実二次体の不分岐巡回 2-拡大

— 実例と生成元の計算

橋本 喜一朗

khasimot@waseda.jp
早稲田大学・基幹理工学部

27,Sep., 2019

Plan

Outline of the planned talk

- §1. Introduction　　背景と問題と ···
- §2. 二次体の Genus theory (復習と応用)
- §3. 4 次巡回拡大の Parametrization
- §4. 実二次体の C_4-Hilbert 類体・生成元の計算
- §5. 実二次体の C_8-Hilbert 類体・生成元の計算

- 虚二次体の Hilbert 類体構成 (Kronecker's Jugendtraum)
- $k = \mathbb{Q}(\sqrt{D_k})$ $(D_k < 0)$: 虚二次体, $\mathcal{O}_k = \overline{\mathbb{Z}} \cap k$.
- $^\forall\, \mathfrak{a} = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 \subset k$ ($\mathcal{O}_k$-イデアル), $\alpha_1/\alpha_2 \in \mathfrak{H}$

$$j(\mathfrak{a}) := j(\alpha_1/\alpha_2) : \text{ 類 } [\mathfrak{a}] \in C\ell(k) \text{ のみに依存}$$

- 虚数乗法論.
  1. $j(\mathfrak{a}) \in \overline{\mathbb{Z}}$, $k(j(\mathfrak{a})) = H_k$: k の Hilbert 類体
  2. $C\ell(k) = \{[\mathfrak{a}_1], \cdots, [\mathfrak{a}_h]\}$
     $\Rightarrow$ $j(\mathfrak{a}_1), \cdots, j(\mathfrak{a}_h)$ は H_k/k の完全共役系
  3. $\mathrm{Gal}(H_k/k) \cong Cl(k)$ (類体論)

$$\begin{array}{ccc} C\ell(k) & \overset{j}{\cong} & \{j(\mathfrak{a}_1), \cdots, j(\mathfrak{a}_h)\} \\ {\scriptstyle \mathfrak{p}^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma_{\mathfrak{p}}} \\ C\ell(k) & \overset{j}{\cong} & \{j(\mathfrak{a}_1), \cdots, j(\mathfrak{a}_h)\} \end{array} \qquad \boxed{j(\mathfrak{a})^{\sigma_{\mathfrak{p}}} = j(\mathfrak{a}\mathfrak{p}^{-1})}$$

• 楕円モジュラー関数 $j(\tau)$

$$j:\ \mathfrak{H} \overset{\text{正則}}{\to} \mathbb{C}, \qquad j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau),\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

$$\begin{aligned} j(\tau) &:= \frac{1728 E_2(\tau)^3}{E_4(\tau)^3 - E_3(\tau)^2} \\ &= q^{-1} + 744 + 196884 q^2 + \cdots \qquad (q = e^{2\pi i \tau}) \\ E_k(\tau) &:= \frac{1}{2\zeta(2k)} \sum_{(m,n)\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^{2k}} \\ &= 1 + (-1)^k \frac{4k}{B_k} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n \quad \text{(Eisenstein series)} \end{aligned}$$

• Kronecker's Jugendtraum の実二次体版

- $k = \mathbb{Q}(\sqrt{D_k})$ $(D_k > 0)$
- 問題 : $H_k = k(\xi_k)$: k の Hilbert 類体

  「良い生成元」の構成 = 対応 $(k \mapsto \xi_k)$ のモジュラー性
- 金子・繁木のアプローチ
- $^{\forall}\mathfrak{a} = c[a, r+\omega] \subset k$ $(\mathcal{O}_k$-イデアル, $a = \mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}) > 0, r \in \mathbb{Z})$
- $j(\tau) \to j_R : \partial_R\mathfrak{H} = \{\tau \in \mathbb{R} \,|\, [\mathbb{Q}(\tau) : \mathbb{Q}] = 2\}$ への数論的拡張
- $j_R(\tau)$ がみたすべき性質 $(\tau \in \partial_R\mathfrak{H})$

$$\begin{cases} j_R(\tau) & := j(\gamma(\tau)), \quad \gamma \in \mathrm{SL}_2(\mathbb{Z}) \\ j_R(\mathfrak{a}) & := j(\dfrac{r+\omega}{a}) \quad \text{類 } [\mathfrak{a}] \in C\ell(k) \text{ のみに依存} \\ j(\mathfrak{a}) & \in \overline{\mathbb{Z}}, \ k(j(\mathfrak{a})) = H_k \end{cases}$$

§2. 二次体の Genus theory (記号の設定)

- $k = \mathbb{Q}(\sqrt{m})$ $(m \in \mathbb{Z},$ square free, $m \neq 1)$
- $\mathcal{O}_k = \overline{\mathbb{Z}} \cap k = [1, \omega]$

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} \cdots m \equiv 1 \pmod 4 \\ \sqrt{m} \cdots m \equiv 2, 3 \pmod 4 \end{cases} \qquad D_k = \begin{cases} m \\ 4m \end{cases} \quad \text{(判別式)}$$

- D_k の素冪基本判別式への分解

$$D_k = {p_1}^* \cdots {p_r}^*, \quad {p_i}^* := \begin{cases} (\frac{-1}{p_i}) p_i \cdots p_i \neq 2 \\ -4 \cdots p_i = 2, \ m \equiv 3 \pmod 4 \\ \pm 8 \cdots p_i = 2, \ m \equiv \pm 2 \pmod 8 \end{cases}$$

• $k = \mathbb{Q}(\sqrt{D_k})$ の Genus theory(狭義)

- 代数体 K の genus field K^*

$$K^* := \max\{L \subset \mathbb{Q}^{ab}K \mid L/K : {}^{\forall}\wp\,(\text{有限素点})\text{ で不分岐 }\}$$

- 二次体 $k = \mathbb{Q}(\sqrt{D_k})$ の genus field
- $C\ell^{(+)} = C\ell^{(+)}(k)$: k の狭義イデアル類群

$$C\ell^{(+)2} = \bigcap_{\chi \in \mathrm{Hom}(C\ell^{(+)}, \{\pm 1\})} \mathrm{Ker}(\chi)$$

$$\mathrm{Gal}(k^*/k) \cong C\ell^{(+)}/C\ell^{(+)2} \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus r-1}$$

$$r - 1 = \dim_{\mathbb{F}_2}\left(C\ell^{(+)}/C\ell^{(+)2}\right) \quad : \quad C\ell^{(+)} \text{ の 2-rank}$$

- 応用

$$k^* = k(\sqrt{{p_1}^*}, \cdots, \sqrt{{p_r}^*}) = \mathbb{Q}(\sqrt{{p_1}^*}, \cdots, \sqrt{{p_r}^*})$$

$$\{\overbrace{k \subset M}^{2} \subset k^*\} \overset{1:1}{\longleftrightarrow} \{\{{D_1}^*, {D_2}^*\} \mid {D_1}^* {D_2}^* = D^*\}$$

$$M = k(\sqrt{{D_1}^*}) = k(\sqrt{{D_2}^*})$$

- $k = \mathbb{Q}(\sqrt{D_k})$ の (狭義) 不分岐二次拡大はすべてこの形

$$(\because) \quad \overbrace{k \subset M}^{2} \subset H_k \overset{1:1}{\longleftrightarrow} \overbrace{C\ell^{(+)} \supset N}^{2} \supset C\ell^{(+)\,2}$$

• $k=\mathbb{Q}(\sqrt{D_k})$ の Genus theory(広義)

- 実二次体 $k=\mathbb{Q}(\sqrt{D_k})$ の不分岐二次拡大

$$\{\overbrace{k\subset M}^{2}\subset k^*\} \overset{1:1}{\longleftrightarrow} \{\{{D_1}^*,{D_2}^*\}\,|\,{D_1}^*{D_2}^*=D^*\}$$
$$M=k(\sqrt{{D_1}^*})=k(\sqrt{{D_2}^*})$$

- ${p_i}^*<0 \Leftrightarrow \begin{cases} p_i\equiv 3 \pmod 4,\ p_i=2\,\&D_k/4\equiv 3 \pmod 4 \\ p_i=2,\ \&D_k/4\equiv -2 \pmod 8 \end{cases}$
- M/k=広義不分岐二次拡大 $\Leftrightarrow$ ${D_1}^*,{D_2}^*>0$
- $\Rightarrow$ $C\ell(k)$ (広義イデアル類群) の 2-rank

$$\dim_{\mathbb{F}_2}(C\ell/C\ell^2)=\begin{cases} r-1 & \cdots {}^{\forall}\ {p_i}^*>0 \\ r-2 & \cdots {}^{\exists}\ {p_i}^*<0 \end{cases}$$

- $C\ell(k)[2^\infty]$ が巡回群となる実二次体

- $C\ell(k)[2^\infty]$(2-part) が巡回群となる条件

$$\dim_{\mathbb{F}_2}\left(C\ell/C\ell^2\right)=1 \Leftrightarrow \begin{cases} r=2, & {p_1}^*,\ {p_2}^*>0 \\ r=3, & {}^{\exists!}\ {p_i}^*>0 \end{cases}$$

- このとき k の (広義) 不分岐 2 次拡大 M/k は unique

$$M=\begin{cases} k(\sqrt{p_1}) = k(\sqrt{p_2}), & ({p_1}^*,\ {p_2}^*>0) \\ k(\sqrt{p_1}) = k(\sqrt{p_2p_3}), & ({p_1}^*>0,\ {p_2}^*, {p_3}^*<0) \end{cases}$$

§3. 4 次巡回拡大の Parametrization

- 定理 C4. $K(\sqrt{\delta})/K$ が 4 次巡回拡大 $^{\exists}\, L/K$ の中間拡大

$$\Leftrightarrow \quad \delta = x^2 + y^2, \quad (^{\exists}\, x, y \in K^{\times})$$

$$\text{このとき} \quad L = K\left(\sqrt{\eta(\delta + x\sqrt{\delta})}\right) \quad (^{\exists}\, \eta \in K^{\times})$$

$$\mathrm{Gal}(L/K) = \langle \sigma \rangle, \ \ \sigma\left(\sqrt{\eta(\delta + x\sqrt{\delta})}\right) = \sqrt{\eta(\delta - x\sqrt{\delta})}$$

- $\longrightarrow \quad K^3 \ni (\delta, x, \eta)$: 4 次巡回拡大のパラメータ

- (ポイント) $\zeta_4 = \sqrt{-1} \in K$ のときは Kummer 理論:

$$4 \text{ 次巡回拡大 } L = K(\sqrt[4]{a}) \ \leftrightarrow \ a \in K^{\times}/(K^{\times})^4$$

条件 $\zeta_4 = \sqrt{-1} \in K$ を外すことが問題.

- 証明のスケッチ. $K^\times \cap \{x^2+y^2\}$ は群をなすことから

$$\delta = x^2+y^2 \ \Leftrightarrow\ \delta \in \mathrm{N}_{K(\sqrt{\delta})/K} \ \Leftrightarrow\ -1 \in \mathrm{N}_{K(\sqrt{\delta})/K}.$$

$$(i)\ \mathrm{Gal}(L/K) = \langle\sigma\rangle \cong \mathbb{Z}/4\mathbb{Z},\ K(\sqrt{\delta}) \subset L$$

$$\Rightarrow L = K(\sqrt{\delta}, \sqrt{\alpha}),\ {}^\exists\,\alpha \in K(\sqrt{\delta})$$

$$\Rightarrow \beta := \sigma(\alpha)/\alpha \in K(\sqrt{\delta}),\ \beta\sigma(\beta) = \sigma^2(\beta)/\beta = -1$$

$$\Rightarrow \mathrm{N}_{K(\sqrt{\delta})/K}(\beta) = -1 \ \Rightarrow\ \delta = x^2+y^2.$$

$$(ii)\ \mathrm{N}_{K(\sqrt{\delta})/K}(\beta) = -1 \overset{\textit{Hilbert}\ 90}{\Rightarrow} \beta^2 = \overline{\sigma}(\alpha)/\alpha,\ {}^\exists\,\alpha \in K(\sqrt{\delta})$$

$$\Rightarrow \alpha \notin K(\sqrt{\delta})^{\times 2},\ L := K(\sqrt{\delta}, \sqrt{\alpha})\ (4\text{ 次拡大})$$

$$K[X] \ni (X^2-\alpha)(X^2-\overline{\sigma}(\alpha)) = (X^2-\alpha)(X^2-\beta^2\alpha) = \mathrm{Irr}(\sqrt{\alpha}, K)$$

$$\Rightarrow L = K(\sqrt{\alpha})/K : \text{Galois ext},\ {}^\exists\,\sigma \in \mathrm{Gal}(L/K) :\ \sigma|_{K(\sqrt{\delta})} = \overline{\sigma}$$

$$\Rightarrow \sigma(\sqrt{\alpha}) := \beta\sqrt{\alpha} \ \Rightarrow\ \mathrm{Gal}(L/K) = \langle\sigma\rangle \cong \mathbb{Z}/4\mathbb{Z}$$

- 定理の記号では $\beta = (\delta - x\sqrt{\delta})/(y\sqrt{\delta}),\ \alpha = \eta(\delta + x\sqrt{\delta})$

• $\mathbb{Q}$ 上の 4 次巡回拡大：Gauss 周期

- 奇素数 p: $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \langle\sigma\rangle \overset{can}{=} {\mathbb{F}_p}^{\times} \cong \mathbb{Z}/(p-1)\mathbb{Z}$

$$\mathbb{Q}(\zeta_p) \supseteq^{\exists} L \text{ (4 次巡回体)} \quad \Leftrightarrow \quad p \equiv 1 \pmod 4$$

$$\text{このとき} \quad L = \mathbb{Q}(\xi) \supset \mathbb{Q}(\sqrt{p}),\ \xi \in \{\xi_i \,|\, (0 \le i \le 3)\}$$

$$\text{Gauss 周期} : \xi_i := \sum_{j=1}^{(p-1)/4} \sigma^{4j+i}(\zeta_p), \quad \sqrt{p} = \sum_{j=1}^{p-1} (\frac{j}{p})\sigma^j(\zeta_p)$$

- Corollary. 定理 C4 より $p = x^2 + y^2$ $({}^{\exists}\, x, y \in \mathbb{Q}^{\times})$
- 問題. 対応 $\mathbb{Q}(\sqrt{\eta(p + x\sqrt{p})} \mapsto (p, x, \eta)$ の「モジュラー性」

- $\mathrm{Irr}(\xi, \mathbb{Q})$: **Gauss 周期 ξ の最小多項式**

$$\mathrm{Irr}(\xi, \mathbb{Q}) = X^4 + X^3 + \frac{1}{8}(3 - p - 2(\frac{2}{p})p)X^2 + c_1(p)X + c_0(p)$$

$$c_1(p) = \frac{1}{16}(1 - p - 2p(\frac{2}{p}) + pa_p), \quad c_0(p) = \cdots$$

p	a_p	$\mathrm{Irr}(\xi, \mathbb{Q})$
5	-2	$1 + X + X^2 + X^3 + X^4$
13	6	$3 - 4X + 2X^2 + X^3 + X^4$
17	2	$1 - X - 6X^2 + X^3 + X^4$
29	-10	$23 + 20X + 4X^2 + X^3 + X^4$
37	-2	$49 + 7X + 5X^2 + X^3 + X^4$
41	10	$-4 + 18X - 15X^2 + X^3 + X^4$
53	14	$47 - 43X + 7X^2 + X^3 + X^4$
61	-10	$117 + 42X + 8X^2 + X^3 + X^4$
73	-6	$2 - 41X - 27X^2 + X^3 + X^4$
89	10	$8 + 39X - 33X^2 + X^3 + X^4$
97	18	$-61 + 91X - 36X^2 + X^3 + X^4$

• a_p の数論的意味 $\cdots$ $\sqrt{-1} \in \mathrm{End}(E)$ instead of Kummer ext'n.

- 定理 (Fermat,1630's). 奇素数 p :

  $p = x^2 + y^2$ $(^\exists x, y \in \mathbb{Z})$ $\Leftrightarrow$ $p \equiv 1 \pmod 4$, *i.e.* $p = p^*$

- 定理 (Jacobsthal,1906). $JS_p(c) := \sum_{k \in \mathbb{F}_p} \left(\frac{k(k^2 - c)}{p} \right)$

$$\Rightarrow p = \left(\frac{1}{2} JS_p(a) \right)^2 + \left(\frac{1}{2} JS_p(b) \right)^2, \quad {\mathbb{F}_p}^\times / ({\mathbb{F}_p}^\times)^2 = \{a, b\}$$

- $a_p = -JS_p(1) = \mathrm{Tr}\ (\sigma_p : E \otimes \mathbb{F}_p \to E \otimes \mathbb{F}_p)$
- $\left| E(\mathbb{F}_p) \right| = p + 1 - a_p$ (楕円曲線 $E : y^2 = x^3 - x$)
- $^{\exists!}\, f = \sum_{n=1}^{\infty} a_n q^n \in S_2(32) = \mathbb{C} f, \quad a_1 = 1$

4 次巡回拡大族 $\{L/\mathbb{Q} \mid D(L/\mathbb{Q}) = p^3\}_p$ の「モジュラー性」

- $^{\forall} p \equiv 1 \pmod 4 \ \mapsto \ ^{\exists}!\ L = \mathbb{Q}(\sqrt{\eta(p + a_p\sqrt{p}/2)}\ (\eta \in \mathbb{Q})$
  4 次巡回体 s.t. $D(L/\mathbb{Q}) = p^3$
- 対応 $\mathbb{Q}(\sqrt{\eta(p + a_p\sqrt{p})} \mapsto (p, a_p, \eta)$ は「モジュラー的」:

$$\begin{cases} a_p &= \int_0^1 e^{-2\pi i p(x+iy)} f(x+iy)\, dx \ ^{\exists}! \quad f \in S_2(32) \\ \eta &= (\frac{2}{p})2 \end{cases}$$

$$L \cong \mathbb{Q}[X]/(\mathrm{Irr}(\xi, \mathbb{Q})) \cong \mathbb{Q}[X]/(X^4 - 2p\eta X^2 + p\eta {b_p}^2/4),$$
$$4p = {a_p}^2 + {b_p}^2$$

- 問題. $D(L/\mathbb{Q}) \neq p^3$ の場合は？

§4. 実二次体の $C4$-Hilbert 類体・生成元

- $k = \mathbb{Q}(\sqrt{D_k})$ $(D_k = {p_1}^* \cdots {p_r}^* > 0)$, $\quad C\ell(k) \cong \mathbb{Z}/4\mathbb{Z}$
- H_k/k : Hilbert 類体 (不分岐 $C4$ 拡大 of k)

$$\Rightarrow \quad {}^{\exists !}\, M_k = k(\sqrt{p^*})/k \subset H_k/k,$$
$$p^* = p|D_k,\ p = x^2 + y^2 \geq 2$$
$$H_k = k(\sqrt{\eta(p + x\sqrt{p})}), \quad \eta \in k^\times$$

- 問題. パラメータ (p, x, η) の計算, その「モジュラー性 ?」

• $\eta \in k$ の計算　$k = \mathbb{Q}(\sqrt{D_k})$

- 共役差積 (Differente) の連鎖律

$$\mathcal{D}(K) = \mathcal{D}(K/k)\mathcal{D}(k) \quad (\mathbb{Q} \subseteq k \subseteq K \text{ 有限次拡大})$$
$$\therefore \quad D(K) = D_{K/k} \cdot D_k{}^{[K:k]} \quad (\mathrm{N}_{K/\mathbb{Q}} = \mathrm{N}_{k/\mathbb{Q}} \circ \mathrm{N}_{K/k})$$

- 判定条件:

$$H_k/k : \text{不分岐} \ \Leftrightarrow \ \mathcal{D}(H_k/k) = 1 \ \Leftrightarrow \ D(H_k) = D_k{}^{[K:k]}$$

• MATHEMATICA による $\eta \in k$ の計算例　$k = \mathbb{Q}(\sqrt{D_k})$

- 条件 $\mathcal{D}(H_k/k) = 1 \Leftrightarrow D(H_k/\mathbb{Q}) = {D_k}^4$
- $D_k = 145 = 5{\cdot}29$ の場合　$\overbrace{k \subset M}^{2} = k(\sqrt{5}) = k(\sqrt{29})$

• Input= Table[{nn, NumberFieldDiscriminant[Sqrt[
(5*nn + Sqrt[5*29])*(5 + Sqrt[5])]] // FactorInteger },{nn, 1, 6 }]

• Output= {
{1, {{2, 6}, {3, 2}, {5, 4}, {29, 4} }},
{2, {{2, 12}, {5, 4}, {29, 4} }},
{3, {{5, 4} {29, 4} }},
{4, {{2, 12}, {3, 2}, {5, 4}, {17, 2}, {29, 4} }},
{5, {{2, 10}, {3, 2}, {5, 4}, {29, 4} },
{6, {{2, 12}, {5, 4}, {29, 4}, {151, 2}} },
}

• $\Rightarrow \ (p, \eta) = (5, 15 + \sqrt{145})$!!

• MATHEMATICA による $\eta \in k$ の計算例　$k = \mathbb{Q}(\sqrt{D_k})$

- 条件 $\mathcal{D}(H_k/k) = 1 \Leftrightarrow D(H_k/\mathbb{Q}) = {D_k}^4$
- $D_k = 145 = 5{\cdot}29$ の場合　$\overbrace{k \subset M}^{2} = k(\sqrt{5}) = k(\sqrt{29})$

• Input= Table[{nn, NumberFieldDiscriminant[Sqrt[
(29*nn + 2*Sqrt[5*29])*(29 + 2*Sqrt[29])]] // FactorInteger },{nn, 1, 6 }]

• Output= {
{1, {{5, 4} {29, 4} }},
{2, {{2, 6}, {3, 2}, {5, 4}, {29, 4} }},
{3, {{2, 8}, {5, 4}, {29, 4}, {241, 2} }},
{4, {{2, 12}, {3, 2}, {5, 4}, {29, 4}, {37, 2} }},
{5, {{3, 2}, {5, 6}, {29, 4}, {47, 2} } },
{6, {{5, 4}, {29, 4}} },
}

• $\Rightarrow \ (p, \eta) = (29, 29 + 2\sqrt{145}),\ (29, 29{\cdot}6 + 2\sqrt{145})$!!

- $C\ell(k) \cong \mathbb{Z}/4\mathbb{Z}$ をみたす実二次体 $k = \mathbb{Q}(\sqrt{D_k})$

$$
\begin{aligned}
&\{D_k \mid C\ell(k) \cong \mathbb{Z}/4\mathbb{Z}, \quad 0 < D_k < 6000\} \\
=&\{145, 328, 445, 505, 689, 777, 793, 876, 897, 901, 905, \\
&1045, 1096, 1145, 1164, 1221, 1288, 1292, 113, 1677, 1736, \\
&1745, 1752, 2005, 2056, 2249, 2289, 2316, 2328, 2501, 2504, \\
&2533, 2545, 2632, 2669, 2696, 2824, 2849, 2892, 2924, 2945, \\
&3029, 3161, 3164, 3245, 3272, 3341, 3477, 3545, 3656, 3756, \\
&3772, 3805, 3836, 3845, 3905, 3916, 4012, 4017, 4044, 4045, \\
&4053, 4081, 4168, 4173, 4268, 4424, 4552, 4556, 4616, 4632, \\
&4705, 4744, 4777, 4908, 4972, 4981, 5037, 5045, 5084, 5105, \\
&5109, 4953, 5181, 5217, 5245, 5421, 5484, 5545, 5548, 5605, \\
&5644, 5704, 5768, 5809, 5817, 5848, 5933, 5973\} \quad \# = 99
\end{aligned}
$$

- $M_k = k(\sqrt{p})$ $(p|D_k,\ p = x^2 + y^2)$, $\quad H_k = k(\sqrt{\eta(p + x\sqrt{p})}),\ \eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
145	$5, 29$	$(5, 1, 2)$	$15 + \sqrt{145}$	$7 + 2\sqrt{5}$
328	$2^3, 41$	$(2, 1, 1)$	$2(20 + \sqrt{328})$	$7 + 2\sqrt{2}$
445	$5, 89$	$(5, 1, 2)$	$25 + \sqrt{445}$	$13 + 4\sqrt{5}$
505	$5, 101$	$(5, 1, 2)$	$35 + \sqrt{505}$	$11 + 2\sqrt{5}$
689	$13, 53$	$(13, 2, 3)$	$2(39 + \sqrt{689})$	$\left(15 + \sqrt{13}\right)/2$
777	$-3, -7, 37$	$(37, 1, 6)$	$3(37 + \sqrt{777})$	$11 + 2\sqrt{21}$
793	$13, 61$	$(13, 2, 4)$	$2(91 + \sqrt{793})$	$\left(19 + 3\sqrt{13}\right)/2$
876	$-2^2, -3, 73$	$(73, 3, 8)$	$2(292 + \sqrt{876})$	$11 + 4\sqrt{3}$
897	$-3, 13, -23$	$(13, 2, 3)$	$2(247 + \sqrt{897})$	$11 + 2\sqrt{13}$
901	$17, 53$	$(17, 1, 4)$	$(51 + \sqrt{901})$	$11 + 2\sqrt{17}$
905	$5, 181$	$(5, 1, 2)$	$(35 + \sqrt{905})$	$19 + 6\sqrt{5}$
1045	$5, -11, -19$	$(5, 1, 2)$	$(45 + \sqrt{1045})$	$17 + 4\sqrt{5}$

$H_k = k(\sqrt{\theta_0})$, (θ_0 in Yamamura's list)

- $M_k = k(\sqrt{p})$ $(p|D_k,\ p = x^2 + y^2)$, $\quad H_k = k(\sqrt{\eta(p + x\sqrt{p})}),\ \eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
1096	$2^3, 137$	$(2, 1, 1)$	$36 + \sqrt{1096}$	$13 + 4\sqrt{2}$
1145	$5, 229$	$(2, 1, 1)$	$35 + \sqrt{1145}$	$\left(31 + 3\sqrt{5}\right)/2$
1164	$-2^2, -3, 97$	$(97, 4, 9)$	$388 + 3\sqrt{1164}$	$17 + 8\sqrt{3}$
1221	$-3, -11, 37$	$(37, 1, 6)$	$37 + \sqrt{1221}$	$\left(25 + \sqrt{33}\right)/2$
1288	$2^3, -7, -23$	$(2, 1, 1)$	$36 + \sqrt{1288}$	$17 + 8\sqrt{2}$
1292	$-2^2, 17, -19$	$(17, 1, 4)$	$68 + \sqrt{1294}$	$6 + \sqrt{17}$
1313	$13, 101$	$(13, 2, 3)$	$2(39 + \sqrt{1313})$	$31 + 2\sqrt{13}$
1677	$-3, 13, -43$	$(13, 2, 3)$	$2(65 + \sqrt{1677})$	$\left(23 + \sqrt{13}\right)/2$
1736	$2^3, -7, -31$	$(2, 1, 1)$	$2(52 + \sqrt{1736})$	$15 + 2\sqrt{2}$
1745	$5, 349$	$(5, 1, 2)$	$55 + \sqrt{1745}$	$23 + 6\sqrt{5}$
1752	$-2^3, -3, 73$	$(73, 3, 8)$	$73 + \sqrt{1752}$	$13 + 4\sqrt{6}$
2005	$5, 401$	$(5, 1, 2)$	$45 + \sqrt{2005}$	$\left(43 + 7\sqrt{5}\right)/2$

- $M_k = k(\sqrt{p})$ $(p|D_k,\ p = x^2 + y^2)$, $\quad H_k = k(\sqrt{\eta(p + x\sqrt{p})}),\ \eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
2056	$2^3, 257$	$(2, 1, 1)$	$2(52 + \sqrt{2056})$	$17 + 4\sqrt{2}$
2249	$13, 173$	$(13, 2, 3)$	$117 + 2\sqrt{2249}$	$15 + 2\sqrt{13}$
2289	$-3, -7, 109$	$(109, 3, 10)$	$2(109 + 2\sqrt{2289})$	$(31 + 5\sqrt{21})/2$
2316	$-2^2, -3, 193$	$(193, 7, 12)$	$2(1351 + 6\sqrt{2316})$	$25 + 12\sqrt{3}$
2328	$-2^3, -3, 97$	$(97, 4, 9)$	$2(485 + \sqrt{2328})$	$11 + 2\sqrt{6}$
2501	$41, 61$	$(41, 4, 5)$	$2(451 + \sqrt{2501})$	$15 + 2\sqrt{41}$
2504	$2^3, 313$	$(2, 1, 1)$	$52 + \sqrt{2504}$	$21 + 8\sqrt{2}$
2533	$17, 149$	$(17, 1, 4)$	$51 + \sqrt{2533}$	$(49 + \sqrt{17})/2$
2545	$5, 509$	$(5, 1, 2)$	$95 + 2\sqrt{2545}$	$23 + 2\sqrt{5}$
2632	$2^3, -7, -47$	$(2, 1, 1)$	$2(180 + \sqrt{2632})$	$23 + 10\sqrt{2}$
2669	$17, 157$	$(17, 1, 4)$	$119 + \sqrt{2669}$	$15 + 2\sqrt{17}$
2696	$2^3, 337$	$(2, 1, 1)$	$52 + \sqrt{2696}$	$25 + 12\sqrt{2}$

- $M_k = k(\sqrt{p})$ $(p|D_k,\ p = x^2 + y^2)$, $\quad H_k = k(\sqrt{\eta(p + x\sqrt{p})}),\ \eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
2824	$2^3, 353$	$(2, 1, 1)$	$68 + \sqrt{2824}$	$19 + 2\sqrt{2}$
2849	$-7, -11, 37$	$(37, 1, 6)$	$111 + \sqrt{2849}$	$15 + 2\sqrt{37}$
2892	$-2^2, -3, 241$	$(241, 4, 15)$	$964 + \sqrt{2892}$	$17 + 4\sqrt{3}$
2924	$-2^2, 17, -43$	$(17, 1, 4)$	$2(68 + \sqrt{2924})$	$14 + 3\sqrt{17}$
2945	$5, -19, -31$	$(5, 1, 2)$	$55 + \sqrt{2945}$	$(51 + 7\sqrt{5})/2$
3029	$13, 233$	$(13, 2, 3)$	$2(429 + \sqrt{3029})$	$21 + 4\sqrt{13}$
3161	$29, 109$	$(29, 2, 5)$	$2(1595 + \sqrt{3161})$	$15 + 2\sqrt{29}$
3164	$-2^2, -7, 113$	$(113, 7, 8)$	$2(1808 + \sqrt{3164})$	$15 + 4\sqrt{7}$
3245	$5, -11, -59$	$(5, 1, 2)$	$65 + \sqrt{3245}$	$(51 + \sqrt{5})/2$
3272	$2^3, 409$	$(2, 1, 1)$	$2(68 + \sqrt{3272})$	$21 + 4\sqrt{2}$
3341	$13, 257$	$(13, 2, 3)$	$2(273 + \sqrt{3341})$	$33 + 8\sqrt{13}$
3477	$-3, -19, 61$	$(61, 5, 6)$	$61 + \sqrt{3477}$	$51 + 6\sqrt{57}$

- $M_k = k(\sqrt{p})$ $(p|D_k,\ p = x^2 + y^2)$, $\quad H_k = k(\sqrt{\eta(p + x\sqrt{p})})$, $\eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
3545	$5, 709$	$(5, 1, 2)$	$115 + \sqrt{3545}$	$27 + 2\sqrt{5}$
3656	$2^3, 457$	$(2, 1, 1)$	$68 + \sqrt{3656}$	$23 + 6\sqrt{2}$
3756	$-2^2, -3, 313$	$(313, 12, 13)$	$1252 + 3\sqrt{3756}$	$19 + 4\sqrt{3}$
3772	$-2^2, -23, 41$	$(41, 4, 5)$	$656 + \sqrt{3772}$	$77 + 16\sqrt{23}$
3805	$5, 761$	$(5, 1, 2)$	$105 + \sqrt{3805}$	$29 + 4\sqrt{5}$
3836	$-2^2, -7, 137$	$(137, 4, 11)$	$12056 + \sqrt{3836}$	$41 + 8\sqrt{7}$
3845	$5, 769$	$(5, 1, 2)$	$85 + \sqrt{3845}$	$33 + 8\sqrt{5}$
3905	$5, -11, -71$	$(5, 1, 2)$	$95 + \sqrt{3905}$	$31 + 6\sqrt{5}$
3916	$-2^2, -11, 89$	$(89, 5, 8)$	$2(5340 + \sqrt{3916})$	$49 + 4\sqrt{11}$
4012	$-2^2, 17, -59$	$(17, 1, 4)$	$2(68 + \sqrt{4012})$	$22 + 5\sqrt{17}$
4017	$-3, 13, -103$	$(13, 2, 3)$	$2(767 + \sqrt{4017})$	$19 + 2\sqrt{13}$
4044	$-2^2, -3, 337$	$(337, 9, 16)$	$2(9436 + \sqrt{4044})$	$23 + 8\sqrt{3}$

- $M_k = k(\sqrt{p})$ $(p|D_k,\ p = x^2 + y^2)$, $\quad H_k = k(\sqrt{\eta(p + x\sqrt{p})}),\ \eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
4045	$5, 809$	$(5, 1, 2)$	$65 + \sqrt{4045}$	$(59 + 7\sqrt{5})/2$
4053	$-3, -7, 193$	$(193, 7, 12)$	$2(965 + \sqrt{4053})$	$(31 + 3\sqrt{21})/2$
4081	$-7, -11, 53$	$(53, 2, 7)$	$2(159 + \sqrt{4081})$	$(19 + 7\sqrt{53})/2$
4168	$2^3, 521$	$(2, 1, 1)$	$2(84 + \sqrt{4168})$	$23 + 2\sqrt{2}$
4173	$-3, 13, -107$	$(13, 2, 3)$	$2(65 + \sqrt{4173})$	$(59 + 13\sqrt{13})/2$
4268	$-2^2, -11, 97$	$(97, 4, 9)$	$1164 + \sqrt{4268}$	$41 + 12\sqrt{11}$
4424	$2^3, -7, -79$	$(2, 1, 1)$	$2(68 + \sqrt{4424})$	$29 + 12\sqrt{2}$
4552	$2^3, 569$	$(2, 1, 1)$	$2(180 + \sqrt{4552})$	$31 + 14\sqrt{2}$
4556	$-2^2, 17, -67$	$(17, 1, 4)$	$2(68 + \sqrt{4556})$	$30 + 7\sqrt{17}$
4616	$2^3, 577$	$(2, 1, 1)$	$2(68 + \sqrt{4616})$	$33 + 16\sqrt{2}$
4632	$-2^3, -3, 193$	$(193, 7, 12)$	$193 + \sqrt{4632}$	$17 + 4\sqrt{6}$
4705	$5, 941$	$(5, 1, 2)$	$175 + \sqrt{4744}$	$31 + 2\sqrt{5}$
4744	$2^3, 593$	$(2, 1, 1)$	$84 + \sqrt{4744}$	$25 + 4\sqrt{2}$

- $M_k = k(\sqrt{p})\ (p|D_k,\ p = x^2 + y^2), \quad H_k = k(\sqrt{\eta(p + x\sqrt{p})}),\ \eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
4777	$17, 281$	$(17, 1, 4)$	$85 + \sqrt{4777}$	$37 + 8\sqrt{17}$
4908	$-2^2, -3, 409$	$(409, 3, 20)$	$2(1636 + 15\sqrt{4908})$	$29 + 12\sqrt{3}$
4953	$-3, 13, -127$	$(13, 2, 3)$	$2(91 + \sqrt{4953})$	$(43 + 5\sqrt{13})/2$
4972	$-2^2, -11, 113$	$(113, 7, 8)$	$2(452 + \sqrt{4972})$	$17 + 4\sqrt{11}$
4981	$17, 293$	$(17, 1, 4)$	$187 + \sqrt{4981}$	$19 + 2\sqrt{17}$
5037	$-3, -23, 73$	$(73, 3, 8)$	$2(949 + \sqrt{5037})$	$(19 + \sqrt{69})/2$
5045	$5, 1009$	$(5, 1, 2)$	$125 + \sqrt{5045}$	$33 + 4\sqrt{5}$
5084	$-2^2, -31, 41$	$(41, 4, 5)$	$328 + \sqrt{5084}$	$20 + 3\sqrt{41}$
5105	$5, 1021$	$(5, 1, 2)$	$95 + \sqrt{5105}$	$39 + 10\sqrt{5}$
5109	$-3, 13, -131$	$(13, 2, 3)$	$2(221 + \sqrt{5109})$	$(47 + 7\sqrt{13})/2$
5181	$-3, -11, 157$	$(157, 6, 11)$	$157 + 2\sqrt{5181}$	$51 + 6\sqrt{33}$
5217	$-3, 37, -47$	$(37, 1, 6)$	$370 + 4\sqrt{5217}$	$(71 + 11\sqrt{37})/2$
5245	$5, 1049$	$(5, 1, 2)$	$105 + \sqrt{5245}$	$37 + 8\sqrt{5}$

- $M_k = k(\sqrt{p})$ $(p|D_k,\ p = x^2 + y^2)$, $\quad H_k = k(\sqrt{\eta(p + x\sqrt{p})}),\ \eta \in k$

D_k	p_i^*	(p, x, y)	η	θ_0
5421	$-3, 13, -139$	$(13, 2, 3)$	$2(689 + \sqrt{5421})$	$25 + 4\sqrt{13}$
5484	$-2^2, -3, 457$	$(457, 4, 21)$	$1828 + 7\sqrt{5484}$	$35 + 16\sqrt{3}$
5545	$5, 1109$	$(5, 1, 2)$	$75 + \sqrt{5545}$	$(71 + 11\sqrt{5})/2$
5548	$-2^2, -19, 73$	$(73, 3, 8)$	$2(6716 + \sqrt{5548})$	$39 + 10\sqrt{5}$
5605	$5, -19, -59$	$(5, 1, 2)$	$85 + \sqrt{5605}$	$49 + 16\sqrt{5}$
5644	$-2^2, 17, 83$	$(17, 1, 4)$	$2(204 + \sqrt{5644})$	$10 + \sqrt{17}$
5704	$2^3, -23, -31$	$(2, 1, 1)$	$2(84 + \sqrt{5704})$	
5768	$2^3, -7, -103$	$(2, 1, 1)$	$2(116 + \sqrt{5768})$	
5809	$37, 157$	$(37, 1, 6)$	$962 + 4\sqrt{5809}$	
5817	$-3, -7, 277$	$(277, 9, 14)$	$3(277 + \sqrt{5817})$	
5848	$-2^3, 17, -43$	$(17, 1, 4)$	$2(255 + \sqrt{5848})$	
5933	$17, 349$	$(17, 1, 4)$	$119 + \sqrt{5933}$	
5973	$-3, -11, 181$	$(181, 9, 10)$	$362 + 4\sqrt{5973}$	

$H_k = k(\sqrt{\theta_0})$, (θ_0 in Yamamura's list)

§5. C_8-Hilbert 類体の生成元の計算 $\leftrightarrow$ $\hat{x}, \hat{y}, \hat{\eta} \in M = \mathbb{Q}(\sqrt{D_k}, \sqrt{p})$

- $^{\exists}!\, M/k:\ M = k(\sqrt{p}) \subset k^*, \quad p = p^* \mid D_k,\ p = x^2 + y^2$
- step 1. $^{\exists}!\, L/k$: 4 次巡回拡大 $\quad k \subset M \subset L$

$$\text{定理 C4} \quad \Rightarrow \quad L = k\left(\sqrt{\eta(p + x\sqrt{p})}\right), \quad {}^{\exists}\eta \in k$$

- step 2 (Main). $\mathrm{Gal}(H_k/M) \cong \mathbb{Z}/4\mathbb{Z}$ $\quad M \subset L \subset H_k$

$$M \ni \eta(p + x\sqrt{p}) =: \delta \overset{!!}{=} \hat{x}^2 + \hat{y}^2, \quad \hat{x}, \hat{y} \in M$$

$$\text{定理 C4} \ \Rightarrow \ H_k = k\left(\sqrt{\hat{\eta}(\delta + \hat{x}\sqrt{\delta})}\right), \quad {}^{\exists}\hat{\eta} \in M = k(\sqrt{p})$$

- step 3. H_k/k : 広義不分岐 8 次拡大 $\Leftrightarrow$ $D_{H_k} = {D_k}^8$

- $C\ell(k) \cong \mathbb{Z}/8\mathbb{Z}$ をみたす実二次体 $k = \mathbb{Q}(\sqrt{D_k})$

$$
\begin{aligned}
&\{D_k \mid C\ell(k) \cong \mathbb{Z}/8\mathbb{Z}, \quad 0 < D_k < 10000\} \\
=&\{904, 1705, 2584, 2605, 2705, 3081, 3196, 3201, \\
&\ 3976, 4161, 4669, 5196, 5249, 5305, 5404, 5513, \\
&\ 5713, 5784, 6757, 6953, 7449, 7833, 8005, 8076, \\
&\ 8105, 8229, 8473, 8536, 8653, 9021, 9305, 9608, \\
&\ 9736, 9953\} \quad \# = 34
\end{aligned}
$$

- $C\ell(k) \cong \mathbb{Z}/8\mathbb{Z}$, $M_k = k(\sqrt{\eta(p + x\sqrt{p})}) \subset H_k$ ： 4 次部分体

D_k	p_i^*	(p, x, y)	η
904	$2^3, 113$	$(2, 1, 1)$	$36 + \sqrt{904}$
1705	$5, -11, -31$	$(5, 1, 2)$	$75 + \sqrt{1705}$
2584	$-2^3, 17, -19$	$(17, 1, 4)$	$153 + \sqrt{2584}$
2605	$5, 521$	$(5, 1, 2)$	$65 + \sqrt{2605}$
2705	$5, 541$	$(5, 1, 2)$	$55 + \sqrt{2705}$
3081	$-3, 13, -79$	$(13, 2, 3)$	$2(91 + \sqrt{3081})$
3196	$-2^2, 17, -47$	$(17, 1, 4)$	$2(138 + \sqrt{3196})$
3201	$-3, -11, 97$	$(97, 4, 9)$	$2(97 + \sqrt{3201})$
3976	$2^3, -7, -71$	$(2, 1, 1)$	$2(68 + \sqrt{3976})$
4161	$-3, -19, 73$	$(73, 3, 8)$	$73 + \sqrt{4161}$
4669	$-7, -23, 29$	$(29, 2, 5)$	$2(1305 + \sqrt{4669})$
5196	$-2^2, -3, 433$	$(433, 12, 17)$	$433 + 6\sqrt{5196}$

- $C\ell(k) \cong \mathbb{Z}/8\mathbb{Z}$, $M_k = k(\sqrt{\eta(p + x\sqrt{p})}) \subset H_k$ ： 4 次部分体

D_k	p_i^*	(p, x, y)	η
5249	$29, 181$	$(29, 2, 5)$	$2(667 + 5\sqrt{5249})$
5305	$5, 1061$	$(5, 1, 2)$	$75 + \sqrt{5305}$
5404	$-2^2, -7, 193$	$(193, 7, 12)$	$386 + 4\sqrt{5404}$
5513	$37, 149$	$(37, 1, 6)$	$407 + 3\sqrt{5513}$
5713	$29, 197$	$(29, 2, 5)$	$2(87 + \sqrt{5713})$
5784	$-2^3, -3, 241$	$(241, 4, 15)$	$2(241 + 3\sqrt{5784})$
6757	$29, 233$	$(29, 2, 5)$	$2(261 + \sqrt{6757})$
6953	$17, 409$	$(17, 1, 4)$	$85 + \sqrt{6953}$
7449	$-3, 13, -19$	$(13, 2, 3)$	$2(91 + \sqrt{7449})$
7833	$-3, -7, 373$	$(373, 7, 18)$	$746 + 4\sqrt{7833}$
8005	$5, 1601$	$(5, 1, 2)$	$450 + 4\sqrt{8005}$
8076	$-2^2, -3, 673$	$(673, 12, 23)$	$673 + 2\sqrt{8076}$

- $C\ell(k) \cong \mathbb{Z}/8\mathbb{Z}$, $M_k = k(k(\sqrt{\eta(p + x\sqrt{p})}) \subset H_k$ ： 4 次部分体

D_k	p_i^*	(p, x, y)	η
8105	$5, 1621$	$(5, 1, 2)$	$115 + \sqrt{8105}$
8229	$-3, 13, -211$	$(13, 2, 3)$	$6(91 + \sqrt{8229})$
8473	$37, 229$	$(37, 1, 6)$	$370 + 4\sqrt{8473}$
8536	$-2^3, -11, 97$	$(97, 4, 9)$	$2(97 + \sqrt{8536})$
8653	$17, 509$	$(17, 1, 4)$	$119 + \sqrt{8653}$
9021	$-3, -31, 97$	$97, 4, 9)$	$6(97 + \sqrt{9021})$
9305	$5, 1861$	$(5, 1, 2)$	$115 + \sqrt{9305}$
9608	$2^3, 1201$	$(2, 1, 1)$	$100 + \sqrt{9608}$
9736	$2^3, 1217$	$(2, 1, 1)$	$2(132 + \sqrt{9736})$
9953	$37, 269$	$(37, 1, 6)$	$111 + \sqrt{9953}$