平面曲線のガロア点配置と応用

深澤 知（山形大学理学部）

1. はじめに

本稿は静岡大学で開催された第 60 回代数学シンポジウム (2015 年 8 月 31 から 9 月 3 日) において 「平面曲線のガロア点配置と応用」と題して発表した内容をまとめたものである. より詳しくは, ガロア点の個数の上限について, これまで得られた結果について論じている. またガロア点配置の応用のひとつとして, Ballico-Hefez 曲線上の有理点 (=ガロア点) を用いた代数幾何符号についても述べている.

2. ガロア点

K を標数 $p \geq 0$ の代数閉体とし, $C \subset \mathbb{P}^2$ を次数 $d \geq 4$ の既約平面代数曲線とする[1]. 曲線 C の特異点集合を $\mathrm{Sing}(C)$ で表し, 関数体を $K(C)$ で表す. 平面 $\mathbb{P}^2$ 内の 2 点 $P \neq Q$ を通る直線を $\overline{PQ}$ とかく. $P \in \mathbb{P}^2$ を点とする. このとき, 点 P からの射影 (とよばれる有理写像)

$$\pi_P : C \dashrightarrow \mathbb{P}^1;\ Q \mapsto \overline{PQ}$$

を考えることができる. ($\mathbb{P}^2$ 内の 1 点 P を通る直線全体の集合は射影直線 $\mathbb{P}^1$ と一対一対応が付くことに注意.) この射影により, 関数体の拡大

$$K(C)/\pi_P^* K(\mathbb{P}^1)$$

を得る. この拡大は有限次代数拡大である. 吉原久夫氏は次の定義を与えた.

定義 (吉原久夫, 1996 ([5, 22, 29])). 関数体の拡大 $K(C)/\pi_P^* K(\mathbb{P}^1)$ がガロアであるとき, P を C の**ガロア点**という.

点 P がガロア点のとき, G_P でそのガロア群 $\mathrm{Gal}(K(C)/\pi_P^* K(\mathbb{P}^1))$ を表す.

射影の計算方法について簡単に復習しよう. 点 $P \in \mathbb{P}^2$ が 2 枚の一次方程式 $aX + bY + cZ = dX + eY + fZ = 0$ で定義されているとき, 射影は

$$\pi_P(X : Y : Z) = (aX + bY + cZ : dX + eY + fZ)$$

と与えられる. この有理写像は P の定義連立方程式に依存するが, 部分体 $\pi_P^* K(\mathbb{P}^1) \subset K(C)$ は定義連立方程式に依存しないことに注意する. $P = (1 : 0 : 0)$ であれば, $\pi_P = (Y : Z)$ と書ける. C の定義式を $F(X, Y, Z) = 0$ とし, $f(x, y) = F(x, y, 1)$ とする. このとき $Z = 1$ とすれば π_P によって得られる関数体の拡大は $K(x, y)/K(y)$ であり, その関係式は $f(x, y) = 0$ で与えられる.

本研究は, 日本学術振興会科学研究費補助金・若手研究 (B)(25800002) の援助を受けている.

[1] 次数 $d = 3$ のとき, C 上の点からの射影の次数は 2 となるので (分離的なら) どの点から射影してもガロア拡大を与えるため, 本稿の問題は自明となる. $\mathbb{P}^2 \setminus C$ の点からの射影を考えることにはそれでも意味があるが, 混乱をさける. また高次元については [13, 30] を参照.

これらを踏まえると次の例を観察できる.

例 1. 標数 $p \neq 2, 3$ とし, 次の式で定義される曲線 C を考える:

$$X^3Z + Y^4 + Z^4 = 0.$$

このとき, $P_1 = (1:0:0) \in C$, $P_2 = (0:1:0) \in \mathbb{P}^2 \setminus C$ は共にガロア点である. P_1 でのガロア群 G_{P_1} は位数 3 の, P_2 でのガロア群 G_{P_2} は位数 4 の巡回群である.

正標数においては次の例が考えられる.

例 2. 標数 $p \geq 3$ とし, 次の式で定義される曲線 H を考える:

$$X^pZ + XZ^p - Y^{p+1} = 0.$$

このとき, $P_1 = (1:0:0) \in H$, $P_2 = (0:1:0) \in \mathbb{P}^2 \setminus H$ は共にガロア点である. 特に π_{P_1} は Artin-Schreier 拡大を与える.

射影の中心点 P がガロア点でないときは, 次のような記号を準備する (簡単のため「体拡大 $K(C)/\pi_P^*K(\mathbb{P}^1)$ は分離拡大」とする):

- $L_P := K(C)/\pi_P^*K(\mathbb{P}^1)$ のガロア閉包
- $G_P := \mathrm{Gal}(L_P/\pi_P^*K(\mathbb{P}^1))$

吉原氏は代数曲面の非有理次数 (曲線で言えば gonality[2]) を研究していた際, 代数曲線の関数体について「gonality を与える射による体拡大における中間体の存在・非存在」の考察が必要となった (らしい). 特に非特異平面曲線の gonality を与える射が点からの射影として実現されることに着目し, 次のような問題提起をした ([22, 29, 32]):

(1) いつ P がガロア点となるか?
(2) ガロア点の個数はいくつか?
(3) G_P の構造は?
(4) L_P の構造は?
(5) L_P の非特異モデルの構造 (種数など) は?

これがガロア点を定義する動機となった. それらのうち本稿では, (2) の問題に注目する.

問題 1. 平面曲線 $C \subset \mathbb{P}^2$ に対し, ガロア点の個数はいくつか?

これは他の問題が重要でないことを意味しない. 例えば問題 (3) に関して ($p = 0$ のとき)P が一般点であれば G_P は対称群になるが, これは uniform position principle と関係がある ([24]).

次のように記号を準備する.

- $r : \hat{C} \to C$ は C の正規化を表す.
- $g = g(\hat{C})$ で $\hat{C}$ の種数を表す.
- $\hat{C}_0 := \{\hat{Q} \in \hat{C} \mid$ 接空間の射 $d_{\hat{Q}}r$ が単射 $\} \subset \hat{C}$ [3]
- $\hat{\pi}_P$ は点 $P \in \mathbb{P}^2$ からの射影 $\pi_P : C \to \mathbb{P}^1$ と r との合成 $\pi_P \circ r$ とする.
- $T_QC \subset \mathbb{P}^2$ は点 $Q \in C \setminus \mathrm{Sing}(C)$ での (射影) 接線を表す.

[2] $\mathbb{P}^1$ への dominant rational map で最も低い次数のこと. 定義からわかるように「rational からどれだけ離れているか」を測る量.

[3] $\hat{C}_0 = \hat{C}$ のとき, 多様体論で言えば, r は "はめこみ" である.

- $I_Q(C,l)$ は C と直線 $l \subset \mathbb{P}^2$ の点 $Q \in C \cap l$ での交わりの重複度を表す.
- C の一般点 Q について $M(C) = I_Q(C, T_QC)$ なる値 $M(C)$ が定まる.
- $\hat{Q} \in \hat{C}_0$ なら $\exists$ line $h = 0$ (unique) s.t. $\mathrm{ord}_{\hat{Q}} r^*h \geq M(C)$
  このとき $\nu_{\hat{Q}} := \mathrm{ord}_{\hat{Q}} r^*h$
- $\delta(C) := \#\{P \in C \setminus \mathrm{Sing}(C) \mid P \text{ は } C \text{ のガロア点}\}$
- $\delta'(C) := \#\{P \in \mathbb{P}^2 \setminus C \mid P \text{ は } C \text{ のガロア点}\}$

3. ガロア点の分布のあり方

写像 $\hat{\pi}_P : \hat{C} \to \mathbb{P}^1$ の点 $\hat{Q} \in \hat{C}$ での分岐指数を $e_{\hat{Q}}$ で表す. 像について $Q = r(\hat{Q}) \in C \setminus \mathrm{Sing}(C)$ のときは, $e_{\hat{Q}}$ を e_Q とも表す. 分岐について次のことがわかる.

事実 1. $P \in \mathbb{P}^2$, $\hat{Q} \in \hat{C}$, $Q = r(\hat{Q}) \neq P$ とする. 写像 $\hat{\pi}_P$ について次が成立する.

(1) $P \in C \setminus \mathrm{Sing}(C) \Rightarrow e_P = I_P(C, T_PC) - 1$.
(2) h が直線 $\overline{PQ}$ を定義する一次式のとき, $e_{\hat{Q}} = \mathrm{ord}_{\hat{Q}} r^*h$ である. 特に $Q \in C \setminus \mathrm{Sing}(C)$ なら $e_Q = I_Q(C, \overline{PQ})$ である.

このことから, P と異なる点 $Q \in C \setminus \mathrm{Sing}(C)$ について

$$e_Q \geq 2 \Leftrightarrow \overline{PQ} = T_QC$$

となる.

ここで π_P が非分離となるときを注意しておく. このとき, すべての点 $Q \in C \setminus \mathrm{Sing}(C)$ に対して, $e_Q \geq 2$ が満たされる. 即ち, 上で考察したことから,

$$\pi_P \text{ が非分離} \Leftrightarrow \overline{PQ} = T_QC \text{ for } \forall Q \in C \setminus \mathrm{Sing}(C)$$

が成立する[4]. 簡単な考察により, このような点は 1 点しか存在しないことがわかり, しかもどこにあるかすぐに特定できる. 従ってガロア点を探す際, 射影の分離性についてはほとんど気にしなくて良い.

さらに曲線のガロア被覆について次がある.

事実 2 ([25], III. 7.1, 7.2, 8.2)**.** $\theta : C \to C'$ を非特異曲線の間の次数 d のガロア被覆とし, そのガロア群を G とする. このとき, 次が成立する.

(1) $\forall P \in C$, $\forall \sigma \in G$, $\theta(\sigma(P)) = \theta(P)$.
(2) $\theta(P) = \theta(Q) \Rightarrow \exists \sigma \in G$ s.t. $\sigma(P) = Q$.
(3) 任意の点 $P \in C$ に対して, P でのスタビライザー群 $G(P) := \{\sigma \in G \mid \sigma(P) = P\}$ の位数は分岐指数 e_P に等しい.
(4) $\theta(P) = \theta(Q) \Rightarrow e_P = e_Q$.
(5) 分岐指数 e_P は次数 d を割り切る.

点 P がガロア点のときどのような状況になるか, 上の 2 つを使って説明する. 事実 1(2) と 2(4) により

$$Q, R \in C \setminus (\mathrm{Sing}(C) \cup \{P\}),\ \overline{PQ} = \overline{PR} \Rightarrow I_Q(C, \overline{PQ}) = I_R(C, \overline{PR})$$

[4] このような点 P をもつ曲線は strange 曲線と呼ばれている [14, IV, Section 3].

となる. 即ち, $R \in C$ が直線 $\overline{PQ}$ 上にあるとすると, R は Q と同じ重複度で直線 $\overline{PQ}$ と交わらなければならない. π_P が双有理でなければ (Hurwitz の公式より) 分岐点は必ず存在する. よって標語的に,

ガロア点は多重接線や変曲点での接線たちの交点である

と言える[5]. (ここでは, 接点が 2 つ以上ある接線を多重接線, $I_Q(C, T_QC) \geq 3$ なる点 $Q \in C$ を変曲点と呼んだ.)

4. 非特異平面曲線に関する結果

標数 $p = 0$ で C が非特異のときには, 問題 1 は吉原氏, 三浦敬氏により完全に解決されている. (記号 $\sim$ は射影同値を表すものとする.)

定理 1 (吉原, 三浦 [22, 29])**.** $p = 0$, 曲線 $C \subset \mathbb{P}^2$ は非特異とする. このとき:

(I) $\delta(C) = 0, 1$ or 4.
$\delta(C) = 4 \Leftrightarrow C \sim X^3Z + Y^4 + Z^4 = 0$.

(II) $\delta'(C) = 0, 1$ or 3.
$\delta'(C) = 3 \Leftrightarrow C \sim X^d + Y^d + Z^d = 0$.

標数 $p > 0$ では, 本間正明氏による次の結果がある.

定理 2 (本間 [17])**.** $p > 0$, $q \geq 3$ を p 冪とし, H は Hermitian 曲線[6] $X^qZ + XZ^q - Y^{q+1} = 0$ とする. (H は $\mathbb{F}_{q^2}$ で Fermat 曲線 $F(q+1)$ に射影同値である.) このとき, 点 $P \in \mathbb{P}^2$ について

$$P : \text{ガロア点} \ \Leftrightarrow P : \mathbb{F}_{q^2}\text{-有理点}$$

が成立する. 特に, $\delta(H) = q^3 + 1$, $\delta'(H) = q^4 - q^3 + q^2$ である.

本間氏の結果から, 次数を大きくすればいくらでもガロア点の個数は大きくなるので, 吉原-三浦の定理は正標数では成立していないことがわかる. 正標数ではどうしてこのようなことが起きるのか？主に次のことが考えられる.

- ガロア点からの射影がワイルドに分岐する点をもつことがある.
- generic order of contact $M(C)$ が 2 より大きくなることがある.

ワイルドに分岐している点があると分岐点が極端に少なくなることがあり, $M(C) > 2$ だと変曲点の数え上げが変化する. これら 2 つの現象は, 標数零の証明の「ガロア点ひとつに対して変曲点がたくさん必要であり, 変曲点の数え上げから個数を決める」という基本的なアイデア[7]に影響を与える.

例えば上記曲線 H において, ガロア点 $P = (1 : 0 : 0) \in H$ からの射影 π_P を考察すると, 点 P での分岐指数は $e_P = q$ となることが確認できる. また, 任意の点 $Q \in H$ について, 接線との交わりの重複度は $I_Q(H, T_QH) \geq q$ になっていることも確かめられる.

これら 2 つの現象があまりにも上手く機能してしまっている例が Hermitian 曲線だと言える.

残りの状況を著者が決定し, 結果的には次を得た.

---

[5] このような点が必ずしもガロアになるとは限らないが.

[6] 本来は $\mathbb{F}_{q^2}$ 上で考察する際にそのように呼ぶそうである.

[7] 実は, 多項式の条件だけを使う ([13, Key Lemma]), という代数的な別証明がある. しかしながらこちらも, 正標数においてワイルドに分岐する点をもつ可能性があるときにはそのままでは機能しない.

定理 3 (吉原, 三浦, 本間, 深澤 [7])**.** $\delta(C) \geq 2$ または $\delta'(C) \geq 2$ となる非特異平面曲線 $C \subset \mathbb{P}^2$ は次のいずれかに射影同値.

	$\delta(C)$	標数 p	次数 d	曲線
(1)	q^3+1	>0	$q+1$	Hermitian
(2)	$q+1$	2	$q+1$	$\prod_{\alpha\in\mathbb{F}_q}(x+\alpha y+\alpha^2)+cy^{q+1}=0$ $(c\neq 0,1)$
(3)	4	$\neq 2,3$	4	$x^3+y^4+1=0$

	$\delta'(C)$	標数 p	次数 d	曲線
(1)	$q^4-q^3+q^2$	>0	$q+1$	Hermitian
(2)	7	2	4	Klein quartic
(3)	3	≥ 0	$\not\equiv 0 \bmod p$ $\neq q+1$	Fermat
(4)	3	2	4	$(x^2+x)^2+(x^2+x)(y^2+y)$ $+(y^2+y)^2+c=0$ $(c\neq 0,1)$

5. ガロア点を複数もつ例

非特異平面曲線についてはガロア点の配置が完全にわかったので, 特異曲線についても考えたい. この節では $\delta(C)$ に注目する. $\delta(C) \geq 2$ なる特異曲線は 3 例知られている.

例 3 (三浦 [21], Example 1)**.** $p=0$ とし, $C \subset \mathbb{P}^2$ を $x^4-x^3y+y^3=0$ によって (射影閉包として) 定義される射影曲線とする ($g=0$ である). このとき次が成立する.

(1) 点 $(1:1:0)$, $(8:-16:3) \in C \setminus \mathrm{Sing}(C)$ はガロア点である.
(2) $\delta(C)=2$

この例から次のことがわかるため, 簡単なようだがこの例は貴重である.

- ガロア点は変曲点とは限らない.
- ガロア点の群による作用でガロア点を移したとき, その像はガロア点とは限らない[8].

例 4 (深澤-長谷川 [11])**.** $p>0$, $q=p^e \geq 4$ とし, $C \subset \mathbb{P}^2$ が $x-y^q=0$ で定義されているとする. このとき, すべての非特異点がガロア点, つまり, $\delta(C)=\infty$ である.

例 5 (深澤 [8])**.** $p>0$, $q=p^e \geq 3$ とし, 射

$$\varphi : \mathbb{P}^1 \to \mathbb{P}^2;\ (s:t) \mapsto (s^{q+1} : s^q t + s t^q : t^{q+1})$$

の像 $B := \varphi(\mathbb{P}^1)$ を Ballico-Hefez 曲線という[9]. 点 $P \in \mathbb{P}^2$ に対して

$$P : B \text{ のガロア点} \Leftrightarrow P : \mathbb{F}_q\text{-有理点}$$

[8]非特異曲線のときには自己同型が射影変換の制限という事実 [1, Appendix A, 17 and 18], [3] から, この作用でガロア点はガロア点に移る. 逆に言えば今の場合, ガロア点による作用は $\mathbb{P}^2$ の射影変換から来ない. 下の例 5 についても, $p \geq 3$ であれば, ガロア点による作用は $\mathbb{P}^2$ の射影変換から来ない.

[9]本間氏による命名. 由来は, Ballico-Hefez による $M(C)=d-1$ の分類定理 [2] に出てくる 3 タイプのうちのひとつであるため. 文献 [12] で使用. Hoang-島田の論文ではタイトルの一部になっている.

が成立する. 特に, $\delta(C) = q + 1$.

以上をまとめて次の表を得る (2010 年 11 月頃更新)[10].

	$\delta(C)$	標数 p	次数 d	$M(C)$	曲線	ガロア群
(1)	∞	> 0	q	q	$x - y^q = 0$	巡回群
(2)	$q^3 + 1$	> 0	$q + 1$	q	Hermitian	$(\mathbb{Z}/p\mathbb{Z})^{\oplus e}$
(3)	$q + 1$	> 0	$q + 1$	q	Ballico-Hefez	$(\mathbb{Z}/p\mathbb{Z})^{\oplus e}$
(4)	$q + 1$	2	$q + 1$	2	$\prod_{\alpha\in\mathbb{F}_q}(x + \alpha y + \alpha^2) + cy^{q+1} = 0$ $(c \neq 0, 1)$	$(\mathbb{Z}/2\mathbb{Z})^{\oplus e}$
(5)	4	$\neq 2, 3$	4	2	$x^3 + y^4 + 1 = 0$	巡回群
(6)	2	0	4	2	$x^4 - x^3y + y^3 = 0$	巡回群

2015 年 9 月 1 日現在, $\delta(C) \geq 2$ なる例で現在までに知られている (公表されていない) ものはこの 6 タイプに限られる. これらの例は単発的に見つかっているが, どうしてこれらの例でなくてはならないのだろうか?「ガロア点の個数による特徴づけ」を行うことはそのひとつの理論的解釈を与えることになる. 実際に次の結果がある.

定理 4 (深澤-長谷川 [11])**.** $\delta(C) = \infty \Leftrightarrow p > 0$, d は p 冪であり, C は $x - y^d = 0$ で定義される曲線に射影同値である.

この状況を (FH) と名付ける. (FH) でなければガロア点の個数は有限となるので, 次の問題が浮上する.

問題 2. (FH) の状況にないとき, $\delta(C)$ の上限は何か?

6. ガロア点の個数の上限

特異曲線に対する $\delta(C)$ の上限について考察したものとして, 三浦氏の次の結果がある.

定理 5 (三浦 [21], Theorem 1)**.** $p = 0$, $d - 1$ を素数とする.

(1) C が cusp をもつとき, $d \geq 5$ なら $\delta(C) \leq 1$ であり, $d = 4$ なら $\delta(C) \leq 2$ である.

(2) C が cusp をもたないとき,

$$(A(d, g) + 1)\delta_{d-2}(C) + A(d, g)\delta_0(C) \leq 3(2g + d - 2)$$

が成り立つ[11]. ここで

$$A(d, g) = (d - 3)(2g + 2d - 4)/(d - 2)$$

である.

[10]度々「$\delta(C) \geq 1$ かどうか」を考察しないのか, 或はその判定条件はないのか, という質問を受ける. 非特異平面曲線 (または超曲面) については判定条件が存在する [29, Proposition 5], [30, Corollary 6], [13, Key Lemma]. それら判定条件から $\delta(C) \geq 1$ なる例はたくさんあることがわかる. またガロア理論でガロア拡大について出てくる標準的な多項式を用いれば, それら例を作ることは簡単である. 問題は $\delta(C) \geq 2$ とすることである. ひとつガロア点を作るためにガロア理論の標準形を使うと, もう一点を作ることはたいてい困難である.

[11]$\delta_{i-2}(C)$ は $I_P(C, T_PC) = i$ を満たすガロア点 $P \in C \setminus \mathrm{Sing}(C)$ の個数.

ここでの証明の基本方針は非特異曲線のときと同じで,「ガロア点に必要な変曲点の個数の勘定+変曲点の個数の上限」である. 上の $A(d,g)$ は概ねひとつのガロア点に必要な変曲点の数と思っていよい. 尚, 三浦氏の考察している状況で cusp をもたないときは (特に意識する必要はないが), 複数のガロア点に「共通して使われる分岐点はない」ことも上限を決める上で重要である.

ガロア点が存在すればするほど自己同型群の位数が増えることになるので, 自己同型群の位数の上限からガロア点の個数の上限が得られることは容易に想像できる. 次の補題に注意する.

補題 1. P_1, P_2 がガロア点で $P_1 \neq P_2$ であるとき, $G_{P_1} \cap G_{P_2} = \{1\}$ である.

この補題と Hurwitz 上限を用いることにより, 次のような不等式が得られる.

事実 3 (Hurwitz 上限を使った不等式)**.** $p = 0$, $g \geq 2$ のとき次が成立する.

(1) $(d-1) + (\delta(C)-1)(d-2) = \delta(C)(d-2) + 1 \leq 84(g-1) \quad (\leq 42d(d-3))$
(2) $\delta(C) \geq 2 \Rightarrow (d-1)^2 \leq 84(g-1)$

これらの不等式は雑に作ったので, シャープかどうかわからない (恐らくシャープではない). しかしながら標数零においては,「(g/d) の一次式程度で評価されるべき」ことや「(ガロア点が多いと) あまり多くの特異点を持てない」ことがわかる.

$M(C)$ が大きい場合には $\delta(C)$ は決定されている. 後でも使うのでそれを書いておく[12].

定理 6 ([8])**.** 次が成り立つ.

(1) $M(C) = d$ かつ $\delta(C) \geq 1 \Rightarrow$ (FH)
(2) $M(C) = d-1$ かつ $\delta(C) \geq 1 \Rightarrow C$ は Hermitian 曲線または Ballico-Hefez 曲線に射影同値である.

7. 主結果

主結果は次のように「generic order $M(C)$, 種数 g, 次数 d を用いた上限を与え, それに到達する曲線を分類」したものである.

主定理 ([9, 10])**.** C が (FH) の状況にないとき,

$$\delta(C) \leq (M(C)+1)(2g-2) + 3d$$

が成り立つ. さらに, 等式が成り立つための必要十分条件は C が Hermitian 曲線または Ballico-Hefez 曲線に射影同値であることである.

この結果により, (FH) と合わせて, $\delta(C)$ に関する表の上位 3 つまでが特徴づけられたことになる. 証明の道具を次の節で準備するが, そこで現れるように, この上限は「変曲点の個数の上限」と一致する. $M(C) = 2$ のときは上限 $3(2g-2)+3d$ を得る. $p = 0$ のときは $M(C) = 2$ であるが,「g/d の一次式程度が妥当」と書いたように, 理想からは d 倍程度大きい.

ガロア点で特異点であるものの個数を $\delta_s(C)$ と書けば, 次のこともわかる.

[12] $M(C) = d$ のときの本間の分類定理 [16, Theorem 3.4], $M(C) = d-1$ のときの Ballico-Hefez の分類定理 [2] を用いているため, 著者の貢献度は大したことはない.

系. C が (FH) の状況にないとき,

$$\delta(C)+\delta_s(C)\leq (M(C)+1)(2g-2)+3d+\frac{(d-1)(d-2)}{2}-g$$

が成り立つ. 等式が成立するための必要十分条件は上の定理に同じである.

8. 証明の準備

事実 4 (変曲点の数え上げ [26], Theorem 1.5)**.**

$$\sum_{\hat{Q}\in\hat{C}_0}(\nu_{\hat{Q}}-M(C))\leq (M(C)+1)(2g-2)+3d.$$

事実 5 (Plücker formula [23])**.** d^* を双対曲線 C^* の次数, $s(\gamma)$ を双対写像の分離次数, $q(\gamma)$ を非分離次数とする. このとき次が成り立つ.

(1) $s(\gamma)q(\gamma)d^*\leq 2g-2+2d$
(2) $\hat{C}_0=\hat{C}$ (i.e. $r:\hat{C}\to\mathbb{P}^2$: unramified) $\Rightarrow s(\gamma)q(\gamma)d^*=2g-2+2d$

ここで $M(C)\geq 3$ のときには, Hefez-Kleiman の定理 [15, (3.5) Theorem](または [16, Proposition 4.4]) から, $M(C)=q(\gamma)$ となることに注意しておく.

複数のガロア点に対して「分岐点が共有されるか」という問題は変曲点や多重接線の個数を数え上げる際に重要である. 次のことがわかる.

補題 2. $P_1,P_2\in C\setminus \mathrm{Sing}(C)$ がガロア点で $P_1\neq P_2$ のとき, 次が成立する.

(1) $\overline{P_1P_2}\in\mathbb{P}^1$ は π_{P_1}, π_{P_2} の branch point ではない.
(2) $r:\hat{C}\to\mathbb{P}^2$ が unramified $\Rightarrow$ π_{P_1} と π_{P_2} は分岐点を共有しない[13].

9. 証明のアイデア

$M(C)\geq 3$ の場合に説明する.

証明のポイントは「ガロア点が上限の個数あると仮定すると, ガロア点がすべて変曲点になる」ことである[14]. さらにその途中で「正規化 r が (ほとんどの場合) unramified」であることがわかり, $M(C)$, g, d の正確な情報が得られたり, 楫の定理が使える.

$(M(C)+1)(2g-2)+3d\leq\delta(C)<\infty$ を仮定

(1) $M(C)\leq d-1$ (定理 6(1))
(2) $g\geq 1\Rightarrow r:\hat{C}\to\mathbb{P}^2$ が unramified, を示す
(補題 2(1), 特異点からの射影を考察)
(3) ($g=0$ も含めて) ガロア点が変曲点, を示す
(r が unramified で $M(C)\geq 3$ のときは容易)
(4) 変曲点の数え上げ $\Rightarrow\delta(C)=(M(C)+1)(2g-2)+3d$

[13] unramified でないと特異点で分岐を共有するかもしれない. この (2) は主に $M(C)=2$ の場合の証明で使う.

[14] ここで言う「変曲点」は $I_P(C,T_PC)>M(C)$ となる点 P のことだと考えている. 例 3 の後で注意したように, 一般にはガロア点は変曲点ではない.

曲線の決定

(5) (4) $\Rightarrow I_P(C, T_PC) = M(C) + 1$ かつ $M(C) \mid d-1$ (事実 1(1), 事実 2(5))
(6) $g = 0 \Rightarrow M(C) = d-1 \Rightarrow C \sim$ Ballico-Hefez (定理 6(2))
(7) $g \geq 1 \Rightarrow M(C) \mid 2g-2+2d$ (上の (2) と Plücker formula (2)) $\Rightarrow M(C) \mid 2g$
$\Rightarrow g \neq 1$
(8) $g \geq 2 \Rightarrow g(\hat{C^*}) = g$ & $s(\gamma) = 1$ (上の (2) と楫の定理 [18, 20])
(8-1) $M(C) < d-1$ のとき:
$\exists$ 重複度 $(d-1)/M(C)$ 以上の特異点 on C^* (ガロア点 1 個あたり)
C^* について genus formula (Plücker formula (1) も使用):

$$g \leq \frac{1}{2}\left(\frac{2g-2+2d}{M(C)} - 1\right)\left(\frac{2g-2+2d}{M(C)} - 2\right) - ((M(C)+1)(2g-2)+3d) \times \frac{1}{2}\frac{d-1}{M(C)}\left(\frac{d-1}{M(C)} - 1\right)$$

$\Rightarrow$ 矛盾
(8-2) $M(C) = d-1 \Rightarrow C \sim$ Hermitian (Ballico-Hefez 分類定理 [2])

10. Ballico-Hefez 曲線上の有理点を用いた代数幾何符号

代数幾何符号を簡単に復習する.

代数幾何符号の構成法 (H-construction) ([28, 3.1.1])
材料:

- $\mathbb{F}_q$ 上定義された代数多様体 X (通常はいくつか標準的な仮定)
- 直線束 $\mathcal{L}$ (の global sections $\Gamma(X, \mathcal{L})$)
- $\mathbb{F}_q$-有理点 $P_1, \ldots, P_n$

作り方:

$$\Phi : \Gamma(X, \mathcal{L}) \to \bigoplus_{i=1}^{n} \mathcal{L}_{P_i}/m_{P_i}\mathcal{L}_{P_i} \cong \mathbb{F}_q^{\oplus n}$$

像として符号[15] $C_L := \mathrm{Im}\Phi$ が得られる:

- C_L の符号長 $= n$
- Φ: 単射 $\Rightarrow C_L$ の次元 (情報量) $= \dim_{\mathbb{F}_q} \Gamma(X, \mathcal{L})$
- 符号 C_L の最小距離 (誤り訂正幅)

$$d := \min\{u - v \text{ の零でない成分の個数} \mid u, v \in C_L, u \neq v\}$$

長さ n, 次元 k, 最小距離 d である符号を $[n, k, d]_q$ または $[n, k, d]$ と表し, これらをパラメータと呼ぶ. n, k が計算できる場合であっても, d をきちんと求めることはしばしば難しい. 最小距離の半分くらいまでなら「誤りを訂正できる」ため,「与えられた n, k に対して d が大きな符号」をいかにして作るかが符号理論の基本的な問題である.

[15] 抽象的には単に, $\mathbb{F}_q^{\oplus n}$ の線形部分空間.

BH 曲線上の有理点を用いた代数幾何符号

材料:

- 射影平面 $\mathbb{P}^2(\mathbb{F}_q)$
- 直線束 $\mathcal{O}(m)$　$(\Gamma(\mathbb{P}^2(\mathbb{F}_q), \mathcal{O}(m))$ は $\mathbb{F}_q$ 上 m 次斉次式全体)
- BH 曲線上の有理点全体 $B(\mathbb{F}_q)$　　$(p \geq 3)$
  BH 曲線上の特異点全体 $\mathrm{Sing}(B)$　$(p = 2)$

ここでの d の求め方を簡単に説明する.

$$F \in \Gamma(\mathbb{P}^2, \mathcal{O}(m)) \Rightarrow \Phi(F) = (F(P_i))_{i=1}^n$$

であるから,

$$\Phi(F) \text{ の第 } i \text{ 成分がゼロ} \Leftrightarrow F(P_i) = 0$$

である. 即ち,

$$m \text{ 次曲線が } B(\mathbb{F}_q) \text{ を最大で何点通れるか}$$

を考えればよい. Ballico-Hefez 曲線上の有理点と直線の関係からその最大値が計算できる ($m \geq 2$ でも直線に分解できた方が通れる有理点が多くなる).

符号のパラメータを次のように決定した.

定理 7 (深澤-本間-Kim [12])**.** $m = 1$ とする.

(1) $p \geq 3$ のとき構成される符号は

$$\left[\frac{q^2+q+2}{2},\ 3,\ \frac{q^2-1}{2}\right]$$

というパラメータをもつ.

(2) $p = 2$ のとき構成される符号は

$$\left[\frac{q^2-q}{2},\ 3,\ \frac{q^2-2q}{2}\right]$$

というパラメータをもつ.

これらはいずれも Griesmer 限界 $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$ に到達する.

定理 8 (深澤-本間-Kim [12])**.** q を奇数とする.

(1) $q \geq 5$ かつ $m = 2$ のとき構成される符号は

$$\left[\frac{q^2+q+2}{2},\ 6,\ \frac{q^2-q-4}{2}\right]$$

というパラメータをもつ.

(2) $q \geq 7$ かつ $m = 3$ のとき構成される符号は

$$\left[\frac{q^2+q+2}{2},\ 10,\ \frac{q^2-2q-7}{2}\right]$$

というパラメータをもつ.

$m = 2, 3$ のときの符号は現段階では何かしらの上限に到達しているわけではないが, 知られている符号のテーブルと比較してみると,「現在知られている最も良い符号と同じパラメータをもつ」ということがわかる[16].

$\boxed{m = 2, 3 \text{ のときの符号のテーブルとの比較}}$ [http://www.codetables.de]
$d_q(n,k) := \max\{d \mid \exists[n,k,d]_q\text{-code}\}$

$\underline{q \geq 5\text{: odd}, m = 2} \Rightarrow n = \dfrac{q^2+q+2}{2},\ k = 6,\ d = \dfrac{q^2-q-4}{2}$

q	$n = \dfrac{q^2+q+2}{2}$	$k = 6$	$d_q(n,k)$	$\dfrac{q^2-q-4}{2}$
5	16		8	8
7	29		21-19	19
9	46		36-34	34

$\underline{q \geq 7\text{: odd}, m = 3} \Rightarrow n = \dfrac{q^2+q+2}{2},\ k = 10,\ d = \dfrac{q^2-2q-7}{2}$

q	$n = \dfrac{q^2+q+2}{2}$	$k = 10$	$d_q(n,k)$	$\dfrac{q^2-2q-7}{2}$
7	29		17-14	14
9	46		33-28	28

11. 今後の課題

$\delta(C)$ の上限を決める, ということに関しては一応の満足いく結果が得られたのではないかと考えている. $\delta'(C)$ についても同様に次が問題となる ($\delta'(C) = \infty$ については著者の結果 [6] がある).

問題 3. $\delta'(C) < \infty$ のとき, $\delta'(C)$ の上限はいくつか？

標数零においてはもっと強く, 次が肯定的であろう, と予想されている.

問題 4. $p = 0$ のとき, $\delta(C) \leq 4$, $\delta'(C) \leq 3$ は成り立つか？

実際にこれまでの結果で反例になっているものはない. また三浦氏の $\delta(C)$ に関する上限についても $d = 4$ においては “4” を出力する. $p = 0$ の $\delta'(C)$ については次のことが知られている.

[16]講演中にも質問があり回答したが, それらが符号として同じものかどうかは調べていない. しかしながら少なくとも, 具体的な代数幾何符号として実現されている点に意味がある.

- (Duyaguit-三浦 [4]) d が素数で C が非有理的のとき $\delta'(C) \leq 3$.
- (吉原 [31]) 次数 $d \neq 12, 24, 60$ の有理曲線について $\delta'(C) \leq 3$.

次の問題も自然ではあるが例がほとんど知られておらず, 2011 年頃高橋剛氏によって初めて与えられた ([27], 付録のテーブル (8) の例)[17].

問題 5. 群が異なるガロア点を 2 つもつ平面曲線をみつけよ.

ガロア点全般の未解決問題については [33] があるので, そちらをご覧ください.

12. 付録：複数の外ガロア点をもつ平面曲線のテーブル (2013 年 4 月 2 日更新)

	$\delta'(C)$	標数 p	次数 d	曲線	ガロア群
(1)	∞	> 0	p^e	$\sum_{i=0}^{e}(\alpha_i x^{p^i} + \beta_i y^{p^i}) = 0$	$(\mathbb{Z}/p\mathbb{Z})^{\oplus e}$
(2)	$q^4 - q^3 + q^2$	> 0	$q+1$	Hermitian	巡回群
(3)	$q(q+1)/2$	> 0	$q+1$	Ballico-Hefez	巡回群
(4)	$q+1$ or $q-1$	> 0	$2q$	$(x^q - x)^2 + (x^q - x)(y^q - y)$ $+\lambda(y^q - y)^2 + \mu = 0$ $(\lambda \in \mathbb{F}_q,\ (q, \lambda, \mu) \neq (2, 1, 1))$	$(\mathbb{Z}/p\mathbb{Z})^{\oplus e}$ $\rtimes$ $\mathbb{Z}/2\mathbb{Z}$
(5)	7	2	4	Klein quartic	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$
(6)	3	≥ 0	$\not\equiv 0 \bmod p$ $\neq q+1$	Fermat	巡回群
(7)	3	0		$(s^d : (s+1)^d : 1)$	巡回群
(8)	≥ 2	0	$2m$	$x^{2m} + x^m + y^{2m} = 0$	巡回群 二面体群
(9)	≥ 2 $= 2$ (many cases)	> 0	$q\ell$ $p \nmid \ell,\ \ell \geq 3$ $\ell \mid q-1$	$(x^q - x)^\ell + \lambda(y^q - y)^\ell$ $+\mu = 0$	$(\mathbb{Z}/p\mathbb{Z})^{\oplus e}$ $\rtimes$ $\mathbb{Z}/\ell\mathbb{Z}$

テーブルについての注意

- $\delta'(C)$ を考察する際は, $d \geq 3$ を仮定する.
- $\delta'(C)$ の欄が "≥ 2" となっているものは, 2 以上であることは分かるが, 実際には何個あるか明らかにされていない.
- 標数 p が正のとき, q は p の冪であるとする.
- 標数 p の欄が "0" になっているものは, $p = 0$ で明らかにされているものであり, $p > 0$ でもある程度成立することは容易に推察されるが, 正標数での条件をきちんと述べた文献がないものについてはそのような表記にしてある.
- "ガロア群" はガロア点のガロア群として現れるものを意味する.

[17] 2011 年 6 月に開催された佐渡シンポジウムでの高橋氏の講演で公表された. 金沢-吉原 [19] にも $d = 4$ についての考察がある. 例自体は有名かもしれない. 例えば $d = 4$ のときは Hartshorne [14, I. Ex. 5.1] に (射影同値な例が) 載っている.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, Geometry of Algebraic Curves, Vol. I, Grundlehren der Mathematischen Wissenschaften, **267**, Springer-Verlag, New York (1985).

[2] E. Ballico and A. Hefez, Non-reflexive projective curves of low degree, Manuscripta Math. **70** (1991), 385–396.

[3] H. C. Chang, On plane algebraic curves, Chinese J. Math. **6** (1978), 185–189.

[4] C. Duyaguit and K. Miura, On the number of Galois points for plane curves of prime degree, Nihonkai Math. J. **14** (2003), 55–59.

[5] S. Fukasawa, Galois points for a plane curve in arbitrary characteristic, Geom. Dedicata **139** (2009), 211–218.

[6] S. Fukasawa, Classification of plane curves with infinitely many Galois points, J. Math. Soc. Japan **63** (2011), 195–209.

[7] S. Fukasawa, Complete determination of the number of Galois points for a smooth plane curve, Rend. Sem. Mat. Univ. Padova **129** (2013), 93–113.

[8] S. Fukasawa, Galois points for a non-reflexive plane curve of low degree, Finite Fields Appl. **23** (2013), 69–79.

[9] S. Fukasawa, An upper bound for the number of Galois points for a plane curve, in "Topics in Finite Fields," Contemp. Math. **632**, Amer. Math. Soc., Providence, RI, 2015, pp. 111–119.

[10] S. Fukasawa, Bounds for the number of Galois points for plane curves, preprint, arXiv:1404.4413.

[11] S. Fukasawa and T. Hasegawa, Singular plane curves with infinitely many Galois points, J. Algebra **323** (2010), 10–13.

[12] S. Fukasawa, M. Homma and S. J. Kim, Rational curves with many rational points over a finite field, in "Arithmetic, Geometry, Cryptography and Coding Theory," Contemp. Math. **574**, Amer. Math. Soc., Providence, RI, 2012, pp. 37–48.

[13] S. Fukasawa and T. Takahashi, Galois points for a normal hypersurface, Trans. Amer. Math. Soc. **366** (2014), 1639–1658.

[14] R. Hartshorne, Algebraic Geometry, GTM 52, Springer (1977).

[15] A. Hefez and S. Kleiman, Notes on the duality of projective varieties, "Geometry Today," Prog. Math. vol 60, Birkhäuser, Boston, 1985, pp. 143–183.

[16] M. Homma, Funny plane curves in characteristic $p > 0$, Comm. Algebra **15** (1987), 1469–1501.

[17] M. Homma, Galois points for a Hermitian curve, Comm. Algebra **34** (2006), 4503–4511.

[18] H. Kaji, On the Gauss maps of space curves in characteristic p, Compositio Math. **70** (1989), 177–197.

[19] M. Kanazawa and H. Yoshihara, Galois lines for space elliptic curve with $j = 12^3$, preprint, arXiv:1405.0759.

[20] S. L. Kleiman, Multiple tangents of smooth plane curves (after Kaji), "Algebraic geometry: Sundance 1988," Contemp. Math. **116**, Amer. Math. Soc., Providence, RI, 1991, pp. 71–84.

[21] K. Miura, Galois points on singular plane quartic curves, J. Algebra **287** (2005), 283–293.

[22] K. Miura and H. Yoshihara, Field theory for function fields of plane quartic curves, J. Algebra **226** (2000), 283–294.

[23] R. Piene, Numerical characters of a curve in projective n-space, In: Real and Complex Singularities, Oslo 1976, Sijthoff and Noordhoff, Alphen aan den Rijn, 1977, pp. 475–495.

[24] G. P. Pirola and E. Schlesinger, Monodromy of projective curves, J. Algebraic Geom. **14** (2005), 623–642.

[25] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin (1993).

[26] K. O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) **52** (1986), 1–19.

[27] T. Takahashi, Galois point for a plane curve with one or two singular points, in preparation.

[28] M. A. Tsfasman and S. G. Vlăduţ, Algebraic-Geometric Codes, Mathematics and its Applications, **58**, Kluwer Academic Publishers, Dordrecht (1991).
[29] H. Yoshihara, Function field theory of plane curves by dual curves, J. Algebra **239** (2001), 340–355.
[30] H. Yoshihara, Galois points for smooth hypersurfaces, J. Algebra **264** (2003), 520–534.
[31] H. Yoshihara, Galois points for plane rational curves, Far east J. Math. **25** (2007), 273–284; Errata, ibid. **29** (2008), 209–212.
[32] 吉原久夫, 研究紹介, available at
http://mathweb.sc.niigata-u.ac.jp/staffs/Hisao_Yoshihara.pdf
[33] H. Yoshihara and S. Fukasawa, List of problems, available at
http://hyoshihara.web.fc2.com/openquestion.html

E-mail address: s.fukasawa@sci.kj.yamagata-u.ac.jp