代数体のイデアル類群について

岸 康弘 (福岡教育大学)

2010 年 3 月 18 日

九州代数的整数論 2010

於 九州大学

§1 イデアル類群とは

1.1. 定義

k : 代数体 (i.e. $\mathbb{Q}$ 上の有限次拡大体)
$\mathcal{O}_k$: k の整数環

定義

$I \subset k$ に対し,
(i) $\alpha - \beta \in I$ $(\alpha, \beta \in I)$
(ii) $\lambda\alpha \in I$ $(\lambda \in \mathcal{O}_k, \alpha \in I)$
(iii) $^{\exists}\mu \in \mathcal{O}_k \setminus \{0\}$ s.t. $\mu I \subset \mathcal{O}_k$
を満たすとき, I を 分数イデアル という.
また, $\{0\}$ 以外の分数イデアル全体の集合を I_k と書く.

※ I_k は (無限) アーベル群をなす.

§1 イデアル類群とは

定義

$\alpha \in k$ に対し,

$$(\alpha) := \{\lambda\alpha \mid \lambda \in \mathcal{O}_k\}$$

を 単項分数イデアル という. また, (0) 以外の単項分数イデアル全体の集合を P_k と書く.

定義

$\mathrm{Cl}(k) := I_k/P_k$ を k の イデアル類群 といい, その位数

$$h_k := |\mathrm{Cl}(k)| \ (< \infty)$$

を k の 類数 という.

§1 イデアル類群とは

1.2. 動機

※$_1$ $\mathcal{O}_k$ での既約分解は一意的？

定理

代数体 k において, 次の 3 つは同値:

(i) $h_k = 1$

(ii) $\mathcal{O}_k$: PID

(iii) $\mathcal{O}_k$: UFD

※$_2$ フェルマーの定理との関連

定理 (Kummer, 1847)

$\mathbb{Q}(\zeta_p)$ の類数が p で割れない

$\Longrightarrow$ $x^p + y^p = z^p$ に正の整数解は存在しない

§1 イデアル類群とは

※3 ミステリアスな振舞い

- 虚2次体の類数表

$0 < D \leq 73$ (D:square-free) に対する $\mathbb{Q}(\sqrt{-D})$ の類数:

D	1	2	3	5	6	7	10	11	13	14	15	17
$h_{\mathbb{Q}(\sqrt{-D})}$	1	1	1	2	2	1	2	1	2	4	2	4

D	19	21	22	23	26	29	30	31	33	34	35
$h_{\mathbb{Q}(\sqrt{-D})}$	1	4	2	3	6	6	4	3	4	4	2

D	37	38	39	41	42	43	46	47	51	53	55
$h_{\mathbb{Q}(\sqrt{-D})}$	2	6	4	8	4	1	4	5	2	6	4

D	57	58	59	61	62	65	66	67	69	71	73
$h_{\mathbb{Q}(\sqrt{-D})}$	4	2	3	6	8	8	8	1	8	4	7

§2 問題設定

2.1. 問題設定と 2 つの手法

問題

与えられた 2 以上の整数 n, m に対し,

(1) $n \mid h_k$ なる m 次体 k を無限個構成せよ.
(2) $n \nmid h_k$ なる m 次体 k を無限個構成せよ.
(3) $n \mid h_k$ なる m 次体 k を決定せよ.
(4) $n \nmid h_k$ なる m 次体 k を決定せよ.

素数 p に対し,

(5) p-rank の高い m 次体 k を構成せよ.

$\mathrm{Cl}(k)$ は有限アーベル群なので

$$\mathrm{Cl}(k)/(\mathrm{Cl}(k))^p \simeq C_p \times \cdots \times C_p$$

§2 問題設定

類数が p で割れるものを構成するためには …

手法 1：位数が p のイデアル類を構成する.

不分岐類体論

H_k : k 上の最大不分岐アーベル拡大
$\Longrightarrow \mathrm{Gal}(H_k/k) \simeq \mathrm{Cl}(k)$

$p \mid h_k \Longleftrightarrow \mathrm{Gal}(H_k/k)$ が部分群として C_p を含む.
$\Longleftrightarrow k$ 上に p 次不分岐巡回拡大が存在する.

手法 2：p 次不分岐巡回拡大を構成する.

§2 問題設定

2.2. 不分岐拡大とは？

イデアル論の基本定理 (Dedekind, 1871)

代数体 k の任意のイデアル $\mathfrak{a}$ は素イデアルの積に一意的に書ける:

$$\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r} \quad (m_i \geq 1).$$

L/K : ガロア拡大
K の素イデアル $\mathfrak{p}$ はイデアル論の基本定理より

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^m$$

と表される. このとき,

$$\mathfrak{p} : \underline{\text{分岐}} \iff m \geq 2,$$
$$\mathfrak{p} : \underline{\text{不分岐}} \iff m = 1.$$

K のすべての素イデアルが L において不分岐となるとき, L/K を <u>不分岐拡大</u> という.

§3 2次体の類数の3での可除性

次の事実を用いて, 類数が3で割れる2次体を特徴づける.

- 2次体 k に対し,

$$L/k : 3\text{次不分岐巡回拡大} \implies \mathrm{Gal}(L/\mathbb{Q}) \simeq S_3.$$

- 3次多項式

$$X^3 - \frac{v}{u}X - \frac{v}{u} \ (u, v \in \mathbb{Z})$$

はすべての S_3-拡大を与える.

- 多項式の係数から, 分岐・不分岐の様子がわかる.
(例えば,

$$v = v_1 w^3 \ (v_1 : \text{cube-free})$$

とすると, $\mathfrak{p} \mid v_1$ なる $\mathfrak{p}$ は L/k で分岐.)

§3 2次体の類数の3での可除性

定理 (三宅-K, 1997)

$k := \mathbb{Q}(\sqrt{D})$, $D := 4uw^3 - 27u^2$

$$\left(\begin{array}{l} u,\ w \in \mathbb{Z},\ (u, w) = 1, \\ X^3 - uwX - u^2 : \mathbb{Q} \text{ 上既約}, \\ \text{次のいずれかの条件を満たす:} \\ \text{(a) } 3 \nmid w \\ \text{(b) } 3 \mid w,\ uw \not\equiv 3 \pmod 9,\ u \equiv w \pm 1 \pmod 9 \\ \text{(c) } 3 \mid w,\ uw \equiv 3 \pmod 9,\ u \equiv w \pm 1 \pmod{27} \end{array}\right)$$

$\Longrightarrow 3 \mid h_k$

逆に $3 \mid h_{\mathbb{Q}(\sqrt{D})}$ ならば, 上の条件を満たす $u, w \in \mathbb{Z}$ により

$$D = 4uw^3 - 27u^2$$

と表される.

§3 2次体の類数の3での可除性

定理 (今岡-小松, 1998)

D : square-free
L : $\mathbb{Q}(\sqrt{D})$ 上の3次不分岐巡回拡大
$\Longrightarrow {}^{\exists} a,\ b,\ m \in \mathbb{Z}$ s.t.
(i) $L : X^3 - 3mX - a$ の最小分解体
(ii) $4m^3 = a^2 + 27b^2D$
(iii) $(a, m) = 1$

上記定理の逆は成り立つか？

§3 2次体の類数の3での可除性

(ii), (iii) を満たす a, m に対し, 三宅-K で $u = a^2$, $w = 3m$ とおくと $(u, w) = 1$ であり, さらに三宅-K の条件 (c) を満たす. また

$$X^3 - 3a^2mX - a^4 = 0$$

に $X = aY$ を代入し両辺 a^3 で割ると

$$Y^3 - 3mY - a = 0.$$

従って, 上記条件 (ii), (iii) を満たす a, m に対し, 多項式

$$X^3 - 3mX - a$$

は 既約ならば $\mathbb{Q}(\sqrt{D})$ 上に不分岐拡大を与える.

$X^3 - 3mX - a$がいつ既約になるのか？

§3 2次体の類数の3での可除性

(ii) $4m^3 = a^2 + 27b^2D$

$$\Longrightarrow m^3 = \frac{a^2+27b^2D}{4} = \left(\frac{a+3b\sqrt{-3D}}{2}\right)\left(\frac{a-3b\sqrt{-3D}}{2}\right)$$

補題

$$X^3 - 3mX - a : \text{既約} \iff \frac{a+3b\sqrt{-3D}}{2} \notin \mathbb{Q}(\sqrt{-3D})^3$$

定理 A

$3 \mid h_{\mathbb{Q}(\sqrt{D})}$

$$\iff {}^{\exists}\gamma \in \mathbb{Q}(\sqrt{-3D}) \text{ s.t. } \begin{array}{ll} \text{(i)} & \gamma = \dfrac{a+3b\sqrt{-3D}}{2} \quad (a,b \in \mathbb{Z}) \\ \text{(ii)} & N(\gamma) \in \mathbb{Z}^3 \\ \text{(iii)} & \gamma \notin \mathbb{Q}(\sqrt{-3D})^3 \\ \text{(iv)} & (a, N(\gamma)) = 1 \end{array}$$

§3 2次体の類数の3での可除性

定理 (Scholz, 1932)

$D > 0$: square-free
$s : \mathbb{Q}(\sqrt{D})$ の 3-rank
$r : \mathbb{Q}(\sqrt{-3D})$ の 3-rank
$\Longrightarrow s \leq r \leq s+1$

$\mathbb{Q}(\sqrt{D})$ と $\mathbb{Q}(\sqrt{-3D})$ に対する

- 鏡映関係
- reflection
- Spiegelung relation

などと呼ばれる.

§4 素数3から p への拡張

拡張の方向 ①

類数が 3 で割れる 2 次体

$\Downarrow$

類数が p で割れる 2 次体

2 次体 k に対し,

$$L/k : 3 \text{ 次不分岐巡回拡大} \implies \mathrm{Gal}(L/\mathbb{Q}) \simeq S_3.$$
$$L/k : p \text{ 次不分岐巡回拡大} \implies \mathrm{Gal}(L/\mathbb{Q}) \simeq D_p.$$

問題

$\mathbb{Q}$ 上にすべての D_p-拡大を与えるような多項式を構成せよ. 難

§4 素数 3 から p への拡張

拡張の方向 ②

類数が 3 で割れる 2 次体

$\Downarrow$

類数が p で割れる $p-1$ 次体

$p=5$ の場合については, 定理 A 及び Scholz の不等式の拡張が得られた.

$p \geq 7$ の場合は, すべてではないが, $p \mid h_M$ なる $p-1$ 次巡回体 M の無限族は得られている.

§4 素数3から p への拡張

素数 p に対し,

$$D_p := \langle \sigma, \iota \mid \sigma^p = \iota^2 = 1,\ \iota^{-1}\sigma\iota = \sigma^{-1} \rangle :\ \text{位数 } 2p \text{ の二面体群}$$

$$F_p := \langle \sigma, \iota \mid \sigma^p = \iota^{p-1} = 1,\ \iota^{-1}\sigma\iota = \sigma^a \rangle :\ \text{位数 } p(p-1) \text{ の}$$
$$\text{フロベニウス群}$$

と定義する. ここで, a は modulo p の原始根, すなわち,

$$(\mathbb{Z}/p\mathbb{Z})^\times = \langle \overline{a} \rangle$$

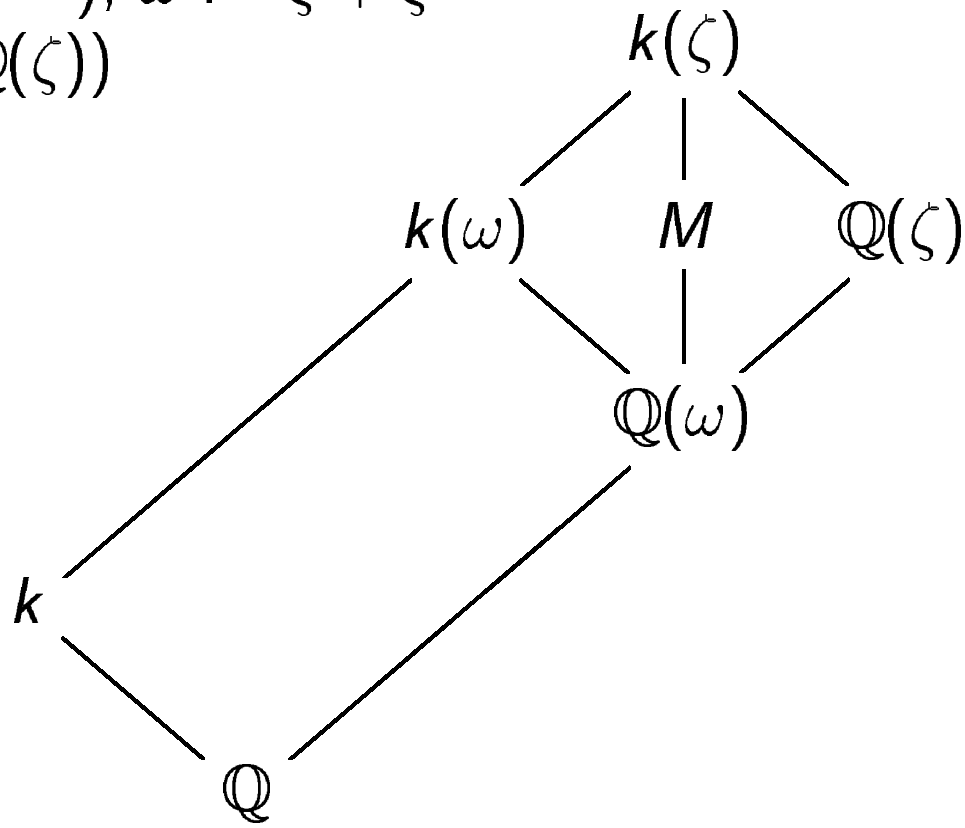
を満たす整数とする.
$p = 3$ のとき,

$$F_3 = D_3 = S_3$$

となる.

§4 素数3から p への拡張

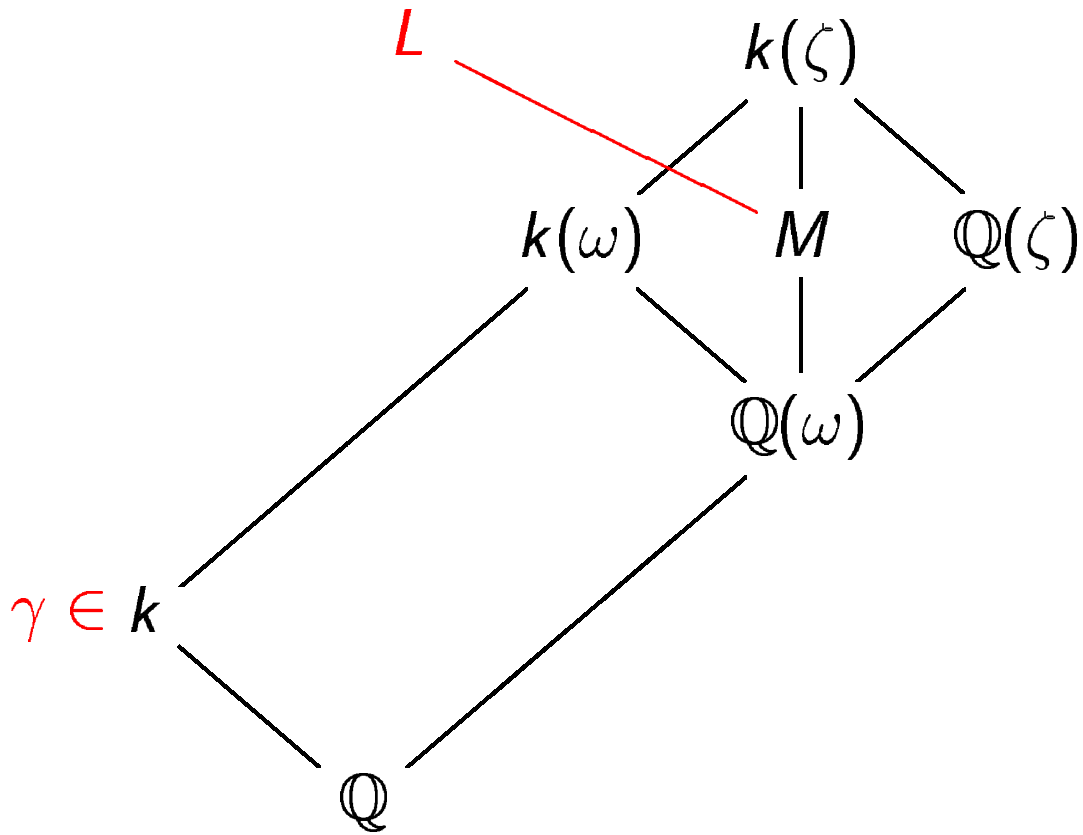
ζ : 1 の原始 p 乗根 $(:= e^{2\pi i/p})$, $\omega := \zeta + \zeta^{-1}$
$k := \mathbb{Q}(\sqrt{d})$: 2 次体 $(\not\subset \mathbb{Q}(\zeta))$



$\Longrightarrow M/\mathbb{Q}$: $p-1$ 次巡回体

k と M には “鏡映関係” がある.

§4 素数3から p への拡張



M を含みある条件を満たす F_p-拡大 L が, k の元 γ から作られる.
最小分解体が L となるような多項式 $f_\gamma(X)$ が γ から構成される.

§4 素数3から p への拡張

$$f_\gamma(X) = \sum_{i=0}^{(p-1)/2} (-N(\gamma))^i \frac{p}{p-2i} \binom{p-i-1}{i} X^{p-2i} - N(\gamma)^{(p-1)/2}\mathrm{Tr}(\gamma)$$

$\Longrightarrow$ ・この多項式を用いて, 類数が p で割れる $p-1$ 次巡回体の無限族を構成した. (K, 2004)

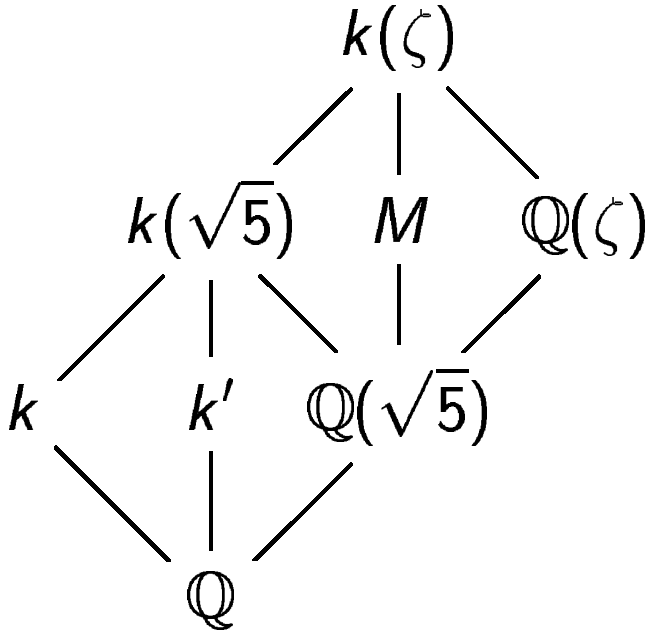
・$p=3$ の場合は, 定理 A と同じ結果が得られる.

・$p=5$ の場合は, 次が得られる.

§4 素数3から p への拡張

$p = 5$ の場合:

$k := \mathbb{Q}(\sqrt{d})$: 2次体 $(\neq \mathbb{Q}(\sqrt{5}))$
ζ : 1の原始5乗根 $(:= e^{2\pi i/5})$



M を含むすべての F_5-拡大は, 多項式

$$f_\gamma(X) = X^5 - 5N(\gamma)X^3 + 5N(\gamma)^2X - N(\gamma)^2\mathrm{Tr}(\gamma) \quad (\gamma \in k \text{ or } \gamma \in k')$$

で与えられる.

§4 素数3から p への拡張

定理

$5 \mid h_M$

$\iff {}^{\exists}\gamma \in \mathcal{O}_k$ or $\gamma \in \mathcal{O}_{k'}$ s.t.

(i) $N(\gamma) \in \mathbb{Z}^5$

(ii) $\gamma \notin k^5$ (resp. $\notin k'^5$)

(iii) $(\mathrm{Tr}(\gamma), N(\gamma)) = 1$

(iv) 次のいずれかを満たす:

$\mathrm{Tr}(\gamma)^2 \equiv 4N(\gamma) \pmod{5^3}$

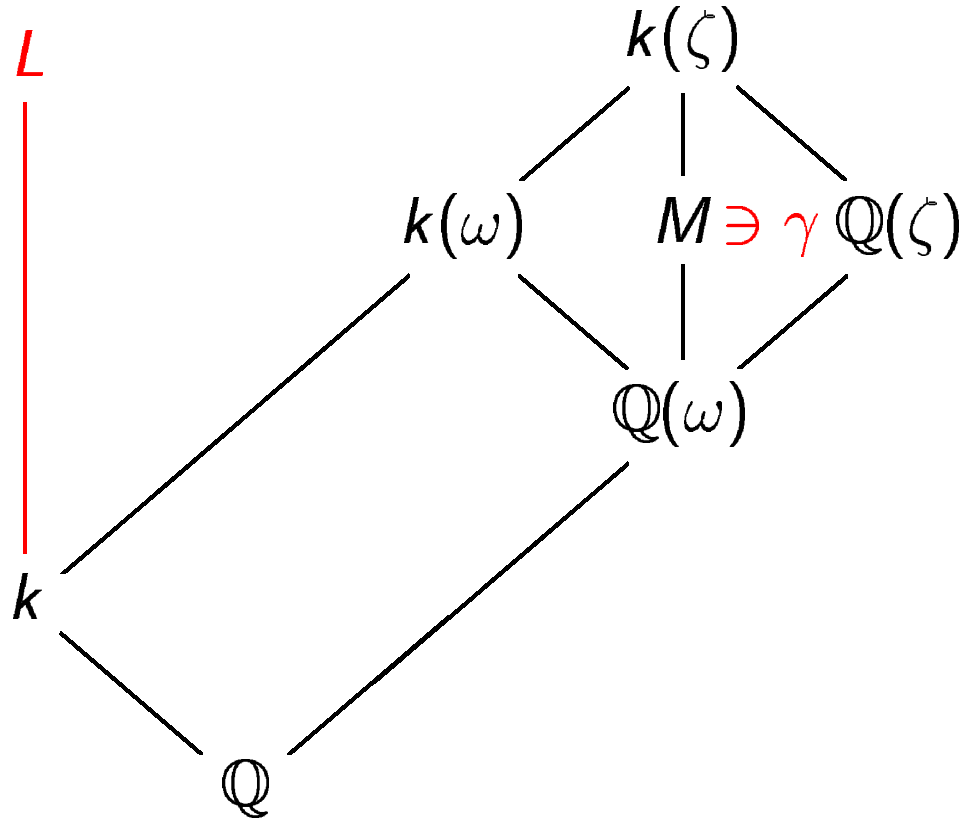
$\mathrm{Tr}(\gamma) \equiv 0 \pmod{5^2}$

$\mathrm{Tr}(\gamma)^2 \equiv N(\gamma) \pmod{5^2}$

$\mathrm{Tr}(\gamma)^2 \equiv 2N(\gamma) \pmod{5^2}$

$\mathrm{Tr}(\gamma)^2 \equiv 3N(\gamma) \pmod{5^2}$

§4 素数3から p への拡張

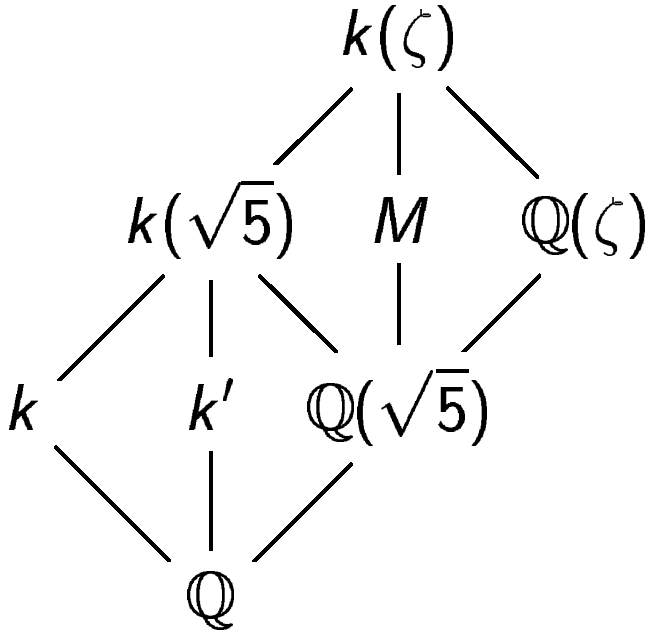


k を含むすべての D_p-拡大 L が, M の元 γ を用いて作られる.
最小分解体が L となるような多項式を γ から構成したい.

§4 素数3から p への拡張

$p = 5$ の場合:

$k := \mathbb{Q}(\sqrt{d})$: 2 次体 $(\neq \mathbb{Q}(\sqrt{5}))$
ζ : 1 の原始 5 乗根 $(:= e^{2\pi i/5})$



k を含むすべての D_5-拡大は, 多項式

$$g_\gamma(X) = X^5 - 10N(\gamma)X^3 - 5N(\gamma)NT(\gamma)X^2 + 5N(\gamma)\{N(\gamma) - NT(\gamma^{1+\tau})\}X - N(\gamma)NT(\gamma^{2+\tau}) \quad (\gamma \in M)$$

で与えられる. 但し, τ は $\mathrm{Gal}(k(\zeta)/k) = \langle\tau\rangle, \zeta^\tau = \zeta^2$.

§4 素数3から p への拡張

$\{F_n\}$: フィボナッチ数列 $(1, 1, 2, 3, 5, 8, 13, \ldots)$
$\{L_n\}$: リュカ数列 $(1, 3, 4, 7, 11, 18, 31, \ldots)$
$d := -F_{2m+1}$

$$\varepsilon := \frac{1+\sqrt{5}}{2} : \mathbb{Q}(\sqrt{5}) \text{ の基本単数}$$

$$\gamma_m := 1 + \varepsilon^m \sqrt{d}(\zeta - \zeta^{-1}) \in M \, (= \mathbb{Q}(\sqrt{d}(\zeta - \zeta^{-1})))$$

$$\begin{aligned} \Longrightarrow g_{\gamma_m}(X) = X^5 - 10X^3 - 20X^2 + 5(20F_{2m+1}^2 - 3)X \\ + 40F_{2m+1}^2((-1)^m L_{2m+1} + 1) - 4 \end{aligned}$$

定理 (K, 2008)

$m \equiv 12 \pmod{5^2}$
$\Longrightarrow g_{\gamma_m}$ は k 上の5次不分岐巡回拡大を与える.
(従って, $\mathbb{Q}(\sqrt{-F_{50s+25}})$ の類数は5で割れる.)

§5 2次体の類数の n での可除性

5.1. イデアル類群が C_n を含む2次体の無限族 (過去の結果)

定理 (Nagel, 1922)

$n, x, z \in \mathbb{Z}$, $n > 0$: 奇数, z : 奇数, $(x, z) = 1$, $z^n > x^2$
n の任意の素因子 q に対し, $q \mid x$, $q^2 \nmid x$,
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{x^2 - z^n})) \supset C_n$

定理 (Ankeny and Chowla, 1955)

$n, x \in \mathbb{Z}$, n : 偶数, x : 偶数, $0 < x < \sqrt{2 \cdot 3^{n-1}}$, $x^2 - 3^n$: square-free
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{x^2 - 3^n})) \supset C_n$

定理 (Gross and Rohrich, 1978)

$n, z \in \mathbb{Z}$, $n \geq 3$: 奇数, $z \geq 2$
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{1 - 4z^n})) \supset C_n$

§5 2次体の類数の n での可除性

定理 (Yamamoto, 1970)

$n \in \mathbb{Z}$, p_i : n の任意の素因子
q_i, q_i' : 次を満たす素数:
$q_i \equiv 1 \pmod{p_i}$ if $p_i \neq 2$, $q_i \equiv 1 \pmod{4}$ if $p_i = 2$
x, z, x', z': 次を満たす $X^2 - 4Z^n = X'^2 - 4Z'^n$ の整数解:
$(x, z) = (x', z') = 1$, $q_i \mid z$, $q_i' \mid z'$
$x\,(x')$ は mod q_i (q_i') の p_i べき剰余でない
$(x + x')/2$ は mod q_i の p_i べき剰余
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{x^2 - 4z^n})) \supset C_n$

定理 (Weinberger, 1973)

$n \in \mathbb{Z}$, $n > 0$: 奇数
$p\,(> n)$: 任意の奇数 e に対し, $X^e - 4$ が $\mathbb{F}_p$ で既約となる素数
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{4 + p^{2n}})) \supset C_n$

定理 (Ichimura, 2003)

$n, z \in \mathbb{Z}$, $n \geq 2$, $z \geq 3$: 奇数
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{4 + z^{2n}})) \supset C_n$

§5 2次体の類数の n での可除性

$$\mathbb{Q}(\sqrt{x^2 - z^n}) : \text{Nagel}$$
$$\mathbb{Q}(\sqrt{x^2 - 3^n}) : \text{Ankeny and Chowla}$$
$$\mathbb{Q}(\sqrt{1 - 4z^n}) : \text{Gross and Rohrich}$$
$$\mathbb{Q}(\sqrt{x^2 - 4z^n}) : \text{Yamamoto}$$
$$\mathbb{Q}(\sqrt{4 + p^{2n}}) : \text{Weinberger}$$
$$\mathbb{Q}(\sqrt{4 + z^{2n}}) : \text{Ichimura}$$
$$\vdots$$

どの2次体も $\mathbb{Q}(\sqrt{X^2 \pm Y^n})$ or $\mathbb{Q}(\sqrt{X^2 \pm 4Y^n})$ の形をしている.

§5 2次体の類数の n での可除性

$\mathbb{Q}(\sqrt{X^2 \pm Y^n})$ (resp. $\mathbb{Q}(\sqrt{X^2 \pm 4Y^n})$) の元 α を

$$\alpha := X + \sqrt{X^2 \pm Y^n} \quad \left(\text{resp. } \alpha := \frac{X + \sqrt{X^2 \pm 4Y^n}}{2} \right)$$

ととる. このとき,

$$N(\alpha) = \mp Y^n.$$

従って, $(\alpha) = \mathfrak{a}^n$ となる2次体のイデアル $\mathfrak{a}$ が存在する.
そこで

> $\mathfrak{a}$ の類 $[\mathfrak{a}]$ の位数が n となる ———————— (☆)

ことを示す. (i.e. 手法1!)

§5 2次体の類数の n での可除性

5.2. 少し前の結果

定理 (Ankeny and Chowla, 1955)

$n, x \in \mathbb{Z}$, n : 偶数, x : 偶数, $0 < x < \sqrt{2 \cdot 3^{n-1}}$, $x^2 - 3^n$: square-free
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{x^2 - 3^n})) \supset C_n$

$x = 2^m$ (x を 2 のべきに) して, 2 つの条件

$$「n : 偶数」,\quad 「x^2 - 3^n : \text{square-free}」$$

をはずす.

定理 (K, 2008)

m, n : $2^{2m} < 3^n$ を満たす任意の正の整数, $(m, n) \neq (2, 3)$
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{2^{2m} - 3^n})) \supset C_n$

§5 2次体の類数の n での可除性

$\mathbb{Q}(\sqrt{2^{2m}-3^n})$ の元 α を

$$\alpha := 2^m + \sqrt{2^{2m}-3^n}$$

ととる. $(\alpha) = \mathfrak{a}^n$ となる $\mathbb{Q}(\sqrt{2^{2m}-3^n})$ のイデアル $\mathfrak{a}$ に対し, (☆) が成り立つことが,

α が $\mathbb{Q}(\sqrt{2^{2m}-3^n})$ の元の p 乗数でない (for $^\forall p$)

ことに帰着される. これは次の補題を用いて示される.

補題 (Bugeaud and Shorey, 2001)

任意の正の整数 m, D_1 に対し, 方程式

$$D_1 x^2 + 2^{2m} = 3^y$$

の正の整数解 (x, y) は高々1つである.

§6 その後の進展

定理 (伊東, 2009)

q : 奇素数
m, n : $2^{2m} < q^n$ を満たすある正の整数
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{2^{2m} - q^n})) \supset C_n$

鏡映関係を用いて次が示される:

定理 (K, 2009)

n : 3 以上の奇数
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{4 - 3^{3n}})) \supset C_{3n} \times C_3$

定理 (K, 2010)

s, n : 正の奇数, ~~$n \geq 3$ or $3 \mid s$~~ $(s, n) \neq (1, 1)$
$\Longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{4 - (3s^2)^{3n}})) \supset C_3 \times C_3$