0$ を満たすとき,

「$B \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha) \not\cong \mathrm{M}_2(\mathbb{Q}(\alpha))$」または「$\dfrac{\alpha}{p} \in \overline{\mathbb{Z}}$ かつ p は $\mathbb{Q}(\alpha)$ で分解」となる．ここで, $\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数閉包, $\overline{\mathbb{Z}}$ は $\mathbb{Z}$ の $\overline{\mathbb{Q}}$ 内での整閉包である．

(ii) $p \in \mathbf{Ram}(B)$ とする．

(a) e が偶数のとき, $M^B(L) \neq \emptyset$ は「$B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-p}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-p}))$」または「$p = 2$ かつ $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))$」と同値.

(b) e が奇数のとき, $M^B(L) \neq \emptyset$ は「$p \equiv 1 \bmod 4$ かつ $\mathbf{Ram}(B) = \{ 2, p \}$」または「$p = 2 \in \mathbf{Ram}(B)$ かつ 2 以外の $\mathbf{Ram}(B)$ の任意の元 q は $q \equiv 3 \bmod 4$ を満たす」と同値.

[Jor86, Theorem 6.3], 定理 2.4, 2.6 を用いると, [Jor86, Example 6.4] を発展させて, 次のような (B を固定して K を動かした場合の) ハッセ原理の反例の明示的な無限族が得られる．

定理 2.7 (1) [Ara18, Proposition 2.6 (1)] $\mathbf{Ram}(B) = \{ 3, 13 \}$ とする． $n \in \mathbb{Z}$ を平方因子をもたない奇数とし, $K = \mathbb{Q}(\sqrt{2n}, \sqrt{-13})$ とする． このとき, $M^B(K) = \emptyset$, および K の任意の素点 v に対して $M^B(K_v) \neq \emptyset$ となる.

(2) [K. Arai and S. Hattori 2024] $\mathbf{Ram}(B) = \{ 3, 13 \}$ とする． $n \in \mathbb{Z}$ は平方因子をもたず, $n > 0$, $n \equiv 1, 10 \bmod 12$, $13 \nmid n$ とし, $K = \mathbb{Q}(\sqrt{-13n})$ とする．このとき, $M^B(K) = \emptyset$, および K の任意の素点 v に対して $M^B(K_v) \neq \emptyset$ となる.

注意 2.8 $\mathbf{Ram}(B) = \{ 3, 13 \}$ のとき, M^B は超楕円曲線 ([Sil86, Exercise 2.14] を参照) となり, その定義方程式のアファイン形は

$$y^2 = -(x^4 + x^3 - x^2 - x + 1)(7x^4 + 23x^3 + 5x^2 - 23x + 7) \tag{2.2}$$

となる ([GM16, Theorem 4.5], [GY17, Table A.1] を参照). 方程式 (2.2) も, 定理 2.7 の K に対して K 上のハッセ原理の反例となる．$\mathbf{Ram}(B) = \{ 3, 13 \}$ の場合の M^B の有理点と (2.2) の解の関係は, [Ara17, 例 3.5 (1)] を参照.

3 Drinfeld-Stuhler 曲線

p を素数とし, $r \in \mathbb{Z}$, $r > 0$, $q = p^r$ とする．表 1 のような, 代数体と関数体の類似が知られている．本節では, 志村曲線の関数体類似である Drinfeld-Stuhler 曲線を用いて, 関数体上のハッセ原理の反例の明示的な無限族を構成する．

表 1　代数体と関数体の類似

代数体側	関数体側
$\mathbb{Q}$	$F=\mathbb{F}_q(t)$
$\mathbb{Z}$	$A=\mathbb{F}_q[t]$
素数 p	既約モニック多項式 $\mathfrak{p}\in A\setminus\mathbb{F}_q$
無限素点 ∞	$\frac{1}{t}\in F$ から定まる付値 ∞
$\mathbb{Q}_p$	F の $\mathfrak{p}$ での完備化 $F_{\mathfrak{p}}$
$\mathbb{Q}_\infty=\mathbb{R}$	$F_\infty=\mathbb{F}_q((\frac{1}{t}))$
有限次拡大体 $K/\mathbb{Q}$	有限次拡大体 K/F
整数環 $\mathcal{O}_K$ $(\subseteq K)$	A の K 内での整閉包 $\mathcal{O}_K$ $(\subseteq K)$
QM アーベル曲面	階数 4 の $\mathscr{D}$-elliptic sheaf
志村曲線 $M^B/\mathbb{Q}$	Drinfeld-Stuhler 曲線 X^D/F

表 1 の「関数体側」の記号を以下で用いる. $d\in\mathbb{Z}$, $d\geq 2$ とし, D を F 上の中心的斜体で $[D:F]=d^2$ を満たすものとする.

$$D\otimes_F F_\infty\cong \mathrm{M}_d(F_\infty)$$

と仮定する. この仮定は, 「B が不定符号」の類似である.

$$\mathbf{Ram}(D)=\{\,\mathfrak{p}\in A\setminus\mathbb{F}_q\text{: 既約モニック多項式}\mid B\otimes_F F_{\mathfrak{p}}\not\cong \mathrm{M}_d(F_{\mathfrak{p}})\,\}$$

とおく. 任意の $\mathfrak{p}\in\mathbf{Ram}(D)$ に対して

$$\mathrm{inv}_{\mathfrak{p}}(D)=\frac{1}{d}\in\mathbb{Q}/\mathbb{Z}$$

と仮定する. この仮定は, [Hau05] の結果を使うためのものである. $X=\mathbb{P}^1_{\mathbb{F}_q}$ とし, D の極大整環と対応する局所自由連接 $\mathcal{O}_X$-代数を, $\mathscr{D}$ で表す (詳細は [LRS93, (1.3)] を参照). S を $\mathbb{F}_q$ 上のスキームとする. S 上の **$\mathscr{D}$-elliptic sheaf** とは, $i\in\mathbb{Z}$ を添字とする

- $\mathscr{E}_i$: $\mathscr{D}$ の作用付きの階数 d^2 の局所自由 $\mathcal{O}_{X\times S}$-加群,
- $j_i:\mathscr{E}_i\hookrightarrow\mathscr{E}_{i+1}$: 単射 $\mathcal{O}_{X\times S}$-線形写像,

- $t_i : {}^{\tau}\mathscr{E}_i \hookrightarrow \mathscr{E}_{i+1}$: 単射 $\mathcal{O}_{X\times S}$-線形写像

の組の列 $(\mathscr{E}_i, j_i, t_i)_{i\in\mathbb{Z}}$ で, j_i, t_i は $\mathscr{D}$ の作用と両立する, などの条件を満たすものである (詳細は [LRS93, (2.2)] を参照). ここで $X \times S$ は $\operatorname{Spec}\mathbb{F}_q$ 上のファイバー積であり, ${}^{\tau}\mathscr{E}_i = (\mathrm{id}_X \times \mathrm{Frob}_S)^*\mathscr{E}_i$ であり, Frob_S は S の q 乗フロベニウス射である. $\mathscr{D}$-elliptic sheaf の F 上の粗モジュライを X^D とする. X^D は F 上の $d-1$ 次元の固有スキームであり, **Drinfeld-Stuhler 多様体**と呼ばれている. $d = 2$ の場合は X^D は F 上の固有スムーズ代数曲線であり, **Drinfeld-Stuhler 曲線**と呼ばれている ([LRS93, Theorem 6.1], [AHKP24, §3.3] を参照).

X^D の関数体上の有理点の非存在について, 次の定理が ($d \geq 2$ に対して) 得られた. 定理の中の $\mathcal{P}(K, \mathfrak{y})$ は, K と $\mathfrak{y}$ から簡単に計算できる $A \setminus \mathbb{F}_q$ の既約モニック多項式の有限集合である.

定理 3.1（[AHKP24, Theorem 8.5]） K を F の d 次拡大体, $\mathfrak{y} \in A \setminus \mathbb{F}_q$ を既約モニック多項式とし, 次の条件 (i)–(v) を全て満たすとする.

(i) $D \otimes_F K \cong \mathrm{M}_d(K)$.
(ii) $\mathfrak{y} \notin \mathbf{Ram}(D)$.
(iii) $\mathfrak{y}$ は K で完全分岐.
(iv) $\mathbf{Ram}(D) \not\subseteq \mathcal{P}(K, \mathfrak{y})$.
(v) 任意の $\mu \in \mathbb{F}_q^{\times}$ に対して, $D \otimes_F F(\sqrt[d]{\mu\mathfrak{y}}) \ncong \mathrm{M}_d(F(\sqrt[d]{\mu\mathfrak{y}}))$.

このとき, $X^D(K) = \emptyset$ となる.

$d = 2$ のとき, X^D の局所体上の有理点の存在・非存在については, 次の 2 つの定理が知られている.

定理 3.2（[Pap12, Theorem 5.10]） $d = 2$ とする.

(1) $X^D(F_\infty) = \emptyset$ となるための必要十分条件は, $\mathbf{Ram}(D)$ が偶数次の元を少なくとも 1 つ含むことである.
(2) L を F_∞ の有限次拡大体とし, $L \neq F_\infty$ とすると, $X^D(L) \neq \emptyset$.

定理 3.3（[Pap12, Theorems 3.1, 4.1]） $d = 2$ とする. $\mathfrak{p} \in A \setminus \mathbb{F}_q$ を既約モニック多項式とし, L を $F_\mathfrak{p}$ の有限次拡大体とする. $L/F_\mathfrak{p}$ の分岐指数を e, 剰余次数を f とする.

(1) f が偶数とすると, $X^D(L) \neq \emptyset$.

(2) f が奇数とする.

　(i) $\mathfrak{p} \notin \mathbf{Ram}(D)$ とすると, $X^D(L) = \emptyset$ は次が成り立つことと同値. $s \in A$, $c \in \mathbb{F}_q^\times$, $\alpha \in \overline{F} \setminus F$ が $\alpha^2 + s\alpha + c\mathfrak{p}^f = 0$ を満たすとき,「$\mathbf{Ram}(D) \cup \{\infty\}$ の少なくとも 1 つの元が $F(\alpha)$ で分解」または「$\dfrac{\alpha}{\mathfrak{p}} \in \overline{A}$ かつ $\mathfrak{p}$ は $F(\alpha)$ で分解」となる. ここで, $\overline{F}$ は F の代数閉包, $\overline{A}$ は A の $\overline{F}$ 内での整閉包である.

　(ii) $\mathfrak{p} \in \mathbf{Ram}(D)$ とする.

　　(a) e が偶数のとき, $X^D(L) = \emptyset$ は「任意の $c \in \mathbb{F}_q^\times$ に対して, $(\mathbf{Ram}(D) \setminus \{\mathfrak{p}\}) \cup \{\infty\}$ の少なくとも 1 つの元が $F(\sqrt{c\mathfrak{p}})$ で分解」と同値.

　　(b) e が奇数のとき, $X^D(L) = \emptyset$.

定理 3.2 は定理 2.1 および注意 2.3 の類似, 定理 3.3 は定理 2.6 の類似である.

定理 3.1, 3.2, 3.3 を用いると, 次のような (D を固定して K を動かした場合の) ハッセ原理の反例の明示的な無限族が得られる.

定理 3.4（[AHKP24, Theorem 9.11]） $d = 2$ とする. $(q, \mathfrak{p}, \mathfrak{q})$ を $(3, t^3 + t^2 + t + 2, t + 1), (3, t^4 + t^3 + 2t + 1, t^2 + 1), (3, t^5 + 2t + 1, t + 2), (5, t^3 + t^2 + 4t + 1, t + 2), (5, t^4 + 2, t^2 + t + 1), (7, t^3 + 2, t + 3)$ のいずれかとする. $\mathfrak{n} \in A \setminus \{0\}$ をモニックで平方因子をもたない元で $t\mathfrak{p}\mathfrak{q}$ と互いに素なものとする. $\varepsilon \in \mathbb{F}_q^\times$ とし, $\mathfrak{n}$ が奇数次のときは ε は $\mathbb{F}_q^\times$ の平方元ではないとする. $K = F(\sqrt{\varepsilon t\mathfrak{p}\mathfrak{q}\mathfrak{n}})$, $\mathbf{Ram}(D) = \{\mathfrak{p}, \mathfrak{q}\}$ とする. このとき, $X^D(K) = \emptyset$, および K の任意の素点 v に対して $X^D(K_v) \neq \emptyset$ となる.

4 証明の概略

本節では, 代数体側の定理 2.4 (あるいは [Jor86, Theorem 6.3]) の証明の概略と, その類似をたどって定理 3.1 を証明するうえでの注意点を述べる.

定理 2.4 の仮定のもとで $M^B(K) \neq \emptyset$ として, 矛盾を導く. 定理 2.1 より, K は実素点をもたない. $M^B(K) \neq \emptyset$ より, 点 $x \in M^B(K)$ がとれる. $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ と仮定すると, x は K 上の QM アーベル曲面 (A, i) と対応する ([Jor86, Theorem 1.1] を参照). $B \otimes_{\mathbb{Q}} K \not\cong \mathrm{M}_2(K)$ のときは, K の 2 次拡大体 K' で $B \otimes_{\mathbb{Q}} K' \cong \mathrm{M}_2(K')$

となるものをとってきて以下と同様の議論をするが, ここでは詳細は略す.

$\mathbf{Ram}(B) \not\subseteq \mathcal{P}(K,\mathfrak{q})$ という仮定により, 素数 $p \in \mathbf{Ram}(B) \setminus \mathcal{P}(K,\mathfrak{q})$ がとれる. $\overline{K}$ を K の代数閉包とし, A の p 等分点のなす群 $A[p](\overline{K})$ を考える. $p \in \mathbf{Ram}(B)$ なので

$$A[p](\overline{K}) \cong \mathcal{O}_B/p\mathcal{O}_B \cong \left\{ \begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} \middle| \, a, b \in \mathbb{F}_{p^2} \right\}$$

となり, これらは $\mathbb{F}_{p^2}$-ベクトル空間の構造をもつ. $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| \, b \in \mathbb{F}_{p^2} \right\} \cong \mathbb{F}_{p^2}$ と対応する $A[p](\overline{K})$ の部分空間は K の絶対ガロワ群 $\mathrm{G}_K = \mathrm{Gal}(\overline{K}/K)$ の作用で安定であり, その作用から指標 (canonical isogeny character)

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

が得られる ([Jor86, Definition 4.5] を参照).

v を K の素点とし, K_v の絶対ガロワ群 $\mathrm{G}_{K_v} \subseteq \mathrm{G}_K$ への ρ の制限 ρ_v を調べる.

(1) v が無限素点の場合, v は複素素点なので $K_v = \mathbb{C}$ となり, ρ_v は自明である.

(2) $v \mid p$ の場合, 合成写像

$$\mathrm{G}_K \xrightarrow{\ \rho\ } \mathbb{F}_{p^2}^{\times} \xrightarrow{N_{\mathbb{F}_{p^2}/\mathbb{F}_p}} \mathbb{F}_p^{\times}$$

が法 p 円分指標になる ([Shimu61, Theorem 2 iv)], [Oht74, Proposition 1.1 (2)] を参照) ことを用いて, ρ_v の大まかな形が分かる. ここに $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ はノルム写像である. 法 p 円分指標になることの証明には, QM アーベル曲面の偏極を用いる.

(3) A は全ての有限素点で potentially good reduction をもつことが分かる ([BBGGLMS79, Exposé III, §6, Proposition] を参照). さらに, good reduction にするための体拡大の様子 (拡大次数など) も分かる ([Jor86, Propositions 3.2, 3.4] を参照). v が有限素点で $v \nmid p$ の場合, 上記のことを用いて ρ_v^{12} が不分岐であることが分かる.

$p \notin \mathcal{P}(K,\mathfrak{q})$ から, $\mathfrak{q} \nmid p$ であることに注意しておく. $\mathfrak{q}$ でのフロベニウス元 $Fr_{\mathfrak{q}} \in \mathrm{G}_K$ を 1 つとり, 12 の倍数 c をうまくとって, (1)–(3) と類体論を用いて $\rho^c(Fr_{\mathfrak{q}})$ を計算する. A は $\mathfrak{q}$ で potentially good reduction をもつので, $K_{\mathfrak{q}}$ のある有限次完全分岐拡大体 L があって, 底変換 A_L は good reduction をもつ. A_L の還元 $\widetilde{A}$ は $\kappa(\mathfrak{q})$ 上の QM アーベル曲面の構造をもち, $p \notin \mathcal{P}(K,\mathfrak{q})$ と $\rho^c(Fr_{\mathfrak{q}})$ の計算結果から, $q \mid \mathrm{Trd}(\pi_{\widetilde{A}})$ が分かる. ここに, $\pi_{\widetilde{A}}$ は $\widetilde{A}/\kappa(\mathfrak{q})$ のフロベニウス自己準同型, Trd

は被約トレースである ([Jor86, p.97] を参照). 自己準同型環 $\mathrm{End}_{\kappa(\mathfrak{q})}(\widetilde{A})$ の分類と拡大次数 $[\kappa(\mathfrak{q}):\mathbb{F}_q]$ が奇数であることを用いると,

$$\begin{cases} B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-q})\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q})) & (q\neq 2\text{ のとき}),\\ B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-1})\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))\text{ または } B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-2})\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-2})) & (q=2\text{ のとき})\end{cases}$$

となり, 定理 2.4 の仮定 (iv) に矛盾する. ゆえに $M^B(K)=\emptyset$ となり, 定理 2.4 の証明が完了する.

関数体側の定理 3.1 を証明する場合は, 定理の仮定のもとで $X^D(K)\neq\emptyset$ として, 矛盾を導く. 点 $x\in X^D(K)$ をとると, $D\otimes_F K\cong \mathrm{M}_d(K)$ により, x は K 上の $\mathscr{D}$-elliptic sheaf と対応する. $\mathfrak{p}\in \mathbf{Ram}(D)\setminus\mathcal{P}(K,\mathfrak{y})$ をとる. 同様のやり方で canonical isogeny character ρ が定義される. v を K の素点とし, ρ の v への制限 ρ_v を調べる. その際の注意点は, 上記の (1)–(3) と比較して, 以下のようになる.

(1') v が無限素点の場合, K_v は代数閉体ではなく, 複雑な絶対ガロワ群をもつので, 真面目に考える必要がある. lemma of the critical index ([BS97, Lemma 3.3.1]) を使い, ある $i\in\mathbb{Z}$ に対して t_i が

$$t_i: {}^{\tau}\mathscr{E}_i \xrightarrow{\cong} \mathscr{E}_i \xrightarrow{j_i} \mathscr{E}_{i+1}$$

と経由することを用いて, ρ_v の振る舞いを制御する. ここで $(\mathscr{E}_i,j_i,t_i)_{i\in\mathbb{Z}}$ は, v の上の素点で還元して得られる有限体上の $\mathscr{D}$-elliptic sheaf である.

(2') $\mathscr{D}$-elliptic sheaf では偏極の議論は使えない. 代わりに t-motive の determinant を計算することで, $v\mid\mathfrak{p}$ の場合の ρ_v の大まかな形を得る.

(3') 関数体上の $\mathscr{D}$-elliptic sheaf は全ての有限素点で potentially good reduction をもち, さらに good reduction にするための体拡大の様子 (拡大次数など) も分かる ([AHKP24, Proposition 4.16]). このことを用いて, v が有限素点で $v\nmid\mathfrak{p}$ の場合に $\rho_v^{q^d-1}$ が不分岐であることが分かる.

あとは同様の議論により, 仮定 (v) への矛盾を導く.

謝辞

2025 年 1 月に京都大学数理解析研究所において研究集会「代数的整数論とその周辺」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プログラム作成委員の三枝洋一氏 (東京大学), 中村健太郎氏 (九州大学), 杉山真吾氏 (金沢大学) に感謝を申し上げます.

本研究は科研費 (16K17578, 21K03187) および東京電機大学総合研究所研究費 (Q20K-01) の助成を受けたものである.

参考文献

[Ara16] K. Arai, *Non-existence of points rational over number fields on Shimura curves*, Acta Arith. **172** (2016), no. 3, 243–250.

[Ara17] 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.

[Ara18] K. Arai, *Rational points on Shimura curves and the Manin obstruction*, Nagoya Math. J. **230** (2018), 144–159.

[AHKP24] K. Arai, S. Hattori, S. Kondo, and M. Papikian, *$\mathscr{D}$-elliptic sheaves and the Hasse principle*, arXiv:2409.19268 [math.NT].

[BS97] A. Blum and U. Stuhler, *Drinfeld modules and elliptic sheaves*, Vector bundles on curves—new directions (Cetraro, 1995), 110–193. Lecture Notes in Math., 1649. Fond. CIME/CIME Found. Subser. Springer-Verlag, Berlin, 1997.

[BBGGLMS79] J.-F. Boutot, L. Breen, P. Gérardin, J. Giraud, J.-P. Labesse, J.S. Milne, and C. Soulé, *Variétés de Shimura et fonctions L*, (French) [Shimura varieties and L-functions], Publ. Math. Univ. Paris VII, 6 [Mathematical Publications of the University of Paris VII], Université de Paris VII, U.E.R. de Mathématiques, Paris, 1979.

[GM16] J. González and S. Molina, *The kernel of Ribet's isogeny for genus three Shimura curves*, J. Math. Soc. Japan **68** (2016), no. 2, 609–635.

[GY17] J.-W. Guo and Y. Yang, *Equations of hyperelliptic Shimura curves*, Compos. Math. **153** (2017), no. 1, 1–40.

[Hau05] T. Hausberger, *Uniformisation des variétés de Laumon-Rapoport-Stuhler et conjecture de Drinfeld-Carayol*, Ann. Inst. Fourier (Grenoble) **55** (2005), no. 4, 1285–1371.

[Jor86] B. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92–114.

[JL85] B. Jordan and R. Livné, *Local Diophantine properties of Shimura* *curves*, Math. Ann. **270** (1985), no. 2, 235–248.

[Kur79] 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.

[LRS93] G. Laumon, M. Rapoport, and U. Stuhler, *$\mathscr{D}$-elliptic sheaves and the Langlands correspondence*, Invent. Math. **113** (1993), no. 2, 217–338.

[Oht74] M. Ohta, *On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), 299–308.

[Pap12] M. Papikian, *Local Diophantine properties of modular curves of $\mathscr{D}$-elliptic sheaves*, J. Reine Angew. Math. **664** (2012), 115–140.

[Poo17] B. Poonen, *Rational Points on Varieties*, Graduate Studies in Mathematics, 186, American Mathematical Society, Providence, RI, 2017.

[RdV14] V. Rotger and C. de Vera-Piquero, *Galois representations over fields of moduli and rational points on Shimura curves*, Canad. J. Math. **66** (2014), 1167–1200.

[Shimi92] 清水 英男, 保型関数, 岩波書店, 1992.

[Shimu61] G. Shimura, *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), 275–331.

[Shimu67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.

[Shimu75] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.

[Sil86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.

[Voi21] J. Voight, *Quaternion algebras*, Grad. Texts in Math., 288, Springer, Cham, [2021].

E-mail address: araik@mail.dendai.ac.jp