数理解析研究所講究録
第378巻 1980年 82-87

16-divisibilities of class numbers of quadratic fields

阪大 理 山本芳彦

§1. Gauss の genus theory.　Kを判別式Dをもつ2次体: $K = \mathbb{Q}(\sqrt{D})$, H, $h^+ = h^+(D)$ をKの狭義のイデアル類群及びその類数とする. Kの(分数)イデアル $\mathfrak{a}$, $\mathfrak{b}$ が同じ類に入るとき $\mathfrak{a} \approx \mathfrak{b}$ と記す. Dの素因子の個数をtとするとDは $D = d_1 d_2 \cdots d_t$ と t個の素判別式(唯一つの素因子をもつ判別式)の積にかける. このとき

<u>定理</u>(genus theory)　H^+ の 2-Sylow 群の生成元は $t-1$個: ($H^+/(H^+)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$).

以後 $t=2$, $D = d_1 d_2$ の場合のみを考える. 素判別式 d_1, d_2 の素因子を夫々 p, q とする; $p \mid d_1$, $q \mid d_2$. このとき H^+ の 2-Sylow 群は巡回群である. 類体論により, Kの(すべての有限素点で)不分岐な2次拡大体 K_2 が一意に定まる(H^+の部分群 $(H^+)^2$ に対応する). 今の場合には

$$K_2 = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = K(\sqrt{d_1}) = K(\sqrt{d_2})$$

となる．$A=\mathbb{Q}(\sqrt{d_1})$，$B=\mathbb{Q}(\sqrt{d_2})$ とおく．p，q は K において分岐するから，その素イデアル分解を

$$(p)=\mathfrak{p}^2,\quad (q)=\mathfrak{q}^2 \quad (\mathfrak{p},\mathfrak{q} \text{ は } K \text{の素イデアル})$$

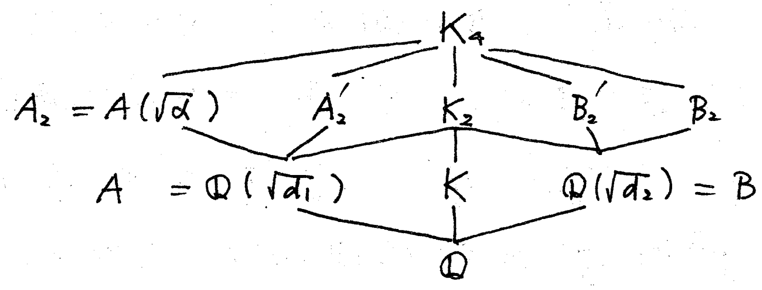
とおくと，$\mathfrak{p}^2 \approx \mathfrak{q}^2 \approx 1$（単項イデアル）だが，少なくとも一方は単項でないことより，$\mathfrak{q} \not\approx 1$ と仮定する．

§2. Divisibility by 4. Kの素イデアル$\mathfrak{q}$が単項でないという仮定より，$\mathfrak{q}$の（H^+における）位数は2である（誤解のおそれのないとき，イデアル$\mathfrak{q}$とそのイデアル類を同じ記号を用いる．）．従って H^+ の 2-Sylow群が巡回群であることより：$4 \mid h^+ \Leftrightarrow \mathfrak{q} \in (H^+)^2 \Leftrightarrow \mathfrak{q}$ は K_2/K で完全分解する．$\Leftrightarrow$ q は $A/\mathbb{Q}$ で完全分解する．$\Leftrightarrow$ $\left(\frac{d_1}{q}\right)=1$ （Kronecker symbol）．K において $\mathfrak{p} \approx 1$ 又は $\mathfrak{p} \approx \mathfrak{q}$ となることより，pとqを区別せずに（仮定 $\mathfrak{q} \not\approx 1$ なしで）次の様に表せる．

<u>定理</u>（Rédei - Reichardt）

$$4 \mid h^+ \Leftrightarrow \left(\frac{d_1}{q}\right)=\left(\frac{d_2}{p}\right)=1$$

§3. Divisibility by 8. 以後 $4 \mid h^+$ とする．このとき $H^+/(H^+)^4$ は位数4の巡回群で $(H^+)^4$ に対応するKの4次の不分岐拡大を K_4 とする．K_4 は $\mathbb{Q}$ 上 normal で $Gal(K_4/\mathbb{Q}) \simeq D_8$（位数8の2面体群）．$K_4$ の部分体は次頁の通り．



ここで $\alpha \in A^{\times} - (A^{\times})^2$. q は A で完全分解するから, q の A における素イデアル分解を $(q) = \mathfrak{q}_A \mathfrak{q}_A'$ とし, かつ A_2/A において $\mathfrak{q}_A$ は分岐, $\mathfrak{q}_A$ 以外の A の素イデアルは不分岐とする. このとき A の類数 $h_1 (= h(d_1) = h^+(d_1))$ は奇数であることより, α として, $d_2 \neq -4$ なら $(\alpha) = \mathfrak{q}_A^{h_1}$, $d_2 = -4$ なら $\alpha = \varepsilon$ (Aの単数) となるものがとれる.

そこで: $8 \mid h^+ \Leftrightarrow \mathfrak{q} \in (H^+)^4 \Leftrightarrow \mathfrak{q}$ は K_4/K で完全分解する. $\Leftrightarrow \mathfrak{q}_A'$ は A_2/A で完全分解する.

最後の条件を α を用いて書き直すことにより, Hasse, Barrucand-Cohn, Bauer, Kaplan 達による様々な $8 \mid h^+$ の必要十分条件が見通しよく統一的に得られる.

<u>例1.</u> $D = pq$, $p \equiv q \equiv 1 \pmod 4$ のとき

$$4 \mid h^+ \Leftrightarrow \left(\frac{p}{q}\right) = 1 \Leftrightarrow \left(\frac{q}{p}\right) = 1$$

$$8 \mid h^+ \Leftrightarrow \left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1 \quad (4\text{乗剰余記号})$$

<u>例2.</u> $D = p(-q)$, $p \equiv -q \equiv 1 \pmod 4$ のとき

$$4 \mid h^+ \Leftrightarrow \left(\frac{p}{q}\right) = 1 \Leftrightarrow \left(\frac{-q}{p}\right) = 1$$

$$8 \mid h^+ \Leftrightarrow \left(\frac{-q}{p}\right)_4 = 1$$

§4. Divisibility by 16. 以後 $8 \mid h^+$ とする. 従って, $H^+/(H^+)^8$ は位数 8 の巡回群となる. $(H^+)^8$ に対応する K の不分岐 8 次巡回拡大体を K_8 とする. K_8 は $\mathbb{Q}$ 上 normal で $Gal(K_8/\mathbb{Q}) \simeq D_{16}$ (位数 16 の 2 面体群). K_8 の部分体として, A_2 の 2 次拡大体 $A_4 = A_2(\sqrt{\alpha_2})$, $\alpha_2 \in A_2^\times$, で, $K_8 = K_4(\sqrt{\alpha_2})(= K_4A_4)$ となるものが存在する. $8 \mid h^+$ より, A_2/A において, $\mathfrak{q}_A$ は分岐, $\mathfrak{q}_A'$ は完全分解するから, A_2 において, $\mathfrak{q}_A = Q^2$, $\mathfrak{q}_A' = Q'Q''$ と素イデアル分解される. さらに, A_4/A_2 において, Q' は分岐, その他の素イデアルは不分岐とする. このとき, 前の§と同様に: $16 \mid h^+ \Leftrightarrow \mathfrak{q} \in (H^+)^8 \Leftrightarrow \mathfrak{q}$ は K_8/K で完全分解する. $\Leftrightarrow$ Q は A_4/A_2 で完全分解する. $\Leftrightarrow$ Q'' は A_4/A_2 で完全分解する. : となる. A_2 の類数 h_2 が奇数であることより, α_2 としては, $\alpha_2 \neq -4$ のとき $(\alpha_2) = Q'^{h_2}$, $\alpha_2 = -4$ なら $\alpha_2 = \varepsilon_2$ (A_2 の単数) ととれる. α_2 をうまく選ぶことにより, $16 \mid h^+$ の条件を α に関する条件で書くことができる.

<u>定理</u> 1. $D = p\mathfrak{q}$, $p \equiv \mathfrak{q} \equiv 1 \pmod 4$, $4 \mid h^+$ とするとき.

$$(*)_p \begin{cases} x^2 - py^2 = 4\mathfrak{q}^{h(p)} \\ \dfrac{x + y\sqrt{p}}{2} \text{ は } \bmod 4 \text{ で平方数と合同 } \left(\text{in } \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]\right) \end{cases}$$

$$(*)_q \begin{cases} x'^2 - q y'^2 = 4 p^{h(q)} \\ \dfrac{x' + y'\sqrt{q}}{2} \text{ は mod 4 で平方数と合同 (in } \mathbb{Z}[\frac{1+\sqrt{q}}{2}]) \end{cases}$$

をみたす　x, y, x', $y' \in \mathbb{Z}$ が存在する．このとき

$$8 \mid h^+ \iff \left(\frac{x}{q}\right) = \left(\frac{x'}{p}\right) = 1$$

$$16 \mid h^+ \iff \left(\frac{x}{q}\right)_4 = \left(\frac{x'}{p}\right)_4 = 1$$

定理 2．$D = p(-q)$，$p \equiv -q \equiv 1 \pmod 4$，$4 \mid h^+$ のとき

$$(*)_{-q} \begin{cases} x'^2 + q y'^2 = 4 p^{h(-q)} \\ \dfrac{x' + y'\sqrt{-q}}{2} \text{ は mod 4 で平方数と合同 (in } \mathbb{Z}[\frac{1+\sqrt{-q}}{2}]) \end{cases}$$

をみたす　x', $y' \in \mathbb{Z}$ が存在する．このとき

$$8 \mid h^+ \iff \left(\frac{x'}{p}\right) = 1$$

$$16 \mid h^+ \iff \left(\frac{x'}{p}\right)_4 = 1$$

定理 3．$D = (-8)q$，$q \equiv 1 \pmod 8$ のとき

$$\begin{cases} x^2 + 2y^2 = q \\ x + y\sqrt{-2} \equiv 1 \text{ 又は } -1 + 2\sqrt{-2} \pmod{4\sqrt{-2}} \end{cases}$$

をみたす　x, $y \in \mathbb{Z}$ が存在する．このとき

$$8 \mid h^+ \iff \left(\frac{x}{q}\right) = 1$$

$$16 \mid h^+ \iff \left(\frac{x}{q}\right)_4 = 1$$

定理 4．$D = 8(-q)$，$q \equiv -1 \pmod 8$ のとき

$$\begin{cases} x^2 + q y^2 = 2^{2+\hat{h}} \\ x \equiv 1 \pmod 4 \end{cases} \qquad \hat{h} = \begin{cases} h(-q) & \text{if } h(-q) \geqq 5 \\ 5 & h(-q) = 1 \\ 9 & h(-q) = 3 \end{cases}$$

となる　x, $y \in \mathbb{Z}$ が存在する．このとき

$$8 \mid h^+ \iff \pi \equiv 1 \pmod 8$$

$$16 \mid h^+ \iff \pi \equiv 1 \pmod{16}$$

References.

L. Rédei – H. Reichardt : Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. reine angew. Math. 170 (1934), 69–74.

H. Hasse : Aequationes. mathematicae 3 (1969), 254–258

" : Crelle 241 (1970) 1–6.

" : J. Number Theory 1 (1969) 231–234 ff.

P. Barrucand – H. Cohn : Crelle 238 (1969) 67–70. ff.