レムニスケートの等分点による非可換拡大の構成

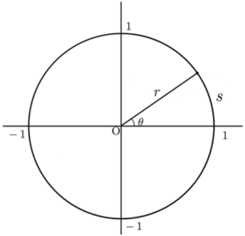
金井和貴

自然科学研究科数理物質科学専攻
星研究室 博士前期課程２年

2017 年 2 月 9 日

イントロダクション

円



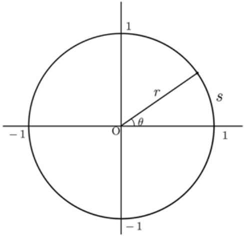
$$r = \cos\theta$$

$$\pi := 2\int_0^1 \frac{1}{\sqrt{1-t^2}}dt$$

$$\approx 3.14159$$

イントロダクション

円



$$r = \cos\theta$$

$$\pi := 2\int_0^1 \frac{1}{\sqrt{1-t^2}}dt$$

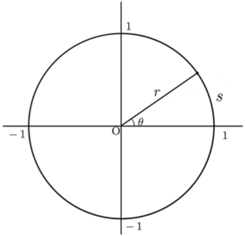
$$\approx 3.14159$$

$$\varpi := 2\int_0^1 \frac{1}{\sqrt{1-t^4}}dt$$

$$\approx 2.62206$$

イントロダクション

円

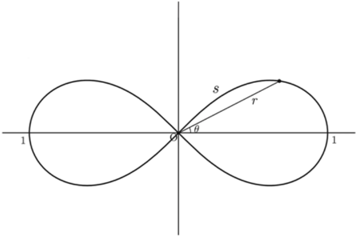


$$r = \cos\theta$$

$$\pi := 2\int_0^1 \frac{1}{\sqrt{1-t^2}}dt$$

$$\approx 3.14159$$

レムニスケート



$$r^2 = \cos(2\theta)$$

$$\varpi := 2\int_0^1 \frac{1}{\sqrt{1-t^4}}dt$$

$$\approx 2.62206$$

発表の流れ

1. レムニスケートの等分点による拡大体 K_β
2. 類体論と最大 Abel 拡大
3. 虚 2 次体 k の最大 Abel 拡大
4. 主結果と今後の課題

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

§1 レムニスケート sin 関数

第 1 象限において，レムニスケートの弧長 s は

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

により与えられる．ここで，

$$\varpi := 2\int_0^1 \frac{1}{\sqrt{1-r^4}} dr \approx 2.62206 \text{ (超越数)}$$

と置けば，周は 2ϖ，n 等分点間の長さは $2\varpi/n$ となる．
(1) の逆関数をレムニスケート sin 関数と呼び，$\mathrm{sn}(\theta)$ と書く．

命題 1.1

$u, v \in \mathbb{R}$ に対して次が成立する．

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

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

複素レムニスケート sin 関数と虚数乗法

定義 1.2 (複素レムニスケート関数)

$z = x + iy \in \mathbb{C}$ 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**と呼ぶ

定理 1.3

(1) $\mathrm{sn}(z)$ は $\mathbb{C}$ 上の有理型関数である．
(2) $\mathrm{sn}(z)$ の零点は $(m + in)\varpi$，極は $(\frac{m}{2} + i\frac{n}{2})\varpi$ であり，位数は全て 1 である．
(3) $\mathrm{sn}(z)$ は $2\varpi\mathbb{Z} + 2\varpi i\mathbb{Z}$ を周期に持つ．

定理 1.4

$\beta \in \mathbb{Z}[i]$ に対して，互いに素な $P_\beta(X), Q_\beta(X) \in \mathbb{Z}[i][X]$ で

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

を満たすものが帰納的に構成できる．

K_β の $k = \mathbb{Q}(\sqrt{-1})$ 上の最小多項式

$k = \mathbb{Q}(\sqrt{-1}), \mathcal{O}_k = \mathbb{Z}[\sqrt{-1}]$, $K_\beta = k\,(\mathrm{sn}\,(2\varpi/\beta))$ とする.

定義 1.5

奇数 $\beta = x + iy \in \mathcal{O}_k (\overset{\text{def}}{\Leftrightarrow} x + y$ が奇数) に対して,

$$\Lambda_\beta(X) = \prod_{[\alpha]\in(\mathcal{O}_k/\beta\mathcal{O}_k)^\times} (X - \mathrm{sn}\,(\alpha(2\varpi/\beta)))$$

を β^{th}-lemnatomic polynomial と呼ぶ.

命題 1.6

奇数 $\beta \in \mathcal{O}_k$ に対して

$$XP_\beta(X^4) = \prod_{\gamma|\beta, \gamma\equiv 1\ (2(1+i))} \Lambda_\gamma(X).$$

定理 1.7 (Eisenstein 1850, Cox-Hyde 2014)

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

K_β の $k = \mathbb{Q}(\sqrt{-1})$ 上の Galois 群

定理 1.8 (Rosen 1981, Cox-Hyde 2014)

奇数 $\beta \in \mathcal{O}_k$ に対して,

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

が成立する.

上の同型は $\alpha \in (\mathcal{O}_k/\beta\mathcal{O}_k)^\times$ に対して, K_β の k 自己同型 $\sigma : \mathrm{sn}(2\varpi/\beta) \mapsto \mathrm{sn}(\alpha(2\varpi/\beta))$ を対応させることにより得られる.

系 1.8

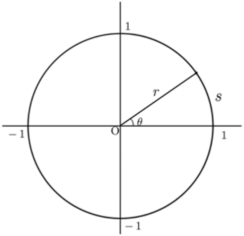
奇数かつ素元な $\beta \in \mathcal{O}_k$ に対して, $N_{k/\mathbb{Q}}\beta = m$ とすると

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

が成立する.

円とレムニスケート

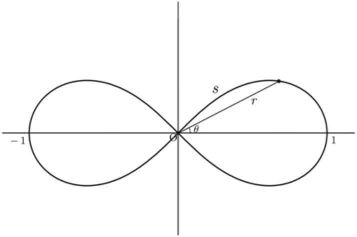
円



$$r = \cos\theta$$

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

レムニスケート



$$r^2 = \cos(2\theta)$$

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

§2 イデアル類群

この節では, $\mathbb{Q} \subset k$ を代数体, $\mathcal{O}_k$ を k の整数環 (k の中の代数的整数全体のなす環) とする.

定義 2.1 (イデアル類群)

$\mathcal{O}_k$ のイデアル全体を I_k, $\mathcal{O}_k$ の単項イデアル全体を P_k とする. このとき,

$$H_k = I_k/P_k$$

を k のイデアル類群と呼ぶ. $\underline{\#H_k = h_k}$ を k の類数と呼ぶ.

H_k は有限 Abel 群である. また, $h_k = 1 \Leftrightarrow \mathcal{O}_k$ は PID.

$$\begin{array}{ccccccccccc}
1 & \longrightarrow & \mathrm{Ker}\,\varphi & \longrightarrow & k & \xrightarrow{\varphi} & I_k & \longrightarrow & \mathrm{Coker}\,\varphi & \longrightarrow & 1 \\
 & & \| & & \cup & & \cup & & \| & & \\
 & & \mathcal{O}_k^\times & & a & \longmapsto & (a) & & H_k & &
\end{array}$$

H_k は $\mathcal{O}_k^\times$ と共に " 数とイデアルのずれ " を表している

Hilbert 類体と射類体

定義 2.2 (Hilbert 類体, Hilbert, 1897)

K/k を代数体の拡大, $\mathfrak{p}$ を k の 1 次の素イデアルとするとき

$$\mathfrak{p} \text{ が } K/k \text{ において完全分解} \iff \mathfrak{p} \in P_k$$

が成立する体 K を k の Hilbert 類体と呼ぶ.

定理 2.3 (Hilbert, 1899)

k の Hilbert 類体 K に対して, $\mathrm{Gal}(K/k) \simeq H_k$.

例. Hilbert 類体

- $k = \mathbb{Q} : h_k = 1, K = \mathbb{Q}$
- $k = \mathbb{Q}(\sqrt{-1}) : h_k = 1, K = k$
- $k = \mathbb{Q}(\sqrt{-5}) : h_k = 2, K = k(\sqrt{-1}) = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$

Hilbert 類体と射類体

定義 2.2 (Hilbert 類体, Hilbert, 1897)

K/k を代数体の拡大, $\mathfrak{p}$ を k の 1 次の素イデアルとするとき

$$\mathfrak{p} \text{ が } K/k \text{ において完全分解} \iff \mathfrak{p} \in P_k$$

が成立する体 K を k の Hilbert 類体と呼ぶ.

イデアル類群のモジュラス $\mathfrak{m}$ ごとの精密化を考える.

定義 2.4 (射類体, 高木貞治, 1920)

K/k を代数体の拡大, $\mathfrak{p}$ をモジュラス $\mathfrak{m}$ と互いに素な k の 1 次の素イデアルとするとき

$$\mathfrak{p} \text{ が } K/k \text{ において完全分解} \iff \mathfrak{p} \in P_k(\mathfrak{m})$$

が成立する体 K を $\mathfrak{m}$ に対する射類体と呼ぶ.

$\mathfrak{m}$ は $\mathcal{O}_k$ のイデアルであり, $\mathfrak{m} = \mathcal{O}_k$ のとき, $P_k(\mathfrak{m}) = P_k$.

Hilbert 類体と射類体

定理 2.5 (高木貞治, 1920)

k のモジュラス $\mathfrak{m}$ に対して，射類体 $L_\mathfrak{m}$ が一意に存在して，

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

例 射類体としての円分体 ($k = \mathbb{Q}, \mathfrak{m} = (n)$ の場合)

円分体 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ と $\mathbb{Q}$ の単項イデアル $\mathfrak{m} = (n)$ に対して，
$I_\mathbb{Q}(\mathfrak{m}) = \{a \in \mathbb{Q} \mid a > 0, (a, n) = 1\}$,
$P_\mathbb{Q}(\mathfrak{m}) = \{a \in I_\mathbb{Q}(l) \mid a \equiv 1 \ (n)\}$,
$H_\mathbb{Q}(\mathfrak{m}) = I_\mathbb{Q}(\mathfrak{m})/P_\mathbb{Q}(\mathfrak{m})$ となる．ここで

$$\Phi : I_\mathbb{Q}(\mathfrak{m}) \ni a \longmapsto \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$$

Φ は全射であり，$\mathrm{Ker}\ \Phi = P_\mathbb{Q}(\mathfrak{m})$ となる．したがって，

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq H_\mathbb{Q}(n)$$

であり，$\mathbb{Q}(\zeta_n)$ は $\mathbb{Q}$ の (n) に対する射類体である．

Kronecker-Weber の定理と $\mathbb{Q}$ の最大 Abel 拡大

定理 2.6 (高木貞治, 1920)

${}^\forall K$: k の Abel 拡大, ${}^\exists\mathfrak{m}$: モジュラス s.t. $K \subset L_\mathfrak{m}$: $\mathfrak{m}$ の射類体.

$\mathbb{Q}$ の場合はより具体的に次のようになる.

定理 2.7 (Kronecker-Weber の定理, 1896)

${}^\forall K$: $\mathbb{Q}$ の Abel 拡大, ${}^\exists n \in \mathbb{N}$ s.t. $K \subset \mathbb{Q}(\zeta_n)$.

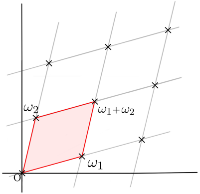
これにより, $\mathbb{Q}$ の最大 Abel 拡大 $\mathbb{Q}^{ab}$ は

$$\mathbb{Q}^{ab} = \mathbb{Q}(\zeta_n \mid n \in \mathbb{N}).$$

問題 (Hilbert の第 12 問題, 1900)

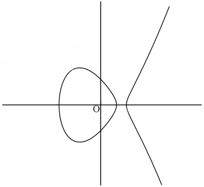
$\zeta_n \in \mathbb{Q}^{ab}$ の対応物を k^{ab} において見つけよ.

§3 複素トーラスと楕円曲線 ($k = \mathbb{Q}(\sqrt{-m})$)



$f : z \longmapsto (\wp(z,\mathfrak{a}), \wp'(z,\mathfrak{a}), 1)$

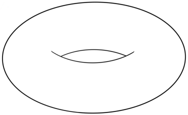
$\longleftrightarrow$



$\mathbb{C}/\mathfrak{a}$, $\mathfrak{a} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$
$(\omega_1, \omega_2 \in \mathbb{C})$

$E : y^2 = 4x^3 + \gamma_2 x + \gamma_3$
$(\gamma_2, \gamma_3 \in \mathbb{C})$

境界を同一視



定義 3.1 (j 不変量)

$$j(E) := 1728 \frac{{\gamma_2}^3}{{\gamma_2}^3 - 27\,{\gamma_3}^2}$$

定理 3.2

以下は同値.

(1) $j(\mathfrak{a}_1) = j(\mathfrak{a}_2)$.
(2) $\mathbb{C}/\mathfrak{a}_1 \simeq \mathbb{C}/\mathfrak{a}_2$.
(3) $E_{\mathfrak{a}_1} \simeq E_{\mathfrak{a}_2}$.

$k = \mathbb{Q}(\sqrt{-m})$ の Hilbert 類体

定理 3.1

$C_i \in H_k$ $(1 \leq i \leq h_k)$ (イデアル類群) とする.

(1) j 不変量は各類 C_i に対する不変量である.

(2) $j(C_i)$ は代数的整数であり, 互いに k 上共役となる.

定理 3.2

$k(j(C_i))$ $(1 \leq {}^\forall i \leq h_k)$ は k の Hilbert 類体である.

例. $k = \mathbb{Q}(\sqrt{-5})$ の j 不変量 $(h_k = 2)$

$H_k = \{C_1 = (1), C_2\}$ とする. このとき,

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

より, k の Hilbert 類体は $k(\sqrt{5}) = \mathbb{Q}(\sqrt{-5}, \sqrt{5})$.

$k = \mathbb{Q}(\sqrt{-m})$ の射類体

定義 3.3 (E の $\mathfrak{a}$ 等分点の成す群)

k に対応する楕円曲線 E, $\mathcal{O}_k$ のイデアル $\mathfrak{a}$ に対して

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

を E の $\mathfrak{a}$ 等分点の成す群 と呼ぶ.

定理 3.4 (高木貞治, 1920)

$k(j(C_i), x(E[\mathfrak{a}]))$ は k の $\mathfrak{a}$ に対する射類体である.
ただし, $P = (x, y) \in E[\mathfrak{a}]$ に対して

$$x(P) = \begin{cases} x & (j(E) \neq 0, 1728) \\ x^2 & (j(E) = 1728) \\ x^3 & (j(E) = 0) \end{cases}$$

定理 3.5

$k(j(C_i), E[\mathfrak{a}])$ は $k(j(C_i))$ 上の Abel 拡大である.

$k=\mathbb{Q}(\sqrt{-m})$ の射類体

例 $k=\mathbb{Q}(\sqrt{-1}), \mathfrak{a}=(3)$ の射類体

k に対応する楕円曲線は $E: y^2=x^3+x$ であり，$E[3]$ は

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

の 9 つの元となる．$\left(\alpha=\sqrt{(2\sqrt{3}-3)/3},\ \beta=\sqrt{2\alpha/\sqrt{3}}\right)$.

$j(E)=1728$ より，$k=\mathbb{Q}(\sqrt{-1}), \mathfrak{a}=(3)$ の射類体は

$$\underline{k(j(E), x(E[3]))=k(x(E[3]))=k(\sqrt{3})}$$

である．また，

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

となる．ここで $k(\beta)$ は

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

より，k 上 Abel 拡大であるが，

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

より，$\mathbb{Q}$ 上非 Abel 拡大となる．

$k = \mathbb{Q}(\sqrt{-m})$ の最大 Abel 拡大

定理 3.6 (高木貞治, 1920)

${}^{\forall}K$: k の Abel 拡大,

$${}^{\exists}\mathfrak{a} \in \mathcal{O}_k \text{ のイデアル } \ \text{s.t. } K \subset k(j(C_i), x(E[\mathfrak{a}])).$$

これにより, k の最大 Abel 拡大 k^{ab} は

$$k^{ab} = k(j(C_i), x(E[\mathfrak{a}]) \mid \mathfrak{a} \in \mathcal{O}_k).$$

ここで $k = \mathbb{Q}(\sqrt{-1})$ など類数が 1 であるとき,

$$\begin{aligned} k^{ab} &= k(j(C_i), x(E[\mathfrak{a}]) \mid \mathfrak{a} \in \mathcal{O}_k) \\ &= k(j(C_i), E[\mathfrak{a}] \mid \mathfrak{a} \in \mathcal{O}_k) \\ &= k(E[\mathfrak{a}] \mid \mathfrak{a} \in \mathcal{O}_k) \end{aligned}$$

が成立する.

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

定理 3.7 (Rosen, 1981)

$k = \mathbb{Q}(\sqrt{-1})$ とする．奇数 $\beta \in \mathcal{O}_k$ に対して，

$$K_\beta = k\left(\mathrm{sn}\left(2\varpi/\beta\right)\right) = k(E[\beta])$$

が成立する．

$j(C_i) = 1728$ より，

$$\begin{aligned} k^{ab} &= k(j(C_i), E[\beta] \mid \beta \in \mathcal{O}_k) \\ &= k\left(\mathrm{sn}\left(2\varpi/\beta\right) \mid \beta \in \mathcal{O}_k\right) \end{aligned}$$

となる．ここから，$\mathbb{Q}$ の最大 Abel 拡大

$$\mathbb{Q}^{ab} = \mathbb{Q}(\zeta_n \mid n \in \mathbb{N})$$

との類似がわかる．

§4 主結果

p が奇素数のとき, $K_p = k(\mathrm{sn}(2\varpi/p))$ の $k = \mathbb{Q}(\sqrt{-1})$ 上最小多項式が $\mathbb{Q}$ 上定義される.

定理 4.1

$p \equiv 1 \pmod 4$ のとき

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

$p \equiv 3 \pmod 4$ のとき

$$\mathrm{Gal}(K_p/\mathbb{Q}) \simeq \langle \sigma, \tau \mid \sigma^{p^2-1} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^p \rangle$$
$$(\simeq C_{p^2-1} \rtimes C_2)$$

となり, 特に $K_p/\mathbb{Q}$ は非可換拡大である. ただし, C_2 による作用は複素共役によるものとする.

今後の課題

- K_p の部分体の決定
- K_p の類数問題と岩澤理論の関係
- 楕円曲線の等分体への応用
- 円分体との類似の追求