J. Korean Math. Soc. **42** (2005), No. 2, pp. 203–222

CLASS FIELDS FROM THE FUNDAMENTAL THOMPSON SERIES OF LEVEL $N = o(g)$

So Young Choi and Ja Kyung Koo

Abstract. Thompson series is a Hauptmodul for a genus zero group which lies between $\Gamma_0(N)$ and its normalizer in $PSL_2(\mathbb{R})$ ([1]). We construct explicit ring class fields over an imaginary quadratic field K from the Thompson series $T_g(\alpha)$ (Theorem 4), which would be an extension of [3], Theorem 3.7.5 (2) by using the Shimura theory and the standard results of complex multiplication. Also we construct various class fields over K, over a CM-field $K(\zeta_N + \zeta_N^{-1})$, and over a field $K(\zeta_N)$. Furthermore, we find an explicit formula for the conjugates of $T_g(\alpha)$ to calculate its minimal polynomial where $\alpha(\in \mathfrak{H})$ is the quotient of a basis of an integral ideal in K.

1. Introduction

The main purpose of this paper is to study the class fields generated by singular values of Thompson series T_g at imaginary quadratic arguments in the complex upper half plane $\mathfrak{H}$, over K, CM-field $K(\zeta_N+\zeta_N^{-1})$ and $K(\zeta_N)$. To this end, we recall the classical results on singular moduli of the elliptic modular function j for $SL_2(\mathbb{Z})$ evaluated at imaginary quadratic arguments ([2], [5], [9], [11]). Let K be an imaginary quadratic field over $\mathbb{Q}$ of discriminant d_K and $\mathcal{O}$ be an order of K of conductor f, discriminant $f^2 d_K$ and class number $h(\mathcal{O})$. Let $\alpha \in \mathfrak{H} \cap \mathcal{O}$ be an imaginary quadratic argument. Then a singular modulus $j(\alpha)$ generates the ring class field L of $\mathcal{O}$ (the Hilbert class field if $\mathcal{O}$ is the maximal order of K).

Helling showed in [6] that the group $\Gamma_0(N)^*$ generated by $\{\Gamma_0(N), \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\}$ has a genus zero exactly for $N = 1 \sim 21, 23 \sim 27, 29, 31, 32, 35, 36, 39, 41, 47, 49, 50, 59, 71$. Moreover, for all such N but 49 and 50,

Received August 6, 2003.
2000 Mathematics Subject Classification: 11F11, 11R04, 11R37.
Key words and phrases: modular functions, Thompson series, class fields.
This work was Supported by KOSEF Research Grant 98-0701-01-01-3.

$\Gamma_0(N)^*$ has a fundamental Thompson series $T_N^*(\alpha)$ corresponding to itself, that is, $T_N^*(\alpha)$ is defined by an element of order N of the Monster group ([4], Table 2). Throughout this paper, we denote α to be a root in $\mathfrak{H}$ of a quadratic equation $az^2 + bz + c = 0$ with $(a, b, c) = 1$ and $a > 0$, and K as an imaginary quadratic field $\mathbb{Q}(\alpha)$. Chen-Yui ([3], Theorem 3.7.5 (2)) showed by using the Shimura reciprocity law that when $(a, N) = 1$, $T_N^*(\alpha)$ generates a ring class field over K.

In §2, we first construct some sort of class fields with $\Gamma_0(N)^*$ by means of Shimura's ideas.

Next in §3, we generate a ring class field $K(T_N^*(\alpha))$ over K under the condition $(a, b, N) \neq N$ or $(\frac{a}{N}, N) \neq 1$. This further generalizes Chen-Yui's result under the assumption $(a, N) = 1$.

On the other hand, it has been known that there exists a fundamental Thompson series T_g of level $N = o(g)$ exactly when $N = 1 \sim 36, 38, 39, 41, 42, 44 \sim 47, 49, 50, 51, 54 \sim 56, 59, 60, 62, 66, 69 \sim 71, 78, 87, 92, 94, 95, 105, 110, 119$ ([4], table 2) where $o(g)$ is the order of element g of the Monster group. In §4, we will construct, from such $T_g, \zeta_N + \zeta_N^{-1}$ *or* ζ_N, not only various class fields over K which are neither ray class fields of conductor N nor ring class fields of order $\mathcal{O}$ with discriminant $N^2 d_K$, but also ray class fields of conductor N by applying Chen-Yui's method. We also demonstrate what sort of class field $T_g(\alpha)$ generates over a CM-field $K(\zeta_N + \zeta_N^{-1})$ and over a field $K(\zeta_N)$.

In §5, we explore an explicit formula for the conjugates of $T_g(\alpha)$ to calculate its minimal polynomial.

Throughout the article we adopt the following notations:

- $\Gamma = SL_2(\mathbb{Z})$
- $\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) | c \equiv 0 \bmod N\}$
- $\Gamma_0(N)^* = \langle \{\Gamma_0(N), \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\} \rangle$
- $\mathbb{Z}_p$ the ring of p-adic integers
- $\mathbb{Q}_p$ the field of p-adic numbers
- $\mathfrak{H}$ upper half complex plane
- $\zeta_N = e^{2\pi i/N}$
- $i = \sqrt{-1}$
- T_N^* a fundamental Thompson series for a genus zero group $\Gamma_0(N)^*$
- T_g a fundamental Thompson series of level $N = o(g)$
- $x \underset{SL_2(\mathbb{Z})}{\sim} y$ means that $x = \gamma y$ for some $\gamma \in SL_2(\mathbb{Z})$
- G_α the stabilizer of α for a group G

2. Class fields obtained by applying Shimura's method

Let Γ be a Fuchsian group of the first kind. Then $X(\Gamma) = \Gamma\backslash\mathfrak{H}^*$ is a compact Riemann surface. Hence there exists a projective nonsingular algebraic curve V_Γ, defined over $\mathbb{C}$, biregularly isomorphic to $\Gamma\backslash\mathfrak{H}^*$. We specify a Γ-invariant holomorphic map φ_Γ of $\mathfrak{H}^*$ to V_Γ which gives a biregular isomorphism of $\Gamma\backslash\mathfrak{H}^*$ to V_Γ. In that situation, we call $(V_\Gamma, \varphi_\Gamma)$ a *model* of $\Gamma\backslash\mathfrak{H}^*$. Through this article we always assume that the genus of $\Gamma\backslash\mathfrak{H}^*$ is zero. Then it's function field $K(X(\Gamma))$ is equal to $\mathbb{C}(J')$ for some $J' \in K(X(\Gamma))$ and the pair $(\mathbb{P}^1(\mathbb{C}), J')$ is a model of $\Gamma\backslash\mathfrak{H}^*$ ([7], Lemma 14).

Let $G_{\mathbb{A}}$ be the adelization of an algebraic group $G = GL_2$ defined over $\mathbb{Q}$.
Put

$$\begin{aligned} G_p &= GL_2(\mathbb{Q}_p) \ (p : \text{rational prime}), \\ G_\infty &= GL_2(\mathbb{R}), \\ G_{\infty+} &= \{x \in G_\infty | \det(x) > 0\}, \\ G_{\mathbb{Q}_+} &= \{x \in GL_2(\mathbb{Q}) | \det(x) > 0\}. \end{aligned}$$

We define the topology of $G_{\mathbb{A}}$ by taking $U = \prod_p GL_2(\mathbb{Z}_p) \times G_{\infty+}$ to be an open subgroup of $G_{\mathbb{A}}$. Let K be an imaginary quadratic field and ξ_z be an embedding of K into $M_2(\mathbb{Q})$. We call ξ_z *normalized* if it is defined by $a\binom{z}{1} = \xi_z(a)\binom{z}{1}$ for $a \in K$ where z is the fixed point of $\xi_z(K^\times)$ $(\subset G_{\mathbb{Q}_+})$ in $\mathfrak{H}$. Observe that the embedding ξ_z defines a continuous homomorphism of $K_{\mathbb{A}}^\times$ into $G_{\mathbb{A}+}$, which we denote again by ξ_z. Here $G_{\mathbb{A}+}$ is the group $G_0 G_{\infty+}$ with G_0 the non-archimedean part of $G_{\mathbb{A}}$ and $K_{\mathbb{A}}^\times$ is the idele group of K. Let $\mathcal{Z}$ be the set of open subgroups S of $G_{\mathbb{A}+}$ containing $\mathbb{Q}^\times G_{\infty+}$ such that $S/\mathbb{Q}^\times G_{\infty+}$ is compact. For $S \in \mathcal{Z}$, we see that $\det(S)$ is open in $\mathbb{Q}_{\mathbb{A}}^\times$. Therefore the subgroup $\mathbb{Q}^\times \det(S)$ of $\mathbb{Q}_{\mathbb{A}}^\times$ corresponds to a finite abelian extension of $\mathbb{Q}$, which we write k_S. Put $\Gamma_S = S \cap G_{\mathbb{Q}_+}$ for $S \in \mathcal{Z}$. As is well known ([11], Proposition 6.27), $\Gamma_S/\mathbb{Q}^\times$ is a Fuchsian group of the first kind commensurable with $PSL_2(\mathbb{Z})$. Let

$$U^0 = \{x = (x_p) \in U | x_p \in U_p^0 \text{ for all finite } p\}$$

and

$$U_*^0 = U^0 \cup U^0 \Phi(N),$$

where

$$U_p^0 = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z}_p) | c \equiv 0 \bmod N\mathbb{Z}_p\},$$

$$\Phi(N) = (x_p) \in G_{A+} \text{ and } x_p = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right).$$

Then we have

LEMMA 1. (i) $\mathbb{Q}^\times U_*^0 \in \mathcal{Z}$,
(ii) $k_S = \mathbb{Q}$,
(iii) $\Gamma_S = \mathbb{Q}^\times \Gamma_0(N)^*$ *if* $S = \mathbb{Q}^\times U_*^0$.

Proof. Since $\mathbb{Q}^\times U_*^0 = \mathbb{Q}^\times U^0 \cup \mathbb{Q}^\times U^0 \Phi(N)$ and $\mathbb{Q}^\times U^0$ is an open subgroup in G_{A+}, $\mathbb{Q}^\times U_*^0$ is also an open subgroup in G_{A+}. Observing that $\mathbb{Q}^\times U^0/\mathbb{Q}^\times G_{\infty+}$ is compact, we obtain $\mathbb{Q}^\times U_*^0 \in \mathcal{Z}$. As for (ii), we see that $\mathbb{Q}$ corresponds to the norm group $\mathbb{Q}^\times \mathbb{Q}_{\mathbb{A}}^{\times\infty}$ with $\mathbb{Q}_{\mathbb{A}}^{\times\infty} = \mathbb{R}^\times \prod_p \mathbb{Z}_p^\times$ and $\det(U_*^0) = N\det(U^0)$. But $\det(U^0) = \mathbb{Q}_{\mathbb{A}}^{\times\infty}$ and hence by the class field theory $k_S = \mathbb{Q}$. Indeed, clearly $\det(U^0)$ is contained in $\mathbb{Q}_{\mathbb{A}}^{\times\infty}$. Conversely, for any element $(\alpha_p) \in \mathbb{Q}_{\mathbb{A}}^{\times\infty}$, take $y_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \alpha_p \end{smallmatrix}\right)$, then $(y_p) \in U_0$ and $\det(y_p) = (\det y_p) = (\alpha_p)$. Lastly, we readily get that $\Gamma_S = \mathbb{Q}^\times U_*^0 \cap G_{\mathbb{Q}+} = \mathbb{Q}^\times \left(U_*^0 \cap G_{\mathbb{Q}+}\right) = \mathbb{Q}^\times \Gamma_0(N)^*$ □

THEOREM 2. *Let K be an imaginary quadratic field. For fixed $z \in K \cap \mathfrak{H}$, let ξ_z be the normalized embedding. Then $T_N^*(z)$ belongs to the maximal abelian extension K^{ab} of K and $K(T_N^*(z))$ is the class field of K corresponding to the subgroup $K^\times \cdot \xi_z^{-1}(\mathbb{Q}^\times U_*^0)$ of $K_{\mathbb{A}}^\times$.*

Proof. We have $k_S = \mathbb{Q}$ and $\Gamma_S = \mathbb{Q}^\times \Gamma_0(N)^*$ by Lemma 1. Since T_N^* gives a model of $X(\Gamma_0(N)^*)$, the assertion follows from [11] Proposition 6.31 and Proposition 6.33. □

3. Ring class fields generated by singular values of T_N^*

In this section, we obtain Theorem 4 which would be an extension of [3], 3.7.5 Theorem(2) by using Shimura's method and the standard results of complex multiplication. To this end, we need the following fact.

THEOREM 3. *Let $\mathfrak{F}_N$ be the field of modular functions of level N rational over $\mathbb{Q}(e^{2\pi i/N})$, and let K be an imaginary quadratic field. Let $\mathcal{O}_K$ be the maximal order of K and $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal such that $\mathfrak{a} = [z_1, z_2]$ and $\alpha = z_1/z_2 \in \mathfrak{H}$. Then the field $K\mathfrak{F}_N(\alpha)$ generated over K by all values $f(\alpha)$ with $f \in \mathfrak{F}_N$ and f defined at α, is the ray class field $K_{(N)}$ over K with modulus N.*

Proof. [9], Ch. 10, Corollary of Theorem 2. □

By class field theory, the reciprocity map induces an isomorphism

$$[\cdot, K] : K_{\mathbb{A}}^\times / K^\times U_{(N)} \xrightarrow{\sim} \mathrm{Gal}(K_{(N)}/K)$$

where $U_{(N)}$ is the subgroup of $K_{\mathbb{A}}^{\times}$ given by

$$U_{(N)} = \{s \in K_{\mathbb{A}}^{\times} \mid s_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ and } s_{\mathfrak{p}} \equiv 1 \bmod N\mathcal{O}_{\mathfrak{p}} \text{ for all finite primes } \mathfrak{p}\}.$$

For a subfield L of $K_{(N)}$, let

$$\Phi_{L/K} : I_K(N) \longrightarrow \mathrm{Gal}(L/K)$$

denote the Artin map. Then $\mathrm{Ker}(\Phi_{K_{(N)}/K}) = P_{K,1}(N)$, where $I_K(N)$ is the ideal group generated by all fractional ideals in K prime to N and $P_{K,1}(N)$ denotes the subgroup of $I_K(N)$ generated by the principal ideals $\beta\mathcal{O}_K$ with $\beta \in \mathcal{O}_K$ and $\beta \equiv 1 \bmod N\mathcal{O}_K$. Of course, $\mathcal{O}_K$ is the ring of integers in K.

THEOREM 4. *Let T_N^* be a fundamental Thompson series for a genus zero group $\Gamma_0(N)^*$. Let α be a root in $\mathfrak{H}$ of a quadradic equation $az^2 + bz + c = 0$ such that $a > 0, (a, b, c) = 1$, and $b^2 - 4ac = m^2 d_K < 0$ $(m > 0)$. Let $K = \mathbb{Q}(\alpha)$ and $\mathcal{O}$ $(= \mathbb{Z}[a\alpha])$ be an order in K of discriminant $m^2 d_K$. Assume that $(a, b, N) \neq N$ or $(\frac{a}{N}, N) \neq 1$. Then $K(T_N^*(\alpha))$ is a ring class field of an imaginary quadratic order $\mathcal{O}'$ of discriminant $f^2 d_K$ where $f = mN/(a, N)$ and d_K is the discriminant of K.*

Proof. First of all, we describe the action of arbitrary prime deal $\wp$ of $\mathcal{O}_K$ on $T_N^*(\alpha)$ under the Artin map $\Phi_{K(T_N^*(\alpha))/K}$ which is guaranteed by Theorem 4. Take a rational prime p which does not divide $2abcmN$ and splits in K. Then $p\mathcal{O}_K = \wp\wp'$, where $\wp = (p, \frac{-r+m\sqrt{d_K}}{2})$, $r^2 = m^2 d_K \bmod p$ and $r \in \mathbb{Z}$ with $b - r$ and $b + r$ both even (since $a\alpha$ is a root of the polynomial $z^2 + bz + ac = 0$ and p splits in K, there exists $r \in \mathbb{Z}$ such that $r^2 = m^2 d_K \bmod p$, $z^2 + bz + ac = (z + \frac{b-r}{2})(z + \frac{b+r}{2}) \bmod p$ and $b - r, b + r \in 2\mathbb{Z}$, and $a\alpha + \frac{b \pm r}{2} = \frac{-b+m\sqrt{d_K}}{2} + \frac{b \pm r}{2} = \frac{\pm r+m\sqrt{d_K}}{2}$). We define $v = \frac{r^2 - m^2 d_K}{4p}$ $(\in \mathbb{Z})$ and hence $\mathrm{ord}_p v = 0$.

We now take an idèle s corresponding to an ideal $\wp$ to be

$$s = (1, \cdots, \frac{-r + m\sqrt{d_K}}{2}, 1, \cdots),$$

where we put 1 at all places except the place corresponding to p. Under the embedding ξ_α: $K_{\mathbb{A}}^{\times} \to G_{\mathbb{A}+}$, s is sent to

$$\xi_\alpha(s) = (\mathbb{I}_2, \cdots, \begin{pmatrix} \frac{-b-r}{2} & -c \\ a & \frac{b-r}{2} \end{pmatrix}, \cdots)$$

because $\frac{-r+m\sqrt{d_K}}{2} = a\alpha + \frac{-r+b}{2}$ and $\frac{-r+m\sqrt{d_K}}{2}\alpha = \frac{-r-b}{2}\alpha - c$. This implies

$$\xi_\alpha(s^{-1}) = (\mathbb{I}_2, \cdots, \frac{1}{pv}\begin{pmatrix} \frac{b-r}{2} & c \\ -a & \frac{-r-b}{2} \end{pmatrix}, \cdots).$$

Let $p_a^{-1}, k, p_N^{-1}, l \in \mathbb{Z}$ be such that $ak + pp_a^{-1} = 1$ and $Nl + pp_N^{-1} = 1$. Then

$$\begin{aligned}\xi_\alpha(s^{-1}) &= (\begin{pmatrix} p & \frac{-(r+b)kNl}{2} \\ 0 & 1 \end{pmatrix}, \cdots, \frac{1}{v}\begin{pmatrix} \frac{b-r}{2} & \frac{v}{a} \\ -a & 0 \end{pmatrix}\begin{pmatrix} 1 & \frac{(r+b)(1-kNla)}{2ap} \\ 0 & 1 \end{pmatrix}, \cdots) \\ &\quad \cdot \begin{pmatrix} \frac{1}{p} & \frac{(r+b)kNl}{2p} \\ 0 & 1 \end{pmatrix} \\ &= u \cdot g.\end{aligned}$$

Since $1 - kNla = p(akp_N^{-1} + p_a^{-1}Nl + pp_a^{-1}p_N^{-1})$, $u = (u_q) \in U$ and $g \in GL_2^+(\mathbb{Q})$. Notice that $u_q \equiv \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod NM_2(\mathbb{Z}_q)$ for every finite prime q and define

$$\widetilde{U_N} = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \text{ and } \widetilde{\mathcal{A}_N} = \begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix}\widetilde{U_N} \in SL_2(\mathbb{Z}/N\mathbb{Z}).$$

Lift $\widetilde{\mathcal{A}_N}$ to a matrix $\mathcal{A}_N$ in $\Gamma_0(N)$. By the Shimura reciprocity law, we get

$$\begin{aligned} T_N^*(\alpha)^{[\wp, K_{ab}/K]} &= T_N^{*\tau(\xi_\alpha(s^{-1}))}(\alpha) &&= T_N^{*\tau(u)\tau(g)}(\alpha) \\ &= T_N^*(A_N g\alpha) &&= T_N^*(g\alpha) \\ &= T_N^*(\begin{pmatrix} 1 & \frac{(r+b)kNl/2}{p} \\ 0 & p \end{pmatrix}\alpha). \end{aligned}$$

Let $\mathcal{A}$ be a matrix $\begin{pmatrix} 1 & \frac{(r+b)kNl/2}{p} \\ 0 & p \end{pmatrix}$ and suppose that $T_N^*(\alpha)^{[\wp, K_{ab}/K]} = T_N^*(\alpha)$. Then

$$\mathcal{A} \in \Gamma_0(N)^* GL_2(\mathbb{Q})_\alpha^+.$$

If $\mathcal{A}$ is contained in $\Gamma_0(N)\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) GL_2^+(\mathbb{Q})_\alpha$, then $\mathcal{A} = \gamma\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} \frac{x}{N} & \frac{y}{N} \\ z & w \end{smallmatrix}\right)$ for some $x, y, z, w \in \mathbb{Z}$ and $\gamma \in \Gamma_0(N)$ with $x\frac{\alpha}{N} + \frac{y}{N} = (z\alpha + w)\alpha$. We also see that $\frac{Nz}{a} = \frac{Nw-x}{b} = \frac{-y}{c} := \lambda \in \mathbb{Z}\backslash\{0\}$ and (λ,N)=1 (because if $\lambda = 0$, then $w = \pm\sqrt{p/N} \notin \mathbb{Z}$. This implies that λ is not zero. We now set $\lambda = \frac{\square}{\triangle}$ with $\square, \triangle \in \mathbb{Z}\backslash\{0\}, (\square, \triangle) = 1$, then $\triangle | (a, b, c) = 1$ and hence $\lambda \in \mathbb{Z}$. Also, $(N, p) = 1$ and $xw - yz = (Nw - b\lambda)w + c\lambda z = p$ imply $(\lambda, N) = 1$). Here, the fact that $z = \frac{a\lambda}{N}$ is an integer means that N divides a. Moreover, since N divides x and $b\lambda = Nw - x$, N divides b and hence $(\frac{a}{N}, N) = 1$. These give a contradiction to our assumption $(a, b, N) \neq N$ or $(\frac{a}{N}, N) \neq 1$. Therefore, $\mathcal{A} \in \Gamma_0(N)M_2(\mathbb{Z})_\alpha^+$ and we can take $\gamma \in \Gamma_0(N)$ and $d, \lambda \in \mathbb{Z}$ such that

$$\mathcal{A} = \begin{pmatrix} 1 & \frac{(r+b)kNl/2}{p} \\ 0 & p \end{pmatrix} = \gamma\left(\begin{smallmatrix} d - b\lambda & -c\lambda \\ a\lambda & d \end{smallmatrix}\right)$$

and $(d - b\lambda)\alpha - c\lambda = \alpha(a\lambda + d)$. Observing $p = ac\lambda^2 - bd\lambda + d^2 = \alpha'(d - a\alpha\lambda - b\lambda) = \alpha'\overline{\alpha'}$ where $\alpha' := d + a\alpha\lambda \in \mathcal{O}(= \mathbb{Z}[a\alpha])$ and $\overline{\alpha'} \in \mathcal{O}$

is the complex conjugate of α', we obtain $p\mathcal{O}_K=(\alpha')(\overline{\alpha'}) =\wp\wp'$. That is, $\wp$ is a principal ideal generated by an element α' (or $\overline{\alpha'}$) in $\mathcal{O}$.

On the other hand, for each $\mathfrak{a} \in I_K(N)$, we can take a prime ideal $\wp \in I_K(2abcmN)$ and a principal ideal $(x) \in P_{K,1}(N)$ with $\mathfrak{a} = (x)\wp$. Indeed, if an ideal $\mathfrak{a}$ in K is prime to N, then $\mathfrak{a} = \mathfrak{a}^*(\beta)$ for some $\mathfrak{a}^* \in I_K(2abcmN)$ and $(\beta) \in P_{K,1}(N)$ ([10], Corollary 3.16 and 3.18), and the ideal $\mathfrak{a}^*$ just given can be factored into $(x)\wp$ for some prime ideal $\wp \in I_K(2abcmN)$ and $(x) \in P_{K,1}(2abcmN)$ ([8] VIII §4 ,Corollary of Theorem 8). Consequently, $\ker(\Phi_{K(T_N^*(\alpha))/K})$ is contained in a subgroup $P_{K,1}(N)(P(\mathcal{O})\cap I_K(N))$ of $I_K(N)$, where $P(\mathcal{O})$ is the group of principal $\mathcal{O}$-ideals. (Of course, we consider elements in $P(\mathcal{O})$ as $\mathcal{O}_K$-ideals.)

Let (β) be a principal ideal of $\mathcal{O}$ relatively prime to N and write $\beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z}(= \mathcal{O})$. We see from Lemma 5 below that the action of (β) on $T_N^*(\alpha)$ is represented by a matrix $\mathcal{A}_\beta \in SL_2(\mathbb{Z})$ whose image in $SL_2(\mathbb{Z}/N\mathbb{Z})$ is equal to $\begin{pmatrix} -bn+l & -cn \\ anN(\beta)^{-1} & lN(\beta)^{-1} \end{pmatrix}$. Thus, we derive that (β) fixes $T_N^*(\alpha)$ if and only if $\mathcal{A}_\beta \in \Gamma_0(N)^*GL_2(\mathbb{Q})_\alpha$. First, suppose that N does not divide a. By similar arguments as we used to show that $\mathcal{A} \in \Gamma_0(N)^*GL_2(\mathbb{Q})_\alpha^+$ implies $\mathcal{A} \in \Gamma_0(N)M_2(\mathbb{Z})_\alpha^+$, we can verify that (β) fixes $T_N^*(\alpha)$ if and only if $\mathcal{A}_\beta \in \Gamma_0(N)SL_2(\mathbb{Z})_\alpha$. But we know that $SL_2(\mathbb{Z})_\alpha$ is trivial unless α is $SL_2(\mathbb{Z})$-equivalent to $e^{2\pi i/r}$ with $r \in \{3,4\}$. Assuming $SL_2(\mathbb{Z})_\alpha = \{\pm 1\}$, we see that $\mathcal{A}_\beta \in \pm\Gamma_0(N)$ if and only if $N|an$. Therefore the principal ideals in $\mathcal{O}$ which fix $T_N^*(\alpha)$ are of the form (β) with $\mathrm{disc}(\beta)$ dividing $(mN/(a,N))^2 d_K$. But these principal ideals are all in $P(\mathcal{O}')$. The cases $\alpha \underset{SL_2(\mathbb{Z})}{\sim} e^{2\pi i/r}$ with r=3 or 4 can be treated similarly. These prove our assertion in the case that N does not divide a. Now suppose that N divides a. Then $\mathcal{A}_\beta$ fixes $T_N^*(\alpha)$ and hence $T_N^*(\alpha)$ generates the ring class field of $\mathcal{O}'$. □

LEMMA 5. *Let f be a modular function of level N with rational Fourier coefficients and (β) a principal ideal of $\mathcal{O}$ relatively prime to N. Write $\beta = n(a\alpha) + l \in \mathbb{Z}(a\alpha) + \mathbb{Z}(= \mathcal{O})$. And let $\mathcal{A}_\beta$ be a matrix in $SL_2(\mathbb{Z})$ whose image in $SL_2(\mathbb{Z}/N\mathbb{Z})$ is equal to $\begin{pmatrix} -bn+l & -cn \\ anN(\beta)^{-1} & lN(\beta)^{-1} \end{pmatrix}$. Then the action of (β) on $f(\alpha)$ is given by*

$$f(\alpha)^{[(\beta),K_{ab}/K]} = f(\mathcal{A}_\beta \cdot \alpha)$$

where $[\,\cdot\,, K_{ab}/K]$ is the Artin map.

Proof. Let (β) correspond to an idele $\mathfrak{s} = (1, \ldots; \beta, \ldots) \in K_{\mathbb{A}}{}^\times$ where we put 1 on each place dividing N and β on the other places. Under the

embedding $\xi_\alpha : {K_{\mathbb{A}}}^\times \to {G_{\mathbb{A}}}^+$, $\mathfrak{s}$ is sent to

$$\xi_\alpha(\mathfrak{s}) = \left(I_2, \begin{pmatrix} -bn+l & -cn \\ an & l \end{pmatrix}, \dots\right)$$

because $\beta \cdot \alpha = (na\alpha + l)\alpha = (-bn+l)\alpha - cn$ and $\beta \cdot 1 = na \cdot \alpha + l$. Then

$$\begin{aligned} \xi_\alpha(\mathfrak{s}^{-1}) &= \left(I_2, \frac{1}{N(\beta)} \begin{pmatrix} l & cn \\ -an & -bn+l \end{pmatrix}, \dots\right) \\ &= \left(\begin{pmatrix} -bn+l & -cn \\ an & l \end{pmatrix}, I_2, \dots\right) \cdot \frac{1}{N(\beta)} \begin{pmatrix} l & cn \\ -an & -bn+l \end{pmatrix} \\ &= u \cdot g \end{aligned}$$

where $u = \left(\begin{pmatrix} -bn+l & -cn \\ an & l \end{pmatrix}, I_2, \dots\right)$ and $g = \frac{1}{N(\beta)} \begin{pmatrix} l & cn \\ -an & -bn+l \end{pmatrix} \in G_{\mathbb{Q}_+}$. Since $\det \begin{pmatrix} -bn+l & -cn \\ an & l \end{pmatrix} = N(\beta)$ is relatively prime to N, u belongs to U. Write $u = (u_p)$. Note that u_p is congruent to $\begin{pmatrix} -bn+l & -cn \\ an & l \end{pmatrix}$ modulo $NM_2(\mathbb{Z}_p)$ for any finite prime p. Put $\widetilde{U_N} = \begin{pmatrix} -bn+l & -cn \\ an & l \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z})$ and $\overline{\mathcal{A}_\beta} = \begin{pmatrix} 1 & 0 \\ 0 & \det(\widetilde{U_N})^{-1} \end{pmatrix} \begin{pmatrix} -bn+l & -cn \\ an & l \end{pmatrix} = \begin{pmatrix} -bn+l & -cn \\ anN(\beta)^{-1} & lN(\beta)^{-1} \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$. We now lift $\overline{\mathcal{A}_\beta}$ to a matrix $\mathcal{A}_\beta$ in $SL_2(\mathbb{Z})$. Then we derive by Shimura reciprocity law

$$\begin{aligned} f(\alpha)^{[(\beta),K_{ab}/K]} &= f^{\tau(\xi_\alpha(\mathfrak{s}^{-1}))}(\alpha) = f^{\tau(u)\tau(g)}(\alpha) \\ &= f(\mathcal{A}_\beta \cdot g\alpha) \quad \text{since } f \text{ has rational Fourier coefficients} \\ &= f(\mathcal{A}_\beta \alpha) \quad \text{since } g = \xi_\alpha(\beta^{-1}). \end{aligned}$$

□

4. Class fields over an imaginary quadratic field K, CM-fields $K(\zeta_N + \zeta_N^{-1})$ and $K(\zeta_N)$

THEOREM 6. *Let T_g be a fundamental Thompson series of level $N = o(g)$. Let α be a root in $\mathfrak{H}$ of a quadratic equation $az^2 + bz + c = 0$ such that $a > 0, (a,b,c) = 1$, and $b^2 - 4ac = d_K < 0$. Let $K = \mathbb{Q}(\alpha)$ and $\mathcal{O}(N)$ be an order $\mathbb{Z} + N\mathcal{O}_K$ in K of discriminant $N^2 d_K$ and put K' be a CM-field $K(\zeta_N + \zeta_N^{-1})$. Under the assumption $(a,N) = 1$ the following assertions hold.*

(1) *$K'(T_g(\alpha))$ is a class field over K with*

$$Gal(K'(T_g(\alpha))/K) \cong I_K(N)/\widetilde{P}_K(N)$$

and

$$[K'(T_g(\alpha)) : K] = \frac{h(\mathcal{O}(N))\psi(N)}{2[\widetilde{P}_K(N) : P_{K,1}(N)]}$$

where $\widetilde{P}_K(N)$ *is a subgroup of* $I_K(N)$ *generated by all principal ideals* $\beta\mathcal{O}_K$ *such that* $\beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z}(= \mathcal{O}_K)$, $N|n$ *and* $l^2 \equiv \pm 1 \mathrm{mod} N$, *and* $\psi(1) = \psi(2) = 2$ *and* ψ *is the Euler* φ*-function for* $N \geq 3$.

(2) $T_g(\alpha)$ *generates a class field* $K'(T_g(\alpha))$ *over* K' *with*

$$Gal(K'(T_g(\alpha))/K') \cong I_{K'}(N)/N_{K'/K}^{-1}(\widetilde{P}_K(N))$$

and

$$[K'(T_g(\alpha)) : K'] = \frac{h(\mathcal{O}(N))}{[\widetilde{P}_K(N) : P_{K,1}(N)]}$$

where $h(\mathcal{O}(N))$ *is the class number of* $\mathcal{O}(N)$ *and* $I_{K'}(N)$ *is the ideal group generated by all fractional ideals in* K' *prime to* N.

Proof. In the proof of Theorem 4, take $m = 1$, give a condition $(N, a) = 1$ and replace $T_N^*(\alpha)$ by $T_g(\alpha)$. Then the arguments from the beginning to the step of letting a matrix $\mathcal{A} = \begin{pmatrix} 1 & \frac{(r+b)kNl}{2} \\ 0 & p \end{pmatrix}$ in $M_2(\mathbb{Z})$ are exactly the same as those in Theorem 4. We assume that $T_g(\alpha)^{[\mathfrak{p}, K_{ab}/K]} = T_g(\alpha)$. Then $\mathcal{A} \in \Gamma_0(N)M_2(\mathbb{Z})_\alpha^+$. Indeed, if $\mathcal{A} \in W_e GL_2^+(\mathbb{Q})_\alpha$, then $\mathcal{A}_\beta = \begin{pmatrix} Ae & B \\ CN & De \end{pmatrix} \begin{pmatrix} d - b\frac{\square}{\triangle} & -c\frac{\square}{\triangle} \\ a\frac{\square}{\triangle} & d \end{pmatrix}$ for $Ae^2 - BcN = e, (\square, \triangle) = 1, e|\triangle, \triangle \neq 1$ and $A, B, C, D, e, \lambda, \triangle, \square \in \mathbb{Z}$. A matrix $\begin{pmatrix} Ae & B \\ CN & De \end{pmatrix}^{-1} \mathcal{A}_\beta$ implies that $a\frac{\square}{\triangle}$ is an integer, and hence e divides a. This is absurd. Here W_e is a non-trivial Atkin-Leher involution. Therefore, likewise as in the proof of Theorem 4, $\ker(\Phi_{K'(T_g(\alpha))/K})$ is contained in a subgroup $P_{K,1}(N)(P(\mathcal{O}_K) \cap I_K(N))$ of $I_K(N)$.

Let (β) be a principal ideal of $\mathcal{O}_K$ relatively prime to N and write $\beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z}(= \mathcal{O}_K)$. Since we see from Lemma 5 that the action of (β) on $T_g(\alpha)$ is represented by a matrix $\mathcal{A}_\beta \in SL_2(\mathbb{Z})$ whose image in $SL_2(\mathbb{Z}/N\mathbb{Z})$ is equal to $\begin{pmatrix} -bn+l & -cn \\ anN(\beta)^{-1} & lN(\beta)^{-1} \end{pmatrix}$, we get that (β) fixes $T_g(\alpha)$ if and only if $\mathcal{A}_\beta \in \Gamma_0(N)SL_2(\mathbb{Z})_\alpha$ by replacing $\mathcal{A}$ by $\mathcal{A}_\beta$ in the above argument. This implies that $(\beta) \in \ker(\Phi_{K'(T_g(\alpha))/K})$ if and only if $\mathcal{A}_\beta \in \Gamma_0(N)SL_2(\mathbb{Z})_\alpha$ and $N(\beta) = \pm 1 \bmod N$. But we know that $SL_2(\mathbb{Z})_\alpha$ is trivial unless α is $SL_2(\mathbb{Z})$-equivalent to $e^{\frac{2\pi i}{r}}$ with $r \in \{3, 4\}$. Assuming $SL_2(\mathbb{Z})_\alpha = \{\pm 1\}$, we obtain that

$$\begin{aligned} (\beta) \in \ker(\Phi_{K'(T_g(\alpha))/K}) &\text{ if and only if } N|an \text{ and } N(\beta) \equiv \pm 1 \bmod N \\ &\text{if and only if } N|n \text{ and } l^2 \equiv \pm 1 \bmod N \\ &\text{if and only if } (\beta) \in \widetilde{P}_K(N). \end{aligned}$$

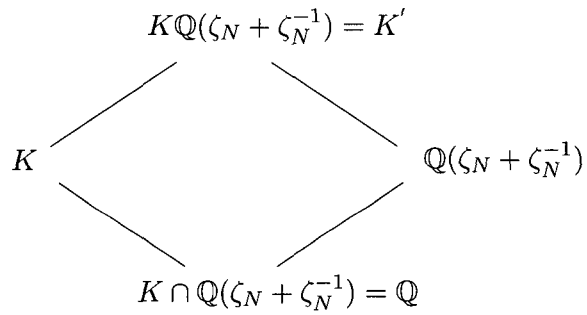
The case where α is $SL_2(\mathbb{Z})$-equivalent to $e^{\frac{2\pi i}{r}}$ with $r \in \{3,4\}$ can be treated similarly. These prove (1).

For any $\mathfrak{a} \in I_{K'}(N), [\mathfrak{a}, K'(T_g(\alpha))/K'] = [N_{K'/K}(\mathfrak{a}), K'(T_g(\alpha))/K]$ and $N_{K'/K}(I_{K'}(N)) \subset I_K(N)$ implies

$$Gal(K'(T_g(\alpha))/K') \cong I_{K'}(N)/N_{K'/K}^{-1}(\widetilde{P}_K(N)).$$

Since $P_{K,1}(N)$ is contained in $\widetilde{P}_K(N)$, we obtain from the field tower below

$$[K'(T_g(\alpha)) : K'] = \frac{\psi(N)h(\mathcal{O}(N))}{2[K_{(N)} : K'(T_g(\alpha))][K' : K]} = \frac{h(\mathcal{O}(N))}{[\widetilde{P}_K(N) : P_{K,1}(N)]}.$$



□

COROLLARY 7. *Under the same assumptions and notations as in Theorem 6, we have that if* $x \in \mathbb{Z}$ *and* $x^2 \equiv \pm 1 \bmod N$ *implies* $x \equiv \pm 1 \bmod N$, *then*

(1) $K'(T_g(\alpha)) = K_{(N)}$ *is the ray class field over* K *with modulus* N *and*

$$[K_{(N)} : K] = \frac{\psi(N)h(\mathcal{O}(N))}{2},$$

(2) $T_g(\alpha)$ *generates a class field* $K'(T_g(\alpha))$ *over* K' *with*

$$Gal(K'(T_g(\alpha))/K') \cong I_{K'}(N)/N_{K'/K}^{-1}(P_{K,1}(N))$$

and

$$[K'(T_g(\alpha)) : K'] = h(\mathcal{O}(N)).$$

Proof. These are clear from Theorem 6 □

EXAMPLES 1. For $N = 2, 3, 4, 6, 7, 9, 11, 14, 18, 19, 22, 23, 27, 31, 38, 46, 47, 54, 59, 62, 71, 94$, $x \in \mathbb{Z}$ and $x^2 \equiv \pm 1 \ mod N$ imply $x \equiv \pm 1 \bmod N$ so that $K(\zeta_N + \zeta_N^{-1}, T_g(\alpha)) = K_{(N)}$ is the ray class field over K with modulus N. On the other hand, observing that

$$\widetilde{P}_K(13) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 13|n \text{ and } l \equiv 1 \text{ or } 5 \pmod{13}\} \rangle,$$

$[\widetilde{P}_K(13) : P_{K,1}(13)] = 2$, and

$$[K(\zeta_{13} + \zeta_{13}^{-1}, T_g(\alpha)) : K(\zeta_{13} + \zeta_{13}^{-1})] = \frac{h(\mathcal{O}(13))}{2}$$

we see that $K(\zeta_{13} + \zeta_{13}^{-1}, T_g(\alpha))$ is neither a ring class field of an order $\mathbb{Z} + 13\mathcal{O}_K$ nor a ray class field $K_{(13)}$ with moduluds 13. We also have similar examples:

$$\widetilde{P}_K(15) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 15|n \text{ and } l \equiv 1 \text{ or } 4 \bmod 15\} \rangle,$$

$$\widetilde{P}_K(16) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 16|n \text{ and } l \equiv 1 \text{ or } 7 \bmod 16\} \rangle,$$

$$\widetilde{P}_K(17) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 17|n \text{ and } l \equiv 1 \text{ or } 4 \bmod 17\} \rangle,$$

$$\widetilde{P}_K(20) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 20|n \text{ and } l \equiv 1 \text{ or } 9 \bmod 20\} \rangle,$$

$$\widetilde{P}_K(21) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 21|n \text{ and } l \equiv 1 \text{ or } 8 \bmod 21\} \rangle,$$

$$\widetilde{P}_K(25) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 25|n \text{ and } l \equiv 1 \text{ or } 7 \bmod 25\} \rangle,$$

$$\widetilde{P}_K(26) = \langle \{\beta\mathcal{O}_K |\ \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 26|n \text{ and } l \equiv 1 \text{ or } 5 \bmod 26\} \rangle,$$

$$\widetilde{P}_K(28) = \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 28|n \text{ and } l \equiv 1 \text{ or } 13 \bmod 28\} \rangle,$$

$$\widetilde{P}_K(29) = \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 29|n \text{ and } l \equiv 1 \text{ or } 12 \bmod 29\} \rangle,$$

$$
\begin{aligned}
&\widetilde{P}_K(30)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 30|n \text{ and } l\equiv 1 \text{ or } 11 \mod 30\}\rangle,\\
&\widetilde{P}_K(32)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 32|n \text{ and } l\equiv 1 \text{ or } 15 \mod 32\}\rangle,\\
&\widetilde{P}_K(33)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 33|n \text{ and } l\equiv 1 \text{ or } 10 \mod 33\}\rangle,\\
&\widetilde{P}_K(34)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 34|n \text{ and } l\equiv 1 \text{ or } 13 \mod 34\}\rangle,\\
&\widetilde{P}_K(35)\\
&=\langle\{\beta\mathcal{O}_K|\ \beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 35|n \text{ and } l\equiv 1 \text{ or } 6 \mod 35\}\rangle,\\
&\widetilde{P}_K(36)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 36|n \text{ and } l\equiv 1 \text{ or } 17 \mod 36\}\rangle,\\
&\widetilde{P}_K(39)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 39|n \text{ and } l\equiv 1 \text{ or } 14 \mod 39\}\rangle,\\
&\widetilde{P}_K(41)\\
&=\langle\{\beta\mathcal{O}_K|\ \beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 41|n \text{ and } l\equiv 1 \text{ or } 9 \mod 41\}\rangle,\\
&\widetilde{P}_K(42)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 42|n \text{ and } l\equiv 1 \text{ or } 13 \mod 42\}\rangle,\\
&\widetilde{P}_K(44)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 44|n \text{ and } l\equiv 1 \text{ or } 21 \mod 44\}\rangle,\\
&\widetilde{P}_K(45)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 45|n \text{ and } l\equiv 1 \text{ or } 19 \mod 45\}\rangle,\\
&\widetilde{P}_K(50)\\
&=\langle\{\beta\mathcal{O}_K|\ \beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 50|n \text{ and } l\equiv 1 \text{ or } 7 \mod 50\}\rangle,\\
&\widetilde{P}_K(51)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 51|n \text{ and } l\equiv 1 \text{ or } 16 \mod 51\}\rangle,\\
&\widetilde{P}_K(55)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 55|n \text{ and } l\equiv 1 \text{ or } 21 \mod 55\}\rangle,\\
&\widetilde{P}_K(66)\\
&=\langle\{\beta\mathcal{O}_K|\beta=na\alpha+l\in\mathbb{Z}a\alpha+\mathbb{Z},\ \ 66|n \text{ and } l\equiv 1 \text{ or } 23 \mod 66\}\rangle,
\end{aligned}
$$

$$\widetilde{P}_K(69)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 69|n \text{ and } l \equiv 1 \text{ or } 22 \mod 69\} \rangle,$$

$$\widetilde{P}_K(70)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 70|n \text{ and } l \equiv 1 \text{ or } 29 \mod 70\} \rangle,$$

$$\widetilde{P}_K(78)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 78|n \text{ and } l \equiv 1 \text{ or } 25 \mod 78\} \rangle,$$

$$\widetilde{P}_K(87)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 87|n \text{ and } l \equiv 1 \text{ or } 28 \mod 87\} \rangle,$$

$$\widetilde{P}_K(92)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 92|n \text{ and } l \equiv 1 \text{ or } 45 \mod 92\} \rangle,$$

$$\widetilde{P}_K(95)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 95|n \text{ and } l \equiv 1 \text{ or } 39 \mod 95\} \rangle,$$

$$\widetilde{P}_K(110)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 110|n \text{ and } l \equiv 1 \text{ or } 21 \mod 110\} \rangle,$$

$$\widetilde{P}_K(119)$$
$$= \langle \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 119|n \text{ and } l \equiv 1 \text{ or } 50 \mod 119\} \rangle,$$

$[\widetilde{P}_K(N) : P_{K,1}(N)] = 2$, and $[K(\zeta_N + \zeta_N^{-1}, T_g(\alpha)) : K(\zeta_N + \zeta_N^{-1})] = \frac{h(\mathcal{O}(N))}{2}$ for $N = 13, 15, 16, 17, 20, 21, 25, 26, 28, 29, 30, 32, 33, 34, 35, 36, 39, 41, 42, 44, 45, 50, 51, 55, 66, 69, 70, 78, 87, 92, 95, 110, 119$. Meanwhile

$$\widetilde{P}_K(56) =< \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 56|n \text{ and } l \equiv 1 \text{ or } 13 \text{ or } 15 \text{ or } 27 \pmod{56}\}t >,$$

$$\widetilde{P}_K(60) =< \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 60|n \text{ and } l \equiv 1 \text{ or } 11 \text{ or } 19 \text{ or } 29 \pmod{60}\} >,$$

$$\widetilde{P}_K(105) =< \{\beta\mathcal{O}_K | \beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z},\ 105|n \text{ and } l \equiv 1 \text{ or } 29 \text{ or } 34 \text{ or } 41 \pmod{105}\} >,$$

$[\widetilde{P}_K(N) : P_{K,1}(N)] = 4$, and $[K(\zeta_N + \zeta_N^{-1}, T_g(\alpha)) : K(\zeta_N + \zeta_N^{-1})] = \frac{h(\mathcal{O}(N))}{4}$ for $N = 56, 60, 105$.

THEOREM 8. *Under the same assumptions and notations as in Theorem 6, we let* $E = K(\zeta_N) = \mathbb{Q}(\alpha, \zeta_N)$. *Then the followings hold :* (1) $E(T_g(\alpha))$ *is a class field over* K *with*

$$Gal(E(T_g(\alpha))/K) \cong I_K(N)/\widetilde{\widetilde{P}}_K(N)$$

and

$$[E(T_g(\alpha)) : K] = \frac{h(\mathcal{O}(N))\psi(N)}{2[\widetilde{\widetilde{P}}_K(N) : P_{K,1}(N)]},$$

where $\widetilde{\widetilde{P}}_K(N)$ *is a subgroup of* $I_K(N)$ *generated by all principal ideal* $\beta\mathcal{O}_K$ *such that* $\beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z}(= \mathcal{O}_K)$, $N|n$ *and* $l^2 \equiv 1 \bmod N$.

(2) $T_g(\alpha)$ *generates a class field* $E(T_g(\alpha))$ *over* E *with*

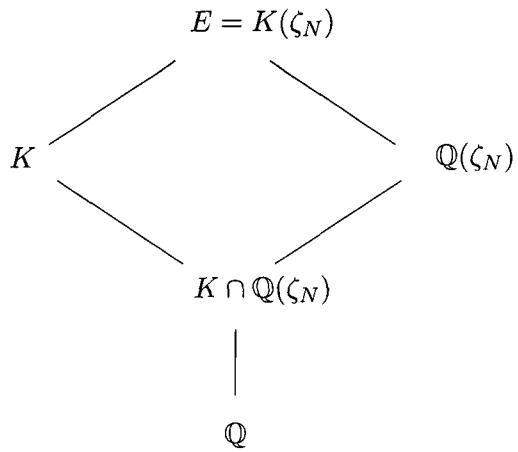
$$Gal(E(T_g(\alpha))/E) \cong I_E(N)/N_{E/K}^{-1}(\widetilde{\widetilde{P}}_K(N))$$

and

$$[E(T_g(\alpha)) : E] = \begin{cases} \dfrac{h(\mathcal{O}(N))}{[\widetilde{\widetilde{P}}_K(N):P_{K,1}(N)]} & if\ K \subset \mathbb{Q}(\zeta_N), \\ \dfrac{h(\mathcal{O}(N))}{2[\widetilde{\widetilde{P}}_K(N):P_{K,1}(N)]} & otherwise \end{cases}$$

where $I_E(N)$ *is the ideal group generated by all fractional ideals in* E *prime to* N.

Proof. We can show (1) by the same arguments as in Theorem 6. Considering the field tower bellow we have (2).



□

COROLLARY 9. *Under the same assumptions and notations as in Theorem 8, We derive that if* $x^2 \equiv 1 \bmod N$ *implies* $x \equiv \pm 1 \bmod N$ *then*

(1) $E(T_g(\alpha)) = K_{(N)}$ *is a ray class field over* K *with modulus* N *and*

$$[K_{(N)} : K] = \frac{\psi(N)h(\mathcal{O}(N))}{2},$$

(2) $T_g(\alpha)$ *generates a class field* $E(T_g(\alpha))$ *over* E *with*

$$Gal(E(T_g(\alpha))/E) \cong I_E(N)/N_{E/K}^{-1}(P_{K,1}(N))$$

and

$$[E(T_g(\alpha)) : E] = \begin{cases} h(\mathcal{O}(N)) & if\ K \subset \mathbb{Q}(\zeta_N), \\ \frac{h(\mathcal{O}(N))}{2} & otherwise. \end{cases}$$

Proof. They are clear from Theorem 8. □

EXAMPLES 2. For $N = 5, 10, 13, 17, 25, 26, 29, 41, 50$, $x^2 \equiv 1 \bmod N$ implies $x \equiv \pm 1 \bmod N$ and hence $K(\zeta_N, T_g(\alpha)) = K_{(N)}$ is the ray class field over K with modulus N.

On the other hand, taking α as a root in $\mathfrak{H}$ of the equation $z^2 + 2 = 0$ we have

$$\begin{aligned} K &= \mathbb{Q}(\sqrt{-2})(\not\subset \mathbb{Q}(\zeta_6)), [\mathbb{Q}(\sqrt{-2},\ \zeta_6)(T_6^*(\sqrt{-2})) : \mathbb{Q}(\sqrt{-2},\ \zeta_6)] \\ &= \frac{h(\mathcal{O}(N))}{2} \text{ and } \mathbb{Q}(\sqrt{-2},\ \zeta_6,\ T_6^*(\sqrt{-2})) \\ &= \mathbb{Q}(\sqrt{-2},\ \zeta_6 + \zeta_6^{-1},\ T_6^*(\sqrt{-2})) = \mathbb{Q}(\sqrt{-2})_{(6)}. \end{aligned}$$

Taking α as a root $\mathfrak{H}$ of the equation $z^2 + 3 = 0$ we also get that

$$\begin{aligned} K &= \mathbb{Q}(\sqrt{-3})(\in \mathbb{Q}(\zeta_6)), [\mathbb{Q}(\sqrt{-3},\ \zeta_6)(T_6^*(\sqrt{-3})) : \mathbb{Q}(\sqrt{-3},\ \zeta_6)] \\ &= h(\mathcal{O}(N)) \text{ and } \mathbb{Q}(\sqrt{-3},\ \zeta_6,\ T_6^*(\sqrt{-3})) \\ &= \mathbb{Q}(\sqrt{-3},\ \zeta_6 + \zeta_6^{-1},\ T_6^*(\sqrt{-3})) = \mathbb{Q}(\sqrt{-3})_{(6)}. \end{aligned}$$

REMARK. Under the same assumptions and notations as in Theorem 6,8 let β be a root in $\mathfrak{H}$ of the equation $a'z^2 + b'z + c' = 0$ such that $a' > 0, (a', b', c') = 1$ and $b'^2 - 4a'c' = m^2 d_K$. In fact, if $(a', N) = 1$, then $K'(T_g(\alpha)) = K'(T_g(\beta))$ and $E(T_g(\alpha)) = E(T_g(\beta))$.

By using the same arguments as in Theorem 6, 8 we obtain the following two theorems.

THEOREM 10. *Under the same assumptions and notations as in Theorem 4, let* K' *be a CM-field* $K(\zeta_N + \zeta_N^{-1})$. *Then the following assertions hold.*

(1) $K'(T_N^*(\alpha))$ *is a class field over* K *with*

$$Gal(K'(T_N^*(\alpha))/K) \cong I_K(N)/P_{K,1}(N)\widetilde{P}_K(N,\alpha)$$

and

$$[K'(T_N^*(\alpha)) : K] = \frac{h(\mathcal{O}(N))\psi(N)}{2[P_{K,1}(N)\widetilde{P}_K(N,\alpha) : P_{K,1}(N)]},$$

where $\widetilde{P}_K(N,\alpha)$ *is a subgroup of* $I_K(N)$ *generated by all principal ideal* $\beta\mathcal{O}_K$ *such that* $\beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z}(= \mathcal{O})$, $N|an$ *and* $l^2 - bnl \equiv \pm 1 \bmod N$, *and* $\psi(1) = \psi(2) = 2$ *and* ψ *is the Euler* φ*-function for* $N \geq 3$.

(2) $T_N^*(\alpha)$ *generates a class field* $K'(T_N^*(\alpha))$ *over* K' *with*

$$Gal(K'(T_N^*(\alpha))/K') \cong I_{K'}(N)/N_{K'/K}^{-1}(P_{K,1}(N)\widetilde{P}_K(N,\alpha))$$

and

$$[K'(T_N^*(\alpha)) : K'] = \frac{h(\mathcal{O}(N))}{[P_{K,1}(N)\widetilde{P}_K(N,\alpha) : P_{K,1}(N)]}$$

where $h(\mathcal{O}(N))$ *is the class number of* $\mathcal{O}(N)(= \mathbb{Z} + N\mathcal{O}_K)$ *and* $I_{K'}(N)$ *is the ideal group generated by all fractional ideals in* K' *prime to* N.

THEOREM 11. *Under the same assumptions and notations as in Theorem 4, let* $E = K(\zeta_N)$. *Then the following assertions hold.*

(1) $E(T_N^*(\alpha))$ *is a class field over* K *with*

$$Gal(E(T_N^*(\alpha))/K) \cong I_K(N)/P_{K,1}(N)\widetilde{\widetilde{P}}_K(N,\alpha),$$

where $\widetilde{\widetilde{P}}_K(N,\alpha)$ *is a subgroup of* $I_K(N)$ *generated by all principal ideal* $\beta\mathcal{O}_K$ *such that* $\beta = na\alpha + l \in \mathbb{Z}a\alpha + \mathbb{Z}(= \mathcal{O})$, $N|an$ *and* $l^2 - bnl \equiv 1 \bmod N$,

(2) $T_N^*(\alpha)$ *generates a class field* $E(T_N^*(\alpha))$ *over* E *with*

$$Gal(E(T_N^*(\alpha))/E) \cong I_E(N)/N_{E/K}^{-1}(P_{K,1}(N)\widetilde{\widetilde{P}}_K(N,\alpha)),$$

where $I_E(N)$ *is the ideal group generated by all fractional ideals in* E *prime to* N.

EXAMPLES 3. Let α and β be roots in $\mathfrak{H}$ of two equations $2z^2+2z+1 = 0$ and $4z^2 + 8z + 5 = 0$, respectively. Then $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(i)$.

(1) Observing that $\widetilde{P}_K(36,\alpha) = < \{\gamma\mathcal{O}_K |\ \gamma = n2\alpha + l, 18|n \text{ and } l \equiv 1 \text{ or } 17 \bmod 36\} >$, we see that $P_{K,1}(36) \subset \widetilde{P}_K(36,\alpha) = I_K(36) \cap P_{K,1}(18) = P_{K,1}(18)$. Hence by class field theory, $K(\zeta_{36} + \zeta_{36}^{-1}, T_{36}^*(\alpha))$ is the ray class field over K with modulus $18\mathcal{O}_K$.

(2) Notice that the similar result as in (1) may not be obtained and that the class field $K'(T_{26}^*(\alpha))$ over K depends on the choice of α. Indeed, we obtain that $\widetilde{P}_K(26,\beta)=<\{\gamma\mathcal{O}_K|\ \gamma = n4\beta + l, 13|n \text{ and } l \equiv 1 \text{ or } 5 \bmod 26\}>$ is contained in $\widetilde{P}_K(26,\alpha) =<\{\gamma\mathcal{O}_K|\gamma = n2\alpha + l, 13|n \text{ and } l \equiv 1 \text{ or } 5 \bmod 26\}>$ and $P_{K,1}(26)$ is contained in $\widetilde{P}_K(26,\alpha)$ by definition. Since $\widetilde{P}_K(26,\alpha)$ is not equal to $I_K(26)\cap P_{K,1}(13)$ (because $5\mathcal{O}_K \in \widetilde{P}_K(26,\alpha)$ but $5\mathcal{O}_K \notin I_K(26)\cap P_{K,1}(13)$), $K(\zeta_{26}+\zeta_{26}^{-1}, T_{26}^*(\alpha))$ is not the ray class field over K with modulus $13\mathcal{O}_K$.
Suppose that $\gamma = n2\alpha + l, 13|n$ and $l \equiv 1$ or $5 \bmod 26$. Then $\gamma^2 \equiv l^2 \equiv \pm 1 \bmod 26$ and hence $\gamma^2\mathcal{O}_K P_{K,1}(26) = P_{K,1}(26)$. Now, if $26|n$ and $l \equiv 5 \bmod 26$, then $\gamma\mathcal{O}_K P_{K,1}(26) = (5)P_{K,1}(26)$. Meanwhile, if $n = 26k+13$ for some integer k and $l \equiv 5 \bmod 26$, then $\gamma\mathcal{O}_K P_{K,1}(26) = (13\cdot 2\alpha + 5)\mathcal{O}_K P_{K,1}(26)$. Lastly, if $n = 26k + 13$ for some integer k and $l \equiv 1 \bmod 26$, then $\gamma\mathcal{O}_K P_{K,1}(26) = (13\cdot 2\alpha + 1)\mathcal{O}_K P_{K,1}(26)$. These imply $[\widetilde{P}_K(26,\alpha) : P_{K,1}(26)] = 4$. Moreover $[P_{K,1}(26)\widetilde{P}_K(26,\beta) : P_{K,1}(26)] = 2$ because $4\beta = 2(2\alpha) - 2$.

(3) We see that $\widetilde{\widetilde{P}}_K(26,\alpha)=<\{\gamma\mathcal{O}_K|\ \gamma = n2\alpha + l, 13|n \text{ and } l \equiv 1 \bmod 26\}>$ is contained in $\widetilde{P}_K(26,\alpha)$. But $\widetilde{\widetilde{P}}_K(26,\alpha) = I_K(26)\cap P_{K,1}(13)$. Indeed, if $\gamma = n2\alpha + l, 13|n$ and $l \equiv 1 \bmod 13$, then $N(\gamma) \equiv l^2 \bmod 2$ and hence l must be an odd number (i.e. $l \equiv 1 \bmod 26$) for $\gamma\mathcal{O}_K$ to be contained in $I_K(26)$. Therefore by class field theory, $K(\zeta_{26}, T_{26}^*(\alpha))$ is the ray class field over K with modulus $13\mathcal{O}_K$ and $[\widetilde{\widetilde{P}}_K(26,\alpha) : P_{K,1}(26)] = 2$.

Notice that $P_{K,1}(26)\widetilde{P}_K(26,\beta)$, $\widetilde{\widetilde{P}}_K(26,\alpha)$ and $\widetilde{P}_K(26,\alpha)$ are congruence groups with the same modulus $26\mathcal{O}_K$ for K, but they are all distinct and correspond to different class fields over K.

5. Explicit calculation of minimal polynomials

We will find an explicit formula for the conjugates of $T_g(\alpha)$ permitting the numerical calculation of its minimal polynomial. Let $Q_{d_K}(N)$ be the set of primitive quadratic forms $[a', b', c']$ having discriminant d_K with the property that $a' > 0$ and $(a', N) = 1$. For $\gamma \in \Gamma_0(N)$ and $Q \in Q_{d_K}(N)$, $Q\circ\gamma$ again belongs to $Q_{d_K}(N)$. Hence the quotient $Q_{d_K}(N)/\Gamma_0(N)$ is well-defined.

THEOREM 12. *Under the same conditions and notations as in Theorem 6, the following assertions hold.*

(1) $|Q_{d_K}(N)/\Gamma_0(N)| = h(\mathcal{O}(N))$ *where* $\mathcal{O}(N) = \mathbb{Z} + N\mathcal{O}_K$,

(2) $K(T_g(\alpha))$ *is the ring class field of* $\mathcal{O}(N)$ *so that* $[K(T_g(\alpha)) : K] = h(\mathcal{O}(N))$,

(3) *Let* $\{Q_i\}_{i=1,\ldots,h(\mathcal{O}(N))}$ *be a complete set of representatives for* $Q_{d_K}(N)/\Gamma_0(N)$. *If we define a polynomial* $f(x)$ *by*

$$f(x) = \prod_{i=1}^{h(\mathcal{O})} (x - T_g(\tau_{Q_i}))$$

then $f(x)$ *is the minimal polynomial of* $T_g(\alpha)$ *over* K. *Here* τ_{Q_i} *are the roots in* $\mathfrak{H}$ *of the equation* $Q_i(z, 1) = 0$,

(4) $f(x) \in \mathbb{Z}[x]$.

Proof. Since there is a one-one correspondence between $Q_{d_K}(N)/\Gamma_0(N)$ and $I_K(N)/P_{K,\mathbb{Z}}(N)$ ([3], Proposition 41), we obtain (1).

As for (2), the arguments from the beginning to the step of taking a matrix $\mathcal{A}_\beta$ in $SL_2(\mathbb{Z})$ are the same as those used in the proof of Theorem 6. Thus $(\beta) \in ker(\Phi_{K(T_g(\alpha))/K})$ if and only if $\mathcal{A}_\beta \in \Gamma_0(N)SL_2(\mathbb{Z})_\alpha$. But we know that $SL_2(\mathbb{Z})_\alpha$ is trivial unless α is $SL_2(\mathbb{Z})$-equivalent to $e^{2\pi i/r}$ with $r \in \{3, 4\}$. Assuming that $SL_2(\mathbb{Z})_\alpha = \{\pm 1\}$, we have that $\mathcal{A}_\beta \in \pm\Gamma_0(N)$ if and only if $N|n$. Therefore the principal ideals in $\mathcal{O}_K$ fixing $T_g(\alpha)$ are of the form (β) with $\mathrm{disc}(\beta)$ dividing $N^2 d_K$. And these principal ideals are all in $P(\mathcal{O}(N))$. The cases $\alpha \underset{SL_2(\mathbb{Z})}{\sim} e^{2\pi i/r}$ with r=3 or 4 can be done similarly. These prove the assertion (2).

Since $\mathcal{O}_\mathfrak{a} = \mathcal{O}_K = [1,\ a\alpha]$, $b^2 - 4ac = d_K, a > 0$ and $(a, N) = 1, [a, b, c]$ lies in $Q_{d_K}(N)$. This means that $T_g(\alpha) = T_g(\tau_{Q_i})$ for some i and hence $f(x)$ certainly has $T_g(\alpha)$ as a root. Now we claim that the conjugate of $T_g(\alpha)$ over K must be of the form $T_g(\tau_{Q_j})$ for some j. Indeed, let $\sigma(\neq id_{K(T_g(\alpha))}) \in Gal(K(T_g(\alpha))/K)$. Then there exists a prime ideal $\mathfrak{p}$ such that $\sigma = [\mathfrak{p},\ K(T_g(\alpha))/K]$ and $\mathfrak{p} \cap \mathbb{Z} = (p)$ splits in K (see the proof of Theorem 4). As shown in the proof of Theorem 4, the action of $\mathfrak{p}$ is represented by a matrix $\mathcal{A} = \left(\begin{smallmatrix} 1 & t \\ 0 & p \end{smallmatrix}\right) \in M_2(\mathbb{Z})$, that is, $T_g(\alpha)^\sigma = T_g(\mathcal{A}\alpha)$. Put $\tau' = \mathcal{A}\alpha$. Then $p\tau' = \alpha + t$; hence $a(p\tau' - t)^2 + b(p\tau' - t) + c = 0$ and $ap^2\tau'^2 + (bp - 2apt)\tau' + at^2 - bt + c = 0$. Dividing the coefficients of τ' by their greatest common divisor, we obtain that $a'\tau'^2 + b'\tau' + c' = 0, (a', b', c') = 1$ and $a' > 0$. Since $(N, p) = 1$ and $(N, a) = 1$, $(N, a') = 1$. This implies that $[a', b', c']$ lies in $Q_{d_K}(N)$ and so $T_g(\alpha)^\sigma = T_g(\tau_{Q_j})$ for some j.

Since $|Q_{d_K}(N)/\Gamma_0(N)| = h(\mathcal{O}(N))$ and there are exactly $h(\mathcal{O}(N))$ conjugates of $T_g(\alpha)$ over K, $f(x)$ is the minimal polynomial of $T_g(\alpha)$ over K. Therefore, (3) is verified.

Let $T_g(z) = q^{-1} + \sum_{n\geq 1} H_n q^n$ ($H_n \in \mathbb{Z}$) be the Fourier expansion of T_g. Write $\tau_Q = x + yi \in \tilde{\mathfrak{H}}$ and consider

$$\begin{aligned}\overline{T_g(\tau_Q)} &= \overline{e^{-2\pi i(x+yi)}} + \sum_{n\geq 1} H_n \overline{e^{-2\pi in(x+yi)}} \\ &= e^{-2\pi i(-x+yi)} + \sum_{n\geq 1} H_n e^{-2\pi in(-x+yi)} \\ &= T_g(-x+yi) \\ &= T_g(\tau_{\overline{Q}}),\end{aligned}$$

where $\overline{Q}$ is defined to be $[a,-b,c]$ when $Q = [a,b,c]$. This shows that the complex conjugate fixes the roots of $f(x)$ and hence $f(x) \in \mathbb{R}[x]$. Moreover, since $T_g(\alpha)$ is an algebraic integer ([3], Theorem I), $f(x)$ lies in $\mathbb{Z}[x]$. This proves (4). □

THEOREM 13. *Under the same assumptions and notations as in Theorem 6, let $g(x) \in K'[x]$ be a monic irreducible factor of $f(x)$ having $T_g(\alpha)$ as a root. Then $g(x)$ is the minimal polynomial over K' and lies in $\mathcal{O}_{K'}[x]$. In particular, under the same conditions as in Corollary 7, $f(x)$ is the minimal polynomial of $T_g(\alpha)$ over K' where $f(x)$ is given as in Theorem 12.*

Proof. Obvious. □

THEOREM 14. *Under the same assumptions and notations as in Theorem 8, let $h(x) \in E[x]$ be a monic irreducible factor of $f(x)$ having $T_g(\alpha)$ as a root. Then $h(x)$ is the minimal polynomial over E and lies in $\mathcal{O}_E[x]$. In particular, under the same conditions as in Corollary 9, $f(x)$ is the minimal polynomial of $T_g(\alpha)$ over E if $K \subset \mathbb{Q}(\zeta_N)$, where $f(x)$ is defined as in Theorem 12.*

Proof. Clear. □

EXAMPLES 4. Take $K = \mathbb{Q}(\sqrt{-1})$, $T_g = T_{12}^*$ and $\mathfrak{a} = [1, \sqrt{-1}] = \mathcal{O}_K$. Then the degree of $K(T_{12}^*(\sqrt{-1}))$ over K is $h(\mathbb{Z} + 12\mathcal{O}_K) = 8$. Observe that

$$\begin{aligned}Q_{d_K}(12)/\Gamma_0(12) = \{&[1,0,1],[5,4,1],[5,6,2],[17,8,1],[17,-8,1],\\ &[13,10,2],[37,12,1],[25,14,2]\}.\end{aligned}$$

Now, Theorem 12 allows us to have an explicit calculation of the minimal polynomial of $T_{12}^*(\sqrt{-1})$. In fact, by approximating $T_{12}^*(\tau_{Q_i})$ with the aid of a computer we can get $f(x) = x^8 - 560x^7 + 9616x^6 - 71984x^5 + 302704x^4 - 773120x^3 + 1201528x^2 - 1053392x + 401848$ because $f(x)$ has integer coefficients. Moreover factoring $f(x)$ by using a computer we see that $x^4 - (156\sqrt{3} + 280)x^3 + (1198\sqrt{3} + 2112)x^2 - (5296 + 3020\sqrt{3})x + 4366 + 2494\sqrt{3}$ is the minimal polynomial of $T_{12}^*(\sqrt{-1})$ over $\mathbb{Q}(e^{\frac{\pi i}{6}}, i)$ and over $\mathbb{Q}(e^{\frac{\pi i}{6}} + e^{\frac{-\pi i}{6}}, i)$. Notice that K is contained in $\mathbb{Q}(e^{\frac{\pi i}{6}}, i) = \mathbb{Q}(e^{\frac{\pi i}{6}} + e^{\frac{-\pi i}{6}}, i)$.

References

[1] R. Borchers, *Monstrus moonshine and monstrous Lie superalgebras*, Invent. Math. **109** (1992), 405–444.

[2] A. Borl, S. Chowls, C. Herz, K. Iwasawa, and J.-P. Serre, *Seminar on Complex Multiplicaton*, Lectrue Notes in Math **21**, Springer-Verlag, 1966.

[3] I. Chen and N. Yui, *Singular values of Thompson series; Groups, Difference sets and Monster*, eds., de Gruyter, 1995, 255–326.

[4] J. H. Conway and S. P. Norton, *Monstrous moonshine*, Bull. London Math. Soc. **11** (1979), 308–339.

[5] D. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley and Sons, 1989.

[6] H. Helling, *Note uber das Geschlecht gewisser arithmetischer Gruppen*, Math. Ann. **205** (1973), 173–179.

[7] C. H. Kim and J. K. Koo, *Arithmetic of the modular function $j_{1,4}$*, Acta Arith. **84** (1998), 129–143.

[8] S. Lang, *Algebraic Number Theory*, Springer-Verlag, 1991.

[9] ———, *Elliptic Functions*, Springer-Verlag, 1987.

[10] J. S. Milne, *Algebraic Number Theory*, Lecture Notes in Math **676**, University of Michgan, Fall 1991.

[11] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, no. 11, Tokyo Prineton, 1971.

So Young Choi and Ja Kyung Koo
Korea Advanced Institute of Science and Techology
Department of Mathematics
Daejeon 305-701, Korea
E-mail: young@math.kaist.ac.kr
jkkoo@math.kaist.ac.kr