数理解析研究所講究録
274巻 1976年 132-147

イデアル類群が3-及び5-部分群をもつ実二次体について

佐賀大 理工 中原 徹

§1. 序

本文の目的はイデアル類群が巡回3-及び5-部分群だけではなく任意に与えられた奇数位数の巡回群を部分群にもつような実二次体の一つの新しい特徴付けを与えることである.

$Q(\sqrt{\Delta})$を有理数体Q上の判別式がΔに等しい二次体, $J(\Delta)$をそのイデアル類群とする.

$Q(\sqrt{\Delta})$が虚二次体のときは T. Nagel [9], S.-N. Kuroda [8] による$J(\Delta)$が任意の有限巡回群を部分群にもつ場合, $J(\Delta)$が或る種の非巡回部分群をもつときは Y. Yamamoto [11], D. Shanks and P. Weinberger [12], D. Shanks [13] により$Q(\sqrt{\Delta})$の構成法が得られている. 一方$J(\Delta)$の2-部分群については種数が1に等しい$Q(\sqrt{\Delta})$の類数が2巾で割り切れるための有理的な判定法が種の理論を駆使して虚及び実二次体に対して Hasse [1], [2] [3], [4] により得られ, 同等の結果が二次形式のみを用いた P. Kaplan [7] にある.

実二次体の場合は虚のときと異なり単数群が自明でないことが本質的に効いて$\mathcal{J}(\Delta)$の階数が上がる場合，すなわち$\mathcal{J}(\Delta)$が非巡回部分群をもつ$Q(\sqrt{\Delta})$の初等的な構成法はGaupの種の理論による2-部分群以外は現在までのところ発見されていないようである．$\mathcal{J}(\Delta)$の3-部分群については T. Honda [6], Y. Yamamoto [17], O. Neumann [11] の類体論を用いた$Q(\sqrt{\Delta})$の特徴付け及び W. Shanks and P. Weinberger [12] の結果がある．さらに$\mathcal{J}(\Delta)$が与えられた巡回群を含む場合は実二次体がR-Q型（[10] 参照）すなわち$Q(\sqrt{\Delta})$の基本単数の連分数展開の周期の長さが高々3に等しいとき，P. Weinberger [16], K. Tanahashi [15]による結果がある．

われわれは以下の§§で [6], [11], [17] と異なる [12] の方法を用い，[12] を含み，[15], [16] と異なる実二次体の新しい類を決定する．

§2. 素数位数pのイデアル類の構成．

$\Delta = A^{2p} + 4B^{2p}$を実二次体$Q(\sqrt{\Delta})$の判別式，ただし$\Delta$は平方因数を含まず，$A \cdot B \neq 1$，$p$は奇素数とする．このとき$Q(\sqrt{\Delta})$の整数環$\mathcal{O}$は$\mathbb{Z}$-加群$[1, (1+\sqrt{\Delta})/2]$となる．以下$\mathbb{Z}$は有理整数環，$[\alpha, \beta]$は$\alpha$, βを底とする$\mathbb{Z}$-加群を意味する．

いま　$\delta_1 = 2B^p + \sqrt{\Delta}$，　$\delta_2 = (A^p + \sqrt{\Delta})/2$，　$\gamma = (2B^p + A^p + \sqrt{\Delta})/2$

$$\mathfrak{a}=[A,\ \delta_1-\gamma],\qquad \mathfrak{b}=[B,\ \delta_2]$$

とおけば $\delta_1,\delta_2,\gamma\in\mathfrak{o}$ かつ $\mathfrak{a}$, $\mathfrak{b}$ は $Q(\sqrt{\Delta})$ のイデアルとなりこれらの底は、いずれも標準的底である（Hasse [5], Takagi [14] 参照）．このとき

$$\mathfrak{a}\cdot\mathfrak{b}=\mathfrak{c}=[AB,\ \gamma]$$

$$N\mathfrak{a}=A,\qquad N\mathfrak{b}=B,\qquad N\mathfrak{c}=AB$$

を得る．さらに

$$\mathfrak{a}^p=[A^p,\ \delta_1-\gamma]$$

であるから $2^2\mathfrak{a}^{2p}=(4A^{2p},\ 4A^p,\ 4(\delta_1-\gamma)^2)$．

ここで $(\alpha_1,\cdots,\alpha_n)$ は $\alpha_1,\cdots,\alpha_n$ から生成される $Q(\sqrt{\Delta})$ のイデアルをあらわす．$N\delta_1=-A^{2p}$，$2(\delta_1-\gamma)=\delta_1-A^p$ を用いて

$$2^2\mathfrak{a}^{2p}\subseteqq(\delta_1),$$

ところが $(A,2)=1$，$(\delta_1,2)=1$ より

$$\mathfrak{a}^{2p}\subseteqq(\delta_1)$$

となるからノルムを比較して $\mathfrak{a}^{2p}=(\delta_1)$ を得る．同様に

$$(*)\qquad \mathfrak{a}^{2p}\cong\delta_1,\quad \mathfrak{b}^{2p}\cong\delta_2,\quad \mathfrak{c}^p\cong\gamma$$

が成立する．ここに $\cong$ は両辺がイデアルとして等しいことを意味する．

<u>補助定理 1</u>．もしも $AB\neq1$，整数 $\xi=(u+v\sqrt{\Delta})/2$ に対して

$$0<|v|\leqq\Delta^{(p-1)/2}/2^{p-1}$$

ならば任意の整数 η について

$$\xi \neq \eta^p$$

が成立する.

証明. 任意の $\eta \in \mathcal{O}$ に対して $\eta = (\tau + s\sqrt{\Delta})/2$, $\tau, s \in \mathbb{Z}$ とおくことができる. いまて: $\sqrt{\Delta} \longrightarrow -\sqrt{\Delta}$ を $Q(\sqrt{\Delta})/Q$ の共役写像とする. $\xi = \eta^p$ とすれば

$$2^{p-1}(\eta^p - \eta^{\tau p})/\sqrt{\Delta} = s\sum_{\substack{j=0 \\ 2\nmid j}}^{p} \tau^j s^{p-j-1} \Delta^{(p-j-1)/2} = 2^{p-1} v.$$

$s \neq 0$ より

$$|v| = |\eta^p - \eta^{\tau p}|/\sqrt{\Delta} > \Delta^{(p-1)/2}/2^{p-1}$$

が成立する. 証明終り.

定義. 数 $\alpha \in Q(\sqrt{\Delta})$ が primary とは

$$\alpha > 0 \quad \text{かつ} \quad 1 \leqq |\alpha/\alpha^{\tau}| < \varepsilon^2$$

となる整数 α をいう. ここに $\varepsilon > 1$ は $Q(\sqrt{\Delta})$ の基本単数である.

補助定理 2. (i) $A \cdot B \neq 1$ ならば $\gamma = (2B^p + A^p + \sqrt{\Delta})/2$ は primary である.

(ii) $A \neq 1$ ならば $\delta_1 = 2B^p + \sqrt{\Delta}$ は primary である.

(iii) $B \neq 1$ ならば $\delta_2 = (A^p + \sqrt{\Delta})/2$ は primary である.

証明. 定義より

$$\alpha \text{ が primary} \iff 1 \leqq \alpha/|N\alpha|^{1/2} < \varepsilon$$

が成立する．一方 $\Delta = A^{2p} + 4B^{2p}$ に対して $\begin{Bmatrix} A^p \\ 2B^p \end{Bmatrix} < \sqrt{\Delta} < 2\varepsilon$ は常に成立する．

(i) $\gamma / |N\gamma|^{1/2} = \gamma / (AB)^{p/2} > \begin{Bmatrix} \gamma > B^p, & A < B \\ \gamma > A^p, & A > B \end{Bmatrix} > 1$

他方，$\gamma / (AB)^{p/2} < 3\sqrt{\Delta} / 2(AB)^{p/2} < 3\varepsilon / (AB)^{p/2} < \varepsilon$．最後の不等号は $p \geq 3$，$A, B > 1$ のとき成立する．$A = 1$，$B > 1$ のとき $Q(\sqrt{\Delta})$ は $R - d0$ 型であるから $\varepsilon = 2B^p + \sqrt{\Delta}$ となる．ゆえに $3\sqrt{\Delta} / 2(AB)^{p/2} < \sqrt{\Delta} < \varepsilon$ が成立する．$A > 1$, $B = 1$ のとき $Q(\sqrt{\Delta})$ はやはり $R - d0$ 型であるから $\varepsilon = (A^p + \sqrt{\Delta})/2$

$$\gamma = (2 + A^p + \sqrt{\Delta})/2 < 2^{3/2} \cdot (A^p + \sqrt{\Delta})/2 \leqq (AB)^{p/2} \cdot \varepsilon$$

が成立する．

(ii) $A > 1$ $\delta_1 / |N\delta_1|^{1/2} = \delta_1 / A^p > 1$．他方 $\delta_1 / A^p < 4\varepsilon / A^p < \varepsilon$．

(iii) $B > 1$ $\delta_2 / |N\delta_2|^{1/2} = \delta_2 / B^p > 1$．他方 $\delta_2 / B^p < 4\varepsilon / 2B^p < \varepsilon$ を得る．　　証明終り．

さて (ρ)，$\rho > 0$ を $Q(\sqrt{\Delta})$ の任意の単項イデアルとすれば

$$1 \leqq \rho \varepsilon^j / |N\rho|^{1/2} < \varepsilon$$

が成立するためには

$$j \in [\ \log(|N\rho|^{1/2}/\rho) / \log \varepsilon,\ \log(|N\rho|^{1/2}/\rho) / \log \varepsilon + 1)$$

が必要十分である．ところが $(\rho) = (\rho\varepsilon^j)$ であるからすべての単項整イデアルは primary なる整数によって一意的に生成

される.

(*)から $\mathrm{ord}[\mathfrak{a}^2] \mid p$ または $\mathrm{ord}[\mathfrak{b}^2] \mid p$ が成立する.
ここに $[\mathfrak{a}]$ はイデアル $\mathfrak{a}$ の属するイデアル類をあらわす.
p は素数であるから $\mathrm{ord}[\mathfrak{a}^2] = \{1\}$, $\mathrm{ord}[\mathfrak{b}^2] = \{1\}$.
いま $\mathfrak{a}^2 \cong \alpha$, $\mathfrak{b}^2 \cong \beta$ としよう. このとき $\mathfrak{c}^2 \cong \sigma$ となる. ここに α, β, σ はすべて primary としてよい. (*)より

$$\alpha^p = \delta_1 \varepsilon^i, \quad \beta^p = \delta_2 \varepsilon^j, \quad \sigma^p = \gamma \varepsilon^k$$

なる指数 $i, j, k \in \mathbb{Z}$ が存在する. 他方 $\mathfrak{c}^2 \cong \alpha\beta$ より

$$\sigma^2 = \alpha\beta\varepsilon^m$$

なる指数 $m \in \mathbb{Z}$ が存在する. この両辺を p 乗すれば $\delta_1\delta_2 = \gamma^2$ に注意して i, j, k, m について

(**) $$i + j + mp = 2k$$

が成立しなければならない.

さて整数 γ が primary ならば

$$1 \leqq |\gamma/\gamma'| = |\sigma/\sigma'|^p \cdot \varepsilon^{-2k} < \varepsilon^2$$

が必要である. 一方 σ は primary であるから

$$1 \cdot \varepsilon^{-2k} \not< \varepsilon^2 \qquad \therefore \quad k > -1$$

$$\varepsilon^{2p} \cdot \varepsilon^{-2k} \not< 1 \qquad \therefore \quad k < p$$

さらに $k = 0$ ならば $\gamma = \sigma^p$. ところが $A \cdot B > 1$ ならば補助定理1より不合理である. ゆえに

$A \cdot B > 1$ ならば $1 \leqq k \leqq p-1$

同様に

$A > 1$ ならば $1 \leqq i \leqq p-1$, $B > 1$ ならば $1 \leqq j \leqq p-1$ が成立する. 他方,

$$1 \leqq |\alpha/\alpha'|^2 = |\alpha/\alpha'| \cdot |\beta/\beta'| \cdot \varepsilon^{2m} < \varepsilon^4$$

したがって $\varepsilon^{2m} \not\geqq \varepsilon^4$ $\therefore m < 2$, $\varepsilon^2 \cdot \varepsilon^2 \cdot \varepsilon^{2m} \not\leqq 1$ $\therefore m > -2$

すなわち $-1 \leqq m \leqq 1$ が必要である.

さて不定方定式(**)を(イ) $A > 1$, $B > 1$, (ロ) $A = 1$, $B > 1$ (ハ) $A > 1$, $B = 1$ の三つの場合に適当に区別して考察する.

(ロ)の場合は $Q(\sqrt{D})$ は R-$\mathcal{U}$ 型となり $\varepsilon = 2B^p + \sqrt{D} = \delta_1$, $\alpha = 1$ より $i = -1$. 一方 $B \neq 1$ より δ_2, γ は primary, よって $1 \leqq j, k \leqq p-1$. さらに $-1 + j + mp = 2k$ より $0 \leqq m \leqq 1$ が必要である.

(ハ)の場合も $Q(\sqrt{D})$ は R-$\mathcal{U}$ 型であり(ロ)と同様に $j = -1$, $1 \leqq i, k \leqq p-1$, $0 \leqq m \leqq 1$ が必要である. よって (**) を $1 \leqq |i|, |j|, k \leqq p-1$, $0 \leqq |m| \leqq 1$ なる条件のもとで考察すれば十分である.

δ_1, δ_2, γ に関して次の命題が成たがう.

<u>命題1.</u> 上と同じ記号のもとで, もしも $A, B \neq 1$ ならば $s, t, u \in \mathbb{Z}$ に対して

$$0 < s + t + u \leqq p-2, \quad s, t, u \geqq 0$$

のとき

$$\delta_1^s \delta_2^t \gamma^u, \quad \delta_1^{\tau s} \delta_2^t \gamma^u, \quad \delta_1^s \delta_2^{\tau t} \gamma^u$$

及びこれらの共役数はすべて $Q(\sqrt{\Delta})$ の整数の p 乗ではない.

とくに $\delta_1^s \delta_2^t \gamma^u$ は $A \cdot B \neq 1$ のときも p 乗数ではない.

証明. $\mathfrak{Z}$, $\eta \in \mathcal{O}$ に対し $\eta^p = \mathfrak{Z}$ ならば $(\eta^\tau)^p = \mathfrak{Z}^\tau$ となるから始めの三個の場合について証明すれば十分である. まず $\delta_1^s \delta_2^t \gamma^u$ について調べよう. $s \equiv t \equiv u \equiv 1 \bmod 2$ の場合.

$$v = 2^{p-1} \left| \delta_1^s \delta_2^t \gamma^u - \delta_1^{\tau s} \delta_2^{\tau t} \gamma^{\tau u} \right| / \sqrt{\Delta}$$

$$= 2^{p-1-t-u} \left\{ \sum_{2 \nmid l}' \cdot \sum_{2 \nmid m}' \cdot \sum_{2 \mid n}' + \sum_{2 \mid l}' \sum_{2 \mid m}' \cdot \Delta \cdot \sum_{2 \mid n}' + \sum_{2 \nmid l}' \sum_{2 \mid m}' \cdot \sum_{2 \nmid n}' + \sum_{2 \mid l}' \cdot \sum_{2 \nmid m}' \cdot \sum_{2 \nmid n}' \right\}$$

ここに

$$\sum_{2 \nmid l}' = \sum_{2 \nmid l} \binom{s}{l} (2B^p)^l \Delta^{(s-l)/2}, \quad \sum_{2 \mid l}' = \sum_{2 \mid l} \binom{s}{l} (2B^p)^l \Delta^{(s-l-1)/2}$$

$$\sum_{2 \nmid m}' = \sum_{2 \nmid m} \binom{t}{m} (A^p)^m \Delta^{(t-m)/2}, \quad \sum_{2 \mid m}' = \sum_{2 \mid m} \binom{t}{m} (A^p)^m \Delta^{(t-m-1)/2}$$

$$\sum_{2 \nmid n}' = \sum_{2 \nmid n} \binom{u}{n} (2B^p + A^p)^n \Delta^{(u-n)/2}, \quad \sum_{2 \mid n}' = \sum_{2 \mid n} \binom{u}{n} (2B^p + A^p)^n \Delta^{(u-n-1)/2}$$

を意味する. このとき $A \cdot B > 1$ を用いて

$$v < 2^{p-1-t-u} \left\{ 2^s \cdot \Delta^{s/2} \cdot 2^t \cdot \Delta^{t/2} \cdot 2^{2u} \Delta^{(u-1)/2} \right.$$

$$+ 2^s \cdot \Delta^{(s-1)/2} \cdot 2^t \cdot \Delta^{(t-1)/2} \cdot \Delta \cdot 2^{2u} \cdot \Delta^{(u-1)/2} + 2^s \cdot \Delta^{s/2} \cdot 2^t \cdot \Delta^{(t-1)/2} \cdot 2^{2u} \Delta^{u/2}$$

$$\left. + 2^s \Delta^{(s-1)/2} \cdot 2^t \cdot \Delta^{t/2} \cdot 2^{2u} \cdot \Delta^{u/2} \right\}$$

$$= 2^{p+s+u+1} \Delta^{(s+t+u-1)/2} < \Delta^{(s+t+u+1)/2} \leqq \Delta^{(p-1)/2}.$$

他方 $v > 0$ だから補助定理1より $\delta_1^s \delta_2^t \gamma^u$ は p 乗数ではない.

次に $\xi = \delta_1^{\tau^s}\delta_2^{t}\gamma^u$ について. $s \equiv t \equiv u \equiv 1 \bmod 2$ の場合.

$$v = 2^{p-1}\left|\delta_1^{\tau^s}\delta_2^{t}\gamma^u - \delta_1^{s}\delta_2^{\tau^t}\gamma^{\tau u}\right| / \sqrt{\Delta}$$

$$< 2^{p-1-t-u}\left\{\sum_{2\nmid l}'\sum_{2\nmid m}'\sum_{2\nmid n}' + \left|-\sum_{2\mid l}'\right|\sum_{2\mid m}'\cdot\Delta\cdot\sum_{2\mid n}' + \sum_{2\nmid l}'\sum_{2\mid m}'\sum_{2\nmid n}' + \left|-\sum_{2\mid l}'\right|\sum_{2\nmid m}'\sum_{2\nmid n}'\right\}.$$

これは前の場合と同じだから $v \leqq \Delta^{(p-1)/2}$ を得る. 他方もしも $\xi \in Q$ とすれば $\xi^{\tau} = \xi$ が成立する. このとき

$$\sum_{2\nmid l}' = \sum_{\substack{l=1\\ 2\nmid l}}^{s}\binom{s}{l}(2B^p)^l\Delta^{(s-l)/2} \equiv 0 \bmod 2B^p$$

を用いて

$$(1)\quad 2\sum_{2\mid l}'\sum_{2\mid m}'\cdot\Delta\cdot\sum_{2\mid n}' + 2\sum_{2\mid l}'\sum_{2\nmid m}'\sum_{2\nmid n}' \equiv 0 \bmod 2B^p$$

を得る. ここで $\Delta \equiv A^{2p} \bmod 2B^p$ であるから

$$\sum_{2\mid l}' = \sum_{\substack{l=0\\ 2\mid l}}^{s}\binom{s}{l}(2B^p)^l\Delta^{(s-l-1)/2} \equiv \Delta^{(s-1)/2} \equiv (A^p)^{s-1} \bmod 2B^p$$

$$\sum_{2\mid m}' \equiv (A^p)^{t-1}\sum_{2\mid m}\binom{t}{m}, \quad \sum_{2\nmid m}' \equiv (A^p)^{t}\sum_{2\nmid m}\binom{t}{m} \bmod 2B^p$$

$$\sum_{2\mid n}' \equiv (A^p)^{u-1}\sum_{2\mid n}\binom{u}{n}, \quad \sum_{2\nmid n}' \equiv (A^p)^{u}\sum_{2\nmid n}\binom{u}{n} \bmod 2B^p$$

したがって

$$2(A^p)^{s+t+u-1}\left\{\sum_{2\mid m}\binom{t}{m}\sum_{2\mid n}\binom{u}{n} + \sum_{2\nmid m}\binom{t}{m}\sum_{2\nmid n}\binom{u}{n}\right\} \equiv 0 \bmod 2B^p.$$

ところが $B > 1$ だから

$$0 < \sum_{2\mid m}\binom{t}{m}\cdot\sum_{2\mid n}\binom{u}{n} + \sum_{2\nmid m}\binom{t}{m}\sum_{2\nmid n}\binom{u}{n} < 2^{t+u} < B^p$$

かつ $(A, B) = 1$ より 合同式(1)の左辺 $\not\equiv 0 \bmod 2B^p$ となり不合理である. よって $v > 0$. ゆえに補助定理1により ξ は p 乗数ではない. 最後に $\xi = \delta_1^{s}\delta_2^{\tau^t}\gamma^u$ について調べる.

$s \equiv t \equiv u \equiv 1 \bmod 2$ の場合.

$v = 2^{p-1}\left|\delta_1^{s}\delta_2^{\tau^t}\gamma^u - \delta_1^{\tau^s}\delta_2^{t}\gamma^{\tau u}\right| / \sqrt{\Delta}$ に対し $v \leqq \Delta^{(p-1)/2}$

は先と同じく成立する．他方もしも $\zeta \in Q$ とすれば $\zeta = \zeta^\tau$ であるから $\sum'_{2\nmid l}\sum'_{2\nmid m}\sum'_{2\nmid n} + \sum'_{2\nmid l}(-\sum)\Delta\sum'_{2\nmid n} + \sum'_{2\nmid l}(-\sum')\sum'_{2\nmid m 2\nmid n} + \sum'_{2\nmid l}\sum'_{2\nmid m 2\nmid n}$
$= \sum'_{2\nmid l}\sum'_{2\nmid m}(-\sum'_{2\nmid n}) + (-\sum'_{2\nmid l})\sum'_{2\nmid m}\Delta(-\sum'_{2\nmid n}) + \sum'_{2\nmid l}\sum'_{2\nmid m}\sum'_{2\nmid n} + (-\sum'_{2\nmid l})\sum'_{2\nmid m}\sum'_{2\nmid n}$
を得る．$\sum'_{2\nmid m} \equiv 0 \bmod A^p$ を用いて

$$2(2B^p)^{\lambda+\mu+\nu-1}\left\{\sum_{2\nmid l}\binom{\lambda}{l}\sum_{2\nmid n}\binom{\mu}{n} + \sum_{2\nmid l}\binom{\lambda}{l}\sum_{2\nmid n}\binom{\mu}{n}\right\} \equiv 0 \bmod A^p$$

が成立しなければならない．ところが仮定より $(A, 2B)=1$, $A>1$, さらに $0 < \sum_{2\nmid l}\binom{\lambda}{l}\sum_{2\nmid n}\binom{\mu}{n} + \sum_{2\nmid l}\binom{\lambda}{l}\sum_{2\nmid n}\binom{\mu}{n} < 2^{\lambda+\mu} < A^p$ ゆえに不合理である．よって $\nu > 0$．したがって補助定理1より ζ は p 無数ではない．ζ についての以上の評価はその他の $\lambda, \mu, \nu \bmod 2$ についても同様である．ゆえに命題1の証明は完了した．

さて $\rho \in Q(\sqrt{\Delta})$, $\zeta \in \mathfrak{O}$ について $\rho^p = \zeta$ ならば実は $\rho \in \mathfrak{O}$ となる，すなわち $\mathfrak{O}$ は整閉であることに注意しよう．

不定方程式

$$(**) \qquad i + j + mp = 2k$$

をまず $|i| = |j|$ のとき考える．$i = j$ ならば $(-B^2\alpha/\beta)^p = \delta_1\delta_2^\tau$．ところが $\nu = 2^{p-1}|\delta_1\delta_2^\tau - \delta_1^\tau\delta_2|/\sqrt{\Delta} = 2^{p-1}|2B^p - A^p| > 0$．他方 $\nu < 2^{p-1}\cdot 2\cdot\Delta^{1/2} < \Delta \leqq \Delta^{(p-1)/2}$．$i = -j$ ならば $(\alpha\cdot\beta)^p = \delta_1\delta_2$．$\nu = 2^{p-1}|\delta_1\delta_2 - \delta_1^\tau\delta_2^\tau|/\sqrt{\Delta} = 2^{p-1}(2B^p + A^p) > 0$．他方 $\nu \leqq \Delta^{(p-1)/2}$．ゆえにいずれの場合も補助定理

1に矛盾する．次に $|i|+|j|$ の場合を調べる．

$m=-1$ ならば (ロ), (ハ) の場合は生じないから $i>0, j>0$．(**) の左辺 $\leqq (p-1)+(p-2)-p=p-3=2k$ $\therefore 1\leqq k\leqq (p-3)/2$ これより $p\geqq 5$ だから $p=3$ のときこの場合は生じない（W. Shanks and P. Weinberger [12] 参照）．いま $s=t=k=(i+j-p)/2$, $u=|i-j|$ とおく．このとき $s+t+u\leqq p-2$ である．$i>j$ のとき $(-s)i+tj+uk=0$．したがって $(-A^2\cdot\alpha^{-s}\cdot\beta^{t}\cdot\sigma^{u})^p=\delta_1^{\tau s}\delta_2^{t}\gamma^{u}$ を得る．$i<j$ のとき $si+(-t)j+uk=0$．したがって $(-B^2\cdot\alpha^{s}\cdot\beta^{-t}\cdot\sigma^{u})^p=\delta_1^{s}\delta_2^{\tau t}\gamma^{u}$ となる．しかしいずれの場合も命題1に矛盾する．

$m=1$ ならば (**) より $1\leqq i+j\leqq p-2$．(ロ) の場合とくに $i=-1$, $j=p-1$ のときは $k=j$，すなわち $(AB\cdot\beta\cdot\sigma^{-1})^p=\delta_2\cdot\gamma^{\tau}$ が成立する．$v=2^{p-1}|\delta_2\gamma^{\tau}-\delta_2^{\tau}\gamma|/\sqrt{\Delta}=2^{p-1}B^p>0$，他方 $v<\Delta\leqq\Delta^{(p-1)/2}$．(ハ) の場合，とくに $i=p-1$, $j=-1$ のとき $k=i$ であるから $(AB\cdot\alpha\cdot\sigma^{-1})^p=\delta\gamma^{\tau}$ を得る．$v=2^{p-1}|\delta_1\gamma^{\tau}-\delta_1^{\tau}\gamma|/\sqrt{\Delta}=2^{p-1}A^p>0$．他方 $v\leqq\Delta^{(p-1)/2}$ となる．ゆえに補助定理1により双方とも除外される．よって $m=1$ のときは $|i|+|j|\leqq p-2$ の場合を調べれば十分である．いま $s=|j|$, $t=|i|$, $u=0$ とおく．$i, j>0$ のとき $(-s)i+tj=0$．このとき

$(-A^{2s}\cdot\alpha^{-s}\beta^{t})^{p}=\delta_1^{\tau s}\delta_2^{t}$. $i=-1$のとき $j>0$だから $si+tj=0$, $\therefore$ $(\alpha^{s}\beta)^{p}=\delta_1^{s}\delta_2$. $j=-1$のとき $(\alpha\cdot\beta^{t})^{p}=\delta_1\delta_2^{t}$ を得る. しかしいずれの場合も命題1により不合理となる.

$m=0$のとき (**) $i+j=2k$ より $i\equiv j \bmod 2$. ゆえに $i\equiv j\equiv 0 \bmod 2$のとき $s=i/2$, $t=j/2$, $u=0$ とおく. $i\neq j$の場合であるから $s+t+u\leq p-2$. さらに $si+tj=0$ $\therefore$ $(-A^{2s}\cdot\alpha^{-s}\cdot\beta^{t})^{p}=\delta_1^{\tau s}\delta_2^{t}$. $i\equiv j\equiv 1 \bmod 2$のとき $j\geq 1$ ならば $s=(j-1)/2$, $t=(i+1)/2$ $u=1$とおく. このとき $i\neq j$より $s+t+u\leq p-2$, $si+(-t)j+uk=0$ となる. ゆえに $(-B^{2t}\cdot\alpha^{s}\cdot\beta^{-t}\cdot\alpha)^{p}=\delta_1^{s}\delta_2^{\tau t}\gamma$. $j=-1$のとき $i\equiv 1 \bmod 2$ ゆえ $k\leq(p-3)/2$. いま $s=0$, $t=k$, $u=1$とおく. このとき $s+t+u\leq p-2$, $tj+uk=0$. ゆえに $(\beta^{t}\alpha)^{p}=\delta_2^{t}\gamma$. しかし各々の場合, 命題1により すべて不合理となる. ゆえに不定方程式(**)は解をもたない. すなわち $\mathrm{ord}[\mathfrak{a}^2]=p$ または $\mathrm{ord}[\mathfrak{b}^2]=p$ が成立する. したがって判別式 $\Delta=A^{2p}+4B^{2p}\equiv 1 \bmod 2$, $A\cdot B\neq 1$ に対する実二次体 $Q(\sqrt{\Delta})$ のイデアル類群 $\mathcal{J}(\Delta)$ は素数位数 p の巡回群を含む.

§3. 素数巾位数 p^e のイデアル類の構成.

判別式 $\Delta = A^{2p} + 4B^{2p} \equiv 1 \bmod 2$, $A \cdot B \neq 1$ の real 二次体 $Q(\sqrt{\Delta})$ の二つのイデアル:

$$\mathfrak{a} = [A, (2B^p - A^p + \sqrt{\Delta})/2], \quad \mathfrak{b} = [B, (A^p + \sqrt{\Delta})/2]$$

は §2 の通りとする.

いま $A = a^{p^{e-1}}$, $B = b^{p^{e-1}}$, $e \geq 1$ に対して

$$\mathfrak{a}_0 = [a, (2b^{p^e} - a^{p^e} + \sqrt{\Delta})/2], \quad \mathfrak{b}_0 = [b, (a^{p^e} + \sqrt{\Delta})/2]$$

とおく. このとき $\mathfrak{a}_0$, $\mathfrak{b}_0$ は $Q(\sqrt{\Delta})$ の標準的底表示のイデアルとなり $N\mathfrak{a}_0 = a$, $N\mathfrak{b}_0 = b$ を得る. さらに

$$\mathfrak{a}_0^{p^{e-1}} = [A^{p^{e-1}}, (2b^{p^e} - a^{p^e} + \sqrt{\Delta})/2], \quad \mathfrak{b}_0^{p^{e-1}} = [B^{p^{e-1}}, (a^{p^e} + \sqrt{\Delta})/2]$$

すなわち $\mathfrak{a}_0^{p^{e-1}} = \mathfrak{a}$, $\mathfrak{b}_0^{p^{e-1}} = \mathfrak{b}$ が成立する. いま $\mathrm{ord}[\mathfrak{a}^2] = p$ とすれば $\mathrm{ord}[\mathfrak{a}_0^2] \mid p^e$ を得る. 一方もしも $\mathrm{ord}[\mathfrak{a}_0^2] = p^s$, $0 \leq s < e$ とすれば $\mathfrak{a}^2 = (\mathfrak{a}_0^2)^{p^{e-1}} = (\mathfrak{a}_0^{2p^s})^{p^{e-1-s}} \cong \mathfrak{o}$, これは矛盾である. ゆえに $\mathrm{ord}[\mathfrak{a}_0^2] = p^e$ が成立する. ゆえに奇素数 p に対して $Q(\sqrt{\Delta})$ のイデアル類群 $\mathfrak{H}(\Delta)$ は位数 p^e の巡回部分群をもつ.

§4. 定理.

われわれは §3 までの考察から次の定理を得る.

定理1. もしも奇数 $m>1$ に対し $\Delta=A^{2m}+4B^{2m}>5$ が平方因数を含まないならば実二次体 $Q(\sqrt{\Delta})$ のイデアル類群は位数 m の巡回部分群をもつ.

証明 m の標準分解を $m=\prod_j p_j^{e_j}$, $e_j>0$, p_j は互いに素な奇素数, とする. いま A_j, B_j をそれぞれ $A_j=A^{m/p_j^{e_j}}$, $B_j=B^{m/p_j^{e_j}}$ とおけば $\Delta=A_j^{2p_j^{e_j}}+4B_j^{2p_j^{e_j}}$ とあらわされる. このとき §3 の結果より $\mathcal{J}(\Delta)$ は素数巾 $p_j^{e_j}$ の巡回部分群を含む. この事実は素数 $p_j \mid m$ の選び方に依存しない. そうすれば $\mathcal{J}(\Delta)$ はアーベル群, $(p_i, p_j)=1$ $(i\neq j)$ であるから $Q(\sqrt{\Delta})$ のイデアル類群 $\mathcal{J}(\Delta)$ は位数 $\prod_j p_j^{e_j}$ の巡回部分群をもつ.

証明終り.

注意. 実験例の中で定理1の内容を超えるものがみつかった. すなわち $p=3$ のとき $\Delta=13^6+4\cdot 2^6=4827065$ $=5\cdot 17\cdot 109\cdot 521$ に対する実二次体 $Q(\sqrt{\Delta})$ のイデアル類群は非巡回3部分群をもつ. なお $Q(\sqrt{\Delta})$ の基本単数 ε は比較的小さく

$$\varepsilon=6355010792+2892509\sqrt{\Delta},\quad N\varepsilon=-1$$

である.

参 考 文 献

(1) H. Hasse, Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \bmod 2^3$, Aequationes Math., 3(1969), 165-169.

(2) H. Hasse, Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, J. Number Theory, 1(1969), 231-234

(3) H. Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl imaginär-quadratische Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, J. Reine Angew. Math., 241(1970), 1-6.

(4) H. Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, Math. Nachr., 46(1970), 61-70.

(5) H. Hasse, Vorlesungen über Zahlentheorie, Berlin- Gottingen-Heidelberg-New York, 1964.

(6) T. Honda, On Real Quadratic Fields whose Class Numbers are Multiples of 3, J. Reine Angew. Math., 233(1968), 101-102.

(7) P. Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclic, et reciprocité biquadratique, J. Math. Soc. Japan, 25(1973), 596-608.

(8) S.-N. Kuroda,On the Class Number of Imaginary Quadratic Number Fields, Proc. Japan Acad., 40(1964), 365-367.

(9) T. Nagel, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, 1(1922), 140-150.

(10) T. Nakahara, On the fundamental units and an estimate of the class numbers of real quadratic fields, Rep. Fac. Sci. Engin., Saga Univ., 2(1974), 1-13.

〔11〕 O. Neumann, Relativ-quadratische Zahlkörper, deren Klassenzahlen durch 3 teilbar sind, Math. Nachr., 56(1973), 281-306.

〔12〕 D. Shanks and P. Weinberger, A quadratic field of prime discriminant requiring three generators for its class group, and related theory, Acta Arith., 21(1972), 71-87.

〔13〕 D. Shanks, New Types of Quadratic Fields Having Three Invariants Divisible by 3, J. Number Theory, 4(1972), 537-556.

〔14〕 T. Takagi, 初等整数論講義, Tokyo, 1931.

〔15〕 K. Tanahashi, 実二次体の類数について, 本講究録.

〔16〕 P. Weinberger, Real Quadratic Fields with Class Numbers Divisible by n, J. Number Theory, 5(1973), 237-241.

〔17〕 Y. Yamamoto, On unramified galois extensions of quadratic number fields, Osaka J, Math., 7(1970), 57-76.