

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 (分岐) イデアル α, β が同じ類に入る
とき $\alpha \approx \beta$ 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) の積にかけらる. このとき

定理 (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; $p|d_1, q|d_2$.
このとき H^+ の 2-Sylow 群は巡回群である. 類体論により,
 K の (すべての有限素数で) 不分裂な 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). この場合には

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

<1>

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

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

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はないことより, $\mathfrak{q} \neq 1$ と仮定する.

§2. Divisibility by 4. K の素イデアル \mathfrak{q} が単項では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. $\Leftrightarrow f$ は A/\mathbb{Q} で完全分解する. \Leftrightarrow

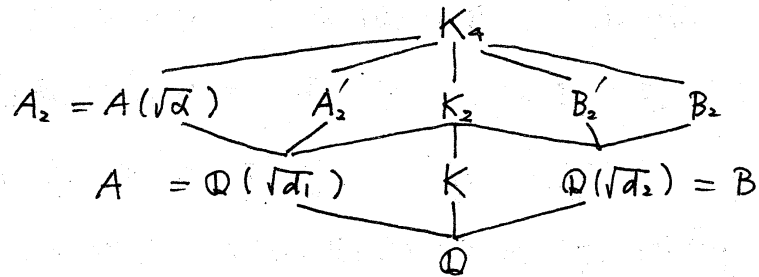
$$\left(\frac{d_1}{f}\right) = 1 \quad (\text{Kronecker symbol}). \quad K \text{ において}$$

$\mathfrak{p} \approx 1$ 又は $\mathfrak{p} \approx \mathfrak{q}$ となることより, p と f をそれぞれ p と f (仮定 $\mathfrak{q} \neq 1$ として) 次の様に表せる.

定理 (Rédei - Reichardt)

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

§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 τ ($H^+)^4$ 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 $\text{Gal}(K_4/\mathbb{Q}) \simeq D_8$ (位数 8 の 2 面体群). K_4 の部分体は次頁の通り.



ここで $\alpha \in A^\times - (A^\times)^2$. f は A で完全分解するから, f の A における素イデアル分解を $(f) = \mathfrak{p}_A \mathfrak{p}'_A$ とし, \mathfrak{p}_A は A_2/A において \mathfrak{p}_A は分岐, \mathfrak{p}'_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, $d_2 \neq -4$ ならば $(\alpha) = \mathfrak{p}_A^{h_1} \mathfrak{p}'_A$ $d_2 = -4$ ならば $\alpha = \varepsilon$ (A の単数) とするものだとおける. すると: $8 \mid h^+ \Leftrightarrow \mathfrak{p}_A \in (H^+)^4 \Leftrightarrow \mathfrak{p}_A$ は K_4/K で完全分解する. $\Leftrightarrow \mathfrak{p}'_A$ 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 連による様子は $8 \mid h^+$ の必要十分条件が見通しよく統一的に得られる.

例 1. $D = pf$, $p \equiv f \equiv 1 \pmod{4}$ のとき

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

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

例 2. $D = p(-f)$, $p \equiv -f \equiv 1 \pmod{4}$ のとき

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

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

§4. Divisibility by 16. 以後 $8 \mid h^+$ とする. 従って, $H^+/(H^+)^8$ は位数 8 の巡回群と見る. $(H^+)^8$ に対応する K の不分裂 8 次巡回拡大体を K_8 とする. K_8 は \mathbb{Q} 上 normal で $\text{Gal}(K_8/\mathbb{Q}) \simeq D_{16}$ (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, $K_8 = K_4(\sqrt{\alpha_2}) (= K_4 A_4)$ と見るものが存在する.

$8 \mid h^+$ より, A_2/A において, φ_A は分裂, φ'_A は完全分解するから, A_2 において, $\varphi_A = Q^2$, $\varphi'_A = Q'Q''$ と素イデアル分解される. さらに, A_4/A_2 において, Q' は分裂, その他の素イデアルは不分裂とする. このとき, 前の § と同様に: $16 \mid h^+ \Leftrightarrow \varphi_B \in (H^+)^8 \Leftrightarrow \varphi_B$ 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. : と見る. 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 $(\alpha_2) = Q'^{h_2}$, $\alpha_2 = -4$ ならば $\alpha_2 = \varepsilon_2$ (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.

定理 1. $D = p\delta$, $p \equiv \delta \equiv 1 \pmod{4}$, $4 \mid h^+$ とすると

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

<4>

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

⇔ 存在する $x, y, x', y' \in \mathbb{Z}$ が存在する。このとき

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

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

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

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

⇔ 存在する $x', y' \in \mathbb{Z}$ が存在する。このとき

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

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

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

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

⇔ 存在する $x, y \in \mathbb{Z}$ が存在する。このとき

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

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

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

$$\begin{cases} x^2 + f y^2 = 2^{2+\tilde{h}} \\ x \equiv 1 \pmod{4} \end{cases} \quad \tilde{h} = \begin{cases} h(-f) & \text{if } h(-f) \geq 5 \\ 5 & \text{if } h(-f) = 1 \\ 9 & \text{if } h(-f) = 3 \end{cases}$$

⇔ 存在する $x, y \in \mathbb{Z}$ が存在する。このとき

$$8 \mid h^+ \Leftrightarrow x \equiv 1 \pmod{8}$$

$$16 \mid h^+ \Leftrightarrow x \equiv 1 \pmod{16}$$

References.

L. Rédei - H. Reichardt : Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. reine angew. Math. 170 (1937), 69-74.

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

" : Crelle 241 (1970) 1-6.

" : J. Number Theory 1 (1969) 231-234 te.

P. Barrucand - H. Cohn : Crelle 238 (1969) 67-70. te.