レムニスケートの等分点による非可換拡大の構成

金井　和貴

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

本論文では, 虚数乗法論的な見地からレムニスケートの等分点による拡大体 K_β についての概説を行い, K_β の $\mathbb{Q}$ 上の Galois 群の構造の決定を行う. 3.4 節のみ著者が得た結果を証明付きで述べた. 他の節の証明は以下で述べる各章ごとの参考文献を参照されたい.

1 章では, 類体論, 楕円関数論, 楕円曲線論から必要最小限の準備を行った. 類体論については, 主に [河田] の方針に基づいて概説をした. 証明については [高木] を参照されたい. また, 後半の解析的な部分については [ノイキルヒ] を参考にした. 楕円関数論については, [三宅] の方針に従った. [竹内] には, 本論文では触れなかった楕円積分や Jacobi の楕円関数, ϑ 関数などの解析的な記述が充実している. 楕円曲線については, おおむね [Sil2] の虚数乗法の章の導入部を, [Sil1], [ST], [横山], [三宅] により補った形となっている.

2 章では, 楕円曲線を用いた虚 2 次体のシュトラール類体の構成について述べた. 2.1 節, 2.2 節は共に [Sil2], [河田] に基づいている. また, 解析的な議論は [BCHIS] に証明がある. また, [Shi] はおおむね [Sil2] と同じ方針であるが, 虚数乗法の Abel 多様体への拡張について触れられている.

3 章では, レムニスケートの等分点による拡大体について述べた. 3.1 節, 3.2 節については [Cox2], [CH] に基づいている. これらは共にレムニスケートの等分体の Galois 理論について述べているが, [CH] では古典的な円分多項式との類似物である, lemnatomic polynomial を導入した証明を与え, さらに Chebyshev 多項式との類似を見出している. このことが [Cox2] と異なる点である. 3.3 節では, 奇である Gauss 整数 β に対して, レムニスケートの β 等分点による拡大体が, β を法としたイデアル群に対してのシュトラール類体の部分体となることを [CH], [Ros] に基づいて述べた. また, 高木貞治が類体論に先駆けて, $k = \mathbb{Q}(\sqrt{-1})$ において Kronecker の青春の夢を解決した [Tak1] で述べられている判別式についての結果を紹介した. 3.4 節では, 奇素数 p に対して, $\mathbb{Q}(\sqrt{-1})$ 上のレムニスケートによる等分点による拡大体 K_p の k 上の最小多項式が $\mathbb{Q}$ 上定義され, その最小分解体は K_p と一致することを示し, さらに Galois 群の具体的な構造を特定した. この群は p に依らず常に非可換群となる.

今後の研究としては, K_β やその部分体の数論的な性質, 特にイデアル類群についての研究を行いたいと考えている. β が $4k+1$ 型の素数であるとき, 最小多項式の定数項は 1 である. これに着目し, 最小多項式の定数項が 1 である拡大の単数群について述べた [Sha], [SW] 等の応用を模索している. また, 楕円曲線の岩澤理論の応用も視野に入れている. これらに対して, さらなる学習と研究を進めていきたい.

謝辞

学部から 3 年間に渡りご指導頂きました星明考先生には, 数多くの知識や教養を賜りました. ここに深い感謝の意を表します. また, セミナーや議論を通じて多くの知識や示唆を頂いた, 星研究室の三浦正道先輩と同期である長谷川寿人君, 小島研究室の長峰孝典先輩に心より感謝致します.

目次

1　準備

類体論, 楕円関数論, 楕円曲線論について概説する．1.1 節では, 2 章の主題となる類体の定義を与え, その性質や重要性について述べる．1.2 節, 1.3 節では, 2 章以降で共に重要な役割を果たす, 楕円関数と $\mathbb{C}$ 上の楕円曲線の関係を明確にすることを目標とする．その過程で, モジュラー不変量などの重要かつ基本的な事項について述べる．主に 1.1 節は [河田], 1.2 節は [三宅], 1.3 節は [河田], [Sil2] に基づいている．

1.1　類体論

有理数体 $\mathbb{Q}$ の有限次拡大体を代数体と呼ぶ．この節では代数体における古典的な類体論の主定理や基本的な結果を紹介する．まず, Hilbert 類体と呼ばれる類体の雛形となった体の定義を与える．

定義　K を代数体 k の拡大体, $\mathfrak{p}$ を k の 1 次, すなわち, $\mathrm{N}_{k/\mathbb{Q}}\mathfrak{p} = p$ (p は素数) となる素イデアルとする．このとき, $\mathfrak{p}$ が K/k において完全分解することと $\mathfrak{p}$ が k の単項イデアルであることが必要十分であるとき, K を k の **Hilbert 類体** (Hilbert class field) と呼ぶ.

k のイデアル類群を Cl_k とすれば, イデアル $\mathfrak{p}$ が k の単項イデアルであることは, $\mathfrak{p}$ の類が k の単位元 1 の類であることと同値である．Hilbert は上記の体を類体と名付け, 代数体 k に対して必ずこのような体が一意的に存在し, k の素イデアル $\mathfrak{p}$ の K での素イデアル分解が, $\mathfrak{p}$ の属するイデアル類のみによって定まることを予想した．このことから, 上記の体は現在では Hilbert 類体などと呼ばれている．

高木貞治はこの予想を一般化した形で証明するこに成功した．それらの主張は, イデアル類群をイデアル $\mathfrak{m}$ ごとに精密化したシュトラール類群によって述べられる．

定義　K/k を代数体の拡大, k の整数環を $\mathcal{O}_k$ とする．$\mathcal{O}_k$ のイデアル $\mathfrak{m}$ に対して

$$
\begin{aligned}
&I_k(\mathfrak{m}) := \{\mathfrak{a} \subset k \mid \mathfrak{a} \text{は分数イデアル}, (\mathfrak{a}, \mathfrak{m}) = 1\},\\
&P_k(\mathfrak{m}) := \{(\alpha) \mid \alpha \in k^\times, \alpha \equiv 1(\mathfrak{m}), \alpha\text{は総正 }\},\\
&Cl_k(\mathfrak{m}) := I_k(\mathfrak{m})/P_k(\mathfrak{m})
\end{aligned}
$$

と置く．$P_k(\mathfrak{m})$ を $\mathfrak{m}$ を法とする**シュトラール** (ray) と呼び, $Cl_k(\mathfrak{m})$ を $\mathfrak{m}$ を法とする**シュトラール類群** (ray class group) と呼ぶ．ただし $\alpha \in k^\times$ が**総正** (totally real) とは, α の実共役が全て正であることである．また, $I_k(\mathfrak{m})$ の乗法的部分群 $H_k(\mathfrak{m})$ で $P_k(\mathfrak{m})$ を含む

ものを **($\mathfrak{m}$ を法とする) イデアル群** (ideal group modulo $\mathfrak{m}$) と呼び, $I_k(\mathfrak{m})/H_k(\mathfrak{m})$ を $H_k(\mathfrak{m})$ **に対するイデアル類群** (ideal class group modulo $\mathfrak{m}$) と呼ぶ.

定義 代数体 k に対して, $\mathfrak{m}, \mathfrak{n}$ を法とするイデアル群をそれぞれ $H_k(\mathfrak{m}), H_k(\mathfrak{n})$ とする. このとき, $H_k(\mathfrak{m}) \cap I_k(\mathfrak{mn}) = H_k(\mathfrak{n}) \cap I_k(\mathfrak{mn})$ により, $H_k(\mathfrak{m})$ と $H_k(\mathfrak{n})$ の同値関係を定める. このとき $H_k(\mathfrak{m})$ と同値なイデアル群 $H_k(\mathfrak{m}')$ でイデアル $\mathfrak{m}'$ が包含関係で最小なものが存在する. この $\mathfrak{m}'$ を $H_k(\mathfrak{m})$ の**導手** (conductor) と呼ぶ.

後で述べるように, 導手は分岐についての情報を持っている. 次に類体の定義を与える.

定義 K/k を代数体 k の Galois 拡大とする. このとき, $\mathfrak{m}$ を割らない k の 1 次の素イデアル $\mathfrak{p}$ に対して, $\mathfrak{p}$ が K/k において完全分解することと $\mathfrak{p} \in H_k(\mathfrak{m})$ であることが必要十分であるとき, K を k の $\mathfrak{m}$ を法とするイデアル群 $H_k(\mathfrak{m})$ **に対する類体** (class field for $H_k(\mathfrak{m})$) であると呼ぶ. また, 代数体 k の $\mathfrak{m}$ を法とするシュトラールに対しての類体を**シュトラール類体** (ray class field) と呼ぶ.

このとき, $\mathfrak{m} = \mathcal{O}_k$ であれば, $I_k(\mathfrak{m})$ は分数イデアル全体 I_k となる. $H_k(\mathfrak{m})$ として k の単項イデアル全体 P_k をとれば, P_k に対するイデアル類群は $I_k/P_k = Cl_k$ となり, イデアル群 $H_k(\mathfrak{m})$ に対する類体は Hilbert 類体となる.

類体とは平たく言えば, 基礎体のイデアル類により完全分解する素イデアルが決定される体のことである. 次の類体論の主定理は類体の著しい性質を簡潔に表している.

定理 1.1 k を代数体とするとき以下が成立する.

(1) (**存在定理**) イデアル群 $H_k(\mathfrak{m})$ に対して, $H_k(\mathfrak{m})$ に対する類体 K/k が存在する.

(2) (**同型定理**) $H_k(\mathfrak{m})$ に対する類体 K/k は Abel 拡大であり

$$\mathrm{Gal}(K/k) \simeq I_k(\mathfrak{m})/H_k(\mathfrak{m}).$$

(3) (**導手定理**) $H_k(\mathfrak{m})$ に対する類体 K/k の相対判別式イデアル $\mathfrak{b}_{K/k}$ に含まれる素イデアル (すなわち K/k 分岐する素イデアル) は, $H_k(\mathfrak{m})$ の導手 $\mathfrak{f}$ に含まれる素イデアルに限る.

(4) (**分解定理**) $H_k(\mathfrak{m})$ の導手 $\mathfrak{f}$ と互いに素な素イデアル $\mathfrak{p}$ は, $H_k(\mathfrak{m})$ に対する類体 K/k において, $\mathfrak{p}^f \in H_k(\mathfrak{m})$ となる最小の f に対して

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g,\ \mathrm{N}_{K/k}\mathfrak{P}_i = \mathfrak{p}^f \quad (i = 1, \cdots, g)$$

と分解される.

また, 定理 1.1 と関連して, 比較的容易に次が成立する.

定理 1.2 代数体 k のイデアル群 $H_k(\mathfrak{m}_1), H_k(\mathfrak{m}_2)$ に対する類体をそれぞれ K_1, K_2 とするとき以下が成立する.

(1) (**順序定理**) 以下は同値である.
  (i) $K_1 \supset K_2$.
  (ii) $H_k(\mathfrak{m}_1) \cap I_k(\mathfrak{m}_1\mathfrak{m}_2) \subset H_k(\mathfrak{m}_2) \cap I_k(\mathfrak{m}_1\mathfrak{m}_2)$.
  特に, $H_k(\mathfrak{m})$ に対応する類体の存在は一意である.

(2) (**結合定理**) 合併体 K_1K_2 は $H_k(\mathfrak{m}_1) \cap H_k(\mathfrak{m}_2)$ に対する類体である.

(3) (**推進定理**) k のイデアル群 $H_k(\mathfrak{m})$ に対する類体を K とする. Ω を k を含む任意の代数体とするとき, $K\Omega/\Omega$ は, Ω のイデアル群 $H' := \{\mathfrak{a} \mid N_{\Omega/k}\mathfrak{a} \in H_k(\mathfrak{m})\}$ に対する類体である.

(4) (**終結定理**) k のイデアル群 $H_k(\mathfrak{m})$ に対する類体を K とし, Ω/k を任意の代数体とする. このとき, $H_\Omega(\mathfrak{m}) \subset H_k(\mathfrak{m})$ ならば, $\Omega \supset K$ である. また, $H_\Omega(\mathfrak{m}) = H_k(\mathfrak{m})$ ならば K は Ω/k に含まれる最大の Abel 拡大である.

(1), (2), (3) は類体の相互関係について述べており, (4) は類体論で統制出来る範囲が Abel 拡大までであることを表している.

定理 1.1 によれば, 類体は Abel 拡大であるが, 逆にどのような体が類体となり得るだろうか. このことを述べたのが類体論における基本定理と呼ばれる次の定理である.

定理 1.3 (類体論の基本定理, 高木貞治, 1920) 代数体 k の任意の Abel 拡大 K に対して, k のイデアル $\mathfrak{m}$ で $H_k(\mathfrak{m})$ に対する類体が K となるものが存在する.

定理 1.3 は, 驚くべきことに, 任意の Abel 拡大は類体であることを述べている. さらに注意すべきは, 定理 1.1 や定理 1.2 において, 類体の性質は基礎体 k のイデアル群 $H_k(\mathfrak{m})$ によって記述されていることである. 基礎体 k 上の任意の Abel 拡大についての情報は基礎体 k 自身に秘められているということを類体論は述べている.

高木の類体論を受けて, Artin により同型定理を具体的な写像で記述する方法が考案された. これは同型を表すだけではなく, 分解定理をも含む画期的な方法であった. この写像を表すために Artin 記号と呼ばれる記号を導入する.

K/k を Galois 拡大とする. このとき k の素イデアル $\mathfrak{p}$ に対して

$$P_\mathfrak{p} := \{\mathfrak{P} : K \text{ の素イデアル} \mid \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_k\}$$

とすると, K/k の Galois 群 $\mathrm{Gal}(K/k)$ は $P_\mathfrak{p}$ に推移的に作用する.

$\mathfrak{P}$ が K で不分岐であるとき, $\mathfrak{P}$ に対して Frobenius 自己同型

$$\left[\frac{K/k}{\mathfrak{P}}\right] = \sigma \in \mathrm{Gal}(K/k)$$

が定まる. 言い換えれば, Frobenius 自己同型は任意の $\alpha \in \mathcal{O}_K$ に対して

$$\alpha^{\sigma} \equiv \alpha^{\mathrm{N}_{k/\mathbb{Q}}\mathfrak{p}} \pmod{\mathfrak{P}}$$

によって一意に定まる自己同型である. このとき, $\tau \in \mathrm{Gal}(K/k)$ に対して

$$\left[\frac{K/k}{\mathfrak{P}^{\tau}}\right] = \tau^{-1}\sigma\tau \tag{1}$$

が成立する.

K/k を Abel 拡大とすると, (1) 式から

$$\left[\frac{K/k}{\mathfrak{P}^{\tau}}\right] = \left[\frac{K/k}{\mathfrak{P}}\right]$$

が成り立つ. すなわち, $\mathfrak{P}$ の K/k に関する Frobenius 自己同型は共役に依らず, $\mathfrak{P}$ が割る k の素イデアル $\mathfrak{p}$ のみに依存する. したがってこのとき $\left[\frac{K/k}{\mathfrak{P}}\right]$ を

$$\left(\frac{K/k}{\mathfrak{p}}\right)$$

と書き, k の素イデアル $\mathfrak{p}$ の **Artin 記号** (Artin symbol) と呼ぶ. ここで次が成立する.

定理 1.4 K/k を代数体の Abel 拡大, $\mathfrak{p}$ を k の素イデアルとする. このとき, 以下は同値である.

(1) 素イデアル $\mathfrak{p}$ が K で完全分解する.
(2) $\left(\frac{K/k}{\mathfrak{p}}\right) = 1$.

ここで, K/k で分岐する素イデアル $\mathfrak{p}$ は有限個であるから, 全ての分岐する素イデアルを素因子に持つ $\mathfrak{m}$ をとる. $\mathfrak{m}$ と互いに素なイデアル $\mathfrak{a} \in I_k(\mathfrak{m})$ に対して, $\mathfrak{a}$ を

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$$

と素イデアル分解したとき, Artin 記号を拡張して

$$\left(\frac{K/k}{\mathfrak{a}}\right) = \prod_i \left(\frac{K/k}{\mathfrak{p}_i}\right)^{e_i} \in \mathrm{Gal}(K/k)$$

と定義する. $\mathrm{Gal}(K/k)$ は Abel 群であるから

$$\left(\frac{K/k}{\mathfrak{ab}}\right) = \left(\frac{K/k}{\mathfrak{a}}\right)\left(\frac{K/k}{\mathfrak{b}}\right)$$

となる.

このとき次の定理が成り立つ.

定理 1.5 (Artin の相互律, Artin, 1927) k を代数体, $\mathfrak{m}$ を法とするイデアル群 $H_k(\mathfrak{m})$ に対する類体を K とする. このとき Artin 写像と呼ばれる準同型写像を

$$\Phi : I_k(\mathfrak{m}) \ni \mathfrak{a} \longmapsto \left(\frac{K/k}{\mathfrak{a}}\right) \in \mathrm{Gal}(K/k)$$

とすると次が成立する.

(1) $\mathrm{Ker}\ \Phi = H_k(\mathfrak{m})$,
(2) $I_k(\mathfrak{m})/H_k(\mathfrak{m}) \simeq \mathrm{Gal}(K/k)$.

これが, Artin の相互律と呼ばれるものであり, 定理 1.1 の (1), (2) を具体的に表している. 定理 1.5 の (1) は素イデアルが Artin 写像の核に属することと完全分解することは同値であること, (2) は Artin 写像は全射であり, そのことから K の k 上の Galois 群と $H_k(\mathfrak{m})$ に対するイデアル類群が同型となることをそれぞれ意味している.

Artin の相互律は 2 次体においては平方剰余の相互法則の一般化と捉えることができる.

例として, 奇素数 l に対して, 円の l 分体の Artin 写像を計算する.

例 1.6 (l 分体における Artin 写像) l を奇素数, $\zeta = e^{\frac{2\pi i}{l}}, k = \mathbb{Q}(\zeta)$ とする. l 分体の $\mathbb{Q}$ 上の Galois 群は $\mathbb{F}_l^\times$ と同型であり, 位数 $l-1$ の巡回群となる. $l-1$ の約数と部分群が 1 対 1 に対応することから, Galois 対応により中間体も $l-1$ の約数に 1 対 1 に対応する. 具体的には, k の n 次の部分体を k_n と置くと,

$$\mathrm{Gal}(k_n/\mathbb{Q}) \simeq \mathbb{F}_l^\times/(\mathbb{F}_l^\times)^n$$

である.

l 分体の判別式は $\Delta_k = (-1)^{\frac{l-1}{2}} l^{l-2}$ であるから, $p \neq l$ である素数 p は $k/\mathbb{Q}$ において不分岐である. したがって, 任意の中間体においても p は不分岐である.

このとき, $\mathbb{Q}$ において分数イデアルは $\mathbb{Q}$ の正の元と同一視される. したがって,

$$\begin{aligned} &I_{\mathbb{Q}}(l) = \{a \in \mathbb{Q} \mid a > 0, (a, l) = 1\}, \\ &P_{\mathbb{Q}}(l) = \{a \in I_{\mathbb{Q}}(l) \mid a \equiv 1\ (l)\}, \\ &Cl_{\mathbb{Q}}(l) = I_{\mathbb{Q}}(l)/P_{\mathbb{Q}}(l) \end{aligned}$$

となる．ここで, $(a,l)=1$ とは, $a=b/c$ に対して, $(l,b)=(l,c)=1$ である．また, $\mathbb{Q}$ の共役は自明なものしかないため, $P_{\mathbb{Q}}(l)$ の総正という条件は常に満たされる．このとき, k_n に対して,

$$H_{\mathbb{Q},n}(l)=\{a\in I_{\mathbb{Q}}(l)\mid a\equiv x^n\ (l)\ \ (\exists x\in\mathbb{N})\}$$

とすると, $H_{\mathbb{Q},l-1}(l)=P_{\mathbb{Q}}(l)$ であり, $H_{\mathbb{Q},1}(l)=I_{\mathbb{Q}}(l)$ である．さらに, $m\mid n$ に対して, $H_{\mathbb{Q},n}(l)\subset H_{\mathbb{Q},m}(l)$ となる．

このとき,

$$\mathrm{Gal}(k_n/\mathbb{Q})\simeq\mathbb{F}_l^{\times}/(\mathbb{F}_l^{\times})^n$$

であるから, 各 k_n に対しての Artin 写像は

$$\Phi_n : I_{\mathbb{Q}}(l)\ni a\longmapsto \overline{a}\bmod(\mathbb{F}_l^{\times})\in\mathbb{F}_l^{\times}/(\mathbb{F}_l^{\times})^n$$

と同一視することができる．この, Φ_n は全射であり,

$$\mathrm{Ker}\ \Phi_n=H_{\mathbb{Q},n}(l)$$

となる．したがって

$$\mathrm{Gal}(k_n/\mathbb{Q})\simeq I_{\mathbb{Q}}(l)/H_{\mathbb{Q},n}(l)$$

となる．類体の一意性から, l 分体は $H_{\mathbb{Q},l-1}(l)=P_{\mathbb{Q}}(l)$ に対するシュトラール類体であり, 各部分体 k_n はイデアル群 $H_{\mathbb{Q},n}(l)$ に対する類体である．

節の最後に解析的な考察を行う．代数体 k において, k の素イデアル全体の集合を P とすると, $M\subset P$ に対して

$$\mu(s,M):=\sum_{\mathfrak{p}\in M}\frac{1}{(\mathrm{N}_{k/\mathbb{Q}}\mathfrak{p})^s}$$

とおくと $\mathrm{Re}(s)>1$ で右辺は絶対収束し, 複素変数 s に関する正則関数となる．これは k の Dedekind ゼータ関数の部分級数である．

定義　代数体 k の素イデアル全体の集合 P の部分集合 M に対して

$$d(M):=\lim_{s\to 1+0}\frac{\mu(s,M)}{\mu(s,P)}$$

が存在するとき, $d(M)$ を M の **Dirichlet 密度** (Dirichlet density) と呼ぶ.

このとき, 1 次の素イデアルの集合を

$$P^* := \{\mathfrak{p} : k \text{ の素イデアル} \mid \mathrm{N}_{k/\mathbb{Q}}\mathfrak{p} = p\}$$

とおくと, k の素イデアルの“ほとんど”は P^* に属することを表す, 次の定理が成立する.

定理 1.7 代数体 k に対して

$$d(P^*) = 1.$$

また, 次の Dirichlet の算術級数定理の拡張が成立する.

定理 1.8 k を代数体, $H_k(\mathfrak{m})$ を $\mathfrak{m}$ を法とするイデアル群, P を k の素イデアル全体の集合とする. このとき, $I_k(\mathfrak{m})/H_k(\mathfrak{m})$ の任意の剰余類 $C_\mathfrak{m}$ に対して

$$d(C_\mathfrak{m} \cap P) = d(C_\mathfrak{m} \cap P^*) = \frac{1}{h_\mathfrak{m}}, h_\mathfrak{m} = [I_k(\mathfrak{m}) : H_k(\mathfrak{m})]$$

である. 特に, 任意の $C_\mathfrak{m}$ は $N\mathfrak{p} = p$ となる素イデアルを無限に多く含む.

ここで $k = \mathbb{Q}, \mathfrak{m} = (m)$ とすれば $H_k(\mathfrak{m})$ は $\mathbb{Q}$ の素イデアル全体の集合 P となる. したがって, $I_\mathbb{Q}(\mathfrak{m})/P \simeq \mathbb{Z}/p\mathbb{Z}$ となり, 通常の Dirichlet の算術級数定理の一般化であることがわかる.

類体論は Abel 体の理論であるが, 必ずしも Abel 拡大ではない一般の Galois 拡大に対しての情報ももたらす.

(1) 式と Galois 群の $P_\mathfrak{p}$ への作用が推移的なことにより, 同じ $\mathfrak{p}$ の上の素イデアルの Frobenius 自己同型は同じ共役類に属し, Frobenius 自己同型の共役類は $\mathfrak{p}$ の上の素イデアルの取り方に依らず $\mathfrak{p}$ ごとに一つずつ定まる. この Frobenius 自己同型の共役類のことを **Frobenius 共役類** (Frobenius conjugacy class) と呼ぶ.

このとき, 次の定理が成立する.

定理 1.9 (Chebotarev の密度定理, Chebotarev, 1926) K/k を代数体の Galois 拡大とする. Galois 群 $G := \mathrm{Gal}(K/k)$ の一つの共役類 $C_\sigma := \{\tau\sigma\tau^{-1} \mid \tau \in G\}$ を定める. このとき K/k で不分岐な k の素イデアルの集合を I_k とすると

$$M(C_\sigma) := \{\mathfrak{p} \in I_k \mid \mathfrak{p} \text{ の Frobenius 共役類が } C_\sigma \text{となる }\}$$

に対して

$$d(M(C_\sigma)) = \frac{\#C_\sigma}{\#G}$$

が成立する.

このとき, $\mathfrak{p}$ に対して定まる, Frobenius 自己同型の共役類の型と $\mathfrak{p}$ の分解の仕方が対応することが Artin により示されている. 以下に, A_5 拡大体における分解の例を述べる.

例 1.10 (A_5 拡大体における分解) $\mathrm{Gal}(K/k) = A_5$ のとき, 各共役類の個数と代表元は

$e = (1)(2)(3)(4)(5)$	1 個
$(12)(34)(5)$	15 個
$(123)(4)(5)$	20 個
(12345)	12 個
(13452)	12 個

となる. このとき, 各分解の型の密度は次のようになる.

$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4\mathfrak{P}_5,$	$\dfrac{1}{60}$
$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_1^{'}\mathfrak{P}_2$	$\dfrac{15}{60} = \dfrac{1}{4}$
$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_2^{'}$	$\dfrac{20}{60} = \dfrac{1}{3}$
$\mathfrak{p} = \mathfrak{P}$	$\dfrac{24}{60} = \dfrac{2}{5}$

共役類の最後の 2 つの型は同じであるから, 2 つ合わせれば分解の最後の型と対応する.

例 1.10 のような現象は, 素イデアル分解の様子が Galois 群のみによって統制されていることを表している. 定理 1.9 は特に, Galois 拡大 K/k において完全分解する素数の密度は $1/\#G$ であることを表しているが, この逆とも言える次の定理が成り立つ.

定理 1.11 K/k を代数体の n 次拡大とし, $P(K/k)$ を K で完全分解する k の素イデアルの成す集合とする. このとき以下は同値である.

(1) $d(P(K/k)) = \frac{1}{n}$.
(2) K/k は Galois 拡大.

さらに次の結果も成り立つ.

定理 1.12 K_1/k, K_2/k を代数体の Galois 拡大とし, $P(K_i/k)$ を K_i で完全分解する k の素イデアルの成す集合とする. このとき以下は同値である.

(1) $K_1 = K_2$.
(2) $P(K_1/k) = P(K_2/k)$.

定理 1.12 は完全分解する素イデアルの集合が, 代数体の Galois 拡大における完全不変量であることを述べている. この結果は本稿では用いないが, 古典的な類体論から得られる著しい結果であるため紹介した.

類体論は, ある体が与えられたときに, その体のイデアルの類によって, Abel 拡大すなわち類体を統制出来ることを述べている. しかしながら, 全ての Abel 拡大の合併である最大 Abel 拡大がどのように構成出来るのかという問題の解答は, 類体論の証明からは得ることができない. 実際, 実 2 次体に対してさえも, このような問題は難しく, 現在でも一般には未解決問題である.

有理数体 $\mathbb{Q}$ の場合は古くから Kronecker-Weber の定理として知られている.

定理 1.13 $\mathbb{Q}$ の任意の Abel 拡大 K に対して, ある自然数 m が存在し, K はイデアル群 H_m に対する類体となる. 特に, K はシュトラール S_m に対する類体 $\mathbb{Q}(\zeta_m)$ に含まれる.

これにより, 最大 Abel 拡大は円の n 分体全ての合併により得られる.

すでに解決されているケースとしては, 与えられた体が, 虚 2 次体の場合, CM 体 (総実代数体上の総虚な 2 次拡大) の場合, 有限体上の 1 変数代数関数体の場合, 局所体の場合が挙げられる.

次章では, 虚 2 次体の場合を扱う. $\mathbb{Q}$ においての円分体の類似物として, 各虚 2 次体 k に対応する楕円曲線の等分点による体を用いることによって k 上の最大 Abel 拡大を得ることができる. これは類体論の完成と同時に高木貞治自身により解決された $\mathbb{Q}$ の場合を除いて, 最も単純なケースである.

以下の場合は本論文では扱わないが, CM 体の場合については, 虚 2 次体場合の一般化となっており, 志村 · 谷山が楕円曲線の高次元化である Abel 多様体の等分点を用いることにより最大 Abel 拡大を得ることができることを示した. また, 有限体上の 1 変数代数関数体の場合は Drinfeld により, Drinfeld 加群の等分点, 局所体の場合には Lubin-Tate により形式群の等分点を用いれば良いことが知られている.

1.2 楕円関数

この節では楕円関数と Weierstrass の $\wp$ 関数, さらに楕円関数体について述べる. 次節で述べるように, 楕円関数は $\wp$ 関数を通して, 楕円曲線と密接に関係する. まず, 楕円関数の定義を与える.

定義　$\mathbb{R}$ 上独立な複素数 ϖ_1, ϖ_2 に対して

$$\mathfrak{m}(\varpi_1, \varpi_2) := \mathbb{Z}\varpi_1 + \mathbb{Z}\varpi_2 = \{m\varpi_1 + n\varpi_2 \mid m, n \in \mathbb{Z}\}$$

を**周期加群**と呼ぶ. ただし, ϖ_1, ϖ_2 の添字は, 必要ならば入れ替えて, $\mathrm{Im}(\varpi_1/\varpi_2) > 0$ となるように取るものとする.

定義 $f(z)$ を $\mathbb{C}$ 上で定義された有理型関数とする. $f(z)$ が $\mathbb{R}$ 上独立した二つの周期 ϖ_1, ϖ_2 を持つとき, **楕円関数** (elliptic function) と呼ぶ. このとき $f(z)$ は $\mathbb{Z}$ に係数を持つ ϖ_1, ϖ_2 の線型結合のすべてを周期に持っており, 楕円関数 $f(z)$ の周期加群を $\mathfrak{m}(\varpi_1, \varpi_2)$ で表す.

また, 周期加群 $\mathfrak{m}(\varpi_1, \varpi_2)$ は加法群 $\mathbb{C}$ の離散閉部分群であるから, 剰余群 $\mathbb{C}/\mathfrak{m}(\varpi_1, \varpi_2)$ は自然に位相群となり, 複素トーラスを与える. したがって, ϖ_1, ϖ_2 を周期に持つ楕円関数は複素トーラス $\mathbb{C}/\mathfrak{m}(\varpi_1, \varpi_2)$ 上の有理型関数と見なすことができ, 逆に $\mathbb{C}/\mathfrak{m}(\varpi_1, \varpi_2)$ 上の有理型関数は ϖ_1, ϖ_2 を周期に持つ楕円関数を与えることがわかる.

与えられた周期加群に対して, それを周期として持つような楕円関数はあるのだろうか. 言い換えれば, 複素トーラス上に定数関数でない有理型関数は存在するのだろうか. この答えは肯定的であり, 次のように与えられる Weierstras の $\wp$ 関数を考えれば良い.

定義　$\mathfrak{m} := \mathfrak{m}(\varpi_1, \varpi_2)$ を周期加群とする. このとき, 級数

$$\wp(z) = \wp(\mathfrak{m}; z) := \frac{1}{z^2} + \sum_{\varpi \in \mathfrak{m} \setminus \{0\}} \left(\frac{1}{(z-\varpi)^2} - \frac{1}{\varpi^2} \right)$$

を **Weierstrass の $\wp$ 関数** (Weierstrass elliptic function) と呼ぶ.

定理 1.14　$\mathfrak{m} := \mathfrak{m}(\varpi_1, \varpi_2)$ を周期加群とする. このとき $\wp(\mathfrak{m}; z)$ は $\mathbb{C}$ 上の有理型関数であり, $\wp(\mathfrak{m}; z)$ の極は $\mathfrak{m}$ の各点, すなわち $m\varpi_1 + n\varpi_2 (m, n \in \mathbb{Z})$ であり, それらの位数は 2 である. さらに, $\wp(\mathfrak{m}; z)$ は $\mathfrak{m}(\varpi_1, \varpi_2)$ を周期加群として持つ楕円関数である.

Weierstrass の $\wp$ 関数の微分は次のような性質を持つ.

命題 1.15　$\mathfrak{m}$ を周期加群とする. このとき $\wp(\mathfrak{m}; z)$ の導関数は

$$\wp'(\mathfrak{m}; z) = \sum_{\varpi \in \mathfrak{m}} \frac{1}{(z-\varpi)^3}$$

であり, 極は $\mathfrak{m}$ の各点であり, それらの位数は 3 である. さらに, $\wp'(\mathfrak{m}; z)$ は $\mathfrak{m}$ を周期加群として持つ楕円関数である.

また, 次の $\wp$ 関数の加法公式が成り立つ.

定理 1.16 $\mathfrak{m}$ を周期加群とする. $z_1, z_2 \in \mathbb{C}$ に対して加法公式

$$\wp(z_1+z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)}\right),$$
$$\wp'(z_1+z_2) = \frac{\wp'(z_1)(\wp(z_1+z_2)-\wp(z_2)) - \wp'(z_2)(\wp(z_1+z_2)-\wp(z_1))}{\wp(z_1)-\wp(z_2)}$$

が成立する.

次の定理は $\wp(z)$, $\wp'(z)$ の関係性を述べており, 楕円曲線と $\wp$ 関数の関係を示唆する重要な定理である.

定理 1.17 $\wp(z)$, $\wp'(z)$ は **Weierstrass の関係式** (Weierstrass equation) と呼ばれる次の関係式を満たす:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

さらに, この関係式の右辺の $\wp(z)$ についての三次多項式は重根を持たない. ただし

$$g_2 = g_2(\mathfrak{m}) := 20 \cdot 3G_4(\mathfrak{m}) = 60 \sum_{\varpi \in \mathfrak{m}-\{0\}} \frac{1}{\varpi^4},$$
$$g_3 = g_3(\mathfrak{m}) := 28 \cdot 5G_6(\mathfrak{m}) = 140 \sum_{\varpi \in \mathfrak{m}-\{0\}} \frac{1}{\varpi^6}$$

であり, $G_k(\mathfrak{m})$ は $\mathfrak{m}$ に対しての Eisenstein 級数を表す.

実際, Weierstrass の関係式の右辺の $\wp(z)$ についての三次多項式の根は

$$\epsilon_1 := \wp(\frac{\varpi_1}{2}), \epsilon_2 := \wp(\frac{\varpi_1+\varpi_2}{2}), \epsilon_3 := \wp(\frac{\varpi_2}{2})$$

である. すなわち $\Delta(\mathfrak{m})$ を右辺の $\wp(z)$ についての三次多項式の判別式とすれば

$$\begin{aligned}\Delta(\mathfrak{m}) &= g_2^3 - 27g_3^2 \\ &= 16\{(\epsilon_1-\epsilon_2)(\epsilon_2-\epsilon_3)(\epsilon_3-\epsilon_1)\} \neq 0\end{aligned}$$

が成り立つ.

また, $\mathbb{C}$ 上の有理型関数全体は体を成し, $\mathbb{C}(\wp(\mathfrak{m};z))$ はその部分体になることに注意すれば, 次の著しい結果が示される.

定理 1.18 $\mathfrak{m}$ を周期加群, $f(z)$ を楕円関数で $\mathfrak{m}$ を含むような周期加群を持つものとする. このとき, $f(z)$ は $\wp(\mathfrak{m};z)$ による二つの有理式 $Q(\wp(\mathfrak{m};z)), R(\wp(\mathfrak{m};z)) \in \mathbb{C}(\wp(\mathfrak{m};z))$ と $\wp'(\mathfrak{m};z)$ により

$$f(z) = Q(\wp(\mathfrak{m};z)) + R(\wp(\mathfrak{m};z)) \cdot \wp'(\mathfrak{m};z)$$

と表される.

また, 次のような $\mathbb{C}$ 上の有理型関数全体の成す体の部分体を考えることができる.

定義 $\mathfrak{m}$ を周期加群とする. このとき

$$K_{\mathfrak{m}} = \{f(z) \mid f : \text{楕円関数で } \mathfrak{m} \text{ を含むような周期加群を持つもの}\}$$

を**楕円関数体** (field of elliptic functions) と呼ぶ.

実際, $f, g \in K_{\mathfrak{m}}$ の周期加群を $\mathfrak{m}_1, \mathfrak{m}_2$ とすれば $f+g$ の周期加群 $\mathfrak{m}$ は $\mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \mathfrak{m}$ となり, 和について閉じる. 積についても同様である. f の $\mathbb{C}$ 上の有理型関数全体の成す体においての逆元を考えれば, 周期もまた $\mathfrak{m}_1$ であり, $K_{\mathfrak{m}}$ 体を成すことがわかる.

また, 定数関数は任意の複素数を周期として持つため, 楕円関数体に含まれる. したがって, 定数関数と $\mathbb{C}$ を同一視することにより楕円関数体は $\mathbb{C}$ の拡大体と見ることができる.

定理 1.18 と Weierstrass の関係式から次が従う.

系 1.19 $\mathfrak{m}$ を周期加群とするとき, 次が成立する.

(1) $K_{\mathfrak{m}} = \mathbb{C}(\wp(\mathfrak{m};z), \wp'(\mathfrak{m};z))$.
(2) $K_{\mathfrak{m}}$ は $\wp(\mathfrak{m};z)$ に関する 1 変数有理関数体 $\mathbb{C}(\wp(\mathfrak{m};z))$ の 2 次拡大体である.
(3) X, Y を二つの独立変数とするとき, $K_{\mathfrak{m}}$ は整域 $\mathbb{C}[X,Y]/(Y^2 - 4X^3 + g_2(\mathfrak{m})X + g_3(\mathfrak{m}))$ の商体と $\mathbb{C}$ 同型である.

このことから, 楕円関数体 $K_{\mathfrak{m}}$ は二つの複素数 $g_2(\mathfrak{m}), g_3(\mathfrak{m})$ によって決定されることがわかる.

1.3 楕円曲線

この節では, 楕円関数と楕円曲線の関係について述べる. まず, 一般の体 K 上で楕円曲線を定義する.

定義　体 K の射影平面を $\mathbb{P}^2(K)$ とする. $\mathbb{P}^2(K)$ 上の次の関係式により与えられる非特異な種数 1 の 3 次曲線を**楕円曲線** (elliptic curve) と呼ぶ :

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \quad (\gamma_2, \gamma_3 \in K).$$

ここで, 体 K の標数が 2 でも 3 でもなければ, 変数変換により

$$E : y^2z = 4x^3 - \gamma_2xz^2 + \gamma_3z^3 \quad (\gamma_2, \gamma_3 \in K)$$

と書くことができる. さらに, E が非特異であることから, 右辺の 3 次多項式が重根を持たない. よって, 判別式に関する条件

$$\Delta(E) = \gamma_2^3 - 27\gamma_3^2 \neq 0$$

を満たさなければならない. E は Weierstrass の関係式を斉次化した形と同じであり, 重根を持たないという条件も一致している.

また, 今後必要に応じて $(x : y : 1)$ と (x, y) を同一視して, 2 次元アフィン空間での曲線

$$y^2 = 4x^3 - \gamma_2x + \gamma_3 \quad (\gamma_2, \gamma_3 \in K)$$

も考える.

楕円曲線上の有理点に対して次のような和を定義することができる. この和は標数に依らずに定義することができるが, 本論文では簡単のため標数が 2 でも 3 でもないとして定義を与える.

定義　K を標数が 2 でも 3 でもない体とする. $\mathbb{P}^2(K)$ 上の楕円曲線 E

$$\begin{aligned} &E : y^2z = 4x^3 - \gamma_2xz^2 + \gamma_3z^3 \quad (\gamma_2, \gamma_3 \in K), \\ &\Delta(E) = \gamma_2^3 - 27\gamma_3^2 \neq 0 \end{aligned}$$

に対して, E 上の二つの K 上の有理点

$$P := (x_1 : y_1 : 1),\ Q := (x_2 : y_2 : 1)$$

に対して, P, Q を通る $\mathbb{P}^2(K)$ 上の直線を l とする. ただし, $P = Q$ のときは l を P の接線とする. l と E が交わる第 3 の点を $R = (x_3 : y_3 : 1)$ とするとき, E 上の加法は

$$P + Q := (x_3 : -y_3 : 1) \tag{2}$$

で与えられる. 加法の単位元は無限遠点 $O = (0 : 1 : 0)$ である.

この和について次が成り立つ.

命題 1.20 (2) で定めた加法により, 楕円曲線上の有理点は Abel 群をなす.

上の命題で述べた群は重要であるから, 定義の形で述べておく.

定義 E を体 K 上の楕円曲線とする. このとき, E 上の K 有理点全体を $E(K)$ と書き, **Mordell-Weil 群** (Mordell-Weil group) と呼ぶ.

Mordell-Weil 群について次の定理が知られている.

定理 1.21 (Mordell-Weil, 1922) $E(K)$ は有限生成 Abel 群である. すなわち

$$E(K) \simeq \mathbb{Z}^{\oplus r} \oplus E(K)_{\mathrm{tors}}$$

と書ける. ただし $E(K)_{\mathrm{tors}}$ は $E(K)$ のねじれ部分を表す.

一般に体 K に対して, $E(K)$ の構造の決定は難しく, 楕円曲線についての重要な問題のひとつである. $K = \mathbb{Q}$ の場合は完全に決定されており, 次が知られている.

定理 1.22 (Mazur, 1977) $E(\mathbb{Q})_{\mathrm{tors}}$ 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) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, 1 \leq m \leq 4$.

楕円曲線の間の同型は次のように定義される.

定義 E_1, E_2 を体 K 上の楕円曲線とする. 写像 $\phi : E_1 \to E_2$ が次の条件を満たすとき**同種写像** (isogeny map) と呼び, E_1, E_2 は**同種** (isogenous) であると言う.

(1) $P = (x, y) \in E_1$ に対して, $\phi(P) \in E_2$ の各座標が x, y の有理式で表される.
(2) 加法に関して準同型である.

全単射である同種写像 $\phi : E_1 \to E_2$ が存在するとき, E_1 と E_2 は**同型** (isomorphic) であると言う.

同種写像の重要な例として, m 倍写像が挙げられる.

定義 E を標数が 0 の体 K 上の楕円曲線とする. このとき $m \in \mathbb{Z} \setminus \{0\}$ に対して

$$[m] : E \ni P \longmapsto mP \in E$$

を m 倍写像と呼ぶ. m 倍写像の核, すなわち位数 m のねじれ元のなす $E(K)_{\mathrm{tors}}$ の部分群を $E[m]$ と書く. また, K に $E[m]$ の元全ての (x, y) 座標を添加した体を $K(E[m])$ と書く.

$E[m]$ の構造は次のようになる.

定理 1.23 E を標数 0 の体 K 上の楕円曲線とする. このとき $m \in \mathbb{Z} \setminus \{0\}$ に対して

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

K を代数体とすると, 拡大体 $K(E[m])$ に対して次が成り立つ.

命題 1.24 K を代数体, K 上の楕円曲線を

$$E : y^2 = 4x^3 - \gamma_2 x + \gamma_3 \quad (\gamma_2, \gamma_3 \in K)$$

とする. このとき $P = (x, y) \in E[m]$, すなわち E の位数 m の点とすると, その座標 x, y は $\mathbb{Q}$ 上代数的である. また, $K(E[m])$ は K 上 Galois 拡大である.

K のアフィン空間で考えた楕円曲線の K 有理点全体の集合

$$E(K) := \{(x, y) \mid x, y \in K, y^2 = 4x^3 - \gamma_2 x + \gamma_3 (\gamma \in \mathbb{Q})\} \cup \{O\}$$

を考える. ここで O は無限遠点を表し, これも K 有理点に含めるものとする. このとき, $\sigma \in \mathrm{Gal}(K(E[m])/K)$ による $P \in E(K)$ への作用が

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) & (P = (x, y)) \\ O & (P = O) \end{cases}$$

により定まる.

定理 1.23 より, $E[m]$ の基底 P_1, P_2 が存在する. $E[m]$ 上の準同型 h を考えれば, $a_h, b_h, c_h, d_h \in \mathbb{Z}/m\mathbb{Z}$ として

$$h(P_1) = a_h P_1 + b_h P_2,$$
$$h(P_2) = c_h P_1 + d_h P_2$$

と書け, h に対して行列

$$A_h = \begin{pmatrix} a_h & b_h \\ c_h & d_h \end{pmatrix}$$

が対応する. 特に, $E[m]$ の自己同型に対しては, 逆写像が存在し, ここから逆行列が得られ, 正則行列が対応することがわかる. 命題 1.24 より, $\sigma \in \mathrm{Gal}(K(E[m])/k)$ から $E[m]$ の自己同型が得られる. したがって, 対応する正則行列が求まり, Galois 表現が得られる.

定理 1.25 K を代数体, E を K 上の楕円曲線とする. このとき

$$\rho_m : \mathrm{Gal}(K(E(m))/K) \hookrightarrow GL_2(\mathbb{Z}/m\mathbb{Z}).$$

定理 1.25 は, 円分体 $\mathbb{Q}(\zeta_m), \zeta_m = e^{\frac{2\pi i}{m}}$ に対しての

$$t_m : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})) \hookrightarrow GL_1(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^\times$$

の類似となっている.

定理 1.25 の ρ_m はいつ全射になるだろうか. 実は定理 1.26 で述べるように, かなり多く楕円曲線については, ほとんどの m に対して全射となることが知られている.

$\mathrm{G}L_2(\mathbb{Z}/m\mathbb{Z})$ は $m > 2$ であるとき, 非可換群である. 次章の目標は, 類体の構成すなわち Abel 拡大の構成であるから, ρ_m が全射になってしまうことは, むしろ都合が悪い. しかしながら, 次節で述べる, 虚数乗法を持つ楕円曲線に対しては $\mathrm{Gal}(K(E(m))/K)$ は $\mathrm{G}L_2(\mathbb{Z}/m\mathbb{Z})$ より真に小さい Abel 群となることがわかる.

次の Serre により与えられた定理は, 先ほどの ρ_m がいつ全射になるかを述べている.

定理 1.26 (Serre, 1972) E を代数体 K 上の虚数乗法を持たない楕円曲線とする. このとき E により決まる自然数 n が存在し, n と互いに素である m に対して Galois 表現

$$\rho_m : \mathrm{Gal}(K(E(m))/K)) \to GL_2(\mathbb{Z}/m\mathbb{Z})$$

は同型写像となる.

次に $K = \mathbb{C}$ とし, 楕円曲線と周期加群の関係を述べる.

定理 1.27 $\gamma_2, \gamma_3 \in \mathbb{C}$ が

$$\gamma_2^3 - 27\gamma_3^2 \neq 0$$

を満たすならば, 周期加群 $\mathfrak{m} = \mathfrak{m}(\varpi_1, \varpi_2)$ で

$$g_2(\mathfrak{m}) = \gamma_2,\ g_3(\mathfrak{m}) = \gamma_3$$

を共に満たすものが存在する.

これは, 周期加群 $\mathfrak{m}$ に対しての $\wp$ 関数により, 与えられた $\gamma_2, \gamma_3 \in \mathbb{C}$ を係数に持つ楕円曲線を構成することを表している.

これにより, 次の同型が $\mathbb{C}$ 上全ての楕円曲線に対して存在することがわかる.

定理 1.28 $\mathfrak{m}$ を周期加群とすると

$$f : \mathbb{C}/\mathfrak{m} \ni z \longmapsto (\wp(z,\mathfrak{m}), \wp'(z,\mathfrak{m}), 1) \in E(\mathbb{C})$$

は複素解析的同型写像となる.

f は加法に関しての準同型である. $z_1, z_2 \in \mathbb{C}$ に対して,

$$x_1 := \wp(z_1),\ y_1 := \wp'(z_1),\ x_2 := \wp(z_2),\ y_2 := \wp'(z_2)$$

と置けば, 4 変数の有理式 $F(X_1,Y_1,X_2,Y_2), G(X_1,Y_1,X_2,Y_2) \in \mathbb{Q}(X,Y,Z,W)$ により

$$\begin{aligned} x_3 &:= \wp(z_1+z_2) = F(x_1,y_1,x_2,y_2), \\ y_3 &:= \wp^{'}(z_1+z_2) = G(x_1,y_1,x_2,y_2), \end{aligned}$$

の形に書くことができる. ここで, 定理 1.28 を用いれば

$$\begin{aligned} f(z_1) &= (x_1 : y_1 : 1), \\ f(z_2) &= (x_2 : y_2 : 1), \end{aligned}$$

に対して,

$$f(z_1+z_2) = (F(x_1,y_1,x_2,y_2) : G(x_1,y_1,x_2,y_2) : 1)$$

と表される. これは写像 $E \times E \to E$ を与え, 複素トーラスにおける加法を楕円曲線上に移したものである. この写像によって定まる楕円曲線上での加法は, 前節で述べた楕円曲線上での加法と一致する. したがって, 楕円曲線上での加法は, 楕円関数の言葉で言えば $\wp$ 関数の加法公式と対応し, 定理 1.28 は加法に関する群同型写像にもなる. この同型により楕円曲線と周期加群 $\mathfrak{m}$ から定まる Riemann 面 $\mathbb{C}/\mathfrak{m}$ を演算込みで同一視することができる.

ここで, 楕円関数体と代数関数体 $\mathbb{C}(x,y)$ が同型になる必要十分条件は次のようになる.

定理 1.29 $\mathbb{C}$ 上の楕円曲線を

$$\begin{aligned} &E : y^2z = 4x^3 - \gamma_2 x + \gamma_3 \quad (\gamma_i \in C), \\ &\Delta(E) = \gamma_2^3 - 27\gamma_3^2 \neq 0 \end{aligned}$$

とする. このとき, 代数関数体 $\mathbb{C}(x,y)$ と楕円関数体 $K_{\mathfrak{m}} = \mathbb{C}(\wp(z), \wp'(z))$ に対して以下は同値である.

(1) $\mathbb{C}(x,y) \simeq K_{\mathfrak{m}}$.

(2) $\dfrac{{\gamma_2}^3}{{\gamma_2}^3 - 27{\gamma_3}^2} = \dfrac{{g_2}^3}{{g_2}^3 - 27{g_3}^2}$.

定義 周期加群 $\mathfrak{m}$ に対する楕円関数体に対して, 複素数

$$j(\mathfrak{m}) := 12^3 \frac{{g_2}^3}{{g_2}^3 - 27{g_3}^2}$$

を $K_{\mathfrak{m}}$ の**モデュラス** (modulus) と呼ぶ.

定理 1.29 からわかるように, モデュラスは楕円関数体の完全不変量である. また, $\mathfrak{m}(\varpi_1, \varpi_2)$ に対して $\tau := \varpi_1/\varpi_2 \in \mathcal{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ とすると,

$$j(\mathfrak{m}) = j(\varpi_1, \varpi_2) = j(\tau, 1) =: j(\tau)$$

とできる. 二つ目の等号では Eisenstein 級数が

$$G_k(\varpi_1, \varpi_2) = \frac{1}{\varpi_2^k} G_k(\tau, 1)$$

を満たし, $k > 2$ で $G_k(\tau, 1)$ は上半平面で広義一様に絶対収束するという性質を用いた. これにより, $j(\tau)$ は上半平面 $\mathcal{H}$ で正則な関数であることがわかった.

定義 上半平面 $\mathcal{H}$ で正則な関数 $j(\tau)$ を j **不変量** (j-invariant) と呼ぶ.

$SL_2(\mathbb{Z})$ は上半平面 $\mathcal{H}$ に対して, 1 次分数変換として作用していることに注意しておく. ここで次が成立する.

定理 1.30 周期加群 $\mathfrak{m}_1, \mathfrak{m}_2$, 各々に対し $\tau_1, \tau_2 \in \mathcal{H}$ とする. このとき, 以下は同値となる.

(1) $\mathbb{C}/\mathfrak{m}_1 \simeq \mathbb{C}/\mathfrak{m}_2$.
(2) $\tau_1 = A(\tau_2)$ を満たす $A \in SL_2(\mathbb{Z})$ が存在する.

定理 1.31 $A \in SL_2(\mathbb{Z}), \tau \in \mathcal{H}$ に対して

$$j(\tau) = j(A(\tau)).$$

定理 1.31 は $j(\tau)$ が $SL_2(\mathbb{Z})$ に対する重さ 0 のモジュラー形式であることを表している. j 不変量は楕円関数体の完全不変量であったが, 定理 1.30, 定理 1.31 から, $\mathbb{C}/\mathfrak{m}$ の複素解析的同型に対しての完全不変量でもあることがわかった.

定理 1.28, 定理 1.29, 定理 1.30, 定理 1.31 をまとめれば次が成り立つ.

定理 1.32 $\mathfrak{m}_1, \mathfrak{m}_2$ を周期加群とし, それぞれに対応する楕円関数体を $K_{\mathfrak{m}_1}, K_{\mathfrak{m}_2}$, Weierstrass 関係式から定まる $\mathbb{C}$ 上の楕円曲線を $E_{\mathfrak{m}_1}, E_{\mathfrak{m}_2}$ とすると, 以下は同値である.

(1) $j(\mathfrak{m}_1) = j(\mathfrak{m}_2)$.
(2) $K_{\mathfrak{m}_1} \simeq K_{\mathfrak{m}_2}$.
(3) $\mathbb{C}/\mathfrak{m}_1 \simeq \mathbb{C}/\mathfrak{m}_2$.
(4) $\tau_1 = A(\tau_2)$ を満たす $A \in SL_2(\mathbb{Z})$ が存在する.
(5) $E_{\mathfrak{m}_1} \simeq E_{\mathfrak{m}_2}$.

これにより, 周期加群から定まる種数 1 の Riemann 面, 楕円関数体, 楕円曲線のすべてが同一視できることがわかった.

以上の準備の元, 次章では虚 2 次体上の Hilbert 類体の構成を行う.

2 虚 2 次体上のシュトラール類体の構成

Kronecker-Weber の定理として知られているように, $\mathbb{Q}$ 上の任意の Abel 拡大は円分体に含まれる. これと並行して, 虚 2 次体上の任意の Abel 拡大は, 対応する楕円曲線の j 不変量とねじれ点の x 座標 (例外的に $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ のときはそれぞれ x 座標の 2 乗, 3 乗) を添加した体に含まれる. この事実について, 証明を与えずに概観するのがこの章の目標である. これらを踏まえると, 次章で扱うレムニスケートが $\mathbb{Q}(\sqrt{-1})$ 上での円の類似物となり得ることが類体論的に理解出来る. 実際, 任意の Abel 拡大がレムニスケートの等分点を添加した体に含まれる. 2.1 節, 2.2 節は共に [河田], [Sil2] に基づいている.

2.1 虚 2 次体上の Hilbert 類体の構成

まず, 虚数乗法の定義を与える.

定義 $\mathfrak{m}$ を周期加群とする. このとき, $\mathfrak{m}$ に対して, $\lambda\mathfrak{m} \subset \mathfrak{m}$ となる $\lambda \in \mathbb{C} \setminus \mathbb{R}$ が存在するとき, $\mathbb{C}/\mathfrak{m}$ は**虚数乗法** (complex multiplication) を持つと呼ぶ.

上のような λ に対して, $f \in K_{\mathfrak{m}}$ は $f(z) = f(\lambda z)$ を満たすことが確かめられる. $\mathbb{C}/\mathfrak{m}$ が虚数乗法を持つための必要十分条件は次のように与えられる.

命題 2.1 $\mathfrak{m}(\varpi_1, \varpi_2)$ を周期加群とする. このとき以下は同値である.

(1) $\mathbb{C}/\mathfrak{m}$ が虚数乗法を持つ.
(2) $\tau = \varpi_2/\varpi_1 \in \mathcal{H}$ が 2 次の代数的数である.

$k=\mathbb{Q}(\sqrt{-m})$ とする．このとき, k の整数環 $\mathcal{O}_k$ は

$$\mathcal{O}_k=\begin{cases}\mathbb{Z}\left[\sqrt{-m}\right]=\mathbb{Z}+\mathbb{Z}\sqrt{-m} & (m\equiv 2,3 \pmod 4)\\ \mathbb{Z}\left[\frac{1+\sqrt{-m}}{2}\right]=\mathbb{Z}+\mathbb{Z}\frac{1+\sqrt{-m}}{2} & (m\equiv 1 \pmod 4)\end{cases}$$

であるから, 周期加群と見なすことができる．したがって, $\mathcal{O}_k$ のイデアル $\mathfrak{a}$ も $\mathbb{Z}$ 基底を持ち, 周期加群とみなすことができる．$\mathfrak{a}$ に対して,

$$A(\mathfrak{a}):=\{\lambda\in\mathbb{C}\mid \lambda\mathfrak{a}\subset\mathfrak{a}\}$$

と置くと $A(\mathfrak{a})$ は環を成す．$A(\mathfrak{a})$ は $\mathbb{C}$ の中にどの位 $\mathbb{C}/\mathfrak{a}$ の虚数乗法になるような $\lambda\in\mathbb{C}$ が存在するかを表している．このとき,

$$A(\mathcal{O}_k)=\mathcal{O}_k$$

となる．右向きの包含は $\mathcal{O}_k$ が環であることからわかる．左向きの包含は $1\in\mathcal{O}_k$ より, $\lambda\in A(\mathcal{O}_k)$ ならば $\lambda\cdot 1\in\mathcal{O}_k$ によりわかる．より一般に次が成り立つ.

命題 2.2 $k=\mathbb{Q}(\sqrt{-m})$ とすると, 以下が成立する.

(1) $\mathfrak{a}\subset\mathcal{O}_k$ に対して, $A(\mathfrak{a})=\mathcal{O}_k$.
(2) $\mathfrak{a}_1,\mathfrak{a}_2\subset\mathcal{O}_k$ に対して, 以下は同値である.
  (i) $\mathfrak{a}_1=\lambda\mathfrak{a}_2$ となる $\lambda\in k$ が存在する.
  (ii) $j(\mathfrak{a}_1)=j(\mathfrak{a}_2)$.

(1) から, $\mathcal{O}_k$ のゼロではないイデアルに対して, $\mathbb{C}/\mathfrak{a}$ は虚数乗法を持つことがわかる. (2) は, j 不変量が k の各イデアル類 C_i ごとに定まることを表している．すなわち, j 不変量はイデアル類に対する不変量である．以降, $j(C_i)$ で k のイデアル類群の各類に対する j 不変量を表す．定理 1.32 から, $\mathfrak{a}_1,\mathfrak{a}_2$ から定まる $\mathbb{C}$ 上の楕円曲線 $E_{\mathfrak{a}_1},E_{\mathfrak{a}_2}$ が同型であるかを調べるためには, $\mathfrak{a}_1,\mathfrak{a}_2$ が k のイデアル類群の同じ類に属するかを調べれば良いこともわかる.

虚数乗法を持つことは $\mathbb{C}/\mathfrak{m}$ 上の自己準同型をより多く持つと考えることができる．したがって, 現代的には虚数乗法は複素トーラスの自己準同型の言葉で記述される．この方法を用いると虚 2 次体と虚数乗法の関係を捉えやすい.

命題 2.3 周期加群を $\mathfrak{m}=\mathbb{Z}\varpi_1+\mathbb{Z}\varpi_2$, $\tau:=\varpi_1/\varpi_2\in\mathcal{H}$ とする．このとき, 複素トーラス $T:=\mathbb{C}/\mathfrak{m}$ の自己準同型環 $\mathrm{End}(T)$ に対して,

$$\mathrm{End}_{\mathbb{Q}}(T):=\mathrm{End}(T)\otimes_{\mathbb{Z}}\mathbb{Q}$$

は有理数体 $\mathbb{Q}$, または, 虚 2 次体 $\mathbb{Q}(\tau)$ に同型である. また, そのとき $\mathrm{End}(T)$ は $\mathbb{Q}(\tau)$ の整数環と同型である.

このことから, 虚 2 次体と虚数乗法の関係は次のようになる.

命題 2.4 $\mathfrak{m}$ を周期加群, $T := \mathbb{C}/\mathfrak{m}$ を複素トーラスとする. このとき, 以下は同値である.

(1) T が虚数乗法を持つ.
(2) $\mathrm{End}_{\mathbb{Q}}(T) = \mathbb{Q}(\sqrt{-m})$ となる $m \in \mathbb{N}$ が存在する.

これらのことから, 虚 2 次体 k に対して,

$$EL(\mathcal{O}_k) := \frac{\{\mathrm{End}(E) \simeq \mathcal{O}_k\text{である楕円曲線 } E/\mathbb{C}\}}{\mathbb{C} \text{ 上の同型}}$$

という商集合を考えれば,

$$\frac{\{\mathrm{End}(E) \simeq \mathcal{O}_k\text{である楕円曲線 } E/\mathbb{C}\}}{\mathbb{C} \text{ 上の同型}} \overset{1:1}{\longleftrightarrow} \frac{\{\mathrm{End}(\mathbb{C}/\mathfrak{m}) \simeq \mathcal{O}_k\text{である周期加群 } \mathfrak{m}\}}{\text{相似変換}}$$

となる. また, j 不変量が $\mathbb{C}$ 上の楕円曲線の完全不変量であり, イデアル類に対する不変量であるから, イデアル類群からの写像

$$Cl_k \ni \overline{\mathfrak{a}} \longmapsto E_{\mathfrak{a}} \in EL(\mathcal{O}_k)$$

が存在する. また, 周期加群を Λ とする楕円曲線 $E_\Lambda \in EL(\mathcal{O}_k)$ に対して, K の 0 でないイデアル $\mathfrak{a}$ による乗法

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r \mid \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

が定義できる. 命題 2.2 の (2) より, $E_{\mathfrak{a}\Lambda}$ と $E_{\mathfrak{b}\Lambda}$ が同型であるための必要十分条件は $\mathfrak{a}$ と $\mathfrak{b}$ が同じイデアル類に属することであるから, イデアル類群 Cl_k の $EL(\mathcal{O}_k)$ への作用が

$$\overline{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

により定まる. この作用は単純推移的となる. すなわち, $EL(\mathcal{O}_k)$ の任意の 2 元 $E_{\Lambda_1}, E_{\Lambda_2}$ に対して, $\overline{\mathfrak{a}} \in Cl_k$ が唯一つ存在して $\overline{\mathfrak{a}} * E_{\Lambda_1} = E_{\Lambda_2}$ とできる.

また, $\mathrm{End}_{\mathbb{Q}}(\mathbb{C}/\mathfrak{m})$ が虚 2 次体であるとき, E は m 倍写像以外のねじれ点を持つ可能性がある.

定義 $\mathrm{End}_{\mathbb{Q}}(\mathbb{C}/\mathfrak{m})$ が虚 2 次体 k であり, $\mathfrak{a}$ を $\mathcal{O}_k$ の整イデアルとする. $\mathfrak{a}$ に対応する楕円曲線を E とする. このとき, $\alpha \in \mathfrak{a}$ に対して, $\mathbb{C}/\mathfrak{a}$ の虚数乗法による自己準同

型 $\alpha : \mathbb{C}/\mathfrak{a} \ni z \mapsto \alpha z \in \mathbb{C}/\mathfrak{a}$ と Weierstrass 標準形から得られる定理 1.28 の同型 $f : E \to \mathbb{C}/\mathfrak{a}$ により, $[\alpha] := f \circ \alpha \circ f^{-1}$ とする. $[\alpha]$ を E の α **倍写像** と呼ぶ. また, $\mathbb{C}$ 上の楕円曲線 E に対して, α 倍写像が存在するとき, E **は虚数乗法を持つ** と呼ぶ.

すなわち, f により, $\mathbb{C}/\mathfrak{a}$ が虚数乗法を持つことと, 対応する $\mathbb{C}$ 上の楕円曲線が虚数乗法を持つことが同一視される.

このとき, m を整数として, $\mathfrak{a} = m\mathcal{O}_k$ をとれば $E[m]$ と一致するため, これは m 倍写像の一般化となっている. ここで楕円曲線 E に対する $\mathfrak{a}$ 等分点の群を定義する.

定義 $\mathrm{End}_{\mathbb{Q}}(\mathbb{C}/\mathfrak{m})$ が虚 2 次体 k であり, $\mathfrak{a}$ を $\mathcal{O}_k$ の整イデアルとする.

$$E[\mathfrak{a}] = \{P \in E \mid \text{任意の}\alpha \in \mathfrak{a} \text{ に対して } [\alpha]P = O\}$$

を E **の** $\mathfrak{a}$ **等分点の群** (group of $\mathfrak{a}$-division points) と呼ぶ.

このとき, $E[\mathfrak{a}]$ の構造に対しては次が成り立つ.

命題 2.5 k を虚 2 次体, $\overline{E} \in EL(\mathcal{O}_k)$, Λ を E に対応する格子, $\mathfrak{a}$ を $\mathcal{O}_k$ の整イデアルとする. このとき, $\phi : E \mapsto \alpha * E$ とすると,

$$\mathrm{Ker}\ \phi = E[\mathfrak{a}] \simeq \mathfrak{a}^{-1}\Lambda/\Lambda \simeq \mathcal{O}_k/\mathfrak{a}$$

が成立する.

したがって, $[\alpha]$ の位数は $\#\mathcal{O}_k/\mathfrak{a}$ であることもわかる.

例 2.6 ($\mathbb{Q}(\sqrt{-1})$ に対応する楕円曲線の虚数乗法) $k = \mathbb{Q}(\sqrt{-1})$ の整数環は $\mathcal{O}_k = \mathbb{Z}[\sqrt{-1}]$ であり, $\mathcal{O}_k$ に対応する楕円曲線は

$$E : y^2 = x^3 + x$$

となる. このとき, E は $\mathcal{O}_k$ による虚数乗法を持つ. 具体的に虚数単位 i に対して $[i]$ は,

$$[i] : E \to E, (x, y) \mapsto (-x, iy)$$

により与えられる.

次に任意の虚 2 次体の j 不変量が代数的数であることを述べる. 楕円曲線に対して, 絶対 Galois 群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の係数への作用を考える. このとき, 次が成り立つ.

命題 2.7 E を $\mathbb{C}$ 上の楕円曲線とする. $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ に対して

$$\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E)$$

が成立する. また j 不変量に対して

$$j(E^\sigma) = j(E)^\sigma$$

が成立する.

$k = \mathrm{End}_{\mathbb{Q}}(\mathbb{C}/\mathfrak{m})$ が虚 2 次体のとき, $\mathfrak{m}$ に対応する楕円曲線を E とすると, $\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E) \simeq \mathcal{O}_k$ であるから, E^σ は再び虚数乗法を持つ楕円曲線となる. 虚数乗法持つ楕円曲線の同型と j 不変量が一致することが必要十分であったことと, j 不変量が虚 2 次体のイデアル類の不変量であったことに注意すれば, j 不変量の共役の個数はイデアル類群の位数以下であることがわかる. さらに, Cl_k の $EL(\mathcal{O}_k)$ への作用は単純推移的となるから $\#Cl_k = \#EL(\mathcal{O}_k)$ であり, j 不変量の共役の個数はイデアル類群の位数と等しくなる. これにより, 次が成立する.

定理 2.8 虚 2 次体のイデアル類群の各類の j 不変量 $j(C_i)$ は代数的であり, 互いに共役である.

実際には, さらに強く次が成立する.

定理 2.9 虚 2 次体のイデアル類群の各類の j 不変量 $j(C_i)$ は代数的整数である.

これは, モジュラー関数を用いた解析的な議論により $j(C_i)$ を根に持つモニック多項式を具体的に構成することにより示すことができる. ([BCHIS, Chapter 3], [Sil2, Chapter 2] 参照)

定理 2.8 とその直前の議論から次が従う.

命題 2.10 k を虚 2 次体とする. このとき $k(j(C_1), \ldots, j(C_{\#Cl_k}))$ は k の Galois 拡大である.

$j(C_i)$ は互いに共役だから $k(j(C_1), \ldots, j(C_{\#Cl_k})) = k(j(C_i))$ である.

次の定理も解析的な議論により示される. ([BCHIS, Chapter 4] 参照)

定理 2.11 k を虚 2 次体, $\mathfrak{p}$ を $\mathcal{O}_k$ の 1 次の素イデアル, $C_\mathfrak{p}$ を $\mathfrak{p}$ を含むイデアル類とする. このとき, 任意の Cl_k の類 C に対して

$$j(C_\mathfrak{p}^{-1}C) \equiv j(C)^{N_{k/\mathbb{Q}}\mathfrak{p}} \quad (\mathfrak{p})$$

が成立する.

定理 2.11 に加えて, 定理 1.8 と定理 1.9 より, 定理 2.10 は楕円曲線ではなく類体論的な考察に重きを置いた方法で証明することもできる.

定理 2.11 から次を示すことができる.

定理 2.12 k を虚 2 次体, $\mathfrak{p}$ を $\mathcal{O}_k$ の 1 次の素イデアル, C_i を Cl_k のイデアル類とする. このとき, 以下は同値である.

(1) $\mathfrak{p}$ が $k(j(C_i))/k$ で完全分解する.
(2) $\mathfrak{p}$ が単項イデアル.

定理 2.12, 定理 1.8 と類体の一意性から, $\mathfrak{p}$ が 1 次の単項な素イデアルのみではなく, 単項な素イデアルが $k(j(C_i))/k$ で完全分解することと同値となる. すなわち, 目標の定理が示される.

定理 2.13 k を虚 2 次体, C_i を Cl_k のイデアル類とする. このとき, $k(j(C_i))$ は k の Hilbert 類体である.

以下に, 虚 2 次体の類数とその対応する楕円曲線の j 不変量の例を与える.

例 2.14 (虚 2 次体の j 不変量) 虚 2 次体 $k = \mathbb{Q}(\sqrt{-m})$ に対して, 類数 h_k とする. このとき j 不変量は k 上類数と同じ次数の代数的整数となる. 特に, 類数が 1 のとき, j 不変量は有理整数となる. たとえば, $\mathbb{Q}(\sqrt{-1})$ のときは $2^6 3^3 = 1728$, $\mathbb{Q}(\sqrt{-2})$ のときは $2^6 5^3$, $\mathbb{Q}(\sqrt{-3})$ のときは 0 となっている.

$k = \mathbb{Q}(\sqrt{-5})$ とすると, $h_k = 2$ となる. $\mathcal{O}_k$ の属するイデアル類を C_1, $\mathfrak{a} = 2\mathbb{Z} + (1 + \sqrt{-5})\mathbb{Z}$ を代表元とする位数 2 のイデアル類を C_2 とすると,

$$j(C_1) = 2^3 5(25 + 13\sqrt{5})^3,\ j(C_2) = 2^3 5(25 - 13\sqrt{5})^3$$

となる. ([BCHIS, Chapter 5] 参照)

$j(C_1),\ j(C_2)$ は共役となっており, 定理 2.13 より, k の Hilbert 類体は

$$k(j(C_1)) = k(j(C_2)) = \mathbb{Q}(\sqrt{-5}, \sqrt{5}) = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$$

となる.

2.2 虚 2 次体上のシュトラール類体の構成

虚 2 次体上のシュトラール類体を対応する楕円曲線を用いて構成する. 順序定理から虚 2 次体上の Abel 拡大はあるシュトラール類体に含まれ, k の最大 Abel 拡大も構成することができる. この節の証明は [Sil2] を参照されたい.

まず, 次が成立する.

定理 2.15 k を虚 2 次体, E を $\mathcal{O}_k$ を虚数乗法にもつ楕円曲線, $\mathfrak{m}$ を $\mathcal{O}_k$ の整イデアルとする. このとき

$$L_{\mathfrak{m}} = k(j(C_i), E[\mathfrak{m}])$$

は $k(j(C_i))$ 上の Abel 拡大である. したがって,

$$L = k(j(C_i), \cup_{\mathfrak{m}} E[\mathfrak{m}])$$

も $k(j(C_i))$ 上の Abel 拡大である.

$L_{\mathfrak{m}}$ は $k(j(C_i))$ 上の Abel 拡大であるが, 残念ながらそのままでは $\mathfrak{m}$ のシュトラール類体にはならない. しかしながら, $L_{\mathfrak{m}}$ はシュトラール類体を含んでおり, 次の Weber 関数を用いることで, $L_{\mathfrak{m}}$ の部分体でシュトラール類体となるものを求めることができる.

定義 虚 2 次体 k の Hilbert 類体を H, H 上で定義された楕円曲線を

$$E : y^2 = 4x^3 - \gamma_2 x + \gamma_3 \quad (\gamma_2, \gamma_3 \in H)$$

とする. このとき $P \in E(H)$ に対して

$$h(P) = h(x, y) = \begin{cases} x & (\gamma_2\gamma_3 \neq 0) \\ x^2 & (\gamma_3 = 0) \\ x^3 & (\gamma_2 = 0) \end{cases}$$

を **Weber 関数** (Weber function) と呼ぶ.

虚 2 次体上のシュトラール類体は次のようになる.

定理 2.16 k を虚 2 次体, E を $\mathcal{O}_k$ を虚数乗法にもつ楕円曲線, $\mathfrak{m}$ を $\mathcal{O}_k$ の整イデアル, $h : E \to \mathbb{C}$ を Weber 関数とする. このとき

$$k(j(C_i), h(E[\mathfrak{m}]))$$

は $\mathfrak{m}$ を法とした k のシュトラール類体である.

系 2.17 k を虚 2 次体, E を $\mathcal{O}_k$ を虚数乗法にもつ楕円曲線, $\mathfrak{m}$ を $\mathcal{O}_k$ の整イデアル, $h : E \to \mathbb{C}$ を Weber 関数とする. このとき, k の最大 Abel 拡大を k^{ab} とすると

$$k^{ab} = k\left(j(C_i), h\left(\cup_{\mathfrak{m}} E[\mathfrak{m}]\right)\right).$$

系 2.17 からは, Weber 関数の値ではなく, $\cup_{\mathfrak{m}} E[\mathfrak{m}]$ の値を全て添加した体, すなわち y 座標をも添加した体と最大 Abel 拡大の関係はどうなるのかという疑問が生まれる.

$K := k(j(C_i))$ とすれば, 一般に $k(j(C_i), h(E[\mathfrak{m}])) \subset k(j(C_i), E[\mathfrak{m}])$ である. さらに $L_{\mathfrak{m}} = k(j(C_i), E[\mathfrak{m}])$ は K 上 Abel 拡大となる. したがって,

$$k^{ab} = K\left(h\left(\cup_{\mathfrak{m}} E[\mathfrak{m}]\right)\right) \subset K\left(\cup_{\mathfrak{m}} E[\mathfrak{m}]\right) \subset K^{ab}$$

がしたがう.

ここで, k の類数が 1 ならば, j 不変量は整数となり, $k^{ab} = K^{ab}$ であり,

$$k\left(h\left(\cup_{\mathfrak{m}} E[\mathfrak{m}]\right)\right) = k\left(\cup_{\mathfrak{m}} E[\mathfrak{m}]\right) = k^{ab}$$

となる. これで, この章の目標である虚 2 次体上のシュトラール類体の構成の概説が終わった.

例 2.18 ($\mathbb{Q}(\sqrt{-1})$ のシュトラール類体) $k = \mathbb{Q}(\sqrt{-1})$ において, $\mathfrak{m} = (3)$ に対するシュトラール類体を構成する. そのためには, 対応する楕円曲線

$$E : y^2 = x^3 + x$$

の位数 3 の点を調べれば良い. ここで, $T = (x, y) \in E$ とすれば, 2 倍公式を用いて計算すれば

$$2T = \left(\frac{x^4 - 2x^2 + 1}{4y^2}, \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3}\right)$$

となる. さらに, $x(T)$ で T の x 座標を表せば, $x(2T) = x(T)$ であるとき, $2T = -T$ であることがわかり, 計算を行えば

$$3T = O$$

であることと,

$$3x^4 + 6x^2 - 1 = 0$$

を満たすことが必要十分であることがわかる. この方程式の 4 つの根は

$$\alpha, -\alpha, \frac{1}{\sqrt{3}\alpha}, -\frac{1}{\sqrt{3}\alpha}, \text{ただし}, \alpha = \sqrt{\frac{2\sqrt{3}-3}{3}}$$

となる. $j(C_i) = 1728$ であり, $\gamma_3 = 0$ より, $h(x, y) = x^2$ であるから

$$k(j(C_i), h(E[3])) = k(h(E[3])) = k(\sqrt{3})$$

となる.

ここで, 上で得た 4 つの x の値を $y^2 = x^3 + x$ に代入することにより, $E[3]$ の y 座標を求めることができる. したがって, 計算により

$$\beta = \sqrt[4]{\frac{8\sqrt{3}-12}{9}} = \sqrt{\frac{2\alpha}{\sqrt{3}}}$$

と置けば,

$$E[3] = \left\{O, (\alpha, \pm\beta), (-\alpha, \pm i\beta), \left(\frac{1}{\sqrt{3}\alpha}, \frac{\pm 2}{\sqrt[4]{27}\beta}\right), \left(\frac{-1}{\sqrt{3}\alpha}, \frac{\pm 2i}{\sqrt[4]{27}\beta}\right)\right\}$$

となり, $E[3]$ の 9 つの元が全て求まる. このとき, β の最小多項式は

$$27x^8 + 72x^4 - 16 = 0$$

であり,

$$\mathrm{Gal}(k(\beta)/\mathbb{Q}) \simeq QD_8 = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^3 \rangle$$

である. ここで, QD_8 は位数 16 の準 2 面体群であり, 2 次の部分体として, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{3})$ を含む. さらに, C_n で位数 n の巡回群を表せば

$$\mathrm{Gal}(k(\beta)/k) \simeq C_8$$

であり, k 上 Abel 拡大となり, 定理 2.15 の主張が成り立っている. 計算により

$$k(E[3]) = k(\beta)$$

であるから,

$$[k(E[3]) : k(h(E[3]))] = 4$$

となることもわかる.

3　レムニスケート

奇である $\beta \in \mathbb{Z}[\sqrt{-1}]$ に対して, 虚 2 次体 $\mathbb{Q}(\sqrt{-1})$ のレムニスケートの β 等分点による拡大体は, $\mathbb{Q}(\sqrt{-1})$ の周期加群 $\mathbb{Z}[\sqrt{-1}]$ に対応する楕円曲線から得られる, (β) のシュトラール類体を含む. このことから, Kronecker-Weber の定理の類似が成り立ち, $\mathbb{Q}$ 上の円分体の類似になることがわかる.

2.1 節ではレムニスケート関数の定義を与え, 基本的な性質を調べる. また, レムニスケート関数の $\wp$ 関数による表示を与える.

2.2 節では, レムニスケート関数の等分点による拡大体の Galois 群を調べ円分体との類似を見る. これは [CH] により 2014 年に与えられた, レムニスケートの等分点による拡大体に対する最小多項式を直接決定する方法によりなされる. 最小多項式が具体的に求まるため, 実例を調べるのに役立つ.

2.3 節では レムニスケート関数の等分点による拡大体が, $\mathbb{Z}[\sqrt{-1}]$ のどのようなイデアルのシュトラール類体であるかを述べる. さらに, 判別式に対しての結果を紹介する.

この章は主に [CH], [Cox2], [Ros] に基づいている.

3.1　定義と基本事項

レムニスケートは二つの定点からの距離の積が一定となるような点の軌跡である. この, レムニスケートを表す具体的な式から弧長を求めることにより, 円の類似物と見なせることを述べる.

極座標によるレムニスケートを表す具体的な式を求める. $a > 0$ とし, $A = (a, 0), A' = (-a, 0)$ を二つの定点とする. $P = (x, y)$ を A, A' の二つの点からの距離 PA, PA' の積が一定値 $c^2 (c > 0)$ であるような点とする. これを式で表せば

$$\sqrt{(x-a)^2 + y^2}\sqrt{(x+a)^2 + y^2} = c^2$$

となる. この両辺を 2 乗し, 式を整理すれば

$$(x^2 + y^2 + a^2)^2 - 4a^2x^2 = c^4$$

となる. この曲線が原点 $O = (0, 0)$ を通るとすると, $c = a$ となり, 上式は

$$(x^2 + y^2)^2 = 2a^2(x^2 - y^2)$$

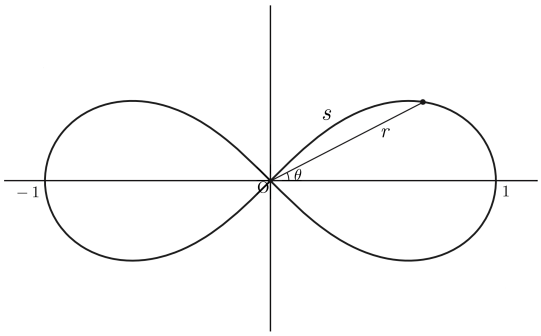
とできる．これを極座標で表す．$x = r\cos\theta$, $y = r\sin\theta$ とし, 倍角の公式を用いれば

$$r^2 = 2a^2\cos 2\theta$$

となる．ここで r の最大値が 1 となるように $a = 1/\sqrt{2}$ と置けば

$$r^2 = \cos 2\theta \tag{3}$$

となる．この曲線を**レムニスケート** (lemniscate) と呼ぶ.



次に弧長を求める．第 1 象限に着目し, θ について解けば

$$\theta = \frac{1}{2}\cos^{-1}(r^2)$$

となり, θ は r の関数となる．ここで, 点 (r_0, θ_0) までの弧長 s_0 は

$$s_0 = \int_0^{r_0} \sqrt{1 + r^2\left(\frac{d\theta}{dr}\right)^2}\, dr$$

によって与えられる．(3) の両辺を微分し計算すれば

$$1 + r^2\left(\frac{d\theta}{dr}\right)^2 = \frac{1}{1 - r^4}$$

となるから, これを用いれば r_0 までのレムニスケートの弧長 s_0 は

$$s_0 = \int_0^{r_0} \frac{1}{\sqrt{1 - r^4}}\, dr \tag{4}$$

と表される．これは円周上の点の弧の長さが

$$\int_0^{r_0} \frac{1}{\sqrt{1 - r^2}}\, dr$$

と表されることの類似となっている.

(4) は広義積分であるが $r_0 = 1$ で収束し, Γ 関数を用いれば

$$\int_0^1 \frac{1}{\sqrt{1-r^4}} dr = \frac{\sqrt{\pi}\ \Gamma\left(\frac{4}{5}\right)}{\Gamma\left(\frac{3}{4}\right)}$$

と表される. このとき, ϖ を

$$\varpi := 2\int_0^1 \frac{1}{\sqrt{1-r^4}} dr \approx 2.62206$$

と定義すれば, レムニスケートの弧長は 2ϖ となり, レムニスケートの弧長の n 等分点間の弧長は $2\varpi/n$ と表される. ϖ は超越数であり, 円周における円周率 π の類似となっている.

ここで (3) の逆関数として

$$\varphi(u) := r \quad (0 \leq u \leq \frac{\varpi}{2})$$

を定義する. これは, 第 1 象限内において, 弧長パラメータによって表示したレムニスケート曲線上の点の極距離を返す関数である.

この $\varphi(u)$ の定義域を拡張していく. $\frac{\varpi}{2} \leq u \leq \varpi$ に対して, $\varphi(u) := \varphi(\varpi - u)$ と定義する. これにより, 定義域を $0 \leq u \leq \varpi$ に拡張できる. さらに, $\varpi \leq u \leq 2\varpi$ に対しては $\varphi(u) := -\varphi(u - \varpi)$ と定義する. したがって, 定義域を $0 \leq u \leq 2\varpi$ をすることができた.

次に $\varphi(u)$ の定義域を周期が 2ϖ となるように $\mathbb{R}$ に拡張する. すなわち $u \in \mathbb{R}$ に対して次のようにレムニスケート上の点 P を対応させる :

- $u = 0 \Rightarrow$ 原点 $O = (0, 0)$ を P とする.
- $u > 0 \Rightarrow$ 原点 O からレムニスケート上を第 1 象限の方向へ動いてゆき, 累計した弧長が u になるまで進み, その点を P とする.
- $u < 0 \Rightarrow$ 原点 O からレムニスケート上を第 3 象限の方向へ動いてゆき, 累計した弧長が $-u$ になるまで進み, その点を P とする.

$|u|$ が大きいときは, P にたどり着くまでに何回も周回する必要があるかもしれないことに注意しておく. 平たく言えば, 周回を法として考えることを意味している. この対応により, $u \in \mathbb{R}$ に対して, $\varphi(u)$ を定義する. このとき, $\varphi(u)$ は上で対応させたレムニスケート上の点 P までの極距離に, P が第 $1, 4$ 象限ならば正の符号, 第 $2, 3$ 象限ならば負の符号をつけたものになっている.

これにより $\varphi : \mathbb{R} \to [-1, 1]$ が定義された．これを**レムニスケート sin 関数** (lemniscate sine) と呼び, 以降 $\mathrm{sn}(u)$ と書く．定義から, $\mathrm{sn}(u)$ は 2ϖ を周期に持ち, $\mathrm{sn}(-u) = -\mathrm{sn}(u)$, $\mathrm{sn}(\varpi - u) = \mathrm{sn}(u)$ が成立する．$\mathrm{sn}(u)$ は通常の円に対する, sin 関数よりも周期が短く, 傾きがやや急な関数になっている．

以下, レムニスケート sin 関数の基本的な性質をまとめておく．

命題 3.1 $u, v \in \mathbb{R}$ に対して次が成立する．

(1) $\mathrm{sn}'^2(u) = 1 - \mathrm{sn}^4(u)$, $\mathrm{sn}''(u) = -2\mathrm{sn}^3(u)$.

(2) $\mathrm{sn}(u \pm v) = \dfrac{\mathrm{sn}(u)\mathrm{sn}'(v) \pm \mathrm{sn}'(u)\mathrm{sn}(v)}{1 + \mathrm{sn}^2(u)\mathrm{sn}^2(v)}$.

(3) $\mathrm{sn}(2u) = \dfrac{2\mathrm{sn}(u)\mathrm{sn}'(u)}{1 + \mathrm{sn}^4(u)}$.

(4) $\mathrm{sn}(3u) = \mathrm{sn}(u)\dfrac{3 - 6\mathrm{sn}^4(u) - \mathrm{sn}^8(u)}{1 + 6\mathrm{sn}^4(u) - 3\mathrm{sn}^8(u)}$.

(1), (2) を見れば $\wp$ 関数と類似がわかる．実際, 後に定義するレムニスケート sin 関数を複素関数として拡張したものは二重周期関数となり, $\wp$ 関数により表される．

(3) は倍角, (4) は 3 倍角の公式に相当する物である．これを用いて, レムニスケートの 6 等分点 $\mathrm{sn}(2\varpi/6)$ を求めることができる．

例 3.2 (レムニスケートの 6 等分点) $r = \mathrm{sn}(2\varpi/6) = \mathrm{sn}(\varpi/3)$ とすると, $u = \varpi/3$ とおけば, $3u = \varpi, \mathrm{sn}(\varpi) = 0$ であるから, 命題 3.1 の (4) から, r は $X^8 + 6X^4 - 3$ の根となる．この多項式はただ一つの正の実数解を持つため

$$r = \sqrt[4]{2\sqrt{3} - 3} \approx 0.825379$$

となる．したがって, レムニスケートの 6 等分点 r は作図可能である．実際, p_i をフェルマー素数 (i は非負整数), すなわち, $p_i = 2^{2^i} + 1$ の形としたとき, $n = 2^k p_0 \cdots p_m$ であることがレムニスケートの n 等分点が作図可能であることの必要十分条件である．これは Abel により示された．$p_0 = 3$ であるから, $n = 6$ のときこの条件を満たしていることがわかる．

n 倍角の公式は次のようになる．

定理 3.3 $n \in \mathbb{N}$ に対して，互いに素な多項式 $P_n(X), Q_n(X) \in \mathbb{Z}[X]$ が存在し,

n が奇数のとき,

$$\mathrm{sn}(nu) = \mathrm{sn}(u)\frac{P_n(\mathrm{sn}^4(u))}{Q_n(\mathrm{sn}^4(u))},$$

n が偶数のとき,

$$\mathrm{sn}(nu) = \mathrm{sn}(u)\mathrm{sn}'(u)\frac{P_n(\mathrm{sn}^4(u))}{Q_n(\mathrm{sn}^4(u))}$$

が成立する．さらに，$Q_n(0) = 1$ が成立する．

これは命題 3.1 から, 帰納的に構成される.

奇数である n に対して, 命題 3.3 において, $u = 2\varpi/n$ とおけば, $nu = 2\varpi, \mathrm{sn}(2\varpi) = 0$ であるから，$r = \mathrm{sn}(\varpi/n)$ は $P_n(x)$ の根となる．次節で示すように，$P_n(X)$ の最大の既約因子を取り出せばレムニスケートの n 等分体の最小多項式を求めることができる．この $P_n(X)$ を **(レムニスケートの)** n **等分多項式** (n-division polynomial) と呼ぶ.

例 3.4 (レムニスケートの 5 等分点) $n = 5$ のとき,

$$\begin{aligned}
P_5(X) &= X^6 + 50X^5 - 125X^4 + 300X^3 - 105X^2 - 62X + 5 \\
&= (5X^2 - 2X + 1)(X^4 - 12X^3 - 26X^2 + 52X + 1), \\
Q_5(X) &= 5X^6 - 62X^5 - 105X^4 + 300X^3 - 125X^2 + 50X + 1 \\
&= (X^2 - 2X + 5)(X^4 + 52X^3 - 26X^2 - 12X + 1).
\end{aligned}$$

したがって，レムニスケートの 5 等分体の最小多項式

$$f(X) = X^{16} + 52X^{12} - 26X^8 - 12X^4 + 1$$

が得られる．$f(X)$ の根は $\epsilon \in \{0, 1, 2, 3\}$ として

$$\begin{aligned}
i^\epsilon \sqrt[4]{a},\ a &= -13 - 6\sqrt{5} - 2\sqrt{85 + 38\sqrt{5}} < 0, \\
i^\epsilon \sqrt[4]{b},\ b &= -13 - 6\sqrt{5} + 2\sqrt{85 + 38\sqrt{5}} < 0, \\
i^\epsilon \sqrt[4]{c},\ c &= -13 + 6\sqrt{5} - 2\sqrt{85 - 38\sqrt{5}} > 0, \\
i^\epsilon \sqrt[4]{d},\ d &= -13 + 6\sqrt{5} + 2\sqrt{85 - 38\sqrt{5}} > 0
\end{aligned}$$

であり，このうち、実根は $\pm\sqrt[4]{c}, \pm\sqrt[4]{d}$ の 4 個である.

n 等分多項式は先ほどの例のように, 実数根のみではなく複素数根も持つ. したがってこれらの根を全て表せるように, レムニスケート sin 関数を複素関数に拡張する.

$|r| < 1$ である $r \in \mathbb{R}$ に対して, $1/(1-r^4)$ のテイラー展開を用いれば

$$\begin{aligned} u = L(r) &= \int_0^r \frac{1}{1-r^4}dt \\ &= \int_0^r \sum_{n=0}^{\infty} \frac{(2n)!}{2^2(n!)^2} t^{4n} dt \\ &= \sum_{n=0}^{\infty} \frac{(4n+1)(2n)!}{2^2(n!)^2} r^{4n+1} \\ &= r + \frac{1}{2}\frac{r^5}{5} + \frac{1\cdot 3}{2\cdot 4}\frac{r^9}{9} + \frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\frac{r^{13}}{13} + \cdots \end{aligned}$$

となる. この級数の逆関数として $\mathrm{sn}(u)$ は定義されていた. この級数は $|r| < 1$ を満たす $r \in \mathbb{C}$ に対しても収束し, r の正則関数 u を定義する. $\frac{du}{dr}(0) = 1$ であるから, 正則関数の逆関数定理により, $r = \mathrm{sn}(u)$ は $u = 0$ の近傍で正則となる.

ここで, $|ir| < 1$ であるから

$$L(ir) = iL(r)$$

が成立する. したがって, 上で取った近傍内の u に対して

$$\mathrm{sn}(iu) = \mathrm{sn}(iL(r)) = \mathrm{sn}(L(ir)) = ir = i\ \mathrm{sn}(u)$$

となり,

$$\mathrm{sn}'(iu) = \mathrm{sn}'(u)$$

を得る.

ここで, 上式と命題 3.1 の (2) を踏まえて, 次のように複素レムニスケート sin 関数を定義する.

定義 $z = x + iy \in \mathbb{C}$ に対して

$$\mathrm{sn}(z) := \frac{\mathrm{sn}(x)\mathrm{sn}'(y) + i\ \mathrm{sn}'(x)\mathrm{sn}(y)}{1 - \mathrm{sn}^2(x)\mathrm{sn}^2(y)}$$

とする. これを**複素レムニスケート sin 関数** (complex lemniscate sine) と呼ぶ.

ここで, 次が成立する.

定理 3.5 $\mathrm{sn}(z)$ は $\mathbb{C}$ 上の有理型関数である. $\mathrm{sn}(z)$ の零点は $(m+in)\varpi, (m,n\in\mathbb{Z})$ であり, $\mathrm{sn}(z)$ の極は $(m+in)\varpi/2, (m,n\in\mathbb{Z}\setminus 2\mathbb{Z})$ であり, それらの位数は 1 である. さらに, $\mathrm{sn}(z)$ は $\Lambda := (1+i)\varpi\mathbb{Z}+(1-i)\varpi\mathbb{Z}$ を周期加群として持つ楕円関数である.

直接的な計算により, $\mathrm{sn}(iz)=i\mathrm{sn}(z), \mathrm{sn}'(iz)=\mathrm{sn}'(z), \mathrm{sn}^2(z)=1-\mathrm{sn}^4(z)$ がわかる.

以降, $\Lambda := (1+i)\varpi\mathbb{Z}+(1-i)\varpi\mathbb{Z}$ とする. 加法公式は次のようになる.

定理 3.6

$$\mathrm{sn}(z+w)=\frac{\mathrm{sn}(z)\mathrm{sn}'(w)+i\ \mathrm{sn}'(z)\mathrm{sn}(w)}{1+\mathrm{sn}^2(z)\mathrm{sn}^2(w)}$$

が両辺が定義される $z,w\in\mathbb{C}$ に対して成立する.

$\mathrm{sn}(z)$ は Λ を周期加群に持つ楕円関数であるから, Λ に対しての $\wp$ 関数 $\wp(\Lambda;z)$ により表される. 具体的には次が成立する.

定理 3.7 $z\in\mathbb{C},\Lambda$ に対して

$$\mathrm{sn}(z)=-2\frac{\wp(\Lambda;z)}{\wp'(\Lambda;z)},$$
$$\mathrm{sn}'(z)=\frac{4\wp(\Lambda;z)^2-1}{4\wp(\Lambda;z)^2+1}.$$

ここで, $\wp(z;\Lambda)$ に対しての Weierstrass 関係式は次のようになる.

定理 3.8 $z\in\mathbb{C},\Lambda$ に対して

$$\wp'(\Lambda;z)^2=4\wp(\Lambda;z)^3+\wp(\Lambda;z)$$

を満たす. すなわち $g_2=-1, g_3=0$ である. (g_2,g_3 の定義は 14 ページ参照)

$\mathbb{Z}[i]=\mathbb{Z}+i\mathbb{Z}$ を周期加群として, $\tau := i/1=i$ と置くと, 周期加群 $\Lambda=(1+i)\varpi\mathbb{Z}+(1-i)\varpi\mathbb{Z}$ に対して,

$$\tau' := \frac{(1+i)\varpi}{(1-i)\varpi}=\tau$$

となり, j 不変量が一致し, これらの周期加群は同型な楕円曲線を与えることがわかる.

$\mathbb{Z}[i]$ の元に対して, 次のように偶奇を定義する.

定義 $\alpha=a+ib\in\mathbb{Z}[i]$ に対して, $a+b$ が奇数であるとき**奇** (odd), $a+b$ が偶数であるとき**偶** (even) と呼ぶ.

この定義は, α のノルム a^2+b^2 の偶奇により偶奇を定義することと同値である. また, α が偶であるとき, $\alpha \in (1+i)$ であることに注意すれば, 奇である α に対して,

$$\alpha \equiv i^{\epsilon} \ (2(1+i))$$

となる $\epsilon \in \{0,1,2,3\}$ が一意的に定まる. $\epsilon = 0$ であるとき α は**正規** (normal) であると言う.

ところで, ゼロではない $\beta \in \mathbb{Z}[i]$ と Λ に対して, $\mathbb{Z}[i]$ 加群としての同型

$$\frac{1}{\beta}\Lambda/\Lambda \simeq \mathbb{Z}[i]/\beta\mathbb{Z}[i]$$

が成立する. このとき, 次を定義する.

定義 ゼロではない $\beta \in \mathbb{Z}[i]$ と $\Lambda = (1+i)\varpi\mathbb{Z} + (1-i)\varpi\mathbb{Z}$ に対して, $[\delta] \in \frac{1}{\beta}\Lambda/\Lambda$ が $\mathbb{Z}[i]$ 加群としての生成元であるとき δ を **β-torsion generator** と呼ぶ.

ここで δ, δ' を二つの β-torsion generator, $[\alpha] \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^{\times}$ とすると

$$\delta \equiv \alpha\delta' \quad (\Lambda)$$

となる. β が奇であるとき, $\frac{2\varpi}{\beta}$ は β-torsion generator である. したがって, 以降 β-torsion generator について考える.

次に, レムニスケート sin 関数の n 倍角の公式の一般化である, 複素レムニスケート sin 関数に対しての $\mathbb{Z}[i]$ の奇数倍角の公式について述べる. これは, 虚 2 次体 $\mathbb{Q}(\sqrt{-1})$ においての虚数乗法に対応する.

定理 3.9 奇である $\beta \in \mathbb{Z}[i]$ に対して, δ_β を β-torsion generator, ϵ を $\beta \equiv i^{\epsilon}(2(1+i))$ により定まる $\epsilon \in \{0,1,2,3\}$ とする. このとき互いに素な多項式 $P_\beta(X), Q_\beta(X) \in \mathbb{Z}[i][X]$ で以下を満たすものが存在する :

(1) 任意の $z \in \mathbb{C}$ に対して,

$$\mathrm{sn}(\beta z) = i^{\epsilon}\mathrm{sn}(z)\frac{P_\beta(\mathrm{sn}^4(z))}{Q_\beta(\mathrm{sn}^4(z))}.$$

(2) $N_{k/\mathbb{Q}}(\beta) = m$ とすると, $\deg P_\beta = \deg Q_\beta = (m-1)/4$.

(3) $XP_\beta(X^4)$ の根全体 R_β は

$$R_\beta = \{\mathrm{sn}(\alpha\delta_\beta) \mid [\alpha] \in \mathbb{Z}[i]/\beta\mathbb{Z}[i]\}$$

となる.

(4) $P_\beta(X)$ はモニックであり, $d := \deg P_\beta$ とすると, $Q_\beta(X) = X^d P_\beta\left(\frac{1}{X}\right)$ を満たす.

(1) は $\mathbb{Z}[i]$ の奇数倍角の公式を表している. (2) と (3) から等分多項式の根全体が $\mathrm{sn}(\alpha\frac{2\varpi}{\beta})$ であり, その個数は $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$ の位数, すなわち β のノルムに等しいことがわかる. さらに, $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$ の代表系を固定すれば, $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$ と R_β は 1 対 1 に対応することもわかる. (4) は例 2.12 のように, $Q_\beta(X)$ の係数が $P_\beta(X)$ の係数と逆順で対称になっていることを表している.

定理 3.9 の P_β をレムニスケートの n 等分多項式と同様に **(レムニスケートの)β 等分多項式** (β-division polynomial) と呼ぶ.

定理 3.9 (1) は, $\beta = n + im$ に対して, $n + i$ で n に関する帰納法を用い, さらに $n + im$ で m に関する帰納法を用いることで $P_\beta(X), Q_\beta(X)$ は構成できる.

実際, $\beta = n + im$ に対して, n が奇数のとき

$$\begin{aligned}
P_{n+i}(X) =& - P_{(n-2)+i}(X)\{Q_{(n-1)+i}(X)^2 - X(1-X)P_{(n-1)+i}(X)^2\} \\
&+ 2(1-X)P_{(n-1)+i}(X)Q_{(n-1)+i}(X)Q_{(n-2)+i}(X), \\
Q_{n+i}(X) =& Q_{(n-2)+i}(X)\{Q_{(n-1)+i}(X)^2 - X(1-X)P_{(n-1)+i}(X)^2\},
\end{aligned}$$

n が偶数のとき

$$\begin{aligned}
P_{n+i}(X) =& - P_{(n-2)+i}(X)\{Q_{(n-1)+i}(X)^2 - X(1-X)P_{(n-1)+i}(X)^2\} \\
&+ 2P_{(n-1)+i}(X)Q_{(n-1)+i}(X)Q_{(n-2)+i}(X), \\
Q_{n+i}(X) =& Q_{(n-2)+i}(X)\{Q_{(n-1)+i}(X)^2 - XP_{(n-1)+i}(X)^2\}
\end{aligned}$$

と, $\beta = n + im$ が奇のとき

$$\begin{aligned}
P_{n+im}(X) =& - P_{n+i(m-2)}(X)\{Q_{n+i(m-1)}(X)^2 - XP_{n+i(m-1)}(X)^2\} \\
&+ 2P_{n+i(m-1)}(X)Q_{n+i(m-1)}(X)Q_{n+i(m-2)}(X), \\
Q_{n+im}(X) =& Q_{n+i(m-2)}(X)\{Q_{n+i(m-1)}(X)^2 - XP_{n+i(m-1)}(X)^2\},
\end{aligned}$$

$\beta = n + im$ が偶のとき

$$\begin{aligned}
P_{n+im}(X) =& - P_{n+i(m-2)}(X)\{Q_{n+i(m-1)}(X)^2 - X(1-X)P_{n+i(m-1)}(X)^2\} \\
&+ 2P_{n+i(m-1)}(X)Q_{n+i(m-1)}(X)Q_{n+i(m-2)}(X), \\
Q_{n+im}(X) =& Q_{n+i(m-2)}(X)\{Q_{n+i(m-1)}(X)^2 - X(1-X)P_{n+i(m-1)}(X)^2\}
\end{aligned}$$

により構成される. そこから, 必要に応じて, 共通因子を取り除き, $(\mathbb{Z}[i])^\times$ の元をかけることで (2), (3), (4) を満たすようにすることができることが示される.

例 3.10 (レムニスケートの $1+2i$ 等分多項式) $\beta = 1+2i$ のとき，$N_{\mathbb{Q}(i)/\mathbb{Q}}\beta = 5$ より，$\deg P_\beta = \deg Q_\beta = 1$ であり，$\beta \equiv -1 \quad (2(1+i))$ である．このとき

$$P_\beta(X) = X + (-1+2i),$$
$$Q_\beta(X) = (-1+2i)X + 1$$

となる．

3.2 等分点による拡大体の Galois 理論

以降，$k = \mathbb{Q}(\sqrt{-1}), \mathcal{O}_k = \mathbb{Z}\left[\sqrt{-1}\right]$ とする．この節では, 奇である $\beta \in \mathcal{O}_k$ に対して，レムニスケートの β 等分点による拡大体 $K_\beta = k(\mathrm{sn}(\delta_\beta))$ の k 上の Galois 群を [CH] の方法により決定する．これは円分体と類似した方法である．

まず, 円分多項式の類似物である, lemnatomic polynomial を定義する．

定義 $\beta \in \mathcal{O}_k$ を奇, δ_β を β-torsion generator とする．このとき

$$\Lambda_\beta(X) = \prod_{[\alpha]\in(\mathcal{O}_k/\beta\mathcal{O}_k)^\times} (X - \mathrm{sn}(\alpha\delta_\beta))$$

を β^{th}-lemnatomic polynomial と呼ぶ．

このとき, 前節で定義した β 等分多項式 $P_\beta(X)$ と β^{th}-lemnatomic polynomial $\Lambda_\beta(X)$ には次のような関係がある．

命題 3.11 奇である $\beta \in \mathcal{O}_k$ に対して

$$XP_\beta(X^4) = \prod_{\gamma|\beta,\gamma:\text{ 正規}} \Lambda_\gamma(X)$$

が成立する．

これは, 円分多項式 Φ_n に対する

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

の類似であり, 同様の方法によって証明される．

$\Lambda_\beta(X)$ の係数について次が示される．

命題 3.12 奇である $\beta \in \mathcal{O}_k \setminus \mathcal{O}_k^\times$ に対して, いずれかが成立する．

(1) $\beta = u\pi^k \quad (u \in \mathcal{O}_k^\times, \pi \in \mathcal{O}_k$: 正規かつ素元) であるとき, $\Lambda_\beta(0) = \pi$.
(2) β が (1) の形の元ではないとき, $\Lambda_\beta(0) = 1$.

このことから, 奇である β 等分多項式 P_β の既約性が示される.

定理 3.13 奇である $\beta \in \mathcal{O}_k$ に対して, $\Lambda_\beta(X)$ は k 上既約である.

この証明も, 古典的な円分多項式の既約性の証明と類似の方法により行うことができる. また, β が奇かつ素元であるときの β 等分多項式 P_β の既約性は古くから知られており, 1850 年に Eisenstein により示されている.

歴史的には, この P_β の既約性を示すために, Eisenstein の判定法が示されたと言われている. $\mathbb{Z}[i]$ 上での方法が $\mathbb{Z}$ 上でも適用出来ることに Eisenstein 自身が気づき, 現在良く用いられる形となった.

これにより, この節の目標であった次の定理が従う.

定理 3.14 奇である $\beta \in \mathcal{O}_k$ に対して,

$$\mathrm{Gal}(K_\beta/k) \simeq (\mathcal{O}_k/\beta\mathcal{O}_k)^\times$$

が成立する.

同型は $\alpha \in (\mathcal{O}_k/\beta\mathcal{O}_k)^\times$ に対して, K_β の k 自己同型 $\sigma : \mathrm{sn}(\delta_\beta) \mapsto \mathrm{sn}(\alpha\delta_\beta)$ を対応させることによって得られる. この定理から, 次の系が得られる.

系 3.15 奇かつ素元である $\beta \in \mathcal{O}_k$ に対して, $N_{k/\mathbb{Q}}\beta = m$ とすると

$$\mathrm{Gal}(K_\beta/k) \simeq C_{m-1}$$

が成立する.

円分多項式の類似による Galois 群の決定により, レムニスケートの等分体と円分体との Galois 理論的な類似が得られた. この節で述べた事柄の証明は, 類体論を用いずに行えることに注意しておく. この方法は 2014 年に [CH] によって示されたものであり, 類体論を用いた証明は 1981 年に [Ros] により得られている.

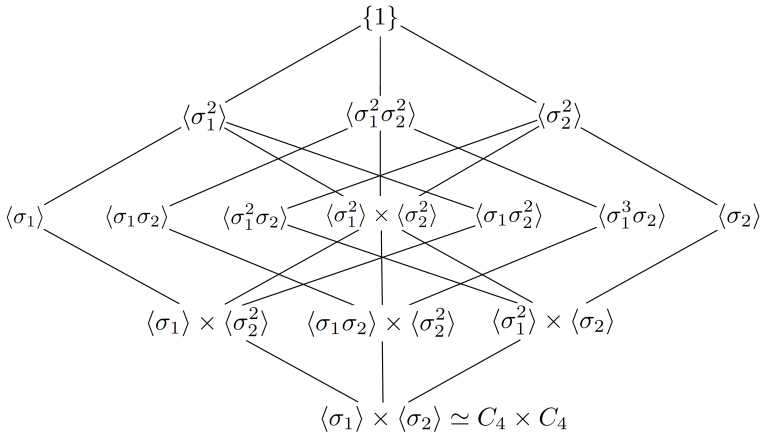
例 3.16 (K_5/k の Galois 群) $\beta = 5$ のとき, $\mathcal{O}_k$ で

$$(5) = (1+2i)(1-2i)$$

と素イデアル分解される. 中国剰余定理を用いれば

$$\begin{aligned}\mathrm{Gal}(K_5/k) &\simeq (\mathcal{O}_k/5\mathcal{O}_k)^\times \\ &\simeq (\mathcal{O}_k/(1+2i)\,\mathcal{O}_k)^\times \times (\mathcal{O}_k/\,(1-2i)\,\mathcal{O}_k)^\times \\ &\simeq C_4 \times C_4\end{aligned}$$

を得る. したがって, σ_1, σ_2 をそれぞれの C_4 の生成元とすれば, 包含関係による $\mathrm{Gal}(K_5/k)$ のハッセ図は



となる.

$$\begin{aligned}P_5(X) &= X^6 + 50X^5 - 125X^4 + 300X^3 - 105X^2 - 62X + 5 \\ &= (X^2 - 2X + 5)(X^4 - 12X^3 - 26X^2 + 52X + 1)\end{aligned}$$

から,

$$\begin{aligned}XP_5(X^4) &= X^{25} + 50X^{21} - 125X^{17} + 300X^{13} - 105X^9 - 62X^5 + 5X \\ &= \Lambda_1(X)\Lambda_{1+2i}(X)\Lambda_{1-2i}(X)\Lambda_5(X) \\ &= X(X^4 - 1 + 2i)(X^4 - 1 - 2i)(X^{16} - 12X^{12} - 26X^8 + 52X^4 + 1)\end{aligned}$$

となる. したがって, レムニスケートの 5 等分体の最小多項式

$$f(X) = X^{16} - 12X^{12} - 26X^8 + 52X^4 + 1$$

が得られる.

3.3 等分点による拡大体の類体論

まず, レムニスケートの等分点による拡大体と, 第 2 章で構成した類体, すなわち楕円曲線の等分点による拡大体との関係を $\wp$ 関数を用いて明らかにする.

この節においても, $k = \mathbb{Q}(\sqrt{-1}), \mathcal{O}_k = \mathbb{Z}\left[\sqrt{-1}\right]$ とし, $\beta \in \mathcal{O}_k$ に対して, レムニスケートの β 等分点による拡大体を $K_\beta = k(\mathrm{sn}(\delta_\beta))$ とする.

定理 3.17 奇である $\beta \in \mathcal{O}_k$ に対して, δ_β を β-torsion generator とする. このとき

$$K_\beta = k(\mathrm{sn}(\delta_\beta), \mathrm{sn}'(\delta_\beta)) = k(\wp(\delta_\beta), \wp'(\delta_\beta)) = k(E[\beta])$$

が成立する.

すなわち, $\wp$ 関数を通して, レムニスケートの等分点の体 K_β と楕円曲線の等分点の体 $k(E[\beta])$ が結びついたのである. これは, $\mathrm{sn}'(\delta_\beta) \in K_\beta$ という驚くべき事実に基づいている.

k の類数は 1 であるから, 2.2 節の最後に述べたように, $k^{ab} = k(h(\cup_\beta E[\beta])) = k(\cup_\beta E[\beta])$ である.

β の生成する単項イデアル (β) のシュトラール類体は $k(h(E[\beta]))$ であり, $K_\beta = k(E[\beta])$ であるから, $k(h(E[\beta])) \subset K_\beta$ である. したがって, K_β は (β) のシュトラール類体ではないが, 次のことがわかる.

定理 3.18 奇である $\beta \in \mathcal{O}_k$ に対して, δ_β を β-torsion generator とする. このとき, イデアル $(2(1+i)\beta)$ に対して,

$$K_\beta = k(h(E[(2(1+i)\beta)]))$$

が成り立つ. すなわち, K_β は $(2(1+i)\beta)$ に対するシュトラール類体である.

したがって, k のイデアルの K_β においての素イデアル分解は, 分解定理より, $(2(1+i)\beta)$ を法とするシュトラール類群を調べることによってわかる. さらに, 定理 1.2(3) の結合定理を用いれば, β_1, β_2 等分点による拡大体の合成体がイデアル群 $H_k(2(1+i)\beta_1) \cap H_k(2(1+i)\beta_2)$ に対する類体であることがわかる.

判別式については, [Tak1] による次の結果がある.

定理 3.19 奇かつ素元である $\beta \in \mathcal{O}_k$ に対して, $m := N_{k/\mathbb{Q}}\beta$ とする. このとき K_β の k 上の相対判別式は $2^{m-1}\beta^{m-2}$ となる.

また, 同じく [Tak1] により, $(1+i)$ 等分点による拡大体の相対判別式は因子に $(1+i)$ のみを持つことが示されている. さらに, 素元 β のべき等分点による拡大体においては, β が完全分岐することが示されている. これは, 円の p べき分体において, p が完全分岐することの類似である.

ここで一般に, $L/K, L'/K$ を $L \cap L' = K$ を満たす代数体の Galois 拡大とすると, $L/K, L'/K$ のそれぞれの拡大次数を n, n', 相対判別式を d, d' と置けば, 合成体 LL' の判別式は dd' となることが知られている.

したがって, 互いに素である $\beta_1, \beta_2 \in \mathcal{O}_k$ と $t, s \in \mathbb{N}$ に対して, $K_{\beta_1^t} \cap K_{\beta_2^s} = k$ であり,

$$K_{\beta_1^t \beta_2^s} = K_{\beta_1^t} K_{\beta_2^s}$$

であることから, 任意のレムニスケートの β 等分点による拡大体に対して, その相対判別式が β で割れることがわかる.

3.4 p 等分点による拡大体の $\mathbb{Q}$ 上の Galois 群

定理 3.3 により, 奇素数 p に対して, レムニスケートの p 等分多項式 $P_p(X)$ は $\mathbb{Z}$ 係数多項式となる. このことから, レムニスケートの p 等分点による拡大体 K_p の $k = \mathbb{Q}(\sqrt{-1})$ 上の最小多項式 $f(X)$ は k 上のみならず, $\mathbb{Q}$ 上でも定義される. このとき, $f(X)$ の $\mathbb{Q}$ 上の最小分解体が K_p と一致することを示す.

まず, 次の補題を用意する.

補題 3.20 p を奇素数, K_p をレムニスケートの p 等分点による拡大体とし, その最小多項式を $f(X)$ とする. このとき, ある多項式 $g(X) \in \mathbb{Z}[X]$ が存在し, $f(X) = g(X^4)$ となる.

証明 $p \equiv 3 \ (4)$ のとき, p は $\mathcal{O}_k$ における素元であるから, $P_p(X)$ を p 等分多項式とすれば, $f(X) = P_p(X^4)$ であるから良い.
$p \equiv 1 \ (4)$ のとき, p は $\mathcal{O}_k$ において完全分解する. $\mathcal{O}_k$ は PID であるから UFD であり, $p = \pi\overline{\pi}$ と素元分解される. したがって, 命題 3.11 により, $XP_p(X^4)$

$$XP_p(X^4) = \Lambda_1(X)\Lambda_\pi(X)\Lambda_{\overline{\pi}}(X)\Lambda_p(X)$$

と分解される. $\Lambda_1(X) = X$ であるから,

$$P_p(X^4) = \Lambda_\pi(X)\Lambda_{\overline{\pi}}(X)\Lambda_p(X)$$

となる. ここで, π は素元であるから

$$P_\pi(X^4) = \Lambda_\pi(X)$$

より, X^4 の式となる. $\overline{\tau}$ についても同様である. したがって, 最小多項式 $f(X) = \Lambda_p(X)$ も X^4 の式となる. □

このことから, 次が成り立つ.

命題 3.21 p を奇素数, K_p をレムニスケートの p 等分点による k の拡大体とし, その k 上の最小多項式を $f(X)$ とする. このとき

$$\mathrm{Spl}_{\mathbb{Q}}(f(X)) = K_p$$

証明 $\mathrm{Spl}_{\mathbb{Q}}(f(X)) \subset K_p$ は $f(X)$ が k 上 K_p の最小多項式であることから明らか.

$\mathrm{Spl}_{\mathbb{Q}}(f(X)) \supset K_p$ を示す. このとき, $k \subset \mathrm{Spl}_{\mathbb{Q}}(f(X))$, すなわち, $\sqrt{-1} \in \mathrm{Spl}_{\mathbb{Q}}(f(X))$ を示せば良い.

補題 3.20 より, $Y = X^4$ と置き, $f(Y)$ の根を α_t とすれば, $f(Y)$ は重根を持たないから, $f(X)$ の全ての根は

$$i^{\epsilon}\sqrt[4]{\alpha_t}, \quad (i = 0, 1, 2, 3)$$

となり, $\sqrt{-1} \in \mathrm{spl}_{\mathbb{Q}}(f(X))$ を得る. □

このとき, $K_p/\mathbb{Q}$ の Galois 群は次のようになる.

定理 3.22 p を奇素数, K_p をレムニスケートの p 等分点による拡大体とする. このとき

$$\mathrm{Gal}(K_p/\mathbb{Q}) \simeq \begin{cases} C_{p-1} \wr C_2 \simeq (C_{p-1} \times C_{p-1}) \rtimes C_2 & (p \equiv 1\ (4)) \\ \langle \sigma, \tau \mid \sigma^{p^2-1} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^p \rangle \simeq C_{p^2-1} \rtimes C_2 & (p \equiv 3\ (4)) \end{cases}$$

となる. ただし, C_2 は複素共役として作用する.

証明 まず, $\mathrm{Gal}(k/\mathbb{Q})$ の元を K_p の自己同型写像に延長することにより, 完全系列

$$1 \longrightarrow \mathrm{Gal}(K_p/k) \longrightarrow \mathrm{Gal}(K_p/\mathbb{Q}) \longrightarrow \mathrm{Gal}(k/\mathbb{Q}) \longrightarrow 1$$

が分裂することがわかる. したがって

$$\mathrm{Gal}(K_p/\mathbb{Q}) \simeq \mathrm{Gal}(K_p/k) \rtimes \mathrm{Gal}(k/\mathbb{Q})$$

となる. このとき, $\mathrm{Gal}(k/\mathbb{Q}) \simeq C_2$ であり, $\mathrm{Gal}(k/\mathbb{Q})$ の位数 2 の元は複素共役である. 以下, それぞれの場合に分けて示す.

$p \equiv 1\ (4)$ のとき, p は $\mathcal{O}_k$ において完全分解する. $\mathcal{O}_k$ は PID であるから, $p = \pi\overline{\pi}$ と素元分解される. $\pi = a + bi$ とすれば, 中国剰余定理より

$$\begin{aligned}\mathrm{Gal}(K_p/k) &\simeq (\mathcal{O}_k/p\mathcal{O}_k)^\times \\ &\simeq (\mathcal{O}_k/(a+bi)\,\mathcal{O}_k)^\times \times (\mathcal{O}_k/(a-bi)\,\mathcal{O}_k)^\times \\ &\simeq C_{p-1} \times C_{p-1}\end{aligned}$$

となる. したがって, $\mathrm{Gal}(k/\mathbb{Q})$ による作用は生成元を取り替える作用となる. これにより,

$$\mathrm{Gal}(K_p/\mathbb{Q}) \simeq C_{p-1} \wr C_2$$

となる.

$p \equiv 3\ (4)$ のとき, p は $\mathcal{O}_k$ において素元である. したがって,

$$\mathrm{Gal}(K_p/k) \simeq (\mathcal{O}_k/p\mathcal{O}_k)^\times \simeq C_{p^2-1}$$

となる. このとき,

$$(\mathcal{O}_k/p\mathcal{O}_k)^\times = \langle\sigma\rangle$$

とする. ここで, $[\mathcal{O}_k/p\mathcal{O}_k : \mathbb{F}_p] = 2$ より, 複素共役 τ は p の Frobenius 自己同型となる. Frobenius 自己同型の定義より

$$\alpha^\tau \equiv \alpha^p \quad (p), \quad \alpha \in \mathcal{O}_k$$

が成立する. これにより,

$$\begin{aligned}\tau^{-1}\sigma\tau &= (1,\tau)(\sigma,1)(1,\tau) \\ &= (\sigma,\tau)(1,\tau) \\ &= (\sigma^\tau,1) \\ &= (\sigma^p,1) \\ &= \sigma^p\end{aligned}$$

となる. したがって,

$$\mathrm{Gal}(K_p/\mathbb{Q}) \simeq \langle\sigma,\tau \mid \sigma^{p^2-1} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^p\rangle$$

を得る. □

定理 3.22 において, $p = 3$ とすれば,

$$\mathrm{Gal}(K_3/\mathbb{Q}) \simeq \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^3 \rangle$$

となり, これは準 2 面体群 QD_8 の生成関係式となる. $p = 3$ のときにのみ, $\mathrm{Gal}(K_p/k)$ は 2 群となる. また, 定理 3.17 より, $k(E[(3)]) = K_3$ であることから, 例 2.3 と一致することがわかる.

定理 3.22 に基づき, レムニスケートの等分体とその部分体の数論的性質を調べていくことが今後の課題である.

参考文献

[足立/三宅] 足立恒雄, 三宅克哉, 類体論講義, 日本評論社, 1998.

[加藤/黒川/斎藤] 加藤和也, 黒川信重, 斎藤毅, 数論 1, 2, 岩波書店, 1996, 1998.

[河田] 河田敬義, 数論 III, 岩波書店, 1979.

[高木] 高木貞治, 代数的整数論 第 2 版, 岩波書店, 1971.

[竹内] 竹内端三, 楕圓函數論, 岩波書店, 1936.

[ノイキルヒ] J. ノイキルヒ, 代数的整数論（足立恒雄監修, 梅垣敦紀訳）, シュプリンガー・フェアラーク東京, 2003.

[三宅] 三宅克哉, 楕円関数概観, 共立出版, 2015.

[横山] 横山俊一, 計算する立場からの楕円曲線論入門, 2014.
以下の URL から入手可能.
https://www.dropbox.com/s/8j43nzwl14y4tq7/2014Yamagata.pdf

[BCHIS] A. Borel, S. Chowa, C. S. Herz, K. Iwasawa, J-P. Serre, *Seminar on complex multiplication*, LNM 21, Springer-Verlag, 1966.

[Cox1] D. A. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, Inc., 1989.

[Cox2] D. A. Cox, *Galois Theory*, 2nd Edition, John Wiley & Sons, Inc., 2012.

[CH] D. A. Cox, T. Hyde, *The Galois theory for the lemniscates*, J. Number Theory **135** (2014), 43–59.

[Neu] J. Neukirch, *Class field theory -The Bonn Lectures-*, Springer-Verlag, 2013.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Springer-Verlag, 2008.

[Lub] R. Lubiana, *Takagi's theorem on lemniscate extensions*, Master thesis, Bordeaux university, 2014. 以下の URL から入手可能.
http://algant.eu/documents/theses/lubiana.pdf

[Ros] M. Rosen, *Abel's theorem on the lemniscate*, Amer. Math. Monthly **88** (1981), 387–395.

[SW] R. Schoof, L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988),

543–556.

[Sha] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

[Shi] G. Shimura, *Arithmetic theory of automorphic functions*, Iwanami Shoten, 1982.

[Sil1] J. H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.

[Sil2] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, 1994.

[ST] J. H. Silverman, J. T. Tate, *Rational points on elliptic curves*, UTM 106, Springer-Verlag, 1986.

[Tak1] T. Takagi, *Über die im Bereiche der rationalen complexen Zahlen Abel'schen Zahlkörper*, J. Coll, Sci. Imp. Univ. Tokyo **19** (1903), 1–42.

[Tak2] T. Takagi, *Über eine Theorie der relativ-Abel'schen Zahlkörper*, J. Coll, Sci. Imp. Univ. Tokyo **41** (1920), 1–133.