Complete 2-descent を用いた
楕円曲線のモーデル・ヴェイユ群の計算について

池田　愛輝

新潟大学大学院自然科学研究科博士前期課程
数理物質科学専攻

概要

筆者は大学院で J. H. Silverman 著の The Arithmetic of Elliptic Curves ([Sil1]) をセミナーの教科書として, 楕円曲線の理論を学んできた. 本論文はその中でとくに興味をもった Complete 2-descent とよばれる定理について, セミナーで発表した内容を基に, 簡潔かつ丁寧な証明を心がけてまとめたものである.

本論文の特色を 2 つ述べる. 1 つ目の特色は, 代数体 K 上の楕円曲線 E と, E 上の K 有理点全体からなる群 $E(K)$ を研究対象とし, とくに $E(\mathbb{Q})$ を計算するのに有用な Complete 2-descent に主題をおいた点である. 筆者は本論文を, 各命題の結びつきが見やすくなるように気をつけながら, Complete 2-descent を用いた $E(\mathbb{Q})$ の計算に必要な定理と命題を中心にまとめた. その中で, とくに重要な命題は良い還元において $E(K)$ のねじれ部分群を有限体上の楕円曲線に埋め込む定理, $E(\mathbb{Q})$ が有限生成アーベル群であるというモーデルの定理, そして $E(K)/2E(K)$ からある有限群への良い埋め込みの存在を主張する m-Descent とよばれる定理である. これらの定理を用いて, Complete 2-descent の証明と $E(\mathbb{Q})$ の計算例の詳しい記述を行った. 2 つ目の特色は, 楕円曲線の標準的な教科書である [Sil1] を補強する内容を掲載した点である. 第 2 章以降において, ヘンゼルの補題を除いたすべての命題に証明が付いている. それらの証明は簡潔で分かりやすいよう心がけ, 必要に応じて補題を準備した. 本論文において, 楕円曲線から誘導される形式群を定義する議論, 合同数問題と関連する楕円曲線のねじれ部分群を記述する命題の証明, $E(\mathbb{Q})$ 上の高さ関数を構成する命題の証明は [Sil1] と比べてより詳細に記述した. また, 定義や命題の記述を [Sil1] と比較して少し一般化するなどの細かな工夫を行った. 例えば還元写像は離散付値環 R 上の楕円曲線 E に対して定義されており, [Sil1] のように, 還元写像で写す上で E が極小ワイエルシュトラス形式であるかどうかを気にする必要がない. それに対応して, いくつかの命題を R 上の楕円曲線に対して記述している. また, [Neu] を含む様々な文献を参考にしながら, [Sil1] と少し異なる形で弱モーデル・ヴェイユの定理の証明をまとめた. [Sil1] では, この定理は K 上の体拡大の条件 (i) 高々指数が m である, かつ (ii) K の素点からなる有限集合 S の外不分岐, をみたす中での最大のアーベル拡大 L/K が有限次拡大であることを用いて証明される. 本論文では, この定理の証明を写像 $\Gamma : \mathrm{Hom}(G_K, E[m]) \longrightarrow \mathcal{L}$ を定義し, Γ の性質と $\Gamma \circ \delta_K$ を調べる方法で行った. ただし, ここで $\mathcal{L}$ は特定の条件をみたす K 上の拡大体からなる集合, δ_K はクンマー理論から定まる写像である. この証明を紹介した理由は $E(K)/mE(K)$ と $\mathcal{L}$ を結びつけることで, $E(K)/mE(K)$ の有限性を示す部分がより分かりやすくなると考えたからである.

本論文は 4 つの章からなっている. 第 1 章はアフィン空間や射影空間, 射影曲線の関数体といった, [Sil1] で述べられている代数幾何の初歩的な定義を既知として, 第 2 章以降で必要となる定義や命題をまとめた. 1.1 節から 1.7 節は [Sil1] を参考に, 楕円曲線における基本的な内容がまとめてある. そして, 1.8 節は [NSW] を参考にガロアコホモロジーについて, 1.9 節は [高木] を参考に有限次クンマー拡大について, 1.10 節は [Sil1] を参考に環上の形式群について, 1.11 節は [Sil1] を参考にアーベル群に対する降下定理についてまとめた. 第 2 章以降は [Sil1] を参考にしている. 第 2 章では, まず楕円曲線から誘導される形式群 $\hat{E}$, x, y に関するローラン級数, そして還元写像を定義する. 次に還元写像の核 $E_1(K)$ と, $\hat{E}$ から誘導される群 $\hat{E}(\mathcal{M})$ が群同型であることを x, y に関するローラン級数を用いて証明する. そして, 群同型 $E_1(K) \cong \hat{E}(\mathcal{M})$ を通して, 形式群の一般論を $E_1(K)$ に適用することで, モーデル・ヴェイユ群 $E(K)$ のねじれ部分群の計算に有用な定理を証明した. 最後にその定理を用いて, いくつかの楕円曲線に対し, $E(K)$ のねじれ部分群の計算を行った. 第 3 章では, モーデルの定理の証明を行う. まず 3.1 節で一般の代数体に対する弱モーデル・ヴェイユの定理を証明し, 3.2 節でアーベル群に対する降下定理を適用するために, $E(\mathbb{Q})$ 上の高さ関数を構成した. そして続く 3.3 節で, これらを用いてモーデルの定理を証明し, モーデル・ヴェイユ群の階数の定義を行った. その後, ねじれ部分群や階数に関して知られている結果や話題を少し紹介した. 第 4 章では, m-Descent とよばれる定理を用いて Complete 2-descent を証明する. $E[m] \subset E(K)$ をみたす自然数 m に対して, m-Descent は $E(K)/mE(K) \times E[m]$ から $K^*/(K^*)^m$ へ良い双線形写像が存在することを主張する. Complete 2-descent を適用することで, $E(K)/2E(K)$ は単射 Φ により有限群 $K(S_{E,2}) \times K(S_{E,2})$ に埋め込まれる. さらに, $P \in E(K)/2E(K)$ が $\mathrm{Im}(\Phi)$ に含まれる必要十分条件が, P から定まる変数 z_1, z_2, z_3 に関する方程式の解の有無によって記述される. 4.2 節で, $E(K)$ の計算が $E(K)$ のねじれ部分群と $E(K)/2E(K)$ の計算に帰着されることを述べた後, Complete 2-descent を用いた $\mathbb{Q}$ 上の楕円曲線 E のモーデル・ヴェイユ群 $E(\mathbb{Q})$ の計算例を詳しく記載した. そして, 4.3 節でセルマー群を定義し, 今後の展望について述べた.

謝辞

主指導教員である星明考先生には, 学部をあわせた 3 年間のセミナーを通して, 数学の見方や研究のとり組み方をはじめとする様々な助言をいただきました. 星先生は私の性格や状況を見ながら, そのときどきで適切なアドバイスと辛抱強い指導をしてくださいました. そして, 大変なときには常に温和な励ましをしてくださったことに心から感謝いたします. また, 副指導教員である小島秀雄先生, 印南信宏先生は質問をした際に, いつも丁寧に応えてくださいました. そして, 学部と大学院を通して丹念に数学を教えてくださいました. ここに深い感謝の意を表します.

星研究室の長谷川寿人先輩, 金井和貴先輩, 小柴将和先輩, 小川紘平先輩は私が困ったときにいつも快く助けてくださいました. 時間をとり, 数学の議論を交わしてくださったこと, そして本論文に関することを含め, 様々な相談にのってくださったことに深く感謝いたします. また, 本論文に関して丁寧なアドバイスをくださりました小島研究室の長峰孝典先輩に感謝の意を表します.

最後に, 難しいときも常に応援し支えてくれた家族に, 心からの感謝を申し上げます.

目次

記号

本論文で用いる記号や用語に関する注意をはじめに述べておく.

- $\mathbb{N}$ を自然数全体，$\mathbb{Z}$ を整数環，$\mathbb{Q}$ を有理数体，$\mathbb{R}$ を実数体，$\mathbb{C}$ を複素数体とする.
- $\mathbb{F}_q$ を位数が q の有限体とする.
- $\mathbb{Q}_p$ を素数 p に関する p 進数体とする.
- $\#A$ で集合 A の位数を表す.
- 群 G, H に対し, $H \leq G$ で H が G の部分群であることを表す. また, $H \triangleleft G$ で H が G の正規部分群であることを表す.
- $\overline{k}$ を体 k の代数的閉包とする.
- μ_m を 1 の m 乗根全体からなる有限群とする.
- 体 K に対し, $\mathrm{char}(K)$ で K の標数を表す.
- G_K で体 K の絶対ガロア群を表す.
- 体拡大 L/K に対し, $G_{L/K}$ で L/K のガロア群を表す.
- 体拡大 L/K に対し, $[L:K]$ で L/K の拡大次数を表す.
- 代数体 K に対し, $M_K, M_K^{\infty}, M_K^0, \mathcal{O}_K, I_K, \Delta_K$ で, それぞれ K の素点全体, K の無限素点全体, K の有限素点全体, K の整数環, K の分数イデアルからなる群, K の判別式を表す. また, $\mathfrak{p} \in M_k^0$ に対し, $\mathrm{ord}_{\mathfrak{p}} : I_K \longrightarrow \mathbb{Z} \cup \{\infty\}$ で $\mathfrak{p}$ の正規離散付値を表す.
- 体 K と自然数 n に対し, $\mathbb{A}^n$ で $\overline{K}$ 上の n 次元アフィン空間を表す. また, $\mathbb{A}^n(K)$ で座標がすべて K の元である n 次元アフィン空間の元全体を表す.
- $(x_1, \ldots, x_n)$ で n 次元アフィン空間 $\mathbb{A}^n$ の座標を表す.
- 体 K と自然数 n に対し, $\mathbb{P}^n$ で $\overline{K}$ 上の n 次元射影空間を表す. また, $\mathbb{P}^n(K)$ で座標がすべて K の元で表せる n 次元射影空間の元全体を表す.
- $[x_1, \ldots, x_{n+1}]$ で n 次元射影空間 $\mathbb{P}^n$ の斉次座標を表す.
- 基礎体 K 上の代数曲線 C に対し, $K(C)$ で C の関数体を表す.
- 環 R に対し, $R[[X_1, \ldots, X_m]]$ で R 上の m 変数べき級数環を表す.
- 体 K に対し, $K((X_1, \ldots, X_m))$ で K 上の m 変数べき級数体を表す

1　準備

この章では, 第 2 章以降で必要となる定義や命題をまとめた. 1.1 節から 1.7 節は楕円曲線に関する基本的な内容を復習しており, 主に [Sil1] に基づいている. 1.1 節で楕円曲線を定義し, 楕円曲線がワイエルシュトラス形式で与えられた射影曲線と無限遠点の組としてよいことを見る. 1.2 節でワイエルシュトラス形式で与えられた射影曲線の判別式を定義する. そして, 1.3 節で楕円曲線にガロア加群の構造を定義する. この作用は離散的ガロア加群であることが 1.8 節で分かる. 1.4 節でねじれ部分群を定義し, ねじれ点の群構造を調べる. 1.5 節で楕円曲線の同型と, 楕円曲線上の点からなる集合を添加した体の定義を行う. 1.6 節で因子を定義し, 楕円曲線の主因子の計算例を見る. 1.7 節でヴェイユペアリングを定義し, 非退化性, 双線形性といったヴェイユペアリングのもつ良い性質について復習する. そして, 1.8 節は [NSW] を参考にガロアコホモロジーについて, 1.9 節を [高木] を参考に有限次クンマー拡大について, 1.10 節を [Sil1] を参考に環上の形式群について, 1.11 節を [Sil1] を参考にアーベル群に対する降下定理についてまとめた.

本章における命題の証明は基本的に割愛するが, 各命題には参考文献を明記した. また, 参考文献が記載されていない命題については証明を付けた.

この章を通して基礎体 K は完全体, すなわち K は非分離拡大体をもたない体とする.

1.1　楕円曲線

定義　種数 1 の非特異射影曲線 E と, その曲線上の点 O からなる 2 つ組 (E, O) を, **楕円曲線 (elliptic curve)** という.

楕円曲線 (E, O) は, E の定義方程式の係数がすべて K の元であり, かつ $O \in \mathbb{P}^n(K)$ であるときに ***K* 上で定義されている**といい, E/K により表す. また, E は ***K* 上の楕円曲線である**ともいう.

上で定義した楕円曲線は, 定義方程式の個数や形について何も言及されていない. しかし, 任意の K 上の楕円曲線 (E, O) は

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

という形で与えられる非特異射影曲線と同型となることが知られている ([Sil1, III, 3.1.]). この形の方程式を**ワイエルシュトラス方程式 (Weierstrass equation)** といい, 定義多項式がワイエルシュトラス方程式で与えられた射影曲線を**ワイエルシュトラス形式**

(Weierstrass form) という. また, E と C の同型を, 与えられていた点 O が斉次座標で $[0,1,0]$ に写るようにできる ([Sil1, III, 3.1.]). この事実により, 楕円曲線はワイエルシュトラス形式で与えられた射影曲線 E と, E 上の点 $[0,1,0]$ からなる 2 つ組 $(E,[0,1,0])$ であるとしてよい. 以後, $\mathbb{P}^2(K)$ 内の固定点 $[0,1,0]$ を O で表す.

また, 射影空間の中で斉次座標により表された楕円曲線

$$E_{\mathrm{proj}} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

において, $Z = 1$ とすると E_{proj} はアフィン平面で

$$E_{\mathrm{aff}} : y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$$

と表される. ここで, O は E_{proj} 上で $Z = 0$ をみたす唯一の元である. したがって, O を E の**無限遠点 (point at infinity)** という. E_{proj} は E_{aff} に無限遠点 O を加えた集合と見ることができる. そのため, 以下ではとくに断りがない場合, 斉次座標で与えられた楕円曲線もアフィン平面で与えられた表記をする.

注意 一般に, アフィン代数多様体 V を斉次化して得られた射影代数多様体 $\overline{V}$ に対し, $\overline{V} \setminus V$ の元を無限遠点とよぶ ([Sil1, I, 2.7.]). 実際, E_{proj} は E_{aff} を $x = X/Z, y = Y/Z$ により斉次化して得られており, また $E_{\mathrm{proj}} \setminus E_{\mathrm{aff}} = \{O\}$ である.

ワイエルシュトラス形式で与えられた射影曲線がいつ楕円曲線であるかは, 1.2 節で定義する判別式を計算することで判定できる (命題 1.3). ワイエルシュトラス形式で与えられた楕円曲線の例をいくつかあげておく.

例 1.1 以下のワイエルシュトラス形式で与えられた射影曲線はすべて $\mathbb{Q}$ 上の楕円曲線である.

- $E_1 : y^2 = x^3 + 3$
- $E_2 : y^2 = x^3 - x$.
- $E_3 : y^2 = x(x-12)(x-36)$.
- $E_4 : y(y+1) = x(x+1)(x+2)$.

K 上の楕円曲線 $E : y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$ が与えられたとき, 座標がすべて K の元である E 上の点を $\boldsymbol{K}$ **有理点 (**$\boldsymbol{K}$**-rational point)** という. 例えば, 例 1.1 において, $(1,2)$ は E_1 の $\mathbb{Q}$ 有理点である. ここで, 楕円曲線上の $\mathbb{Q}$ 有理点に関する応用を紹介する.

正の有理数 n に対し, n が**合同数 (congruent number)** であるとは, 辺の長さがすべて有理数であり, かつ面積が n となる直角三角形が存在するときをいう. いつ正の有理数 n が合同数となるかという問いは合同数問題とよばれ, 古くから研究されていた. 例えば 1 は合同数でないが, 7 は合同数である. このような初等的な問いは難しいことが多いが, 合同数問題はそのうちの一つであり, 現在でも完全には解決されていない. 楕円曲線は合同数問題と次のような関係がある.

命題 1.2 ([Kob, I, §1, 18.]) n を正の有理数とする. このとき, 以下は同値である.

(a) n は合同数である.
(b) 楕円曲線 $E/\mathbb{Q} : y^2 = x^3 - n^2x$ に無限個の $\mathbb{Q}$ 有理点が存在する.

このように, n が合同数であるか否かが n から定まる楕円曲線の $\mathbb{Q}$ 有理点の個数と結びつく. 合同数問題に関するさらに詳しい内容は [Kob] を参照してほしい.

1.2 判別式

前節で, 楕円曲線はとくにワイエルシュトラス方程式を定義多項式としてよいことを復習した. それでは逆に, ワイエルシュトラス方程式により定義された射影曲線 E はすべて楕円曲線となるだろうか. 一般に, n 次斉次多項式で定義される射影平面曲線の種数は $(n-1)(n-2)/2$ であるので, E の種数が 1 であることはよい. また, 既約であることも計算により確かめることができる. したがって, 問題となるのは非特異性の部分である.

ワイエルシュトラス方程式から定まる射影曲線の非特異性は, 以下に定義する判別式によってなされる.

定義 K 上の射影曲線 $E : y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$ に対して,

- $b_2 := a_1^2 + 4a_2$,
- $b_4 := 2a_4 + a_1a_3$,
- $b_6 := a_3^2 + 4a_6$,
- $b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$

と定める. そして,

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

と定義し, E の**判別式 (discriminant)** という.

命題 1.3 ([Sil1, III, 1.4.]) ワイエルシュトラス方程式で定義された射影曲線 E に対し, 以下は同値である.

(1) E は非特異である.
(2) $\Delta_E \neq 0$.

注意 命題 1.3 より, ワイエルシュトラス方程式から定まる射影曲線 E に対して, E が楕円曲線であることと $\Delta_E \neq 0$ は同値である.

例 1.4 K 上の射影曲線

$$E_A : y^2 = x^3 + Ax$$

に対し, $b_2 = 0$, $b_4 = 2A$, $b_6 = 0$, $b_8 = -A^2$ より $\Delta_{E_A} = -2^6 A^3$ である. したがって, K の標数が 2 でなく, かつ $A \neq 0$ なら, E_A は楕円曲線である.

例 1.5 K 上の射影曲線

$$E_B : y^2 = x^3 + B$$

に対し, $b_2 = 0$, $b_4 = 0$, $b_6 = 4B$, $b_8 = 0$ より $\Delta_{E_B} = -2^4 3^3 B^2$ である. したがって, K の標数が 2, または 3 でなく, かつ $B \neq 0$ なら, E_B は楕円曲線である.

1.3 群法則とガロア作用

この節では, 楕円曲線に群構造を定義する. そして, G_K の作用により, 楕円曲線がガロア加群となることを復習する.

定義 K 上の楕円曲線 $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ について, E 上の点 $P = (x_1,\ y_1)$, $Q = (x_2,\ y_2)$ に対し, 次のように演算 $\oplus$ と $\ominus$ を定義する.

- $\ominus P = (x_1,\ -y_1 - a_1x_1 - a_3)$,
- $P \oplus Q = \big(\lambda^2 + a_1\lambda - a_2 - x_1 - x_3,\ -(\lambda + a_1)x_3 - \nu - a_3\big)$.

ただし, ここで λ, ν は以下のように定める.

- $x_1 = x_2$ のとき, $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$, $\nu = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$,
- $x_1 \neq x_2$ のとき, $\lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$, $\nu = \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$.

上で定めた加法 $\oplus$ によって, E はアーベル群となる ([Sil1, III, 2.3.]). このとき, 無限

遠点 O が単位元となり, また P の逆元は $\ominus P$ となる. さらに, この加法は K 有理点に関して閉じており, E 上の K 有理点全体からなる集合 $E(K)$ もアーベル群となる ([Sil1, III, 2.2.]). すなわち, $E(K)$ は E の部分群となる. $E(K)$ が群であることが分かったところで, $E(K)$ に名前を付けておく.

定義 E/K を楕円曲線とする. このとき,

$$E(K) = \{(x, y) \in E \mid x, y \in K\} \cup \{O\}$$

を**モーデル・ヴェイユ群 (Mordell-Weil group)** という.

注意 楕円曲線の演算は, 幾何的に見ると次の事柄に対応している. $P, Q \in E$ に対し, P と Q を通る直線 L ($P = Q$ の場合は L を P における接線とする) と E の交点を R とする. そして, L_1 を R と O を通る直線とすれば, L_1 と E の交点が $P \oplus Q$ である. ここで 任意の楕円曲線と直線は必ず 3 点で交わるが, これらを P, Q, R とすると $P \oplus Q \oplus R = O$ が成り立つ. 詳細は [Hus, 1, §5.] や [Sil1, III.2.] を参照してほしい.

次に, 楕円曲線 E/K に対して絶対ガロア群 G_K の左作用を, 以下のように定義する.

定義 E/K を楕円曲線とする. このとき, G_K から E への作用を, $P = [x, y, z] \in E$, $\sigma \in G_K$ に対して

$$\sigma(P) := [\sigma(x), \sigma(y), \sigma(z)]$$

で定義する.

注意 m 倍写像が多項式の有理式の形, すなわち有理写像であるので, E は G_K 加群となる. このように, E を単なる集合として見るのではなく, ガロア加群として見ることが重要である. その理由は次節で定義する m 倍写像 $[m] : E \longrightarrow E$ から定まる完全系列に対し, 1.8 節で導入するガロアコホモロジーを適用することで, 調べたい対象をコホモロジーと結びつけることができる点にある.

以降において, $\sigma \in G_K$, $x \in \overline{K}$, $P \in E$ に対して, $\sigma(x)$ を x^σ, $\sigma(P)$ を P^σ と書く. そのため, 作用の順序を合わせるために $x^{\sigma\tau} := (x^\tau)^\sigma$, $P^{\sigma\tau} := (P^\tau)^\sigma$ と定義する.

1.4 m 倍写像とねじれ点

この節では, 楕円曲線の m 倍写像と, $E(K)$ のねじれ部分群を定義する. また, 各自然数 m に対し, E の m ねじれ点からなる群の構造について述べる.

この節を通して, とくに断りがない場合 E/K は楕円曲線とする.

定義　整数 m に対して, E から E への m 倍写像

$$[m] : E \to E;\ P \longmapsto [m]P$$

を自然に定義する. すなわち, $m > 0$ のときは

$$[m]P := \underbrace{P \oplus \cdots \oplus P}_{m\ 個},$$

$m < 0$ のときは $[m]P := \ominus[-m]P$, そして $[0]P := O$ と定める.

例 1.6 ([Sil1, III, 2.3.])　$P = (x, y) \in E$ に対して, $[2]P$ の x 座標 $x([2]P)$ は

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

で与えられる. これを **2 倍公式 (duplication formula)** という.

定義　自然数 m に対して,

$$E[m] := \{P \in E \mid [m]P = 0\},$$
$$E(K)[m] := \{P \in E(K) \mid [m]P = 0\}$$

と定義する. また,

$$E_{\mathrm{tors}} := \bigcup_{m=1}^{\infty} E[m],$$
$$E(K)_{\mathrm{tors}} := \{P \in E_{\mathrm{tors}} \mid P \in K\}$$

と定義する. E_{tors} は E のねじれ部分群であり, $E(K)_{\mathrm{tors}}$ は位数有限で, かつ K 有理点である元全体からなる集合である.

次の命題は $E[m]$ の群構造を記述する重要な命題である.

命題 1.7 ([Sil1, III, 6.4.])　E/K を楕円曲線, m を自然数とする. また $p = \mathrm{char}(K)$ に対して, $p = 0$, または $p > 0$ かつ $p \nmid m$ であるとする. このとき,

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

が成り立つ.

注意　命題 1.7 より, 楕円曲線 E/K に対して, とくに K の標数が正のときには常に $E[m]$ は有限位数であることが分かる. 実際には, 任意の標数に対して $E[m]$ は有限位数である ([Sil1, III, 6.4.]).

1.5　同種写像

この節では, 楕円曲線の同種写像の定義を行う. そして, 同種写像を用いて楕円曲線の同型の定義をし, 2 つの楕円曲線が同型ならば, そのモーデル・ヴェイユ群も群同型となることを示す. そして, 同型である楕円曲線の例をあげる. また, この節で楕円曲線 E/K の部分集合 A に対し, K に A を添加した体の定義が行われる.

定義　E_1, E_2 を K 上の楕円曲線とする. このとき, 代数多様体の射 $\phi : E_1 \longrightarrow E_2$ で $\phi(O) = O$ をみたすものを**同種写像 (isogeny)** という.

例 1.8 整数 m に対して,

$$[m] : E \longrightarrow E; P \longmapsto [m]P$$

は同種写像である.

同種写像に関して, 次の重要な命題が成り立つ.

命題 1.9 ([Sil1, III, 4.8.]) E_1, E_2 を K 上の楕円曲線, $\phi : E_1 \longrightarrow E_2$ を同種写像とする. このとき, $P, Q \in E$ に対して

$$\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$$

が成り立つ.

上の命題から, K 上で定義された同種写像 $\phi : E_1 \longrightarrow E_2$ はモーデル・ヴェイユ群上の準同型写像 $E_1(K) \longrightarrow E_2(K)$ を引き起こす. したがって, ϕ が全単射な同種写像であるとき, $E_1(K)$ と $E_2(K)$ は群同型となる. このことを定理の形で述べておく.

定理 1.10 ([Sil1, III]) E_1, E_2 を K 上の楕円曲線, $\phi : E_1 \longrightarrow E_2$ を K 上で定義された全単射な同種写像とする. このとき, $E_1(K)$ と $E_2(K)$ は群同型である.

注意　同種写像の定義において, “代数多様体の射”の部分を“有理写像”としてもよい. これは次の事実からしたがう.

- 非特異射影曲線から代数多様体への有理写像は, 代数多様体の射となる ([Sil1, II, 2.1.]).
- 全単射である代数多様体の射は, 代数多様体の同型写像である ([Sil1, II, 2.4.1.]).

定理 1.10 を踏まえて, K 上の楕円曲線の同型を次で定義する.

定義 E_1, E_2 を K 上の楕円曲線とする. E_1 と E_2 は**同型 (isomorphic)** であるとは, K 上で定義された全単射な同種写像 $\phi : E_1 \longrightarrow E_2$ が存在するときをいい, $E_1 \cong E_2$ で表す.

例 1.11 代数体 K 上の楕円曲線 E_1, E_2, E_3, E_4 を,

$$\begin{aligned} E_1 &: y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x^2 + a_6, \\ E_2 &: y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \\ E_3 &: y^2 = x^3 - 27c_4x - 54c_6, \\ E_4 &: y^2 = x^3 + Ax + B \end{aligned}$$

とする. ただし, ここで

- $c_4 = b_2 - 24b_4$,
- $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$

であり, さらに $c_4 = e_4/d_4, c_6 = e_6/d_6$ $(d_4, d_6, e_4, d_6 \in \mathcal{O}_K)$ に対して,

- $A = -27d_4^5d_6^6e_4$,
- $B = -54d_4^6d_6^5e_6$

である. すると, 変数変換

$$\begin{aligned} \phi_1 : E_1 \longrightarrow E_2; (x, y) &\longmapsto \left(x, \frac{y - a_1x - a_3}{2} \right), \\ \phi_2 : E_2 \longrightarrow E_3; (x, y) &\longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right), \\ \phi_3 : E_3 \longrightarrow E_4; (x, y) &\longmapsto \left(\frac{x}{d_4^2d_6^2}, \frac{y}{d_4^3d_6^3} \right) \end{aligned}$$

から定まる代数多様体の射は全単射な同種写像である. したがって,

$$E_1(K) \cong E_2(K) \cong E_3(K) \cong E_4(K)$$

である.

例 1.11 における変数変換 $\phi_1 : E_1 \longrightarrow E_2$ を用いることで, $E[2]$ の元が次のように記述できる.

命題 1.12 楕円曲線 E/K に対し, $4X^3 + b_2X^2 + 2b_4X + b_6$ の根を $\alpha_1, \alpha_2, \alpha_3$ とする. このとき, $P \in E \setminus \{O\}$ に対して以下は同値である.

(1) $P \in E[2]$.
(2) P の x 座標は $\alpha_1, \alpha_2, \alpha_3$ のいずれかである.

とくに, $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ に対して

$$E[2] = \{(\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0), O\}$$

である.

証明 K 上の楕円曲線

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

は, 変数変換 $\phi_1 : (x, y) \longmapsto (x, (y - a_1x - a_3)/2)$ によって

$$E' : y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6$$

と同型である. ここで ϕ_1 が x 座標を動かさないので, E の二等分点の x 座標と E' の二等分点の x 座標は等しい. すると, $P = (x, y) \in E \setminus O$ に対して, $P \in E'[2]$ と $P = \ominus P$ が同値であることに注意すれば, $\ominus P = (x, -y)$ より x は $F(X)$ の根である. また $F(X)$ は重根をもたないので, $\alpha_1, \alpha_2, \alpha_3$ は相異なる. ここで命題 1.7 より $\#E[2] = 4$ であるから, $\alpha_1, \alpha_2, \alpha_3$ によって $E[2] \setminus \{O\}$ の元における x 座標は尽くされている. 以上により, 命題の後半もしたがう. □

次に, 楕円曲線上の点を添加した体を定義する.

定義 E を K 上の楕円曲線, A を E の部分集合とする. このとき,

$$K(A) := K\left(x, y \mid P = (x, y) \in A \setminus \{O\}\right)$$

と定義し, $K(A)$ のことを K に ***A* を添加した体**という. また, 楕円曲線の間の同種写像 $\phi : E_1 \longrightarrow E_2$ と E_2 の部分集合 A に対して

$$K(\phi^{-1}A) := K\left(x, y \mid P = (x, y) \in E_1 \setminus \{O\},\ \phi(P) \in A\right)$$

と定義する. すなわち, $K(\phi^{-1}A)$ は ϕ による A の逆像を添加した体である.

例 1.13 K に添加した体の例をあげる.

- $\mathbb{Q}$ 上の楕円曲線 $E_1 : y^2 = x^3 + 3$ に対し, $K(\{(0, \sqrt{3})\}) = K(\sqrt{3})$.
- K 上の楕円曲線 $E : y^2 = (x - e_1)(x - e_2)(x - e_2)$ に対し, 命題 1.12 より $K(E[2]) = K(e_1, e_2, e_3)$.

定理 1.9 を用いることにより, m 倍写像 $[m] : E \longrightarrow E$ による $E(K)$ の逆像を添加した体 $K([m]^{-1}E(K))$ が同型に関しする不変量であることが分かる.

命題 1.14 E_1, E_2 を K 上の楕円曲線, $\phi : E_1 \longrightarrow E_2$ を K 上で定義された同種写像とする. このとき, ϕ が全単射ならば $K([m]^{-1}E_1(K)) = K([m]^{-1}E_2(K))$ が成り立つ.

証明 $Q \in [m]^{-1}E_2(K)$ を任意にとる. すると, ϕ は全射なので $\phi(P) = Q$ となる $P \in E_1$ が存在する. ここで定理 1.9 より,

$$\phi([m]P) = [m]\phi(P) = [m]Q$$

なので, Q のとり方から $[m]P = \phi^{-1}([m]Q) \in E_1(K)$ である. したがって, $P \in [m]^{-1}E_1(K)$ を得る. すると Q の各座標は $[m]^{-1}E_1(K)$ の元と K の元による多項式の形で書けているので, $K([m]^{-1}E_2(K)) \subset K([m]^{-1}E_1(K))$ である. 同様にして逆の包含が成り立つので, $K([m]^{-1}E_2(K)) = K([m]^{-1}E_1(K))$ を得る. □

注意 命題 1.14 は 3.1 節の命題 3.7 の証明で, より扱いやすい同型な楕円曲線を選んで一般性を失わないことを示す部分に使われる.

この節の最後に, 全射な同種写像について成り立つ命題を述べる. この命題の内容は, 楕円関数体に関するガロアの基本定理とよばれる定理中から抜粋したものである. この定理に興味がある場合は, [Sil1, III, 4.10.] を参照してほしい.

命題 1.15 ([Sil1, III, 4.10.]) E_1, E_2 を K 上の楕円曲線, $\phi : E_1 \longrightarrow E_2$ を全射な同種写像とする. このとき, 任意の $Q \in E_2$ に対して $\#\phi^{-1}(Q)$ は有限集合である.

注意 命題 1.15 は命題 3.7 (2) の証明で, $P \in E(K)$ に対して体拡大 $K([m]^{-1}(P))/K$ が有限次拡大であることを示す部分で使われる.

1.6 因子

この節では因子の復習を行う. その中で, 命題 1.17 は定理 4.3 (Complete 2-descent) の証明に関わる重要な命題である. この節を通して, 射影曲線 C と K 上のアフィン代数多様体 V に対し, 以下の記号を用いる.

- $\overline{K}(C)$ で C の関数体を表す.
- $P \in C$ に対して, $\overline{K}[C]_P$ で P における C の局所環を表す.
- $\overline{K}[V]$ で V のアフィン座標環を表す.
- $P \in V$ に対して, $M_P := \{f \in \overline{K}[V] \mid f(P) = 0\}$ で P から定まる $\overline{K}[V]$ の極大イデアル, $\overline{K}[V]_P$ で P における V の局所環を表す.

定義 C を射影曲線とする. このとき, C 上の点による整数係数の形式和

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

で, 有限個の点を除いて $n_P = 0$ となるものを C 上の**因子 (divisor)** という. そして, C 上の因子からなる群を $\mathrm{Div}(C)$ で表し, C 上の**因子群 (divisor group)** という. また D の次数を

$$\deg D := \sum_{P \in C} n_P$$

によって定義する. そして, C 上の次数が 0 の因子からなる群を $\mathrm{Div}^0(C)$ で表す.

次に, 主因子を説明するために必要な命題を述べていく.

命題 1.16 ([Sil1, II, 1.1.]) C を射影曲線とする. このとき, $P \in C$ が非特異点ならば, $\overline{K}[C]_P$ は離散付値環である.

命題 1.16 より, C を非特異射影曲線とすれば, 自然に $\overline{K}(C)$ に付値が定めることができる. これを述べたのが, 次の定義である.

定義 C を射影曲線, $P \in C$ を非特異点とする. このとき, $\overline{K}[C]_P$ 上の**付値 (valuation)** を

$$\mathrm{ord}_P : \overline{K}[C]_P \longrightarrow \{n \in \mathbb{Z} \mid n \geq 0\} \cup \{\infty\};\ f \longmapsto \sup\{d \in \mathbb{Z} \mid f \in M_P^d\}$$

で定める. $f \neq 0$ ならば $\sup\{d \in \mathbb{Z} \mid f \in M_P^d\} < \infty$ である. また, 付値 ord_P を

$\mathrm{ord}_P(f/g) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ と定めることにより,

$$\mathrm{ord}_P : \overline{K}(C) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

と $\overline{K}(C)$ 上に延長する.

定義 C を非特異射影曲線とする. このとき,

$$\mathrm{div} : \overline{K}(C)^* \longrightarrow \mathrm{Div}(C);\ f \longmapsto \sum_{P \in C} \mathrm{ord}_P(f)(P)$$

と写像を定める. ここで, $\mathrm{div}(f) \in \mathrm{Div}(C)$ であることは, $f \in \overline{K}(C) \setminus \{0\}$ に対して f の極または零点となる C 上の点は高々有限個しか存在しないことからしたがう ([Sil1, II, 1. 1.]). $\mathrm{div}(f)$ を $\boldsymbol{f}$ **の因子 (divisor of** $\boldsymbol{f}$**)** という.

注意 各 P に対して ord_P が付値であるから, $\mathrm{div} : \overline{K}(C)^* \longrightarrow \mathrm{Div}(C)$ はアーベル群の準同型写像である.

次に, 非特異射影曲線上の因子が主因子であることの定義を行う.

定義 C を非特異射影曲線とする. このとき, C 上の因子 D が**主因子 (principal divisor)** であるとは, $D = \mathrm{div}(f)$ となる $f \in \overline{K}(C)^*$ が存在するときをいう.

命題 1.17 ([Sil1, II, 3.3.]) K を $\mathrm{char}(K) \neq 2$ である体, $e_1, e_2, e_3 \in K$ を相異なる元とする. このとき, K 上の楕円曲線

$$E : y^2 z = (x - e_1 z)(x - e_2 z)(x - e_3 z)$$

について, $P_1 = [e_1, 0, 1], P_2 = [e_2, 0, 1], P_3 = [e_3, 0, 1]$ とおけば, 以下が成り立つ.

(1) $\mathrm{div}(x - e_i z) = 2(P_i) - 2(O)$ $(i = 1, 2, 3)$.
(2) $\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(O)$.

証明 (1) まず $\mathrm{div}(x - e_1 z) = 2(P_1) - 2(O)$ を示す. $P \in E$ を任意にとる. 以下において, P が $P_1 = [e_1, 0, 1], O = [0, 1, 0], Q = [x_0, y_0, 1]$ $(x_0 \neq 0)$ であるときに, それぞれ $\mathrm{ord}_P(x - e_1 z)$ を求めていく.

$P = P_1$ のとき, 定義より

$$M_P = \left\{ F \in \overline{K}[E]_{(e_1,0)} \mid F(e_1, 0) = 0 \right\}$$

である. したがって, $(x-e_2)(x-e_3) \notin M_{(e_1,0)}$ に注意すれば,

$$\begin{aligned} M_{(e_1,1)} &= (x-e_1, y) \\ &= \left(\frac{y^2}{(x-e_2)(x-e_3)}, y \right) \\ &= (y) \end{aligned}$$

を得る. ただし, ここで $(x-e_1, y)$ は $x-e_1$ と y によって生成されるイデアルを表している. したがって,

$$\begin{aligned} \mathrm{ord}_{P_1}(x-e_1 z) &= \mathrm{ord}_{(e_1,0)}(x-e_1) \\ &= \mathrm{ord}_{(e_1,0)} \left(\frac{y^2}{(x-e_2)(x-e_3)} \right) \\ &= \mathrm{ord}_{(e_1,0)}(y^2) \\ &= 2 \end{aligned}$$

である.

$P = O$ のとき, 定義より

$$M_P = \left\{ F \in \overline{K}[E]_{(0,0)} \mid F((0,0)) = 0 \right\}$$

である. ここで, $y = 1$ より $z = (x-e_1 z)(x-e_2 z)(x-e_3 z)$ であるので,

$$z = \left\{ \frac{x^2 - (e_1+e_2+e_3)xz + (e_1e_2 + e_2e_3 + e_3e_1 z^2)}{1 + e_1e_2e_3z^2} \right\} \cdot x$$

である. また, $1 + e_1e_2e_3z^2 \notin M_{(0,0)}$ であるから,

$$M_{(0,0)} = (x)$$

である. これより,

$$\mathrm{ord}_O(x-e_2z) = \mathrm{ord}_O(x-e_3z) = -1$$

を得る. したがって,

$$\begin{aligned} \mathrm{ord}_O(x-e_1z) &= \mathrm{ord}_{(0,0)}(x-e_1z) \\ &= \mathrm{ord}_{(0,0)} \left(\frac{1}{(x-e_2z)(x-e_3z)} \right) \\ &= -2 \end{aligned}$$

である.

$P = Q$ のとき, 定義より

$$M_P = \left\{ F \in \overline{K}[E]_{(x_0,y_0)} \mid F((x_0, y_0)) = 0 \right\}$$

である. したがって, $(x - e_1 z) \notin M_{(x_0,y_0)}$ なので,

$$\mathrm{ord}_Q(x - e_1 z) = \mathrm{ord}_{(x_0,y_0)}(x - e_1) = 0$$

である. 以上より,

$$\mathrm{div}(x - e_1 z) = 2(P_1) - 2(O)$$

が示された.

P_2, P_3 に対しても, P_1 の場合と同様の議論により,

$$\begin{aligned} \mathrm{div}(x - e_2 z) &= 2(P_2) - 2(O), \\ \mathrm{div}(x - e_3 z) &= 2(P_3) - 2(O) \end{aligned}$$

が示される.

(2) div が準同型であるので,

$$\begin{aligned} \mathrm{div}(y) &= \frac{1}{2}\mathrm{div}(y^2) \\ &= \frac{1}{2}\mathrm{div}\big((x - e_1 z)(x - e_2 z)(x - e_3 z)\big) \\ &= \frac{1}{2}\left\{2(P_1) + 2(P_2) + 2(P_3) - 6(O)\right\} \\ &= (P_1) + (P_2) + (P_3) - 3(O) \end{aligned}$$

と計算できる. □

注意 命題 1.17 は 4.1 節で定理 4.3 (Complete 2-descent) を示すときに使われる. 定理 4.3 は 4.1 節における定理 4.1 (m-Descent) を $m = 2$ で適用することで示される. 命題 1.17 は定理 4.1 (4) における f_T の因子の状況を, $(x - e_i z)$ がみたしていることを主張している.

1.7 ヴェイユペアリング

この節では, ヴェイユペアリングを定義する. ヴェイユペアリングは $E[m] \times E[m]$ から μ_m への写像であり, 双線形性, 交代性, 非退化性, ガロア不変性, 全射性という性質をもつ. また, 楕円曲線 E/K に対し, $\mu_m \subset K^*$ が $E[m] \subset E(K)$ であるための必要条件であ

ることを復習する. この節を通して, m は $p = \mathrm{char}(K) > 0$ ならば $p \nmid m$ をみたす自然数とする.

定義 E/K を楕円曲線とする. このとき, 次の写像が定義できる.

$$e_m : E[m] \times E[m] \longrightarrow \mu_m;\ (S,T) \longmapsto \frac{g_T(X \oplus S)}{g_T(X)}.$$

ただし, ここで $g_T \in \overline{K}(E)$ と $X \in E$ は以下の条件をみたす.

- $f_T \circ [m] = g_T^m$ かつ $\mathrm{div}(f_T) = m(T) - m(O)$ をみたす $f_T \in \overline{K}(E)$ が存在する.
- $g_T(X) \neq 0$ かつ g_T は X, $X \oplus S$ 上で定義されている.

この楕円曲線 E と自然数 m から定まる写像 e_m を**ヴェイユペアリング (Weil pairing)** という.

注意 ヴェイユペアリングの定義において, 条件をみたす $f_T, g_T \in \overline{K}(E)$ の存在や, $X \in E$ に関する well-defined 性については [Sil1, III, 8.] を参照してほしい.

次の命題で述べるように, ヴェイユペアリング e_m は双線形性と非退化性をはじめとする良い性質をもっている.

命題 1.18 ([Sil1, III, 8.1.]) E/K を楕円曲線, e_m を付随するヴェイユペアリングとしたとき, 以下の性質が成り立つ.

(1) e_m は双線形である. すなわち, $S, T, S_1, S_2, T_1, T_2 \in E[m]$ に対して

$$e_m(S_1 \oplus S_2, T) = e_m(S_1, T)e_m(S_2, T),$$
$$e_m(S \oplus T_1, T_2) = e_m(S, T_1)e_m(S, T_2).$$

(2) e_m は交代的である. すなわち, $T \in E[m]$ に対して

$$e_m(T, T) = 1.$$

(3) e_m は非退化である. すなわち,

$$e_m(S', T) = 1\ (\forall S' \in E[m]) \Rightarrow T = O,$$
$$e_m(S, T') = 1\ (\forall T' \in E[m]) \Rightarrow S = O.$$

(4) e_m はガロア不変である. すなわち, $S, T \in E[m], \sigma \in G_K$ に対して

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma).$$

また, 次の命題で述べるように, ヴェイユペアリングは全射である.

命題 1.19 ([Sil1, III, 8.1.1.]) E/K を楕円曲線, e_m を付随するヴェイユペアリングとする. このとき, $e_m(S,T)$ が原始 m 乗根となる $S,T \in E[m]$ が存在する. よって, とくに $E[m] \subset E(K)$ ならば $\mu_m \subset K^*$ が成り立つ.

1.8 ガロアコホモロジー

この節では, ガロアコホモロジーについて復習する. ガロアコホモロジーとは, 副有限群の位相を考慮して定義された群コホモロジーである. 1.3 節で定義した G_K から E へのガロア作用により, E は副有限群 G_K の離散的ガロア加群となる. また, クンマー理論における同型写像 $\delta_K : K^*/(K^*)^m \longrightarrow \mathrm{Hom}(G_K, \mu_m)$ を定義する. この節は [NSW] を参考にした.

定義 M をアーベル群, G を副有限群とする.

(1) G が M に左から作用しているとき, M を**抽象的 G 加群 (abstract G-module)** という,
(2) G が M に左から連続的に作用しているとき, M を**離散的 G 加群 (discrete G-module)** という. ただし, M を離散位相による位相群として見る.

注意 G が有限群のとき, 抽象的 G 加群と離散的 G 加群は一致する. したがって, 離散的 G 加群は有限群の G 加群の一般化である. また, ガロアコホモロジーは有限群のコホモロジーに他ならない.

以降においてとくに断りがない場合, 副有限群 G に対して G 加群とは離散的 G 加群を表す.

定義 G を副有限群, M を G 加群とする. このとき,

$$M^G := \{x \in M \mid x^\sigma = x \ (\forall \sigma \in G)\}$$

を副有限群 G の M 係数 **0 次コホモロジー群 (0^{th}cohomology group)** という.

定義 G を副有限群, M を G 加群とする. このとき,

$$C^1(G,M) := \{\xi : G \longrightarrow M \mid \xi \text{ は } G \text{ から } M \text{ への連続写像 }\}$$

と定義し, $C^1(G,M)$ の元を G から M への **1 コチェイン (1-cochain)** という. ξ が 1-コ

チェインであるとき, $\sigma \in G$ に対して $\xi(\sigma)$ を ξ_σ で表す. また,

$$Z^1(G,M) := \{\xi \in C^1(G,M) \mid \xi_{\sigma\tau} = \xi_\sigma + (\xi_\tau)^\sigma \ (\forall \sigma, \tau \in G_K)\},$$
$$B^1(G,M) := \{\xi \in C^1(G,M) \mid \exists x \in M \text{s.t.}, \ \xi_\sigma = x^\sigma - x \ (\forall \sigma, \tau \in G_K)\}$$

と定義し, $Z^1(G,M)$ の元を **1 コサイクル (1-cocycle)**, $B^1(G,M)$ の元を **1 コバウンダリー (1-coboundary)** という. $B^1(G,M) \subset Z^1(G,M)$ であることが簡単に確かめられる. そして, $Z^1(G,M)$ の $B^1(G,M)$ による商群

$$H^1(G,M) := \frac{Z^1(G,M)}{B^1(G,M)}$$

を副有限群 G の M 係数 **1 次コホモロジー群 (1^{st}-cohomology group)** という.

次の命題は離散的 G 加群を考える上で基本的である.

命題 1.20 ([NSW, I, §1, 1.1.8.]) G を副有限群, M を抽象的 G 加群とする. このとき, 以下は同値である.

(1) M は離散的 G 加群である.
(2) 任意の $x \in M$ に対して, $G_x := \{\sigma \in G \mid x^\sigma = x\}$ は開部分群である.
(3) U が G の開部分群をすべて走るとき, $A = \bigcup A^U$ である.

注意 E を K 上の楕円曲線とする. このとき, 命題 1.20 (2) より, 1.3 節で定義した G_K から E への作用で E は離散的 G_K 加群となる.

次の命題は蛇の補題とよばれ, ホモロジー代数において基本的な命題である.

命題 1.21 (**蛇の補題**) R を環とし, 以下の図式

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{i_1} & M_2 & \xrightarrow{i_2} & M_3 \longrightarrow 0 \\ & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} \\ 0 & \longrightarrow & N_1 & \xrightarrow{j_1} & N_2 & \xrightarrow{j_1} & N_3 \end{array}$$

は R 加群の可換図式で, 各行は完全系列であるとする. このとき,

$$\mathrm{Ker}(\phi_1) \longrightarrow \mathrm{Ker}(\phi_2) \longrightarrow \mathrm{Ker}(\phi_3) \xrightarrow{\delta} \mathrm{Coker}(\phi_1) \longrightarrow \mathrm{Coker}(\phi_2) \longrightarrow \mathrm{Coker}(\phi_3)$$

を完全系列とする**連結準同型 (connecting homomorphism)** とよばれる R 加群の準同型 $\delta : \mathrm{Ker}(\phi_3) \longrightarrow \mathrm{Coker}(\phi_1)$ が存在する. ただし, ここで δ 以外の準同型は最初の可換図式から自然に定まる準同型である. また, δ は以下のように定義される.

$a_3 \in \mathrm{Ker}(\phi_3)$ に対し, $\phi_2 : M_2 \longrightarrow M_3$ の全射性から $i_2(a_2) = a_3$ となる $a_2 \in M_2$ が存在する. ここで $b_2 = \phi(a_2)$ とおけば, 図式の可換性より $j_2(b_2) = 0$ となるので, $b_2 = j_1(b_1)$ となる $b_1 \in N_1$ が存在する. この b_1 の $\mathrm{Coker}(\phi_1)$ における像を $\delta(a_3)$ と定める.

以下において, G を群, $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ を抽象的 G 加群の完全系列とする. すると, 全射性から完全系列

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \xi_A} & & \downarrow{\scriptstyle \xi_B} & & \downarrow{\scriptstyle \xi_C} & & \\ 0 & \longrightarrow & Z^1(G,A) & \xrightarrow{f\circ} & Z^1(G,B) & \xrightarrow{g\circ} & Z^1(G,C) & & \end{array}$$

が得られる. ただし, ここで ξ_A は $a \in A$ に対して

$$Z^1(G,A) \ni \xi_A(a) : G \longrightarrow A;\ \sigma \mapsto a^\sigma - a$$

により自然に定まる準同型であり, ξ_B, ξ_C についても同様である. この可換図式に対して蛇の補題を使えば, 完全系列

$$A^G \xrightarrow{f} B^G \xrightarrow{g} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{\tilde{f}} H^1(G,B) \xrightarrow{\tilde{g}} H^1(G,C)$$

を得る.

以上の考察をクルル位相による副有限群 G_K に適用することで, 次の命題が得られる.

命題 1.22 ([NSW, I, §3, 1.3.2.]) K を体, $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ を G_K 加群の完全系列とする. このとき, 写像 $\delta : C^{G_K} \longrightarrow H^1(G_K, A)$ を, $c \in C^{G_K}$ に対して

$$\xi_c : G_K \longrightarrow A;\ \sigma \longmapsto b^\sigma - b,$$
$$(\text{ただし, ここで } b \in B \text{ は } g(b) = c \text{ をみたす元})$$

と定める写像と, ξ_c を $H^1(G_K, A)$ の中の類に写す写像の合成で定義すれば,

$$0 \longrightarrow A^{G_K} \xrightarrow{f} B^{G_K} \xrightarrow{g} C^{G_K} \xrightarrow{\delta} H^1(G_K,A) \xrightarrow{\tilde{f}} H^1(G_K,B) \xrightarrow{\tilde{g}} H^1(G_K,C)$$

は完全系列である. とくに, 完全系列

$$0 \longrightarrow C^G/g(B^G) \xrightarrow{\tilde{\delta}} H^1(G_K,A) \xrightarrow{\tilde{f}} H^1(G_K,B)[\tilde{g}] \longrightarrow 0$$

を得る. ただし, $H^1(G_K,B)[\tilde{g}] := \mathrm{Ker}(\tilde{g})$.

次の命題が有名なヒルベルトの定理 90 である.

命題 1.23 (**ヒルベルトの定理 90**) ガロア拡大 L/K に対し, $H^1(G_{L/K}, L^*) = \{1\}$ である.

注意 命題 1.23 の証明は [NSW, VI, §2, 6.2.1.] が詳しい.

ヒルベルトの定理 90 を命題 1.22 用いることで, クンマー理論を示すことができる.

定理 1.24 (**クンマー理論**) m を $p = \mathrm{char}(K) > 0$ なら $p \nmid m$ である自然数, K を $\mu_m \subset K$ である体, λ_m を m 乗写像とする. このとき,

$$\begin{aligned} \delta_K : K^*/(K^*)^m &\longrightarrow \mathrm{Hom}(G_K, \mu_m); \\ b \bmod (K^*)^m &\longmapsto \xi_b : G_K \longrightarrow \mu_m;\ \sigma \mapsto \frac{\beta^\sigma}{\beta} \\ (\text{ただし, ここで } \beta \in \overline{K^*} &\text{は } \beta^m = b \text{ をみたす任意の元}) \end{aligned}$$

は群同型である.

証明 G_K 加群の完全系列

$$1 \longrightarrow \mu_m \longrightarrow \overline{K}^* \xrightarrow{\lambda_m} \overline{K}^* \longrightarrow 1$$

に命題 1.22 を用いることで, 完全系列

$$1 \longrightarrow K^*/(K^*)^m \xrightarrow{\delta_K} H^1(G_K, \mu_m) \longrightarrow H^1(G_K, \overline{K}^*)[\lambda_m] \longrightarrow 0$$

を得る. ここで, $\mu_m \subset K$ より $\mathrm{Hom}(G_K, \mu_m) = H^1(G_K, \mu_m)$ であることに注意する. すると, ヒルベルトの定理 90 より $\delta_K : K^*/(K^*)^m \longrightarrow \mathrm{Hom}(G_K, \mu_m)$ は同型である. □

定義 群同型 $K^*/(K^*)^m \longrightarrow H^1(G_K, \mu_m)$ を δ_K で表す.

次節では, とくに有限次クンマー拡大における分岐の様子を調べる.

1.9 有限次クンマー拡大

この節では, 有限次クンマー拡大に関して成り立つ内容を復習する. 巡回拡大となるクンマー拡大において, 素イデアルが分岐する必要十分条件が法 m で記述できる点が重要である. この節は [高木] の第 15 章を参考にした.

定義　K を $\mu_m \subset K$ である代数体, m を自然数とする. このとき, 体拡大 L/K が有限次の**クンマー拡大 (Kummer extension)** であるとは,

$$L = K(\sqrt[m]{a_1}, \ldots, \sqrt[m]{a_n})$$

となる $a_1, \ldots a_n \in K$ が存在するときをいう. また, L を K 上の m に関する**クンマー体 (Kummer field)** とよぶ.

例 1.25 以下の体拡大は有限次クンマー拡大である.

- 2 次拡大 $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$.
- 有理数 r と自然数 m に対し, $\mathbb{Q}(\sqrt[m]{r}, \zeta_m)/\mathbb{Q}(\zeta_m)$.

有限次クンマー拡大に関して, 以下の性質が成り立つ.

命題 1.26 [高木, 15 章, §1, 定理 1] K を $\mu_m \subset K$ である代数体, $L = K(\sqrt[m]{a})$ を K 上のクンマー体とする. このとき, L/K は高々指数が m の巡回拡大である.

注意　体のガロア拡大 L/K が高々指数が m であるとは, ガロア群 $G_{L/K}$ の任意の元が m ねじれ点となることである.

次の命題は, クンマー拡大が有限次アーベル拡大という枠組みの中で, 高々指数が m という条件で特徴づけられることを述べている.

命題 1.27 K を $\mu_m \subset K$ である代数体, L/K を高々指数が m の有限次アーベル拡大とする. このとき, L/K は m に関するクンマー拡大である. とくに, L/K が巡回拡大ならば

$$L = K(\sqrt[m]{a})$$

となる $a \in K^*$ が存在する.

クンマー拡大における素イデアルの分岐について, 次の命題が成り立つ.

命題 1.28 [高木, 15 章, §2, 定理 1] K を $\mu_m \subset K$ である代数体, $L = K(\sqrt[m]{a})$ を K 上のクンマー体とする. このとき, $\mathrm{ord}_{\mathfrak{p}}(m) = 0$ をみたす $\mathfrak{p} \in M_K^0$ に対して, 以下は同値である.

(1) $\mathfrak{p}$ は L/K で不分岐である.
(2) a の $\mathfrak{p}$ 成分の指数は m の倍数である.

注意　整数論に関する内容は [高木] や [Ono] を参照されたい.

1.10　環上の形式群

この節では, 可換環 R 上の形式群に関する基礎的な事項を復習する. この節で, R は可換環を表すものとする. この節は [Sil1, IV.2.] を参考にした.

定義　$F(X,Y) \in R[[X,Y]]$, $i(T) \in R[[T]]$ に対して 2 つ組 $\mathcal{F} = (F(X,Y), i(T))$ が R 上の**形式群 (formal group)** であるとは, 変数 X, Y, Z, T に対して, 次の条件をみたすときをいう.

(1) $F(X,Y) = X + Y +$ (次数が 2 以上の項).
(2) $F(X, F(Y,Z)) = F(F(X,Y), Z)$.
(3) $F(X,Y) = F(Y,X)$.
(4) $F(i(T), T) = F(T, i(T)) = 0$.
(5) $F(X,0) = X,\ F(0,Y) = Y$.

注意　(1), (2), (3), (5) をみたすとき, $F(i(T),T) = F(T,i(T)) = 0$ をみたす $i(T) \in R[[T]]$ はただ一つに定まる. 条件 (4) は逆元の存在とその一意性に対応している.

とくに R が完備付値環である場合, R 上の形式群から R の極大イデアルに群演算が誘導される. これを述べたのが次の定義である.

定義　R を完備付値環, $\mathcal{M}$ を R の極大イデアル, k を剰余体とする. $\mathcal{F} = (F, i)$ を R 上の形式群とする. このとき, 以下のように $\mathcal{F}(\mathcal{M})$ と $\mathcal{F}(\mathcal{M}^n)$ に群構造を定義する:

(1) $\mathcal{F}(\mathcal{M})$ は集合として $\mathcal{M}$ と等しいものとし, また $\mathcal{M}$ に演算 $\oplus_{\mathcal{F}}$ と $\ominus_{\mathcal{F}}$ を, $x, y \in \mathcal{M}$ に対して

$$x \oplus_{\mathcal{F}} y = F(x,y),$$
$$\ominus_{\mathcal{F}} x = i(x)$$

により定義する. すると, 形式群の定義より, $\mathcal{F}(\mathcal{M})$ は $\ominus_{\mathcal{F}} x$ を x の逆元とする群となる. この群 $\mathcal{F}(\mathcal{M})$ を**形式群から誘導される群 (the group associated to an formal group** という.
(2) 自然数 n に対し, $\mathcal{F}(\mathcal{M}^n)$ を集合として $\mathcal{M}^n$ に等しく, 演算を $\oplus_{\mathcal{F}}$ で入れることによ

り定義する.

形式群から誘導される群について, 次の重要な命題が成り立つ.

命題 1.29 ([Sil1, IV, 3.2.]) R を完備付値環, $\mathcal{M}$ を R の極大イデアル, k を剰余体とする. このとき, 以下が成り立つ.

(1) 任意の自然数 n に対して $\mathcal{F}(\mathcal{M}^n) \triangleleft \mathcal{F}(\mathcal{M}^{n+1})$ であり, 自然に定まる準同型

$$\mathcal{F}(\mathcal{M}^n)/\mathcal{F}(\mathcal{M}^{n+1}) \longrightarrow \mathcal{M}^n/\mathcal{M}^{n+1};\ x \longmapsto x$$

は全単射である.

(2) $x \in \mathcal{F}(\mathcal{M})$ に対し, x の位数 $\mathrm{ord}(x)$ が有限位数であるとする. このとき, 以下が成り立つ.

（a）$p = \mathrm{char}(k) > 0$ のとき, ある非負整数 $n \in \mathbb{Z}$ が存在して $\mathrm{ord}(x) = p^n$.

（b）$\mathrm{char}(k) = 0$ のとき, $x = 0$.

注意 楕円曲線から誘導される形式群 $\hat{E}$ の存在を 2.1 節で証明する. そして, $\hat{E}$ に命題 1.29 を適用し, $E(K)$ のねじれ部分群を求める上で有用である定理 2.6 を導く.

1.11 アーベル群上の高さ関数と降下定理

この節では, アーベル群 A と自然数 m に対して, A 上の m に関する高さ関数を定義する. そして, アーベル群に対する降下定理を, m に関する高さ関数を用いて記述する. 降下定理によって, アーベル群が有限生成であることを示す方針を得る. この節は [Sil1, VIII.3.] を参考にした.

定義 A をアーベル群, m を 2 以上の自然数とする.

(1) このとき, 写像 $h : A \longrightarrow \mathbb{R}$ が **m に関する高さ関数 (height function with respect to m)** であるとは, 以下の条件をみたすときをいう.

（a）$Q \in A$ に対し, 各 $P \in A$ において

$$h(P+Q) \leq 2h(P) + C_1$$

をみたす Q, A のみによる定数 $C_1 = C_1(Q, A)$ が存在する.

（b）各 $P \in A$ において

$$h(mP) \geq m^2 h(P) - C_2$$

をみたす A のみによる非負定数 $C_2 = C_2(A)$ が存在する.

（c）任意の定数 C_3 に対し, 集合

$$\{P \in A \mid h(P) \leq C_3\}$$

は有限集合である.

(2) このとき, 写像 $h : A \longrightarrow \mathbb{R}$ が A 上の**高さ関数 (height function)** であるとは, ある 2 以上の自然数 m に対して, h が m に関する高さ関数であるときをいう.

これらの用語の元で, アーベル群に対する降下定理は次のように述べられる.

定理 1.30 (**降下定理**) A をアーベル群, m を 2 以上の自然数, 写像 $h : A \longrightarrow \mathbb{R}$ を m に関する高さ関数とする. このとき A/mA が有限群ならば, A は有限生成アーベル群である.

注意 定理 1.30 より, 与えられたアーベル群 A が有限生成であることを示す方針の一つは

(i) A/mA は有限群.

(ii) A に m に関する高さ関数が存在する.

をみたす 2 以上の自然数 m を見つけることである. 第 3 章の 3.3 節で, 降下定理を $A = E(\mathbb{Q})$ として適用し, $E(\mathbb{Q})$ が有限生成アーベル群であるというモーデルの定理を示す. 3.1 節で示す弱モーデル・ヴェイユの定理が (i) に, そして 3.2 節で示す命題 3.12 が (ii) に対応する内容である.

2　モーデル・ヴェイユ群のねじれ部分群

この章では, まず楕円曲線 E から誘導される形式群 $\hat{E}$ を定義する. $\hat{E}$ の定義は 2.1 節で, E と同型な楕円曲線 E' における議論を通してなされる. 本論文では E と E' の間に同型写像 $\phi : E \longrightarrow E'$ と $\psi : E' \longrightarrow E$ を定義し, どちらの平面で議論が行われているかを明示した. 次に, 完備離散付値体 K 上の楕円曲線 E から, K の剰余体上の楕円曲線 $\tilde{E}/k$ に対して定まる還元写像を定義する. 還元写像は準同型であり, その重要な点は還元写像の核が $\hat{E}$ から誘導される群 $\hat{E}(\mathcal{M})$ と群同型となることである (2.2 節の命題 2.5). 命題 2.5 を用いて, 楕円曲線のねじれ部分群の性質が形式群の一般論から導き出される (2.3 節の定理 2.6). そして, 定理 2.6 を用いて, 楕円曲線のモーデル・ヴェイユ群のねじれ部分群の計算を行った. この章は [Sil1] における IV 章 1 節, VII 章 2 節, VII 章 3 節を参考にした.

2.1　楕円曲線から誘導される形式群

変数 x, y, ξ により斉次式で表された K 上の楕円曲線

$$E : y^2\xi + a_1xy\xi + a_3y\xi^2 = x^3 + a_2x^2\xi + a_4x\xi^2 + a_6\xi^3$$

を考える. そして, 変数 z, w, η により斉次式で表された曲線 E' を

$$E' : \eta^2w - a_1z\eta w - a_3\eta w^2 = z^3 + a_2z^2w + a_4zw^2 + a_6w^3$$

とおく. ここで, $\phi : E \longrightarrow E'$ を

$$[x, y, \xi] \longmapsto \begin{cases} \left[-\dfrac{x}{y}, 1, -\dfrac{\xi}{y}\right] & y \neq 0 \text{ のとき,} \\ [x, 0, \xi] & y = 0 \text{ のとき.} \end{cases}$$

で定めると, ϕ は同型写像である. 実際, $\psi : E' \longrightarrow E$ を

$$[z, \eta, w] \longmapsto \begin{cases} \left[\dfrac{z}{w}, -\dfrac{\eta}{w}, 1\right] & w \neq 0 \text{ のとき,} \\ [0, 1, 0] & w = 0 \text{ のとき.} \end{cases}$$

により定めれば, ψ は ϕ の逆写像である. また ϕ により, E において $\xi = 1$ としたアフィン平面は E' において $\eta = 1$ としたアフィン平面が対応している. $\eta = 1$ とした E' のアフィン平面の方程式は

$$E' : w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3$$

である. ここで, 左辺の w を次々に右辺の w に代入することで, $w = w(z) \in K[[z]]$ で $[z, 1, w(z)]$ という E' の解が得られそうである. このアイディアが実際に成り立つことを意味しているのが, 次の命題である.

命題 2.1 ([Sil1, IV, 1.1.]) K を体, $a_1, \ldots, a_6 \in K$ とし,

$$S = \begin{cases} \mathbb{Z}[a_1, \ldots, a_6] & \mathrm{char}(K) = 0 \text{ のとき}, \\ \mathbb{F}_p[a_1, \ldots, a_6] & p = \mathrm{char}(K) > 0 \text{ のとき}. \end{cases}$$

とおく. また,

$$\begin{array}{ll} f_1(z, w) & := z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 z w^2 + a_6 w^3, \\ f_{m+1}(z, w) & := f_m(z, f_1(z, w)) \ (m \in \mathbb{N}), \\ g_1(z) & := f_1(z, 0), \\ g_m(z) & := f_m(z, 0) \ (m \in \mathbb{N}) \end{array}$$

と帰納的に定義し,

$$w(z) = \lim_{m \to \infty} g_m(z)$$

とする. このとき, 以下が成り立つ.

(1) $w(z) \in S[[z]]$ である. さらに, 自然数 m に対し, g_m を z^3 で括って

$$g_m(z) = z^3\{A_{0,m} + \cdots + A_{m,m} z^m + (\text{次数が } m+1 \text{ 以上の項})\}$$
$$(A_{0,m}, \ldots, A_{m,m} \in S)$$

と書いたとき, 任意の自然数に対して,

$$w(z) = z^3\{A_{0,m} + A_{1,m} z + \cdots + A_{m,m} z^m + (\text{次数が } m+1 \text{ 以上の項})\}$$

である.

(2) $w(z) = f(z, w(z))$ である. さらに, $w(z)$ は $S[[z]]$ の中でこの関係式をみたすただ一つの元である.

命題 2.1 は次のヘンゼルの補題を用いて示される.

補題 2.2 (**ヘンゼルの補題**) ([Sil1, IV, 1.2.]) R をイデアル $I \subset R$ による完備離散付値環とし, $n \in \mathbb{N}$, $a \in R$, $F(w) \in R[w]$ は

$$F(a) \in I^n \text{かつ } F'(a) \in R^*$$

をみたすとする. このとき, $\alpha \equiv F'(a) \bmod I$ をみたす $\alpha \in R^*$ に対して,

$$w_0 := a,$$
$$w_{m+1} := w_m - \frac{F(w_m)}{\alpha} \ (m \in \mathbb{Z},\ m \geq 0)$$

と R 数列 $\{w_m\}_{m=0}^{\infty}$ を帰納的に定義すると, 以下が成り立つ.

(1) $b := \lim_{m\to\infty} w_m$ は以下をみたす R の元である.
  (a) $F(b) = 0$.
  (b) $w_m \equiv w_{m+1} \bmod I^{m+n}$ $(\forall m \in \mathbb{Z},\ m \geq 0)$.
    とくに, $b \equiv a \bmod I^n$.

(2) R が整域なら, (1) における b は一意的に定まる.

ヘンゼルの補題は帰納法により示されるが, [Sil1, IV, 1.2.] で詳しく述べられているため, ここでは証明を省略する.

ヘンゼルの補題を用いて命題 2.1 を証明する. ここで,

$$R = S[[z]], \qquad I = (z), \qquad n = 3,$$
$$F(w) = f_1(z, w) - w, \qquad a = 0, \qquad \alpha = -1$$

ととれば,

$$F(a) = z^3 \in I^3, \qquad F'(a) = -1 + a_1 z + a_2 z^2 \in R^*,$$
$$F'(a) = -1 \in R^*, \qquad w_0 = 0, \qquad w_m = g_m(z)$$

を得る. そして, $f_{m+1}(z, w) = f_1(z, f_m(z, w))$ $(\forall m \in \mathbb{Z},\ m \geq 0)$ であることに注意すれば,

$$\begin{aligned} -\frac{F(g_m(z))}{\alpha} &= F(g_m(z)) \\ &= f_1(z, g_m(z)) - g_m(z) \\ &= f_1(z, f_m(z, 0)) - g_m(z) \\ &= f_{m+1}(z, 0) - g_m(z) \\ &= g_{m+1}(z) - g_m(z) \end{aligned}$$

となるので, g_m はヘンゼルの補題における w_m の条件をみたす. 以上により, 命題 2.1 が示された.

命題 2.1 (1) から, 楕円曲線

$$E' : w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 z w^2 + a_6 w^3$$

が与えられたとき,

$$w(z) = z^3\left(1 + A_1 z + A_2 z^2 + \cdots\right) \in S[[z]]$$

というべき級数の元が誘導されることが分かった. さらに, 命題 2.1 (2) から, E' をべき級数体 $K((z))$ 上の楕円曲線と見ることで,

$$[z, 1, w(z)] \in E'(K((z)))$$

を得る. すると, ϕ の逆写像 ψ により $[z, 1, w(z)]$ を写すことで $E(K((z)))$ の元を得ることができる. したがって, $\psi([z, 1, w(z)])$ の z 変数のべき級数の形で書かれた x 座標と y 座標が重要である.

定義 E/K を楕円曲線, $w(z) \in S[[z]]$ を E から誘導されるべき級数とする. このとき

$$x(z) := \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 + \cdots,$$
$$y(z) := -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + \cdots$$

と定義し, ***x* と *y* に関するローラン級数 (Laurent series for *x*, and *y*)** という.

以下で, 楕円曲線 E から形式群が誘導されることを, x と y に関するローラン級数を用いて示す. 変数 z_1, z_2 に対して,

$$P = [z_1, 1, w(z_1)],\ Q = [z_2, 1, w(z_2)] \in E'$$

とおく. さらに, $F(z_1, z_2) \in S((z_1, z_2))$ を

$$P \oplus' Q = [F(z_1, z_2), 1, w(F(z_1, z_2))]$$

となるように定める. ただし, ここで $\oplus'$ は E' 上の群演算である. すると,

$$\psi(P) = \left[\frac{z_1}{w(z_1)}, -\frac{1}{w(z_1)}, 1\right] = [x(z_1), y(z_1), 1]$$

より

$$\psi(\ominus' P) = \ominus\psi(P) = [x(z_1), -y(z_1) - a_1 x(z_1) - a_3, 1]$$

であるから,

$$\begin{aligned}\ominus' P &= \phi\left([x(z_1), -y(z_1) - a_1 x(z_1) - a_3, 1]\right) \\ &= \left[\frac{x(z_1)}{y(z_2) + a_1 x(z_1) + a_3}, 1, \frac{1}{y(z_2) + a_1 x(z_1) + a_3}\right]\end{aligned}$$

となる. したがって, ここで

$$i(z_1) = \frac{x(z_1)}{y(z_2) + a_1 x(z_1) + a_3}$$

とおけば, 楕円曲線がアーベル群であることより, 2 つ組 $(F(z_1, z_2), i(z_1))$ は形式群であるための条件 (3), (4) をみたす. したがって, $(F(z_1, z_2), i(z_1))$ が形式群であることをいうには, 次の主張を示せば十分である.

主張 2.3 上で定義した $F(z_1, z_2)$ と $i(z_1)$ について,

- $F(z_1, z_2) = z_1 + z_2 +$ (次数が 2 以上の項).
- $i(z_1) \in S[[z_1]]$.

が成り立つ.

主張の証明 L を P, Q を通る直線とすれば,

$$L : w = \lambda z + \upsilon,\ \lambda = \frac{w(z_1) - w(z_2)}{z_1 - z_2},\ \upsilon = w(z_1) - \lambda z_1$$

である. ここで, $w(z) = z^3 \left(A_0 + A_1 z + A_2 z^2 + \cdots\right)$ より,

$$\lambda = \sum_{n=3}^{\infty} A_{n-3} \frac{z_2^n - z_1^n}{z_2 - z_1} = \sum_{n=3}^{\infty} A_{n-3} \left(\sum_{i=0}^{n-1} z_2^{n-1-i} z_1^i \right)$$

であるから, $\lambda = \lambda(z_1, z_2) \in S[[z_1, z_2]]$ の次数は 2 以上である. また,

$$\upsilon = w(z_1) - \lambda(z_1, z_2) z_1$$

と定めていたので, $\upsilon = \upsilon(z_1, z_2) \in S[[z_1, z_2]]$ の次数も 2 以上である.

次に, R を直線 L と E' の交点として $R = [z_3, 1, w_3]$ とおく. $i(z_1)$ を調べるために, まず $z_3 = z_3(z_1, z_2)$ を調べていく. z_3 を z_1, z_2 で表すため, λ, υ を定数と見て

$$G(z) = f(z, \lambda z) - \lambda z + \upsilon$$

とおく. ただし,

$$f(z, w) := z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 z w^2 + a_6 w^3$$

である. すなわち, f は E' をアフィン平面の式で表したときの右辺である. すると, λ, υ のとり方と $(z_3, w_3) \in E'$ より, $G(z)$ の根は z_1, z_2, z_3 である. ここで,

$$H(z) = \prod_{i=1}^{3} (z - z_i) = z^3 + \alpha_1 z^2 + \alpha_2 z^1 + \alpha_3$$

とおく. すると, $G(z)$ を計算し, z_2 の係数を比較することにより,

$$\alpha_1 = \frac{a_1 + a_3\lambda^2 + a_2\upsilon + 2a_4\lambda\upsilon + 3a_6\lambda^2\upsilon}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \tag{2.1}$$

を得る. $\lambda = \lambda(z_1, z_2)$ と見て, 式 (2.1) の分母を

$$g(z_1, z_2) = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3$$

とおけば, $\lambda(z_1, z_2)$ の次数は 2 以上であったので $g(z_1, g_2)^{-1} \in S[[z_1, z_2]]$ である. したがって, 式 (2.1) より

$$\alpha_1 = \alpha_1(z_1, z_2) \in S[[z_1, z_2]]$$

を得る. また, 式 (2.1) の分子に注意すれば, $\alpha_1(z_1, z_2)$ の次数は 2 以上である. ここで, 解と係数の関係より

$$z_1 + z_2 + z_3 = -\alpha_1$$

であるから,

$$z_3 = -z_1 - z_2 - \underbrace{\alpha_1(z_1, z_2)}_{\text{次数が 2 以上}} \in S[[z_1, z_2]] \tag{2.2}$$

を得る. 以上により, $R = [-z_1 - z_2 - \alpha_1(z_1, z_2), 1, w_3]$ を得た. ここで, $F(z_1, z_2) = i(z_3)$ であるから, $F(z_1, z_2)$ を調べるには, $i(z_1)$ のべき級数表示を求めればよい. $z = z_1$ と変数をおき直すと,

$$\begin{aligned} i(z) &= \frac{x(z)}{y(z) + a_1x(z) + a_3} \\ &= \left(\frac{1}{z^2} - \frac{a_1}{z} - \cdots\right) \Big/ \left(-\frac{1}{z^3} + \frac{2a_1}{z^2} + \cdots\right) \\ &= \frac{-z + a_1z^2 + \cdots}{1 - 2a_1z + \cdots} \\ &= -z + (\text{次数が 2 以上の項}) \end{aligned}$$

となる. よって, $i(z_1) \in S[[z_1]]$ である. また, 式 (2.2) より

$$\begin{aligned} F(z_1, z_2) &= i(z_3(z_1, z_2)) \\ &= i(-z_1 - z_2 - \alpha_1(z_1, z_2)) \\ &= z_1 + z_2 + \alpha_1(z_1, z_2) + (\text{次数が 2 以上の項}) \end{aligned}$$

となるが, $\alpha_1(z_1, z_2)$ の次数は 2 以上であったから,

$$F(z_1, z_2) = z_1 + z_2 + (\text{次数が } 2 \text{ 以上の項})$$

と書けている. 以上により, 主張 2.3 が証明された. □

定義 楕円曲線 E に対して, 上記によって得られた形式群を $\hat{E}$ で表し, **楕円曲線から誘導される形式群 (the formal group associated to an elliptic curve)** という.

2.2 還元写像

この節では, 楕円曲線の還元写像を定義し, その性質を調べる. 還元写像は群準同型であり, 自然に完全系列が得られる. そして, 還元写像の核は $\hat{E}$ から誘導される群 $\hat{E}(\mathcal{M})$ と同型になる. この 2 つの結果を示すことが本節の目標である. この節を通して, K を完備離散付値体, $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ を K の正規離散付値, R を K の離散付値環, $\mathcal{M}$ を R の極大イデアル, k を R の剰余体とする. また, $a \in R$ に対し, $\tilde{a}$ で $a \bmod \mathcal{M}$ を表す.

定義 楕円曲線 E/K で, ワイエルシュトラス方程式の係数がすべて R の元であるものを考える:

$$E/K : y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x^2 + a_6 \ (a_i \in R).$$

このとき, E の係数をすべて $\mathcal{M}$ を法とすることで, k 上の曲線 $\tilde{E}/k$ が定まる:

$$\tilde{E}/k : y^2 + \tilde{a}_1xy + \tilde{a}_3y^2 = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x^2 + \tilde{a}_6 \ (\tilde{a}_i \in k).$$

この曲線 $\tilde{E}/k$ を, E/K から定まる**還元曲線 (reduced curve)** という. そして, $E(K)$ から $\tilde{E}(k)$ へ自然に定まる写像

$$E(K) \longrightarrow \tilde{E}(k);\ P = [x, y, z] \longmapsto \tilde{P} := [\tilde{x}, \tilde{y}, \tilde{z}]$$

を**還元写像 (reduction map)** という. ただし, x, y, z はすべて R の元で, かつ x, y, z のいずれか一つは R^* の元となるよう斉次座標を選ぶ.

注意 $P = [x, y, z] \in E(K)$ を還元写像で写すときの, 斉次座標のとり方に関する条件は $\min\{v(x), v(y), v(z)\} = 0$ と述べても同じことである. また, 還元写像は非特異射影曲線から射影曲線への写像であるので well-defined である.

以下において, 楕円曲線 E/K が R 上で定義されていることを E/R で表す. ただし, 楕円曲線 E が ***R* 上で定義されている**とは, ワイエルシュトラス方程式の係数がすべて R の元であることを意味する.

注意　楕円曲線 E/R に対して, その還元曲線は楕円曲線とは限らない. 例えば $\mathbb{Q}_p$ 上の楕円曲線 $E_A : y^2 = x^3 + Ax$ の判別式は例 1.4 より -2^6A^3 であるので,

$$\widetilde{E_A}\text{は楕円曲線} \Leftrightarrow \mathrm{ord}_p(2A) = 0$$

である.

定義　楕円曲線 E/R に対し,

$$E_1(K) := \{P \in E(K) \mid \tilde{P} = \tilde{O}\}$$

と定義する.

命題 2.4 ([Sil1, VII, 2.1.])　E/R を楕円曲線に対し, E から定まる還元曲線 $\tilde{E}/k$ が楕円曲線であるとする. このとき, 以下が成り立つ.

(1) 還元写像は準同型である.
(2) 還元写像から定まる系列

$$0 \longrightarrow E_1(K) \longrightarrow E(K) \longrightarrow \tilde{E}(k) \longrightarrow 0$$

は完全系列である.

証明　(1) $\tilde{E}/k$ が楕円曲線であるので, 定義より還元写像は準同型である.
(2) 定義より, E_1 は還元写像の核であるので, 還元写像が全射であることを示せばよい.

$$f(X,Y) := Y^2 + a_1XY + a_3 - (X^3 + a_2X^2 + a_4X + a_6) \in R[X,Y],$$
$$\tilde{f}(X,Y) := (x,y) := Y^2 + \widetilde{a_1}XY + \widetilde{a_3} - (X^3 + \widetilde{a_2}X^2 + \widetilde{a_4}X + \widetilde{a_6}) \in k[X,Y]$$

とおき, 任意の $Q \in \tilde{E}(k)$ をとる. そして, $Q = [x,y,z]$ を $\min\{v(x), v(y), v(z)\} = 0$ となるよう斉次座標を選ぶ. ここで, k の中で $z = 0$ なら, $\widetilde{O} = Q$ なので, $z \neq 0$ としてよい. すると, いま k が R の $\mathcal{M}$ による剰余体であることに注意すれば, $z_1 \in k$ に対して

$$z_1 \neq 0 \Leftrightarrow z_1 \notin \mathcal{M} \Leftrightarrow z_1 \in R^* \Leftrightarrow v(z_1) = 0$$

なので, $v(z) = 0$ である. したがって, x, y をそれぞれ $x/z,\ y/z$ ととり直すことで

$$Q = [x,y,1]$$

としてよい. ここで,

$$x = \widetilde{x_0},\ y = \widetilde{y_0}\ (x_0, y_0 \in R)$$

と x_0, y_0 をおく. すると, Q が非特異点であるから

$$\text{(i) } \frac{\partial \tilde{f}}{\partial X}(\widetilde{x_0}, \widetilde{y_0}) \neq 0, \text{ または (ii) } \frac{\partial \tilde{f}}{\partial Y}(\widetilde{x_0}, \widetilde{y_0}) \neq 0$$

が成り立つ. まず, (i) が成り立つとして命題を示そう. ここで,

$$F(w) := f(w, y_0) \in R[w]$$

とおけば, $\widetilde{F(x)} = \tilde{f}(\widetilde{x_0}, \widetilde{y_0}) = \tilde{0}$ より

$$f(x_0, y_0) \in \mathcal{M}$$

を得る. 一方,

$$\widetilde{F'(x_0)} = \frac{\partial \tilde{f}}{\partial X}(\widetilde{x_0}, \widetilde{y_0}) \neq 0$$

であるので, $F'(x_0) \neq \mathcal{M}$, すなわち

$$F'(x_0) \in R^*$$

を得る. すると, ヘンゼルの補題より

- $F(b) = 0$,
- $b \equiv x_0 \bmod \mathcal{M}$

をみたす $b \in R$ が存在する. すると, $P := [b, y_0, 1] \in E(K)$ に対して,

$$\tilde{P} = [\tilde{b}, \widetilde{y_0}, \tilde{1}] = [\widetilde{x_0}, \widetilde{y_0}, \tilde{1}] = Q$$

となるので, 還元写像は全射である.

また, (ii) が成り立つときは $F(w) := f(x_0, w) \in R[w]$ とし, (i) と同様の議論を行うことで還元写像の全射性が示される. 以上により, 還元写像が全射であることが示された. □

次の命題は, $\hat{E}$ から誘導される群と $E_1(K)$ の関係を記述する重要な命題である.

命題 2.5 ([Sil1, VII, 2.2.]) E/K を R 上の楕円曲線とするとき, 以下が成り立つ.

$$\tau : \hat{E}(\mathcal{M}) \longrightarrow E_1(K);\ z \longmapsto [x(z), y(z), 1]$$

は群同型写像である.

証明　E から誘導される形式群の定義より,

$$\hat{E}(\mathcal{M}) \longrightarrow E'(K);\ z \longmapsto [z, 1, w(z)]$$

は群準同型である. ただし, E' は 2.1 節で定めた E と同型な楕円曲線である. また, 2.1 節における $\psi : E' \longrightarrow E$ を $E'(K)$ に制限することで, 群準同型

$$E'(K) \longrightarrow E(K);\ [z, 1, w(z)] \longmapsto [x(z), y(z), 1]$$

を得る. したがって, これらの合成

$$\hat{E}(\mathcal{M}) \longrightarrow E(K);\ z \longmapsto [x(z), y(z), 1]$$

は群準同型である. また, $z \in \mathcal{M}$ に対して $\tau(z) := [x(Z), y(z), 1]$ と定めれば,

$$\tau(z) = [-z, 1, -w(z)] = [-z, 1, -z^3(1 + \cdots)]$$

となるので, $\widetilde{\tau(z)} = [\tilde{0}, \tilde{1}, \tilde{0}] = \tilde{O}$ を得る. したがって,

$$\tau : \hat{E}(\mathcal{M}) \longrightarrow E_1(K);\ z \longmapsto [x(z), y(z), 1]$$

は well-defined な群準同型である.

次に τ が全単射であることを示す. τ の全単射性を示すには,

$$\omega : E_1(K) \longrightarrow \hat{E}(\mathcal{M});\ (x, y) \longmapsto -\frac{x}{y}$$

が well-defined であることをいえば十分である. 実際, これは次のようにして分かる. 変数 t に対して, E を $K[[t]]$ 上で定義された楕円曲線と見る. すると, E から誘導される形式群の定義より

$$\Lambda : \hat{E}(\mathcal{M}_t) \longrightarrow E(K((t)));\ g(t) \longmapsto (x(g(t)), y(g(t)))$$

と

$$\Upsilon : E(K((t))) \longrightarrow \hat{E}(\mathcal{M}_t);\ P(t) = (x(P(t)), y(P(t))) \longmapsto -\frac{x(P(t))}{y(P(t))}$$

は互いに逆写像である. ただし, ここで $\mathcal{M}_t$ は $K[[t]]$ の極大イデアルである. K が完備離散付値体であることに注意すれば, $z \in \mathcal{M}$ に対して $z = t$ と代入できるから, τ と ω は互いの逆写像となる.

以下で, ω が well-defined であることを示す. $P = [x, y, 1] \in E_1(K)$ を任意にとる. ここで $y = 0$ とすると, $\tilde{P} = [\tilde{x}, \tilde{0}, \tilde{1}] \neq \tilde{O}$ となり $P \in E_1$ に矛盾するので $y \neq 0$ で

ある．次に $-(x/y) \in \mathcal{M}$ であることを示す．$x_0, y_0, z_0 \in R$ を，$P = [x_0, y_0, z_0]$ で $\min\{\upsilon(x_0), \upsilon(y_0), \upsilon(z_0)\} = 0$ となるようにとる．すると，$\tilde{P} = [\tilde{0}, \tilde{1}, \tilde{0}]$ より

$$\widetilde{x_0} = \widetilde{0},\ \widetilde{y_0} = \tilde{1},\ \widetilde{z_0} = \tilde{0}$$

である．とくに，$x_0 \in \mathcal{M}, y_0 \notin \mathcal{M}$ であるから $\upsilon(x_0) > 0, \upsilon(y_0) = 0$．すると，

$$\frac{x}{y} = -\frac{\left(\frac{x_0}{z_0}\right)}{\left(\frac{y_0}{z_0}\right)} = \frac{x_0}{y_0}$$

より，

$$\upsilon\left(-\frac{x}{y}\right) = \upsilon(x_0) - \upsilon(y_0) = \upsilon(x_0) > 0$$

を得る．したがって，$-(x/y) \in \mathcal{M}$ であるのから ω の well-defined 性が示された．以上により，$\tau : \hat{E}(\mathcal{M}) \longrightarrow E_1(K)$ は群同型写像である． □

注意 次節における定理 2.6 は局所体上の楕円曲線 E/K に対して，特定の条件をみたす $m \in \mathbb{N}$ については，還元写像が埋め込み $E(K)[m] \hookrightarrow \tilde{E}(k)$ を誘導することを主張している．命題 2.4 と命題 2.5 は還元写像の単射性を示す部分で，形式群の一般論を適用するために用いられる．

2.3 モーデル・ヴェイユ群のねじれ部分群の計算例

この節では，まず局所体上の楕円曲線 E/K のねじれ部分群について考察する．特定の条件をみたす $m \in \mathbb{N}$ について，埋め込み $E(K)[m] \hookrightarrow \tilde{E}(k)$ の存在を主張する定理 2.6 が重要である．次に定理 2.6 を，楕円曲線 $E/\mathbb{Q}$ のねじれ部分群の計算に応用し，無限個の $\mathbb{Q}$ 有理点をもつ楕円曲線の例や，ねじれ部分群が $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である楕円曲線の例を計算した．

定理 2.6 ([Sil1, VII, 3.1.]) K を完備離散付値体，υ を K の正規離散付値，R を K の整数環，k を剰余体，p を k の標数とする．そして，E/K を R 上で定義された楕円曲線，$\tilde{E}/k$ を E の還元曲線とする．このとき，$p \nmid m$ をみたす自然数 m に対して，以下が成り立つ．

(1) $E_1(K)$ は位数が m の元をもたない．
(2) $\tilde{E}/k$ は楕円曲線，すなわち $\upsilon(\Delta_E) = 0$ であるとする．このとき，

$$E(K)[m] \longrightarrow \tilde{E}(k);\ P \longmapsto \tilde{P}$$

は単射準同型である.

証明 (1) $\hat{E}$ を E から誘導される形式群とする. すると, 命題 1.29 より $\hat{E}(\mathcal{M})$ のねじれ点の位数は p べきである. ところが, $p \nmid m$ であるから, $\hat{E}(\mathcal{M})$ に位数が m の元は存在しない. 一方, 命題 2.5 より $\hat{E} \cong E_1(K)$ であるから, $E_1(K)$ にも位数が m の元は存在しない.
(2) $\tilde{E}(k)$ が非特異なので, 命題 2.4 (2) より群準同型

$$E(K) \longrightarrow \tilde{E}(k);\ P \longrightarrow \tilde{P}$$

を得る. 任意の $P \in E(K)[m]$ をとる. このとき, $\tilde{P} = \tilde{O}$ ならば $P = O$ を示せば十分である. ここで, $\tilde{P} = \tilde{O}$ ならば $P \in E_1$ であるが, (1) より P の位数は p べきである. よって, $P \neq O$ とすると $p \nmid m$ に矛盾する. したがって, $P = O$ である. □

まず具体的に与えられた楕円曲線をとり扱うことで, 定理 2.6 がどのようにモーデル・ヴェイユ群のねじれ部分群の計算に使われるのか感覚をつかんでおこう.

例 2.7 ([Sil1, VII, 3.3.1.]) $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + 3$ に対し,

$$E(\mathbb{Q})_{\mathrm{tors}} = \{O\}$$

である.

証明 例 1.5 より, $\Delta_E = -2^4 3^5$ である. ここで, 各素数 p に対し, E を $\mathbb{Q}_p$ 上の楕円曲線と見れば, 各自然数 m に対して

$$E(\mathbb{Q})[m] \hookrightarrow E(\mathbb{Q}_p)[m]$$

という単射準同型がある. この埋め込みにより, $E(\mathbb{Q})$ のねじれ部分群の情報を, $E(\mathbb{Q}_p)$ のねじれ部分群を調べることで得ることができる. 完備離散付値体 $\mathbb{Q}_p$ の剰余体は $\mathbb{F}_p$ と同一視できるので, 定理 2.6 の条件をみたす素数 p に対して, $E(\mathbb{Q})[m]$ から $\tilde{E}(\mathbb{F}_p)$ への単射が存在する. いま述べたことを用いて, 任意の $m \in \mathbb{N}$ に対して $E(\mathbb{Q})[m] = \{O\}$ を証明しよう. 有限回の計算により,

$\tilde{E}(\mathbb{F}_5) = \{(1,2), (1,3), (2,1), (2,4), (3,0), \tilde{O}\}$,
$\tilde{E}(\mathbb{F}_7) = \{(1,2), (1,5), (2,2), (2,5), (3,3), (3,4), (4,2), (4,5), (5,3), (5,4), (6,3), (6,4), \tilde{O}\}$

が分かるので, $\#\tilde{E}(\mathbb{F}_5) = 6$, $\#\tilde{E}(\mathbb{F}_7) = 13$ を得る. すると, 定理 2.6 から

$$E(\mathbb{Q})[3] \hookrightarrow \tilde{E}(\mathbb{F}_7) \text{ より } E(\mathbb{Q})[3] = \{0\},$$
$$E(\mathbb{Q})[5] \hookrightarrow \tilde{E}(\mathbb{F}_7) \text{ より } E(\mathbb{Q})[5] = \{0\},$$
$$E(\mathbb{Q})[7] \hookrightarrow \tilde{E}(\mathbb{F}_5) \text{ より } E(\mathbb{Q})[7] = \{0\}$$

である. また, 任意の 7 以上の奇素数 l に対して,

$$E(\mathbb{Q})[l] \hookrightarrow \tilde{E}(\mathbb{F}_5) \text{ より } E(\mathbb{Q})[l] = \{0\}$$

である. したがって, $E(\mathbb{Q})_{\mathrm{tors}}$ に奇数の位数をもつねじれ点が存在しないことが示された. また, 命題 1.12 より

$$E(\mathbb{Q})[2] = \{O\}$$

であるので, $E(\mathbb{Q})_{\mathrm{tors}}$ に位数が偶数であるねじれ点は存在しない. 以上により, $E(\mathbb{Q})_{\mathrm{tors}} = \{O\}$ が示された.

注意 例 2.7 における楕円曲線 E は有理点 $(1, 2)$ をもつが, $E(\mathbb{Q})_{\mathrm{tors}} = \{O\}$ なので, $(1, 2)$ は無限位数の点である. したがって, $E(\mathbb{Q})$ が無限個の有理点をもつ.

次に定理 2.6 を用いて, 特定の形をした楕円曲線の族のねじれ部分群について考察する. 命題 2.8 における楕円曲線は合同数問題と関連する (1.1 節や [Kob] を参照). 命題 2.8 の証明を前半部分は [Sil1] で得られた結果を用いて, 後半部分は [Kob, I, §9, 17.] を参考にして行った.

命題 2.8 $\mathbb{Q}$ 上の楕円曲線 $E_D : y^2 = x^3 - D^2x$ $(D \in \mathbb{N})$ に対し,

$$E_D(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

が成り立つ.

証明 例 1.4 より $\Delta_{E_D} = -2^6D^6$ であるから, 命題 1.3 より, すべての $D \in \mathbb{N}$ に対して E_D は楕円曲線である. また, $x^3 - Dx$ は $x(x - D)(x + D)$ と因数分解されるから, 命題 1.12 より

$$E_D(\mathbb{Q})[2] = \{(0, 0), (D, 0), (-D, 0), O\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

である. $E_D(\mathbb{Q})[2]$ の元以外に $E_D(\mathbb{Q})$ にねじれ点が存在しないことを示そう. 以下, $E_D(\mathbb{Q})_{\mathrm{tors}}$ に位数が 2 より大きい元が存在すると仮定して矛盾を導く. $P \in E_D(\mathbb{Q})_{\mathrm{tors}}$ の位数を m とし, $m > 2$ であるとする. すると $E_D(\mathbb{Q})$ に 2 等分点が存在することから, 次のうち, いずれか一方は必ず成り立つ.

(1) $E_D(\mathbb{Q})_{\mathrm{tors}}$ は位数が奇素数である元 Q をもつ.
(2) $E_D(\mathbb{Q})_{\mathrm{tors}}$ は位数が 8 であるの元 Q をもつ.

(1), (2) のどちらの場合でも, Q で生成された $E_D(\mathbb{Q})_{\mathrm{tors}}$ の部分群を S とおき, $m = \#S$ と定める. すなわち, m は Q の位数である. 定理 2.6 から, $\gcd(p, m\Delta_{E_D}) = 1$ をみたす素数 p に対して単射 $E_D(\mathbb{Q})[m] \hookrightarrow \tilde{E}_D(\mathbb{F}_p)$ が存在する. したがって $\tilde{E}_D(\mathbb{F}_p)$ の位数が重要になるが, $x^3 - D^2X$ が奇関数であることに注目することで $\tilde{E}_D(\mathbb{F}_p)$ の個数について次が成り立つ.

補題 2.9 $p \equiv 3 \pmod 4$ をみたす素数 p に対して, $\#\tilde{E}_D(\mathbb{F}_p) = p + 1$ である.

補題の証明 記号 $\left(\frac{*}{p}\right)$ をルジャンドル記号とする. $f(x) = x^3 - D^2x$ とおくと,

$$\#\tilde{E}_D(\mathbb{F}_p) = 1 + 1 + \sum_{x \in \mathbb{F}_p^*} \left\{ 1 + \left(\frac{f(x)}{p} \right) \right\}$$

である. ここで最初の $+1$ は無限遠点 O の分, 続く $+1$ は $x = 0$ の分である. すると, $p \equiv 3 \bmod 4$ と f が奇関数であることより,

$$\left(\frac{f(-x)}{p} \right) = \left(\frac{-f(x)}{p} \right) = \left(\frac{-1}{p} \right) \cdot \left(\frac{f(x)}{p} \right) = (-1) \cdot \left(\frac{f(x)}{p} \right)$$

を得る. これより

$$\sum_{x \in \mathbb{F}_p^*} \left(\frac{f(x)}{p} \right) = 0$$

であるから, $\#\tilde{E}_D(\mathbb{F}_p) = p + 1$ を得る. 以上により, 補題 2.9 が示された □

命題 2.8 の証明に戻る. 定理 2.6 と補題 2.9 より, 素数 p が次の 3 つの条件

(a) $p \equiv 3 \pmod 4$.
(b) $\gcd(p, \Delta_E) = 1$.
(c) $\gcd(p, m) = 1$

をみたすなら, $p \equiv -1 \pmod m$ が成り立つことが分かった. この状況を用いて, $m = 8$, m は奇数かつ $3 \nmid m$, m は奇数かつ $3 \mid m$ の各場合において矛盾が生じることを示す. 以下で $a, b \in \mathbb{Z}$ と素数 p に対して p が $ak + b$ 型の素数であるとは, ある自然数 k があって $p = ak + b$ となるときをいう.

$m = 8$ とする. このとき,

$$\mathcal{P}_8 = \{p \mid p \text{ は } 8k+3 \text{ 型の素数で, かつ } \gcd(p, \Delta_E) = 1\}$$

とおけば, ディリクレの算術級数定理より $\mathcal{P}_8$ は無限集合である. したがって, とくに $p \in \mathcal{P}$ が存在する. p は条件 (a), (b), (c) をみたすから $p \equiv -1 \pmod 8$ である. ところが p は $8k+3$ 型 の素数なので, $4 \equiv 0 \pmod 8$ となって矛盾する.

次に, m は奇素数かつ $3 \nmid m$ とする. このとき,

$$\mathcal{P}_m = \{p \mid p \text{ は } 4mk+3 \text{ 型の素数で, かつ } \gcd(p, \Delta_E) = 1\}$$

とおけば, ディリクレの算術級数定理より $\mathcal{P}_m$ は無限集合である. したがって, とくに $p \in \mathcal{P}$ が存在する. このとき $\gcd(p, m) = 1$ である. 実際, $\gcd(p, m) = a > 1$ とすれば p は素数であるから $a = p$ であり, p が $4mk+3$ 型の素数であることから $p = 3$ を得る. しかし , これは $3 \nmid m$ に矛盾する. したがって, p は条件 (a), (b), (c) をみたすから $p \equiv -1 \pmod m$ である. ところが p は $4mk+3$ 型 の素数なので, $4 \equiv 0 \pmod m$ となって m が奇数であることに矛盾する.

最後に, m は奇素数かつ $3 \mid m$, すなわち $m = 3$ とする. このとき,

$$\mathcal{P}_3 = \{p \mid p \text{ は } 12k+31 \text{ 型の素数で, かつ } \gcd(p, 7\Delta_E) = 1\}$$

とおけば, ディリクレの算術級数定理より $\mathcal{P}_3$ は無限集合である. したがって, とくに $p \in \mathcal{P}$ が存在する. $\gcd(p, 3) = 1$ であるので, p は条件 (a), (b), (c) をみたす. よって $p \equiv -1 \pmod 3$ である. ところが p は $12k+31$ 型 の素数なので, $2^5 \equiv 0 \pmod 3$ となって矛盾する.

以上により, $E_D(\mathbb{Q})_{\text{tors}} = \{(0,0), (D,0), (-D,0), O\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が示された. □

注意 命題 2.8 は, はじめは $\gcd(21, D) = 1$ という条件を付けていたが, [Kob] を参考にディリクレの算術級数定理を用いて $\gcd(21, D) = 1$ という条件を外してある. なお, 同様の議論により,

$$E : y^2 = x^3 - Dx \ (D \in \mathbb{N}, D \notin \mathbb{Z}^2)$$

という楕円曲線の族に対し, $\#E(\mathbb{Q})_{\text{tors}} = 2, 4$ を示すことができる.

例 2.10 有理数体上の楕円曲線

- $y^2 = x^3 - 4x$.
- $y^2 = x^3 - 25x$.

- $y^2 = x^3 - 36x$.

のねじれ部分群は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ と同型である.

3　モーデルの定理

この章では, $E(\mathbb{Q})$ が有限生成アーベル群であるというモーデルの定理を証明する. 3.1 節で一般の代数体に対して弱モーデル・ヴェイユの定理を証明したのち, 3.2 節で $\mathbb{Q}$ 上の楕円曲線のモーデル・ヴェイユ群に 2 に関する高さ関数 (1.11 節) が存在することを示す. そして 3.3 節で, 3.1, 3.2 節で得た結果を用いてモーデルの定理を証明する. その後, モーデル・ヴェイユ群の階数の定義を行い, ねじれ部分群や階数に関して知られている結果や話題を少し述べる. この章は [Sil1] における VIII 章 1 節, VIII 章 2 節, VIII 章 4 節を参考にした.

3.1　弱モーデル・ヴェイユの定理

この節では, 代数体 K 上で定義された楕円曲線について, 弱モーデル・ヴェイユの定理を証明する. まず弱モーデル・ヴェイユの定理を証明する上で, $E[m] \subset E(K)$ を仮定して一般性を失わないことを示す. 次に, クンマーペアリング κ を定義し, κ を用いて m 倍写像で写した先が $E(K)$ の元となる E 上の点全体を K に添加した体 $K([m]^{-1}E(K))$ の性質を調べる (命題 3.7). そして, ディリクレの S 単数定理とイデアル類群の有限性を用いて, 特定の条件をみたす K 上の代数拡大は有限個しかないことを示す (定理 3.9). 最後に, 命題 3.7 と定理 3.9 を用いて, 次の弱モーデル・ヴェイユの定理を証明する.

定理 3.1 (**弱モーデル・ヴェイユの定理**) m を自然数, K を代数体, E/K を楕円曲線とする. このとき, $E(K)/mE(K)$ は有限集合である.

定理 3.1 を証明する上で $E[m] \subset E(K)$ を仮定して一般性を失わないことが次の二つの補題から分かる.

補題 3.2 m を自然数, K を代数体, E/K を楕円曲線, L を K 上の有限次ガロア拡大とする. このとき, $E(L)/mE(L)$ が有限集合ならば $E(K)/mE(K)$ も有限集合である.

証明　$G_{L/K}$ 加群の完全系列

$$0 \longrightarrow E(L)[m] \longrightarrow E(L) \xrightarrow{[m]} E(L) \longrightarrow 0$$

に蛇の補題を用いることで, 単射な連結準同型

$$\delta_E : E(K)/mE(K) \longrightarrow H^1(G_{L/K}, E(L)[m])$$

を得る. いま, 仮定より $\#G_{L/K} < \infty$ である. また, 命題 1.7 より

$$E(L)[m] \subset E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

なので, $\#H^1(G_{L/K}, E(L)[m]) < \infty$ である. 以上により, $\#E(K)/mE(K) < \infty$ である. □

補題 3.3 K を代数体, E/K を楕円曲線とする. このとき, $M = K(E[m])$ に対して, M/K は有限次ガロア拡大である.

証明 M/K が有限次拡大であることは, $\#E[m] < \infty$ よりしたがう. 次に, M/K がガロア拡大であることを示そう. K の標数が 0 なので, M/K が分離拡大であることはよい. M/K が正規拡大であることを示す. 任意の $\sigma \in G_K, P \in E[m]$ をとる. すると, m 倍写像の定義と E が K 上で定義されていることから,

$$[m](P^\sigma) = [m](P)^\sigma = O^\sigma = O$$

となるので $P^\sigma \in E[m]$ を得る. すると, M の定め方より $P^\sigma \in M$. 以上より $M^\sigma \subset K$ である. したがって, M/K が正規拡大であることが示された. □

補題 3.4 弱モーデル・ヴェイユの定理の証明において

$$E[m] \subset E(K)$$

を仮定して一般性を失わない.

証明 $E_1[m] \subset E_1(F)$ をみたす体 F 上の楕円曲線 E_1 に対し, $E_1(F)/mE_1(F)$ は有限集合であると仮定する. すると, 楕円曲線 E/K に対し,

$$M = K(E[m])$$

とおけば, 仮定より $E(M)/mE(M)$ は有限集合である. すると, 補題 3.3 より, 補題 3.2 を $L = M$ として適用できるので, $E(K)/mE(K)$ は有限集合である. □

定義 K を体, m を自然数, E/K を $E[m] \subset E(K)$ をみたす楕円曲線とする. このとき G_K 加群の完全系列

$$0 \longrightarrow E[m] \longrightarrow E \xrightarrow{[m]} E \longrightarrow 0$$

に蛇の補題を用いることで,

$$\delta_E : E(K) \longrightarrow H^1(G_K, E[m])$$

で $\mathrm{Ker}(\delta_E) = mE(K)$ となる連結準同型を得る. ここで $E[m] \subset E(K)$ に注意すれば, $H^1(G_K, E[m]) = \mathrm{Hom}(G_K, E[m])$ であるから, 写像

$$\kappa : E(K) \times G_K \longrightarrow E[m];\ (P, \sigma) \longmapsto Q^\sigma \ominus Q$$

が定義できる. ただし, ここで $Q \in E$ は $[m]Q = P$ をみたす E 上の点である. この写像 κ を**クンマーペアリング (Kummer pairing)** という.

クンマーペアリングについて, 次の性質が成り立つ.

命題 3.5 K を代数体, m を自然数, E/K は $E[m] \subset E(K)$ をみたす楕円曲線とする. このとき, 以下が成り立つ.

(1) クンマーペアリング $\kappa : E(K) \times G_K \longrightarrow E[m]$ は well-defined な双線形写像である.
(2) 準同型 $L_\kappa : E(K) \longrightarrow \mathrm{Hom}(G_K, E[m]);\ P \longmapsto \kappa(P, *)$ について,

$$\mathrm{Ker}(L_\kappa) = mE(K)$$

である.
(3) $L = K([m]^{-1}E(K))$ とおくとき, L/K はガロア拡大である.
(4) 準同型 $R_\kappa : G_K \longrightarrow \mathrm{Hom}(E(K), E[m]);\ \sigma \longmapsto \kappa(\sigma, *)$ について,

$$\mathrm{Ker}(R_\kappa) = G_{\overline{K}/L}$$

である.
(5) $\overline{\kappa} : E(K)/mE(K) \times G_{L/K} \longrightarrow E[m];\ (\overline{P}, \sigma) \longmapsto \kappa(P, \sigma)$ は well-defined な非退化双線形写像である. ただし, ここで $P \in E(K)$ に対し, $\overline{P}$ は $P \bmod mE(K)$ を表す.

証明 (1), (2) クンマーペアリングの定義より成り立つ.
(3) 任意の $Q \in E$ で $[m]Q \in E(K)$ をみたすものをとる. すると, $\sigma \in G_K$ に対して

$$[m](Q^\sigma) = [m](Q)^\sigma = [m]Q \in E(K)$$

であるから, L/K は正規拡大である. また, K の標数が 0 なので, L/K はガロア拡大である.
(4) $\sigma \in G_K$ に対し,

$$\begin{aligned}
\sigma \in \mathrm{Ker}(R_\kappa) &\iff \kappa(P, \sigma) = O\ (\forall P \in E(K)) \\
&\iff Q^\sigma = Q\ (\forall P \in E(K), \forall Q \in E, [m]Q = P) \\
&\iff Q^\sigma = Q\ (\forall Q \in [m]^{-1}E(K)) \\
&\iff \sigma \in G_{\overline{K}/L}
\end{aligned}$$

であるから, $\mathrm{Ker}(R_\kappa) = G_{\overline{K}/L}$ である.
(5) $G_{L/K} \cong G_{\overline{K}/K}/G_{\overline{K}/L}$ という同一視と (2), (4) よりしたがう. □

記号の復習を行う. 代数体 K に対し, $M_K, M_K^\infty, M_K^0, \mathcal{O}_K, I_K, \Delta_K$ で, それぞれ K の素点全体, K の無限素点全体, K の有限素点全体, K の整数環, K の分数イデアルからなる群, K の判別式を表す. また, $\mathfrak{p} \in M_k^0$ に対し, $\mathrm{ord}_\mathfrak{p} : I_K \longrightarrow \mathbb{Z} \cup \{\infty\}$ で $\mathfrak{p}$ の正規離散付値を表す. また, 楕円曲線 E/K の部分集合 A に対し, $K(A)$ で K に A の点を添加した体を表す.

例 3.6 ここで, 有理数体 $\mathbb{Q}$, $3 \in \mathbb{Z}$ に対して, 正規付値による計算例をあげておく

- $\mathrm{ord}_3(3) = 1,\ \mathrm{ord}_3(3^2) = 2,\ \mathrm{ord}_3(3^3) = 3,\ \cdots$
- $\mathrm{ord}_3(5^3 \cdot 7) = 0,\ \mathrm{ord}_3(3 \cdot 5^3 \cdot 7) = 1,\ \mathrm{ord}_3(3^2 \cdot 5^3 \cdot 7^2) = 2.$
- $\mathrm{ord}_3(3^{-1}) = -1,\ \mathrm{ord}_3(11 \cdot 17 \cdot 3^{-2}) = -2,\ \mathrm{ord}_3(7 \cdot 27^{-1}) = -3.$

定義 K を代数体, E を $\mathcal{O}_K$ 上で定義された楕円曲線とする. このとき, 自然数 m に対して

$$S_{E,m} := \{\mathfrak{p} \in M_K^0 \mid \mathrm{ord}_\mathfrak{p}(m) > 0\} \cup \{\mathfrak{p} \in M_K^0 \mid \mathrm{ord}_\mathfrak{p}(\Delta_E) > 0\} \cup M_K^\infty,$$

と定める.

注意 E が $\mathcal{O}_K$ 上で定義されているので, $\mathrm{ord}_\mathfrak{p}(\Delta_E) \geq 0$ である. $S_{E,m}$ は悪い素点を集めたものである.

命題 3.7 K を代数体, m を自然数, E/K は $E[m] \subset E(K)$ をみたす楕円曲線とする. E_0 を E と同型な $\mathcal{O}_K$ 上の楕円曲線とする. このとき, 以下が成り立つ.

(1) $L = K([m]^{-1}E(K))$ とおく. すると, L/K は
  (a) 指数が高々 m であるアーベル拡大,
  (b) $S_{E_0,m}$ の外不分岐
  をみたす体拡大である.
(2) $P \in E(K)$ に対して $K_P = K([m]^{-1}(P))$ とおく. すると, K_P/K は
  (a) 指数が高々 m である有限次アーベル拡大,
  (b) $S_{E_0,m}$ の外不分岐
  をみたす体拡大である.

証明 (1) まず (a) を示す. L/K がガロア拡大であることは命題 3.5 (3) よりしたがう. ま

た, 同命題 (5) より $G_{L/K}$ は $\mathrm{Hom}(E(K)/mE(K), E[m])$ に埋め込まれている. ここで, $E[m]$ は指数が高々 m であるので, $\mathrm{Hom}(E(K)/mE(K), E[m])$ の指数も高々 m である. したがって, $G_{L/K}$ の指数も高々 m である.

次に (b) を示す. $\mathfrak{p} \in M_K \setminus S_{E_0,m}$ を任意にとる. $M_K^\infty \subset S_{E_0,m}$ なので, $\mathfrak{p} \in M_K^0$ である. $\mathfrak{P}, L_\mathfrak{P}, M_\mathfrak{P}, k_\mathfrak{P}$ を, それぞれ $\mathfrak{p}$ の上にある L の素イデアル, $\mathfrak{P}$ による L の完備化, $L_\mathfrak{P}$ の極大イデアル, 剰余体とする. さらに, $I_\mathfrak{P}$ を L/K に関する惰性群とする. $Q \in [m]^{-1}E(K)$, $\sigma \in I_\mathfrak{P}$ を任意にとる. このとき, $\mathfrak{p}$ が L/K で不分岐であることを示すには, $I_\mathfrak{P} = \{0\}$ をいえばよい. すなわち, $Q^\sigma = Q$ を示せば十分である. ここで, 命題 1.14 より, E が R 上で定義されているとして一般性を失わない. したがって, E を $L_\mathfrak{P}$ 上の楕円曲線として見れば, $S_{E_0,m}$ のとり方より定理 2.6 が使えるので

$$E(L)[m] \hookrightarrow E(L_\mathfrak{P})[m] \hookrightarrow E(k_\mathfrak{P})$$

を得る. $P = Q^\sigma \ominus Q$ とおけば, $[m]Q \in E(K)$ より

$$\begin{aligned}[m]P &= [m](Q^\sigma \ominus Q) \\ &= [m]Q^\sigma - [m]Q \\ &= O\end{aligned}$$

となるので, $P \in E(L)[m]$ を得る. 一方, 還元写像で P を写せば, $\sigma \in I_\mathfrak{P}$ であるから

$$\tilde{P} = \tilde{Q^\sigma} \ominus \tilde{Q} = \tilde{O}$$

となる. 以上により, $P = O$, すなわち $Q^\sigma = Q$ が示された.

(2) K_P/K が有限次拡大であることは, 命題 1.15 の $\#[m]^{-1}(P) < \infty$ よりしたがう. 以下 K_P/K がガロア拡大であることを示す. $\sigma \in G_K$ と $Q \in E, [m]Q = P$ に対し, $P \in E(K)$ なので

$$[m](Q^\sigma) = [m]Q^\sigma = P^\sigma = P$$

である. したがって, $Q^\sigma \in [m]^{-1}(P)$ である. 以上より, K_P/K はガロア拡大である.

また, (1) の証明と同様の議論により, K_P/K は指数が高々 m である有限次アーベル拡大であり, かつ $S_{E_0,m}$ の外不分岐である. □

ここで, 整数論におけるディリクレの S 単数定理を復習する.

定義 K を代数体, $S \subset M_K$ を M_K^∞ を含む有限集合とする. このとき,

$$R_S := \{\alpha \in K \mid \mathrm{ord}_\mathfrak{p}(\alpha) \geq 0 \ (\forall \mathfrak{p} \in M_K \setminus S)\}$$

と定め, R_S^* の元を ***S* 単数 (*S*-unit)**, S 単数からなる集合 R_S^* を ***S* 単数群**という.

注意　$R_S^* = \{\alpha \in K^* \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0\ (\forall \mathfrak{p} \in M_K \setminus S)\}$ であるから, とくに $S = M_K^\infty$ のとき, R_S は K の整数環である. したがって, 次の命題 3.8 は, ディリクレの単数定理を S 単数群に関して一般化したものである. この命題の証明の詳細は [Lan, V, §1] や [Neu, I, §1, 11.7.] を参照してほしい.

命題 3.8 (**ディリクレの S 単数定理**) K を代数体, $S \subset M_K$ は M_K^∞ を含む有限集合とする. このとき,

$$R_S^* \cong \mu(K) \times \mathbb{Z}^{\#S-1}$$

が成り立つ. ただし, ここで $\mu(K)$ は K に含まれる 1 のべき根からなる群である.

注意　命題 3.8 において, $\mu(K)$ は有限群であるから, $\#S - 1$ が R_S^* の $\mathbb{Z}$ 階数である.

次の命題を用いて, 弱モーデル・ヴェイユの定理の証明が行われる.

命題 3.9 K を $\mu_m \subset K$ である代数体, m を自然数, $S \subset M_K$ は M_K^∞ を含む有限集合とする. このとき,

$$\mathcal{C}_m^S = \left\{L \subset \overline{K} \mid L/K \text{ は } [L:M] \text{ が } m \text{ を割る巡回拡大であり, かつ } S \text{ の外不分岐}\right\}$$

に対し, $\#\mathcal{C}_m^S < \infty$ が成り立つ.

証明　$\mathcal{C} = \mathcal{C}_m^S$ と略記し, $\mathcal{C}_m = \{L \subset \overline{K} \mid L/K \text{ は } [L:K] \leq m \text{ をみたす巡回拡大 }\}$ とおく. $\mathcal{C} \subset \mathcal{C}_m$ である. $\mu_m \subset K$ に注意すれば, 有限次クンマー拡大の理論より, 写像

$$\Psi : K^*/(K^*)^m \longrightarrow \mathcal{C}_m;\ a \longmapsto K(\sqrt[m]{a})$$

は全射である. 以下, 少し S を広げる細工を行う. Cl_K を K のイデアル類群とすれば, イデアル類群の有限性より, ある自然数 n と整イデアル $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ が存在して,

$$Cl_K = \langle [\mathfrak{a}_i] \mid i = 1, \ldots n \rangle$$

となる. ただし, ここで $[\mathfrak{a}_i]$ は $\mathfrak{a}_i$ の属するイデアル類を表し, 上式の右辺は $[\mathfrak{a}_1], \ldots [\mathfrak{a}_n]$ によって Cl_K が生成されていることを表している. ここで

$$S^+ = \{\mathfrak{p} \in M_K^0 \mid \text{ある } i = 1, \ldots, n \text{ で } \mathfrak{p} \text{ は } \mathfrak{a}_i \text{を割る }\} \cup \{\mathfrak{p} \in M_K^0 \mid \mathrm{ord}_{\mathfrak{p}}(m) > 0\} \cup S$$

とおく. S^+ は有限集合であることに注意しておく.

ここで次の補題により, 定理を証明する十分条件を S^+ の言葉で述べておく.

補題 3.10 任意の $L \in \mathcal{C}$ に対し, $L = K(\sqrt[m]{a})$ をみたす $a \in R_{S^+}^*$ が存在するならば $\#\mathcal{C}_m^S < \infty$ である.

補題の証明　自然な $R^*_{S^+}/(R^*_{S^+})^m \subset K^*/(K^*)^m$ があることに注意すれば, 仮定より Ψ の $R^*_{S^+}/(R^*_{S^+})^m$ への制限

$$R^*_{S^+}/(R^*_{S^+})^m \longrightarrow \mathcal{C}_m;\ a \longmapsto K(\sqrt[m]{a})$$

は全射である. よって, とくに $\#\mathcal{C} \leq \#(R^*_{S^+}/(R^*_{S^+})^m)$ である. また, 命題 3.8 より $\#(R^*_{S^+}/(R^*_{S^+})^m) < \infty$ である. したがって, 補題 3.10 が示された. □

命題 3.9 の証明に戻る. $L \in \mathcal{C}$ を任意にとる. すると, $\mathcal{C} \subset \mathcal{C}_m$ より Ψ の全射性から $L = K(\sqrt[m]{a})$ となる $a \in K^*$ が存在する. 必要なら適切な $b \in \mathcal{O}_K$ をとって $c = ab^m$ ととり直すことで, $c \in \mathcal{O}_K$ かつ $L = K(\sqrt[m]{c})$ となるので, $a \in \mathcal{O}_K \setminus \{0\}$ として一般性を失わない. ここで, a で生成されるイデアル (a) の素イデアル分解を

$$(a) = \prod_{\mathfrak{p}} \mathfrak{p}^{\epsilon_\mathfrak{p}}\ (\epsilon_\mathfrak{p} \in \mathbb{Z},\ \epsilon_\mathfrak{p} \geq 0)$$

とおく. さらに, この素イデアル分解を

$$(a) = \left(\prod_{\mathfrak{q} \in S^+} \mathfrak{q}^{\epsilon_\mathfrak{q}}\right) \cdot \left(\prod_{\mathfrak{p} \notin S^+} \mathfrak{p}^{e_\mathfrak{p}}\right) \tag{3.1}$$

と分ける. $R^*_S = \{\alpha \in K^* \mid \mathrm{ord}_\mathfrak{p}(\alpha) = 0\ (\forall \mathfrak{p} \in M_K \setminus S)\}$ であるから, 補題 3.10 における十分条件を示すために, 式 (3.1) の積における 2 項目が消えるように a を ab^m の形でとり替えたい. 以下において, a を上手くとり替えられることを示す. $\mathfrak{p} \in M^0_K \setminus S_+$ を任意にとる. すると, $L = K(\sqrt[m]{a})$ より有限次クンマー拡大の理論から,

$$\mathfrak{p} \text{ は } L/K \text{ で不分岐} \Leftrightarrow \mathrm{ord}_\mathfrak{p}(a) \equiv 0 \pmod{m}$$

であるので, 各 $\mathfrak{p} \in M^0_K \setminus S_+$ に対して $e_\mathfrak{p} = a_\mathfrak{p} m$ となる非負整数 $a_\mathfrak{p}$ が存在する. これを式 (3.1) に代入すれば,

$$(a) = \left(\prod_{\mathfrak{q} \in S^+} \mathfrak{q}^{\epsilon_\mathfrak{q}}\right) \cdot I^m \tag{3.2}$$

である. ただし, ここで $I = \prod_{\mathfrak{p} \notin S^+} \mathfrak{p}^{a_\mathfrak{p}}$ である. すると $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ のとり方より,

$$I^{-1}\mathfrak{a}_i = (b)\ (1 \leq \exists i \leq n, \exists b \in K^*) \tag{3.3}$$

が成り立つ. すると, 式 (3.2) と (3.3) より,

$$\begin{aligned}(ab^m) &= \left(\prod_{\mathfrak{q}\in S^+}\mathfrak{q}^{\epsilon_\mathfrak{q}}\right)\cdot I^m\cdot\left(I^{-m}\mathfrak{a}_i^m\right)\\ &= \left(\prod_{\mathfrak{q}\in S^+}\mathfrak{q}^{\epsilon_\mathfrak{q}}\right)\cdot\mathfrak{a}_i^m\end{aligned}$$

を得る. ここで, S^+ は $\mathfrak{a}_i$ の素因子をすべて含むようにとってあったので,

$$(ab^m) = \prod_{\mathfrak{q}\in S^+}\mathfrak{q}^{\epsilon_\mathfrak{q}}\ (\epsilon'_\mathfrak{q}\in\mathbb{Z}, \epsilon'_\mathfrak{q}\geq 0)$$

と書ける. 以上により, $ab^m \in R^*_{S^+}$ かつ $L = K(\sqrt[m]{a}) = K(\sqrt[m]{ab^m})$ であるから, 補題 3.10 における十分条件が示された. したがって, $\#(R^*_{S^+}/(R^*_{S^+})^m) < \infty$ が成り立つ. □

以上の準備の元で, 弱モーデル・ヴェイユの定理の証明を行う.

定理 3.1 (弱モーデル・ヴェイユの定理) の証明 m を自然数, K を代数体, E/K を楕円曲線とする. 定理 1.10 より, E は $\mathcal{O}_K$ 上で定義されているとしてよい. 定義より,

$$S_{E,m} = \{\mathfrak{p}\in M_K^0 \mid \mathrm{ord}_\mathfrak{p}(m) > 0\}\cup\{\mathfrak{p}\in M_K^0 \mid \mathrm{ord}_\mathfrak{p}(\Delta_E) > 0\}\cup M_K^\infty$$

である. また, クンマーペアリングを定義した際に用いた連結準同型 δ_E から定まる単射準同型 $E(K)/mE(K)\hookrightarrow \mathrm{Hom}(G_K, E[m])$ を, 同じ記号 δ_E で表す.

まず補題 3.4 より, $E[m]\subset E(K)$ としてよい. すると, 命題 1.19 より, $\mu_m\subset K^*$ である. ここで,

$$\mathcal{L} = \left\{L\subset\overline{K} \mid L/K \text{ は } G_{L/K}\leq\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z} \text{ をみたすガロア拡大}\right\}$$

とおき, 写像 Γ を

$$\Gamma : \mathrm{Hom}(G_K, E[m])\longrightarrow\mathcal{L};\ f\longmapsto L_f := \overline{\mathbb{Q}}^{\mathrm{Ker}(f)}$$

と定義する. 写像の well-defined 性は $f\in\mathrm{Hom}(G_K, E[m])$ に対して,

$$G_{L_f/K}\cong G_K/G_{L_f} = G_K/\mathrm{Ker}(f) = \mathrm{Im}(f)\leq E[m]\cong\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$$

よりしたがう. ただし, 途中で準同型定理と命題 1.7 を使った. 次の補題を準備する.

補題 3.11 Γ について, 以下が成り立つ.

(1) Γ は高々 m^4 対 1 写像である. すなわち, 任意の $L \in \mathcal{L}$ に対して $\#\Gamma^{-1} \leq m^4$ である.
(2) $\mathrm{Im}(\Gamma \circ \delta_E)$ は有限集合である.

補題の証明 (1) $L \in \mathcal{L}$ を任意にとる. $\Gamma^{-1}(L) =$ のときは明らかなので, ある $f \in \mathrm{Hom}(G_K, E[m])$ に対して $\Gamma(f) = L_1$ としてよい. $H = \mathrm{Ker}(f)$ とおく. すると, $g \in \mathrm{Hom}(G_K, E[m])$ をとれば, ガロア対応より

$$\Gamma(f) = \Gamma(g) \Leftrightarrow \mathrm{Ker}(f) = \mathrm{Ker}(g) = H$$

であるから, 準同型定理より $g \in \Gamma^{-1}(f)$ に対して $g \in \mathrm{Hom}(G_K/H, E[m])$ とみなせる. 別のいい方をすれば, 自然な単射 $\Gamma^{-1}(f) \longrightarrow \mathrm{Hom}(G_K/H, E[m])$ が存在する. ここで $L \in \mathcal{L}$ と, $\Gamma(f) = L$ かつ $H = \mathrm{Ker}(f)$ に注意すれば,

$$G_K/H = G_K/G_L \cong G_{L/K} \leq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

を得る. したがって,

$$\#\Gamma^{-1}(f) \leq \#\mathrm{Hom}(G_K/H, E[m]) \leq \#\mathrm{Map}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = m^4$$

より Γ は高々 4 対 1 写像である.

(2) $P \in E(K)/mE(K)$ を任意にとる. すると, δ_E の定義より

$$\mathrm{Ker}(\delta_E(P)) = \{\sigma \in G_K \mid Q^\sigma = Q \ (Q \in [m]^{-1}(P))\}$$

である. したがって, Γ の定義とガロア対応より

$$\Gamma \circ \delta_E(P) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\delta_E(P))} = K([m]^{-1}(P))$$

を得るので, 命題 3.7 から体拡大 $\Gamma \circ \delta_E(P)/K$ は $S_{E,m}$ の外不分岐である. ここで,

$$\mathcal{C}' = \left\{L \subset \overline{K} \mid L/K \text{ は } [L:M] \text{ が } m \text{ を割る巡回拡大であり, かつ } S_{E,m} \text{の外不分岐}\right\}$$

とおけば, 命題 3.9 より $\mathcal{C}'$ は有限集合である. 一方, Γ の定義より

$$G_{\Gamma \circ \delta_E(P)/K} \leq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

なので, 一般に体拡大 F/k が k の素点 $\mathfrak{p}$ で不分岐なら, 中間体 M についても M/k で $\mathfrak{p}$ が不分岐であることに注意すれば,

$$\Gamma \circ \delta_E(P) = L_1 L_2 \ (\exists L_1, L_2 \in \mathcal{C}')$$

が成り立つ. したがって,

$$\#\mathrm{Im}(\Gamma \circ \delta_E(P)) \leq (\#\mathcal{C}')^2$$

であるから $\Gamma \circ \delta_E(P)$ は有限集合である. 以上により, 補題 3.11 が証明された. □

弱モーデル・ヴェイユの定理の証明に戻る. δ_E の単射性と補題 3.11 より

$$\begin{aligned} \#E(K)/mE(K) &= \#\delta_E(E(K)/mE(K)) \\ &\leq m^4 \cdot \#\mathrm{Im}(\Gamma \circ \delta_E(P)) \\ &< \infty \end{aligned}$$

であるから, 弱モーデル・ヴェイユの定理が示された. □

3.2 モーデル・ヴェイユ群上の高さ関数

この節では, 有理数の高さを定義した後, 楕円曲線 $E/\mathbb{Q}$ に対して $E(\mathbb{Q})$ の高さ関数を定義する. そして, $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z})$ が与えられたとき, $E(\mathbb{Q})$ 上の高さ関数を構成できることを見る (命題 3.12). 命題 3.12 における証明は $P = (x, y) \in E$ に対して, x, y を既約分数表示してから議論を進めるなど, [Sil1, VIII, 4.1.] と比べてより細かな議論を積み重ねる記述を行った.

定義 $t \in \mathbb{Q}$ に対し, $t = \dfrac{p}{q}$ と既約分数表示をしたとき,

$$H(t) = \max\{|p|, |q|\}$$

と定めて, ***t* の高さ (height of *t*)** という.

定義 楕円曲線 $E/\mathbb{Q}$ に対して,

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R};$$

$$P \longmapsto \begin{cases} \log H(x(P)) & P \neq 0 \text{ のとき}, \\ 0 & P = O \text{ のとき}. \end{cases}$$

と定めて, ***E*(ℚ) 上の高さ (height on *E*(ℚ))** という.

次の命題は, 楕円曲線 $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z})$ に対し, $E(\mathbb{Q})$ 上の高さ h_x が 2 に関する高さ関数となることを主張している.

命題 3.12 ([Sil1, VIII, 4.1.]) 楕円曲線 $E/\mathbb{Q}$ が, ワイエルシュトラス方程式

$$y^2 = x^3 + Ax + B \ (A, B \in \mathbb{Z})$$

で与えられているとする. このとき, 以下が成り立つ.

(1) $Q \in E(\mathbb{Q})$ に対し, 各 $P \in E(\mathbb{Q})$ において

$$h_x(P+Q) \leq 2h_x(P) + C_1$$

をみたす A, B のみによる定数 $C_1 = C_1(Q, A, B)$ が存在する.

(2) 各 $P \in E(\mathbb{Q})$ において

$$h_x([2]P) \geq 4h_x(P) - C_2$$

をみたす A, B のみによる非負定数 $C_2 = C_2(A, B)$ が存在する.

(3) 任意の定数 C_3 に対し, 集合

$$\{P \in E(\mathbb{Q}) \mid h_x(P) \leq C_3\}$$

は有限集合である.

証明 (1) 証明の方針は $P = (x(P), y(P)) \in E(\mathbb{Q})$ に対して $P = (a/d^2, b/d^3)$ の形で書き, それから $H(x(P \oplus Q)) \leq C_1 H(x(P))^2$ の形を目指すことである.

任意に $P \in E(\mathbb{Q})$ をとり, $x(P) = a/q$ と互いに素な整数 a, q により既約分数で表示する. ただし, $q \in \mathbb{N}$ であるようにとる. すると, $h_x(P) = \log(\max\{|a|, |q|\})$ である. ここで $d = \sqrt{q}$ とおけば $x(P) = a/d^2$ である. また,

$$\begin{aligned} y(P)^2 &= \frac{a^3}{q^3} + A\frac{a}{q} + B \\ &= \frac{a^3}{d^6} + A\frac{a}{d^2} + B \\ &= \frac{a^3 + Aad^4 + Bd^6}{d^6} \end{aligned}$$

より $y(P) = b/d^3$, $b = \pm\sqrt{a^3 + Aad^4 + Bd^6}$ と書ける. したがって, 任意の $P \in E(\mathbb{Q})$ に対して $x(P) = a/d^2, y(P) = b/d^3$, $(a \in \mathbb{Z},\ b, d \in \mathbb{Z},\ b^2 \in \mathbb{Z},\ d^2 \in \mathbb{N}, \gcd(a, d^2) = 1)$ と書けることが分かった.

上記で述べたことから, 任意の $P = (x, y), Q = (x_0, y_0) \in E(\mathbb{Q})$ に対して,

$$P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right),\ Q = \left(\frac{e}{c^2}, \frac{f}{c^3}\right) \tag{3.4}$$

を $a, e \in \mathbb{Z},\ b, d, f, c \in \overline{\mathbb{Z}},\ b^2, f^2 \in \mathbb{Z},\ d^2, c^2 \in \mathbb{N},\ \gcd(a, d^2) = 1, \gcd(e, c^2) = 1$ となるようにおける. ただし, ここで $\overline{\mathbb{Z}}$ は $\mathbb{Z}$ 上整な元からなる集合である. ここで, $x(Q) \neq x(P)$ として一般性を失わない. 実際, $x(Q) \neq x(P)$ のときに定数 C_1 がとれることが示され

れば, $Q \in E(\mathbb{Q})$ に対して $x(Q) = x(P)$ となる $p \in E(\mathbb{Q})$ は有限個なので, 後から $h_x(P \oplus Q) \leq h_x(P) + C_1'$ となるように定数をとり替えられる. すると, 演算 $\oplus$ の定義より,

$$\begin{aligned} x(P \oplus Q) &= \frac{y - y_0}{x - x_0} - x - x_0 \\ &= \frac{(y^2 - x^3) + (y_0^2 - x_0^3) - 2yy_0 - x^2x_0 - xx_0^2}{(x - x_0)^2} \end{aligned}$$

を得る. ここで, 式 (3.4) を代入して整理すれば, $x(P \oplus Q)$ は

$$\frac{(Ac^4)ad^2 + (Ac^2e)d^4 + 2(Bc^4)d^4 + (c^2e^2)a^2 + ad^2e^2 - (2cf)bd}{a^2c^4 - (2c^2e)ad^2 + d^4e^2} \tag{3.5}$$

に等しい. ここで, 式 (3.5) の分子を p, 分母を q とおくと, $q \in \mathbb{Z}$ である. また,

$$bd = \frac{b}{d^3} \cdot d^4 = y(P) \cdot d^4 \in \mathbb{Q}$$

より, $bd \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ であるから, $bd \in \mathbb{Z}$ である. 同様にして $cf \in \mathbb{Z}$ であるから, $p \in \mathbb{Z}$ も成り立っている. すると, 約分する前の方が有理数の高さの値は大きくなるので,

$$H(x(P \oplus Q)) \leq \max\{|p|, |q|\}$$

である. また, 式 (3.5) の形から,

$$\max\{|p|, |q|\} \leq C_1' \max\{a^2, d^4, |bd|\} \tag{3.6}$$

となる A, B, c, e, f のみによる定数 C_1' が存在する. これは, 例えば $\max\{a^2, d^4, |bd|\} = d^4$ の場合は $a \leq d^2$ かつ $|bd| \leq d^4$ であるから, $|p| \leq C_{1,1}$ となる A, B, c, e, f のみによる定数 $C_{1,1}$ の存在が分かる. 同様にして, $|q| \leq C_{1,2}$ となる A, B, c, e, f のみによる定数 $C_{1,2}$ が存在するので , $C_{1,1}$ と $C_{1,2}$ で大きい方を C_1' とすれば C_1' は式 (3.6) をみたす A, B, c, e, f のみによる定数である. また, $\max\{a^2, d^4, |bd|\}$ が a^2, もしくは $|bd|$ の場合も, $\max\{a^2, d^4, |bd|\} = d^4$ のときと同様の議論により, 式 (3.6) をみたす A, B, c, e, f のみによる定数 C_1' の存在が分かる. したがって, 定数 C_1' に関して

$$H(x(P \oplus Q)) \leq C_1' \max\{a^2, d^4, |bd|\}$$

が成り立つ. 以下において, $|bd|$ を上から評価をしていく.

$y(P)^2 = x(P)^3 + Ax(P) + B$ より

$$\left(\frac{b}{d^3}\right)^2 = \left(\frac{a}{d^2}\right) + A\left(\frac{a}{d^2}\right) + B$$

である. これに両辺に b^8 を掛ければ

$$(bd)^2 = a^3d^2 + Aad^6 + Bd^8$$

となるので, 三角不等式から

$$|bd| \leq d\sqrt{a^3} + \sqrt{A}d^3\sqrt{a} + d^4\sqrt{B}$$

を得る. すると,

$$\begin{aligned} &a^2 \leq d^4 \text{とすると}, \sqrt{a^3} = (a^2)^{\frac{3}{4}} \leq (d^4)^{\frac{3}{4}} \leq d^3 \text{ より} \sqrt{a} = (a^2)^{\frac{1}{4}} \leq (d^4)^{\frac{1}{4}} = d, \\ &d^4 \leq a^2 \text{とすると}, d = (d^4)^{\frac{1}{4}} \leq \sqrt{a} \text{ より } d^3 = (d^4)^{\frac{3}{4}} \leq (a^2)^{\frac{3}{4}} = \sqrt{a^3} \end{aligned}$$

であるから,

$$\sqrt{A}d^3\sqrt{a} + d^4\sqrt{B} \leq C_1'' \max\{a^2, d^4\}$$

をみたす A, B のみによる定数 C_1'' が存在する. 以上より, $C_1 = \max\{C_1', C_1''\}$ とおけば C_1 は A, B, c, e, f のみによる定数で,

$$H(x(P \oplus Q)) \leq C_1 \max\{a^2, d^4\}$$

をみたす. ここで, 最初に $x(P) = (a/d^2)$, $\gcd(a, d^2) = 1$ とおいたことを思い出せば,

$$\max\{a^2, d^4\} = H(x(P))^2$$

である. したがって, $H(x(P \oplus Q)) \leq H(x(P))^2$ となり, 両辺に log をとることによって $h_x(x(P \oplus Q)) \leq 2h_x(P) + C_1$ を得る. □

(2) $h_x([2]P) \geq 4h_x(P) - C_2$ をみたす A, B のみによる定数 C_2 の存在を示すには,

$$H(x([2]P)) \geq H(x(P))^4 \cdot \frac{1}{C_2}$$

をみたす A, B のみによる非負定数 C_2 の存在を示せばよい. $P = (x(P), y(P)) \in E(\mathbb{Q})$ を任意にとる. $P = O$ なら $h_x(P) = h_x([2]P) = 0$ なので, 示したい不等式は成り立つ. したがって, $P \neq O$ としてよい. まず, $P \in E(\mathbb{Q})[2]$ のときを考える. 命題 1.12 より, $x(P)$ は

$$G(X) := 4X^3 + 4AX + 4B = 4(X^3 + AX + B)$$

の根なので, ガウスの補題より $x(P) \in \mathbb{Z}$ かつ $x(P) \mid B$ をみたす. したがって, とくに $|x(P)| \leq |B|$ であるから,

$$h_x(P) = \log|H(x(P))| = \log|x(P)| \leq \log|B|$$

を得る. したがって, $C_2' := \log|B|$ とすれば

$$h_x([2]P) \geq 4h_x(P) - C_2'$$

である.

次に, $[2]P \neq O$ のときを考える. $P = (x, y)$ と略記すると, 2 倍公式より

$$x([2]P) = \frac{x^4 - 2Ax^2 - 8B + A^2}{4x^3 + 4Ax + 4B}$$

を得る. 上式の右辺で $x = X/Z$ とおけば,

$$\begin{aligned} F(X, Z) &:= X^4 - 2AX^2Z - 8BXZ^3 + A^2Z^4, \\ G(X, Z) &:= 4(X^3Z + AXZ^3 + BZ^4). \end{aligned}$$

がそれぞれ右辺の分子と分母になる. したがって,

$$x(P) = \frac{a}{b} \ (a \in \mathbb{Z}, b \in \mathbb{N}, \gcd(a, b) = 1)$$

とおけば,

$$x([2]P) = \frac{F(a, b)}{G(a, b)}$$

である. よって, $d(P) := \gcd(F(a, b), G(a, b))$ とおくと

$$H(x([2]P)) = \frac{\max\{|F(a, b)|, |G(a, b)|\}}{d(P)} \tag{3.7}$$

を得る. 以下, 不等号は保持したままで, $d(P)$ を P によらない定数でおき換えることを目指す. 計算により, 次が成り立つことが分かる.

補題 3.13

$$\begin{aligned} \Delta(A, B) &:= 4A^3 + 27B^2, \\ f_1(X, Z) &:= 12X^2Z + 16AZ^3, \\ g_1(X, Z) &:= 3X^3 - 5AXZ^2 - 27BZ^3, \\ f_2(X, Z) &:= 4\Delta X^3 - 4A^2BX^2Z + 4A(3A^3 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3, \\ g_2(X, Z) &:= -A^2BX^3 - A(5A^3 + 32B^2)X^2Z \\ &\quad - 2B(13A^3 + 96B^2)XZ^2 + 3A^2(A^3 + 8B^2)Z_3 \end{aligned}$$

に対して, 以下が成り立つ.

(1) $f_1(X,Z)F(X,Z) - g_1(X,Z)G(X,Z) = 4\Delta Z^7$.
(2) $f_2(X,Z)F(X,Z) - g_2(X,Z)G(X,Z) = 4\Delta X^7$.

補題 3.13 より,

$$\begin{aligned} f_1(a,b)F(a,b) - g_1(a,b)G(a,b) &= 4\Delta b^7, \\ f_2(a,b)F(a,b) - g_2(a,b)G(a,b) &= 4\Delta a^7 \end{aligned} \tag{3.8}$$

が成り立つ. したがって, $d(P)$ のとり方より $d(P) \mid 4\Delta a^7$, $d(P) \mid 4\Delta b^7$ である. ここで $\gcd(a,b) = 1$ なので, $d(P) \mid 4\Delta$. よって,

$$\frac{1}{d(P)} \geq \frac{1}{|4\Delta|} \tag{3.9}$$

であるから, 式 (3.7) とあわせて

$$H(x([2]P)) = \frac{\max\{|F(a,b)|, |G(a,b)|\}}{d(P)} \geq \frac{\max\{|F(a,b)|, |G(a,b)|\}}{4|\Delta|} \tag{3.10}$$

を得る. また, 式 (3.8) に対して三角不等式を用いれば,

$$\begin{aligned} |f_1(a,b)F(a,b) - g_1(a,b)G(a,b)| &\leq |f_1(a,b)F(a,b)| + |g_1(a,b)G(a,b)|, \\ |f_2(a,b)F(a,b) - g_2(a,b)G(a,b)| &\leq |f_2(a,b)F(a,b)| + |g_2(a,b)G(a,b)| \end{aligned}$$

より

$$\begin{aligned} |4\Delta b^7| &\leq 2\max\{f_1(a,b), g_1(a,b)\} \cdot \max\{F(a,b), G(a,b)\}, \\ |4\Delta a^7| &\leq 2\max\{f_2(a,b), g_2(a,b)\} \cdot \max\{F(a,b), G(a,b)\} \end{aligned} \tag{3.11}$$

を得る. ここで $f_1(X,Y), g_1(X,Y)$ の各項の次数を見れば,

$$\max\{f_1(a,b), g_1(a,b)\} \leq C\max\{|a|^3, |b|^3\}$$

をみたす A, B のみによる非負定数の存在が分かる. $f_2(X,Y), g_2(X,Y)$ についても同様なので, 大きい方の非負定数をとることで, A, B にのみよる非負定数 C_2'' で

$$\begin{aligned} \max\{f_1(a,b), g_1(a,b)\} &\leq C\max\{|a|^3, |b|^3\}, \\ \max\{f_2(a,b), g_2(a,b)\} &\leq C\max\{|a|^3, |b|^3\} \end{aligned}$$

をみたすものが存在する. すると, 不等式 (3.11) より

$$\max\{|4\Delta a^7|, |4\Delta b^7|\} \leq 2C\max\{|a|^3, |b|^3\} \cdot \max\{F(a,b), G(a,b)\} \tag{3.12}$$

を得る. ここで a, b のとり方より, $H(x(P)) = \max\{|a|, |b|\}$ であるから,

$$\max\{|4\Delta a^7|, |4\Delta b^7|\} = 4|\Delta| \max\{|a^7|, |b^7|\},$$
$$\max\{|a|^3, |b|^3\} = (\max\{|a|, |b|\})^3 = H(x(P))^4$$

が成り立つ. したがって, 不等式 (3.12) より,

$$\frac{\max\{F(a,b), G(a,b)\}}{4\Delta} \geq H(x(P))^4 \cdot \frac{1}{2C}$$

となる. すると, 不等式 (3.10) より,

$$H(x([2]P)) \geq H(x(P))^4 \cdot \frac{1}{2C}$$

であるから, $C_2'' := \log(2C)$ とすれば, C_2'' は A, B のみによる非負定数で

$$h_x([2]P) \geq 4h_x(P) - C_2$$

をみたす. 以上により, $C_2 := \max\{C_2', C_2''\}$ とすれば, C_2 は A, B のみによる非負定数で任意の $P \in E(\mathbb{Q})$ に対して $h_x([2]P) \geq 4h_x(P) - C_2$ をみたすことが示された. □

(3) C_3 を任意の定数とする. このとき, $H(\mathbb{Q}) \subset \mathbb{Z}$ であることに注意すれば $\{t \in \mathbb{Q} \mid H(t) \leq C_3\}$ は有限集合である. したがって, $\{P \in \mathbb{Q} \mid h_x(P) \leq C_3\}$ も有限集合である. □

3.3 モーデルの定理

この節では, 3.3 節で示した定理 3.1 (弱モーデル・ヴェイユの定理) と 3.2 節で示した命題 3.12 を, 1.11 節における定理 1.30 (降下定理) に適用し, モーデルの定理を証明する. そして, モーデル・ヴェイユ群の階数の定義を行う. その後, Mazur による $E(\mathbb{Q})_{\mathrm{tors}}$ の決定や, BSD 予想など, モーデル・ヴェイユ群に関して知られている結果や話題を少し述べる.

定理 3.14 (**モーデルの定理**) $E/\mathbb{Q}$ を楕円曲線とする. このとき, $E(\mathbb{Q})$ は有限生成アーベル群である. したがって,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$$

となる非負整数 r が存在する.

証明　$E/\mathbb{Q}$ を楕円曲線とする．このとき, 例 1.11 より $E/\mathbb{Q}$ は

$$E : y^2 = x^3 + Ax + B \ (A, B \in \mathbb{Z})$$

というワイエルシュトラス形式であるとして一般性を失わない．すると命題 3.12 より, $E(\mathbb{Q})$ 上の高さ $h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}$ は, 2 に関する $E(\mathbb{Q})$ 上の高さ関数である．また, 弱モーデル・ヴェイユの定理より $E(\mathbb{Q})/2E(\mathbb{Q})$ は有限集合であるから, アーベル群に対する降下定理より, $E(\mathbb{Q})$ は有限生成アーベル群である．　□

定義　$E/\mathbb{Q}$ を楕円曲線とする．このとき, モーデルの定理より

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$$

と定まる非負整数 r を $\mathrm{rank}(E)$ で表し, $E(\mathbb{Q})$ の **階数 (rank)** という．

モーデルの定理は基礎体を代数体 K にした場合でも成り立つ．すなわち, 次の定理が成り立つ．

定理 3.15 E を代数体 K 上の楕円曲線とする．このとき, $E(K)$ は有限生成アーベル群である．

この定理はモーデル・ヴェイユの定理とよばれ, $E(\mathbb{Q})$ に対して定義した高さを $E(K)$ に拡張することで証明される．証明の詳細は [Sil1, VIII.5.] を参照してほしい．モーデル・ヴェイユの定理より, 一般の代数体 K に対しても $E(K) \cong E(K)_{\mathrm{tors}} \times \mathbb{Z}^r$ となる r が存在する．$K = \mathbb{Q}$ のときと同様に, r を $E(K)$ の階数という．

代数体 K と, 楕円曲線 E/K が与えられたとき, 一般に $E(K)$ の構造を決定するアルゴリズムは現在のところ知られていない．そのため, 楕円曲線 E/K を動かしたときに, $E(K)_{\mathrm{tors}}$ に現れる群を決定することや, $\mathrm{rank}(E)$ を求めることは楕円曲線に関する重要な問題の一つである．K が有理数体の場合, $E(K)_{\mathrm{tors}}$ は完全に決定されており, Mazur による次の結果は有名である．

定理 3.16 (Mazur [Maz] 1977) E を $\mathbb{Q}$ 上の楕円曲線とするとき, $E(\mathbb{Q})_{\mathrm{tors}}$ は次のいずれかに同型である．

(i) $\mathbb{Z}/m\mathbb{Z}$ $(1 \leq m \leq 12,\ m \neq 11)$.
(ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ $(1 \leq m \leq 4)$.

注意　定理 3.16 における有限群 G に対し, G ををねじれ部分群にもつ $\mathbb{Q}$ 上の楕円曲線が存在する．

また, $E/\mathbb{Q}$ の階数については Birch と Swinnerton-Dyer による次の予想が有名である.

予想 (**BSD 予想**) 素数 p に対して $a_p(E) := p + 1 - \#\tilde{E}(\mathbb{F}_p)$ とおき, 楕円曲線 E の L 関数を

$$L_E(s) := \prod_{p:\text{素数}} \left(1 - a_p(E)^{-s} + p^{1-2s}\right)^{-1}$$

で定義する. このとき, $L_E(s)$ の $s = 1$ での零点の位数と $\mathrm{rank}(E)$ は等しい.

この予想が正しければ, 階数の計算を解析的に行うことができる. この予想は正しいと思われており, 多くの数学者によって研究されているが, 一般の楕円曲線に対しては未解決である. また, 上記の予想を含んだ内容で, 同じく BSD 予想とよばれる $L_E(s)$ の $s = 1$ での留数が楕円曲線の代数的な情報で表せるという予想もなされている. BSD 予想に関する進展とより詳しい内容については [Sil1, Appendix, C.16.] を参照してほしい.

注意 基礎体が代数体でない状況でも, 弱モーデル・ヴェイユの定理が成り立つ場合が知られている. C/k を代数閉体上の射影曲線とし, その関数体を $F = \overline{k}(C)$ とする. このとき, F を基礎体とする楕円曲線 E について, $E(F)/2E(F)$ は有限群となる. また, $E(\overline{k}(C))$ の有限生成アーベル群となる十分条件を, E から C に自然に定まる有理写像の性質で述べることができる. このように, 基礎体を関数体とする楕円曲線の詳細は [Sil1] の続編である [Sil2, III.] を参照してほしい.

4　モーデル・ヴェイユ群の計算

この章では [Sil1] の X 章 1 節を参考に, 定理 4.1 (m-Descent) を証明した後, それを用いて定理 4.3 (Complete 2-descent) を証明する. 定理 4.1 で重要なところはこれまでに現れた写像 κ, δ_K, δ_E, e_m を組み合わせ, $E(K)/mE(K)$ を有限群に埋め込む点である. まず $E[m] \subset E(K)$ である楕円曲線 E/K に対し, $E(K)/mE(K) \times E[m]$ から $K^*/(K^*)^m$ への双線形写像 B を δ_K, δ_E, e_m を用いて定義する. すると, B の像が $K(S_{E,m})$ という有限群に含まれることが体拡大 $K([m]^{-1}E(K))/K$ における分岐の様子と有限次クンマー理論から示される. さらに, B は左非退化であることが示され, $E(K)/mE(K)$ が $\mathrm{Hom}(E[m], K^*/(K^*)^m)$ に埋め込まれる. そして, $E[m]$ の元 T に対し, $f_T \in K(E)$ が m 倍写像と因子に関してある条件をみたすなら, $B(P,T)$ の計算が f_T によって行えることが示される. これらの性質をまとめて m-Descent とよぶ.

定理 4.3 (Complete 2-descent) において, とくに重要なところは次の二点である. 一点目は双線形写像 B から定まる単射準同型 Φ により, $E(K)/2E(K)$ が $E(S_{E,2}) \times E(S_{E,2})$ という有限群に埋め込まれ, さらに写像 Φ による元の対応が明示的に書き下される点である. 二点目は $P \in E(K)/2E(K)$ が $\mathrm{Im}(\Phi)$ に含まれる必要十分条件が, P から定まる変数 z_1, z_2 ,z_3 に関する方程式の解の有無によって記述される点である. そして最後に, モーデル・ヴェイユ群の計算が Complete 2-descent を用いてどのように行われるのか, ある $\mathbb{Q}$ 上の楕円曲線を例に詳しく解説した.

4.1　m-Descent と Complete 2-descent

以降において, とくに混乱が起きない場合, 商群の元として見たときとそうでないときを同じ記号で表す. もしくは, 剰余群 G/H と $g \in G$ に対し, $\bar{g}$ で $g \bmod H$ を表す.

定義　K を代数体, E/K を $\mathcal{O}_K$ 上の楕円曲線とする. このとき, 自然数 m に対して

$$K(S_{E,m}) := \{\bar{b} \in K^*/(K^*)^m \mid b \in K^*, \mathrm{ord}_{\mathfrak{p}}(b) \equiv 0 \bmod m \ \ (\forall \mathfrak{p} \in M_K \setminus S_{E,m})\}$$

と定める. ただし, $S_{E,m}$ は 3.1 節で定義した

$$S_{E,m} = \{\mathfrak{p} \in M_K^0 \mid \mathrm{ord}_{\mathfrak{p}}(m) > 0\} \cup \{\mathfrak{p} \in M_K^0 \mid \mathrm{ord}_{\mathfrak{p}}(\Delta_E) > 0\} \cup M_K^\infty$$

である.

定理 4.1 (***m*-Descent**) K を代数体, m を自然数, E/K を $E[m] \subset E(K)$ である楕円曲線とする. このとき, 以下が成り立つ.

(1) 双線形写像 $B : E(K)/mE(K) \times E[m] \longrightarrow K^*/(K^*)^m$ で,

$$e_m(\delta_E(P)(*), T) = \delta_K(B(P,T))(*) \ (\forall P \in E(K), \forall T \in E[m])$$

をみたすものが存在する.

(2) 双線形写像 B は左非退化である. すなわち

$$B(P,T) = 1 \ (\forall T \in E[m]) \Rightarrow P = O \in E(K)/mE(K)$$

をみたす.

(3) $\mathrm{Im}(B) \subset K(S_{E,m})$.

(4) $T \in E[m]$ に対し, $f_T, g_T \in K(E)$ は

（a） $f_T \circ [m] = g_T^m$,

（b） $\mathrm{div}(f_T) = m(T) - m(O)$

をみたすとする. このとき, 任意の $T \in E[m]$, $P \in E(K) \setminus \{T, O\}$ に対して

$$B(P,T) = f_T(P) \bmod (K^*)^m$$

である.

証明 (1) $P \in E(K)/mE(K)$, $T \in E[m]$ をとる. このとき, 命題 1.18 におけるヴェイユペアリングの双線形性と δ_K の準同型性より $e_m(\delta_E(P)(*), T) \in \mathrm{Hom}(G_K, \mu_m)$ である. したがって,

$$B(P,T) := \delta_K^{-1}(e_m(\delta_E(P)(*), T))$$

と定義すればよい.

(2) $P \in E(K)/mE(K)$ をとり, $B(P,T) = 1$ $(\forall T \in E[m])$ とする. 両辺を δ_K で送り, (1) を使えば,

$$e_m(\delta_E(P)(*), T) = 1 \quad (\forall T \in E[m])$$

を得る. ただし, ここで右辺の 1 は $\mathrm{Hom}(G_K, \mu_m)$ の単位元である. すると, 命題 1.18 の e_m における非退化性を各 σ に対して用いることで,

$$\delta_E(P)(\sigma) = O \ (\forall \sigma \in G_K)$$

を得る. これは $\delta_E(P)$ が $\mathrm{Hom}(G_K, E[m])$ の単位元であることを意味しているが, δ_E は単射準同型であったので $P = O \in E(K)/mE(K)$ を得る.

(3) まず次の補題を準備する.

補題 4.2 $b \bmod (K^*)^m \in \mathrm{Im}(B)$ に対して,

$$b = \beta^m \ (\exists \beta \in \overline{K}^*) \Rightarrow \beta \in K([m]^{-1}E(K))$$

が成り立つ.

補題の証明 以降では, 章の冒頭で注意をしたように, $b = b \bmod (K^*)^m$ と商群の元として見たときとそうでないときを同じ記号で表す. そして, $K([m]^{-1}E(K))$ を命題 3.5 と同じ記号 L で表す. また,

$$b = B(P,T) \ (P \in E(K),\ T \in E[m])$$

とおく. すると, (1) より

$$\delta_K(b) = \delta_K\left(B(P,T)\right) = e_m(\delta_E(P)(*),T) \in \mathrm{Hom}(G_K, \mu_m)$$

である. ここで, δ_K は同型写像であるから,

$$\gamma^m \in K^*,\ e_m(\delta_E(P)(\sigma),T) = \frac{\gamma^\sigma}{\gamma}\ (\forall \sigma \in G_K)$$

をみたす $\gamma \in \overline{K}^*$ が存在する. $c = \gamma^m$ とおけば,

$$\begin{aligned} c \bmod (K^*)^m &= \delta_K^{-1}(e_m(\delta_E(P)(*),T)) \\ &= B(P,T) \\ &= b \bmod (K^*)^m \end{aligned}$$

であるから, ある $a \in K^*$ が存在して $b = a^m c$ となる. すると, $\beta^m = (a\gamma)^m$ であるから, いま $\mu_m \in K$ であることに注意すれば,

$$\beta \in L \Leftrightarrow \gamma \in L$$

を得る. 以下で $\gamma \in L$ を示す. 任意の $\sigma \in G_{\overline{K}/L}$ をとる. すると, 命題 3.5 より,

$$G_{\overline{K}/L} = \mathrm{Ker}\left(G_K \longrightarrow \mathrm{Hom}(E(K), E[m]);\ \sigma \longmapsto \kappa(*,\sigma)\right)$$

であるから,

$$\begin{aligned} \frac{\gamma^\sigma}{\gamma} &= e_m(\delta_E(P)(\sigma),T) \\ &= e_m(\kappa(P,\sigma),T) \\ &= e_m(O,T) \\ &= 1 \end{aligned}$$

である. あとはガロア対応より, $\gamma \in \overline{K}^{G_{\overline{K}/L}} = L$ であるから, 補題 4.2 が示された. $\square$

定理の証明に戻る. $P \in E(K)$, $T \in E[m]$ を任意にとり, $b = B(P,T)$ とおく. $\beta \in \overline{K}^*$ を $\beta^m = b$ となる元とする. すると, 補題 4.2 より $\beta \in L := K([m]^{-1}E(K))$ であるから, $K(\beta) \subset L$ を得る. また, 命題 3.7 より L/K は $S_{E,m}$ の外不分岐であるから, $K(\beta)/K$ も $S_{E,m}$ の外不分岐である. したがって, 有限次クンマー拡大の理論より, $\mathfrak{p} \in M_K^0$ に対して

$$\mathfrak{p} \text{ は } L/K \text{ で不分岐} \Leftrightarrow \mathrm{ord}_{\mathfrak{p}}(b) \equiv 0 \pmod{m}$$

である. 以上より, $b \in K(S_{E,m})$ が示された.

(4) $P \in E(K) \setminus \{T, O\}$, $T \in E[m]$ を任意にとり, $f_T, g_T \in K(E)$ を

$$f_T \circ [m] = g_T^m$$

をみたすものとする. また $P = [m]Q$ をみたす $Q \in E$ を任意にとり, $b = B(P,T)$ とおく. ここで, $\beta \in \overline{K}^*$ を $b = \beta^m$ をみたすようにとれば, 定理 4.1 (1) より,

$$\begin{aligned} e_m(\delta_E(P)(\sigma), T) &= \delta_K(b)(\sigma) \\ &= \frac{\beta^\sigma}{\beta} \end{aligned}$$

が任意の $\sigma \in G_K$ に対して成り立つ. 一方, δ_E, e_m の定義と Q のとり方より, 以下の 2 条件

- $g_T(X) \neq 0$,
- g_T は X, $X \oplus (Q^\sigma \ominus Q)$ 上で定義されている.

をみたす X に対して,

$$\begin{aligned} e_m(\delta_E(P)(\sigma), T) &= e_m(Q^\sigma \ominus Q, T) \\ &= \frac{g_T\left(X \oplus (Q^\sigma \ominus Q)\right)}{g_T(X)}. \end{aligned}$$

が成り立つ. ここで, 仮定 $P \in E(K)$, $P \neq T, O$ より, $X = Q$ と代入できるから,

$$\frac{g_T\left(X \oplus (Q^\sigma \ominus Q)\right)}{g_T(X)} = \frac{g_T(Q^\sigma)}{g_T(Q)}$$

を得る. ここで, 仮定より $g_T \in K(E)$ なので,

$$\frac{g_T(Q^\sigma)}{g_T(Q)} = \frac{g_T(Q)^\sigma}{g_T(Q)}$$

である. したがって,

$$\frac{g_T(Q)^\sigma}{g_T(Q)} = \frac{\beta^\sigma}{\beta} \ (\forall \sigma \in G_K)$$

を得る. また, $f_T \circ [m] = g_T^m$, $f_T \in K(E)$ より

$$\begin{aligned} g_T(Q)^m &= f_T \circ [m](Q) \\ &= f_T(P) \\ &\in K^* \end{aligned}$$

となるから, δ_K の全単射性より

$$g_T(Q)^m \equiv \beta^m \bmod (K^*)^m$$

である. したがって,

$$f_T(P) = f_T \circ [m](Q) = g_T(Q)^m \equiv \beta^m = b = B(P,T) \bmod (K^*)^m$$

である. □

注意 定理 4.1 において, $T \in E[m]$ に対して

(a) $f_T \circ [m] = g_T^m$,
(b) $\mathrm{div}(f_T) = m(T) - m(O)$

をみたす $f_T, g_T \in \overline{K}(E)$ が必ず存在することはヴェイユペアリングの定義のところで注意した. しかし, $T \in E[m]$ に対し, $T \in E(K)$ のときに f_T, g_T を $K(E)$ の元でとれかは明らかではない. しかし, 次のようにして $f_T, g_T \in K(E)$ でとれることが示される.

$T \in E[m]$ に対し, $f_T, g_T \in \overline{K}(E)$ を $f_T \circ [m] = g_T^m, \mathrm{div}(f_T) = m(T) - m(O)$ をみたす元とする. すると, $T \in E(K)$ より, 任意の $\sigma \in G_K$ に対して

$$\mathrm{div}(g_T) = \mathrm{div}(g_T^\sigma)$$

である. すると, $f \in \mathrm{Div}(E)$ に対して $\mathrm{div}(f) = 0 \Leftrightarrow f \in K^*$ であることを用いれば,

$$g_T = a_\sigma g_T^\sigma$$

をみたす $a_\sigma \in K^*$ が存在する. ここで,

$$\xi : G_K \longrightarrow \overline{K}^*; \ \sigma \longmapsto a_\sigma$$

と定めれば, ξ は 1-コサイクルである. すると, ヒルベルトの定理 90 より

$$a_\sigma = \frac{\alpha^\sigma}{\alpha} \ (\forall \sigma \in G_K)$$

をみたす $\alpha \in \overline{K}^*$ が存在する. したがって, $g_T \in K(E)$ ととり直すことができる.

上の議論で用いた因子群に対するガロア作用や, $f \in \mathrm{Div}(E)$ に対して f の因子の次数が 0 であることと $f \in \overline{K}^*$ が同値であることなどの, 射影曲線に関する内容は [Sil1, II. 3.] を参照されたい.

定理 4.1 (m-Descent) を用いて, 定理 4.3 (Complete 2-descent) を証明する. 定理 4.3 の証明で重要な点の一つは, 定理 4.1 における f_T を求めることで, 双線形写像 B の対応が具体的に書き下せる点である.

定理 4.3 (Complete 2-descent) K を代数体, E を相異なる K の元 e_1, e_2, e_3 により

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

で与えられた K 上の楕円曲線とする. このとき, 以下が成り立つ.

(1) 以下で定まる写像 Φ は well-defined な単射準同型である.

$$\Phi : E(K)/2E(K) \longrightarrow K(S_{E,2}) \times K(S_{E,2});$$

$$P = (x, y) \longmapsto \begin{cases} (x - e_1, x - e_2) & x \neq e_1, e_2 \text{のとき}, \\ \left(\dfrac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2 \right) & x = e_1 \text{のとき}, \\ \left(e_2 - e_1, \dfrac{e_2 - e_3}{e_2 - e_1} \right) & x = e_2 \text{のとき}, \\ (1, 1) & P = O \text{ のとき}. \end{cases}$$

(2) $(b_1, b_2) \in K(S_{E,2}) \times K(S_{E,2}) \setminus \{\Phi(O), \Phi((e_1, 0)), \Phi((e_2, 0))\}$ に対して, 以下は同値である.

（a）$(b_1, b_2) \in \mathrm{Im}(\Phi)$.

（b）変数 z_1, z_2, z_3 に関する方程式

$$\begin{aligned} b_1 z_1^2 - b_2 z_2^2 &= e_2 - e_1, \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= e_3 - e_1 \end{aligned}$$

の解 $(z_1, z_2, z_3) \in K^* \times K^* \times K$ が存在する.

また, (b) が成り立つとき, $\Phi(b_1z_1^2+e_1, b_1b_2z_1z_2z_3)=(b_1,b_2)$ である.

証明 (1) $T_1=(e_1,0),\ T_2=(e_2,0),\ T_3=(e_3,0)$ とおく. すると, 命題 1.12 より

$$E[2]=\{T_1,\ T_2,\ T_3,\ O\}$$

である. すると, 仮定 $e_1,\ e_2,\ e_3\in\mathbb{Q}$ から $E[2]\subset E(\mathbb{Q})$ である. したがって, 定理 4.1 を $m=2$ のときに適用できる. 定理 4.1 における双線形写像 B の像が $K(S_{E,m})$ に含まれているので, $m=2$ のとき B は単射準同型

$$E(K)/2E(K)\longrightarrow \mathrm{Hom}(E[2],K(S_{E,2}));\ P\longmapsto B(P,*)$$

を引き起こす. また, T_1,T_2 を $E[2]$ の生成元, すなわち $E[2]=\langle T_1,T_2\rangle$ となるように T_1,T_2 を選んでおけば,

$$\mathrm{Hom}(E[2],K(S_{E,2}))\longrightarrow K(S_{E,2})\times K(S_{E,2});\ \rho\longmapsto(\rho(T_1),\rho(T_2))$$

は群同型写像である. したがって, これらを合成することで単射準同型

$$\Phi: E(K)/mE(K)\longrightarrow K(S_{E,2})\times K(S_{E,2});\ P\longmapsto(B(P,T_1),B(P,T_2))$$

が定まる.

定理 4.1 (4) より, 因子の条件と m 倍写像を合成した状況がよい $f_{T_1},\ f_{T_2}\in E(K)$ がそれぞれ見つかれば, $B(P,T_1),B(P,T_2)$ が $f_{T_1},\ f_{T_2}\in E(K)$ を用いて計算できる. 次の補題は $f_{T_1},\ f_{T_2}$ をそれぞれ $(x-e_1),\ (x-e_2)$ ととれることを述べている.

補題 4.4 e を集合 $\{e_1,\ e_2,\ e_3\}$ の中から任意にとり, $T=(e,0)$ とおく. このとき, 以下が成り立つ.

(1) $\mathrm{div}(x-e)=2(T)-2(O)$.
(2) $(x-e)\circ[2]=g^2$ をみたす $g\in K(E)$ が存在する.

補題の証明 (1) 命題 1.17 よりしたがう.

(2) $e=e_1$ であるとし, $(x-e_1)(x-e_2)(x-e_3)=x^3+a_2x^2+a_4x+a_6$ とおく. すると, E は $(x,y)\longmapsto(X,Y):=(x+(a_2/3),y)$ により,

$$E': Y^2=(X-f_1)(X-f_2)(X-f_3),$$

$$f_1=e_1+\frac{a_2}{3},\ f_2=e_2+\frac{a_2}{3},\ f_3=e_3+\frac{a_2}{3}$$

と写り, E' の右辺は X^3+AX+B の形である. ここで, E' に対して $(X-f_1)\circ[2]=G^2$ をみたす $G\in K(X,Y)$ が存在すれば, $(x-e_1)\circ[2]=g^2$ をみたす $g\in K(E)$ が存在する. したがって, $E: y^2=X^3+AX+B$ の形であるとして一般性を失わない. 2 倍公式を用いれば,

$$\begin{aligned}(x-e_1)\circ[2] &= \frac{x^4-2Ax^2-8Bx+A^2}{(2y)^2}-e_1\\ &= \frac{x^4-2Ax^2-8Bx+A^2-4e_1(x^3+Ax+B)}{(2y)^2}\\ &= \frac{x^4-4e_1x^3-2Ax^2+(-4e_1A-8B)-4e_1}{(2y)^2}\end{aligned}$$

を得る. 最後の式の分子を $F(x)$ とおく. すると, 補題を示すには, $F(x)=g(x)^2$ となる $g(x)\in K[x]$ の存在を示せばよい. 変数 a,b に対して, $g(x)=x^2-2e_1x+(b+A)$ とおき, $g(x)^2$ と $F(x)$ の係数を比較することで $a=-2e_1,\ b=-2e_2-2A$ を得る. 以上により, $g(x)=x^2-2ex+(-2e^2-A)$ ととれば, $(x-e_1)\circ[2]=(g(x)/2y)^2$ が成り立つ.

また, いまの議論は e_2, e_3 についても成り立つので, 補題 4.4 が証明された. □

定理の証明に戻る. Φ による $P=(x,y)\in E(K)/mE(K)$ の行き先を, 定理 4.1 (4) を用いることにより調べよう. まず, $P\neq T_1,T_2,O$ のとき,

$$\begin{aligned}B(P,T_1)&=(x-e_1)(P)=x-e_1,\\ B(P,T_2)&=(x-e_2)(P)=x-e_2\end{aligned}$$

であるから, $\Phi(P)=(x-e_1,x-e_2)$ である. また, $P\neq T_1,T_2,O$ のときは以下のように計算ができる. $P\neq T_1,T_2,O$ の場合で, とくに

$$\begin{aligned}B(T_1,T_3)&=e_1-e_3,\ B(T_1,T_2)=e_1-e_2,\\ B(T_2,T_3)&=e_2-e_3,\ B(T_2,T_1)=e_2-e_1\end{aligned}$$

であるから, B の双線形性に注意すれば,

$$\begin{aligned}B(T_1,T_1) &= B(T_1,T_1\oplus T_2)\cdot B(T_1,T_2)^{-1}\\ &= B(T_1,T_3)\cdot B(T_1,T_2)^{-1}\\ &= \frac{e_1-e_3}{e_1-e_2}\end{aligned}$$

を得る. したがって, $\Phi(T_1) = (e_1 - e_3)/(e_1 - e_2)$ である. 同様にして

$$\begin{aligned} B(T_2, T_2) &= B(T_2, T_1 \oplus T_2) \cdot B(T_2, T_1)^{-1} \\ &= B(T_2, T_3) \cdot B(T_2, T_1)^{-1} \\ &= \frac{e_2 - e_1}{e_2 - e_1} \end{aligned}$$

を得る. 以上により, Φ の構成と, Φ による P の行き先が記述された.

(2) 任意の $(b_1, b_2) \in K(S_{E,2}) \times K(S_{E,2}) \setminus \{\Phi(O), \Phi(T_1), \Phi(T_2)\}$ をとる. このとき, (1) と, 定理 4.1 (4) より,

$$\begin{aligned} &(b_1, b_2) = \Phi(P) \ (\exists P = (x, y) \in E(K) \setminus \{T_1, T_2, O\}) \\ \Leftrightarrow &\begin{cases} B(P, T_1) = b_1, \\ B(P, T_2) = b_2. \end{cases} \quad (\exists P = (x, y) \in E(K) \setminus \{T_1, T_2, O\}) \\ \Leftrightarrow &\begin{cases} b_1 \equiv x - e_1 \bmod (K^*)^m, \\ b_2 \equiv x - e_2 \bmod (K^*)^m. \end{cases} \quad (\exists P = (x, y) \in E(K) \setminus \{T_1, T_2, O\}) \\ \Leftrightarrow &\begin{cases} y^2 = (x - e_1)(x - e_2)(x - e_3), \\ b_1 z_1^2 = x - e_1, \\ b_2 z_2^2 = x - e_2. \end{cases} \quad (\exists (x, y, z_1, z_2) \in K \times K \times K^* \times K^*) \\ \Leftrightarrow &\begin{cases} y^2 = b_1 b_2 z_1^2 z_2^2 (x - e_3), \\ b_1 z_1^2 = x - e_1, \\ b_2 z_2^2 = x - e_2. \end{cases} \quad (\exists (x, y, z_1, z_2) \in K \times K \times K^* \times K^*) \end{aligned}$$

と同値変形できる. また, ここで $z_3 := \dfrac{y}{b_1 b_2 z_1 z_2}$ とすれば,

$$\Leftrightarrow \begin{cases} b_1 b_2 z_3^2 = x - e_3, \\ b_1 z_1^2 = x - e_1, \\ b_2 z_2^2 = x - e_2. \end{cases} \quad (\exists (x, z_1, z_2, z_3) \in K \times K^* \times K^* \times K)$$

となる. さらに, $x = b_1 z_1^2 + e_1$ を代入すれば,

$$\Leftrightarrow \begin{cases} b_1 b_2 z_3^2 = b_1 z_1^2 + (e_1 - e_3), \\ b_2 z_2^2 = (e_1 - e_2) + b_1 z_1^2. \end{cases} \quad (\exists (z_1, z_2, z_3) \in K^* \times K^* \times K)$$

となる. いまの変形において, $x = e_1 + b_1 z_1^2$, $y = b_1 b_2 z_1 z_2 z_3$ であった. したがって, 以上により定理 4.3 (Complete 2-descent) が証明された. □

4.2　モーデル・ヴェイユ群の計算例

この節では, 定理 4.3 (Complete 2-descent) を用いたモーデル・ヴェイユ群の計算を行う. 楕円曲線 $E/\mathbb{Q}$ の階数を計算するには, $E(\mathbb{Q})[2]$ の構造と $E(\mathbb{Q})/2E(\mathbb{Q})$ の個数が分かれば十分である. 実際, r を $E/\mathbb{Q}$ の階数, t を $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^t$ $(0 \leq t \leq 2)$ とすれば,

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{Z}/2\mathbb{Z})^t$$

である. したがって,

$$2^{r+t} = \#(E(\mathbb{Q})/2E(\mathbb{Q}))$$

と表せる. 次の例で見るように, $E(\mathbb{Q})/2E(\mathbb{Q})$ の位数を, $\mathrm{Im}(\Phi)$ の個数を数えあげることによって得る.

例 4.5 有理数体 $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 = x(x-12)(x-36)$$

のモーデル・ヴェイユ群の構造は

$$E(\mathbb{Q}) \cong \mathbb{Z}/2Z \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

である.

証明　以下において, Φ を定理 4.3 (Complete 2-descent) における写像とする. まず, $E(\mathbb{Q})$ のねじれ部分群を計算する. 判別式を計算すると

$$\Delta_E = 2^{18} \times 3^8$$

である. したがって, 定理 2.6 より $E(\mathbb{Q})$ を $p \neq 2, 3$ をみたす素数 p で還元した楕円曲線 $\tilde{E}/\mathbb{F}_p$ に埋め込める. 有限回の計算により, $\#\tilde{E}(\mathbb{F}_5) = 8$ が分かる. よって, 再び定理 2.6 を用いれば, 任意の奇素数 $l \neq 5$ に対して単射

$$E(\mathbb{Q})[l] \hookrightarrow \tilde{E}(\mathbb{F}_5)$$

が存在する. したがって, $E(\mathbb{Q})[l] = \{O\}$ である. また, 計算により $\#\tilde{E}(\mathbb{F}_7) = 12$ が分かる. したがって, 埋め込み

$$E(\mathbb{Q})[2^n] \hookrightarrow \tilde{E}(\mathbb{F}_7),$$
$$E(\mathbb{Q})[5] \hookrightarrow \tilde{E}(\mathbb{F}_7)$$

から $E(\mathbb{Q})[2^n] \leq 4$, $E(\mathbb{Q})[5] = \{O\}$ を得る. また, 命題 1.12 より

$$E(\mathbb{Q})[2] = \{(0,0), (12,0), (36,0), O\}$$

である. 以上により,

$$E(\mathbb{Q})_{\mathrm{tors}} = E(\mathbb{Q})[2] = \{(0,0), (12,0), (36,0), O\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}2\mathbb{Z}$$

である.

次に, 定理 4.3 を用いて $\mathrm{Im}(\Phi)$ の個数を数える. $e_1 = 0, e_2 = 12, e_3 = 36$ とおく. すると, 定理 4.3 における変数 z_1, z_2, z_3 に関する方程式は

$$b_1 z_1^2 - b_2 z_2^2 = 12, \tag{4.1}$$
$$b_1 z_1^2 - b_1 b_2 z_3^2 = 36 \tag{4.2}$$

となる. また, $\Delta_E = 2^{18} \times 3^8$ より $\mathbb{Q}(S_{E,2})$ の完全代表系に $T = \{\pm 1, \pm 2, \pm 3, \pm 6\}$ をとれるので, $\mathbb{Q}(S_{E,2})$ と T を同一視する. 以下, 各 $b_1, b_2 \in T \times T$ から定まる方程式 (4.1), (4.2) に対し, 解 $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$ の存在を考察していく.

Step 1: $P_1 = (e_1, 0), P_2 = (e_2, 0), P_3 = (e_3, 0)$ とおく. すると, Φ の定義より,

$$\begin{aligned} \Phi(O) &= (1,1), \\ \Phi(P_1) &= (3,-3), \\ \Phi(P_2) &= (3,-2), \\ \Phi(P_3) &= (1,6) \end{aligned}$$

である. ただし, $\mathbb{Q}(S_{E,2})$ の定義より, 平方数は 1 と等しいことに注意する.

Step 2: $b_1 < 0$ かつ $b_2 > 0$ のとき, 方程式 (4.1) に実数解が存在しない. 実際, もし方程式 (4.1) をみたす実数解 z_1, z_2 が存在したとすれば,

$$0 < b_2 z_2^2 + 12 = b_1 z_1^2 < 0$$

となって矛盾する. したがって, とくに有理数解が存在しない.

Step 3: $b_1 < 0$ かつ $b_2 < 0$ のとき, 方程式 (4.2) に実数解が存在しない. 実際, もし方程式 (4.2) をみたす実数解 z_1, z_3 が存在したとすれば,

$$0 < b_1 b_2 z_3^2 + 36 = b_1 z_1^2 < 0$$

となって矛盾する. したがって, とくに有理数解が存在しない.

Step 4: $(b_1, b_2) = (1, -2)$ のとき, 方程式 (4.1), (4.2) は

$$z_1^2 + 2z_2^2 = 12, \tag{4.3}$$
$$z_1^2 + 2z_3^2 = 36 \tag{4.4}$$

となる. よって $(z_1, z_2, z_3) = (\pm 2, \pm 2, \pm 4)$ は方程式 (4.3), (4.4) の解であるから, 定理 4.3 より $(1, -2) \in \mathrm{Im}(\Phi)$ である.

Step 5: Step 1 より $(3, -3), (3, -2), (1, 6) \in \mathrm{Im}(\Phi)$, Step 4 より $(1, -2) \in \mathrm{Im}(\Phi)$ であることに注意すれば,

$$\begin{aligned}(3, 6) &= (1, -2) \cdot (3, -3),\\ (3, 1) &= (1, -2) \cdot (3, -2),\\ (1, -3) &= (1, -2) \cdot (1, 6)\end{aligned}$$

なので, $(3, 6), (3, 1), (1, -3) \in \mathrm{Im}(\Phi)$ を得る.

Step 6: $(b_1, b_2) = (1, -1)$ のとき, 方程式 (4.1), (4.2) は

$$z_1^2 + z_2^2 = 12, \tag{4.5}$$
$$z_1^2 + z_3^2 = 36 \tag{4.6}$$

となる. 方程式 (4.5) をみたす $z_1, z_2 \in \mathbb{Q}^*$ が存在する. そして

$$z_1 = \frac{a}{d}, z_2 = \frac{b}{d} \ (a, b, d, \in \mathbb{Z}, d > 0)$$

とおいて, これを方程式 (4.5) に代入すれば,

$$a^2 + b^2 = 12d^2$$

を得る. すると, a, b はどちらも 3 で割れるので,

$$a = 3a_1, b = 3b_2 \ (a_1, b_2 \in \mathbb{Z})$$

と表せる. すると, d も 3 で割れることになるが, これより方程式 $a^2 + b^2 = 12d^2$ は d に関して無限に小さい整数解の列をもつことになり矛盾が生じる. したがって, $(1, -1) \notin \mathrm{Im}(\Phi)$ である.

Step 7: Step 1 より $(1, 6) \in \mathrm{Im}(\Phi)$, Step 4 より $(1, -2) \in \mathrm{Im}(\Phi)$, Step 5 より $(1, -3) \in \mathrm{Im}(\Phi)$, Step 6 より $(1, -1) \notin \mathrm{Im}(\Phi)$ であることに注意すると,

$$\begin{aligned}(1, -6) &= (1, -1) \cdot (1, 6),\\ (1, -2) &= (1, -1) \cdot (1, 2),\\ (1, -3) &= (1, -1) \cdot (1, 3)\end{aligned}$$

なので, $(1,2),(1,3),(1,6) \notin \mathrm{Im}(\Phi)$ を得る.

Step 8: Step 1 より $(3,-3),(3,-2) \in \mathrm{Im}(\Phi)$, Step 5 より $(3,6),(3,1) \in \mathrm{Im}(\Phi)$, Step 6 より $(1,-1) \notin \mathrm{Im}(\Phi)$ に注意すると,

$$\begin{aligned}(3,2) &= (1,-1)\cdot(3,-3),\\ (3,3) &= (1,-1)\cdot(3,-2),\\ (3,-6) &= (1,-1)\cdot(3,6),\\ (3,-1) &= (1,-1)\cdot(3,1)\end{aligned}$$

なので,$(3,-1),(3,-6),(3,2),(3,3) \notin \mathrm{Im}(\Phi)$ を得る.

Step 9: $(b_1,b_2) = (6,-1)$ のとき, 方程式 (4.1), (4.2) は

$$6z_1^2 + z_2^2 = 12, \tag{4.7}$$
$$6z_1^2 + 6z_3^2 = 36 \tag{4.8}$$

となる. このとき, 方程式 (4.7), (4.8) をみたす $(z_1,z_2,z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$ が存在すると仮定する. すると, $z_3 = 0$ なら 方程式 (4.8) を方程式 (4.7) に代入することで, $z_2^2 < 0$ と矛盾が生じる. したがって, $z_3 = 0$ である. すると, Step 6 の議論と同様にして方程式 (4.8) をみたす $z_1, z_3 \in \mathbb{Q}^*$ の存在に矛盾する. したがって, $(6,-1) \notin \mathrm{Im}(\Phi)$ である.

Step 10: Step 1 より $(3,-3),(3,-2),(1,6) \in \mathrm{Im}(\Phi)$, Step 4 より $(1,-2) \in \mathrm{Im}(\Phi)$, Step 5 より $(3,6),(3,-2),(1,-3) \in \mathrm{Im}(\Phi)$, Step 9 より $(6,-1) \notin \mathrm{Im}(\Phi)$ であることに注意すれば,

$$\begin{aligned}(2,3) &= (6,-1)\cdot(3,-3),\\ (2,2) &= (6,-1)\cdot(3,-2),\\ (6,-6) &= (6,-1)\cdot(1,6),\\ (6,2) &= (6,-1)\cdot(1,-2),\\ (2,-6) &= (6,-1)\cdot(3,6),\\ (2,-1) &= (6,-1)\cdot(3,1),\\ (6,3) &= (6,-1)\cdot(1,-3)\end{aligned}$$

なので, $(2,3),(2,2),(6,-6),(6,2),(2,-6),(2,-1),(6,3) \notin \mathrm{Im}(\Phi)$ を得る.

Step 11: $(b_1,b_2) = (2,-2)$ のとき, 方程式 (4.1), (4.2) は

$$2z_1^2 + 2z_2^2 = 12, \tag{4.9}$$
$$2z_1^2 + 4z_3^2 = 36 \tag{4.10}$$

となる. ここで, 方程式 (4.9) には非自明な有理数解が存在しないことが Step 9 より示されているので, $(2,-2) \notin \mathrm{Im}(\Phi)$ を得る.

Step 12: Step 4 より $(1,-2) \in \mathrm{Im}(\Phi)$, Step 5 より $(1,-3) \in \mathrm{Im}(\Phi)$, Step 11 より $(2,-2) \notin \mathrm{Im}(\Phi)$ であることに注意すれば,

$$\begin{aligned}(2,1) &= (2,-2)\cdot(1,2),\\ (2,6) &= (2,-2)\cdot(1,-3)\end{aligned}$$

なので, $(2,1),(2,6) \notin \mathrm{Im}(\Phi)$ を得る.

Step 13: Step 1 より $(3,-3),(3,-2) \in \mathrm{Im}(\Phi)$, Step 5 より $(3,6),(3,1) \in \mathrm{Im}(\Phi)$, Step 12 より $(2,1) \notin \mathrm{Im}(\Phi)$ であることに注意すれば,

$$\begin{aligned}(6,-3) &= (2,1)\cdot(3,-3),\\ (6,-2) &= (2,1)\cdot(3,-2),\\ (6,6) &= (2,1)\cdot(3,6),\\ (6,1) &= (2,1)\cdot(3,1)\end{aligned}$$

なので, $(6,-3),(6,-2),(6,6),(6,1) \notin \mathrm{Im}(\Phi)$ を得る.

Step 1 から Step 13 より,

$$\mathrm{Im}(\Phi) = \{(1,1),(1,6),(1,-2),(1,-3),(3,1),(3,6),(3,-2),(3,-3)\}$$

が示されたので, $\#\mathrm{Im}(\Phi) = 8$ である. したがって, 定理 4.3 から $\#E(\mathbb{Q})/2E(\mathbb{Q}) = 8$ を得る. すると, $E(\mathbb{Q})$ の階数を r とすれば,

$$2^{r+2} = 8$$

であるから, $r = 1$. 以上により,

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

が示された. □

4.3 セルマー群と今後の展望

前節で $E(\mathbb{Q})$ を定理 4.3 (Complete 2-descent) を用いて計算した. しかし, Complete 2-descent を用いて計算できる楕円曲線の例を一つあげただけであり, 次の疑問には答えることができていない.

- $\#E(\mathbb{Q})[2] = 4$ である楕円曲線 $E/\mathbb{Q}$ に対し, 定理 4.3 を用いて $\#E(\mathbb{Q})/2E(\mathbb{Q})$ は必ず計算できるだろうか. すなわち, $\#E(\mathbb{Q})/2E(\mathbb{Q})$ を計算するアルゴリズムは存在するだろうか.
- $\#E(\mathbb{Q})[2] = 2$, $\#E(\mathbb{Q})[2] = 1$ である楕円曲線 $E/\mathbb{Q}$ のモーデル・ヴェイユ群はどのように計算できるだろうか. これらの場合でも, $E(\mathbb{Q})/2E(\mathbb{Q})$ を計算しやすい有限群に埋め込むことができるだろうか.

この節では, これらの疑問に関連した, 現在筆者が興味をもっている内容について述べる. とくに, 今後研究していきたい内容は定理 4.3 (Complete 2-descent) の中身に関わるヴェイユ・シャトレー群, セルマー群, テイト・シャファレヴィッチ群についてである. この節を通して, K は代数体とする. 以降にでてくる概念は [Hus, 7, §2.] や [Sil1, X.] を参照してほしい.

ヴェイユ・シャトレー群を定義する前に, まず 1 次コホモロジー集合と関連する主等質集合を定義する.

定義 G を群, A を左 G 群とする. このとき, X が **A 上の主等質 G 集合 (principal homogeneous G-set over A)** であるとは, X への単純推移的な右 A 作用

$$X \times A \longrightarrow X;\ (x, a) \longmapsto x \cdot a$$

と, X への左 G 作用

$$G \times X \longrightarrow X;\ (s, x) \longmapsto {}^s x$$

があって, 任意の $s \in G, x \in X, a \in A$ に対して ${}^s(x \cdot a) = {}^s x \cdot {}^s a$ をみたすときをいう.

A 上の主等質 G 集合を同型で割った集合を $\mathrm{Prin}(G, A)$ とする. このとき, 1 次コホモロジー集合 $H^1(G, A)$ と $\mathrm{Prin}(G, A)$ に自然な全単射が存在する ([Hus, 7, §3, 3.9.]). 楕円曲線 E を G_K 加群として見たとき, 主等質 G_K 集合には代数多様体としての構造を加味して考えたい. それが次で定義する楕円曲線の主等質空間である.

定義 E を K 上の楕円曲線とする. このとき, E/K の**主等質空間 (principal homogeneous space)** とは, 作用が代数多様体の射である単純推移的な右 E 作用

$$\mu : C \times E \longrightarrow C$$

をもつ K 上で定義された射影曲線のことをいう.

以下, E の主等質空間 C に対し, 作用の行き先をすべて $p+P$ で表す.

注意 主等質空間 C に対し, 自然な作用

$$G \times C \longrightarrow C;\ (s,p) \longmapsto {}^{s}p := s(p)$$

により, C は E 上の G 集合である.

例 4.6 楕円曲線 E/K に対し, E は右作用

$$\mu : E \times E \longrightarrow E;\ (P,Q) \longmapsto P \oplus Q$$

により, E の主等質空間である.

主等質空間の同型を次で定義する.

定義 E/K を楕円曲線, C_1, C_2 を E の主等質空間とする. このとき, C_1 と C_2 が同型であるとは, 任意の $p \in C_1$, $P \in E$ に対して

$$\phi(p+P) = \phi(p) + P$$

をみたす K 上の同型 $\phi : C_1 \longrightarrow C_2$ が存在するときをいい, $C_1 \sim C_2$ で表す.

主等質空間の間の同型は同値関係である. 主等質空間からなる集合を同型で割った集合が, 次で定義するヴェイユ・シャトレー群である.

定義 K 上の楕円曲線 E に対して,

$$\mathrm{WC}(E/K) := \{C \mid C \text{ は } E \text{ の主等質空間 }\}/\sim$$

と定め, **ヴェイユ・シャトレー群 (Weil-Châtelet group)** という.

このとき, 重要な事実として, 自然な全単射 $\mathrm{WC}(E/K) \longrightarrow H^1(G_K, E)$ が存在する. これは $\mathrm{Prin}(G_K, E)$ の代表元として, E の主等質空間がとれることを意味している. この全単射によりヴェイユ・シャトレー群に群の構造が入る.

この同型により, 次で定義するセルマー群とシャファレヴィッチ・テイト群が重要な意味をもつ.

定義 E, E' を K 上の楕円曲線, $\phi : E \longrightarrow E'$ を $[0]$ でない同種写像とする. M_K を K の素点全体とし, $v \in M_K$ に対して K_v で v による K の完備化を表す. ϕ から定まる完全系列

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

に対してガロアコホモロジーをとることで, 各素点 $\upsilon \in M_K$ に対して次の可換図式を得る.

$$\begin{array}{ccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_K, E[\phi]) & \xrightarrow{i} & H^1(G_K, E) \\ & & \downarrow & & \downarrow{\scriptstyle \alpha_\upsilon} & & \downarrow{\scriptstyle \beta_\upsilon} \\ 0 & \longrightarrow & E'(K_\upsilon)/\phi(E(K_\upsilon)) & \xrightarrow{\delta_\upsilon} & H^1(G_{K_\upsilon}, E[\phi]) & \longrightarrow & H^1(G_{K_\upsilon}, E) \end{array}$$

ただし, ここで縦の写像 α_υ, β_υ は $G_{K_\upsilon} \hookrightarrow G_K$ から定まるコホモロジーの制限写像である. このとき,

$$\mathrm{Sel}^\phi(E/K) := \bigcap_{\upsilon \in M_K} \mathrm{Ker}(\beta_\upsilon \circ i) \subset H^1(G_K, E[\phi]),$$

と定め, ϕ **セルマー群 (ϕ-Selmer group)** という. また,

$$Ш(E/K) := \bigcap_{\upsilon \in M_K} \mathrm{Ker}(\beta_\upsilon) \subset H^1(G_K, E)$$

と定め, **シャファレヴィッチ・テイト群 (Shafarevich-Tate group)** という

定義より,

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} \mathrm{Sel}(E/K) \longrightarrow Ш(E/K)$$

は完全系列である. したがって, シャファレヴィッチ・テイト群 $Ш(E/K)$ が自明ならば, $E'(K)/\phi(E(K))$ がセルマー群に埋め込まれる. これより, $E'(K)/\phi(E(K))$ を計算する上でも, セルマー群とシャファレヴィッチ・テイト群は重要な研究対象である. しかし, シャファレヴィッチ・テイト群の重要性はそれだけではない. C/K を $\mathrm{WC}(E/K)$ の元の代表元としたとき, C/K の類が $\mathrm{WC}(E/K)$ の中で自明であることと $C(K) \neq \emptyset$ が同値であることが知られている ([Sil1, X, 3.3.]). この事実から, $Ш(E/K)$ が非自明であることは, 局所的には解をもつが大域的には解をもたない K 上の非特異射影曲線 C が存在することに他ならない. すなわち, ハッセ原理が成り立たない非特異射影曲線が存在するということである. 楕円曲線 E/K が与えられたとき, ハッセ原理が成り立たない E と同型な非特異射影曲線はどれくらいあるだろうか. この疑問に関して, 任意の楕円曲線のシャファレヴィッチ・テイト群は有限群であるという予想があるが, 現在のところ未解決である. セルマー群とシャファレヴィッチ・テイト群がどのような群である

のかを理解したい. そのために, 筆者の今後の目標はまず定理 4.3 (Complete 2-descent) と $E(K)/2E(K)$ のセルマー群への埋め込みの関係を理解することである. そして, 同型 $\mathrm{WC}(E/K) \longrightarrow H^1(G_K, E)$ の対応において, $H^1(G_K, E)$ の元に対応する $\mathrm{WC}(E/K)$ の代表元 C/K の定義方程式を具体的に求める方法を研究していきたい.

参考文献

[高木] 高木貞治，代数的整数論第 2 版, 岩波書店，1971.

[Hus] D. Husemöller, *Elliptic curves*, with an appendix by Ruth Lawrence, Graduate Texts in Mathematics, 111, Springer-Verlag, New York, 1987.

[Kob] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, 97, Springer-Verlag, New York, 1984.

[Lan] S. Lang, *Algebraic number theory*, Second Edition, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994.

[Maz] B. Mazur, *Modular curves and Eisenstein ideal*, Publ. Math., Inst. Hautes Étud. Sci. **47** (1978) 33–186.

[Neu] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Second edition, Springer-Verlag, Berlin, 2008.

[Ono] T. Ono, *An introduction to algebraic number theory*, Translated from the second Japanese edition by the author, The University Series in Mathematics, Plenum Press, New York, 1990.

[Sil1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition, Graduate Texts in Mathematics 106, Springer-Verlag, Dordrecht, 2009.

[Sil2] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151, Springer-Verlag, New York, 1994.