

2 次体の 2-類群構造の有向グラフ化について

河野 美文*) 中原 徹**)

*(Kohno Yoshifumi) **)(Nakahara Toru)

*)佐賀大学工学系研究科 **)佐賀大学理工学部

§ 1 Introduction

2 次体の狭義イデアル類群の構造, 特に, その 2-part については Gauss 以来多くのアプローチがなされている. 4-rank の決定については, Rédei-reichardt[R-R] の定理が, よく知られている. また, そのグラフ版も Lagarias[L] によって導入され, グラフのタイプによる 4-rank の決定やグラフ上の ζ 関数を用いた 4-rank の有無の判定などが, なされている.([O],[K-K-N])

8-rank についての研究は, Rédei ([R1][R2]) にはじまり, 彼は, 任意の 3 整数 (a, b, c) $a \geq b \geq c \geq 0$ に対して 2-rank = a , 4-rank = b , 8-rank = c となる無限個の実 2 次体の存在を示した. 2-rank = 1 の場合, 即ちイデアル類群の 2-part が, 巡回群となる場合は, 8-rank の判定を与える多くの結果があるが, それらはすべてある Diophantine 方程式の解 という形で与えられている.

§§2-3 においては, P.Morton ([M2],[M3],[M4],[M5],[M6]) P.Stevenhagen ([St1],[St2]) による次の Conjecture に対する応答及びそのグラフ化の試みについて述べる. §4 で我々の例を与える. P.Morton の結果については, [K] に詳述されている.

Conjecture (Cohn-Lagarias [C-L])

d を $d \not\equiv 2 \pmod{4}$ である任意の整数とし, w を 2 巾の自然数とする. このとき, 有理数体上のある正規拡大 M/Q が存在して, d を割らない奇素数 p で $dp \equiv 0, 1 \pmod{4}$ なるものに対して次の性質が成り立つ. 即ち,

$Q\sqrt{dp}$ のイデアル類群 $C(dp)$ の 2-part の w -rank が M/Q における p の Frobenius class のみによって決定される.

Remark 1-1

ここで Frobenius class は, M/Q のガロア群 $Gal(M/Q)$ のある共役類 $\{\tau\sigma\tau^{-1}; \tau \in Gal(M/Q)\}$ であり, その元 σ は次の性質を満たす:

$$\forall x \in M \text{ に対し, } x^\sigma \equiv x^p \pmod{\mathcal{P}}, \quad p \in \mathcal{P}: M \text{ の素イデアル.}$$

Definition 1-1 ([C-L])

$D \not\equiv 2 \pmod{4}$ である任意の整数 d と, 2 巾の自然数 $w = 2^j$ に対して, 有理数体上の正規拡大 M/Q が存在して, d を割らない奇素数 p で $dp \equiv 0, 1 \pmod{4}$ なるものに対して, Conjecture がなりたつとき, その中の最小の体 M を Governing-field (支配体) と呼び $\Omega_j(d)$ と表す.

§ 2 Governing-field と 有向グラフ (1)

Rédei は 2 次体 $Q(\sqrt{d})$ に於ける 2 類群の 4-rank, 8-rank を d -分解と 2 次の乗法的記号 $\{a_1, a_2, a_3\}$ ('条件付きアルティン記号' と呼ばれる) によって特徴付けた. この記号は Q の 8 次拡大に於ける素数の分解に密接に関係している.

そこで, 我々は以下のような 2 次体 $\Omega = Q(\sqrt{-dq})$ に於けるイデアル類群 \mathcal{C} に対して $\mathcal{C}/\mathcal{C}^8$ の構造を考える. 後に同様の議論が実 2 次体 $Q(\sqrt{dq})$ においてもできることに触れる.

$$(2.1) \quad d = p_1 \dots p_r$$

$$(2.2) \quad p_i \equiv 1 \pmod{4}, \quad \left(\frac{p_i}{p_j}\right) = +1 \text{ for } i \neq j$$

$$(2.3) \quad q \equiv 3 \pmod{4}$$

次の定理がこの節の目標である.

Theorem (Morton)

虚 2 次体 $Q(\sqrt{-dq})$ に対して $\exists \Sigma_d/Q$ s.t.

$$\left(\frac{\Sigma_d/Q}{q}\right) : \text{Artin 記号}$$

によって $\mathcal{C}/\mathcal{C}^8$ の構造が決定される. ここで Σ_d は拡大次数 $2^{\binom{r}{2}+2r}$ 次のガロア拡大で d のみによって決まる.

ここで, 与えられた 2 次体の類群の 8-rank までの構造

$$G = \mathcal{C}/\mathcal{C}^8$$

を計算する為に必要ないくつかの Lemmas を用意する. Rédei のアルゴリズムである.

Lemma 2-1

$$\begin{array}{ll} G: & \text{有限アーベル群} \\ \chi_1, \dots, \chi_r: & X_2 \text{ の基底} \quad (X_2; G \text{ 上の 2 次指標の全体}) \\ a_1, \dots, a_r: & A_1 \text{ の基底} \quad (A_1; G \text{ の位数 2 の元の全体}) \end{array}$$

⇒

$$G \text{ の 4-rank } e_4 = s.$$

ここで, s は行列 $M = (\xi \chi_j(a_i))$ ($1 \leq i, j \leq r$)

$$\xi : \{\pm 1\} \longrightarrow \mathbf{F}_2 \quad (\xi(1) = 0, \xi(-1) = 1)$$

に対し $s = r - \text{rank} M$ で決める.

Lemma 2-2

$M = (\xi\chi_j(a_i))$ ($1 \leq i, j \leq r, a_i \in A_1$) に対して,

$$M = \begin{pmatrix} 0 & 0 \\ 0 & I \end{pmatrix}$$

と変形出来、 $I = (r-s) \times (r-s)$ 単位行列とするならば、 χ_1, \dots, χ_s は G の指標群 X において平方根をもつ全ての元の集合の生成系となる. そのとき,

$$e_s = s - \rho : G \text{ の } s\text{-rank}$$

ここで $b_i^2 = a_i$ ($1 \leq i, j \leq s$) を用いて ρ は $M' = (\xi\chi_j(b_i))$ の rank とする.

Lemma 2-3

$\Omega = \mathbf{Q}(\sqrt{\Delta})$, Δ は判別式 とすると, Ω における狭義イデアル類群 \mathcal{C} の 2 次指標群 X_2 は次のようになる.

$$X_2 = \langle \chi_{p_1}, \dots, \chi_{p_{t-1}} \rangle, \chi_{p_i}(\mathcal{A}) = \left(\frac{N\mathcal{A}, \Delta}{p_i} \right), (p_i | \Delta)$$

ここで $t = \#\{p; p | \Delta\}$, \mathcal{A} は Ω における任意の分数イデアル, $\left(\frac{a, b}{p} \right)$ は ヒルベルト記号. 更にいわゆる '積公式'

$$\prod_{p_i | \Delta} \chi_{p_i}(\mathcal{A}) = 1$$

が成り立ち, \mathcal{C} の 2-rank = $t - 1$ である.

Remark 2-1

$a, b \in \mathbf{Z}$ ($a \neq 0, b \neq 0$), p を素数とする. b が平方数であれば $\left(\frac{a, b}{p} \right) = +1$, b が平方数でなければ $\left(\frac{a, b}{p} \right) = \pm 1$ で, $+1$ となるのは a が任意の p^e ($e = 1, 2, \dots$) を法として 2 次体 $k = \mathbf{Q}(\sqrt{b})$ の或る整数 β_e の ノルムと合同であること:

$$a \equiv N_{k/\mathbf{Q}} \beta_e \pmod{p^e} \quad (e = 1, 2, \dots)$$

と定める. その他の場合には, -1 とする.

Lemma 2-4 各 $p_i | \Delta$ に対して, $\mathfrak{P}_i : \Omega$ の素イデアル, s.t.

$$\mathfrak{P}_i^2 = (p_i)$$

となるが, A_1 を, 2 乗して単項イデアルとなるイデアルの類よりなる群とすると,

$$A_1 = \langle \mathfrak{P}_1, \dots, \mathfrak{P}_t \rangle, \prod_{p_i | \Delta} \mathfrak{P}_i^{\varepsilon_{p_i}} \sim 1, \quad \varepsilon_{p_i} = 0 \text{ or } 1.$$

但し, 同値関係 ' \sim ' は, 次のように定義される:

$$A \sim B \iff \exists \alpha \in \Omega, \text{ s.t. } A = (\alpha)B, N\alpha > 0, A, B \text{ は } \Omega \text{ のイデアル.}$$

Lemma 2-5

$$A = \prod_{p_i | \Delta} \mathcal{P}_i^{r_{p_i}}, \quad r_{p_i} = 0 \text{ or } 1.$$

但し, 全ての $r_{p_i} = 0$ ではないとする.

また, A が あるイデアルの平方となり, $a = NA$, 更に (x, y, z) は次式の原始解とする.

$$x^2 - \Delta y^2 - 4az^2 = 0$$

\Rightarrow

$$\exists B^2 \sim A, \text{ s.t. } NB = z$$

Lemma 2-6

$$d \equiv 1 \pmod{4}, \gamma = \frac{x + y\sqrt{d}}{2} \text{ は } Q(\sqrt{d}) \text{ の 整数, } (\gamma, 2) = 1$$

\Rightarrow

$$\gamma^3 = u + v\sqrt{d}, \quad u, v \in Z$$

以上は, Rédei のアルゴリズムを 2 次体 $\Omega = Q(\sqrt{\Delta})$ の狭義イデアル類群 C^+ に適用したものである. ここから, 判別式 $\Delta = -qd$ の場合を考察する. 但し, d, q は, 次の条件を満たすとする.

$$(2.1) \quad d = p_1 \dots p_r$$

$$(2.2) \quad p_i \equiv 1 \pmod{4}, \quad \left(\frac{p_i}{p_j}\right) = +1 \text{ for } i \neq j$$

$$(2.3) \quad q \equiv 3 \pmod{4}$$

まず, Lemma 2-3 より $e_2 = r$, また Lemma 2-1, 3 より $e_4 = s$, 但し

$$s = \#\{p_i; \left(\frac{q}{p_i}\right) = +1\}$$

更に, $e_8 = s - \rho$ 但し,

$$\rho = \text{rank } M', \quad M' = (\xi \chi_j(Z_i)), \quad (1 \leq i, j \leq s)$$

ここで, $Z_i^2 \sim \mathcal{P}_i, (1 \leq i \leq s)$.

次いで、以下の Lemmas により $\chi_j(\mathcal{Z}_i)$ ($1 \leq i \leq s$) の 4 乗剰余記号 $\left(\frac{a}{p}\right)_4$ を用いた表現を与える。但し 4 乗剰余記号は $p \equiv 1 \pmod{4}$ なる素数 p と法 p の平方剰余 a に対しては

$$\left(\frac{a}{p}\right)_4 \equiv a^{\frac{p-1}{4}} \pmod{p}$$

と定義され、 $\left(\frac{a}{p}\right)_4 = 1$ (a : 法 p の 4 乗剰余), または, $= -1$ (a : 法 p のその他の平方剰余) となる。

Lemma 2-7 次が成り立つ:

$$\chi_i(\mathcal{Z}_i) = \left(\frac{d/p_i}{p_i}\right)_4 \cdot \left(\frac{-q}{p_i}\right)_4 \quad (1 \leq i \leq s).$$

(pf)

Lemma 2-3,5 より $\chi_i(\mathcal{Z}_i) = \left(\frac{z}{p_i}\right)$ であり, (x, y, z) は, 次式の $z > 0$ なる原始解である。

$$x^2 + dqy^2 - 4p_i z^2 = 0$$

Lemma 2-6 を用い, Lemma の式は得られる。

Lemma 2-8

$\mathcal{R}_{ij}, \mathcal{D}_{ij}, \mathcal{Q}_{ij}$ を $Q(\sqrt{p_i p_j})$ における次式を満たす整イデアルとする, 但し ($1 \leq i, j \leq s$).

$$\mathcal{D}_{ij} \mathcal{D}'_{ij} = \frac{d}{p_i p_j}, \quad \mathcal{Q}_{ij} \mathcal{Q}'_{ij} = q, \quad \mathcal{D}_{ij} \mathcal{Q}_{ij} \mathcal{R}_{ij}^2 \sim 1 \quad (Q(\sqrt{p_i p_j}) \text{ において})$$

ここで, $(\mathcal{R}_{ij}, 2Dq\mathcal{R}'_{ij}) = 1$ である。このとき

$$\begin{aligned} \chi_j(\mathcal{Z}_i) &= \left(\frac{p_i}{p_j}\right)_4 \cdot \left(\frac{r_{ij}}{p_j}\right) \quad (r_{ij} = N\mathcal{R}_{ij}) \\ &= \left(\frac{p_i}{p_j}\right)_4 \cdot \left(\frac{p_j}{p_i}\right)_4 \cdot \chi_i(\mathcal{Z}_j) \quad (i \neq j) \end{aligned}$$

(pf)

Lemma 2-7 と同様。

以下の Lemmas によって, $\chi_j(\mathcal{Z}_i)$ の値が, Q 上の適当な Galois 拡大における q の分解のみによることを示す。

Lemma 2-9

$$H_i = \{r \in Q; (r, 4p_i) = 1, \left(\frac{r}{p_i}\right) = \left(\frac{r^*}{p_i}\right)_4 = 1\}$$

$r^* = rv(r)$, $v(\neq 1)$: modulo 4 の指標

K_i : H_i に対応する Q 上のアーベル拡大, 即ち mod H_i の ray class field.

$\sigma_i(\neq 1) \in \text{Gal}(K_i/Q(\sqrt{p_i}))$. ($1 \leq i \leq s$)

⇒

$\chi_i(\mathcal{Z}_i)$ は Artin symbol $\left(\frac{K_i}{q}\right)$ のみによって決まる. 特に

$$\chi_i(\mathcal{Z}_i) = \left(\frac{d/p_i}{p_i}\right)_4 \cdot (-1)^{a_i}, \text{ ここで } \left(\frac{K_i}{q}\right) = \sigma_i^{a_i}, a_i = 0 \text{ or } 1.$$

Lemma 2-10

$L_{ij} : \mathbf{Q}(\sqrt{p_i p_j})$ の種の体 $\mathbf{Q}(\sqrt{p_i}, \sqrt{p_j})$ の 2 次拡大

$\lambda_{ij} (\neq 1) \in \text{Gal}(L_{ij}/\mathbf{Q}(\sqrt{p_i}, \sqrt{p_j}))$

$\delta_{ij} \in \text{Gal}(L_{ij}/\mathbf{Q}(\sqrt{p_i p_j}))$

$$\delta_{ij} := \left(\frac{L_{ij}/\mathbf{Q}(\sqrt{p_i p_j})}{\mathcal{D}_{ij}}\right) : \text{Artin 記号}$$

$\delta_{ij} = 1$ or λ_{ij} . ($1 \leq i, j \leq s$, $i \neq j$)

⇒

$$\chi_j(\mathcal{Z}_i) = \left(\frac{p_i}{p_j}\right)_4 \cdot (-1)^{b_{ij}}.$$

ここで $\left(\frac{L_{ij}/\mathbf{Q}(\sqrt{p_i p_j})}{\mathcal{D}_{ij}}\right) = \delta_{ij} \cdot \lambda_{ij}^{b_{ij}}$, $b_{ij} = 0$ or 1 .

Lemma 2-11

$h_i : \mathbf{Q}(\sqrt{p_i})$ の類数

$\mathcal{P}_{ij} : \mathbf{Q}(\sqrt{p_i})$ における p_j 上の素イデアル

$$\mathcal{P}_{ij}^{3h_i} = (\beta_{ij}), \beta_{ij} = x + y\sqrt{p_i}, N\beta_{ij} = p_j^{3h_i} > 0$$

($1 \leq i, j \leq s$)

$$x \equiv \begin{cases} +1 \pmod{4} & \text{if } y \equiv 0 \pmod{4} \\ -1 \pmod{4} & \text{if } y \equiv 2 \pmod{4} \end{cases}$$

⇒

$$L_{ij} = \mathbf{Q}(\sqrt{p_i p_j}, \sqrt{\beta_{ij}}).$$

Definition 2-1

ここで, 以下のように記号を定める.

$$K_{d^+} = K_i \text{ の合成体, } (1 \leq i \leq s)$$

$$\Lambda_{d^+} = L_{ij} \text{ の合成体, } (1 \leq i \leq s)$$

$$\Omega_{d^+} = Q(\sqrt{p_1}, \dots, \sqrt{p_s}), \Sigma_{d^+} = K_{d^+} \Lambda_{d^+}.$$

上記の各体は, 全て d の因子 d^+ のみによって定まり, q には依らない.

また,

$$\Sigma_{d^+} \subseteq \Sigma_d,$$

であり, $K_{d^+}, \Lambda_{d^+}, \Omega_{d^+}$ についても同様である. 更に, Lemma 5-9, 10 より 全て Q 上 ガロア 拡大となる.

Theorem 2-1 (Morton [M2])

d, q は, (2.1), (2.2), (2.3) を満たすとする. また C は $Q(\sqrt{-dq})$ の類群とする.

\Rightarrow

C/C^8 は下の Artin 記号によって完全に決定される.

$$\left(\frac{\Sigma_d/Q}{q} \right), (\Sigma_{d^+} \subseteq \Sigma_d)$$

ここで, Artin 記号の性質より以下のように表せる.

$$\left(\frac{\Sigma_d/Q}{q} \right) = \begin{cases} \left(\frac{\Omega_d/Q}{q} \right) & \text{on } \Omega_d \\ \left(\frac{K_i}{q} \right) & \text{on } K_i, 1 \leq i \leq s, \\ \left(\frac{L_{ij}/Q}{q} \right) & \text{on } L_{ij}, 1 \leq i < j \leq s \end{cases}$$

最後に, Q_{ij} が $Q(\sqrt{p_i p_j})$ における q の素因子イデアルとすると

$$\left(\frac{L_{ij}/Q}{q} \right) = \left(\frac{L_{ij}/Q(\sqrt{p_i p_j})}{Q_{ij}} \right).$$

以上のように C/C^8 の構造は governing field Σ_d における q の分解のみによっている事がわかった. また C/C^8 が, 与えられた構造を有するときの $q \equiv 3 \pmod{4}$ の存在の仕方は フロベニウスの密度定理によって計算可能で, Morton は次の結果も得ている.

Definition 2-2 2次体 $Q(\sqrt{-dq})$ において $d'|d, d' = p_1 \cdots p_s$ に対して以下のような記号を定義する.

$$N(d, \rho) := \#\{R = (\varepsilon_{ij}); \text{rank } R = \rho, (-1)^{\varepsilon_{ij} + \varepsilon_{ji}} = \left(\frac{p_i}{p_j} \right)_4 \left(\frac{p_j}{p_i} \right)_4, 1 \leq i, j \leq s, i \neq j\}$$

$$N(1, 0) = 1$$

Theorem 2-2 (Morton [M2]) d, q は, (2.1), (2.2), (2.3) を満たすとする. C は $Q(\sqrt{-dq})$ の類群とし, $0 \leq \rho \leq s \leq r$ に対して, 下の事が成り立っているとする.

$$C/C^8 \cong C_2^{(r-s)} \times C_4^{(\rho)} \times C_8^{(s-\rho)}$$

但し, $C_n^{(m)}$ は, 位数 n の巡回群 m 個の積を表す.

$$\Rightarrow \partial(d, s, \rho) = 2^{-\binom{r}{s} - r - s - 1} \sum_{\substack{d'|d \\ \nu(d')=s}} N(d', \rho)$$

但し, $\nu(d')$ は d' の素因数の数を表す. また $\partial(*)$ は密度を表す.

同様のことが, 実 2 次体 $Q(\sqrt{dq})$,

$$(2.4) \quad d = p_1 \dots p_r$$

$$(2.5) \quad p_i \equiv 1 \pmod{8}, \quad \left(\frac{p_i}{p_j}\right) = +1 \text{ for } i \neq j$$

$$(2.6) \quad q \equiv 1 \pmod{4}$$

に対しても成り立つ事が Morton [M4] によって示されている. 更に, 実 2 次体においては単数のノルムと狭義イデアル類群の 2-part の構造とが密接に関係していることが指摘されている. 即ち, Rédei は [R1] において次のことを示している.

$$\text{Norm } \eta_q = -1 \iff C_q; \{2, \dots, 2\} \text{ 型アーベル群}$$

但し, η_q は $Q(\sqrt{dq})$ の単数, C_q は $Q(\sqrt{dq})$ のイデアル類群の 2-part である. Morton はこの結果を更に押し進めた. 以下の定理である.

Theorem 2-3 (Morton [M4])

d, q は, (2.4), (2.5), (2.6) を満たしているとする. このとき

$$T: 2\text{-rank} = r \text{ の有限アーベル 2 群}$$

とする. 但し, T の 8-rank 以上はないとする. また $\varepsilon = \pm 1$ を表す.

\Rightarrow

$$\partial(\{q: \text{素数}; C_q \cong T, \text{Norm } \eta_q = \varepsilon\}) > 0$$

上の定理は, 一般にイデアル類群の 2-part C_q のみでは η_q の符号が決まらないことも示している.

§ 3 Governing-field と 有向グラフ (2)

p, q_1, q_2 は素数とする. P.Morton [M5] は, 次の 2 次体

$$\mathbb{Q}(\sqrt{-q_1 q_2 p}) \quad (p \equiv q_1 \equiv q_2 \equiv 3 \pmod{4})$$

の 2 イdeal 類群の 8-rank までの governing-field を決定し, 有向グラフを用いた reciprocity theorem を与えた. まず初めに, [C-L] においてなされた予想について述べ governing field の明確な定義を述べる.

Conjecture $C_j(d)$ ([C-L])

$d (\not\equiv 2 \pmod{4}) \in \mathbb{Z}$ に対し次のような体 K が存在する.

$K = K_j(d) : \text{Galois}/\mathbb{Q}$ であり次の条件 $P_j(d)$ を満たす ($j \in \mathbb{N}$)

$P_j(d) : \begin{cases} \text{もし } p_1, p_2 : \text{素数}, (d, p_i) = 1 \\ \text{s.t. } [(K/\mathbb{Q})/(p_1)] = [(K/\mathbb{Q})/(p_2)] \\ \implies \\ C_2(dp_1), C_2(dp_2) : 2^k\text{-rank が等しい } (1 \leq k \leq j) \end{cases}$

但し, $[(K/\mathbb{Q})/(p_i)] : \text{Frobenius class}$
 i.e. $[(K/\mathbb{Q})/(p_i)] = \bigcup_{\sigma \in \text{Gal}(K/\mathbb{Q})} \{ \sigma \in \text{Gal}(K/\mathbb{Q}) ; x^\sigma \equiv x^{p_i} \pmod{P_i} \text{ for } \forall x \in \mathcal{O}_K \}$
 $C_2(dp_i) : \mathbb{Q}(\sqrt{dp_i})$ のイdeal 類群における 2-sylow 部分群

$j = 3$ のときは, 2-類群が巡回群となる全ての d に対して, また先に触れたように,

$$d = -p_1 p_2 \dots p_k, \quad p_i \equiv 1 \pmod{4}, \quad \left(\frac{p_i}{p_j} \right) = 1, (i \neq j)$$

$$d = p_1 p_2 \dots p_k, \quad p_i \equiv 1 \pmod{8}, \quad \left(\frac{p_i}{p_j} \right) = 1, (i \neq j)$$

となるときは Morton ([M2], [M3], [M4]) によって具体的に拡大体を構成することによって証明された. また, 任意の $d (\not\equiv 2 \pmod{4})$ に対しては, $j = 3$ のとき Steinhagen ([St1], [St2]) によって存在証明が与えられた. 彼は Morton の idea を用いて一般化された類体論, 即ちイdeal 類を用いた類体論によって証明した. 以下の定理である.

Theorem 3-1 ([St1])

d を $d \not\equiv 2 \pmod{4}$ なる任意の $0, \pm 1$ でない整数とする. そのとき体 K を次のように定義する.

$$K = \mathbb{Q}(\sqrt{q} : q \text{ は } q|d \text{ なる素判別式すべてをわたる}).$$

そのとき, $Dp \equiv 0, 1 \pmod{4}$, なる素数 p に対して 2 次体 $\mathbb{Q}(\sqrt{dp})$ の狭義イdeal 類群 $\mathcal{C}(dp)$ のなす商群 $\mathcal{C}(dp)/\mathcal{C}(dp)^8$ の構造は次のように決定される. 即ち, それは K の最大アーベル拡大体における p の Frobenius class のみによって決定される. その体は K 上 $2d \cdot \infty$ 以外では不分岐で K 上 exponent 2 のガロア群をもつ.

したがって, 以下の議論において 8-rank の Governing field の存在は保証されている.

最小の $K_j(d)$ の存在は次の定理によって与えられる.

Theorem 3-2 ([C-L])

各 j (固定) に対して $\exists K_j^{(\lambda)}(d), \lambda \in \Lambda$ (: 適当な添数集合); Galois/ \mathbb{Q} , s.t. $P_j(d)$ を満たす.

\Rightarrow

$\Omega_j(d) = \bigcap_{\lambda \in \Lambda} K_j^{(\lambda)}(d); \text{Galois}/\mathbb{Q}, P_j(d)$ を満たす最小の体.

Definition 3-1 $\Omega_j(d)$ のことを governing field と呼ぶ.

[C-L] においては, 任意に与えられた有限アーベル 2-群 G と同型な 2-類群の存在密度についても予想が与えられている.

Density Conjecture $D_j(d)$ ([C-L])

$$d (\not\equiv 2 \pmod{4}) \in \mathbb{Z}$$

$$G = \prod_{i \in I} G_i : \text{アーベル 2-群}$$

$$G_i : \#G_i \leq 2^{j-1} (j \in \mathbb{N}) \text{ となる巡回群}$$

\Rightarrow

$$\Sigma_j(d, G) = \{(p); C_2(dp) \cong G\} : \text{有理数値の存在密度をもつ.}$$

ここに 密度は $\#\{(p); C_2(dp) \cong G\} / \#\{p; dp \text{ 2次体の判別式}\}$ で与えられる. そして, 最後に $\Omega_3(21)$ について次の予想を与えた. 後で述べるようにこの予想は Morton ([M5]) によって更に一般化された形で証明された.

Conjecture 3-1 (Cohn-Lagarias) (Theorem 2-5 に含まれる.)

$p \equiv 3 \pmod{4}$ と仮定すると

$$\mathcal{C}(-21p) / \mathcal{C}(-21p)^8 \cong \mathbb{Z}_8 \times \mathbb{Z}_2$$

と成るための必要十分条件は以下の (A), (B) または (C) が成立するときである.

$$\left\{ \begin{array}{l} (A) \left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = +1, \quad p : K_A = \mathbb{Q} \left(\sqrt{-3}, \sqrt{-7}, \sqrt{-2(3+\sqrt{21})} \right) \text{ で完全分解} \\ (B) \left(\frac{p}{3}\right) = +1, \left(\frac{p}{7}\right) = -1, \quad p : K_B = \mathbb{Q} \left(\sqrt{-3}, \sqrt{7}, \sqrt{1+2\sqrt{7}} \right) \text{ で完全分解} \\ (C) \left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = -1, \quad p : K_C = \mathbb{Q} \left(\sqrt{3}, \sqrt{7}, \sqrt{2(7+\sqrt{21})} \right) \text{ で完全分解} \end{array} \right.$$

以下ではこの節の目的である Morton ([M5]) により与えられた諸定理を述べる. 特に判別式が 3 素因数からなる場合に reciprocity theorem とそのグラフ化を示す.

Theorem 3-3 (Morton [M5])

$p \equiv q_1 \equiv q_2 \equiv 3 \pmod{4}, \left(\frac{q_2}{q_1}\right) = +1$ と仮定すると

$$\mathcal{C}(-q_1 q_2 p) / \mathcal{C}(-q_1 q_2 p)^8 \cong \mathbb{Z}_8 \times \mathbb{Z}_2$$

と成るための必要十分条件は以下の (A), (B) または (C) が成立するときである.

$$\left\{ \begin{array}{l} (A) \left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = +1, \\ (B) \left(\frac{p}{q_1}\right) = +1, \left(\frac{p}{q_2}\right) = -1, \\ (C) \left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1, \end{array} \right. \begin{array}{l} p: K_A(q_1, q_2) \text{ で完全分解} \\ p: K_B(q_1, q_2) \text{ で完全分解} \\ p: K_C(q_1, q_2) \text{ で完全分解} \end{array}$$

ここで, K_A, K_B, K_C は次の体である.

$$\begin{aligned} K_A(q_1, q_2) &= \mathbf{Q} \left(\sqrt{-q_1}, \sqrt{-q_2}, \sqrt{\pi_{12}} \right) \\ K_B(q_1, q_2) &= \mathbf{Q} \left(\sqrt{-q_1}, \sqrt{q_2}, \sqrt{\pi_1} \right) \\ K_C(q_1, q_2) &= \mathbf{Q} \left(\sqrt{q_1}, \sqrt{q_2}, \sqrt{-\varepsilon_2 \sqrt{q_2} \pi_1} \right) \end{aligned} \quad (3.1)$$

更に $\pi_{12}, \pi_1, \varepsilon_2$ は, 次のように定められる. N は k_*/\mathbf{Q} のノルムとする.

$$\left\{ \begin{array}{l} N_{k_{12}/\mathbf{Q}} \pi_{12} = -q_1 \quad (k_{12} = \mathbf{Q}(\sqrt{q_1 q_2})) \\ \pi_{12} \equiv \left(\frac{2}{q_1}\right) \pmod{4} \\ N_{k_2/\mathbf{Q}} \pi_1 = -q_1^{h_2} \quad (k_2 = \mathbf{Q}(\sqrt{q_2})) \\ h_2 = k_2 \text{ の類数} \\ \pi_1 \equiv 1 \pmod{2} \\ \pi_1 < 0, (\sqrt{q_2} > 0 \text{ に対し}), (\pi_1, 1 - a\sqrt{q_2}) \neq 1, a^2 q_2 - b^2 q_1 = 1, \left(\frac{q_2}{q_1}\right) = +1. \\ \varepsilon_2 > 1: k_2 \text{ の基本単数} \end{array} \right.$$

もし, $\left(\frac{p}{q_1}\right) = -1, \left(\frac{p}{q_2}\right) = +1$ と仮定すると,

$$\mathcal{C}(-q_1 q_2 p) / \mathcal{C}(-q_1 q_2 p)^8 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$$

また, もし (A) から (C) の Legendre 記号条件のうちの一つが満たされるが, p が対応する体において分解しないならば

$$\mathcal{C}(-q_1 q_2 p) / \mathcal{C}(-q_1 q_2 p)^8 \cong \mathbf{Z}_2 \times \mathbf{Z}_4$$

以上の結果と拡大次数に関する考察を併せて $K = K_A K_B K_C$ が $\mathcal{C}(-q_1 q_2 p) / \mathcal{C}(-q_1 q_2 p)^8$ の構造を決定する governing field $\Omega_3(-q_1 q_2)$ となることが示される. 即ち次の定理である.

Theorem 3-4 (Morton [M5])

$K = K_A K_B K_C$, 但し,

$$\begin{aligned} K_A(q_1, q_2) &= \mathcal{Q}\left(\sqrt{-q_1}, \sqrt{-q_2}, \sqrt{\pi_{12}}\right), \\ K_B(q_1, q_2) &= \mathcal{Q}\left(\sqrt{-q_1}, \sqrt{q_2}, \sqrt{\pi_1}\right), \\ K_C(q_1, q_2) &= \mathcal{Q}\left(\sqrt{q_1}, \sqrt{q_2}, \sqrt{-\varepsilon_2 \sqrt{q_2} \pi_1}\right) \end{aligned}$$

のように Theorem 3-2 と同様に定める. そうすると K は $\mathcal{Q}(\sqrt{-1})$ を含み $\mathcal{C}(-q_1 q_2 p) / \mathcal{C}(-q_1 q_2 p)^8$ の構造を決定する \mathcal{Q} 上最小な Galois 拡大体であることがわかる.

$$\text{i.e. } \Omega_3(-q_1 q_2) = K = K_A K_B K_C$$

である.

最後に 3 素数 q_1, q_2, p は全て法 4 で 3 と合同なので, p を q_3 で置き換えると $\mathcal{Q}(\sqrt{-q_1 q_2 q_3})$ は q_1, q_2, q_3 について対称に扱える. 従って, 以下のように有向グラフを定義すると Theorem 7-2 はグラフ表現され, ある種の相互法則を与える.

Definition 3-2 (Morton [M5])

$q_i \equiv 3 \pmod{4}$, ($i = 1, 2, 3$) に対して

$$\left(\frac{q_1}{q_3}\right) = +1, \left(\frac{q_3}{q_2}\right) = +1, \left(\frac{q_2}{q_1}\right) = +1 \quad (3.2)$$

となるとき quadratic cyclic triple といい, そのようになる順序がないとき noncyclic という.

Definition 3-3 (Morton [M5])

頂点集合 $\{q_1, q_2, q_3\}$ からなる有向グラフ G の有向辺を以下のように定義する:

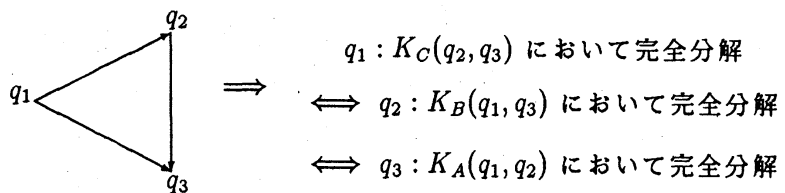
グラフ G の有向辺 (q_i, q_j) (q_i から q_j) は $\left(\frac{q_j}{q_i}\right) = +1$ という条件によって定められる.

Proposition 3-1 (Morton [M5])

(q_1, q_2, q_3) が cyclic (resp. noncyclic) のとき, またそのときのみグラフ G が cyclic (resp. noncyclic) である.

Theorem 3-5 (reciprocity theorem) (Morton [M5])

(q_1, q_2, q_3) : non-cyclic triple, $q_i \equiv 3 \pmod{4}$, ($i = 1, 2, 3$) に対して次のような有向グラフが対応しているとする.



ここで, K_A, K_B, K_C は (3.1) 式で定められたものである.

Remark 3-1

theorem3-2 より

$$C(-q_1q_2q_3)/C(-q_1q_2q_3)^8 \cong \mathbf{Z}_8 \times \mathbf{Z}_2$$

となる.

Remark 3-2

(q_1, q_2, q_3) が cyclic のとき

$$C(-q_1q_2q_3)/C(-q_1q_2q_3)^8 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$$

となる.

§ 4 Examples

ここでは, 前節で示された P.Morton の結果を基にして素数 p, q_j ($1 \leq j \leq 3$) に対し, 次の 2 次体

$$Q(\sqrt{-q_1q_2q_3p}) \quad (p \equiv 1 \pmod{4}, q_i \equiv 3 \pmod{4})$$

のイデアル類群の 2-part の 8-rank に対する Governing-field を探り, いくつかの実験例を与える.

Case 4-1

$$\left(\frac{q_2}{q_1}\right) = \left(\frac{q_3}{q_2}\right) = \left(\frac{q_1}{q_3}\right) = +1, \left(\frac{p}{q_j}\right) = +1, \quad (1 \leq j \leq 3) \quad (4.1)$$

のとき,

$$M = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -1 & -1 \\ -1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}, M' = \left(\begin{array}{cc|c} -1 & 1 & 1 \\ 1 & -1 & 1 \\ \hline 1 & 1 & 1 \\ 1 & 1 & 1 \end{array} \right).$$

したがって, $e_4 = 1$ となり

$$e_8 = 1 \iff \chi_1\chi_2\chi_3(\mathcal{Z}) = +1, (\mathcal{Z}^2 \sim \mathcal{P}, \mathcal{P} \text{ は } p \text{ 上の素イデアル})$$

χ_i の定義 及び Lemma 2-1 より

$$\chi_1\chi_2\chi_3(\mathcal{Z}) = \left(\frac{z}{q_1}\right) \left(\frac{z}{q_2}\right) \left(\frac{z}{q_3}\right).$$

ここで, (x, y, z) は 次の不定方程式の正の原始解である.

$$x^2 + q_1q_2q_3py^2 - 4pz^2 = 0$$

Example 4-1

$q_1 = 3, q_2 = 7, q_3 = 11$ とすると, これらは (4.1) 式の条件を満たす. $p_1 = 421, p_2 = 2269,$
 $p_3 = 2731, p_4 = 8737$ に対して, C_j 及び h_{k_j} をそれぞれ 2 次体 $k_j = Q(-3 \cdot 7 \cdot 11 \cdot p_j)$ の類群
 及び 類数とすると

$$\begin{aligned} h_{k_1} = 64 = 2 \times 2 \times 16, & \text{ i.e. } C_1 \cong Z_{16} \times Z_2 \times Z_2. \\ h_{k_2} = 192 \equiv 0 \pmod{2^6}, & \text{ i.e. } C_2 \cong Z_{48} \times Z_2 \times Z_2. \\ h_{k_3} = 768 \equiv 0 \pmod{2^8}, & \text{ i.e. } C_3 \cong Z_{32} \times Z_2 \times Z_2 \times Z_2. \\ & \text{ or } C_3 \cong Z_{16} \times Z_4 \times Z_2 \times Z_2. \\ & \text{ or } C_3 \cong Z_8 \times Z_8 \times Z_2 \times Z_2. \\ h_{k_4} = 928 \equiv 0 \pmod{2^5}, & \text{ i.e. } C_4 \cong Z_8 \times Z_2 \times Z_2. \end{aligned}$$

となる.

References

- [B-C] P. Barrcand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number and residuacity*, J. reine Angew. Math. **238** (1969), 67-70.
- [C-L] H. Cohn and J. C. Lagarias, *On the existence of Fields Governing the 2-invariants of the Classgroup of $Q(\sqrt{dp})$ as p Varies*, Mathematics of computation Vol.41. Num. 164 Oct. 1983. 711-730
- [K-K-N] 河野美文 (Y. Kohno), 北村三郎 (S. Kitamura), 中原 徹 (T. Nakahara), グラフによる 2 次体の類群の 2 巾階数評価, 数理解析研究所研究集会 '離散数理論における最適組合せ構造' (1992, 7/14-16.) 報告集, 数理解析研究所講究録 820 (1993, 2)
- [K] 河野 美文 (Y. Kohno), 2 次体の類群のグラフによる 2 巾階数評価, 佐賀大学大学院工学系研究科修士論文 (1993), 1-38.
- [L] J. C. Lagarias, *On Determining the 4-Rank of the Ideal Class Group of a Quadratic Field*, J. Number Theory **12**(1980), 191-196.
- [M1] P. Morton, *On Rédei's theory of the Pell equation*, J. reine Angew. Math., **307/308** (1979), 373-398.
- [M2] ———, *Density results for the 2-classgroups of imaginary quadratic fields*, J. reine Angew. Math., **332**(1982), 156-187.
- [M3] ———, *The quadratic number fields with cyclic 2-classgroups*, Pacific Journal of Mathematics Vol. **108**, No. 1, (1983).
- [M4] ———, *Density result for the 2-classgroups and fundamental units of real quadratic field*, Studia Scie. Math. Hungarica **17** (1982), 21-43.
- [M5] ———, *Governing fields for the 2-classgroup of $Q(\sqrt{-q_1 q_2 p})$ and a related reciprocity law*, Acta Arithmetica **LV** (1990)
- [M6] ———, *On the non existence of aberian conditions governing solvability of -1 Pell equation*, J. reine. Math. **405** (1990), 147-155
- [O] 大島 豊 (Y. Oshima), グラフの彩色多項式に関する Unimodal 予想及び 2 次体の類群の Euler グラフを用いた 4-階数評価, 佐賀大学大学院理工学研究科修士論文 (1987), 1-63.

- [R-R] L.Rédei und H.Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J.reine Angew. Math. **170**(1933),69-74.
- [R1] L.Rédei, *Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J.reine Angew. Math. **171** (1935), 131-148.
- [R2] L.Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper*, J. reine Angew. Math. **180** (1939), 1-43.
- [St1] P.Stevenhagen, *Class groups and governing fields*, Ph.D.thesis, Univ.of California at Berkeley, (1988).
- [St2] P.Stevenhagen, *Ray class groups and governing fields*, Academisch proefschrift, Universiteit van Amsterdam, (1989)