Kobe University Repository : Kernel

PDF issue: 2025-07-02

概均質ベクトル空間論の発展（第30回整数論サマースクール報告集、写真なし）

谷口，隆 ； 杉山，和成 ； 石塚，裕大 ； 佐藤，文広 ； 都築，正男 ； Thorne, Frank ； 鈴木，雄太 ； 伊吹山，知義 ； 鈴木，美裕 ； 佐野，薫 ； 山本，修司

(Citation)
第30回整数論サマースクール報告集「概均質ベクトル空間論の発展」:1-421

(Issue Date)
2024-01-31

(Resource Type)
conference proceedings

(Version)
Version of Record

(JaLCDOI)
https://doi.org/10.24546/0100486229

(URL)
https://hdl.handle.net/20.500.14094/0100486229

余正則空間と楕円曲線の Selmer 群

佐野 薫 *

概要

概均質ベクトル空間を一般化した，余正則空間という概念がある．余正則空間の中には，その有理軌道が楕円曲線の Selmer 群の元と自然に対応するものがあることが知られており，Bhargava–Shankar はこの対応を通して数え上げを行うことで，Selmer 群の平均位数に関する結果を得ている．本稿では，この対応についての解説を行う．

目次

1 **はじめに** 2

2 **楕円曲線の基本事項** 3
- 2.1 定義と群演算 3
- 2.2 Mordell–Weil 群のいくつかの予想と定理 5

3 **Galois コホモロジーの翻訳** 7
- 3.1 ひねり 8
- 3.2 トーサー (主等質空間) 9
- 3.3 トーサー因子類ペア 10
- 3.4 n-被覆 11

4 **n-Selmer 群** 13
- 4.1 n-Selmer 群と Tate–Shafarevich 群 13
- 4.2 n-Selmer 群の幾何的な翻訳 15

* 日本電信電話株式会社，NTT コミュニケーション科学基礎研究所，NTT 基礎数学研究センタ

5 余正則空間 15
5.1 種数 1 の曲線の n 次モデル 15
5.2 余正則空間と楕円曲線の Selmer 群 20
5.3 n 次モデルにより定まる滑らかな曲線の種数 21
5.4 Weierstrass モデル 22
5.5 不変式 $c_4, c_6, \Delta \in F[X_n]^{\tilde{\mathcal{G}}_n}$ の存在 24
5.6 幾何不変量 28
5.7 主定理の証明 33

6 曲線の代数幾何の基本事項 35
6.1 曲線，因子 35
6.2 完備線形系 36
6.3 Hilbert 多項式と算術種数 38

1 はじめに

Bhargava–Shankar により執筆された論文のシリーズ [BS13a, BS13b, BS15a, BS15b] において，$2 \leq n \leq 5$ なる n に対し，楕円曲線の n-Selmer 群の平均位数が $\sigma(n)$ に一致することが証明された．その証明は，楕円曲線の n-Selmer 群の元を特定の余正則空間の有理軌道に対応させ，軌道の数え上げを行うものであった．$1 \leq n \leq 4$ のときのこの対応は Bhargava–Shankar 以前から古典的に知られている結果であり，$n = 5$ のときの対応は [Fis] で証明されている．

これらは [AKMMMP01] や [Fis06, Fis08] で簡潔にまとめられている．本稿では $n = 1, 2, 3, 4$ に対し，[Fis06, Fis08] の方法に沿って，n-Selmer 群の元と余正則空間の有理軌道との対応について述べる．

本稿の流れ 2 節では楕円曲線の Mordell–Weil 群の基本的な事実について証明なしに紹介する．3 節では Galois コホモロジーに幾何的な意味づけを行う．4.1 節で n-Selmer 群および Tate–Shafarevich 群を形式的に定義し，4.2 節では 3 節で述べた方法で n-Selmer 群に幾何的な意味づけを行う．ここまでは群作用と独立した，楕円曲線の一般論である．

5.1 節では $n = 1, 2, 3, 4$ に対し，種数 1 の曲線の n 次モデルと，その全体 X_n に作用する群 $\mathcal{G}_n$, $\tilde{\mathcal{G}}_n$ を定義する．5.2 節で余正則空間の定義を行い，$(X_n, \tilde{\mathcal{G}}_n)$ が余正則

空間になることなどのいくつかの性質を定理 5.4 で述べる．定理 5.4 の証明のため，5.4 節で Weierstrass モデルを定義し，不変式環の間の準同型 π_n^* を導く．これらを用いることで $(X_n, \mathcal{G}_n)$ が余正則空間になることが証明できる．この証明は 5.7 節で述べる．余正則空間の軌道と Selmer 群の元との対応を示すためには，ϕ から定まる曲線 C_ϕ に $E_{c_4(\phi),c_6(\phi)}$-トーサーの構造を自然に定める必要があるが，これを定めるために 5.6.2 節で C_ϕ の不変微分形式を明示的に定義する．5.6.1 節で一般に滑らかな種数 1 の曲線の不変微分形式から幾何不変量やトーサーの構造が定まることを見る．5.6.3 節では，群作用による不変微分形式の変化を観察し，π_n^* を通して Weierstrass モデルの場合に帰着することで，不変式と幾何不変量が一致することを証明する．この事実を用いることで，5.7 節で主定理の証明を行う．また，付録的な扱いになるが，6 節では代数幾何的な議論に不慣れな人のために，Riemann–Roch の定理や Hilbert 多項式など基本事項をいくつか述べたので参考にされたい．

本稿を通して，特に断りがなければ K は数体，F は一般の体とする．用語や記号に下線が引かれている場合は，そこでその用語や記号を定義していることを意味している．

2　楕円曲線の基本事項

2.1　定義と群演算

F を体とする．

定義 2.1　F 上定義された種数 1 の滑らかな射影曲線 E と，E の F-有理点 O の組 (E, O) を，F 上の<u>楕円曲線</u>という．

注意 2.2　種数 1 の滑らかな射影曲線だけでは楕円曲線とは呼ばないということに注意．ただし O を省略して単に E で書くことが多い．

定理 2.3　(E, O) を F 上の楕円曲線とすると，F 上で定義された射 $\phi_{\mathcal{L}(3(O))}$ により F は $\mathbb{P}^2$ に埋め込むことができる．またその像の定義方程式は，適宜定数倍の変数変換を行うことで

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

で表せる．

証明 5.1 節を見よ. □

定義 2.4（定義方程式，不変微分形式，幾何不変量） (2.1) の形の方程式，あるいは Z で非斉次化して得られる方程式

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in F) \tag{2.2}$$

を<u>Weierstrass 方程式</u>と呼ぶ．F の標数が $2, 3$ のいずれでもないとき，Weierstrass 方程式 (2.2) の左辺を y に関して平方完成したのち，右辺を x に関して立方完成して変数変換を行うと

$$y^2 = x^3 - 27c_4x - 54c_6 \quad (c_4, c_6 \in F) \tag{2.3}$$

の形の方程式を得る．より具体的な c_4, c_6 の記述については 5.6 節を見よ．

$$\underline{\Delta} = (c_4^3 - c_6^2)/1728$$

とすると，(2.3) で定まる曲線が滑らかなことと $\Delta \neq 0$ であることは同値である．変数変換

$$x = u^2x', \quad y = u^3y' \quad (u \in \overline{F}^\times)$$

により

$$u^4c_4' = c_4, \quad u^6c_6' = c_6, \quad u^{12}\Delta' = \Delta$$

と変換されるが，この変換による任意性を除けば c_4, c_6 は E の F-同型類から一意に定まる不変量である．さらに不変微分形式も固定すると，これらの任意性もなく定まるということを 5.6 節で見る．また

$$\underline{j} = c_4^3/\Delta$$

で定まる不変量 j の値は E の $\overline{F}$ 上の曲線としての同型類と 1 対 1 に対応することが知られている．(2.3) 式で定まる楕円曲線を $\underline{E_{c_4,c_6}}$ で表す．

特に $F = \mathbb{Q}$ のとき，任意の楕円曲線 $E/\mathbb{Q}$ に対し，一意的な $c_4, c_6 \in \mathbb{Z}$ が存在し，任意の素数 p について $p^4 \nmid c_4$ または $p^6 \nmid c_6$ であり，かつ E は E_{c_4,c_6} と $\mathbb{Q}$ 上で同型である．こうした E_{c_4,c_6} のみを考え，この E_{c_4,c_6} の高さ $H(E_{c_4,c_6})$ を

$$H(E_{c_4,c_6}) = \max\left\{|c_4|^3,\ c_6^2\right\}$$

で定めることで，楕円曲線の $\mathbb{Q}$-同型類を並べることができる．

定義 2.5（群構造） (E, O) を (2.2) で定義される F 上の楕円曲線とする．E の 2 つの F-有理点を通る直線は，必ず E ともう一つの F-有理点で交わる．ただしある点で接する場合は重複して交わっているとみなす．E の F-有理点 P, Q について，P, Q を通る直線と E との 3 つ目の交点を R とする．R と O を通る直線と E との 3 つ目の交点を $\underline{P+Q}$ で表す．このようにして定められた演算 $+$ について $E(F)$ は O を単位元とするアーベル群をなす．このアーベル群 $E(F)$ のことを E の<u>Mordell–Weil 群</u>という．同じ点を n 回加える写像を $\underline{[n]}$ で表す．すなわち $[n](P) = P + P + \cdots + P$ である．$\ker([n]\colon E(\overline{F}) \longrightarrow E(\overline{F}))$ のことを $\underline{E[n]}$ で表す．

注意 2.6 ここで定義した演算でアーベル群になることのうち，結合律以外については容易に確認することができる．結合律については式変形を頑張ることでも証明できるが，$E(\overline{F}) \longrightarrow \mathrm{Pic}^0(E); P \mapsto (P) - (O)$ が $E(\overline{F})$ と $\mathrm{Pic}^0(E)$ との全単射を与えることおよび，演算を保ち Galois 作用と可換なことを示すのが標準的である．証明の詳細については [Sil92, III Propotision 3.4] を見よ．

2.2 Mordell–Weil 群のいくつかの予想と定理

この節では楕円曲線の Mordell–Weil 群についてのいくつかの事実を列挙する．K を数体とする．

定義，定理 2.7（Mordell–Weil の定理） E を K 上の楕円曲線とする．このとき Moredell–Weil 群 $E(K)$ は有限生成アーベル群である．したがって有限生成アーベル群の基本定理により

$$E(K) \cong \mathbb{Z}^r \oplus \left(\bigoplus_p \mathbb{Z}/p^{e_p}\mathbb{Z} \right)$$

の形に表せる．この r を E の <u>Mordell–Weil rank</u>，あるいは単に E の<u>階数</u>と呼ぶ．$E(K)$ の有限位数の元の全体を $E(K)$ の<u>ねじれ部分</u>と呼び $\underline{E(K)_{\mathrm{tor}}}$ で表す．

定理 2.7 は次の 2 つのステップに分けて証明される．

Step 1: 完全列

$$0 \longrightarrow E(K)/[n]E(K) \longrightarrow \mathrm{Sel}^{(n)}(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0 \tag{2.4}$$

を与え，$\mathrm{Sel}^{(n)}(E/K)$ が有限群になることを示すことで $E(K)/[n]E(K)$ の有限性

(弱 Mordell–Weil の定理) を証明.

Step 2: 高さ関数と呼ばれる関数を用い，無限降下法により $E(K)$ の有限生成性を証明.

Step 1 の $\mathrm{Sel}^{(n)}(E/K), Ш(E/K)$ 及び完全列については 4 節で詳しく述べる．ねじれ部分については以下が知られている．詳しくは 2021 年の整数論サマースクール「モジュラー曲線と数論」の報告集を見よ.

定理 2.8 E を K 上の楕円曲線とする．このとき以下が成り立つ.

(a) ([Maz77, MG78]) $K = \mathbb{Q}$ のとき

$$E(\mathbb{Q})_{\mathrm{tor}} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & N = 1, 2, \ldots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & 1 \leq N \leq 4. \end{cases}$$

(b) ([KM95]) $[K : \mathbb{Q}] = 2$ のとき

$$E(K)_{\mathrm{tor}} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & N = 1, 2, \ldots 16, 18, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & 1 \leq N \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} & 1 \leq N \leq 2, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

(c) ([Mer98]) 任意の正整数 d について整数 $C(d)$ が存在し，$[K : \mathbb{Q}] \leq d$ のとき

$$\#E(K)_{\mathrm{tor}} \leq C(d)$$

が成り立つ.

階数については，固定した数体 K 上の楕円曲線の階数が有界か否かも未解決であり，$K = \mathbb{Q}$ のとき，Elkies により階数が 28 以上であるような楕円曲線が与えられているものが現在の世界記録である．(階数の世界記録に関しては [Duj] が詳しい．) 具体的な楕円曲線の階数の計算により経験的に以下が予想されている.

予想 2.9 $\mathbb{Q}$ 上の楕円曲線を高さにより並べたとき，階数が 0 のものと 1 のものの割合はちょうど 1/2 ずつである.

注意 2.10 [PPVW19] で導入されたヒューリスティックモデルにおいては，階数 22 以上の $\mathbb{Q}$ 上の楕円曲線の同型類は有限個であろうと帰結されている.

階数が $0, 1$ の楕円曲線の割合に関しては Bhargava–Shankar, Bhargava–Skinner により以下の定理が示された.

定理 2.11（[BS15b], [BS14]） $\mathbb{Q}$ 上の楕円曲線を高さにより並べたとき，階数が $0, 1$ の楕円曲線の割合はいずれも正である.

完全列 (2.4) があるため，$\mathrm{Sel}^{(n)}(E/K)$ の大きさの上界を与えれば $E(K)$ の階数の上界も得られる．これは重要な事実であり，実際，定理 2.11 は以下の定理を用いて証明されている.

定理 2.12（[BS13a, BS13b, BS15a, BS15b]） $\mathbb{Q}$ 上の楕円曲線を高さにより並べたとき，$n = 1, 2, 3, 4, 5$ に対し $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ の平均位数はそれぞれ $1, 3, 4, 7, 6$ である.

定理 2.12を受けて，$\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ の平均位数については以下が予想されている.

予想 2.13 $\mathbb{Q}$ 上の楕円曲線を高さにより並べたとき，任意の正整数 n に対し $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ の平均位数は n の正の約数の総和 $\sigma(n)$ である.

3 Galois コホモロジーの翻訳

本節では通して F を標数 0 の体とし，$\mathrm{Gal}(\overline{F}/F)$ とする．また E を F 上の楕円曲線とする．Galois コホモロジー $H^1(F, E[n])$ が以下のひねりの F-同型類をパラメータ付けすることが知られている．これらは [CFNSS08] で整理されている．このうち 1.，2. について述べるのが本節の目的である.

表 1　Galois コホモロジーの翻訳

		基本対象	ひねり
1.	トーサー因子類ペア	$(E, [n(O)])$	$(C, [D])$
2.	n-被覆	$(E, [n])$	(C, ν)
3.	トーサーの Brauer–Severi 図式	$[E \longrightarrow \mathbb{P}^{n-1}]$	$[C \longrightarrow S]$
4.	$E[n]$-トーサー	$(E[n], +)$	(C, μ)
5.	$E[n]$ の可換 $\mathbb{G}_m$ 拡大	$\mathbb{G}_m \times E[n]$	Λ
6.	テータ群	Θ_E	Θ

本節の内容は 4.1 節で n-Selmer 群の幾何的な意味づけを行う際に用いる．Galois コホモロジーの定義については谷口先生の “本論のための準備”を参考のこと．

本節の流れ　3.1 節においてひねりの定義を復習し，ひねりの F-同型類が Galois コホモロジーでパラメータ付けされる一般的な原理を説明する．この一般的な原理の典型例として 3.2 節では楕円曲線 E のトーサーを導入し，トーサーの F-同型類が $H^1(F,E)$ でパラメータ付けされることを見る．3.3 節ではさらに付加構造を課し，トーサーと次数 n の F-因子類のペアが $H^1(F,E[n])$ でパラメータ付けされることを見る．3.4 節では n-被覆の概念を導入し，n-被覆も $H^1(F,E[n])$ でパラメータ付けされることを見る．さらに，同じ $H^1(F,E[n])$ の元に対応するようなトーサー因子類ペアと n-被覆について，対応を具体的に確認する．いくらかの文献では $H^1(F,E[n])$ と n-被覆との対応が記述されているが，実際に余正則空間の有理軌道との対応付けを見る際には，1. を経由した方が，代数幾何的な構造を与える際に直接的に使えて便利であることに注意しておく．n-被覆との対応は本節で触れるのみで，本稿の以降の節では用いない．

3.1　ひねり

ひねりとは一般に以下の意味である．

定義 3.1　F 上の対象 X に対し，(Y,f) が X のひねりであるとは，F 上の対象 Y と $\overline{F}$-同型射 $f\colon Y \longrightarrow X$ の組のことである．ただし f は省略されることが多い．

X のひねり $(Y_1,f_1),(Y_2,f_2)$ が F-同型であるとは，$f_1 = f_2 \circ \psi$ を満たすような F-同型射 $\psi\colon Y_1 \longrightarrow Y_2$ が存在することとする．また $(Y_1,f_1),(Y_2,f_2)$ が F-同型であることを $(Y_1,f_1) \cong_F (Y_2,f_2)$ で表す．

Galois コホモロジーでひねりをパラメータ付けするときの一般的な原理は以下のとおりである．F 上の対象 X を固定し，基本対象と呼ぶことにする．A を基本対象 X の $\overline{F}$ 上の自己同型群とし，$\mathrm{Gal}(\overline{F}/F)$-作用をもつ群とみなす．このとき X のひねりの F 同型類は $H^1(F,A)$ でパラメータ付けされると期待される．より正確には，$f\colon Y \longrightarrow X$ を $\overline{F}$ 上の同型としたとき，$(\xi_\sigma)_{\sigma\in\mathrm{Gal}(\overline{F/F})} = (\sigma(f)\circ f^{-1})_{\sigma\in\mathrm{Gal}(\overline{F/F})}$ は $\mathrm{Gal}(\overline{F/F})$ の 1-コサイクルを定める．これにより X のひねりの F-同型類全体から Galois コホモロジー $H^1(F,A)$ への単射 φ が得られる．この単射が，我々の所望の

状況では全射でもある．実際，考える圏が準射影多様体の圏のときには Galois 降下により全射性が従う．これは谷口先生の “本論のための準備” の定理 1.14 と数学的には同じことである．証明は [Ser88, Chapter V, Corollary 2-Proposition 12],[Ser02, III§1, Proposition 5], あるいは [Yuk, §8] を参照のこと．

さらに付加構造付きの準射影多様体の圏でひねりを考える場合には，まず基本対象 X の準射影多様体としてのひねり (Y, f) を $\xi \in H^1(F, A)$ から構成し，$\overline{F}$-同型 f を通して X 上の付加構造を Y 上に持ち上げる．この持ち上げにより構成された Y の付加構造は Galois 不変になり，F 上で定義されていること，すなわち X の付加構造付きの準射影多様体としての F 上のひねりであることが示される．したがって φ の全射性が成り立つ．

以降の 3.2 節, 3.3 節, 3.4 節で見る Galois コホモロジーによるパラメータ付けはいずれも，

- 付加構造とその同型の定義
- 基本対象の定義
- 基本対象の $\overline{F}$ 上の自己同型群の計算

をルーチンワークとして行うことで確認される．

3.2 トーサー (主等質空間)

本節では楕円曲線のトーサーを導入し，3.1節の一般的な議論の典型例として，楕円曲線 E/F のトーサーの F-同型類を $H^1(F, E)$ でパラメータ付けする．

定義 3.2（E-トーサー） (i) (F 上の) <u>E-トーサー</u> (C, μ) とは，F 上の滑らかな種数 1 の射影曲線 C 及び，F 上で定義された射 $\mu\colon E \times C \longrightarrow C$ であって $\overline{F}$-有理点に単純推移的な作用を誘導するようなものとの組のこととする．
(2) 2 つの E-トーサー $(C_1, \mu_1), (C_2, \mu_2)$ について，同型 $\psi\colon (C_1, \mu_1) \xrightarrow{\sim} (C_2, \mu_2)$ とは E-作用と可換な曲線の同型のこととする．
(3) $(E, +)$ を E-トーサーの基本対象とする．

補題 3.3 任意の E-トーサーは基本対象 $(E, +)$ のひねりである．

証明 (C, μ) を E-トーサーとする．このとき $P_0 \in C(\overline{F})$ を固定すると $P \mapsto \mu(P, P_0)$

で定義される射は E-トーサーとしての $F(P_0)$-同型 $(E,+) \longrightarrow (C,\mu)$ を与える． □

補題 3.4 $\mathrm{Aut}(E,+) \cong E$.

証明 $(E,+)$ の E-トーサーとしての自己同型は，E の代数曲線としての自己同型であって平行移動写像と可換なものと言い換えられる．またそれは E の平行移動写像に他ならない． □

命題 3.5 E-トーサーを $(E,+)$ のひねりとみなすと，それらは F-同型を除いて $H^1(F,E)$ でパラメータ付けされる．

このように $H^1(F,E)$ を $(E,+)$ のひねりの F-同型類の集合として解釈したものを Weil–Châtelet 群と呼び $\mathrm{WC}(E/F)$ で表す．以降，μ を省略して単に C で E-トーサーを表すことがある．また，E が明らかな場合は省略して単にトーサーと呼ぶことがある．

以下の E-トーサーの自明性についての主張は 4.1 節で n-Selmer 群に幾何的な意味づけを行う際に用いる．

命題 3.6 E-トーサー (C,μ) が $(E,+)$ と F 上で同型であるための必要十分条件は C が F-有理点をもつことである．

証明 E-トーサー (C,μ) が $(E,+)$ と F 上で同型なときに，C が F-有理点を持つことは自明．逆に C が F-有理点 P_0 をもつとき，$P \mapsto \mu(P,P_0)$ は F-同型 $(E,+) \longrightarrow (C,\mu)$ を定める． □

定義 3.7（可解トーサー） 数体 K 上の楕円曲線 E のトーサー C が可解 (soluble) とは $C(K) \neq \emptyset$ であること，すなわち K 上で自明なトーサー $(E,+)$ に同型であることとする．C が局所可解(everywhere locally soluble) とは，任意の付値 $v \in \mathcal{M}_K$ に対して $C(K_v) \neq \emptyset$ であることとする．

3.3 トーサー因子類ペア

定義 3.8（トーサー因子類ペア）(i) n 次のトーサー因子類ペア $(C,[D])$ とは，E-トーサー C と F-有理因子類 $[D]$ の組で $\deg[D] = n$ を満たすもののこととする．

(2) 2 つの n 次トーサー因子類ペア $(C_1,[D_1])$, $(C_2,[D_2])$ について，トーサー因子類

ペアの同型射 $\psi\colon (C_1,[D_1]) \xrightarrow{\sim} (C_2,[D_2])$ とは，E-トーサーの同型 $\psi\colon C_1 \longrightarrow C_2$ であって，$\psi^* D_2 \sim D_1$ を満たすもののこととする．
(3) $(E,[n(O)])$ をトーサー因子類ペアの基本対象とする．

補題 3.9 任意の n 次トーサー因子類ペアは基本対象 $(E,[n(O)])$ のひねりである．

証明 $(C,[D])$ を n 次トーサー因子ペアとする．C を E-トーサーとしての $(E,+)$ のひねりとみなすことで $\overline{F}$-同型 $f\colon C \xrightarrow{\sim} E$ をとる．適宜平行移動と合成したものに取り換えることで $f^*(n(O)) \sim D$ を満たすようにできる． □

補題 3.10 $\mathrm{Aut}(E,[n(O)]) \cong E[n]$.

証明 $(E,+)$ の E-トーサーとしての自己同型はある $P \in E(\overline{F})$ による平行移動写像 τ_P であった．$P \in E[n]$ であることが $\tau_P^*(n(O)) \sim n(O)$ となるための必要十分条件であることが確認できるので，主張が従う． □

命題 3.11 n 次トーサー因子類ペアを $(E,[n(O)])$ のひねりとみなすと，それらは F-同型を除いて $H^1(F,E[n])$ でパラメータ付けされる．

3.4 n-被覆

定義 3.12（被覆）(i) <u>被覆</u> (C,ν) とは, 滑らかな射影曲線 C と非定数射 $\nu\colon C \longrightarrow E$ のこととする．
(ii) 2 つの被覆 (C_1,ν_1), (C_2,ν_2) について，被覆の同型 $\psi\colon (C_1,\nu_1) \xrightarrow{\sim} (C_2,\nu_2)$ とは，曲線としての同型 $\psi\colon C_1 \longrightarrow C_2$ であって $\nu_1 = \nu_2 \circ \psi$ を満たすもののこととする．
(iii) $(E,[n])$ を被覆の基本対象とする．

定義 3.13（n-被覆） 基本対象 $(E,[n])$ の被覆としてのひねりのことを n-被覆と呼ぶ.

注意 3.14 ひねりと言った時点で，固定された $\overline{F}$-同型を省略して表記していることに注意せよ．すなわち (C,ν) が n-被覆であるとは，$\overline{F}$-同型 $f\colon C \longrightarrow E$ と F 上の非定数射 $\nu\colon C \longrightarrow E$ の組であって $\nu = [n] \circ f$ を満たすもののことである．

補題 3.15 $\mathrm{Aut}(E,[n]) \cong E[n]$.

証明 $f \in \mathrm{Aut}(E,[n])$ をとると $[n] = [n] \circ f$ を満たす．したがって $[n] \circ (f - \mathrm{id}) = 0$ を満たす．このことから $f - \mathrm{id}$ が全射でない，すなわち定数射であることが従う．ゆえにある $P \in E(\overline{F})$ を用いて $f = \tau_P$ と表せるが，改めて $[n] = [n] \circ f = [n] \circ \tau_P = \tau_{[n]P} \circ [n]$ 及び $[n]$ の全射性から $P \in E[n]$ であることが従う．逆に $P \in E[n]$ に対して τ_P が $(E,[n])$ の被覆としての自己同型になることは明らかである． □

命題 3.16 n-被覆を $(E,[n])$ のひねりとみなすと，それらは F-同型を除いて $H^1(F,E[n])$ でパラメータ付けされる．

証明 3.1 節で述べた方法で証明されるが，ここでは後のため n-被覆から定まる $H^1(F,E[n])$ の元を具体的に構成しておく．(C,ν) を n-被覆とし，ひねりを定めている $\overline{F}$-同型を $f\colon (C,\nu) \longrightarrow (E,[n])$ とする．ひねりの定義から $[n] \circ f = \nu$ が成り立つ．ここで $\sigma \in \mathrm{Gal}(\overline{F/F})$ に対し

$$\begin{aligned}&[n] \circ (\sigma(f) - f) = \sigma([n] \circ f) - [n] \circ f \\ &= \sigma(\nu) - \nu = \nu - \nu = 0\end{aligned}$$

であるから，$\sigma(f) - f\colon C \longrightarrow E$ は $E[n]$ に値を取る定数射になる．この像を P_σ とすると $(P_\sigma)_\sigma$ は 1-コサイクルであり，$H^1(F,E[n])$ の元が定まる． □

命題 3.17 (i) n 次トーサー因子類ペア $(C,[D])$ に対し $\nu\colon C \longrightarrow \mathrm{Pic}^0(C) \cong E; P \mapsto [n(P) - D]$ は n-被覆となる．
(ii) (C,ν) が n-被覆であるとき，定義から $\overline{F}$-同型 $f\colon C \longrightarrow E$ であって $\nu = [n] \circ f$ をみたすものがある．$(P,Q) \mapsto f^{-1}(P + f(Q))$ で定まる射 $\mu\colon E \times C \longrightarrow C$ は C に E-トーサーの構造を与える．このトーサーの構造により $(C,[f^*(n(O))])$ は n 次トーサー因子類ペアとなる．
(iii) (i), (ii) の対応は $H^1(F,E)$ によるパラメータ付けと可換な対応であり，特に互いに逆の対応である．

証明 (i) $(E,n(O))$ のひねりを定めている $\overline{F}$-同型射 $f\colon (C,[D]) \longrightarrow (E,n(O))$ を考え，$D' = f^*(O)$ とする．このとき $\mathrm{Pic}^0(C) \cong E$ とみなすと $f\colon C \longrightarrow \mathrm{Pic}^0(C)$ は $f(P) = [(P) - D']$ に他ならない．また D' の定め方から明らかに $[n] \circ f = n[(P) - D'] = [n(P) - D] = \nu(P)$ が成り立ち，(C,ν) が n-被覆であることが確認される．

(ii) 主張の内，μ が F 上で定義されることだけがやや非自明なのでこれを示す．まず，命題 3.16 の証明中で述べたように，各 σ に対し $P_\sigma \in E[n]$ があり，$\sigma(f) - f$ は P_σ を値に取る定数射である．任意の $P \in E(\overline{F}), Q \in C(\overline{F})$ に対し $\sigma(\mu(P,Q)) = \mu(\sigma(P), \sigma(Q))$ であることが以下で確認でき，主張が示される．

$$\begin{aligned}\sigma(\mu(P,Q)) &= \sigma(f^{-1}(P + f(Q))) \\ &= \sigma(f^{-1})(\sigma(P) + \sigma(f)(\sigma(Q))) \\ &= f^{-1}(-P_\sigma + \sigma(P) + (f(\sigma(Q)) + P_\sigma)) \\ &= \mu(\sigma(P), \sigma(Q)).\end{aligned}$$

(iii) 確認せよ．

□

補題 3.18 $\mathrm{Aut}(E \longrightarrow \mathbb{P}^{n-1}, \omega_E) \cong E[n]$

証明 E の自己同型 α であって $\alpha^*\omega_E = \omega_E$ となるものは E の平行移動に他ならない．したがって $\alpha = \tau_P (P \in E(\overline{K}))$ と書ける．さらに $\phi_{\mathcal{L}(n(O))} \colon E \longrightarrow \mathbb{P}^{n-1}$ と可換であることから $\tau_P^*(n(O)) = n(O)$ であり，$P \in E[n]$ とわかる．逆に $P \in E[n]$ に対して τ_P^* が $(E \longrightarrow \mathbb{P}^{n-1}, \omega_E)$ の自己同型を定めることは直ちにわかる． □

命題 3.19 $(E \longrightarrow \mathbb{P}^{n-1}, \omega_E)$ のひねりは，F-同型を除いて $H^1(F, E[n])$ でパラメータ付けされる．

4 n-Selmer 群

4.1節で n-Selmer 群 $\mathrm{Sel}^{(n)}(E/K)$ 及び Tate–Shafarevich 群 $Ш(E/K)$ の定義を形式的に行い，完全列 (2.4) があることを見る．また，3 節で紹介した Galois コホモロジーの翻訳を用いて，4.2節で $\mathrm{Sel}^{(n)}(E/K)$ および $E(K)/[n]E(K)$ に幾何的な意味づけを行う．

4.1 n-Selmer 群と Tate–Shafarevich 群

定義 4.1 (n-Selmer 群) F を体, , E を F 上の楕円曲線とする．このとき $\mathrm{Gal}\,\overline{F}/F$-加群としての完全列

$$0 \longrightarrow E[n] \longrightarrow E \longrightarrow E \longrightarrow 0$$

に対して長完全列を考えると

$$\begin{tikzcd}
0 \arrow[r] & E[n](F) \arrow[r] & E(F) \arrow[r, "{[n]}"] & E(F) \arrow[dll, "\delta"'] \\
& H^1(F, E[n]) \arrow[r] & H^1(F, E) \arrow[r, "{[n]}"] & H^1(F, E) \arrow[dll] \\
& \cdots &&
\end{tikzcd}$$

を得るので，この一部を取り出して

$$0 \longrightarrow E(F)/[n]E(F) \longrightarrow H^1(F, E[n]) \xrightarrow{\iota} H^1(F, E)[n] \longrightarrow 0 \qquad (4.1)$$

を得る．完全列 (4.1) は任意の体 F 上で考えられるので，F が数体 K のときの楕円曲線 E/K 及び，K を各素点 v での完備化 K_v に拡大した場合に考えることで，可換図式

$$\begin{tikzcd}
0 \arrow[r] & E(K)/[n]E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[n]) \arrow[r, "\iota"] \arrow[d] \arrow[dr, "①"] & H^1(K, E)[n] \arrow[r] \arrow[d, "②"] & 0 \\
0 \arrow[r] & \prod_{v \in \mathcal{M}_K} E(K_v)/[n]E(K_v) \arrow[r] & \prod_{v \in \mathcal{M}_K} H^1(K_v, E[n]) \arrow[r, "\iota"] & \prod_{v \in \mathcal{M}_K} H^1(K_v, E)[n] \arrow[r] & 0
\end{tikzcd}$$

を得る．この図式中の準同型を用いて $\mathrm{Sel}^{(n)}(E/K)$ 及び $Ш(E/K)$ を

$$\underline{\mathrm{Sel}^{(n)}(E/K)} = \ker\left(①\colon H^1(K, E[n]) \longrightarrow \prod_{v \in \mathcal{M}_K} H^1(K_v, E)[n]\right)$$

$$\underline{Ш(E/K)} = \ker\left(②\colon H^1(K, E) \longrightarrow \prod_{v \in \mathcal{M}_K} H^1(K_v, E)\right)$$

により定める．

定義から直ちに次の命題が成り立つ．

命題 4.2　数体 K 上の楕円曲線 E に対して完全列 (2.4)

$$0 \longrightarrow E(K)/[n]E(K) \longrightarrow \mathrm{Sel}^{(n)}(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0$$

がある．

4.2 n-Selmer 群の幾何的な翻訳

K を数体，E を K 上の楕円曲線とする．まず $H^1(K,E)$ と $H^1(K,E[n])$ の元はそれぞれ，E/K のトーサーの K-同型類の集合および，n 次トーサー因子類ペアの K-同型類の集合とみなせるのであった．

完全列 (4.1) 中の射 $\iota\colon H^1(K,E[n]) \xrightarrow{\iota} H^1(K,E)$ の構成を思い出すと，n 次トーサー因子類ペア $(C,[D])$ に対し C を対応させる写像になっている．δ により $E(K)/[n]E(K)$ を $H^1(K,E[n])$ の部分集合とみなすと，命題 3.6，定義 3.7より

$$E(K)/[n]E(K) = \ker\iota = \left\{ (C,[D]) \;\middle|\; \begin{array}{c} n \text{ 次トーサー因子類ペア} \\ C \text{ は可解 } E\text{-トーサー} \end{array} \right\} / \cong_K$$

とみなせる．また同様に命題 3.6，定義 3.7 より，

$$\mathrm{Sel}^{(n)}(E/K) = \left\{ (C,[D]) \;\middle|\; \begin{array}{c} n \text{ 次トーサー因子類ペア} \\ C \text{ は局所可解な } E\text{-トーサー)} \end{array} \right\} / \cong_K$$
$$Ш(E/K) = \{C \mid \text{局所可解な } E\text{-トーサー }\} / \cong_K$$

とみなせる．

5 余正則空間

5.1 節で種数 1 の曲線の n 次モデルとその全体 X_n 及び，X_n に作用する代数群 $\mathcal{G}_n, \tilde{\mathcal{G}}_n$ を定義する．5.2 節で余正則空間を定義する．$(X_n, \tilde{\mathcal{G}}_n)$ が余正則空間になることなど，いくつかの性質を定理 5.4 で述べる．5.4 節で Weierstrass モデルの定義をする．Weierstrass モデルを中心的に扱うことで，5.7 節で定理 5.4 の証明を得る．

楕円曲線 $E_{\mathcal{C}_4,\mathcal{C}_6}$ に対し，$\mathrm{Sel}^{(n)}(E_{\mathcal{C}_4,\mathcal{C}_6}/K)$ の元と，不変量 $\mathcal{C}_4, \mathcal{C}_6$ を持ち局所可解なモデルの $\tilde{\mathcal{G}}_n(K)$-軌道との対応（定理 5.25） を同じく 5.7 節で見る．

5.1 種数 1 の曲線の n 次モデル

K を数体とする．4.2 節で見たように，楕円曲線 E/K の n-Selmer 群の各元は n 次トーサー因子類ペア $(C,[D])$ であって C が局所可解なものに対応するのであった．本節では，局所可解なトーサー因子類ペア $(C,[D])$ に対して，$\mathcal{L}(mD)$ $(m = 1,2,3,\ldots)$ を考えることで C の射影空間への良い埋め込みを見つけ，さらにこうし

た埋め込みの任意性が代数群の作用で記述できることを見る．これらの観察を通して，種数 1 の曲線の n 次モデルを定義する．種数 1 の曲線の n 次モデルがまさに余正則空間の元を定める．ここで，K 上の埋め込みを構成するためには次の事実が重要である．

定理 5.1（[Cas62, Lemma 7.1]） (C,μ) を局所可解な E-トーサーとし，$[D]$ を C の K-有理因子類とする．このとき $[D]$ を代表する K-有理因子 D' が存在する．

以下，一般に F を体，E/F を楕円曲線，$(C,[D])$ を E の n 次トーサー因子類ペアとし，D は F-有理因子とする．まず楕円曲線の定義から E の種数は 1 であり，$\overline{F}$ 上では C と E は同型なので C の種数も 1 である．定理 6.3 (v) より $m=1,2,3,\ldots$ に対して

$$\ell(mD)=\deg mD=mn$$

である．また D が F-有理因子であるので，定理 6.3 (viii) より $\mathcal{L}(D)$ には $F(C)$ の元からなる基底が存在する．以下ではこれらの事実を断りなく用いる．

以下，$n=1,2,3,4$ それぞれの場合に埋め込みの構成をし，構成された埋め込みを表すデータを動機づけとして n 次モデルを定義する．n 次モデル全体を$\underline{X_n}$で表す．また埋め込みのデータの任意性を見たのち，X_n に作用する群 $\underline{\mathcal{G}_n}$ を定義する．$\mathcal{G}_n$ の交換子群を $\underline{\tilde{\mathcal{G}}_n}$ とする．

$\underline{n=1}$

(埋め込みの構成) $\ell(D)=1\neq 0$ なので $f\in F(C)$ があり $\operatorname{div} f+D\geq 0$ である．これを改めて D とすることで以下では $D\geq 0$ とする．$\deg D=1$，$D\geq 0$，かつ D は F-有理因子なので，ある $O\in C(F)$ があり $D=(O)$ と表せる．したがってこの場合は (C,O) は楕円曲線である．

$\mathcal{L}(D)\supset\overline{F}$ と $\ell(D)=1$ より $\mathcal{L}$ は定数関数 $1\in F(C)$ を基底にもつ．1 は $\mathcal{L}(2D)$ の元でもある．$\ell(2D)=2$ なので 1 と $\overline{F}$ 上一次独立な元 $x\in F(C)$ が存在する．$1,x$ は $\mathcal{L}(3D)$ の元でもある．$\ell(3D)=3$ なのでこれらと $\overline{F}$ 上一次独立な $y\in F(C)$ が存在する．$\mathcal{L}(6D)$ には $1,x,y$ を用いて表される $1,\ x,\ y,\ x^2,\ xy,\ y^3,\ x^3$ という 7 つの元があるが，$\ell(6D)=6$ なのでこれらは一次従属である．したがって $(A_1,A_2,\ldots,A_7)\in F^7\setminus\{(0,0,\ldots,0)\}$ が存在し，

$$A_1+A_2x+A_3y+A_4x^2+A_5xy+A_6y^2+A_7x^3=0$$

を満たす．もし A_6 または A_7 が 0 であれば，すべての項が O を極としてもち，かつその位数が異なるので，左辺は関数として 0 になり得ない．したがって A_6,A_7 はいずれも 0 でない．両辺を $A_6^3A_7^4$ で割り，x, y をそれぞれ $-A_6A_7x, A_6A_7^2y$ で置き換えることで，Weierstrass 方程式 (2.2)

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

を得る．定理 6.3 (vii) より, $1, x, y$ で定まる $C \hookrightarrow \mathbb{P}^2$ は埋め込みであり．(2.2) は C の像の定義方程式である．したがって C を表すデータとして，係数 $(a_1, a_2, a_3, a_4, a_6) \in F^5$ が得られた.

(モデル)　F^5 の元のことを種数 1 の曲線の 1 次モデルという．1 次モデル $\phi = (a_1, a_2, a_3, a_4, a_6)$ に対し，(2.2) で定まる曲線を C_ϕ で表す.

(データの任意性)　Weierstrass 方程式 (2.2) を保つような基底の取り換えは $u \in F^\times$, $r, s, t \in F$ を用いて

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

の形の変数変換を (2.2) に施したのちに u^6 で両辺を割ることで得られる.

(作用する群)　上記の方法で得られる変換 $[u; r, s, t]$ 全体のなす群のことを $\mathcal{G}_1$ で表す．このとき交換子群は

$$\tilde{\mathcal{G}}_1 = \{[1; r, s, t] \in \mathcal{G}_1\}$$

となる．$\mathcal{G}_1, \tilde{\mathcal{G}}_1$ は X_1 に作用する.

<u>$n = 2$</u>

(埋め込みの構成)　$\mathcal{L}(D)$ の基底を $x, z \in F(C)$ とする．$\mathcal{L}(2D)$ には一次独立な 3 つの元 x^2, xz, z^2 がある．$\ell(2D) = 4$ なのでこれらと一次独立な $y \in F(C)$ が存在する．$\mathcal{L}(4D)$ には x^4, x^3z, x^2z^2, xz^3, z^4, x^2y, xzy, z^2y, y^2 の 9 個の元がある．$\ell(4D) = 8$ なのでこれらは一次従属である．したがって $(\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e) \in F^8 \setminus \{(0, 0, \ldots, 0)\}$ が存在し，

$$y^2 + (\alpha_0x^2 + \alpha_1xz + \alpha_2z^2)y = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 \tag{5.1}$$

をみたす．ここで定理 6.3 (vii) より，x, y, z で定まる $C \hookrightarrow \mathbb{P}(1, 2, 1)$ は埋め込みであり，(5.1) は C の像の定義方程式である．ただしここで，(5.1) の y^2 の係数が 0 であれば C が滑らかであることに矛盾するので，予めその係数で割ることで y^2 の係数を

1 にしていることに注意せよ．以上より，C を表すデータとして，2 次および 4 次の 2 元斉次式の組

$$p(x,z) = \alpha_0 x^2 + \alpha_1 xz + \alpha_2 z^2$$
$$q(x,z) = ax^4 + bx^3 z + cx^2 z^2 + dxz^3 + ez^4$$

が得られ，C の定義方程式は

$$y^2 + p(x,z)y = q(x,z) \tag{5.2}$$

で与えられる．

(モデル) 2 次および 4 次の 2 元斉次式のペアのことを種数 1 の曲線の 2 次モデルという．2 次モデル $\phi = (p,q)$ に対し，(5.2) で定まる曲線を C_ϕ で表す．

(データの任意性) 上記で得たデータ p, q は，x, z 及び y の取り方と線形関係式の取り方に依存している．これらの任意性はすべて，$B \in \mathrm{GL}_2(F)$, $\mu \in F^\times$, $r_0, r_1, r_2 \in F$ を用いた変数変換

$$(x,z) = (x',z')B$$
$$y = \mu^{-1}y' + r_0 x'^2 + r_1 x'z' + r_2 z'^2$$

を (5.2) に施したのちに両辺を μ^2 倍することで得られる．

(作用する群) 上記の方法で得られる変換 $[\mu; r, B]$ 全体のなす群のことを $\mathcal{G}_2$ で表す．このとき交換子群は

$$\tilde{\mathcal{G}}_2 = \{[1; r, B] \in \mathcal{G}_2 \mid B \in \mathrm{SL}_2(F)\}$$

となる．$\mathcal{G}_2, \tilde{\mathcal{G}}_2$ は X_2 に作用する．

<u>$n = 3$</u>

(埋め込みの構成) $\mathcal{L}(D)$ の基底を $x, y, z \in F(C)$ とすると $\mathcal{L}(3D)$ には x^3, y^3, z^3, x^2y, x^2z, y^2x, y^2z, z^2x, z^2y, xyz の 10 個の元がある．$\ell(3D) = 9$ なのでこれらは一次従属である．したがって 3 元 3 次斉次式 $T(x,y,z)$ があり，

$$T(x,y,z) = 0 \tag{5.3}$$

となる．ここで定理 6.3 (vii) より，x, y, z で定まる $C \hookrightarrow \mathbb{P}^2$ は埋め込みであり．$T = 0$ は C の像の定義方程式である．以上より，C を表すデータとして，3 元 3 次斉次式 T が得られた．

(モデル) 3 元 3 次斉次式のことを種数の 3 次モデルという．3 次モデル $\phi = (T)$ に対し，(5.3) で定まる曲線を C_ϕ で表す．
(データの任意性) 上記で得たデータ f は，x, y, z の取り方と線形関係式の取り方に依存している．これらの任意性はすべて，$B \in \mathrm{GL}_2(F)$ を用いた変数変換

$$(x, y, z) = (x', y', z')B$$

を (5.3) に施したのちに両辺に $\mu \in F^\times$ を掛けることで得られる．
(作用する群) 上記の方法で得られる変換 $[\mu; B]$ 全体のなす群 $\mathbb{G}_m \times \mathrm{GL}_3$ のことを $\mathcal{G}_3$ で表す．このとき交換子群は

$$\tilde{\mathcal{G}}_3 = \mathrm{SL}_3$$

となる．$\mathcal{G}_3, \tilde{\mathcal{G}}_3$ は X_3 に作用する．
<u>$n = 4$</u>
(埋め込みの構成) $\mathcal{L}(D)$ の基底を x_1, x_2, x_3, $x_4 \in F(C)$ とすると $\mathcal{L}(2D)$ には x_1^2, x_2^2, x_3^2, x_4^2, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4 の 10 個の元がある．$\ell(2D) = 8$ なので線形写像

$$\begin{aligned} \overline{F}^{10} &\longrightarrow \mathcal{L}(2D) \\ (a_1, a_2, \ldots, a_{10}) &\mapsto a_1x_1^2 + a_2x_2^2 + \cdots a_{10}x_3x_4 \end{aligned}$$

の核は 2 次元である．またこの写像は F 係数行列で表現できるので，核は F 係数のベクトルからなる基底をもつ．したがって F 係数 4 元 2 次式の組 ${}^t(q_1, q_2)$ があり，

$$\begin{pmatrix} q_1(x_1, x_2, x_3, x_4) \\ q_2(x_1, x_2, x_3, x_4) \end{pmatrix} = 0 \tag{5.4}$$

となる．ここで定理 6.3 (vii) より，x_1, x_2, x_3, x_4 で定まる射 $C \hookrightarrow \mathbb{P}^3$ は埋め込みであり．(5.4) は C の像の定義方程式である．以上より，C を表すデータとして，2 元 2 次式の組 ${}^t(q_1, q_2)$ が得られた．
(モデル) 2 元 2 次式の組 ${}^t(q_1, q_2)$ のことを種数 1 のの 4 次モデルという．4 次モデル $\phi = {}^t(q_1, q_2)$ に対し，(5.4) で定まる曲線を C_ϕ で表す．
(データの任意性) 上記で得たデータ q_1, q_2 は，x_1, x_2, x_3, x_4 の取り方と線形関係式の取り方に依存している．従ってこれらの任意性は全て $B \in \mathrm{GL}_4(F)$ を用いた変数変換

$$(x_1, x_2, x_3, x_4) = (x_1', x_2', x_3', x_4')B$$

を (5.4) に施したのちに両辺に $A \in \mathrm{GL}_2(F)$ を掛けることで得られる．

(作用する群)　上記の方法で得られる変換 $[A, B]$ 全体のなす群 $\mathrm{GL}_2 \times \mathrm{GL}_4$ のことを $\mathcal{G}_4$ で表す．このとき交換子群は

$$\tilde{\mathcal{G}}_4 = \mathrm{SL}_2 \times \mathrm{SL}_4$$

となる．$\mathcal{G}_4, \tilde{\mathcal{G}}_4$ は X_4 に作用する．

5.2　余正則空間と楕円曲線の Selmer 群

定義 5.2　F-ベクトル空間 V および V に作用する F 上の代数群 G について，$F[V]^G$ が環として多項式環に同型であるとき，(V, G) は余正則空間であるという．

定義 5.3　$n = 1, 2, 3, 4$ について X_n はそれぞれ次元が $N = 5, 8, 10, 20$ のアフィン空間であるので，その座標環 $F[X_n]$ は N 変数多項式環である．$n = 3, 4$ に対し，$F[X_n]$ を通常の次数により次数付けを行う．$n = 1, 2$ に対し，

$$\begin{aligned} F[X_1] &= F[a_1, a_2, a_3, a_4, a_6] \\ F[X_2] &= F[\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e] \end{aligned}$$

で表したとき $\deg a_i = i$, $\deg \alpha_i = 1$, および $\deg a = \deg b = \ldots = \deg e = 2$ により次数付けを行う．不変式環 $F[X_n]^{\tilde{\mathcal{G}}_n}$ を

$$F[X_n]^{\tilde{\mathcal{G}}_n} = \{f \in F[X_n] \mid \text{すべての } g \in \tilde{\mathcal{G}}_n(\overline{F}) \text{ に対し } f \circ g = f\}$$

で定める．また有理指標 $\det\colon \mathcal{G}_n \longrightarrow \mathbb{G}_m$ を

$$\begin{array}{lll} n = 1 & [u; r, s, t] & \mapsto u^{-1} \\ n = 2 & [\mu, r, B] & \mapsto \mu \det B \\ n = 3 & [\mu, B] & \mapsto \mu \det B \\ n = 4 & [A, B] & \mapsto \det A \det B \end{array}$$

で定める．

重さ k の不変式の空間 $F[X_n]_k^{\tilde{\mathcal{G}}_n}$ を

$$F[X_n]_k^{\tilde{\mathcal{G}}_n} = \{f \in F[X_n] \mid \text{すべての } g \in \mathcal{G}_n(\overline{K}) \text{ に対し } f \circ g = (\det g)^k f\}$$

で定める．重さにより $F[X_n]^{\tilde{\mathcal{G}}_n}$ に次数付き環の構造が定まる．

定理 5.4　$n = 1, 2, 3, 4$ とする．それぞれ重さ $4, 6, 12$ の不変式 $c_4, c_6, \Delta \in F[X_n]^{\tilde{\mathcal{G}}_n}$ が存在し，$c_4^3 - c_6^2 = 1728\Delta$ および次を満たす．

(i) F の標数が $2,3$ でないとき，$F[X_n]^{\tilde{\mathcal{G}}_n} = F[c_4, c_6]$．すなわち $(X_n, \tilde{\mathcal{G}}_n)$ は余正則空間である．

(ii) $\phi \in X_n$ について，C_ϕ が滑らかな種数 1 の曲線であることと $\Delta(\phi) \neq 0$ は同値．

(iii) F の標数が $2,3$ でないとする．$\phi \in X_n$ が $\Delta(\phi) \neq 0$ をみたすとき E を

$$y^2 = x^3 - 27c_4(\phi) - 54c_6(\phi)$$

で定まる楕円曲線とすると，C_ϕ には自然に E-トーサーの構造が入り，E は C_ϕ の Jacobi 多様体となる．

定理 5.4の証明の概略は 5.7節で述べる．

5.3 n 次モデルにより定まる滑らかな曲線の種数

F を代数閉体とする．本節では次の定理を証明する．

定理 5.5 $n = 1, 2, 3, 4$ とし，n 次モデル $\phi \in X_n$ を考える．C_ϕ が滑らかなとき，C_ϕ は種数 1 の曲線となる．$n = 3, 4$ で C_ϕ が滑らかなとき，$C_\phi \subset \mathbb{P}^{n-1}$ は次数 n の曲線となる．

証明 $n = 1, 2$ ではよく知られた事実であるので，以降，本節中は $n = 3, 4$ とする．R_n を F 係数の n 変数多項式環とする．C_ϕ の定義イデアルを $I_\phi \subset R_n$ とおく．このとき $n = 3, 4$ のそれぞれで R_n/I_ϕ の Hilbert 多項式が以下のように計算できる．

<u>$n = 3$</u> I_ϕ は一つの 3 次斉次多項式 $T \in R_3$ で生成される．したがって完全列

$$0 \longrightarrow R_3(-3) \xrightarrow{T} R_3 \longrightarrow R_3/I_\phi \longrightarrow 0$$

があり，定理 6.6 (ii),(iii) より

$$h_{C_\phi}(t) = \binom{t+2}{2} - \binom{t-1}{2} = 3t$$

となる．

<u>$n = 4$</u> I_ϕ は 2 次斉次多項式 $q_1, q_2 \in R_4$ で生成される．C_ϕ は 1 次元なので q_1, q_2 は互いに素であり，完全列

$$0 \longrightarrow R_4(-4) \xrightarrow{\binom{-q_2}{q_1}} R_4(-2)^2 \xrightarrow{(q_1 q_2)} R_4 \longrightarrow R_4/I_\phi \longrightarrow 0$$

がある．短完全列に分解して計算することで定理 6.6 (ii),(iii) より

$$h_{C_\phi}(t) = \binom{t+3}{3} - 2\binom{t+1}{3} + \binom{t-1}{3} = 4t$$

となる．

$n = 3, 4$ いずれの場合についても，仮定から C_ϕ が滑らかであることに注意すると，定理 6.6 (v) より $g = 1$ および次数 n であることがわかる． □

5.4 Weierstrass モデル

本節では n 次の Weierstrass モデルを定義し，$\pi_n^*\colon F[X_n]^{\tilde{\mathcal{G}}_n} \longrightarrow F[X_1]^{\tilde{\mathcal{G}}_1}$ を定める．Weierstrass モデルと π_n^* は $(X_n, \tilde{\mathcal{G}}_n)$ が余正則空間であることの証明で中心的な役割を担う．

E を (2.2) で定まる楕円曲線とし，E を定める 1 次モデルを ϕ とする．$(E, [n(O)])$ を n 次トーサー因子類ペアとみなしたとき，$n = 2, 3, 4$ に対し埋め込み

$$\begin{aligned}
&n = 2 \quad E \longrightarrow \mathbb{P}(1,2,1); \quad && (x, y) \mapsto (x : y : 1) \\
&n = 3 \quad E \longrightarrow \mathbb{P}^2; && (x, y) \mapsto (x : y : 1) \\
&n = 4 \quad E \longrightarrow \mathbb{P}^3; && (x, y) \mapsto (1 : x : y : x^2)
\end{aligned}$$

が定まる．この像を表す n 次モデルを $\pi_n(\phi) \in X_n$ とする．$\pi_n(\phi)$ を計算するとそれぞれ

$$\begin{aligned}
\pi_2(\phi) &= (a_1xz + a_3z^2,\ x^3z + a_2x^2z^2 + a_4xz^3 + a_6z^4) \\
\pi_3(\phi) &= (x_1x_3^2 + a_1x_1x_2x_3 + a_3x_1^2x_3 - x_2^3 - a_2x_1x_2^2 - a_4x_1^2x_2 - a_6x_1^3) \\
\pi_4(\phi) &= \begin{pmatrix} x_1x_4 - x_2^2 \\ x_3^2 + a_1x_2x_3 + a_3x_1x_3 - x_2x_4 - a_2x_2^2 - a_4x_1x_2 - a_6x_1^2 \end{pmatrix}
\end{aligned}$$

となる．また $g = [u; r, s, t] \in \mathcal{G}_1$ を作用させてから同様に計算して得られるモデル

は，上記で計算したモデルに以下の $\gamma_n(g) \in \mathcal{G}_n$ を作用させたものになる．

$$\gamma_2(g) = \left[u^{-3};\ (0, u^2, s, t),\ \begin{pmatrix} u^2 & 0 \\ r & 1 \end{pmatrix}\right]$$
$$\gamma_3(g) = \left[u^{-6};\ \begin{pmatrix} 1 & r & t \\ 0 & u^2 & u^2 s \\ 0 & 0 & u^3 \end{pmatrix}\right]$$
$$\gamma_4(g) = \left[\begin{pmatrix} u^{-4} & 0 \\ u^{-6r} & u^{-6} \end{pmatrix},\ \begin{pmatrix} 1 & r & t & r^2 \\ 0 & u^2 & u^2 s & 2u^2 r \\ 0 & 0 & u^3 & 0 \\ 0 & 0 & 0 & u^4 \end{pmatrix}\right]$$

以上の式により，一般に $\phi \in X_1$ と $g \in \mathcal{G}_1$ に対して $\pi_n(\phi)$ と $\gamma_n(g)$ を定めることで射

$$\pi_n \colon X_1 \longrightarrow X_n, \quad \gamma_n \colon \mathcal{G}_1 \longrightarrow \mathcal{G}_n$$

が定まり，多項式環の準同型

$$\pi_n^* \colon F[X_n] \longrightarrow F[X_1];\ f \mapsto f \circ \pi_n$$

が定まる．また，直接計算することで以下が分かる．

命題 5.6　$n = 2, 3, 4$ とする．

(i) $\phi' = \pi_n(\phi)$ のとき C_ϕ と $C_{\phi'}$ は曲線として同型.
(ii) γ_n は群スキームの準同型を定める．
(iii) 任意の $g \in \mathcal{G}_1$ と $\phi \in X_1$ に対し $(\gamma_n g)(\pi_n \phi) = \pi_n(g\phi)$.
(iv) 任意の $g \in \mathcal{G}_1$ に対し $\det(\gamma_n g) = \det g$.

したがって次数付き F-代数としての準同型

$$\pi_n^* \colon F[X_n]^{\tilde{\mathcal{G}}_n} \longrightarrow F[X_1]^{\tilde{\mathcal{G}}_1}$$

が誘導される．

命題 5.7　$F = \overline{F}$ かつ F の標数が $2, 3$ でないとする．C_ϕ が滑らかな種数 1 の曲線であるような n 次モデル ϕ に対し，一意的な $A, B \in F$ が存在し，ある $g \in \tilde{\mathcal{G}}_n$ について

$$g\phi = \pi_n(0, 0, 0, A, B)$$

を満たす．

証明 まず $g \in \mathcal{G}_n$ と $A', B' \in F$ で $g'\phi = \pi_n(0,0,0,A',B')$ を満たすものが存在することはよく知られている．g を適宜定数倍すると $\det g = 1$ であるように取れる．このときの $g\phi$ を $\pi_n(0,0,0,A,B)$ とすればよい．$\mathcal{G}_n$-作用による不変微分形式の変化を命題 5.23 で計算する．A, B の一意性はこの計算から従う． □

5.5 不変式 $c_4, c_6, \Delta \in F[X_n]^{\tilde{\mathcal{G}}_n}$ の存在

本節では π_n^* を通して，不変式 c_4, c_6, Δ の存在を証明する．詳細が気になる場合は [Fis08] を見よ．

補題 5.8 F の標数が $2, 3$ でないとき，1 次モデル $\phi \in X_1$ に対して c_4, c_6 を 2節で述べた方法で定義された不変式とすると $F[X_1]^{\tilde{\mathcal{G}}_1} = F[c_4, c_6]$ が成り立つ．

証明 $\phi \in X_1$ について，C_ϕ が滑らかなとき，(2.3) で定まる楕円曲線と F 上で同型である．このことと $\tilde{\mathcal{G}}_1$-作用で移りあう Weierstrass 方程式の標準的な計算により，

$$\iota\colon \mathbb{A}^2 \longrightarrow X_1; \quad (c_4, c_6) \mapsto (0,0,0,-c_4/48, -c_6/864)$$

が同型 $\iota^*\colon F[X_1]^{\tilde{\mathcal{G}}_1} \longrightarrow F[c_4, c_6]$ を導くことがわかる． □

補題 5.9 $f \in \overline{F}[X_1]^{\tilde{\mathcal{G}}_1} = \overline{F}[c_4, c_6]$ を斉次元とすると非負整数 p, q, r, s および $t_j \in \overline{F} \setminus \{0,1\}$ $(1 \le j \le s)$，$\alpha \in \overline{F}^\times$ があり

$$f = \alpha c_4^p c_6^q \Delta^r \prod_{j=1}^{s} (c_4^3 - t_j c_6^2)$$

と表せる．

証明 次数 $4, 6, 12$ の斉次元は以下に挙げたものの定数倍で尽くされる．

次数	斉次元
4	c_4
6	c_6
12	c_4^3, c_6^2, $c_4^3 - tc_6^2$ $(t \in \overline{F} \setminus \{0,1\})$

f の既約分解を

$$f = \prod_{j=1}^{u} f_j$$

とする．f_j は自然に斉次元になることに注意．$\deg f_j \equiv 4 \mod 12$ のとき，c_4 が f_j を割り切り，既約性から f_j は c_4 の定数倍である．$\deg f_j \equiv 6 \mod 12$ のとき，c_6 が f_j を割り切り，既約性から f_j は c_6 の定数倍である．$\deg f_j \equiv 2, 8, 10$ のとき，c_4c_6 が f_j を割り切るがこれは f_j の既約性に反する．$\deg f_j \equiv 0 \mod 12$ のとき，f_j は c_4^3, c_6^2 に関する斉次多項式である．したがって $\tilde{f}_j = f_j/c_6^{2\cdot\frac{\deg f_j}{12}}$ は c_4^3/c_6^2 に関する 1 変数の多項式であり，f_j の既約性から $\overline{F}$ 上でただ一つの根 t_j をもつ．ゆえに f_j は $c_4^3 - t_jc_6^2$ の定数倍である．ただし $t_j = 1$ のときは Δ の定数倍である．以上より主張が従う． □

命題 5.10 $n = 1, 2, 3, 4$ について

$$X_n^{\mathrm{sing}} = \{\phi \in X_n \mid C_\phi \text{は種数 1 の滑らかな曲線でない}\}$$

を考えるとこれは X_n の既約な真の Zariski 閉集合である．

証明 C_ϕ が滑らかであるとする．このとき定理 5.5より C_ϕ の種数は 1 である．$F = \overline{F}$ のときに示せば十分である．このとき X_n^{sing} は C_ϕ が滑らかでないような ϕ の全体である．$n = 1, 2$ では判別式 Δ で定義される部分なので主張が従う．$n = 3, 4$ について述べる．Zariski 閉集合になることに関しては Jacobi 行列の階数が落ちることが係数に関する方程式で書けることから従う．また

$$B_3 = \{x_1f_1(x_2, x_3) + f_2(x_2, x_3) \in X_3\} \subset X_3$$
$$B_4 = \left\{ \begin{pmatrix} \lambda x_1x_2 + g_1(x_2, x_3, x_4) \\ g_2(x_2, x_3, x_4) \end{pmatrix} \in X_4 \right\} \subset X_4$$

を考えると，X_n^{sing} は $\mathcal{G}_n \times B_n \longrightarrow X_n$ の像と同一視でき，また $\mathcal{G}_n, B_n$ が既約なことから X_n^{sing} の既約性が従う． □

補題 5.11 写像 $\pi_n^*\colon F[X_n]^{\tilde{\mathcal{G}}_n} \longrightarrow F[X_1]^{\tilde{\mathcal{G}}_1}$ は次数付き代数の単射である．

証明 F が代数閉体のときに証明すれば十分である．$f \in \ker \pi_n^*$ とする．閉体上で考えているので，任意の $\phi \in X_n \setminus X_n^{\mathrm{sing}}$ に対し $g \in \mathcal{G}_n$ が存在して $g \cdot \phi$ は Weierstrass モデルになる．したがって f の取り方から $\det(g)f(\phi) = f(g \cdot \phi) = 0$ となり，$\det(g) \neq 0$ なので $f(\phi) = 0$ が従う．つまり f は $X_n \setminus X_n^{\mathrm{sing}}$ 上で 0 である．命題 5.10より X_n^{sing} は真の Zariski 閉集合なので，f は X_n 全体で恒等的に 0 である．したがって π_n^* は単射である． □

補題 5.12 F を代数閉体とする．C_ϕ が滑らかな種数 1 の曲線であるような $\phi \in X_n$ について，ϕ の $\mathcal{G}_n$-軌道の Zariski 閉包は既約な不変式 $f \in K[X_n]^{\tilde{\mathcal{G}}_n}$ の零点集合になる．さらに，$\phi' \in X_n$ について $f(\phi') = 0$ であることと，ϕ と ϕ' の $\mathcal{G}_n$-軌道が一致することは同値である．

証明 $\mathbb{P}(X_n)$ では，ϕ の $\tilde{\mathcal{G}}_n$-軌道と $\mathcal{G}_n$-軌道は一致する．$\mathcal{G}_n$-作用の安定化部分群が有限なことが容易に確認でき，$\overline{\tilde{\mathcal{G}}_n\phi}$ の次元は $\mathcal{G}_n$ の次元に等しい．また $\dim \tilde{\mathcal{G}}_n = \dim X_n - 2$ に注意すると，$\overline{\tilde{\mathcal{G}}_n\phi}$ は $\mathbb{P}(X_n)$ の中で余次元 1 である．$\tilde{\mathcal{G}}_n$ の既約性から既約多項式 $f \in \overline{F}[X_n]$ が存在して $\overline{\tilde{\mathcal{G}}_n\phi} = (f = 0) \subset \mathbb{P}(X_n)$ となる．また ϕ の $\tilde{\mathcal{G}}_n$-軌道から f はスカラー倍を除いて一意的に定まるので f は $\tilde{\mathcal{G}}_n$-不変である．

ϕ, ϕ' の $\mathcal{G}_n$-軌道が一致することから $f(\phi') = 0$ が従うことは，f の定め方から明らか．逆の主張を示す．$f(\overline{\phi'}) = 0$ とする．ϕ' に対しても同様にして $\overline{\tilde{\mathcal{G}}_n\phi'} = (f' = 0)$ を満たす既約な不変式 f' がある．一方 $\phi' \in \overline{\tilde{\mathcal{G}}_n\phi}$ なので $\overline{\tilde{\mathcal{G}}_n\phi'} \subset \overline{\tilde{\mathcal{G}}_n\phi}$ であり，次元が等しい既約な閉部分集合なのでこれらは一致する．$\overline{\tilde{\mathcal{G}}_n\phi'} = \overline{\tilde{\mathcal{G}}_n\phi}$ は $\tilde{\mathcal{G}}_n\phi', \tilde{\mathcal{G}}_n\phi$ をいずれも開部分集合として稠密に含むので，これらは共通部分を持つ．したがって ϕ, ϕ' の $\mathcal{G}_n$-軌道は一致する． □

補題 5.13 F を標数が $2, 3$ でない代数閉体とする．このとき既約な不変式 $f_4, f_6 \in F[X_n]^{\tilde{\mathcal{G}}_n}$ と正の整数 p, q があり，$\pi_n^*(f_4) = c_4^p$, $\pi_n^*(f_6) = c_6^q$ を満たす．

証明 C_ϕ の j-不変量が 0 であるような Weierstrass モデル $\phi \in X_n$ をとる．ϕ から補題 5.12 により定まる既約な不変式を f_4 とすると，$\pi_n^*(f_4)$ は斉次元である．

$$\pi_n^*(f_4) = \alpha c_4^p c_6^q \Delta^r \prod_{j=1}^{s} (c_4^3 - t_j c_6^2)$$

を補題 5.9 で得られる既約分解とする．f_4 を定数倍で取り直すことで $\alpha = 1$ としてよい．

$C_{\phi'}$ の j-不変量が 0 でない滑らかな種数 1 の曲線であるような, 任意の Weierstrass モデル $\phi' = \pi_n^*(\phi_1) \in X_n$ に対し，f_4 の定め方から $f_4(\phi') \neq 0$ である．このことから $q = s = 0$ となる．次に C'_ϕ が j-不変量が 0 でなく滑らかでもないような，任意の Weierstrass モデル $\phi' = \pi_n^*(\phi_1) \in X_n$ に対し，f_4 の定め方から $f_4(\phi') \neq 0$ である．このことから $r = 0$ となる．

f_6 については，C_ϕ の j-不変量が 1728 であるような Weierstrass モデル $\phi \in X_n$ から始めて同様の議論をすればよい． □

補題 5.14 F が標数 0 の代数閉体のとき，c_4, c_6 は π_n^* の像の元であり，したがって $\pi_n^*\colon F[X_n]^{\tilde{\mathcal{G}}_n} \longrightarrow F[X_1]^{\tilde{\mathcal{G}}_1}$ は全射である．

証明 $\mathbb{F}$ を関数体 $F(X_n)$ とし，$\phi \in X_n(\mathbb{F})$ を生成的モデルとする．例えば $n = 2$ のときには X_2 の元は係数を抜き出すことで 8 次元のアフィン空間の元 $(\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e)$ と同一視できるが，各成分を文字とみなして得られるモデル $(\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e) \in X_n(\mathbb{F})$ を考える．$n = 3, 4$ でも同様．このとき $\det g = 1$ であるような $g \in \mathcal{G}_n(\overline{\mathbb{F}})$ および一意的な $A, B \in \overline{\mathbb{F}}$ が存在して，$g\phi = \pi_n(0, 0, 0, A, B)$ $(A, B \in \overline{\mathbb{F}})$ となる．ここで一意性より，A, B が Galois 不変であることが従い，つまり $A, B \in \mathbb{F}$ となる．

$f_4, f_6 \in F[X_n]^{\tilde{\mathcal{G}}_n}$ を補題 5.13 で構成した既約な不変式とする．このとき

$$\begin{aligned} f_4 &= f_4(\phi) = f_4(g\phi) = f_4(\pi_n(0,0,0,A,B)) \\ &= \pi_n^* f_4(0,0,0,A,B) = (-48A)^p \\ f_6 &= f_6(\phi) = f_6(g\phi) = f_6(\pi_n(0,0,0,A,B)) \\ &= \pi_n^* f_6(0,0,0,A,B) = (-864B)^q \end{aligned}$$

となる．$\mathbb{F}$ の中で $K[X_n]$ は整閉なので $-48A, -864B$ はいずれも $F[X_n]$ の元であることが分かり，また f_4, f_6 の既約性から $p = q = 1$ となる． □

補題 5.15 補題 5.14を $F = \overline{\mathbb{Q}}$ に適用すると，π_n^* による像が c_4, c_6, Δ である元 $f_4, f_6, \tilde{\Delta}$ が得られる．これらは $\mathbb{Z}[X_n]$ の元である．

証明 $c_4, c_6 \in \mathbb{Z}[X_1]$ であったことに注意すると，f_4, f_6 の Galois 共役の π_n^* による像もまた c_4, c_6 である．π_n^* の単射性から f_4, f_6 が Galois 不変であることが従い，ゆえに f_4, f_6 は $\mathbb{Q}[X_n]$ の元である．f を $f_4, f_6, \tilde{\Delta}$ のいずれかとする．$f \notin \mathbb{Z}[X_n]$ と仮定すると $p^{r+1} f \in \mathbb{Z}_p[X_n]$, $p^r f \notin \mathbb{Z}_p[X_n]$ であるような素数 p と整数 $r \geq 0$ が存在する．$g = p^{r+1} f \mod p \in \mathbb{F}_p[X_n]$ とすると，r の取り方から $p^{r+1} f$ の係数には p で割り切れないものがあり $g \neq 0$ である．ところが

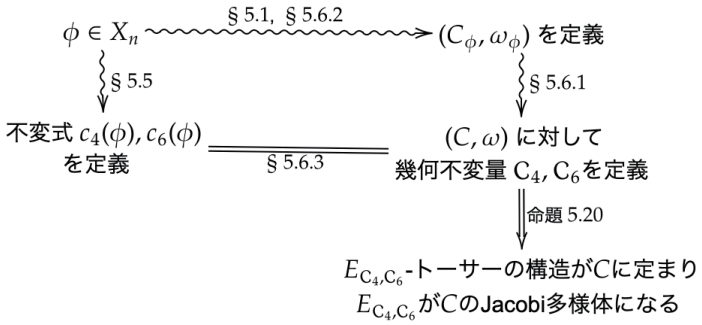
$$\pi_n^* g = p^{r+1} \pi_n^* f \mod p = 0$$

となり，これは π_n^* の単射性に矛盾する． □

$f_4, f_6, \tilde{\Delta} \in \mathbb{Z}[x_n]$ のことも c_4, c_6, Δ で表すことにする．

5.6 幾何不変量

本節では幾何不変量 $\mathcal{C}_4, \mathcal{C}_6$ を定義し，不変式 c_4, c_6 と一致することを証明する．主な構造は以下の通りである．



5.6.1 幾何不変量とトーサー

C を F 上の滑らかな種数 1 の曲線とし，C 上の F 上で定義された 0 でない正則微分形式 ω を固定する．ω を C の不変微分形式と呼ぶ．本節では (C, ω) に対して幾何不変量 c_4, c_6 を定め，幾何不変量と Jacobi 多様体の関係について述べる．

定義 5.16 $\overline{F}$ 上では (C, ω) は

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

および

$$\omega = dx/(2y + a_1x + a_3)$$

と表せる．

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6
\end{aligned}$$

とする．c_4, c_6 は $(a_1, a_2, a_3, a_4, a_6)$ は (C, ω) のみに依存しており，従って Galois 不変である．ゆえに F の元である．これら c_4, c_6 を (C, ω) の幾何不変量と呼ぶ．混乱を避けるため，以降では幾何不変量を $\mathcal{C}_4, \mathcal{C}_6$ で表す．

補題 5.17 F を標数が $2, 3$ でない体とする．E を F 上の楕円曲線，ω を E の不変微分形式とする．α を E の代数多様体としての自己同型とする．このとき α が平行移動写像であることとは $\alpha^*\omega = \omega$ であることと同値である．

証明 $P \in E$ による平行移動写像を $\tau_P \colon E \longrightarrow E$ で表す．すると $P \mapsto \tau_P^*\omega/\omega$ が射 $E \longrightarrow \mathbb{G}_m$ を定めるが，これは定数写像しかない．特に $P = O$ とすると $\tau_P^*\omega = \omega$ が従う．

逆に α が平行移動写像でないと仮定すると $\alpha - \mathrm{id}$ は定数写像ではなく，従って全射である．特に $O \in \mathrm{Im}(\alpha - \mathrm{id})$ なので α は固定点を持つ．この点による平行移動で共役を取ることで，固定点は O であるとしてよい．このとき α は群同型である．また標数の仮定から E は (2.3) で与えられるとしてよい．このとき (E, O) の自己同型 α は $(x, y) \mapsto (u^2x, u^3y)$ の形で与えられるが，ω は dx/y の定数倍なので α により不変である． □

補題 5.18 E/F を楕円曲線とし，C を E-トーサーとする．$Q_0 \in C(\overline{F})$ を固定して

$$\begin{aligned} \mathrm{sum}\colon \mathrm{Div}^0(C) &\longrightarrow E \\ \sum n_i(Q_i) &\longmapsto \sum [n_i](Q_i - Q_0) \end{aligned}$$

で定まる写像を考える．このとき以下が成り立ち, E は C の Jacobi 多様体となる．

(a) 以下の完全列がある

$$1 \longrightarrow \overline{F}^\times \longrightarrow \overline{F}(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \xrightarrow{\mathrm{sum}} E \longrightarrow 0.$$

(b) 写像 sum は Q_0 の取り方に依らない．

(c) 写像 sum は $\mathrm{Div}^0(C)$ および E への $\mathrm{Gal}(\overline{F}/F)$-作用と可換である．特に

$$\mathrm{Pic}^0_F(C) \cong E(F)$$

が成り立つ．

証明 [Sil92, Chapter X, Theorem 3.8] を見よ． □

補題 5.19　F の標数が $2,3$ でないとする．楕円曲線 E と滑らかな種数 1 の曲線 C がいずれも F 上で定義されているとする．ω_E, ω_C をそれぞれ E, C の不変微分形式とする．もし $\alpha^*\omega_E = \omega_C$ を満たすような同型射 $\alpha\colon C \longrightarrow E/\overline{F}$ があれば，C には自然に E-トーサーの構造が定まる．

証明 $\sigma \in \mathrm{Gal}(\overline{F}/F)$ に対し，自己同型 $\xi_\sigma = \sigma(\alpha)\alpha^{-1}$ を考える．すると $\xi_\sigma^*\omega_E = \omega_E$ を満たすので補題 5.17 から ξ_σ は平行移動写像である．これを $P_\sigma \in E$ による平行移動であるとすると，C は $(P_\sigma) \in H^1(K, E)$ に対応する E のひねりである．特に

$$\mu(P, Q) = \alpha^{-1}(P + \alpha(Q))$$

で定まる $\mu\colon E \times C \longrightarrow C$ により C に E-トーサーの構造が定まる．　□

命題 5.20　F の標数は $2,3$ でないとする．F 上の滑らかな種数 1 の曲線 C と F 上で定義された不変微分形式 ω に対し，幾何不変量が $\mathcal{C}_4, \mathcal{C}_6$ であるとき，E を

$$y^2 = x^3 - 27\mathcal{C}_4 - 54\mathcal{C}_6$$

で定めると C には自然に E-トーサーの構造が定まる．

証明 (C, ω) と $(E, 3dx/y)$ は同じ幾何不変量をもつので $\overline{F}$ 上では同型である．補題 5.19 により主張が従う．　□

5.6.2　n 次モデルから定まる不変微分形式

本節では C_ϕ が滑らかな種数 1 の曲線であるような n 次モデル ϕ $(n = 1, 2, 3, 4)$ に対して，C_ϕ 上の不変微分形式 ω_ϕ を定め，$\mathcal{G}_n$-作用による ω_ϕ の変化を見ることで，(C_ϕ, ω_ϕ) の幾何不変量 c_4, c_6 と不変式 $c_4(\phi), c_6(\phi)$ が一致することを証明する．

定義 5.21（不変微分形式）　n 次モデル ϕ に対し，C_ϕ 上の不変微分形式 $\underline{\omega_\phi}$ を以下で定める．

$$n=1 \quad \omega_\phi = \frac{dx}{2y+a_1x+a_3} \qquad \text{for } \phi=(a_1,a_2,a_3,a_4,a_6)$$

$$n=2 \quad \omega_\phi = \frac{z^2 d(x/z)}{2y+a_1xz+a_3z^2} \quad \text{for } \phi=(p(x,z),q(x,z))$$

$$n=3 \quad \omega_\phi = \frac{x_1^2 d(x_2/x_1)}{\partial T/\partial x_3} \qquad \text{for } \phi=(T)$$

$$n=4 \quad \omega_\phi = \frac{x_1^2 d(x_2/x_1)}{\frac{\partial q_1}{\partial x_4}\frac{\partial q_2}{\partial x_3}-\frac{\partial q_1}{\partial x_3}\frac{\partial q_2}{\partial x_4}} \quad \text{for } \phi=\begin{pmatrix} q_1(x_1,x_2,x_3,x_4) \\ q_2(x_1,x_2,x_3,x_4)\end{pmatrix}$$

とする．ここで $n=3,4$ のとき，定理 5.5 の証明中で用いた完全列を

$$\mathcal{F}_\bullet(\phi)\colon 0 \longrightarrow \mathcal{F}_{n-2} \xrightarrow{\varphi_{n-2}} \mathcal{F}_{n-3} \longrightarrow \cdots \longrightarrow \mathcal{F}_1 \xrightarrow{\varphi_1} R_n \longrightarrow R_n/I_\phi \longrightarrow 0$$

とすると

$$\omega_\phi = \frac{x_1^2 d(x_2/x_1)}{(\partial\varphi_1/\partial x_3)\cdots(\partial\varphi_{n-2}/\partial x_n)}$$

であることに注意せよ．ただし分母の行列の偏微分は，各成分ごとの偏微分を表している．

ω_ϕ の定義は一見アドホックに見えるが，次の補題が成り立つように定めている．

補題 5.22 $n=2,3,4$ とする．C_{ϕ_1} が滑らかな種数 1 の曲線であるような 1 次モデル ϕ_1 に対し，Weierstrass モデル $\phi=\pi_n(\phi_1)$ を考える．このとき自然に定まる同型 $\gamma\colon C_{\phi_1} \longrightarrow C_\phi$ について $\gamma^*\omega_\phi=\omega_{\phi_1}$ を満たす．

証明 π_n と ω_ϕ の定義から直接的な計算で確認できる． □

命題 5.23 C_ϕ が滑らかな種数 1 の曲線であるような n 次モデル ϕ を考える．$g\in\mathcal{G}_n$ に対して $\phi'=g\phi$ とし，g によって誘導される曲線の同型を $\gamma\colon C_{\phi'} \longrightarrow C_\phi$ とすると，

$$\gamma^*\omega_\phi = (\det g)\omega_{\phi'}$$

を満たす．

証明 $n=1,2$ に対してはよく知られた事実であるので $n=3,4$ に対して証明する．$\mathcal{G}_n$ の生成元に対して示せば良い．$g=[1,B]$ であって，B の対角成分が全て 0 でな

く，対角成分以外に高々 1 つだけ 0 でない成分がある場合，主張は容易に確認できる．$n=3$ かつ $g=[\mu, I_3]$ の場合も容易に確認できる．$n=4$ かつ $g=[A, I_4]$ の場合，$\mathcal{F}_\bullet(\phi')$ と $\mathcal{F}_\bullet(\phi)$ についての可換図式

$$\begin{tikzcd}
0 \arrow[r] & R_4(-4) \arrow[r, "\varphi_2'"] \arrow[d, "\det A"] & R_4(-2)^2 \arrow[r, "\varphi_1'"] \arrow[d, "{}^tA"] & R_4 \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & R_4(-4) \arrow[r, "\varphi_2"] & R_4(-2)^2 \arrow[r, "\varphi_1"] & R_4 \arrow[r] & 0
\end{tikzcd}$$

がある．

$$\frac{\partial \varphi_2'}{\partial x_4} = \frac{\partial\left(({}^tA)^{-1}\varphi_2 \det A\right)}{\partial x_4} = ({}^tA)^{-1}\frac{\partial \varphi_2}{\partial x_4}\det A$$
$$\frac{\partial \varphi_1'}{\partial x_3} = \frac{\partial(\varphi_1 {}^tA)}{\partial x_3} = \frac{\partial \varphi_1}{\partial x_3}\cdot {}^tA$$

に注意すると

$$\frac{\partial \varphi_1}{\partial x_3}\frac{\partial \varphi_2}{\partial x_4} = \det A \frac{\partial \varphi_1'}{\partial x_3}\frac{\partial \varphi_2'}{\partial x_4}$$

が従い，これにより

$$\gamma^*\omega_\phi = \frac{x_1^2 d(x_2/x_1)}{(\partial\varphi_1/\partial x_3)(\partial\varphi_2/\partial x_4)} = \det A \frac{x_1^2 d(x_2/x_1)}{(\partial\varphi_1'/\partial x_3)(\partial\varphi_2'/\partial x_4)} = (\det g)\omega_{\phi'}$$

を得る．

あとは $g=[1, B]$ で B が置換行列の場合に証明すればよい．さらにその置換が隣接互換 $(a\ b)$ の場合に主張を証明すればよい．$(a\ b)=(1\ 2)$ のとき

$$x_1^2 d(x_2/x_1) = x_1 dx_2 - x_2 dx_1 = -x_2^2 d(x_1/x_2)$$

なのでよい．また φ_1 の成分が I_ϕ の元であることと $\displaystyle\sum_{i=1}^n \frac{\partial \varphi_1}{\partial x_i}x_i = (\deg \varphi_1)\varphi_1$ が成り立つことに気をつけると

$$\begin{aligned}
x_1^2 \sum_{i=2}^n \frac{\partial \varphi_1}{\partial x_i} d\left(\frac{x_i}{x_1}\right) &= \sum_{i=2}^n \frac{\partial \varphi_1}{\partial x_i}(x_1 dx_i - x_i dx_1) \\
&= \sum_{i=2}^n \frac{\partial \varphi_1}{\partial x_i} x_1 dx_i - \deg \varphi_1 \cdot \varphi_1 dx_1 + \frac{\partial \varphi_1}{\partial x_1} x_1 dx_1 \\
&= \sum_{i=1}^n \frac{\partial \varphi_1}{\partial x_i} x_1 dx_i = x_1 d\varphi_1 = 0
\end{aligned} \tag{5.5}$$

を得る．$n=3$，$(a\ b)=(2\ 3)$ のときの主張はこれから従う．

$n=4$ とし，$\varphi=\begin{pmatrix} q_1 \\ q_2 \end{pmatrix}$ とする．$(a\ b)=(3\ 4)$ のとき

$$\frac{\partial\varphi_1}{\partial x_3}\frac{\partial\varphi_2}{\partial x_4}=\begin{pmatrix} \dfrac{\partial q_1}{\partial x_3} & \dfrac{\partial q_2}{\partial x_3} \end{pmatrix}\begin{pmatrix} -\dfrac{\partial q_2}{\partial x_4} \\ \dfrac{\partial q_1}{\partial x_4} \end{pmatrix}$$
$$=-\frac{\partial q_1}{\partial x_3}\frac{\partial q_2}{\partial x_4}+\frac{\partial q_2}{\partial x_3}\frac{\partial q_1}{\partial x_4}=-\gamma^*\omega_\phi$$

が成り立つことから主張が従う．$(a\ b)=(2\ 3)$ のとき

$$\frac{x_1^2 d\left(\dfrac{x_2}{x_1}\right)}{\dfrac{\partial\varphi_1}{\partial x_3}\dfrac{\partial\varphi_2}{\partial x_4}}=-\frac{x_1^2 d\left(\dfrac{x_3}{x_1}\right)}{\dfrac{\partial\varphi_1}{\partial x_2}\dfrac{\partial\varphi_2}{\partial x_4}}$$

を示せばよいが，(5.5) を用いると両辺の差が 0 であることがわかる． □

5.6.3 幾何不変量と不変式の一致

命題 5.24 F の標数が $2,3$ でないとし，$n=1,2,3,4$ とする．n 次モデル ϕ で，C_ϕ が滑らかな種数 1 の曲線であるとする．(C_ϕ,ω_ϕ) の幾何不変量を $\mathcal{C}_4,\mathcal{C}_6$ とすると

$$c_4(\phi)=\mathcal{C}_4,\quad c_6(\phi)=\mathcal{C}_6$$

が成り立つ．

証明 命題 5.7より，$\tilde{\mathcal{G}}_n(\overline{F})$-作用で ϕ は Weierstrass モデルに移る．命題 5.23 および補題 5.22 により $n=1$ の場合に帰着される．$n=1$ のときは c_4,c_6 と幾何不変量の定義は一致しているので自明． □

5.7 主定理の証明

定理 5.4の証明 (i) $c_4,c_6,\Delta\in\mathbb{Z}[X_n]$ の $F[X_n]$ での像を改めて c_4,c_6,Δ で表す．これらは 0 でない．補題 5.11, 5.8 より

$$\pi_n^*\colon F[X_n]^{\tilde{\mathcal{G}}_n}\longrightarrow F[X_1]^{\tilde{\mathcal{G}}_1}=F[c_4,c_6]$$

が単射であり，$c_4,c_6\in F[X_n]$ が $\mathbb{Z}$ 上で定義されていたことから全射性が従う．

(ii) F は代数閉体であると仮定してよい．C_ϕ が滑らかな種数 1 の曲線を定めるような $\phi \in X_n$ は $\tilde{\mathcal{G}}_n$ 作用により Weierstrass モデル移る．このとき $\Delta(\phi) \neq 0$ となる．したがって包含関係

$$\{\phi \in X_n \mid \Delta(\phi) = 0\} \subset X_n^{\mathrm{sing}}$$

がある．命題 5.10 から X_n^{sing} は既約なので，この包含は実際は等号であることが従う．
(iii) 命題 5.24 より $c_4(\phi), c_6(\phi)$ は (C_ϕ, ω_ϕ) の幾何不変量に一致する．ゆえに補題 5.20 から主張が従う．

□

定理 5.25 K を数体とし，$n = 2, 3, 4$ とする．$\mathcal{C}_4, \mathcal{C}_6 \in K$ とする．

$$y^2 = x^3 - 27\mathcal{C}_4 x - 54\mathcal{C}_6$$

で定まる楕円曲線 E/K に対し，集合

$$\{\phi \in X_n \mid c_4(\phi) = \mathcal{C}_4,\ c_6(\phi) = \mathcal{C}_6,\ C_\phi \text{は局所可解}\}$$

の $\tilde{\mathcal{G}}_n(K)$-軌道と，$\mathrm{Sel}^{(n)}(E/K)$ の元とが 1 対 1 に対応する．

証明 局所可解な n 次トーサー因子類ペア $(C, [D])$ から n 次モデル ϕ' が $\mathcal{G}_n(K)$-作用の任意性を除いて一意に定まることは 5.1節で見た．$(C, [D])$ が $E_{\mathcal{C}_4, \mathcal{C}_6}$-トーサーであることから，$c_4(\phi) = \mathcal{C}$ かつ $c_6(\phi) = \mathcal{C}_6$ を満たすような n 次モデル ϕ が，この ϕ' の $\tilde{\mathcal{G}}_n(K)$-軌道上に $\tilde{\mathcal{G}}_n(K)$-作用を除いて一意に存在する．

逆の対応について述べる．$\phi \in X_n$ を $\Delta(\phi) \neq 0$ かつ C_ϕ が局所可解な n 次モデルで，不変量 $c_4(\phi) = \mathcal{C}_4$, $c_6(\phi) = \mathcal{C}_6$ をもつものとする．このとき定理 5.4 (ii) から C_ϕ は滑らかな種数 1 の曲線である．$n = 1$ のとき，$\Delta(\phi) \neq 0$ なら C_ϕ は次数 1 の K-有理因子 $D = (0 : 1 : 0)$ をもつ．$n = 2$ のとき，y について平方完成を行うことで，ϕ は $\tilde{\mathcal{G}}_n(K)$-作用により $(0, q)$ の形の 2 次モデルに移る．このモデルについては $D = (1 : \sqrt{a} : 0) + (1 : -\sqrt{a} : 0)$ が次数 2 の K-有理因子である．一般には平方完成の操作を逆にたどって D を引き戻せばよい．$n = 3, 4$ のとき，D を $C_\phi \subset \mathbb{P}^{n-1}$ の超平面切断とすると D は次数 n の K-有理因子である．また定理 5.4 (iii) から C_ϕ に自然に $E_{\mathcal{C}_4, \mathcal{C}_6}$-トーサーの構造が入り，これにより $(C_\phi, [D])$ は $E_{\mathcal{C}_4, \mathcal{C}_6}$ の n 次トーサー因子類ペアになる．これらは互いに逆の対応を与える． □

6　曲線の代数幾何の基本事項

本節は代数幾何的な言葉遣いや取扱いに不慣れな方のための付録である．内容は [Har77] 及び [Sil92] を参考にした．詳細が気になる場合はこれらを見よ．

6.1　曲線，因子

曲線とは，次元 1 の射影代数多様体のこととする．以下，C を体 F 上の曲線とする．

定義 6.1　C の因子群 $\mathrm{Div}(C)$ とは $C(\overline{F})$ の元で生成される自由生成アーベル群のこととし，その元を因子と呼ぶ．因子 D は一般に有限個以外は 0 であるような整数 n_P を用いて

$$D = \sum_{P \in C(\overline{F})} n_P(P)$$

と表せる．楕円曲線の加法との混同を避けるため，$P \in C(\overline{F})$ を因子とみなす際は括弧をつけて (P) で表記する．

$f \in \overline{F}(C)^\times$ に対して

$$\mathrm{div}(f) = \sum_{P \in C(\overline{F})} \mathrm{ord}_P(f)(P)$$

により因子が構成される．ここで $\mathrm{ord}_P(f)$ は f の P での位数を表している．このように構成される因子のことを主因子 (Principal divisor) と呼び，主因子全体の集合のことを $\mathrm{Princ}(C)$ で表す．$\mathrm{Princ}(C)$ は $\mathrm{Div}(C)$ の部分群をなす．$\mathrm{Div}(C)$ の $\mathrm{Princ}(C)$ による剰余群のことを $\mathrm{Pic}(C)$ で表し，C の Picard 群と呼ぶ．因子 D で代表される $\mathrm{Pic}(C)$ の元のことを $[D]$ で表す．2 つの因子 D_1, D_2 について $D_1 - D_2$ が $\mathrm{Princ}(C)$ の元であるとき $D_1 \sim D_2$ と表す．

定義 6.2（Galois 作用）　C の因子 $D = \sum n_P(P)$ と $\sigma \in G_F$ に対して $\sigma(D)$ を

$$\sum_{P \in C(\overline{F})} n_P(\sigma(P))$$

で定義する．任意の $\sigma \in G_F$ に対して $\sigma(D) = D$ が成り立つような因子 D 全体の集合を $\mathrm{Div}_F(C)$ で表し，その元のことを F-有理因子と呼ぶ．また任意の $\sigma \in G_F$ に

対して $\sigma(D) \sim D$ が成り立つ，つまり $[\sigma(D)] = [D]$ が成り立つような因子 D 全体の集合を $\underline{\mathrm{Pic}_F(C)}$ で表し，その元を $\underline{F\text{-有理因子類}}$と呼ぶ.

6.2 完備線形系

F を体，C を F 上の滑らかな射影曲線とする．C の因子 $D = \sum n_P(P)$ について，すべての P に対して $n_P \geq 0$ であることを$\underline{D \geq 0}$ で表す．また因子 D について

$$\mathcal{L}(D) = \{f \in \overline{F}(C)^\times \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

は自然に有限次元 $\overline{F}$-ベクトル空間の構造をもつ．この空間の次元を

$$\ell(D) = \dim_{\overline{F}} \mathcal{L}(D)$$

で表す．$D = \sum n_P(P)$ としたとき，$\mathrm{div}(f) + D \geq 0$ が成り立つことは，$n_P \geq 0$ であるような P については f が P を高々位数 n_P の極にもち，$n_P \leq 0$ であるような P については f が P を $-n_P$ 以上の位数の零点にもつことを意味する.

$D = \sum n_P(P)$ の次数 $\deg D$ を $\sum n_P$ で定める.

定理 6.3 (i) C を F 上の滑らかな射影曲線とする．このとき標準因子と呼ばれる因子 K_C 及び整数 $g \geq 0$ があり，任意の因子 $D \in \mathrm{Div}(C)$ に対して

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1$$

が成り立つ．この g を C の (幾何) 種数と呼ぶ.

(ii) $\ell(K_C) = g$.

(iii) $\deg K_C = 2g - 2$.

(iv) $f \in \overline{F}(C)^\times$ について $\deg \mathrm{div}(f) = 0$.

(v) $\deg D > 2g - 2$ のとき

$$\ell(D) = \deg D - g + 1$$

が成り立つ.

(vi) $\deg D \geq 2g$ のとき D は base point free である．つまり $\mathcal{L}(D)$ の元に共通零点はなく，$\mathcal{L}(D)$ の基底を並べることで定まる有理写像 $C \dashrightarrow \mathbb{P}^{\dim \mathcal{L}(D)-1}$ は射になる.

(vii) $\deg D \geq 2g + 1$ のとき D は非常に豊富であり，$\mathcal{L}(D)$ の基底を並べることで定まる射 $C \longrightarrow \mathbb{P}^{\dim \mathcal{L}(D)-1}$ は埋め込みになる.

(viii) $D \in \mathrm{Div}_F(C)$ のとき，$\mathcal{L}(D)$ には $F(C)$ の元からなる基底が存在する．

証明 (i) [Har77, IV Theorem 1.3] を見よ

(ii) $\mathcal{L}(0) = \overline{F}$ に注意し，$D = 0$ に対して (i) を適用すると分かる．

(iii) $D = K_C$ に対して (i) を適用すると分かる．

(iv) f で定まる射 $C \longrightarrow \mathbb{P}^1$ を考える．$D = (Q)$ の引き戻し $f^*(Q)$ は $\sum_{P \in f^{-1}(Q)} e_f(P)(P)$ で定められる．ここで $e_f(P)$ は f の P での分岐指数である．一般の因子の引き戻しはこの定義を $\mathbb{Z}$-線形に拡張して得られる．すると Riemann–Hurwitz の公式から $\deg f^*(Q) = \sum_{P \in f^{-1}(Q)} e_f(P) = \deg f$ が成り立ち，従って

$$\deg \mathrm{div}(f) = \deg f^*((0) - (\infty)) = \deg f - \deg f = 0$$

と計算できる．

(v) $\ell(K_C - D) = 0$ を示せば，(i) と合わせることで主張が従う．$\deg D > 2g - 2$ のとき，(iii) より $\deg K_C - D < 0$ なので，$\deg(\mathrm{div}(f) + K_C - D) < 0$ が任意の $f \in \overline{F}(C)^\times$ に対して成り立つ．従って $\ell(K_C - D) = 0$ である．

(vi) [Har77, IV Corollary 3.2 (a)] を見よ．

(vii) [Har77, IV Corollary 3.2(b)] を見よ．

(viii) D が F 上で定義されているので，任意の $\sigma \in \mathrm{Gal}(\overline{F}/F)$ と任意の $f \in \mathcal{L}(D)$ に対して

$$\sigma(f) \in \mathcal{L}(\sigma(D)) = \mathcal{L}(D)$$

である．したがって $\mathrm{Gal}(\overline{F}/F)$ は $\mathcal{L}(D)$ に作用する．主張は次の補題から従う．

□

補題 6.4 V を $\overline{F}$-ベクトル空間とし，$\mathrm{Gal}(\overline{F}/F)$ が V に $\overline{F}$ の作用と可換かつ連続に作用しているとき

$$V_F = V^{\mathrm{Gal}(\overline{F}/F)} = \{v \in V \mid \text{任意の } \sigma \in \mathrm{Gal}(\overline{F}/F) \text{ に対し } \sigma(v) = v\}$$

とすると

$$V \cong \overline{F} \otimes_F V_F$$

が成り立つ．

注意 6.5 $\mathrm{Gal}(\overline{F}/F)$ が V に連続に作用するとは任意の $v \in V$ に対して

$$\mathrm{Stab}(v) = \{\sigma \in \mathrm{Gal}(\overline{F}/F) \mid \sigma(v) = v\}$$

が $\mathrm{Gal}(\overline{F}/F)$ の有限指数の部分群であることとする．

証明 任意の $v \in V$ が V_F の元の $\overline{F}$-線形和で書けることを示せばよい．指数有限正規部分群 $\mathrm{Stab}(v) \subset \mathrm{Gal}(\overline{F}/F)$ に対応する F の有限次ガロア拡大を L とする．$\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ を L/F の基底とし，$\mathrm{Gal}(L/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ とする．各 $1 \leq i \leq n$ についてベクトル

$$w_i = \sum_{j=1}^{n} \sigma_j(\alpha_i v) = \mathrm{Tr}_{L/F}(\alpha_i v)$$

を考えると，w_i は $\mathrm{Gal}(\overline{F}/F)$ 不変なので V_F の元である．また行列 $(\sigma_j(\alpha_i))_{1 \leq i,j \leq n}$ が正則であることは体論でよく知られた事実である．したがって任意の j について $\sigma_j(v)$ は w_i たちの L-線形和で表せ，特に $v = \mathrm{id}(v)$ は w_i たちの L-線形和で表せる． □

6.3 Hilbert 多項式と算術種数

定義，定理 6.6 F を代数閉体とし，$R_n = F[x_0, x_1, \ldots, x_n]$ とする．

(i) R_n 上の有限生成次数付き加群 $M = \bigoplus_{l \geq 0} M_l$ に対して，一意的な $\mathbb{Q}$-係数多項式 $h_M(t)$ が存在し，十分大きな任意の l について

$$h_M(l) = \dim_F M_l$$

が成り立つ．この多項式 $h_M(t)$ を M の<u>Hilbert 多項式</u>という．さらに $Z(\mathrm{Ann}\, M) \subset \mathbb{P}^n$ を斉次イデアル $\mathrm{Ann}\, M$ から定まる閉部分スキームとすると，$\dim Z(\mathrm{Ann}\, M) = \deg h_M(t)$ を満たす．

(ii) R_n 自身を多項式の次数により次数付き R_n-加群とみなし，次数 d の部分を $(R_n)_d$ で表すことにすると Hilbert 多項式は二項係数を用いて

$$h_{R_n}(t) = \binom{t+n-1}{n-1}$$

で表せる．また k を整数とすると，$(R_n(k))_d = (R_n)_{d+k}$ により次数付けした次数付き加群 $R_n(k)$ に対する Hilbert 多項式は

$$h_{R_n(k)}(t) = \binom{t+k+n-1}{n-1}$$

となる．

(iii) R_n 上の有限生成次数付き加群の短完全列

$$0 \longrightarrow M^{(1)} \longrightarrow M^{(2)} \longrightarrow M^{(3)} \longrightarrow 0$$

があるとき

$$h_{M^{(1)}}(t) - h_{M^{(2)}}(t) + h_{M^{(3)}}(t) = 0$$

が成り立つ．

(iv) $Y \subset \mathbb{P}^n$ を r 次元の閉部分スキームとし，Y を定める斉次イデアルを $I(Y)$ とする．このとき Y の斉次座標環 $R_n/I(Y)$ に対する Hilbert 多項式を単に h_Y で表す．h_Y の最高次係数に $r!$ をかけた値を，Y の<u>次数</u>という．$C \subset \mathbb{P}^{n-1}$ が滑らかな次数 d 種数 g の射影曲線のとき，Hirbert 多項式 h_C は

$$h_C(t) = dt + (1-g)$$

となる．

(v) r 次元射影代数多様体 Y に対し，算術種数 $\underline{p_a(Y)}$ を $(-1)^r(h_Y(0)-1)$ で定める．C が滑らかな射影曲線のとき $p_a(C)$ は幾何種数 $g(C)$ に一致する．

証明 (i) [Har77, I Theorem 7.5] を見よ．

(ii) $h_{R_n}(t)$ についての主張は標準的な計算から従う．また $R_n(k)$ と Hilbert 多項式の定義から $h_{R_n(k)}(t) = h_{R_n}(t+k)$ となる．

(iii) 各次数の F 上の次元の加法性と Hilbert 多項式の定義から明らか．

(iv) 次数の定義と算術種数の定義及び (iv) から従う．

(v) 算術種数及び幾何種数にはいずれにも，コホモロジーを用いた表示方法がある．滑らかな射影曲線のときにはこれらは Serre 双対性で結ばれ，等しい値になる．詳しくは [Har77, III Remark 7.12.2] を見よ．

□

謝辞

準備段階でのアドバイスや当日のきめ細やかな運営をしていただいた，整数論サマースクール 2023 世話人の谷口隆さん，杉山和成さん，石塚裕大さんに感謝いたします．特に石塚さんには講演者としての推薦，準備段階でのセミナー，参考文献の提示や，私の不理解な部分へのアドバイスなど，たいへんお世話になりました．私は概均質ベクトル空間や余正則空間については全くの素人でしたが，今回の講演の準備を通して大変勉強になりました．このことに関しましても，改めましてオーガナイザーの皆様に感謝を申し上げます．また，予稿を入念に読みたくさんの誤植をご指摘くださった小野雅隆さんに感謝いたします．

参考文献

[AKMMMP01] S. Y. An, S. Y. Kim, C. C. Marshall, S. H. Marshall, W. G. MaCallum, and A. R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90** (2001) 304–315.

[BH16] M. Bhargava and W. Ho, *Coregular spaces and genus one curves*, Camb. J. Math **4** (2016), no. 1, 1–119.

[BS13a] M. Bhargava and A. Shankar, *The average number of elements in the 4-Selmer groups of elliptic curves is 7*, Preprint, arXiv: 1312.7333

[BS13b] M. Bhargava and A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, Preprint, arXiv: 1312.7859

[BS15a] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. **181** (2015), 191–242.

[BS15b] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. **181**(2015), 587–621.

[BS14] M. Bhargava and C. Skinner, *A positive proportion of elliptic curves over* $\mathbb{Q}$ *have rank one*, preprint, arXiv: 1401.0233.

[Cas62] J.W.S. Cassels, *Arithmetic on Curves of Genus 1. IV. Proof of the Hauptvermutung.*, vol.1962, no. 211 (1962), 95–112.

[CFNSS08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves, I. Algebra*, vol. 2008, no.615 (2008), 121–155

[Duj] A. Dujella, *History of elliptic curves rank records*, `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`

[Fis] T. A. Fisher, *Genus one curves defined by Pfaffians*, Preprint, `http://dpmms.cam.ac.uk/~taf1000/`

[Fis06] T. A. Fisher, *Testing equivalence of ternary cubics*, Algorithmic Number Theory, Lecture Notes in Comput. Sci. **4076**, Springer-Verlag, New York, 2006, 333–345.

[Fis08] T. A. Fiisher, *The invariants of a genus one curves*, Proc. London Math. Soc. (3) **97** (2008), 753–782.

[Har77] R. Hartshorne, *Algebraic Geometry* volume 52 of Graduate Texts in Math., Springer-Verlag, New York, 1977.

[KM95] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, in Columbia university number theory seminar - New York, 1992, Astérisque, no. 228 (1995), 81–98.

[Maz77] B. Mazur, *Modular curves and the eisenstein ideal*, Publications Mathématiques de L'Institut des Hautes Scientifiques **47**, (1977) 33–186.

[MG78] B. Mazur and D. Goldfeld, *Rational isogenies of prime degree*, Invent Math **44** (1978), 129–162

[Mer98] Loïc Merel. *Rational points and Dirichlet series (Points rationnels et séries de Dirichlet)*, Documenta Mathematica, (1998), 183–186.

[PPVW19] J. Park, B. Poonen, J. Voight, and M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. **21**, (2019) 2859–2903.

[Ser88] J.-P. Serre, *Algebraic Groups and Class Fields*, volume 117 of Graduate Texts in Math., Springer-Verlag, NewYork-Berlin, 1988.

[Ser02] J.-P. Serre, *Galois cohomology*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, volume 106 of Graduate Texts in Math., Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Yuk] A. Yukie, *Rational orbit decomposition of prehomogeneous vector spaces*, available from `https://www.math.kyoto-u.ac.jp/~yukie/`.