

ある種のクラス2拡大における素イデアル分解について

富山医薬大 白井 進

§ 1. 有理数体上のクラス2拡大に関する結果のまとめと
問題及び答の形.

クラス2拡大というのは, その Galois 群が中零群としてクラス2であるような Galois 拡大のことである. 始めに, Fröhlich [2], Shirai [12], [13] に従って, 有理数体 $\mathbb{Q}$ 上のクラス2拡大の Galois 群についての結果をまとめる. 「有理的に」という言葉をしばしば用いるが, それは基礎体だけの概念を用いてという意味である.

m を自然数, K_m を m 円分体, $\mathfrak{f}_m$ を $K_m/\mathbb{Q}$ の Geschlechtermodul, $\hat{K}_m$ を K_m の Strahl 類体 $\text{mod } \mathfrak{f}_m$ に含まれた $K_m/\mathbb{Q}$ の最大の中心的拡大とする. $\hat{K}_m$ を $K_m/\mathbb{Q}$ の central class field $\text{mod } m p_\infty$ という (p_∞ は $\mathbb{Q}$ の実無限素因子). 明らかに, $\hat{K}_m/\mathbb{Q}$ はクラス2拡大である. この $\hat{K}_m$ に関して以下の結果が知られている.

[定理 A] ([2], [13, Theorem A])

$L/\mathbb{Q}$ を任意の有限次クラス 2 拡大とすると, $\hat{K}_m \supset L$ となる自然数 m が存在する.

つまり $\hat{K}_m$ は $\mathbb{Q}$ 上のクラス 2 拡大全体の中で, Strahl 類体に相当する役割を演じている. 従って, $\mathbb{Q}$ 上のクラス 2 拡大に関する事柄はこの $\hat{K}_m$ について決定すれば十分である.

[定理 B] ([2, Theorem 3], [12, Theorem 32])

m の素因数分解が $m = 2^{\nu} q_1^{\alpha_1} \cdots q_r^{\alpha_r}$, $\nu \geq 3$ ならば,

$$\text{Galois 群 } G(\hat{K}_m/K_m) \cong H^3(G(K_m/\mathbb{Q}), \mathbb{Z}).$$

($\mathbb{Z}$ は有理整数の加法群. $\nu = 3$ のときには, 右辺は位数 2 のある部分群で割られる)

この結果と円分体における Hasse の積公式の使用によって, Galois 群 $G(\hat{K}_m/\mathbb{Q})$ を有理的に決定することが出来る.

[定理 C] ([2, Theorem 4], [13, Theorem 6])

$G(\hat{K}_m/\mathbb{Q})$ は generator と relation の言葉で有理的に記述される.

次に問題になるのは, $\hat{K}_m$ における有理素数の分解法則(様式)の決定であるが, これについては以下の様になる.

$$\text{Ord}(m, p) = \text{order of } p \text{ mod } m,$$

$$H = K_m/\mathbb{Q} \text{ に関する total norm residue の群,}$$

$$S(m) = \{ a \in \mathbb{Q}^* \mid a \equiv 1 \pmod{m p_\infty} \},$$

$$\varphi(m) = \prod_{p|m} (1 - \zeta_p) \quad , \quad \zeta_m \text{ は } 1 \text{ の原始 } m \text{ 乗根,}$$

$$S(\eta(m)) = \{ \alpha \in K_m^* \mid \alpha \equiv 1 \pmod{\eta(m)} \},$$

$$N_{K_m/\mathbb{Q}} = \text{Norm 写像}$$

とおく,

[定理' D] ([12, Lemma 28]) m を割らない有理素数 p は $\hat{K}_m$ において不分岐である. そして $p^{\text{Ord}(m,p)}$ の $H \cap S(m) / N_{K_m/\mathbb{Q}} S(\eta(m))$ における order を f とすると, p は $\hat{K}_m$ において $\text{Ord}(m,p)f$ 次の素 ideal の積に分解する.

この定理で満足してしまえば, それで御仕舞であるが「有理的に」という見地からは不十分である. というのは分子の $H \cap S(m)$ は有理的に把握可能であるが, 分母の $N_{K_m/\mathbb{Q}} S(\eta(m))$ が有理的に把握されていないからである.

本稿の目的は exponent $G(\hat{K}_m/K_m) = 2$ なるワラス拡張 $\hat{K}_m$ における有理素数 p の分解様式の有理的決定であるが, この場合の「有理的」の意味は次の様になる. この分野のこれまでの結果, 特に, $\mathbb{Q}$ 上 8 次の Galois 拡大における分解法則を扱った結果 (Rédei, Kuroda, Fröhlich, Furuta 等の文献参照) の大くは, p のある 2 次部分体における quadratic decomposition の解を経由して, 4 中剰余記号と関連している. 本稿もこの line の延長線上にある. 従って, それ上 $\hat{K}_m$ が Abelian になるある 2 次部分体における p , 又は p の中の quadratic decomposition の解を用いる. そして結果のすべてを平方剰余記号で書く. けれども都合の良いことには,

$\exp G(\hat{K}_m/K_m) = 2$ なる場合には, その解が有理的な Jacobsthal sum で表現されるのである.

§ 2. 問題を四つの場合に還元すること及び使われる道具

先ず, 定理 B の右辺の Schur multiplier の構造から, 一般の $\hat{K}_m$ は 次の四つの type の m (数体) より作られる central class field mod $m p_\infty$ の合併体として得られることが分る.

$$(1) \quad m = q_1^{\nu_1} q_2^{\nu_2}, \quad [\hat{K}_m : K_m] = (\varphi(q_1^{\nu_1}), \varphi(q_2^{\nu_2})).$$

$$(2) \quad m = 2^{\nu} q^{\nu}, \quad [\hat{K}_m : K_m] = 2.$$

$$(3) \quad m = 2^{\nu}, \quad (\nu \geq 4), \quad [\hat{K}_m : K_m] = 2.$$

$$(4) \quad K'_m = \mathbb{Q}(\zeta_{2^{\nu}} + \zeta_{2^{\nu}}^{-1}, \zeta_{q^{\nu}}), \quad (\nu \geq 3),$$

$$[\hat{K}_m : K_{2^{\nu} q^{\nu}}] = (2^{\nu-2}, \varphi(q^{\nu})).$$

但し, q_1, q_2, q は奇素数, $\varphi(\cdot)$ は Euler 関数, $(\cdot, \cdot)$ は最大公約数である. この四つの場合には, Galois 群 $G(\hat{K}_m/\mathbb{Q})$ は比較的簡単に簡単な構造を持つので, その共役類を決定することが出来る. そしてこのことと数体の範囲内での Hasse の積公式の使用によって, K_m であまり分解しない有理素数の $\hat{K}_m$ における分解様式を有理的に決定することが出来る. ([16] 参照). けれども, この群論的な手法は, 数体の範囲でよく分解する有理素数, 例えば, 完全分解するものに対しては全く無力である.

上記により, $\exp G(\hat{K}_m/K_m) = 2$ なるクラス 2 拡大 $\hat{K}_m$ における

分解様式の決定問題は、次の四つの type の m (及び K'_m) より作られる $\hat{K}_m$ (及び $\hat{K}'_m$) の場合に還元されることが分る。

$$(イ) \quad m = q_1 q_2, \quad (q_1 - 1, q_2 - 1) = 2, \quad [\hat{K}_m : K_m] = 2.$$

$$(ロ) \quad m = 2^2 q, \quad [\hat{K}_m : K_m] = 2.$$

$$(ハ) \quad m = 2^4, \quad [\hat{K}_m : K_m] = 2.$$

$$(ニ) \quad K'_m = \mathbb{Q}(\sqrt{-2}, \zeta_q), \quad [\hat{K}'_m : \mathbb{Q}(\zeta_{2^3 q})] = 2.$$

以下の各々で (ロ), (ハ), (ニ) の場合の結果を述べる。(イ) の場合は複雑になるので省略。使われる道具は、定理 C と Hasse の積公式、そして更に (ロ), (ハ) の場合には Jacobsthal [9] の結果、(ニ) の場合には Whiteman [19] の結果である。Whiteman [19] はこれらの Jacobsthal type の結果を cyclotomy の立場より統一的に誘導している。同様に (イ) の場合に必要となる Dickson-Hummitz sum のある性質も cyclotomy を用いて証明される。従って、 $\exp G(\hat{K}_m/K_m) = 2$ なるクラス 2 拡大 $\hat{K}_m/\mathbb{Q}$ における分解法則 (様式) の研究は cyclotomy に関連していると言ってよいように思われる。

以下、有理素数 p の K_m (又は $\mathbb{Q}(\zeta_{2^3 q})$) に於ける素因子の一つを常に β_p で示す。そのとき、中心拡大の故に、Artin symbol $\left(\frac{\hat{K}_m/K_m}{\beta_p} \right)$ は β_p の選択に依存しない。relative degree = 2 なので、この記号の値を ± 1 と同一視することにする。実際に問題になるのは、この記号の有理的な表現である。

§ 3. (ロ) $m = 2^2 q$ の場合の結果

$k = \mathbb{Q}(\sqrt{-1})$, $K = K_m = \mathbb{Q}(\sqrt{-1}, \zeta_q)$, $\hat{K} = \hat{K}_m$ とおく. K/k は cyclic なので, $\hat{K}/k$ は Abelian である. そして central class field mod $m p_\infty$ の定義により, $\hat{K}/k$ の導手が $f(\hat{K}/k) = q$ で与えられることが分る ([12, §2] 参照). このことが $\hat{K}/k$ に関する norm 剰余記号の計算の基礎を与える. さて $p \equiv 3 \pmod{4}$ とすると, §2 でちょっと述べた群論的方法によつて, $(\frac{\hat{K}/K}{\mathfrak{p}_p}) = 1$ なることが証明される. ここで $p \equiv 1 \pmod{4}$ とする. すると [9] により

$$p = a^2 + b^2, \quad a = \phi_2(1)/2, \quad b = \phi_2(p)/2, \quad a \equiv -1 \pmod{4}$$

と書ける. ここに g は $\text{mod } p$ の原始根の一つであり, $\phi_2(n)$ は Jacobsthal sum

$$\phi_2(n) = \sum_{h=1}^{p-1} \left(\frac{h}{p}\right) \left(\frac{h^2 + n}{p}\right), \quad \left(\frac{0}{p}\right) = 0$$

である. 但し, $(\frac{h}{p})$ は Legendre symbol. そして

$$\lambda(p) = a + b\sqrt{-1}$$

と置き, これに対し, $\hat{K}/k$ に関する Hasse の積公式を適用する. $f(\hat{K}/k) = q$ に注意して計算し, 更に両辺を $\text{Ord}(q, p)$ 乗すると

$$\left(\frac{\hat{K}/K}{\mathfrak{p}_p}\right) = \left\{ \prod_{\mathfrak{f} | \mathfrak{q}} \left(\frac{\lambda(p), \hat{K}/k}{\mathfrak{f}}\right) \right\}^{\text{Ord}(q, p)}$$

となる. 後は, この右辺を定理 C の generator で表現し, その relation を用いてそれが何時 1 になるかを調べる. $q \equiv 3$

$(\text{mod } 4)$ のときには, 更にその結果を (有理的な表現のために) $\hat{K}$ の $\mathbb{Q}$ 上の algebra としての正則表現を通じて $SL_2(\mathbb{Z}/q\mathbb{Z})$ の中で表わす. そうすると以下の様になる.

[定理] $p \equiv q \equiv 1 \pmod{4}$ のとき,

$$\left(\frac{\hat{K}/K}{\mathfrak{p}_p}\right) = \left(\frac{a+br}{q}\right)^{\text{Ord}(q,p)},$$

ここに, r は $r^2 \equiv -1 \pmod{q}$ なる有理整数である.

Furuta [7, Theorem 5.4] によれば, $p \equiv q \equiv 1 \pmod{4}$, $\left(\frac{q}{p}\right) = 1$ のとき,

$$\left(\frac{\hat{K}/K}{\mathfrak{p}_p}\right) = \left(\frac{q}{p}\right)_4 \left(\frac{p}{q}\right)_4 = [-1, q, p]$$

である. 但し, $(-)_4$ は 4 中剰余記号である. 記号 $[d_1, d_2, a]$ については, 白井・古田 [15] の後半, 古田 [8] を参照のこと. しかし, この二つの表現は Fröhlich [3, Theorem 7], 或は Burde [1] の rational biquadratic reciprocity を用いれば, 同値であることが分る.

[定理] $p \equiv 1 \pmod{4}$, $q \equiv 3 \pmod{4}$ のとき

$$[\lambda(p)] = aI + bR, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad (\because R^2 = -I)$$

とおく. このとき, $\mathfrak{p}_p$ が $\hat{K}$ において完全分解するための N.S.C. は $[\lambda(p)]^{\text{Ord}(q,p)}$ が $SL_2(\mathbb{Z}/q\mathbb{Z})$ の元として平方になることである.

$m = 2^2 q$ の場合に, あと残った素数は $\hat{K}/\mathbb{Q}$ で分岐する 2

と q である. この $\hat{K}/K$ における分解様式も同様の手法で決定される.

[定理] ([14]) β_q が $\hat{K}/K$ で不分岐であるための N.S.C. は $q \equiv 1 \pmod{4}$ であり, β_2 が $\hat{K}/K$ で不分岐であるための N.S.C. は $q \equiv 1, 7 \pmod{8}$ である.

これより, $q \equiv 1 \pmod{8}$ のとき, $2^2 q$ 円分体の類数は偶数になるが, それは知られた結果からも従う.

[定理] $q \equiv 1 \pmod{4}$ のとき

$$\left(\frac{\hat{K}/K}{\beta_q}\right) = \left(\frac{C}{q}\right), \quad C = \left(\frac{\frac{q-1}{2}}{\frac{q-1}{4}}\right) \quad (2\text{項係数}).$$

この定理の証明には, Gauss の結果

$$q = a^2 + b^2, \quad a \equiv -1 \pmod{4} \Rightarrow 2a \equiv \overline{C} \pmod{q}$$

が必要である.

[定理]

- (i) $q \equiv 1 \pmod{8}$ のとき, $r^2 \equiv -1 \pmod{q}$ なる $r \in \mathbb{Z}$ を取ると,

$$\left(\frac{\hat{K}/K}{\beta_2}\right) = \left(\frac{1+r}{q}\right)^{\text{Ord}(q,2)}$$
- (ii) $q \equiv 7 \pmod{8}$ のとき, β_2 が $\hat{K}/K$ で完全分解するための N.S.C. は $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{\text{Ord}(q,2)}$ が $SL_2(\mathbb{Z}/q\mathbb{Z})$ の元として平方となることである.

§4. (A) $m = 2^t$ の場合の結果

$K = \mathbb{Q}(\sqrt{-1})$, $K = K_m = \mathbb{Q}(S_{2^t})$, $\hat{K} = \hat{K}_m$ とおく. $\hat{K}/K$ は Abelian

であり, それは $\text{mod } 2^3$ で定義される. $p \equiv 3 \pmod{4}$ とすると, §3 と同じく $(\frac{\hat{K}/K}{\mathfrak{p}_p}) = 1$ となるので, $p \equiv 1 \pmod{4}$ とする. そのとき, §3 の $\lambda(p)$ が定義される. この $\lambda(p)$ に対して, $\hat{K}/\mathbb{Q}$ に関する Hasse の積公式を適用するわけだが, 今度は $f(\hat{K}/\mathbb{Q}) | 2^3$ なので, $\mathbb{Q}$ における $\text{mod } 2^3$ の既約剰余類群の basis の素ideal $(1-\sqrt{-1})$ に関する norm 剰余記号を計算する必要がある. このことにのみ注意すれば, おもむきよと同じである. 結果は

[定理]

- (i) $p \not\equiv 1 \pmod{2^4}$ ならば, $(\frac{\hat{K}/K}{\mathfrak{p}_p}) = 1$
- (ii) $p \equiv 1 \pmod{2^4}$ のとき, $(\frac{\hat{K}/K}{\mathfrak{p}_p}) = 1$ となるための N.S.C. は $\phi_2(g) \equiv 0 \pmod{2^4}$ である. ここに g は $\text{mod } p$ の原始根であり, $\phi_2(\cdot)$ は Jacobsthal sum である. そして $p \equiv 1 \pmod{2^3}$ ならばつねに $\phi_2(g) \equiv 0 \pmod{2^3}$ である.
- (iii) 2 は $\hat{K}/\mathbb{Q}$ で totally ramified する.

§ 5. (二) $K'_m = \mathbb{Q}(\sqrt{-2}, 3q)$ の場合の結果

$\mathbb{Q} = \mathbb{Q}(\sqrt{-2})$, $K = \mathbb{Q}(\sqrt{-2}, 3q)$, $\hat{K}' = \hat{K}'_m$ とおく. $\hat{K}'/\mathbb{Q}$ は Abelian であり, それは $\text{mod } 2\sqrt{-2}q$ で定義される. $p \not\equiv 1 \pmod{8}$ のときは容易なので, $p \equiv 1 \pmod{8}$ としてよい. このとき [19] によ

$$(*) \quad \begin{cases} p = a^2 + 2b^2 \\ a = \phi_4(1)/4, \quad b = \phi_4(2)/4, \quad a \equiv (-1)^{\frac{p-1}{8}+1} \pmod{4} \end{cases}$$

9

と書ける. そこで, $\lambda(p) = a + b\sqrt{-2}$ とおき, この $\lambda(p)$ に対して $\hat{K}/K$ に関する Hasse の積公式を適用する. あとは $\mathfrak{p}$ と同じであるが, この場合には Galois 群 $G(\hat{K}/Q)$ の relation が複雑になるので, その分だけ結果も面倒になる.

[定理] $p \equiv 1 \pmod{8}$ とする. このとき, $q \equiv 1, 3 \pmod{8}$ ならば,

$$\left(\frac{\hat{K}/K}{\mathfrak{p}} \right) = \left\{ (-1)^{\frac{q-1}{2} \cdot \frac{p+7}{8}} \left(\frac{a+b\gamma}{q} \right) \right\}^{\text{Ord}(q,p)}$$

である. ここに a, b は (*) によって定義された有理的な量であり, γ は $\gamma^2 \equiv -2 \pmod{q}$ なる有理整数である.

[定理] $p \equiv 1 \pmod{8}$ とする. (*) の a, b を用いて

$$[\lambda(p)] = aI + bR, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad R = \begin{bmatrix} 0 & -2 \\ 1 & 0 \end{bmatrix} \quad (\because R^2 = -2I)$$

とおく.

(i) $q \equiv 7 \pmod{8}$ のとき, $\mathfrak{p}$ が $\hat{K}/K$ で完全分解するための N.S.C. は $[\lambda(p)]^{\text{Ord}(q,p)}$ が $SL_2(\mathbb{Z}/q\mathbb{Z})$ の元として平方になることである.

(ii) $q \equiv 5 \pmod{8}$ のとき, $\frac{p+7}{8} \text{Ord}(q,p) \equiv 0 \pmod{2}$ ならば, $\mathfrak{p}$ が $\hat{K}/K$ で完全分解するための N.S.C. は $[\lambda(p)]^{\text{Ord}(q,p)}$ が $SL_2(\mathbb{Z}/q\mathbb{Z})$ の元として平方になり且 $[\lambda(p)]^{\text{Ord}(q,p)} \neq -I$ となることである.

(iii) $q \equiv 5 \pmod{8}$ のとき, $\frac{p+7}{8} \text{Ord}(q,p) \equiv 1 \pmod{2}$ ならば, $\mathfrak{p}$ が $\hat{K}/K$ で完全分解するための N.S.C. は $[\lambda(p)]^{\text{Ord}(q,p)}$ が SL_2

$(\mathbb{Z}/q\mathbb{Z})$ の元の平方とならないか, 又は $[\lambda(p)]^{\text{Ord}(q,p)} = -1$ となることである.

次に $\hat{K}'/\mathbb{Q}$ で分岐する 2 と q の分解様式について述べる.

[定理] ([14]) $\mathfrak{p}_2$ が $\hat{K}'/\mathbb{K}$ で不分岐であるための N. S. C. は $q \equiv 1, 7 \pmod{8}$ であり, $\mathfrak{p}_q$ が $\hat{K}'/\mathbb{K}$ で不分岐であるための N. S. C. は $q \equiv 1, 3 \pmod{8}$ である.

[定理]

(i) $q \equiv 1 \pmod{8}$ のとき, $r^2 \equiv -2 \pmod{q}$ なる $r \in \mathbb{Z}$ に対して

$$\left(\frac{\hat{K}'/\mathbb{K}}{\mathfrak{p}_2}\right) = \left(\frac{r}{q}\right)^{\text{Ord}(q,2)}$$

(ii) $q \equiv 7 \pmod{8}$ のとき, $\mathfrak{p}_2$ が $\hat{K}'/\mathbb{K}$ で完全分解するための N. S. C. は $\begin{bmatrix} 0 & -2 \\ 1 & 0 \end{bmatrix}^{\text{Ord}(q,2)}$ が $SL_2(\mathbb{Z}/q\mathbb{Z})$ の元として平方になることである.

[定理]

(i) $q \equiv 1 \pmod{8}$ のとき,

$$\left(\frac{\hat{K}'/\mathbb{K}}{\mathfrak{p}_q}\right) = \left(\frac{c}{q}\right), \quad c = \left(\frac{\frac{q-1}{2}}{\frac{q-1}{4}}\right) \quad (2 \text{ 項係数}).$$

(ii) $q \equiv 3 \pmod{8}$ のとき, $\mathfrak{p}_q$ は $\hat{K}'$ で 2 次の素 ideal に留まる.

この定理の (i) を証明するには, Stern [18] の結果

$$q = a^2 + 2b^2, \quad a \equiv (-1)^{\frac{q-1}{8}+1} \pmod{4} \Rightarrow 2a \equiv -c \pmod{q}$$

が必要である.

最後に, 一般のクラス 2 拡大 K_m における分解法則 (様式) に

ついで少し触れる。§2で述べたように、問題は(イ)、(ロ)、(ハ)、(ニ)の場合に還元される。この内、(ロ)、(ハ)の場合は(ロ'), (ハ')の場合より容易に従う。(ニ)の場合も p のある中の norm 形式による表現の解を用いれば、本稿の方法がそのまま適用出来る。但し、その解が有理的には表現出来ないのだが、残った(イ)の場合については、今の所全く分らない。

参考文献

- [1] K. Burde, Ein rationales biquadratisches Reziprozitätsgesetz, J. Reine Angew. Math., 235 (1969), 175-184.
- [2] A. Fröhlich, On fields of class two, Proc. London Math. Soc., (3), 4 (1954), 235-256.
- [3] ———, The restricted biquadratic residue symbol, Proc. London Math. Soc., (3), 9 (1959), 189-207.
- [4] ———, A prime decomposition symbol for certain non Abelian number fields, Acta Sci. Math., 21 (1960), 229-246.
- [5] Y. Furuta, A reciprocity law of the power residue symbol, J. Math. Soc. Japan, 10 (1958), 46-54.
- [6] ———, Note on class number factors and prime de-

- compositions, Nagoya Math. J., 66 (1977), 167-182.
- [7] ———, A prime decomposition symbol for a non-abelian central extension which is abelian over a bi-cyclic biquadratic field, Nagoya Math. J., 79 (1980), 79-109.
- [8] 古田孝臣, 素イデアル分解記号と整係数2次形式 (Hookeyの結果の応用), 整数論研究会報告集 (於金沢大学理学部), (1980), 99-106.
- [9] E. Jacobsthal, Über die Darstellung der Primzahlen der Form $4n+1$ als Summe zweier Quadrate, J. Reine u. Angew. Math., 132 (1907), 238-245.
- [10] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern, J. Math. Soc. Japan, 3 (1) (1951), 148-156.
- [11] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, J. Reine Angew. Math., 180 (1939), 1-43.
- [12] S. Shirai, On the central class field mod m of Galois extensions of an algebraic number field, Nagoya Math. J., 71 (1978), 61-85.
- [13] ———, On Galois groups of class two extensions

over the rational number field, *Nagoya Math. J.* 75 (1979), 121-131.

- [14] ———, On the central ideal class group of cyclotomic fields, *Nagoya Math. J.*, 75 (1979), 133-143.
- [15] 白井・古田, 代数体の中心的拡大について, 第25回代数学シンポジウム報告集, (1979), 36-54.
- [16] 白井 進, ある種の条件を満足する有理素数の class 2 拡大に於ける分解法則について, 日本数学会代数学分科会講演アブストラクト, (1979年10月), 98-99.
- [17] ———, On the decomposition laws of rational primes in certain class 2-extensions (投稿予定).
- [18] M. Stern, Eine Bemerkung zur Zahlentheorie, *J. Reine Angew. Math.*, 32 (1846), 89-90.
- [19] A. L. Whiteman, Theorems analogous to Jacobsthal's theorem, *Duke Math. J.*, 16 (1949), 619-626.
- [20] ———, Cyclotomy and Jacobsthal sums, *Amer. J. Math.*, 74 (1952), 89-99.