ACTA ARITHMETICA
XCIII.3 (2000)

Generation of class fields by the modular function $j_{1,12}$

by

Kuk Jin Hong and Ja Kyung Koo (Taejon)

Dedicated to Professor Takashi Ono
on the occasion of his 70th birthday

1. Introduction. Let $\mathfrak{H}$ be the complex upper half plane and let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Since the group Γ acts on $\mathfrak{H}$ by linear fractional transformations, we get the modular curve $X(\Gamma) = \Gamma\backslash\mathfrak{H}^*$, as the projective closure of smooth affine curve $\Gamma\backslash\mathfrak{H}$, with genus g_Γ. Since $g_{1,N} = 0$ only for the eleven cases $1 \le N \le 10$ and $N = 12$ ([12]) when $\Gamma = \Gamma_1(N)$ $\big(= \big\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N\big\}\big)$, the function field $K(X_1(12))$ over the curve $X_1(12) = \Gamma_1(12)\backslash\mathfrak{H}^*$ is a rational function field $\mathbb{C}(j_{1,12})$ where $j_{1,12}(z) := \theta_3(2z)/\theta_3(6z)$ for $z \in \mathfrak{H}$ and θ_3 is the classical Jacobi theta series.

In this article we will construct in Section 3 some sort of class fields by means of Shimura's ideas for the congruence subgroups $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$. In Section 4 we will generate the ray class field $K_{(12)}$ with conductor 12 of imaginary quadratic fields K by applying standard results of complex multiplication to the modular function $j_{1,12}(z)$. In Section 5 by using Chen–Yui's result [1], we shall investigate when the subfield of $K_{(12)}$ generated by $j_{1,12}(\alpha)$ is equal to a ray class field $K_{\mathfrak{f}}$ for a conductor $\mathfrak{f}$ dividing 12 where α is the quotient of a basis of an $\mathcal{O}_K$-ideal (Theorems 20, 21 and 23). Lastly, in Section 6 we will explore an explicit formula for the conjugates of the Hauptmodul $N(j_{1,12}(\alpha))$ permitting the numerical computation of its minimal polynomial. We thank the referee for his valuable comments which enabled us to improve Sections 5 and 6.

Throughout the article we adopt the following notations:

- $\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv I \pmod N\}$,
- $\Gamma_0(N) = \big\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \,\big|\, c \equiv 0 \pmod N\big\}$,
- $\Gamma^1(N) = \big\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \,\big|\, a \equiv d \equiv 1, b \equiv 0 \pmod N\big\}$,

2000 *Mathematics Subject Classification*: 11F11, 11R04, 11R37, 14H55.
This article was supported by KOSEF 98-0701-01-01-3.

- $\Gamma_0(N,M) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \mid b \equiv 0 \pmod{M}, c \equiv 0 \pmod{N}\}$,
- $M_{k/2}(\widetilde{\Gamma}_0(N))$, the space of modular forms of half integral weight for the group $\Gamma_0(N)$,
- $M_{k/2}(\widetilde{\Gamma}_0(N), \chi) = \{f \in M_{k/2}(\widetilde{\Gamma}_0(N)) \mid f(\gamma z) = \chi(d) j(\gamma, z)^k f(z)$ for all $\gamma = \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)\}$ where χ is a Dirichlet character modulo N and $j(\gamma, z) = (c/d)\varepsilon_d^{-1}\sqrt{cz+d}$ with $\varepsilon_d = 1$ if $d \equiv 1 \pmod 4$ and $= i$ otherwise,
- $\mathbb{Z}_p$, the ring of p-adic integers,
- $\mathbb{Q}_p$, the field of p-adic numbers,
- $q_h = e^{2\pi i z/h}$, $z \in \mathfrak{H}$.

2. Hauptmodul of $K(X_1(12))$ as a quotient of Jacobi theta series. For $\mu, \nu \in \mathbb{R}$ and $z \in \mathfrak{H}$, put

$$\Theta_{\mu,\nu}(z) := \sum_{n \in \mathbb{Z}} \exp\left\{\pi i \left(n + \tfrac{1}{2}\mu\right)^2 z + \pi i n \nu\right\}.$$

This series converges uniformly for $\mathrm{Im}(z) \geq \eta > 0$, and hence defines a holomorphic function on $\mathfrak{H}$. Then the Jacobi theta series θ_2, θ_3 and θ_4 are defined by

$$\begin{aligned} \theta_2(z) &:= \Theta_{1,0}(z) = \sum_{n \in \mathbb{Z}} q_2^{(n+1/2)^2}, \\ \theta_3(z) &:= \Theta_{0,0}(z) = \sum_{n \in \mathbb{Z}} q_2^{n^2}, \\ \theta_4(z) &:= \Theta_{0,1}(z) = \sum_{n \in \mathbb{Z}} (-1)^n q_2^{n^2}. \end{aligned}$$

And we have the following transformation formulas ([17], pp. 218–219):

$$\begin{aligned} \theta_2(z+1) &= e^{\pi i/4}\theta_2(z), & \theta_2(-1/z) &= (-iz)^{1/2}\theta_4(z), \\ \theta_3(z+1) &= \theta_4(z), & \theta_3(-1/z) &= (-iz)^{1/2}\theta_3(z), \\ \theta_4(z+1) &= \theta_3(z), & \theta_4(-1/z) &= (-iz)^{1/2}\theta_2(z). \end{aligned} \tag{1}$$

Furthermore, we have the following theorem at hand. For the definition of modular forms of half integer weight, we refer to [20] or [14].

THEOREM 1. (1) $\theta_3(2z) \in M_{1/2}(\widetilde{\Gamma}_0(4))$ *and* $\theta_3(6z) \in M_{1/2}(\widetilde{\Gamma}_0(12), \chi_3)$.

(2) $K(X_1(12)) = \mathbb{C}(j_{1,12})$ *and* $j_{1,12}$ *takes the following value at each cusp*: $j_{1,12}(\infty) = 1$, $j_{1,12}(0) = \sqrt{3}$, $j_{1,12}(1/2) = 0$ (*a simple zero*), $j_{1,12}(1/3) = i$, $j_{1,12}(1/4) = \sqrt{3}i$, $j_{1,12}(1/5) = -\sqrt{3}$, $j_{1,12}(1/6) = \infty$ (*a simple pole*), $j_{1,12}(1/8) = -\sqrt{3}i$, $j_{1,12}(1/9) = -i$, $j_{1,12}(5/12) = -1$.

Proof. [11], Theorem 4. ∎

3. Generation I. Let Γ be a Fuchsian group of the first kind. Then $\Gamma\backslash\mathfrak{H}^*$ $(= X(\Gamma))$ 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 its function field $K(X(\Gamma))$ is equal to $\mathbb{C}(J')$ for some $J' \in K(X(\Gamma))$.

LEMMA 2. $(\mathbb{P}^1(\mathbb{C}), J')$ *is a model of* $\Gamma\backslash\mathfrak{H}^*$.

Proof. [6], Lemma 14. ∎

Let $G_\mathbb{A}$ be the adelization of an algebraic group $G = \mathrm{GL}_2$ defined over $\mathbb{Q}$. Put

$$\begin{aligned} G_p &= \mathrm{GL}_2(\mathbb{Q}_p) \quad (p \text{ a rational prime}),\\ G_\infty &= \mathrm{GL}_2(\mathbb{R}),\\ G_{\infty+} &= \{x \in G_\infty \mid \det(x) > 0\},\\ G_{\mathbb{Q}+} &= \{x \in \mathrm{GL}_2(\mathbb{Q}) \mid \det(x) > 0\}. \end{aligned}$$

We define the topology of $G_\mathbb{A}$ by taking $U = \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \times G_{\infty+}$ to be an open subgroup of $G_\mathbb{A}$. Let K be an imaginary quadratic field and ξ be an embedding of K into $M_2(\mathbb{Q})$. We call ξ *normalized* if it is defined by

$$a\begin{pmatrix} z \\ 1 \end{pmatrix} = \xi(a)\begin{pmatrix} z \\ 1 \end{pmatrix} \qquad \text{for } a \in K$$

where z is the fixed point of $\xi(K^\times)$ $(\subset G_{\mathbb{Q}+})$ in $\mathfrak{H}$. Observe that the embedding ξ defines a continuous homomorphism of $K_\mathbb{A}^\times$ into $G_{\mathbb{A}+}$, which we denote again by ξ. Here $G_{\mathbb{A}+}$ is the group $G_0 G_{\infty+}$ with G_0 the nonarchimedean 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 $\mathbb{Q}^\times \cdot \det(S)$ 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 ([19], Proposition 6.27), $\Gamma_S/\mathbb{Q}^\times$ is a Fuchsian group of the first kind commensurable with $\Gamma(1)/\{\pm 1\}$.

PROPOSITION 3. *Let Γ' be a discrete subgroup of $G_{\infty+}/\mathbb{R}^\times$ commensurable with $\mathbb{Q}^\times\Gamma(1)/\mathbb{Q}^\times$, and containing $\Gamma(N)$ for some N. Then $\Gamma' = \Gamma_S/\mathbb{Q}^\times$ for some $S \in \mathcal{Z}$.*

Proof. [19], Proposition 6.30. ∎

In accordance with Proposition 3, we are able to find open compact subgroups S corresponding to $\Gamma_0(N)$, $\Gamma_0(N, M)$, $\Gamma_1(N)$ and $\Gamma^1(N)$. Fix positive integers N and M, and consider the following:

$$U_{(p)} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p) \,\middle|\, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N\mathbb{Z}_p} \right\},$$
$$U_{0,(p)} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p) \,\middle|\, c \equiv 0 \pmod{N\mathbb{Z}_p} \right\},$$
$$U_{0,(p)}^0 = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p) \,\middle|\, b \equiv 0 \pmod{M\mathbb{Z}_p},\ c \equiv 0 \pmod{N\mathbb{Z}_p} \right\},$$
$$U_{1,(p)} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p) \,\middle|\, a \equiv d \equiv 1,\ c \equiv 0 \pmod{N\mathbb{Z}_p} \right\},$$
$$U_{(p)}^1 = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p) \,\middle|\, a \equiv d \equiv 1,\ b \equiv 0 \pmod{N\mathbb{Z}_p} \right\},$$
$$U_N = \{x = (x_p) \in U \mid x_p \in U_{(p)} \text{ for all finite } p\},$$
$$U_0 = \{x = (x_p) \in U \mid x_p \in U_{0,(p)} \text{ for all finite } p\},$$
$$U_0^0 = \{x = (x_p) \in U \mid x_p \in U_{0,(p)}^0 \text{ for all finite } p\},$$
$$U_1 = \{x = (x_p) \in U \mid x_p \in U_{1,(p)} \text{ for all finite } p\},$$
$$U^1 = \{x = (x_p) \in U \mid x_p \in U_{(p)}^1 \text{ for all finite } p\}.$$

Put

$$S = \mathbb{Q}^\times U_N, \quad S_0 = \mathbb{Q}^\times U_0, \quad S_0^0 = \mathbb{Q}^\times U_0^0, \quad S_1 = \mathbb{Q}^\times U_1, \quad S^1 = \mathbb{Q}^\times U^1.$$

We then have the following lemmas.

LEMMA 4. (i) $S_0, S_0^0 \in \mathcal{Z}$.
(ii) $k_{S_0} = k_{S_0^0} = \mathbb{Q}$.
(iii) $\Gamma_{S_0} = \mathbb{Q}^\times \Gamma_0(N)$ *and* $\Gamma_{S_0^0} = \mathbb{Q}^\times \Gamma_0(N, M)$.

Proof. First, we observe that $\mathbb{Q}^\times U_0$ (resp. $\mathbb{Q}^\times U_0^0$) is an open subgroup of $\mathbb{Q}^\times U$ since $\mathbb{Q}^\times U_0$ (resp. $\mathbb{Q}^\times U_0^0$) contains $\mathbb{Q}^\times U_N$ (resp. $\mathbb{Q}^\times U_{\mathrm{l.c.m.}\{N,M\}}$). Hence, for (i), it is enough to show that $\mathbb{Q}^\times U/\mathbb{Q}^\times G_{\infty+}$ is compact. But, we know that $\mathbb{Q}^\times U/\mathbb{Q}^\times G_{\infty+} = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ is compact because each $\mathrm{GL}_2(\mathbb{Z}_p)$ is a profinite group. For (ii), note by class field theory that $\mathbb{Q}$ corresponds to the norm group $\mathbb{Q}^\times \cdot \mathbb{Q}_{\mathbb{A}}^{\times\infty}$ with $\mathbb{Q}_{\mathbb{A}}^{\times\infty} = \mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times$.

We claim that $\det(U_0) = \det(U_0^0) = \mathbb{Q}_{\mathbb{A}}^{\times\infty}$. Indeed, it is obvious that $\det(U_0), \det(U_0^0) \subset \mathbb{Q}_{\mathbb{A}}^{\times\infty}$. 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 $(y_p) \in U_0, U_0^0$ and $\det(y_p) = (\det y_p) = (\alpha_p)$. Finally, we come up with $\Gamma_{S_0} = \mathbb{Q}^\times U_0 \cap G_{\mathbb{Q}+} = \mathbb{Q}^\times (U_0 \cap G_{\mathbb{Q}+}) = \mathbb{Q}^\times \Gamma_0(N)$ and $\Gamma_{S_0^0} = \mathbb{Q}^\times U_0^0 \cap G_{\mathbb{Q}+} = \mathbb{Q}^\times (U_0^0 \cap G_{\mathbb{Q}+}) = \mathbb{Q}^\times \Gamma_0(N, M)$. ∎

LEMMA 5. (i) $S_1, S^1 \in \mathcal{Z}$.
(ii) $k_{S_1} = k_{S^1} = \mathbb{Q}(\zeta_N)$ *where* $\zeta_N = e^{2\pi i/N}$.
(iii) $\Gamma_{S_1} = \mathbb{Q}^\times \Gamma_1(N)$ *and* $\Gamma_{S^1} = \mathbb{Q}^\times \Gamma^1(N)$.

Proof. (i) follows from the same method as in Lemma 4(i). Let

$$V_{Np_\infty} = \{\alpha = (\alpha_p) \in \mathbb{Q}_{\mathbb{A}}^\times \mid \alpha \equiv 1 \ (\mathrm{mod}^*\, Np_\infty),\ \alpha_p \in \mathbb{Z}_p^\times \text{ for } p \nmid N\}$$

where p_∞ denotes the infinite $\mathbb{Q}$-prime. Here $\alpha \equiv 1 \pmod{^* Np_\infty}$ means that each α_{p_i} is congruent to 1 (mod $p_i^{n_i}\mathbb{Z}_{p_i}$) if $N = p_1^{n_1} \dots p_r^{n_r}$ and $\alpha_{p_\infty} > 0$. As is well known ([15], p. 209), $\mathbb{Q}(\zeta_N)$ is the class field corresponding to $\mathbb{Q}^\times V_{Np_\infty}$.

Now as for (ii), it suffices to show that $\det(U_1) = \det(U^1) = V_{Np_\infty}$. For $(x_p) \in U_1, U^1$, $\det(x_p) \equiv 1 \pmod{N\mathbb{Z}_p} \equiv 1 \pmod{p^n\mathbb{Z}_p}$ when $p^n \parallel N$. Hence, $\det(U_1)$, $\det(U^1) \subset V_{Np_\infty}$. Conversely, for $(\alpha_p) \in V_{Np_\infty}$, take $x_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \alpha_p \end{smallmatrix}\right)$. Since $N\mathbb{Z}_p = p^n\mathbb{Z}_p$ and $\alpha_p \equiv 1 \pmod{p^n\mathbb{Z}_p}$ for $p^n \parallel N$, it is clear that $(x_p) \in U_1, U^1$ and $\det(x_p) = \alpha_p$. Finally, we end up with $\Gamma_{S_1} = \mathbb{Q}^\times U_1 \cap G_{\mathbb{Q}+} = \mathbb{Q}^\times(U_1 \cap G_{\mathbb{Q}+}) = \mathbb{Q}^\times \Gamma_1(N)$ and $\Gamma_{S^1} = \mathbb{Q}^\times U^1 \cap G_{\mathbb{Q}+} = \mathbb{Q}^\times(U^1 \cap G_{\mathbb{Q}+}) = \mathbb{Q}^\times \Gamma^1(N)$. ∎

REMARK 6. Now we consider a normalized embedding $\xi_z : K \to M_2(\mathbb{Q})$ defined by $a\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right) = \xi_z(a)\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$ for $a \in K$ and $z \in K \cap \mathfrak{H}$. Then z is the fixed point of $\xi(K^\times)$ in $\mathfrak{H}$. Let (V_T, φ_T) be a model of $\Gamma_T \backslash \mathfrak{H}^*$ for $T \in \{S_0, S_0^0, S_1, S^1\}$. Note that, for convenience, we identify V_T and φ_T with a projective nonsingular algebraic curve V_{Γ_T} and a Γ_T-invariant holomorphic map φ_{Γ_T}, respectively.

We see by [4] that φ_{S_0} can be chosen as the product of Dedekind eta functions and $V_{S_0} = \mathbb{P}^1(\mathbb{C})$. It then follows from [19], Proposition 6.31, that $\varphi_{S_0}(z)$ belongs to $\mathbb{P}^1(K^{\mathrm{ab}})$ for the curves $X_0(N) = \Gamma_0(N)\backslash\mathfrak{H}^*$ where K^{ab} is the maximal abelian extension of K. Furthermore, it is true that the Dedekind eta function $\eta(z)$ has no zeros in $\mathfrak{H}$. Hence we conclude that $\varphi_{S_0}(z)$ in fact belongs to K^{ab} for $z \in K \cap \mathfrak{H}$. On the other hand, since $\left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \Gamma_0(N, M) \left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right) = \Gamma_0(NM)$, two modular curves $X_0(N, M) = \Gamma_0(N, M)\backslash\mathfrak{H}^*$ and $X_0(NM) = \Gamma_0(NM)\backslash\mathfrak{H}^*$ are isomorphic and hence the genera of $X_0(N, M)$ are completely determined by those of $X_0(NM)$, and vice versa.

We recall from [19], Section 6.7, the following general situation.

Let Γ' be another Fuchsian group of the first kind, $\mathfrak{H}^{*\prime}$ the union of $\mathfrak{H}$ and the cusps of Γ', and $(V_{\Gamma'}, \varphi_{\Gamma'})$ a *model* of $\Gamma'\backslash\mathfrak{H}^{*\prime}$. Suppose that $\alpha\Gamma\alpha^{-1} \subset \Gamma'$ with an element α in $G_{\infty+}$. Then we can define a rational map T of V_Γ to $V_{\Gamma'}$ by $T(\varphi_\Gamma(z)) = \varphi_{\Gamma'}(\alpha(z))$, that is, by the following commutative diagram:

$$\begin{array}{ccc} \mathfrak{H}^* & \xrightarrow{\alpha} & \mathfrak{H}^{*\prime} \\ {\scriptstyle\varphi_\Gamma}\downarrow & & \downarrow{\scriptstyle\varphi_{\Gamma'}} \\ V_\Gamma & \xrightarrow{T} & V_{\Gamma'} \end{array}$$

This includes, as special cases, the following two types of maps:

CASE (a): $\alpha = 1$, hence $\Gamma \subset \Gamma'$. Then T is the usual projection map.

CASE (b): $\alpha\Gamma\alpha^{-1} = \Gamma'$. Then T is a biregular isomorphism of V_Γ to $V_{\Gamma'}$.

We shall apply our situation to Case (b). Take $\Gamma = \Gamma_0(N,M)$, $\Gamma' = \Gamma_0(NM)$ and $\alpha = \left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$. Then we have $T(\varphi_{\Gamma_0(N,M)}(z)) = \varphi_{\Gamma_0(NM)}(\alpha(z))$, which means that $(\mathbb{P}^1(\mathbb{C}), \varphi_{\Gamma_0(NM)}(z/M))$ is a model of $\Gamma_0(N,M)\backslash\mathfrak{H}^*$. In particular, since the genera of $\Gamma_0(NM)\backslash\mathfrak{H}^*$ and $\Gamma_0(N,M)\backslash\mathfrak{H}^*$ are all zeros, we can take $\varphi_{\Gamma_0(NM)}(z)$ and $\varphi_{\Gamma_0(NM)}(z/M)$ as Hauptmoduln. Therefore we can construct the following class fields by making use of the Hauptmoduln of genus zero curves $X_0(N)$. We refer to the Appendix for those Hauptmoduln.

THEOREM 7. *Let K be an imaginary quadratic field and let ξ_z be the normalized embedding for fixed $z \in K \cap \mathfrak{H}$. Then $\varphi_{S_0}(z)$ belongs to the maximal abelian extension K^{ab} of K and $K(\varphi_{S_0}(z))$ is the class field of K corresponding to the subgroup $K^\times \cdot \xi_z^{-1}(S_0)$ of $K_{\mathbb{A}}^\times$.*

Proof. In the case of S_0, we have $k_{S_0} = \mathbb{Q}$ and $\Gamma_{S_0} = \mathbb{Q}^\times \Gamma_0(N)$ by Lemma 4(ii) and (iii). Since φ_{S_0} gives a model of the curve $X_0(N)$, the assertion follows from [19], Proposition 6.33, and Remark 6. ∎

Since $\left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right)\xi_{z/M}(a)\left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \xi_z(a)$ for $a \in K$,

$$K^\times \cdot \xi_{z/M}^{-1}(\mathbb{Q}^\times U_0) = K^\times \cdot \xi_z^{-1}(\mathbb{Q}^\times U_0^0)$$

and hence we have the following corollary for $\Gamma_0(N,M)$.

COROLLARY 8. *Notations being as in Theorem 7, $\varphi_{S_0}(z/M)$ is in the maximal abelian extension K^{ab} of K when $g_{\Gamma_0(N,M)} = 0$ and $K(\varphi_{S_0}(z/M))$ is the class field of K corresponding to the subgroup $K^\times \cdot \xi_z^{-1}(S_0^0)$ of $K_{\mathbb{A}}^\times$.*

We refer to the Appendix for the Hauptmoduln of genus zero curves $X(N)$ (except for the case $N = 5$) and $X_1(N)$. Again by [19], Proposition 6.31, each Hauptmodul listed in Table 4 belongs to $\mathbb{P}^1(K^{\mathrm{ab}})$. Since the Hauptmoduln have poles only at ∞, we see that they in fact take values in K^{ab} for $z \in K \cap \mathfrak{H}$. As an analogue of Theorem 7 in the case of $\Gamma(N)$ $(N = 2, 3, 4)$ and $\Gamma_1(N)$ $(1 \le N \le 10$ and $N = 12)$, we get the following theorem.

THEOREM 9. *Let K be an imaginary quadratic field and let ξ_z be the normalized embedding for $z \in K \cap \mathfrak{H}$. Then $N(j_{1,N}(z))$ and $N(j_N(z))$ belong to the maximal abelian extension K^{ab} of K and $K(N(j_{1,N}(z)), \zeta_N)$ (resp. $K(N(j_N(z)), \zeta_N)$) is the class field of K corresponding to the subgroup $K^\times \cdot \xi_z^{-1}(S_1)$ (resp. $K^\times \cdot \xi_z^{-1}(S)$) of $K_{\mathbb{A}}^\times$.*

Proof. As for the cases of S and S_1, by Lemma 5 and [19], we have $k_S = k_{S_1} = \mathbb{Q}(\zeta_N)$, $\Gamma_S = \mathbb{Q}^\times \Gamma(N)$ and $\Gamma_{S_1} = \mathbb{Q}^\times \Gamma_1(N)$. Since $N(j_{1,N})$ (resp. $N(j_N)$) gives a model of the curve $X_1(N)$ (resp. $X(N)$), the assertion follows from [19], Proposition 6.33, and the argument mentioned above. ∎

In particular, when $N = 12$ we would obtain

COROLLARY 10. *Notations being as in Theorem* 7, $K(i,\sqrt{3},N(j_{1,12}(z)))$ *is the class field of* K *corresponding to the subgroup* $K^\times\cdot\xi_z^{-1}(\mathbb{Q}^\times U_1)$ *where* $U_1=\{x=(x_p)\in U\mid x_p\in U_{1,(p)}$ *for all finite* $p\}$ *and* $U_{1,(p)}=\bigl\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in \mathrm{GL}_2(\mathbb{Z}_p)\mid a\equiv d\equiv 1, c\equiv 0 \pmod{12\mathbb{Z}_p}\bigr\}$.

Since $\left(\begin{smallmatrix}N&0\\0&1\end{smallmatrix}\right)^{-1}\Gamma^1(N)\left(\begin{smallmatrix}N&0\\0&1\end{smallmatrix}\right)=\Gamma_1(N)$, we have

$$K^\times\cdot\xi_{z/N}^{-1}(\mathbb{Q}^\times U_1)=K^\times\cdot\xi_z^{-1}(\mathbb{Q}^\times U^1).$$

Therefore we get the following corollary for $\Gamma^1(N)$.

COROLLARY 11. *Notations being as in Theorem* 7, $N(j_{1,N}(z/N))$ *belongs to the maximal abelian extension* K^{ab} *of* K *and* $K(N(j_{1,N}(z/N)),\zeta_N)$ *is the class field of* K *corresponding to the subgroup* $K^\times\cdot\xi_z^{-1}(S^1)$ *of* $K_{\mathbb{A}}^\times$.

4. Generation II. In view of standard results on complex multiplication, we are interested in investigating whether the value $j_{1,12}(\alpha)$ is a generator for a certain full ray class field when α is the quotient of a basis of an ideal belonging to the maximal order in an imaginary quadratic field. To this end we are first in need of a result from complex multiplication.

THEOREM 12. *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 over* K *with conductor* N.

Proof. [16], Ch. 10, Corollary of Theorem 2. ∎

Let $K(X(\Gamma'))$ be the function field of the modular curve $X(\Gamma')=\Gamma'\backslash\mathfrak{H}^*$. Suppose that the genus of $X(\Gamma')$ is zero. Let h be the width of the cusp ∞. By F we denote the field of all modular functions in $K(X(\Gamma'))$ whose Fourier coefficients with respect to q_h belong to $\mathbb{Q}$.

LEMMA 13. *Let* $K(X(\Gamma'))=\mathbb{C}(J')$ *for some* $J'\in K(X(\Gamma'))$. *If* $J'\in F$, *then* $F=\mathbb{Q}(J')$.

Proof. [6], Lemma 4. ∎

THEOREM 14. $\mathbb{Q}(j_{1,12})$ *is the the field of all modular functions in the field* $K(X_1(12))$ *whose Fourier coefficients with respect to* q *are rational numbers.*

Proof. Since $j_{1,12}$ has rational Fourier coefficients, the result follows from Lemma 13. ∎

It follows from [19], Proposition 6.9, that

$$\mathfrak{F}_N=\mathbb{Q}(j,f_{(a_1,a_2)}\mid(a_1,a_2)\in N^{-1}\mathbb{Z}^2,\notin\mathbb{Z}^2). \tag{2}$$

Here j is the classical modular function of level 1 and $f_{(a_1,a_2)}$ is the Fricke function defined by

$$f_a(z) = \frac{g_2(\omega_1,\omega_2)g_3(\omega_1,\omega_2)}{\Delta(\omega_1,\omega_2)}\wp\left(a\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix};\omega_1,\omega_2\right)$$

for $z=\omega_1/\omega_2 \in \mathfrak{H}$ and $a=(a_1,a_2)$. We recall that

$$(3)\qquad f_{(a_1,a_2)} = f_{(b_1,b_2)} \quad \text{if and only if} \quad \pm(a_1,a_2)\equiv(b_1,b_2) \pmod{\mathbb{Z}^2}$$

and

$$(4)\qquad f_{(a_1,a_2)}|_\gamma = f_{(a_1,a_2)\gamma} \quad \text{for } \gamma\in\Gamma(1),$$

where $f(z)|_\gamma = f(\gamma z)$ for a modular function f.

Theorem 15. $K(X_1(12)) = \mathbb{C}(j, f_{(0,t)} \mid t\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z})$ $(=\mathbb{C}(j_{1,12}))$.

P r o o f. Observe that

$$K(X(1)) \subseteq K(X_1(12)) \subseteq K(X(12))$$

where $K(X(12))$ is a Galois extension over $K(X(1))$ with Galois group $\overline{\Gamma}(1)/\overline{\Gamma}(12)$ ([18], Ch. VI, Theorem 4 or [19], p. 31). We consider the Galois group

$$G = \mathrm{Gal}(K(X(12))/\mathbb{C}(j, f_{(0,t)} \mid t\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z})).$$

For $\overline{\gamma}\in\overline{\Gamma}(1)/\overline{\Gamma}(12)$, let $\gamma=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ be its representative in $\Gamma(1)$. Then by (3) and (4),

$$\begin{aligned}\overline{\gamma}\in G &\Leftrightarrow f_{(0,t)} = f_{(0,t)}|_\gamma = f_{(0,t)\gamma} = f_{(tc,td)} \text{ for } t\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z}\\ &\Leftrightarrow (c,d)\equiv\pm(0,1) \pmod{12}\\ &\Leftrightarrow \overline{\gamma}\in\overline{\Gamma}_1(12).\end{aligned}$$

Hence we must have

$$G = \overline{\Gamma}_1(12)/\overline{\Gamma}(12) = \mathrm{Gal}(K(X(12))/K(X_1(12))),$$

from which we end up with $K(X_1(12)) = \mathbb{C}(j, f_{(0,t)} \mid t\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z})$. ∎

Lemma 16. *For* $z\in\mathfrak{H}$, *we get*

$$\mathbb{Q}(j(z), f_{(0,t)}(z) \mid t\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z}) = \mathbb{Q}(j_{1,12}(z)/\sqrt{3}).$$

P r o o f. For $f\in K(X_1(12))$, we let $W_{12}(f) = f|_{\left(\begin{smallmatrix}0 & -1\\ 12 & 0\end{smallmatrix}\right)}$ be the action of the Fricke involution. Since $W_{12}=\left(\begin{smallmatrix}0 & -1\\ 12 & 0\end{smallmatrix}\right)$ belongs to the normalizer of $\Gamma_1(12)$ ([13]), $W_{12}\in\mathrm{Aut}(K(X_1(12)))$. We observe that

$$W_{12}(f) = f|_S(12z) \quad \text{for } S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

Hence it follows that $W_{12}(j(z)) = j(12z)$ and $W_{12}(f_{(0,t)}(z)) = f_{(t,0)}(12z)$. Since $j_{1,12}(z) = \theta_3(2z)/\theta_3(6z)$, we derive, by (1),

$$j_{1,12}(z)\big|_S = \frac{\theta_3(2z)}{\theta_3(6z)}\bigg|_S = \frac{\theta_3\left(-\frac{1}{z/2}\right)}{\theta_3\left(-\frac{1}{z/6}\right)} = \frac{\left(-i\frac{z}{2}\right)^{1/2}\theta_3\left(\frac{z}{2}\right)}{\left(-i\frac{z}{6}\right)^{1/2}\theta_3\left(\frac{z}{6}\right)} = \sqrt{3}/j_{1,12}\left(\frac{z}{12}\right). \tag{5}$$

We denote by $F_{1,12}$ the field of modular functions in $K(X_1(12))$ with rational Fourier coefficients. Considering the Fourier expansions of Fricke functions ([16], p. 66, or [19], p. 141), we know that $f_{(t,0)}(12z)$ has rational Fourier coefficients for $t \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z}$. Thus

$$\mathbb{Q}(W_{12}(j(z)), W_{12}(f_{(0,t)}(z)) \mid t \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z}) \subseteq F_{1,12}.$$

Moreover, we observe by Theorem 15 that

$$\begin{aligned}\mathbb{C}(W_{12}(j(z)), W_{12}(f_{(0,t)}(z)) \mid t \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z}) &= W_{12}(K(X_1(12))) \\ &= K(X_1(12)).\end{aligned}$$

On the other hand, by a similar argument to [6], Lemma 5, we get

$$F_{1,12} = \mathbb{Q}(W_{12}(j(z)), W_{12}(f_{(0,t)}(z)) \mid t \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z}). \tag{6}$$

We then deduce by Theorem 14 and (5) that

$$F_{1,12} = \mathbb{Q}(j_{1,12}(z)) = \mathbb{Q}(W_{12}(j_{1,12}(z)/\sqrt{3})),$$

which by (6) forces

$$W_{12}(\mathbb{Q}(j(z), f_{(0,t)}(z) \mid t \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z})) = W_{12}(\mathbb{Q}(j_{1,12}(z)/\sqrt{3})).$$

Therefore applying the involution W_{12} to the above yields the conclusion. ∎

Lemma 17. *We have*

$$\{(a_1, a_2) \pmod{\mathbb{Z}^2} \mid (a_1, a_2) \in 12^{-1}\mathbb{Z}^2, \notin \mathbb{Z}^2\} = A \cup B \cup C$$

where

$$\begin{aligned}A &= \left\{(0, a_1)\left(\begin{smallmatrix}0 & -1\\ 1 & x\end{smallmatrix}\right) \pmod{\mathbb{Z}^2} \,\middle|\, a_1 \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z},\ x = 0, \ldots, 11\right\},\\ B &= \left\{(0, a_2)\left(\begin{smallmatrix}1 & 0\\ x & 1\end{smallmatrix}\right) \pmod{\mathbb{Z}^2} \,\middle|\, a_2 \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z},\ x = 0, \ldots, 11\right\},\\ C &= \left\{(0, a_2)\left(\begin{smallmatrix}1 & 0\\ y & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -1\\ 0 & 1\end{smallmatrix}\right) \pmod{\mathbb{Z}^2} \,\middle|\, a_2 \in 12^{-1}\mathbb{Z}\backslash\mathbb{Z},\ y = 3, 4, 9, 10\right\}.\end{aligned}$$

Proof. In order to generate the ray class field of an imaginary quadratic field K with conductor 12, we shall use Lemma 16 and the fact that

$$\mathfrak{F}_{12} = \mathbb{Q}(j, f_{(a_1,a_2)} \mid (a_1, a_2) \in 12^{-1}\mathbb{Z}^2, \notin \mathbb{Z}^2).$$

To this end, considering lattice points (modulo 12) in a plane, divide the set proposed in the lemma into subsets by considering elements of the form $(0,t)\gamma$ with $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. Observe that

$$A=\{(a_1,a_1x)\mid a_1\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z},\ x=0,\dots,11\},$$
$$B=\{(a_2x,a_2)\mid a_2\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z},\ x=0,\dots,11\}.$$

Direct computation shows that the elements not in $A\cup B$ form a set

$$\begin{aligned}E=\{&(2,3),(2,9),(3,2),(3,4),(3,8),(3,10),(4,3),(4,6),(4,9),(6,4),(6,8),\\&(8,3),(8,6),(8,9),(9,2),(9,4),(9,8),(9,10),(10,3),(10,9)\}.\end{aligned}$$

Now we embed E into a subset whose elements are of the form $(0,t)\gamma$ with $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. Since $(a_1,a_2)|_T=(a_1,a_1+a_2)\pmod{12}$ for $T=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$,

$$\begin{aligned}E|_T=\{&(2,5),(2,11),(3,5),(3,7),(3,11),(3,1),(4,7),(4,10),(4,1),(6,10),\\&(6,2),(8,11),(8,2),(8,5),(9,11),(9,1),(9,5),(9,7),(10,1),(10,7)\}.\end{aligned}$$

It follows that the congruence $t'y\equiv s'\pmod{12}$ yields $y=3,4,9$ or 10, when $(s,t)T=(s',t')$ for $(s,t)\in E$. Thus we get

$$E|_T\subset\{(a_2y,a_2)\mid a_2\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z},\ y=3,4,9,10\};$$

in other words,

$$E\subset C=\left\{(0,a_2)\begin{pmatrix}1&0\\y&1\end{pmatrix}\begin{pmatrix}1&-1\\0&1\end{pmatrix}\ \middle|\ a_2\in 12^{-1}\mathbb{Z}\backslash\mathbb{Z},\ y=3,4,9,10\right\}$$

which completes the proof. ∎

THEOREM 18. *Let K and α be as in Theorem 12, and let $K_{(12)}$ denote the ray class field over K with conductor 12. Then*

$$\begin{aligned}K_{(12)}=K\bigg(&j_{1,12}\Big(\frac{-1}{\alpha+x}\Big)/\sqrt{3},\ j_{1,12}\Big(\frac{\alpha}{x\alpha+1}\Big)/\sqrt{3},\\&j_{1,12}\Big(\frac{\alpha-1}{y\alpha+1-y}\Big)/\sqrt{3}\ \bigg|\ x=0,\dots,11\text{ and }y=3,4,9,10\bigg).\end{aligned}$$

Proof. For each $z\in\mathfrak{H}$, we have

$$\begin{aligned}\mathfrak{F}_{12}&=\mathbb{Q}(j(z),f_{(a_1,a_2)}(z)\mid(a_1,a_2)\in 12^{-1}\mathbb{Z}^2,\notin\mathbb{Z}^2)\quad\text{by (2)}\\&=\mathbb{Q}(j(z),f_{(0,a_1)}|_{\left(\begin{smallmatrix}0&-1\\1&x\end{smallmatrix}\right)}\mid a_1\in 12^{-1}\mathbb{Z},\notin\mathbb{Z},\ x=0,\dots,11)\\&\quad\cup\mathbb{Q}(j(z),f_{(0,a_2)}|_{\left(\begin{smallmatrix}1&0\\x&1\end{smallmatrix}\right)}\mid a_2\in 12^{-1}\mathbb{Z},\notin\mathbb{Z},\ x=0,\dots,11)\\&\quad\cup\mathbb{Q}(j(z),f_{(0,a_2)}|_{\left(\begin{smallmatrix}1&0\\y&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right)}\mid a_2\in 12^{-1}\mathbb{Z},\notin\mathbb{Z},\ y=3,4,9,10)\\&\qquad\text{by Lemma 17 and (4)}\end{aligned}$$

$$= \mathbb{Q}\Big(j_{1,12}\Big(\frac{-1}{z+x}\Big)/\sqrt{3}, j_{1,12}\Big(\frac{z}{xz+1}\Big)/\sqrt{3}, j_{1,12}\Big(\frac{z-1}{yz+1-y}\Big)/\sqrt{3} \;\Big|\; x=0,\dots,11 \text{ and } y=3,4,9,10\Big) \quad \text{by Lemma 16.}$$

Therefore, the result follows from Theorem 12. ■

By class field theory ([19], Section 5.2, or [21], Theorem 3.6), the reciprocity map induces an isomorphism

$$[\cdot, K] : K_{\mathbb{A}}^{\times}/K^{\times}U_{(12)} \xrightarrow{\sim} \mathrm{Gal}(K_{(12)}/K)$$

where $U_{(12)}$ is the subgroup of $K_{\mathbb{A}}^{\times}$ given by

$$U_{(12)} = \{s \in K_{\mathbb{A}}^{\times} \mid s_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ and } s_{\mathfrak{p}} \equiv 1 \pmod{(12)\mathcal{O}_{\mathfrak{p}}} \text{ for all finite primes } \mathfrak{p}\}.$$

5. Generation III.

Let K be an imaginary quadratic field, $\mathcal{O}_K$ the maximal order of K and $\mathfrak{a} = [z_1, z_2]$ an $\mathcal{O}_K$-ideal with $\alpha := z_1/z_2 \in \mathfrak{H}$. Since α is an imaginary quadratic element, α satisfies an integral equation $az^2 + bz + c = 0$. In this section, we shall find class fields generated by singular values $j_{1,12}(\alpha)$ and $j_{1,12}(\alpha)^2$ under some conditions on a and the discriminant d_K $(= b^2 - 4ac)$ of K. First, we need the following lemma which is a modification of a statement in the proof of Theorem 3.7.5 in [1].

LEMMA 19. *Let f be a modular function of level 12 with rational Fourier coefficients and (β) a principal ideal of $\mathcal{O}_K$ relatively prime to 12. Put $\beta = m + n(a\alpha) \in \mathbb{Z} + \mathbb{Z}(a\alpha) = \mathcal{O}_K$ and let $\mathcal{A}_\beta$ be a matrix in $\mathrm{SL}_2(\mathbb{Z})$ whose image in $\mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z})$ is equal to*

$$\begin{pmatrix} -bn+m & -cn \\ anN(\beta)^{-1} & mN(\beta)^{-1} \end{pmatrix}.$$

Then the action of (β) on $f(\alpha)$ is given by

$$f(\alpha)^{[(\beta), K_{(12)}/K]} = f(\mathcal{A}_\beta \cdot \alpha).$$

In Theorem 18, we generated the ray class field $K_{(12)}$ over K by 28 singular values of $j_{1,12}$. However, whenever a is relatively prime to 12, we now see that $K_{(12)}$ is simply generated by one singular value $j_{1,12}(\alpha)$ and, moreover, $j_{0,12}(\alpha)$ defined below spans some ring class field.

THEOREM 20. *Notations being as above, let $az^2 + bz + c = 0$ be the equation of α such that $a > 0$, $(a, b, c) = 1$, and let $j_{0,12}(z) = j_{1,12}(z)^2 = \theta_3(2z)^2/\theta_3(6z)^2$. Suppose that $(a, 12) = 1$. Then*:

(1) *$j_{0,12}(\alpha)$ generates the ring class field of an imaginary quadratic order $\mathcal{O}$ $(= \mathbb{Z} + 12\mathcal{O}_K)$ with discriminant $12^2 d_K$.*

(2) $j_{1,12}(\alpha)$ *generates the ray class field* $K_{(12)}$ *of* K *with conductor* 12, *and the degree of* $K(j_{1,12}(\alpha))$ *over* K *is* $2h(\mathcal{O})$, *where* $h(\mathcal{O})$ *is the class number of* $\mathcal{O}$.

Proof. (1) By Theorem 1(1), $j_{0,12}(z) \in K(X_0(12))$. We observe that

$$[K(X_1(12)) : \mathbb{C}(j_{0,12}(z))] = [\mathbb{C}(j_{1,12}(z)) : \mathbb{C}(j_{0,12}(z))] = 2.$$

Since $[\overline{\Gamma}_0(N) : \overline{\Gamma}_1(N)] = \frac{1}{2}\phi(N)$ for $N > 2$, with ϕ the Euler phi function, it follows that $[K(X_1(12)) : K(X_0(12))] = [\overline{\Gamma}_0(12) : \overline{\Gamma}_1(12)] = 2$; whence $K(X_0(12)) = \mathbb{C}(j_{0,12}(z))$. This indicates that $j_{0,12}(z)$ is a field generator of a genus zero curve, and so we are able to normalize it as

$$N(j_{0,12}(z)) = \frac{4}{j_{0,12}(z) - 1} + 1 = T_{12I}(z),$$

the Thompson series of type $12I$. Now the result follows from [1], Theorem 3.7.5(1).

(2) Let $L_0 = K(j_{0,12}(\alpha))$ and $L_1 = K(j_{1,12}(\alpha))$. Then we have the following field tower:

$$K \subseteq L_0 \subseteq L_1 \subseteq K_{(12)}.$$

Here the last inclusion follows from Theorem 12. For a subfield L of $K_{(12)}$, let $\Phi_{L/K} : I_K(12) \to \mathrm{Gal}(L/K)$ signify the Artin map, where $I_K(12) = \{\text{fractional ideal } \mathfrak{a} \mid (\mathfrak{a}, 12\mathcal{O}_K) = 1\}$, which forms a group under multiplication. Then $\mathrm{Ker}(\Phi_{K_{(12)}/K}) = P_{K,1}(12)$ and

$$P_{K,1}(12) \subseteq \mathrm{Ker}(\Phi_{L_1/K}) \subseteq \mathrm{Ker}(\Phi_{L_0/K}) \subseteq I_K(12)$$

by class field theory, where $P_{K,1}(12)$ denotes the subgroup of $I_K(12)$ generated by the principal ideals $\beta\mathcal{O}_K$ with $\beta \in \mathcal{O}_K$ and $\beta \equiv 1 \pmod{12\mathcal{O}_K}$. Since L_0 is the ring class field of $\mathcal{O} = \mathbb{Z} + 12\mathcal{O}_K$, it follows from class field theory (e.g. [3]) that

$$\mathrm{Pic}(\mathcal{O}) = I(\mathcal{O}, 12)/P(\mathcal{O}, 12) \cong I_K(12)/P_{K,\mathbb{Z}}(12) \cong \mathrm{Gal}(L_0/K),$$

where the last isomorphism is induced by the Artin map $\Phi_{L_0/K}$, and $P_{K,\mathbb{Z}}(12)$ denotes the subgroup of $I_K(12)$ generated by the principal ideals $\beta\mathcal{O}_K$ with $\beta \in \mathcal{O}_K$ and $\beta \equiv l \pmod{12\mathcal{O}_K}$ for some integer l relatively prime to 12. Therefore we get $\mathrm{Ker}(\Phi_{L_0/K}) = P_{K,\mathbb{Z}}(12)$ and

$$P_{K,1}(12) \subseteq \mathrm{Ker}(\Phi_{L_1/K}) \subseteq P_{K,\mathbb{Z}}(12).$$

Since $P_{K,\mathbb{Z}}(12)/P_{K,1}(12)$ is isomorphic to $(\mathbb{Z}/12\mathbb{Z})^\times/\{\pm 1\}$, the degree of $P_{K,\mathbb{Z}}(12)$ over $P_{K,1}(12)$ is 2. Thus we have either $\mathrm{Ker}(\Phi_{L_1/K}) = P_{K,1}(12)$ or $\mathrm{Ker}(\Phi_{L_1/K}) = P_{K,\mathbb{Z}}(12)$, and hence it remains to prove $\mathrm{Ker}(\Phi_{L_1/K}) = P_{K,1}(12)$.

Now, we take two integers n and m such that $12 \mid n$ and $m \equiv \pm 5 \pmod{12}$. Let (β) be a principal ideal of $\mathcal{O}_K$ prime to 12, and $\mathcal{A}_\beta$ be as in Lemma 19. Then $\mathcal{A}_\beta \in \Gamma_0(12)\setminus \pm\Gamma_1(12)$, and since

$$\chi_3(m\cdot N(\beta)^{-1}) = \left(\frac{3}{m}\right)\left(\frac{1}{N(\beta)^{-1}}\right) = -1\cdot 1 = -1,$$

we get $j_{1,12}(\mathcal{A}_\beta\cdot\alpha) = -j_{1,12}(\alpha)$ by Theorem 1(1). Since $j_{1,12}$ never vanishes on $\mathfrak{H}$, we must have $j_{1,12}(\mathcal{A}_\beta\cdot\alpha)\neq j_{1,12}(\alpha)$.

On the other hand, $j_{0,12}(\mathcal{A}_\beta\cdot\alpha) = j_{1,12}(\mathcal{A}_\beta\cdot\alpha)^2 = j_{0,12}(\alpha)$, from which we get $(\beta)\in \mathrm{Ker}(\Phi_{L_0/K})\setminus \mathrm{Ker}(\Phi_{L_1/K})$. Therefore $\mathrm{Ker}(\Phi_{L_1/K})$ is equal to $P_{K,1}(12)$, and $L_1 = K_{(12)}$ by class field theory. The last assertion follows from the fact that $j_{0,12}(\alpha)$ generates the ring class field of $\mathcal{O}$ and $[K(j_{1,12}(\alpha)) : K(j_{0,12}(\alpha))] = 2$. ∎

Examples. Put $K = \mathbb{Q}(\sqrt{N})$ with N a square-free negative integer. Then $j_{0,12}((1+\sqrt{N})/2)$ (resp. $j_{0,12}(\sqrt{N})$) generates the ring class field of an imaginary quadratic order $\mathcal{O}$ ($= \mathbb{Z}+12\mathcal{O}_K$) with discriminant $12^2 d_K$ provided that $N\equiv 1 \pmod 4$ (resp. $N\equiv 2,3 \pmod 4$) and $j_{1,12}((1+\sqrt{N})/2)$ (resp. $j_{1,12}(\sqrt{N})$) generates the ray class field $K_{(12)}$ of K with conductor 12 if $N\equiv 1 \pmod 4$ (resp. $N\equiv 2,3 \pmod 4$).

As for the construction of the ray class fields over imaginary quadratic fields with conductor strictly dividing 12, we need to consider some other conditions on a and d_K, different from the previous one. We shall illustrate this in two theorems; one excluding the cases $d_K = -3$ and -4, the other only with $d_K = -3$ and -4.

Theorem 21. *Notations being as above, let $az^2+bz+c=0$ be the equation of α such that $a>0$ and $(a,b,c)=1$, and let $K_\mathfrak{f}$ be a ray class field over K with conductor $\mathfrak{f}$. Assume that the discriminant of K is neither -4 nor -3 (i.e. $K\neq \mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-3})$). Then:*

(1) *If $(a,12)=2$, then $j_{1,12}(\alpha)$ generates $K_\mathfrak{f}$ over K with conductor $\mathfrak{f}$ given by*

$$\mathfrak{f} = \begin{cases} 3[2,a\alpha]^3, & d_K\equiv 0 \pmod 4,\\ 3[2,a\alpha][2,a\alpha+1]^2, & d_K\equiv 1 \pmod 8.\end{cases}$$

Furthermore, 2 *ramifies in K when $d_K\equiv 0 \pmod 4$ and splits completely in K if $d_K\equiv 1 \pmod 8$, and so*

$$12\mathcal{O}_K = \begin{cases} 3[2,a\alpha]^4, & d_K\equiv 0 \pmod 4,\\ 3[2,a\alpha]^2[2,a\alpha+1]^2, & d_K\equiv 1 \pmod 8.\end{cases}$$

(2) *If $(a,12)=3$, then $j_{1,12}(\alpha)$ generates $K_\mathfrak{f}$ with conductor $\mathfrak{f}$ given by*

$$\mathfrak{f} = \begin{cases} 4[3,a\alpha], & b\equiv 0 \pmod 3,\\ 4[3,a\alpha+1], & b\equiv 1 \pmod 3,\\ 4[3,a\alpha+2], & b\equiv 2 \pmod 3.\end{cases}$$

Moreover,

$$12\mathcal{O}_K = \begin{cases} 4[3, a\alpha]^2, & b \equiv 0 \pmod 3, \\ 4[3, a\alpha][3, a\alpha+1], & b \equiv 1 \pmod 3, \\ 4[3, a\alpha][3, a\alpha+2], & b \equiv 2 \pmod 3. \end{cases}$$

(3) *If* $(a, 12) = 4$ *and* $d_K \equiv 1 \pmod 8$, *then* $j_{1,12}(\alpha)$ *generates* $K_{\mathfrak{f}}$ *with conductor* $\mathfrak{f} = 3[2, a\alpha+1]^2$ *and* $12\mathcal{O}_K = 3[2, a\alpha]^2[2, a\alpha+1]^2$.

(4) *If* $(a, 12) = 6$ *and* $d_K \not\equiv 5 \pmod 8$, *then* $j_{1,12}(\alpha)$ *generates* $K_{\mathfrak{f}}$ *with conductor* $\mathfrak{f}$ *given by*

$$\mathfrak{f} = \begin{cases} [2, a\alpha]^3[3, a\alpha], & b \equiv 0 \pmod 6, \\ [2, a\alpha][2, a\alpha+1]^2[3, a\alpha+1], & b \equiv 1 \pmod 6, \\ [2, a\alpha]^3[3, a\alpha+2], & b \equiv 2 \pmod 6, \\ [2, a\alpha][2, a\alpha+1]^2[3, a\alpha], & b \equiv 3 \pmod 6, \\ [2, a\alpha]^3[3, a\alpha+1], & b \equiv 4 \pmod 6, \\ [2, a\alpha][2, a\alpha+1]^2[3, a\alpha+2], & b \equiv 5 \pmod 6. \end{cases}$$

Moreover,

$$12\mathcal{O}_K = \begin{cases} [2, a\alpha]^4[3, a\alpha]^2, & b \equiv 0 \pmod 6, \\ [2, a\alpha]^2[2, a\alpha+1]^2[3, a\alpha][3, a\alpha+1], & b \equiv 1 \pmod 6, \\ [2, a\alpha]^4[3, a\alpha][3, a\alpha+2], & b \equiv 2 \pmod 6, \\ [2, a\alpha]^2[2, a\alpha+1]^2[3, a\alpha]^2, & b \equiv 3 \pmod 6, \\ [2, a\alpha]^4[3, a\alpha][3, a\alpha+1], & b \equiv 4 \pmod 6, \\ [2, a\alpha]^2[2, a\alpha+1]^2[3, a\alpha][3, a\alpha+2], & b \equiv 5 \pmod 6. \end{cases}$$

(5) *If* $(a, 12) = 12$ *and* $d_K \equiv 1 \pmod 8$, *then* $j_{1,12}(\alpha)$ *generates* $K_{\mathfrak{f}}$ *with conductor* $\mathfrak{f}$ *given by*

$$\mathfrak{f} = \begin{cases} [2, a\alpha+1]^2[3, a\alpha], & b \equiv 0 \pmod 3, \\ [2, a\alpha+1]^2[3, a\alpha+1], & b \equiv 1 \pmod 3, \\ [2, a\alpha+1]^2[3, a\alpha+2], & b \equiv 2 \pmod 3. \end{cases}$$

Further,

$$12\mathcal{O}_K = \begin{cases} [2, a\alpha]^2[2, a\alpha+1]^2[3, a\alpha]^2, & b \equiv 0 \pmod 3, \\ [2, a\alpha]^2[2, a\alpha+1]^2[3, a\alpha][3, a\alpha+1], & b \equiv 1 \pmod 3, \\ [2, a\alpha]^2[2, a\alpha+1]^2[3, a\alpha][3, a\alpha+2], & b \equiv 2 \pmod 3. \end{cases}$$

Proof. As in Theorem 20, for a subfield L of $K_{(12)}$, let $\Phi_{L/K} : I_K(12) \to \mathrm{Gal}(L/K)$ be the Artin map. Since $j_{1,12}(\alpha) \in K_{(12)}$ by Theorem 12, we have $K \subseteq K(j_{1,12}(\alpha)) \subseteq K_{(12)}$ so that

$$P_{K,1}(12) = \mathrm{Ker}(\Phi_{K_{(12)}/K}) \subseteq \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}).$$

Let $\mathfrak{a} \in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K})$. Then $\Phi_{K(j_{1,12}(\alpha))/K}(\mathfrak{a}) = [\mathfrak{a}, K(j_{1,12}(\alpha))/K]$ fixes $j_{1,12}(\alpha)$ and hence it fixes $j(\alpha)$, too. Since $K(j(\alpha))$ is the Hilbert class field of K, $I_K/P_K \cong \mathrm{Gal}(K(j(\alpha))\,/K)$. And the fact that $[\mathfrak{a}, K(j_{1,12}(\alpha))/K]$ is trivial on $K(j(\alpha))$ implies $\mathfrak{a} \in P_K \cap I_K(12) = P_K(12)$.

Now we write $\mathfrak{a} = \beta\mathcal{O}_K$ with $\beta \in \mathcal{O}_K$ and $(N(\beta), 12) = 1$. Let $\beta = m+n(a\alpha) \in \mathbb{Z}+\mathbb{Z}\cdot(a\alpha) = \mathcal{O}_K$. Considering $\mathcal{A}_\beta$ described in Lemma 19, we see that $(\beta) \in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K})$ if and only if $\mathcal{A}_\beta \in \pm\Gamma_1(12)\cdot\Gamma_\alpha$, where $\Gamma_\alpha = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma(\alpha) = \alpha\}$. Note that Γ_α is nontrivial if and only if α is equivalent to i or $\varrho = e^{2\pi i/3}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$. In view of quadratic forms we see that Γ_α is nontrivial if and only if $d_K = -4$ or -3, that is, $K = \mathbb{Q}(\sqrt{-1})$ or $K = \mathbb{Q}(\sqrt{-3})$. By our assumption, however, Γ_α must be trivial; hence

$$(\beta) \in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) \Leftrightarrow \mathcal{A}_\beta \in \pm\Gamma_1(12).$$

(1) Suppose that $(a, 12) = 2$. Then, for $(\beta) \in I_K(12)$,

$$\begin{aligned}(\beta) \in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) &\Leftrightarrow \mathcal{A}_\beta \in \pm\Gamma_1(12)\\ &\Leftrightarrow 12 \mid an \text{ and } -bn+m \equiv \pm 1 \pmod{12}\\ &\Leftrightarrow 6 \mid n \text{ and } m \in \pm 1 + bn + 12\mathbb{Z} \text{ since } (a,12) = 2\\ &\Leftrightarrow \pm\beta \in 1 + 6[2, a\alpha + b]\\ &\Leftrightarrow (\beta) \in P_{K,1}(\mathfrak{f}) \text{ with } \mathfrak{f} = 6[2, a\alpha + b].\end{aligned}$$

Therefore we have

$$\mathrm{Gal}(K(j_{1,12}(\alpha))/K) \cong I_K(12)/P_{K,1}(\mathfrak{f}) \cap I_K(12) \cong I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f}),$$

and $K(j_{1,12}(\alpha)) = K_\mathfrak{f}$ by class field theory.

We observe that $[2, a\alpha + b]$ is the prime ideal $\mathfrak{p}$ of K lying above $2\mathbb{Z}$ which would be $[2, a\alpha]$ (resp. $[2, a\alpha+1]$) if $d_K \equiv 0 \pmod 4$ (resp. $d_K \equiv 1 \pmod 8$). Since the polynomial $X^2 + bX + ac$ of $a\alpha$ is congruent to

$$\begin{cases} X^2 \pmod 2 & \text{if } d_K \equiv 0 \pmod 4,\\ X(X+1) \pmod 2 & \text{if } d_K \equiv 1 \pmod 8,\end{cases}$$

we see that 2 ramifies into $[2, a\alpha]^2$ when $d_K \equiv 0 \pmod 4$ and splits completely into $[2, a\alpha][2, a\alpha+1]$ if $d_K \equiv 1 \pmod 8$. Note that $I_K(12) = I_K(\mathfrak{f})$ because

$$\mathfrak{f}\,(= 6\mathfrak{p}) = \begin{cases} 3[2, a\alpha]^3, & d_K \equiv 0 \pmod 4,\\ 3[2, a\alpha][2, a\alpha+1]^2, & d_K \equiv 1 \pmod 8\end{cases}$$

and

$$12\mathcal{O}_K = \begin{cases} 3[2, a\alpha]^4, & d_K \equiv 0 \pmod 4,\\ 3[2, a\alpha]^2[2, a\alpha+1]^2, & d_K \equiv 1 \pmod 8.\end{cases}$$

(2) Assume that $(a, 12) = 3$. Then, in a similar manner, we find that for $(\beta) \in I_K(12)$,

$$\begin{aligned}(\beta) \in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) &\Leftrightarrow \mathcal{A}_\beta \in \pm\Gamma_1(12)\\ &\Leftrightarrow \pm\beta \in 1 + 4[3, a\alpha + b]\\ &\Leftrightarrow (\beta) \in P_{K,1}(\mathfrak{f}) \text{ with } \mathfrak{f} = 4[3, a\alpha + b].\end{aligned}$$

Hence $\mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) = P_{K,1}(\mathfrak{f}) \cap I_K(12)$, and so $K(j_{1,12}(\alpha)) = K_{\mathfrak{f}}$.

Here, we note that the prime ideal $[3, a\alpha+b]$ would be $[3, a\alpha+i]$ if $b \equiv i \pmod 3$ for $i = 0, 1, 2$. Since the polynomial $X^2+bX+ac$ of $a\alpha$ is congruent to

$$\begin{cases} X^2 \pmod 3 & \text{if } b \equiv 0 \pmod 3, \\ X(X+1) \pmod 3 & \text{if } b \equiv 1 \pmod 3, \\ X(X+2) \pmod 3 & \text{if } b \equiv 2 \pmod 3, \end{cases}$$

we claim that 3 ramifies into $[3, a\alpha]^2$ when $b \equiv 0 \pmod 3$ and splits completely into $[3, a\alpha][3, a\alpha+1]$ (resp. $[3, a\alpha][3, a\alpha+2]$) when $b \equiv 1 \pmod 3$ (resp. $b \equiv 2 \pmod 3$). Observe in addition that $I_K(12) = I_K(\mathfrak{f})$ only if $d_K \equiv 0 \pmod 3$ (i.e. $b \equiv 0 \pmod 3$) because

$$\begin{aligned} \mathfrak{f} &= 4[3, a\alpha], & 12\mathcal{O}_K &= 4[3, a\alpha]^2, \\ \mathfrak{f} &= 4[3, a\alpha+1], & 12\mathcal{O}_K &= 4[3, a\alpha][3, a\alpha+1], \\ \mathfrak{f} &= 4[3, a\alpha+2], & 12\mathcal{O}_K &= 4[3, a\alpha][3, a\alpha+2]. \end{aligned}$$

(3) Assume that $(a, 12) = 4$. Then, for $(\beta) \in I_K(12)$,

$$\begin{aligned} (\beta) \in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) &\Leftrightarrow \mathcal{A}_\beta \in \pm\Gamma_1(12) \\ &\Leftrightarrow 12 \mid an \text{ and } -bn+m \equiv \pm 1 \pmod{12} \\ &\Leftrightarrow 3 \mid n \text{ and } m \in \pm 1 + bn + 12\mathbb{Z} \text{ since } (a, 12) = 4 \\ &\Leftrightarrow \pm\beta \in 1 + 3[4, a\alpha+b]. \end{aligned}$$

Due to $d_K \equiv 1 \pmod 8$ one can easily show that $[4, a\alpha+b] = [2, a\alpha+1]^2$. Therefore, $K(j_{1,12}(\alpha)) = K_{\mathfrak{f}}$ with $\mathfrak{f} = 3[2, a\alpha+1]^2$.

(4) Assume that $(a, 12) = 6$. Then, for $(\beta) \in I_K(12)$,

$$\begin{aligned} &(\beta) \in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) \\ &\qquad \Leftrightarrow \mathcal{A}_\beta \in \pm\Gamma_1(12) \\ &\qquad \Leftrightarrow \pm\beta \in 1 + 2[6, a\alpha+b] = 1 + 2[2, a\alpha+b][3, a\alpha+b] \\ &\qquad \Leftrightarrow (\beta) \in P_{K,1}(\mathfrak{f}) \text{ with } \mathfrak{f} = 2[2, a\alpha+b][3, a\alpha+b]. \end{aligned}$$

We conclude that $K(j_{1,12}(\alpha)) = K_{\mathfrak{f}}$. Note that $[6, a\alpha+b]$ is equal to

$$\begin{array}{llll} [2, a\alpha][3, a\alpha], & b \equiv 0 \pmod 6, & [2, a\alpha+1][3, a\alpha+1], & b \equiv 1 \pmod 6, \\ [2, a\alpha][3, a\alpha+2], & b \equiv 2 \pmod 6, & [2, a\alpha+1][3, a\alpha], & b \equiv 3 \pmod 6, \\ [2, a\alpha][3, a\alpha+1], & b \equiv 4 \pmod 6, & [2, a\alpha+1][3, a\alpha+2], & b \equiv 5 \pmod 6. \end{array}$$

Since the polynomial $X^2+bX+ac$ of $a\alpha$ is congruent to

$$\begin{cases} X^2 \pmod 2, X^2 \pmod 3 & \text{if } b\equiv 0 \pmod 6,\\ X(X+1) \pmod 2, X(X+1) \pmod 3 & \text{if } b\equiv 1 \pmod 6,\\ X^2 \pmod 2, X(X+2) \pmod 3 & \text{if } b\equiv 2 \pmod 6,\\ X(X+1) \pmod 2, X^2 \pmod 3 & \text{if } b\equiv 3 \pmod 6,\\ X^2 \pmod 2, X(X+1) \pmod 3 & \text{if } b\equiv 4 \pmod 6,\\ X(X+1) \pmod 2, X(X+2) \pmod 3 & \text{if } b\equiv 5 \pmod 6,\end{cases}$$

we see that 2 (resp. 3) ramifies into $[2,a\alpha]^2$ (resp. $[3,a\alpha]^2$) when $d_K\equiv 0 \pmod 6$ (i.e. $b\equiv 0 \pmod 6$), and either 2 or 3 splits completely otherwise. Moreover, observe that $I_K(12)=I_K(\mathfrak{f})$ only if $b\equiv 0$ or $3 \pmod 6$ because

- if $b\equiv 0 \pmod 6$ then

$$\mathfrak{f}=[2,a\alpha]^3[3,a\alpha],\qquad 12\mathcal{O}_K=[2,a\alpha]^4[3,a\alpha]^2,$$

- if $b\equiv 1 \pmod 6$ then

$$\mathfrak{f}=[2,a\alpha][2,a\alpha+1]^2[3,a\alpha+1],\qquad 12\mathcal{O}_K=[2,a\alpha]^2[2,a\alpha+1]^2[3,a\alpha][3,a\alpha+1],$$

- if $b\equiv 2 \pmod 6$ then

$$\mathfrak{f}=[2,a\alpha]^3[3,a\alpha+2],\qquad 12\mathcal{O}_K=[2,a\alpha]^4[3,a\alpha][3,a\alpha+2],$$

- if $b\equiv 3 \pmod 6$ then

$$\mathfrak{f}=[2,a\alpha][2,a\alpha+1]^2[3,a\alpha],\qquad 12\mathcal{O}_K=[2,a\alpha]^2[2,a\alpha+1]^2[3,a\alpha]^2,$$

- if $b\equiv 4 \pmod 6$ then

$$\mathfrak{f}=[2,a\alpha]^3[3,a\alpha+1],\qquad 12\mathcal{O}_K=[2,a\alpha]^4[3,a\alpha][3,a\alpha+1],$$

- if $b\equiv 5 \pmod 6$ then

$$\mathfrak{f}=[2,a\alpha][2,a\alpha+1]^2[3,a\alpha+2],\qquad 12\mathcal{O}_K=[2,a\alpha]^2[2,a\alpha+1]^2[3,a\alpha][3,a\alpha+2].$$

(5) Assume that $(a,12)=12$. Then, for $(\beta)\in I_K(12)$,

$$\begin{aligned}(\beta)\in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) &\Leftrightarrow \mathcal{A}_\beta\in \pm\Gamma_1(12)\\ &\Leftrightarrow 12\,|\,an \text{ and } -bn+m\equiv \pm 1 \pmod{12}\\ &\Leftrightarrow m\in \pm 1+bn+12\mathbb{Z} \text{ since } (a,12)=12\\ &\Leftrightarrow \pm\beta\in 1+[12,a\alpha+b]=1+[3,a\alpha+b][4,a\alpha+b].\end{aligned}$$

Therefore $K(j_{1,12}(\alpha))=K_{\mathfrak{f}}$ with $\mathfrak{f}=[3,a\alpha+b][4,a\alpha+b]$. Note that the conductor $\mathfrak{f}$ would be

$$\begin{cases}[2,a\alpha+1]^2[3,a\alpha], & b\equiv 0 \pmod 3,\\ [2,a\alpha+1]^2[3,a\alpha+1], & b\equiv 1 \pmod 3,\\ [2,a\alpha+1]^2[3,a\alpha+2], & b\equiv 2 \pmod 3. \ \blacksquare\end{cases}$$

REMARK 22. (1) In the cases $(a,12)=2,4,6$ and 12, if $d_K\equiv 5 \pmod 8$, there is no α satisfying the hypothesis.

(2) In the cases $(a,12)=4$ and 12, we see that $[4,a\alpha+b]$ $(=[4,a\alpha]$ or $[4,a\alpha+2])$ does not divide $2\mathcal{O}_K$ if $d_K\equiv 0 \pmod 4$.

EXAMPLES. (1) Take $K=\mathbb{Q}(\sqrt{-2})$ and $\mathfrak{a}=[2,\sqrt{-2}]$. Then $d_K=-8\equiv 0 \pmod 4$, so it follows from Theorem 21(1) that $j_{1,12}(\sqrt{-2}/2)$ generates $K_\mathfrak{f}$ over K with $\mathfrak{f}=3[2,\sqrt{-2}]^3$.

Take $K=\mathbb{Q}(\sqrt{-7})$ and $\mathfrak{a}=[2,(-1+\sqrt{-7})/2]$. Then $d_K=-7\equiv 1 \pmod 8$, so it follows from Theorem 21(1) that $j_{1,12}((-1+\sqrt{-7})/4)$ generates $K_\mathfrak{f}$ with

$$\mathfrak{f}=3\left[2,\frac{-1+\sqrt{-7}}{2}\right]\left[2,\frac{1+\sqrt{-7}}{2}\right]^2.$$

(2) Take $K=\mathbb{Q}(\sqrt{-21})$ and $\mathfrak{a}=[21,\sqrt{-21}]$. Then $d_K=-4\cdot 21\equiv 0 \pmod 3$, so it follows from Theorem 21(2) that $j_{1,12}(\sqrt{-21}/21)$ generates $K_\mathfrak{f}$ over K with $\mathfrak{f}=4[3,\sqrt{-21}]$.

(3) Take $K=\mathbb{Q}(\sqrt{-6})$ and $\mathfrak{a}=[6,\sqrt{-6}]$. Then $d_K=-4\cdot 6\equiv 0 \pmod 6$, so it follows from Theorem 21(4) that $j_{1,12}(\sqrt{-6}/6)$ generates $K_\mathfrak{f}$ over K with $\mathfrak{f}=[2,\sqrt{-6}]^3[3,\sqrt{-6}]$.

Take $K=\mathbb{Q}(\sqrt{-15})$ and $\mathfrak{a}=[6,(-3+\sqrt{-15})/2]$. Then $\alpha=(-3+\sqrt{-15})/12$ satisfies the equation $6X^2+3X+1=0$, so it follows from Theorem 21(4) that $j_{1,12}((-3+\sqrt{-15})/12)$ generates $K_\mathfrak{f}$ over K with

$$\mathfrak{f}=\left[2,\frac{1+\sqrt{-15}}{2}\right]\left[2,\frac{-1+\sqrt{-15}}{2}\right]^2\left[3,\frac{-3+\sqrt{-15}}{2}\right].$$

In Theorem 21, we constructed ray class fields $K_\mathfrak{f}$ with conductor $\mathfrak{f}$ which strictly divide 12 under the assumption $K\neq\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-3})$. As we saw in the course of proof, however, a crucial point making its proof formidable was the nontriviality of Γ_α when $K=\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-3})$. We now give other descriptions for spanning $K_\mathfrak{f}$ in these cases by a thorough analysis of Γ_α.

THEOREM 23. *Notations being as in Theorem* 21 *except for the discriminant*, *we have the following assertions*:

(1) *If* $(a,12)=2$, *then* $j_{1,12}(\alpha)$ *generates* $\mathbb{Q}(\sqrt{-1})_\mathfrak{f}$ *over* $\mathbb{Q}(\sqrt{-1})$ *with conductor* $\mathfrak{f}=3[2,a\alpha]^3$. *In this case*, 2 *ramifies in* $\mathbb{Q}(\sqrt{-1})$ *as* $[2,a\alpha]^2$, *and so we have* $12\mathcal{O}_K=3[2,a\alpha]^4$.

(2) *If* $(a,12)=3$, *then* $j_{1,12}(\alpha)$ *generates* $\mathbb{Q}(\sqrt{-3})_\mathfrak{f}$ *over* $\mathbb{Q}(\sqrt{-3})$ *with conductor* $\mathfrak{f}=4[3,a\alpha]$. *Furthermore*, 3 *ramifies in* $\mathbb{Q}(\sqrt{-3})$ *as* $[3,a\alpha]^2$, *and hence* $12\mathcal{O}_K=4[3,a\alpha]^2$.

REMARK 24. (1) In the case $(a,12)=2$ and $K=\mathbb{Q}(\sqrt{-3})$, we see that there is no α satisfying the hypothesis. For, otherwise, $b^2-4ac=-3$ implies that $b^2\equiv 5 \pmod 8$, which is absurd.

(2) In the case $(a,12)=3$ and $K=\mathbb{Q}(\sqrt{-1})$, no such α exists. Indeed, otherwise, $b^2-4ac=-4$ implies that $b^2\equiv 8 \pmod{12}$, which is impossible, too.

(3) In a similar way, in the cases $(a,12)=4,6$ and 12, we see that there exists no such α for both fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$.

Proof (of Theorem 23). (1) The arguments from the beginning to the nontriviality of Γ_α are exactly the same as those in Theorem 21. Suppose that α is equivalent to i under $\mathrm{SL}_2(\mathbb{Z})$, in which case $d_K=-4$. Put $\mathfrak{f}=6[2,a\alpha]$. Then we have, for $(\beta)\in I_K(12)$,

$$\begin{aligned}(\beta)\in P_{K,1}(\mathfrak{f}) &\Leftrightarrow \ \pm\beta\equiv 1 \pmod{\mathfrak{f}} \text{ or } \ \pm\beta i\equiv 1 \pmod{\mathfrak{f}}\\ &\Leftrightarrow \ \pm\beta\in 1+6[2,a\alpha] \text{ or}\\ &\qquad 6\,\Big|\left(\frac{-b}{2}n+m\right) \text{ and } \frac{b}{2}\left(m-\frac{b}{2}n\right)-n\equiv\pm1 \pmod{12}.\end{aligned}$$

Here, the second statement is due to the fact that $a\alpha=-b/2+i$ and $b^2-4ac=-4$. On the other hand,

$$\begin{aligned}(\beta)\in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K}) &\Leftrightarrow \mathcal{A}_\beta\in\pm\Gamma_1(12)\cdot\Gamma_\alpha\\ &\Leftrightarrow \mathcal{A}_\beta\in\pm\Gamma_1(12) \text{ or}\\ &\qquad \mathcal{A}_\beta\cdot\left(\gamma^{-1}\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\gamma\right)\in\pm\Gamma_1(12),\end{aligned}$$

where $\alpha=\gamma^{-1}i$ for some $\gamma=\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$. Since α is the root of the polynomial $[1,0,1]\circ\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)\left(\begin{smallmatrix}z\\1\end{smallmatrix}\right)=(p^2+r^2)z^2+2(pq+rs)z+(q^2+s^2)$, we get $a=p^2+r^2$, $b=2(pq+rs)$ and $c=q^2+s^2$. Thus we get

$$\gamma^{-1}\begin{pmatrix}0&-1\\1&0\end{pmatrix}\gamma=\begin{pmatrix}-(pq+rs)&-(q^2+s^2)\\p^2+r^2&pq+rs\end{pmatrix}=\begin{pmatrix}-b/2&-c\\a&b/2\end{pmatrix}.$$

Therefore,

$$\begin{aligned}\mathcal{A}_\beta\cdot\left(\gamma^{-1}\begin{pmatrix}0&-1\\1&0\end{pmatrix}\gamma\right)&=\begin{pmatrix}-bn+m&-cn\\anN(\beta)^{-1}&mN(\beta)^{-1}\end{pmatrix}\begin{pmatrix}-b/2&-c\\a&b/2\end{pmatrix}\\ &=\begin{pmatrix}b^2n/2-bm/2-acn&*\\(-abn/2+am)N(\beta)^{-1}&*\end{pmatrix},\end{aligned}$$

where

$$\frac{b^2n}{2}-\frac{bm}{2}-acn=-\frac{b}{2}\left(m-\frac{b}{2}n\right)-n.$$

Then we have

$$\begin{aligned}&\mathcal{A}_\beta\in\pm\Gamma_1(12) \text{ or } \mathcal{A}_\beta\cdot\left(\gamma^{-1}\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\gamma\right)\in\pm\Gamma_1(12)\\ &\quad\Leftrightarrow 12\,|\,an,\ m\in\pm1+bn+12\mathbb{Z}, \text{ or}\\ &\qquad 12\,\Big|\,a\left(m-\frac{b}{2}n\right) \text{ and } -\frac{b}{2}\left(m-\frac{b}{2}n\right)-n\equiv\pm1 \pmod{12}\end{aligned}$$

$$\begin{aligned}&\Leftrightarrow 6\,|\,n,\ \pm\beta\in 1+n(a\alpha+b)+12\mathbb{Z},\ \text{or}\\&\quad 6\,\Big|\,\Big(m-\frac{b}{2}n\Big)\ \text{and}\ -\frac{b}{2}\Big(m-\frac{b}{2}n\Big)-n\equiv\pm1 \pmod{12}\\&\Leftrightarrow\ \pm\beta\in 1+6[2,a\alpha+b]=1+6[2,a\alpha],\ \text{or}\\&\quad 6\,\Big|\,\Big(m-\frac{b}{2}n\Big)\ \text{and}\ \frac{b}{2}\Big(m-\frac{b}{2}n\Big)-n\equiv\pm1 \pmod{12}.\end{aligned}$$

Consequently, we see that $(\beta)\in \mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K})\Leftrightarrow(\beta)\in P_{K,1}(\mathfrak{f})\cap I_K(12)$, and the result follows.

(2) Assume that α is equivalent to ϱ under $\mathrm{SL}_2(\mathbb{Z})$, in which case $d_K=-3$. Since $\Gamma_\varrho=\{\pm I_2,\pm\left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right),\pm\left(\begin{smallmatrix}1&1\\-1&0\end{smallmatrix}\right)\}$, we see that

$$\Gamma_\alpha=\Big\{\pm I_2,\pm\gamma^{-1}\begin{pmatrix}0&-1\\1&1\end{pmatrix}\gamma,\pm\gamma^{-1}\begin{pmatrix}1&1\\-1&0\end{pmatrix}\gamma\Big\}$$

for some $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. Put $\mathfrak{f}=4[3,a\alpha]$. Then we have, for $(\beta)\in I_K(12)$,

$$\begin{aligned}(\beta)\in P_{K,1}(\mathfrak{f})&\Leftrightarrow \pm\beta\equiv1 \pmod{\mathfrak{f}}\ \text{or}\ \pm\beta\varrho\equiv1\pmod{\mathfrak{f}}\\&\qquad\text{or}\ \pm\beta\varrho^2\equiv1\pmod{\mathfrak{f}}\\&\Leftrightarrow\ \pm\beta\in1+4[3,a\alpha],\ \text{or}\\&\qquad 4\,\Big|\,\Big(\frac{b+1}{2}n-m\Big)\ \text{and}\ \frac{b-1}{2}m-\frac{b^2+3}{4}n\equiv\pm1\pmod{12},\ \text{or}\\&\qquad 4\,\Big|\,\Big(\frac{b-1}{2}n-m\Big)\ \text{and}\ -\frac{b+1}{2}m+\frac{b^2+3}{4}n\equiv\pm1\pmod{12}.\end{aligned}$$

Here, the second argument is due to the fact that $\varrho=a\alpha+(b-1)/2$, $\varrho^2=-a\alpha-(b+1)/2$ and $b^2-4ac=-3$. On the other hand,

$$\begin{aligned}(\beta)\in\mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K})&\Leftrightarrow\mathcal{A}_\beta\in\pm\Gamma_1(12)\cdot\Gamma_\alpha\\&\Leftrightarrow\mathcal{A}_\beta\in\pm\Gamma_1(12)\ \text{or}\ \mathcal{A}_\beta\cdot\big(\gamma^{-1}\left(\begin{smallmatrix}1&1\\-1&0\end{smallmatrix}\right)\gamma\big)\in\pm\Gamma_1(12)\\&\qquad\text{or}\ \mathcal{A}_\beta\cdot\big(\gamma^{-1}\left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right)\gamma\big)\in\pm\Gamma_1(12),\end{aligned}$$

where $\alpha=\gamma^{-1}\varrho$ for some $\gamma=\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$. Since α is the root of the polynomial $[1,1,1]\circ\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)\left(\begin{smallmatrix}z\\1\end{smallmatrix}\right)=(p^2+pr+r^2)z^2+(2pq+ps+rq+2rs)z+(q^2+qs+s^2)$, we get $a=p^2+pr+r^2$, $b=2pq+ps+rq+2rs$ $(=2(pq+ps+rs)-1=2(pq+rq+rs)+1)$ and $c=q^2+qs+s^2$. Thus

$$\begin{aligned}\gamma^{-1}\begin{pmatrix}1&1\\-1&0\end{pmatrix}\gamma&=\begin{pmatrix}ps+pq+rs&q^2+sq+s^2\\-(p^2+rp+r^2)&-(qr+pq+rs)\end{pmatrix}\\&=\begin{pmatrix}(b+1)/2&c\\-a&-(b-1)/2\end{pmatrix},\end{aligned}$$

and

$$\mathcal{A}_\beta \cdot \left(\gamma^{-1}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\gamma\right)$$

$$= \begin{pmatrix} -bn+m & -cn \\ anN(\beta)^{-1} & mN(\beta)^{-1} \end{pmatrix}\begin{pmatrix} (b+1)/2 & c \\ -a & -(b-1)/2 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{b+1}{2}(-bn+m)+acn & * \\ \left(\frac{b+1}{2}n-m\right)aN(\beta)^{-1} & * \end{pmatrix},$$

where

$$\frac{b+1}{2}(-bn+m)+acn = -b\left(\frac{b+1}{2}n-m\right)-\frac{b-1}{2}m+\frac{b^2+3}{4}n.$$

In the same manner, we have

$$\gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\gamma = \begin{pmatrix} -(pq+rs+rq) & -(q^2+sq+s^2) \\ p^2+rp+r^2 & pq+ps+rs \end{pmatrix}$$

$$= \begin{pmatrix} -(b-1)/2 & -c \\ a & (b+1)/2 \end{pmatrix}$$

and

$$\mathcal{A}_\beta \cdot \left(\gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\gamma\right) = \begin{pmatrix} -\frac{b-1}{2}(-bn+m)-acn & * \\ \left(-\frac{b-1}{2}n+m\right)aN(\beta)^{-1} & * \end{pmatrix},$$

where

$$-\frac{b-1}{2}(-bn+m)-acn = b\left(\frac{b-1}{2}n-m\right)+\frac{b+1}{2}m-\frac{b^2+3}{4}n.$$

So we get

$$\mathcal{A}_\beta \in \pm\Gamma_1(12) \text{ or } \mathcal{A}_\beta \cdot \left(\gamma^{-1}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\gamma\right) \in \pm\Gamma_1(12)$$

$$\text{or } \mathcal{A}_\beta \cdot \left(\gamma^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\gamma\right) \in \pm\Gamma_1(12)$$

$$\Leftrightarrow 12 \,\Big|\, an,\ m \in \pm 1 + bn + 12\mathbb{Z},\ \text{ or } 12 \,\Big|\, a\left(\frac{b+1}{2}n-m\right) \text{ and}$$

$$-b\left(\frac{b+1}{2}n-m\right)-\frac{b-1}{2}m+\frac{b^2+3}{4}n \equiv \pm 1 \pmod{12},\ \text{ or}$$

$$12 \,\Big|\, a\left(-\frac{b-1}{2}n+m\right) \text{ and } b\left(\frac{b-1}{2}n-m\right)+\frac{b+1}{2}m-\frac{b^2+3}{4}n$$

$$\equiv \pm 1 \pmod{12}$$

$$\Leftrightarrow 4 \,\Big|\, n, m \in \pm 1 + bn + 12\mathbb{Z},\ \text{ or } 4 \,\Big|\, \left(\frac{b+1}{2}n-m\right) \text{ and}$$

$$-b\left(\frac{b+1}{2}n-m\right)-\frac{b-1}{2}m+\frac{b^2+3}{4}n\equiv\pm1 \pmod{12},\ \text{or}$$
$$4\,\Big|\left(-\frac{b-1}{2}n+m\right)\ \text{and}\ b\left(\frac{b-1}{2}n-m\right)+\frac{b+1}{2}m-\frac{b^2+3}{4}n$$
$$\equiv\pm1 \pmod{12}$$
$$\Leftrightarrow\ \pm\beta\in 1+4[3,a\alpha+b]=1+4[3,a\alpha],\ \text{or}$$
$$4\,\Big|\left(\frac{b+1}{2}n-m\right)\ \text{and}\ -\frac{b-1}{2}m+\frac{b^2+3}{4}n\equiv\pm1 \pmod{12},\ \text{or}$$
$$4\,\Big|\left(-\frac{b-1}{2}n+m\right)\ \text{and}\ \frac{b+1}{2}m-\frac{b^2+3}{4}n\equiv\pm1 \pmod{12}.$$

Therefore, we see that

$$(\beta)\in\mathrm{Ker}(\Phi_{K(j_{1,12}(\alpha))/K})\Leftrightarrow(\beta)\in P_{K,1}(\mathfrak{f})\cap I_K(12),$$

and the theorem follows. ■

Examples. (1) Take $K=\mathbb{Q}(\sqrt{-1})$ and $\mathfrak{a}=[1,(1+\sqrt{-1})/2]$. Then $\alpha=(1+\sqrt{-1})/2$ satisfies $2X^2-2X+1=0$. It follows from Theorem 23(1) that $j_{1,12}((1+\sqrt{-1})/2)$ generates $\mathbb{Q}(\sqrt{-1})_{\mathfrak{f}}$ over $\mathbb{Q}(\sqrt{-1})$ with conductor $\mathfrak{f}=3[2,1+\sqrt{-1}]^3$.

(2) Take $K=\mathbb{Q}(\sqrt{-3})$ and $\mathfrak{a}=[3,(-3+\sqrt{-3})/2]$. Then $\alpha=(-3+\sqrt{-3})/6$ satisfies $3X^2+3X+1=0$. We are certain by Theorem 23(2) that $j_{1,12}((-3+\sqrt{-3})/6)$ generates $\mathbb{Q}(\sqrt{-3})_{\mathfrak{f}}$ over $\mathbb{Q}(\sqrt{-3})$ with conductor $\mathfrak{f}=4[3,(-3+\sqrt{-3})/2]$.

Table 1. Conductor $\mathfrak{f}$ of $K(j_{1,12}(\alpha))$
($\times$ means that there is no α satisfying the condition)

	$(a,12)=1$	$(a,12)=2$	$(a,12)=4$
$d_K\equiv0 \pmod 4$	(12)	$3[2,a\alpha]^3$	$\times$
$d_K\equiv1 \pmod 8$	(12)	$3[2,a\alpha][2,a\alpha+1]^2$	$3[2,a\alpha+1]^2$
$d_K\equiv5 \pmod 8$	(12)	$\times$	$\times$

	$(a,12)=3$	$(a,12)=12$, $d_K\equiv1 \pmod 8$	$(a,12)=12$, $d_K\not\equiv1 \pmod 8$
$b\equiv0 \pmod 3$	$4[3,a\alpha]$	$[2,a\alpha+1]^2[3,a\alpha]$	$\times$
$b\equiv1 \pmod 3$	$4[3,a\alpha+1]$	$[2,a\alpha+1]^2[3,a\alpha+1]$	$\times$
$b\equiv2 \pmod 3$	$4[3,a\alpha+2]$	$[2,a\alpha+1]^2[3,a\alpha+2]$	$\times$

Table 1 (cont.)

	$(a,12)=6$, $d_K \not\equiv 5 \pmod 8$	$(a,12)=6$, $d_K \equiv 5 \pmod 8$
$b \equiv 0 \pmod 6$	$[2,a\alpha]^3[3,a\alpha]$	$\times$
$b \equiv 1 \pmod 6$	$[2,a\alpha][2,a\alpha+1]^2[3,a\alpha+1]$	$\times$
$b \equiv 2 \pmod 6$	$[2,a\alpha]^3[3,a\alpha+2]$	$\times$
$b \equiv 3 \pmod 6$	$[2,a\alpha][2,a\alpha+1]^2[3,a\alpha]$	$\times$
$b \equiv 4 \pmod 6$	$[2,a\alpha]^3[3,a\alpha+1]$	$\times$
$b \equiv 5 \pmod 6$	$[2,a\alpha][2,a\alpha+1]^2[3,a\alpha+2]$	$\times$

6. Explicit calculation of minimal polynomials. In this section, we will find an explicit formula for the conjugates of $j_{1,12}(\alpha)$ permitting the numerical calculation of its minimal polynomial. Since $t(\alpha) := N(j_{1,12}(\alpha))$ is an algebraic integer ([11], Corollary 7), it is more convenient to work with t than with $j_{1,12}$ in realizing its minimal polynomial. Let $\mathcal{Q}_{d_K}(N)$ be the set of primitive quadratic forms $[a',b',c']$ having discriminant d_K with conditions $a'>0$ and $(a',N)=1$. For $\gamma \in \Gamma_0(N)$ and $\mathcal{Q} \in \mathcal{Q}_{d_K}(N)$, $\mathcal{Q}\circ\gamma$ again belongs to $\mathcal{Q}_{d_K}(N)$. Hence the quotients $\mathcal{Q}_{d_K}(N)/\Gamma_0(N)$ and $\mathcal{Q}_{d_K}(N)/\Gamma_1(N)$ are well defined.

THEOREM 25. *With K, $\mathfrak{a}$ and α as before, let $az^2+bz+c=0$ be the equation of α such that $a>0$ and $(a,b,c)=1$. Suppose that $(a,12)=1$. Then*:

(1) $|\mathcal{Q}_{d_K}(12)/\Gamma_1(12)| = 2h(\mathcal{O})$, *where $\mathcal{O}=\mathbb{Z}+12\mathcal{O}_K$ and $h(\mathcal{O})$ denotes the class number of $\mathcal{O}$.*

(2) *Let $\{\mathcal{Q}_i\}_{i=1}^{2h(\mathcal{O})}$ be a complete set of representatives for $\mathcal{Q}_{d_K}(12)/\Gamma_1(12)$. Set*

$$f(X)=\prod_{i=1}^{2h(\mathcal{O})}(X-t(\tau_{\mathcal{Q}_i})).$$

Then $f(X)$ is the minimal polynomial of $t(\alpha)$ over K. Here, $\tau_{\mathcal{Q}_i}$ denotes the root of the equation $\mathcal{Q}_i(z,1)=0$ in $\mathfrak{H}$. Moreover, $f(X)\in\mathbb{Z}[X]$.

Proof. First, we recall from [1], Proposition 4.1, that there is a one-to-one correspondence between $\mathcal{Q}_{d_K}(12)/\Gamma_0(12)$ and $I_K(12)/P_{K,\mathbb{Z}}(12)$, which maps $[a,b,c]\in\mathcal{Q}_{d_K}(12)/\Gamma_0(12)$ to $[a,(-b+\sqrt{d_K})/2]\in I_K(12)/P_{K,\mathbb{Z}}(12)$. Hence the cardinality of $\mathcal{Q}_{d_K}(12)/\Gamma_0(12)$ is equal to $h(\mathcal{O})$ because

$$I_K(12)/P_{K,\mathbb{Z}}(12)\cong \mathrm{Gal}(L/K),$$

where L is the ring class field of $\mathcal{O}=\mathbb{Z}+12\mathcal{O}_K$ over K.

Now let $\pi:\mathcal{Q}_{d_K}(12)/\Gamma_1(12)\to\mathcal{Q}_{d_K}(12)/\Gamma_0(12)$ be the natural projection. Choose an element γ in $\Gamma_0(12)\setminus\pm\Gamma_1(12)$, and consider the decomposition $\overline{\Gamma}_0(12)=\overline{\Gamma}_1(12)\cup\gamma\overline{\Gamma}_1(12)$ as transformation groups. It can be easily shown that $\pi^{-1}(\mathcal{Q})=\{\mathcal{Q},\mathcal{Q}\circ\gamma\}$ for each $\mathcal{Q}\in\mathcal{Q}_{d_K}(12)/\Gamma_0(12)$. We claim that $\mathcal{Q}$ cannot be equivalent to $\mathcal{Q}\circ\gamma$ under $\Gamma_1(12)$. Indeed, if $\mathcal{Q}\sim\mathcal{Q}\circ\gamma$ under $\Gamma_1(12)$, then $\mathcal{Q}=\mathcal{Q}\circ\gamma'$ for some $\gamma'\in\Gamma_0(12)\backslash\pm\Gamma_1(12)$. Let $\tau_{\mathcal{Q}}$ $(\in\mathfrak{H})$ be the root of $\mathcal{Q}(z,1)=0$. Then $\gamma'^{-1}\tau_{\mathcal{Q}}$ is the root of $\mathcal{Q}\circ\gamma'$ in $\mathfrak{H}$ and it must be equal to $\tau_{\mathcal{Q}}$. On the other hand, we see that $\Gamma_0(12)$ has no elliptic element ([19], Proposition 1.43). Thus γ' turns out to be trivial, which is a contradiction. This proves (1).

We note that the order $\mathcal{O}_{\mathfrak{a}}$ of an $\mathcal{O}_K$-ideal $\mathfrak{a}$ is $\mathcal{O}_K$ itself. Since $\mathcal{O}_{\mathfrak{a}}=\mathcal{O}_K=[1,a\alpha]$, $b^2-4ac=d_K<0$, $(a,12)=1$ and $(a,b,c)=1$, $[a,b,c]$ belongs to $\mathcal{Q}_{d_K}(12)$. Hence $t(\alpha)=t(\tau_{\mathcal{Q}_i})$ for some i. So $f(X)$ certainly has $t(\alpha)$ as a root. Now we claim that the conjugate of $t(\alpha)$ over K must be of the form $t(\tau')$, where τ' is a root of a quadratic form $[a',b',c']\in\mathcal{Q}_{d_K}(12)$. Indeed, let σ be an embedding of $K_{(12)}$ over K. Then there exists an ideal $\mathfrak{a}\in I_K(12)$ such that $\sigma=[\mathfrak{a},K_{(12)}/K]$. Since t has rational coefficients, we get

$$t(\alpha)^\sigma=t(\alpha)^{[\mathfrak{a},K_{(12)}/K]}=t(\mathcal{A}\cdot\alpha)$$

for some $\mathcal{A}\in G_{\mathbb{Q}+}$ ([1], (3.7.3)). Since $T_{12I}=N(j_{0,12})$ is a rational function of t, it follows that $T_{12I}^\sigma=T_{12I}(\tau')$, where $\tau'=\mathcal{A}\cdot\alpha$. Define $\operatorname{disc}(\tau')=\operatorname{disc}\mathcal{O}_{[1,\tau']}=b'^2-4a'c'$, where $a'\tau'^2+b'\tau'+c'=0$, $a'>0$ and $(a',b',c')=1$. Assume that $\mathcal{A}=\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)\in M_2(\mathbb{Z})$ with $(p,q,r,s)=1$. Put $\operatorname{disc}(\tau')=m^2d_K$. Now, by Theorem 3.7.5(1) of [1], $K(T_{12I}(\tau'))$ is the ring class field of an order $\mathcal{O}'=\mathbb{Z}+f\mathcal{O}_K$, where $f=m\cdot 12/(a',12)$. On the other hand, $K(T_{12I}(\alpha))$ is the ring class field of $\mathcal{O}=\mathbb{Z}+12\mathcal{O}_K$. Since $T_{12I}(\tau')$ is a conjugate of $T_{12I}(\alpha)$, the two fields $K(T_{12I}(\tau'))$ and $K(T_{12I}(\alpha))$ coincide, so that $m=(a',12)$. Let $\mathcal{A}^\iota=\left(\begin{smallmatrix}s&-q\\-r&p\end{smallmatrix}\right)$ be the main involution of $\mathcal{A}$ and $\mathcal{Q}\circ\mathcal{A}^\iota(z,1)=a''z^2+b''z+c''$, where $\mathcal{Q}=[a,b,c]$. Since $\tau'=\mathcal{A}\cdot\alpha$ is a root of the polynomial $\mathcal{Q}\circ\mathcal{A}^\iota(z,1)$ and a'' is positive, it follows that $\mathcal{Q}\circ\mathcal{A}^\iota(z,1)/(a'',b'',c'')=a'z^2+b'z+c'$. By taking discriminants on both sides, we get $\det(\mathcal{A})^2\cdot d_K=(a'',b'',c'')^2\cdot m^2\cdot d_K$, so that m divides $\det(\mathcal{A})$. But $(N(\mathfrak{a}),12)=1$ implies that $(\det(\xi_\alpha(\mathfrak{s}^{-1})),12)=1$, where $\mathfrak{s}$ is an idele corresponding to $\mathfrak{a}$. Thus $(\det(\mathcal{A}),12)=1$ and so $(m,12)=1$. Since $m=(a',12)$, both m and $(a',12)$ must be 1. This shows that $[a',b',c']\in\mathcal{Q}_{d_K}(12)$ and $t(\tau')=t(\tau_{\mathcal{Q}_j})$ for some j. Since $|\mathcal{Q}_{d_K}(12)/\Gamma_1(12)|=2h(\mathcal{O})$ and there are exactly $2h(\mathcal{O})$ conjugates of $t(\alpha)$ (Theorem 20(2)), the first part of the assertion (2) is proved.

For the second part of (2), let $t(z)=q^{-1}+\sum_{n\ge1}H_nq^n$ $(H_n\in\mathbb{Z})$ be the Fourier expansion of t. Write $\tau_{\mathcal{Q}}=x+iy\in\mathfrak{H}$ and consider

$$\begin{aligned}\overline{t(\tau_{\mathcal{Q}})}&=\overline{e^{-2\pi i(x+iy)}}+\sum_{n\ge1}H_n\overline{e^{2\pi in(x+iy)}}=e^{-2\pi i(-x+iy)}+\sum_{n\ge1}H_ne^{2\pi in(-x+iy)}\\&=t(-x+iy)=t(\tau_{\overline{\mathcal{Q}}}),\end{aligned}$$

where $\overline{\mathcal{Q}}$ is defined to be $[a,-b,c]$ when $\mathcal{Q}=[a,b,c]$. Hence the complex conjugate fixes the roots of $f(X)$ and so $f(X)\in\mathbb{R}[X]$. But, since $t(\alpha)$ is an algebraic integer and K is an imaginary quadratic field, $f(X)$ lies in $(\mathbb{R}\cap\mathcal{O}_K)[X]=\mathbb{Z}[X]$. ∎

EXAMPLE. Take $K=\mathbb{Q}(\sqrt{-1})$ and $\mathfrak{a}=[1,\sqrt{-1}]=\mathcal{O}_K$. Then the degree of $K(j_{1,12}(\sqrt{-1}))$ over K is $2h(\mathbb{Z}+12\mathcal{O}_K)=16$. Observe that

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

For any $\gamma\in\Gamma_0(12)\backslash\pm\Gamma_1(12)$, we have

$$\mathcal{Q}_{d_K}(12)/\Gamma_1(12)=\{\mathcal{Q},\mathcal{Q}\circ\gamma\mid\mathcal{Q}\in\mathcal{Q}_{d_K}(12)/\Gamma_0(12)\}.$$

Now Theorem 25(2) permits an explicit calculation of the minimal polynomial of $t(\sqrt{-1})=N(j_{1,12}(\sqrt{-1}))$. In fact, by approximating $t(\tau_{\mathcal{Q}_i})$ with the aid of computer, we can determine the coefficients of $f(X)=\prod_i(X-t(\tau_{\mathcal{Q}_i}))$ because we already know that $f(X)$ is in $\mathbb{Z}[X]$. Taking the representatives of $\mathcal{Q}_{d_K}(12)/\Gamma_0(12)$ as above and $\gamma=\left(\begin{smallmatrix}7&4\\12&7\end{smallmatrix}\right)\in\Gamma_0(12)\backslash\pm\Gamma_1(12)$, we see that the minimal polynomial of $t(\sqrt{-1})$ is

$$\begin{aligned}&X^{16}-520X^{15}-8184X^{14}-59840X^{13}-266800X^{12}-813984X^{11}\\&\quad-1810976X^{10}-3051904X^{9}-3978144X^{8}-4039552X^{7}-317504X^{6}\\&\quad-1886208X^{5}-803584X^{4}-218624X^{3}-26112X^{2}+2048X+256.\end{aligned}$$

THEOREM 26. *Let K, $\mathfrak{a}$ and α be as in Theorem 25. Assume that $(a,12)=2$ and $d_K\equiv 0 \pmod 4$. Let $\mathcal{Q}_{d_K}^{(2)}=\{[a',b',c']\in\mathcal{Q}_{d_K}\mid (a',12)=2\}$, where $\mathcal{Q}_{d_K}$ is the set of positive definite primitive quadratic forms having discriminant d_K. Then the quotient $\mathcal{Q}_{d_K}^{(2)}/\Gamma_1(12)$ is well defined and its cardinality is equal to the class number $h(\mathcal{O})$ of the order $\mathcal{O}=\mathbb{Z}+12\mathcal{O}_K$. Let $\{\mathcal{Q}_i\}_{i=1}^{h(\mathcal{O})}$ be a complete set of representatives for $\mathcal{Q}_{d_K}^{(2)}/\Gamma_1(12)$ and put $f(X)=\prod_{i=1}^{h(\mathcal{O})}(X-t(\tau_{\mathcal{Q}_i}))$. Then $f(X)$ is the minimal polynomial of $t(\alpha)$ over K and lies in $\mathbb{Z}[X]$.*

Proof. We first construct a bijection between $\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)$ and $\mathcal{Q}_{d_K}(6)/\Gamma_0(6)$. Define $\phi:\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)\to\mathcal{Q}_{d_K}(6)/\Gamma_0(6)$ by sending a class of $[a',b',c']$ to that of $[a'/2,b',2c']$. Observe that ϕ sends the class of $[a',b',c']\circ\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)$ (with $\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)\in\Gamma_0(12)$) to the class of $[a'/2,b',2c']\circ\left(\begin{smallmatrix}p&2q\\r/2&s\end{smallmatrix}\right)$, where $\left(\begin{smallmatrix}p&2q\\r/2&s\end{smallmatrix}\right)$ lies in $\Gamma_0(6)$. Thus ϕ is a well defined map. Conversely, we define a map $\psi:\mathcal{Q}_{d_K}(6)/\Gamma_0(6)\to\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)$ as follows: we observe that any class in $\mathcal{Q}_{d_K}(6)/\Gamma_0(6)$ contains a form $[a'',b'',c'']$ with c'' even. In fact, if $[a'',b'',c'']$ is a form in $\mathcal{Q}_{d_K}(6)$ with c'' odd, then we consider $[a'',b'',c'']\circ\left(\begin{smallmatrix}7&1\\6&1\end{smallmatrix}\right)=[*,*,a''+b''+c'']$. Since $d_K=b''^2-4a''c''\equiv 0$

(mod 4), b'' must be even. The fact that both a'' and c'' are odd implies that $a''+b''+c''$ is even, as desired. For such a $[a'',b'',c'']$, we define $\psi([a'',b'',c''])=[2a'',b'',c''/2]$. For $\left(\begin{smallmatrix} u & v \\ w & x \end{smallmatrix}\right)\in\Gamma_0(6)$, let $[a'',b'',c'']\circ\left(\begin{smallmatrix} u & v \\ w & x \end{smallmatrix}\right)=[*,*,a''v^2+b''vx+c''x^2]$ have $a''v^2+b''vx+c''x^2$ even. Then the fact that a'' is odd and b'',c'' are even implies that v should be even. Now ψ maps $[a'',b'',c'']\circ\left(\begin{smallmatrix} u & v \\ w & x \end{smallmatrix}\right)$ to $[2a'',b'',c''/2]\circ\left(\begin{smallmatrix} u & v/2 \\ 2w & x \end{smallmatrix}\right)$, where $\left(\begin{smallmatrix} u & v/2 \\ 2w & x \end{smallmatrix}\right)\in\Gamma_0(12)$. Hence ψ is also well defined. Further, ϕ and ψ are inverses of each other by construction. Thus

$$|\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)|=|\mathcal{Q}_{d_K}(6)/\Gamma_0(6)|=h(\mathbb{Z}+6\mathcal{O}_K)=h(\mathbb{Z}+12\mathcal{O}_K)/2.$$

Now let $\pi:\mathcal{Q}_{d_K}^{(2)}/\Gamma_1(12)\to\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)$ be the natural projection. Then it can be easily seen that $|\pi^{-1}(\mathcal{Q})|=2$ for each $\mathcal{Q}\in\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)$. This proves the first assertion.

For the second, we see that $f(X)$ has $t(\alpha)$ as a root due to the conditions on a, b, c and d_K. If we proceed in a similar manner as in Theorem 25(2), it can be shown that the conjugates of $t(\alpha)$ over K must have the form $t(\tau')$ with τ' being a root of $[a',b',c']\in\mathcal{Q}_{d_K}^{(2)}$. Thus $t(\tau')=t(\tau_{\mathcal{Q}_j})$ for some j. At this stage, we need to know the field degree of $K(t(\alpha))$ over K. By [1], Theorem 3.7.5(i), $K(T_{12I}(\alpha))$ is the ring class field of order $\mathbb{Z}+6\mathcal{O}_K$. Since $[K(t(\alpha)):K]=2h(\mathbb{Z}+6\mathcal{O}_K)=h(\mathbb{Z}+12\mathcal{O}_K)$, each $t(\tau_{\mathcal{Q}_j})$ gives rise to all the conjugates of $t(\alpha)$. Finally, the proof of the fact that $f(X)\in\mathbb{Z}[X]$ is completely the same as that in Theorem 25(2). ∎

Examples. (1) Take $K=\mathbb{Q}(\sqrt{-1})$ and $\mathfrak{a}=[2,1+\sqrt{-1}]$. Then the degree of $K(j_{1,12}((1+\sqrt{-1})/2))$ over K is $h(\mathbb{Z}+12\mathcal{O}_K)=8$. Observe that

$$\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)=\{[2,-2,1],[26,10,1],[10,14,5],[10,-14,5]\}.$$

Taking the representatives of $\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)$ in the above and $\gamma=\left(\begin{smallmatrix} 7 & 4 \\ 12 & 7 \end{smallmatrix}\right)$ in $\Gamma_0(12)\backslash\pm\Gamma_1(12)$, we come up with the following minimal polynomial of $t((1+\sqrt{-1})/2)$

$$X^8+28X^7+124X^6+304X^5+448X^4+340X^3+208X^2+64X+16.$$

(2) Take $K=\mathbb{Q}(\sqrt{-2})$ and $\mathfrak{a}=[2,\sqrt{-2}]$. Then the degree of $j_{1,12}(\sqrt{-2}/2)$ over K is $h(\mathbb{Z}+12\mathcal{O}_K)=8$. Observe that

$$\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)=\{[2,0,1],[22,-28,9],[86,32,3],[134,40,3]\}.$$

Taking the representatives of $\mathcal{Q}_{d_K}^{(2)}/\Gamma_0(12)$ in the above and $\gamma=\left(\begin{smallmatrix} 7 & 4 \\ 12 & 7 \end{smallmatrix}\right)$ in $\Gamma_0(12)\backslash\pm\Gamma_1(12)$, we come up with the following minimal polynomial of $t(\sqrt{-2}/2)$:

$$X^8-80X^7-416X^6-992X^5-1280X^4-896X^3-224X^2+64X+16.$$

Theorem 27. *Notations being as in Theorem* 26, *assume that* $(a,12)=2$ *and* $d_K\equiv 1\pmod 8$. *Then*:

(1) $|\mathcal{Q}_{d_K}/\Gamma_1(12)| = 2h(\mathcal{O})$, *where* $\mathcal{O} = \mathbb{Z} + 12\mathcal{O}_K$.

(2) $g(X) := \prod_{i=1}^{2h(\mathcal{O})}(X - t(\tau_{Q_i}))$ *has* $t(\alpha)$ *as a root and lies in* $\mathbb{Z}[X]$. *Let* $f(X) \in K[X]$ *be the monic irreducible factor of* $g(X)$ *having* $t(\alpha)$ *as a root. Then* $f(X)$ *is the minimal polynomial of* $t(\alpha)$ *over* K *and lies in* $\mathcal{O}_K[X]$.

Proof. (1) We define $\phi : \mathcal{Q}^{(2)}_{d_K}/\Gamma_0(12) \to \mathcal{Q}_{d_K}(6)/\Gamma_0(6,2)$ by sending the class of $[a', b', c']$ to that of $[a'/2, b', 2c']$. Observe that ϕ sends the class of $[a', b', c'] \circ \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ (with $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \Gamma_0(12)$) to that of $[a'/2, b', 2c'] \circ \left(\begin{smallmatrix} p & 2q \\ r/2 & s \end{smallmatrix}\right)$, where $\left(\begin{smallmatrix} p & 2q \\ r/2 & s \end{smallmatrix}\right)$ lies in $\Gamma_0(6,2)$. Thus ϕ is a well defined map. Conversely, we define $\psi : \mathcal{Q}_{d_K}(6)/\Gamma_0(6,2) \to \mathcal{Q}^{(2)}_{d_K}/\Gamma_0(12)$ as follows: we note that, for any class $[a'', b'', c'']$ in $\mathcal{Q}_{d_K}(6)/\Gamma_0(6,2)$, c'' is always even because a'' is odd and $d_K = b''^2 - 4a''c'' \equiv 1 \pmod 8$. Now ψ sends $[a'', b'', c''] \circ \left(\begin{smallmatrix} u & v \\ w & x \end{smallmatrix}\right)$ to $[2a'', b'', c''/2] \circ \left(\begin{smallmatrix} u & v/2 \\ 2w & x \end{smallmatrix}\right)$, where $\left(\begin{smallmatrix} u & v/2 \\ 2w & x \end{smallmatrix}\right) \in \Gamma_0(12)$. Hence ψ is also well defined. Moreover, ϕ and ψ are inverses of each other. Thus

$$|\mathcal{Q}^{(2)}_{d_K}/\Gamma_0(12)| = |\mathcal{Q}_{d_K}(6)/\Gamma_0(6,2)| = 2|\mathcal{Q}_{d_K}(6)/\Gamma_0(6)| = h(\mathcal{O}).$$

This implies that $|\mathcal{Q}^{(2)}_{d_K}/\Gamma_1(12)| = 2h(\mathcal{O})$, which proves (1).

(2) The assertion $g(t(\alpha)) = 0$ and $g(X) \in \mathbb{Z}[X]$ can be proved by the same method as in Theorem 26. The remaining assertions are obvious. ∎

Example. Take $K = \mathbb{Q}(\sqrt{-7})$ and $\mathfrak{a} = [2, (-1+\sqrt{-7})/2]$. The degree of $K(j_{1,12}((-1+\sqrt{-7})/4))$ over K is $h(\mathbb{Z} + 12\mathcal{O}_K) = 8$. Observe that

$$\begin{aligned}\mathcal{Q}^{(2)}_{d_K}/\Gamma_0(12) = \{&[2,1,1],[2,-1,1],[22,13,2],[22,-13,2],\\ &[14,21,8],[14,-21,8],[106,29,2],[106,-29,2]\}.\end{aligned}$$

Then we have an irreducible polynomial over $\mathbb{Z}$,

$$\begin{aligned} g(X) = X^{16} &+ 8X^{15} + 4104X^{14} + 32656X^{13} + 138848X^{12} + 401328X^{11} \\ &+ 866800X^{10} + 1464128X^9 + 1980720X^8 + 2173760X^7 \\ &+ 1946944X^6 + 1423872X^5 + 843008X^4 + 394240X^3 + 138240X^2 \\ &+ 32768X + 4096, \end{aligned}$$

which has $t(\alpha)$ as a root. However, since the degree of $K(t((-1+\sqrt{-7})/4))$ over K is 8, we must factor $g(X)$ into two polynomials in $\mathcal{O}_K[X]$ and one of them is the minimal polynomial of $t(\alpha)$. Indeed, we come up with the following minimal polynomial of $t(\alpha)$ over K:

$$\begin{aligned} X^8 &+ (4-24\sqrt{-7})X^7 + (28-96\sqrt{-7})X^6 + (88-216\sqrt{-7})X^5 \\ &+ (136-312\sqrt{-7})X^4 + (88-312\sqrt{-7})X^3 - (8+216\sqrt{-7})X^2 \\ &- (32+96\sqrt{-7})X - (8+24\sqrt{-7}). \end{aligned}$$

Lastly, for more practical and overall calculation of minimal polynomials, we first need the following lemma.

LEMMA 28. *For each even integer $N \geq 4$, let*

$$\gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \gamma_{n+1} = \begin{pmatrix} n+1 & 1 \\ n & 1 \end{pmatrix} \quad (2 \leq n \leq N-1)$$

and

$$\delta_m = \begin{pmatrix} 2m+1 & 4m+1 \\ 1 & 2 \end{pmatrix} \quad (1 \leq m \leq N/2-1).$$

Then the set $\{\gamma_1, \ldots, \gamma_N, \delta_1, \ldots, \delta_{N/2-1}\}$ is a subset of representatives for $\overline{\Gamma}(1)/\overline{\Gamma}_0(N)$.

Proof. First, we check that $\gamma_i^{-1}\gamma_j \notin \Gamma_0(N)$ for distinct i and j. We have

$$\gamma_2^{-1}\gamma_{n+1} = \begin{pmatrix} n+1 & 1 \\ -1 & 0 \end{pmatrix} \notin \Gamma_0(N) \quad \text{and} \quad \gamma_{m+1}^{-1}\gamma_{n+1} = \begin{pmatrix} 1 & 0 \\ n-m & 1 \end{pmatrix} \in \Gamma_0(N)$$

if and only if $n = m$ because $2 \leq n, m \leq N-1$. And $\gamma_2^{-1}\delta_m = \left(\begin{smallmatrix} * & * \\ -2m & * \end{smallmatrix}\right) \notin \Gamma_0(N)$ since $-N+2 \leq -2m \leq -2$, and $\delta_m^{-1}\delta_n = \left(\begin{smallmatrix} * & * \\ 2(m-n) & * \end{smallmatrix}\right) \in \Gamma_0(N)$ if and only if $m = n$ owing to the fact that $-(N-4) \leq 2(m-n) \leq N-4$. Finally, we get $\gamma_{n+1}^{-1}\delta_m = \left(\begin{smallmatrix} * & * \\ -2mn+1 & * \end{smallmatrix}\right) \notin \Gamma_0(N)$ because $-2mn+1$ is an odd integer. This proves the lemma. ∎

For our case $N = 12$,

$$\gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \gamma_{n+1} = \begin{pmatrix} n+1 & 1 \\ n & 1 \end{pmatrix} \quad (2 \leq n \leq 11)$$

and

$$\delta_m = \begin{pmatrix} 2m+1 & 4m+1 \\ 1 & 2 \end{pmatrix} \quad (1 \leq m \leq 5)$$

constitute a part of the set of representatives for $\overline{\Gamma}(1)/\overline{\Gamma}_0(12)$.

Then from a direct computation we can show that

$$\gamma_{13} = \begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}, \quad \gamma_{14} = \begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix}, \quad \gamma_{15} = \begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}, \quad \gamma_{16} = \begin{pmatrix} 2 & -1 \\ 5 & -2 \end{pmatrix},$$

$$\gamma_{17} = \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix}, \quad \gamma_{18} = \begin{pmatrix} 1 & 1 \\ 10 & 11 \end{pmatrix}, \quad \gamma_{19} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$$

together with $\{\gamma_1, \ldots, \gamma_{12}, \delta_1, \ldots, \delta_5\}$ form a complete set of representatives for $\overline{\Gamma}(1)/\overline{\Gamma}_0(12)$. Define $S = \{\gamma_1, \ldots, \gamma_{19}, \delta_1, \ldots, \delta_5\}$. Since $\left(\begin{smallmatrix} 7 & 4 \\ 12 & 7 \end{smallmatrix}\right) \in \Gamma_0(12) \backslash \pm \Gamma_1(12)$, we see that $S' = S \cup S\left(\begin{smallmatrix} 7 & 4 \\ 12 & 7 \end{smallmatrix}\right)$ is a complete set of representatives for $\overline{\Gamma}(1)/\overline{\Gamma}_1(12)$ as desired.

THEOREM 29. *With K and α as before, let $f(X)$ be the minimal polynomial of $t(\alpha)$ over K and $az^2 + bz + c = 0$ the equation of α such that $a > 0$*

and $(a,b,c)=1$. *Let* $\mathcal{Q}_{d_K}/\Gamma(1)=\{\mathcal{Q}_j\}_{j=1}^{h_K}$ *and* $\overline{\Gamma}(1)/\overline{\Gamma}_1(12)=\{\gamma_k\}_{k=1}^{48}$ *with* $\gamma_k\in S'$, *where* h_K *denotes the class number of* K. *Define*

$$g(X)=\prod_{j=1}^{h_K}\prod_{k=1}^{48}(X-t(\gamma_k^{-1}\tau_{\mathcal{Q}_j})).$$

Then:

(1) $g(X)$ *lies in* $\mathbb{Z}[X]$ *and is divisible by* $f(X)$.

(2) $f(X)$ *lies in* $\mathcal{O}_K[X]\backslash\mathbb{R}[X]$ *if*

$$\begin{cases}(a,12)=2,4,12 \text{ and } d_K\equiv 1 \pmod 8,\\ (a,12)=3 \text{ and } b\not\equiv 0 \pmod 3,\\ (a,12)=6 \text{ and } b\not\equiv 0 \pmod 6\end{cases}$$

and lies in $\mathbb{Z}[X]$ *if*

$$\begin{cases}(a,12)=1,\\ (a,12)=2 \text{ and } d_K\equiv 0 \pmod 4,\\ (a,12)=3 \text{ and } b\equiv 0 \pmod 3,\\ (a,12)=6 \text{ and } b\equiv 0 \pmod 6.\end{cases}$$

(3) $g(X)$ *decomposes in the following way*:

$$\begin{cases}
f_1(X)^3f_3(X)^3 & \text{if } d_K=-3,\\
f_1(X)^2f_2(X)^2 & \text{if } d_K=-4,\\
f_1(X)^{n_1}(f_2(X)\overline{f_2(X)})^{n_2}(f_3(X)\overline{f_3(X)})^{n_3}(f_4(X)\overline{f_4(X)})^{n_4} & \\
\quad\times(f_6(X)\overline{f_6(X)})^{n_6}(f_{12}(X)\overline{f_{12}(X)})^{n_{12}} & \\
 & \text{if } d_K\equiv 1 \pmod 8,\ d_K\equiv \pm 1 \pmod{12},\\
f_1(X)f_2(X)\overline{f_2(X)}f_4(X)\overline{f_4(X)} & \text{if } d_K\equiv 1 \pmod 8,\ d_K\equiv \pm 5 \pmod{12},\\
f_1(X)f_2(X)\overline{f_2(X)}f_3(X)f_4(X)\overline{f_4(X)}f_6(X)\overline{f_6(X)}f_{12}(X)\overline{f_{12}(X)} & \\
 & \text{if } d_K\equiv 1 \pmod 8,\ d_K\equiv 0 \pmod 3,\\
f_1(X)f_3(X)\overline{f_3(X)} & \text{if } d_K\equiv 5 \pmod 8,\ d_K\equiv \pm 1 \pmod{12},\\
f_1(X) & \text{if } d_K\equiv 5 \pmod 8,\ d_K\equiv \pm 5 \pmod{12},\\
f_1(X)f_3(X) & \text{if } d_K\equiv 5 \pmod 8,\ d_K\equiv 0 \pmod 3,\\
f_1(X)f_2(X)f_3(X)f_6(X) & \text{if } d_K\equiv 0 \pmod 4,\ d_K\equiv 0 \pmod 3,\\
f_1(X)f_2(X)f_3(X)\overline{f_3(X)}f_6(X)\overline{f_6(X)} & \\
 & \text{if } d_K\equiv 0 \pmod 4,\ d_K\equiv 1 \pmod 3,\\
f_1(X)f_2(X) & \text{if } d_K\equiv 0 \pmod 4,\ d_K\equiv 2 \pmod 3,
\end{cases}$$

where $f_i(X)$ $(i = 1, 2, 3, 4, 6, 12)$ stands for the minimal polynomial of $t(\alpha)$ over K with $(a, 12) = i$, and $\overline{f_i(X)}$ the complex conjugation of $f_i(X)$. In the third case, each $n_j \geq 1$ and

$$8(n_1 + n_2 + n_3 + n_4) + 4(n_6 + n_{12}) = 48.$$

Proof. (1) Let $\pi : \mathcal{Q}_{d_K}/\Gamma_1(12) \to \mathcal{Q}_{d_K}/\Gamma(1)$ be the natural projection. Then for each $\mathcal{Q}_j \in \mathcal{Q}_{d_K}/\Gamma(1)$, $\pi^{-1}(\mathcal{Q}_j) = \{\mathcal{Q}_j \circ \gamma_k \mid k = 1, \ldots, 48\}$. Hence, $[a, b, c]$ is equivalent under $\Gamma_1(12)$ to $\mathcal{Q}_j \circ \gamma_k$ for some j and k because $[a, b, c]$ belongs to $\mathcal{Q}_{d_K}$. Since $t(\alpha) = t(\gamma_k^{-1}\tau_{\mathcal{Q}_j})$, $g(X)$ certainly has $t(\alpha)$ as a root. Moreover, the fact that $g(X) \in \mathbb{Z}[X]$ can be proved in the same manner as in Theorem 25(2).

(2) Let τ be the map which gives the complex conjugation on $K(t(\alpha))$. Then it can be easily shown that

$$\mathrm{Ker}(\Phi_{K(t(\alpha))^\tau/K}) = (\mathrm{Ker}(\Phi_{K(t(\alpha))/K}))^\tau = P_{K,1}(\mathfrak{f})^\tau$$

where $\mathfrak{f}$ is as in Table 1.

If $(a, 12) \geq 2$ and the conditions in the first statement are satisfied, then we can see from the proof of Theorem 21 that either 2 or 3 splits completely in K, and so $P_{K,1}(\mathfrak{f})^\tau = P_{K,1}(\mathfrak{f}^\tau) \neq P_{K,1}(\mathfrak{f})$. This implies that $K(t(\alpha))^\tau \neq K(t(\alpha))$. Moreover, $f(X)$ differs from $\overline{f(X)}$ because $K(t(\alpha))$ (resp. $K(t(\alpha))^\tau$) is the splitting field of $f(X)$ (resp. $\overline{f(X)}$). Therefore we conclude that $f(X) \notin \mathbb{R}[X]$.

For the cases $(a, 12) = 1$, $(a, 12) = 2$ and $d_K \equiv 0 \pmod 4$, the assertion follows from Theorems 25 and 26 (this can also be proved by the argument below). For the other cases, we note that the conductors $\mathfrak{f}$ are of the form "an integer times a product of ramified prime ideals". Therefore, $\mathfrak{f}$ should be invariant under the action of τ and so

$$\begin{aligned}\mathrm{Gal}(K(t(\alpha))/K) &\cong I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f}) = I_K(\mathfrak{f}^\tau)/P_{K,1}(\mathfrak{f}^\tau)\\ &\cong \mathrm{Gal}(K(t(\alpha))^\tau/K).\end{aligned}$$

Hence, it follows from the uniqueness theorem of class field theory that

$$K(t(\alpha)) = K(t(\alpha))^\tau = K(t(\alpha)^\tau).$$

Then, since both $K(t(\alpha))$ and $K(t(\alpha)^\tau)$ are splitting fields of $f(X)$, they are identical. This yields that

$$f(X) = \overline{f(X)} \quad \text{and} \quad f(X) \in (\mathcal{O}_K \cap \mathbb{R})[X] = \mathbb{Z}[X].$$

(3) If $d_K = -3$ (resp. $d_K = -4$), the decomposition of $g(X)$ is immediately obtained by factorizing the polynomial $\prod_{k=1}^{48}(X - t(\gamma_k^{-1}\varrho))$ (resp. $\prod_{k=1}^{48}(X - t(\gamma_k^{-1}\sqrt{-1})))$ where $\varrho = e^{2\pi i/3}$. Next, suppose that $d_K \neq -3, -4$.

Let $\mathfrak{f}$ be as in Theorem 21. We then see that

$$\begin{aligned}[K_{\mathfrak{f}} : K] &= [K_{\mathfrak{f}} : K(j_{0,12}(\alpha))][K(j_{0,12}(\alpha)) : K] = 2[K(j_{0,12}(\alpha)) : K] \\ &= 2h(\mathcal{O}_f) \quad \text{by [1], Theorem 3.7.5(i),}\end{aligned}$$

for an imaginary quadratic order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ where $f = 12/(a, 12)$. As for the computation of $h(\mathcal{O}_f)$, we recall from [16] or [19] that

$$h(\mathcal{O}_f) = h_K \frac{f}{(\mathcal{O}_K^\times : \mathcal{O}_f^\times)} \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right), \tag{7}$$

where h_K is the class number of K, $\mathcal{O}_K^\times$ and $\mathcal{O}_f^\times$ are the unit groups of $\mathcal{O}_K$ and $\mathcal{O}_f$, respectively, and $\left(\frac{d_K}{p}\right)$ is the quadratic reciprocity, equal to 1 if p splits completely in K, -1 if p inerts, and 0 if p ramifies in K. By the assertion (1), the polynomials on the right hand side are factors of $g(X)$. Furthermore, we see by (7) that the sum of their degrees in each case is equal to the degree of $g(X)$, which is $48h_K$. This completes the proof. ■

Given K and α, factorizing the polynomial $g(X)$ in Theorem 29, we obtain the following table for several $d_K \geq -7$.

Table 2. Minimal polynomial of $t(\alpha)$

$d_K = -3$

α	$(a, 12)$	$\mathfrak{f}$	$\min(t(\alpha), K)$
$\frac{-1+\sqrt{-3}}{2}$	1	(12)	$X^{12} + 240X^{11} + 2172X^{10} + 9752X^9 + 27324X^8 + 52416X^7 + 71520X^6 + 69696X^5 + 47088X^4 + 20480X^3 + 4800X^2 + 384X + 64$
$\frac{-3+\sqrt{-3}}{6}$	3	$4\left[3, \frac{-3+\sqrt{-3}}{2}\right]$	$X^4 + 8X^3 + 12X^{12} + 8X + 4$

$d_K = -4$

α	$(a, 12)$	$\mathfrak{f}$	$\min(t(\alpha), K)$
$\sqrt{-1}$	1	(12)	$X^{16} - 520X^{15} - 8184X^{14} - 59840X^{13} - 266800X^{12} - 813984X^{11} - 1810976X^{10} - 3051904X^9 - 3978144X^8 - 4039552X^7 - 317504X^6 - 1886208X^5 - 803584X^4 - 218624X^3 - 26112X^2 + 2048X + 256$
$\frac{1+\sqrt{-1}}{2}$	2	$3\left[2, 1+\sqrt{-1}\right]^3$	$X^8 + 28X^7 + 124X^6 + 304X^5 + 448X^4 + 340X^3 + 208X^2 + 64X + 16$

Table 2 (cont.)

$d_K = -7$

α	$(a,12)$	$\mathfrak{f}$	$\min(t(\alpha),K)$
$\frac{-1+\sqrt{-7}}{2}$	1	(12)	$X^{16}+4088X^{15}+65544X^{14}$ $+479296X^{13}+2133968X^{12}$ $+6508128X^{11}+14487520X^{10}$ $+24430208X^{9}+31839840X^{8}$ $+32289920X^{7}+25339264X^{6}$ $+15071232X^{5}+6495488X^{4}$ $+1845760X^{3}+268800X^{2}$ $+2048X+256$
$\frac{-1+\sqrt{-7}}{4}$	2	$3\left[2,\frac{-1+\sqrt{-7}}{2}\right]$ $\times\left[2,\frac{1+\sqrt{-7}}{2}\right]^2$	$X^8+(4-24\sqrt{-7})X^7+(28-96\sqrt{-7})X^6$ $+(88-216\sqrt{-7})X^5+(136-312\sqrt{-7})X^4$ $+(88-312\sqrt{-7})X^3-(8+216\sqrt{-7})X^2$ $-(32+96\sqrt{-7})X-(8+24\sqrt{-7})$
$\frac{1+\sqrt{-7}}{4}$	2	$3\left[2,\frac{1+\sqrt{-7}}{2}\right]$ $\times\left[2,\frac{-1+\sqrt{-7}}{2}\right]^2$	$X^8+(4+24\sqrt{-7})X^7+(28+96\sqrt{-7})X^6$ $+(88+216\sqrt{-7})X^5+(136+312\sqrt{-7})X^4$ $+(88+312\sqrt{-7})X^3-(8-216\sqrt{-7})X^2$ $-(32-96\sqrt{-7})X-(8-24\sqrt{-7})$
$\frac{-3+\sqrt{-7}}{8}$	4	$3\left[2,\frac{-1+\sqrt{-7}}{2}\right]^2$	$X^8+\left(\frac{23-3\sqrt{-7}}{2}\right)X^7+(58-6\sqrt{-7})X^6$ $+\left(\frac{311-27\sqrt{-7}}{2}\right)X^5+\left(\frac{467-39\sqrt{-7}}{2}\right)X^4$ $+\left(\frac{371-39\sqrt{-7}}{2}\right)X^3+\left(\frac{119-27\sqrt{-7}}{2}\right)X^2$ $-(2+6\sqrt{-7})X-\left(\frac{1+3\sqrt{-7}}{2}\right)$
$\frac{3+\sqrt{-7}}{8}$	4	$3\left[2,\frac{1+\sqrt{-7}}{2}\right]^2$	$X^8+\left(\frac{23+3\sqrt{-7}}{2}\right)X^7+(58+6\sqrt{-7})X^6$ $+\left(\frac{311+27\sqrt{-7}}{2}\right)X^5+\left(\frac{467+39\sqrt{-7}}{2}\right)X^4$ $+\left(\frac{371+39\sqrt{-7}}{2}\right)X^3+\left(\frac{119+27\sqrt{-7}}{2}\right)X^2$ $-(2-6\sqrt{-7})X-\left(\frac{1-3\sqrt{-7}}{2}\right)$

Here $\min(t(\alpha),K)$ denotes the minimal polynomial of $t(\alpha)$ over K.

Appendix. In Table 3, we give the Hauptmoduln for the genus zero curves $X_0(N)$, due to K. Harada ([4]). Note that each Hauptmodul corresponds to the Thompson series as specified in the table ([2]).

For generation of generators of $K(X_1(N))$, we used the functions:

- $E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$, the normalized Eisenstein series of weight 4,

Table 3

N	Hauptmodul	Type
2	$\frac{\eta(z)^{24}}{\eta(2z)^{24}}$	2B
3	$\frac{\eta(z)^{12}}{\eta(3z)^{12}}$	3B
4	$\frac{\eta(z)^{8}}{\eta(4z)^{8}}, \frac{\eta(2z)^{24}}{\eta(z)^{8}\eta(4z)^{16}}$	4C
5	$\frac{\eta(z)^{6}}{\eta(5z)^{6}}$	5B
6	$\frac{\eta(2z)^{3}\eta(3z)^{9}}{\eta(z)^{3}\eta(6z)^{9}}, \frac{\eta(2z)^{8}\eta(3z)^{4}}{\eta(z)^{4}\eta(6z)^{8}}, \frac{\eta(z)^{5}\eta(3z)}{\eta(2z)\eta(6z)^{5}}$	6E
7	$\frac{\eta(z)^{4}}{\eta(7z)^{4}}$	7B
8	$\frac{\eta(z)^{4}\eta(4z)^{2}}{\eta(2z)^{2}\eta(8z)^{4}}$	8E
9	$\frac{\eta(z)^{3}}{\eta(9z)^{3}}$	9B
10	$\frac{\eta(2z)\eta(5z)^{5}}{\eta(z)\eta(10z)^{5}}, \frac{\eta(2z)^{4}\eta(5z)^{2}}{\eta(z)^{2}\eta(10z)^{4}}, \frac{\eta(z)^{3}\eta(5z)}{\eta(2z)\eta(10z)^{3}}$	10E
12	$\frac{\eta(4z)^{4}\eta(6z)^{2}}{\eta(2z)^{2}\eta(12z)^{4}}, \frac{\eta(3z)^{3}\eta(4z)}{\eta(z)\eta(12z)^{3}}, \frac{\eta(z)^{3}\eta(4z)\eta(6z)^{2}}{\eta(2z)^{2}\eta(3z)\eta(12z)^{3}}$	12I
13	$\frac{\eta(z)^{2}}{\eta(13z)^{2}}$	13B
16	$\frac{\eta(z)^{2}\eta(8z)}{\eta(2z)\eta(16z)^{2}}$	16B
18	$\frac{\eta(6z)\eta(9z)^{3}}{\eta(3z)\eta(18z)^{3}}, \frac{\eta(2z)^{2}\eta(9z)}{\eta(z)\eta(18z)^{2}}, \frac{\eta(z)^{2}\eta(6z)\eta(9z)}{\eta(2z)\eta(3z)\eta(18z)^{2}}$	18D
25	$\frac{\eta(z)}{\eta(25z)}$	25Z

- $\eta(z) = e^{\pi iz/12}\prod_{n=1}^{\infty}(1-q^n)$, the Dedekind eta function,
- $G_2(z) = 2\zeta(2) - 8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^n$, the Eisenstein series of weight 2,
- $E_2(z)$, the normalized Eisenstein series of weight 2,
- $G_2^{(p)}(z) = G_2(z) - pG_2(pz)$ for a prime p,
- $E_2^{(p)}(z) = E_2(z) - pE_2(pz)$ for a prime p,
- $G_2^{(a_1,a_2)\,(\mathrm{mod}\,N)}(z)$, the level N Eisenstein series of weight 2.

In Table 4, we give the Hauptmoduln for genus zero curves $X_1(N)$, due to Kim and Koo ([5]–[11]).

Since

$$\pm\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma(3) \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \Gamma_0(9)$$

and $\eta(z)^3/\eta(9z)^3$ is the Hauptmodul of $X_0(9)$, we see that $j_3(z)$ defined above is the Hauptmodul of $X(3)$. Here, $W_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ is the Fricke involution.

Table 4

N	Hauptmodul	Field generator
2	$N(j_2(z)) = \frac{16}{j_2(z)} - 8$	$j_2(z) = \lambda(z) = \frac{\theta_2(z)^4}{\theta_3(z)^4}$
3	$N(j_3(z)) = j_3(z)$	$j_3(z) = \frac{\eta(z)^3}{\eta(9z)^3}\Big\vert_{\left(\begin{smallmatrix}\frac{1}{3} & 0\\ 0 & 1\end{smallmatrix}\right)}$
4	$N(j_4(z)) = \frac{4}{j_4(z)} + 2$	$j_4(z) = \frac{\theta_3(z/2)}{\theta_4(z/2)}$
2	$N(j_{1,2}(z)) = \frac{2^8}{j_{1,2}(z)} + 24$	$j_{1,2}(z) = \frac{\theta_2(z)^8}{\theta_4(2z)^8}$
3	$N(j_{1,3}(z)) = \frac{240}{j_{1,3}(z)-1} + 9$	$j_{1,3}(z) = \frac{E_4(z)}{E_4(3z)}$
4	$N(j_{1,4}(z)) = \frac{16}{j_{1,4}(z)} - 8$	$j_{1,4}(z) = \frac{\theta_2(2z)^4}{\theta_3(2z)^4}$
5	$N(j_{1,5}(z)) = \frac{-8}{j_{1,5}(z)+44} - 5$	$j_{1,5}(z) = \left(4\frac{\eta(z)^5}{\eta(5z)} + E_2^{(5)}(z)\right)/\frac{\eta(5z)^5}{\eta(z)}$
6	$N(j_{1,6}(z)) = \frac{2}{j_{1,6}(z)-1} - 1$	$j_{1,6}(z) = \frac{G_2^{(2)}(z)-G_2^{(2)}(3z)}{2G_2^{(2)}(z)-G_2^{(3)}(z)}$
7	$N(j_{1,7}(z)) = \frac{-1}{W_7(j_{1,7}(z))-1} - 3$	$j_{1,7}(z) = \frac{G_2^{(0,1)\,(\mathrm{mod}\,7)}-G_2^{(0,2)\,(\mathrm{mod}\,7)}}{G_2^{(0,1)\,(\mathrm{mod}\,7)}-G_2^{(0,3)\,(\mathrm{mod}\,7)}}$
8	$N(j_{1,8}(z)) = \frac{2}{j_{1,8}(z)-1} - 1$	$j_{1,8}(z) = \frac{\theta_3(2z)}{\theta_3(4z)}$
9	$N(j_{1,9}(z)) = \frac{-1}{W_9(j_{1,9}(z))-1} - 2$	$j_{1,9}(z) = \frac{G_2^{(0,1)\,(\mathrm{mod}\,9)}-G_2^{(0,2)\,(\mathrm{mod}\,9)}}{G_2^{(0,1)\,(\mathrm{mod}\,9)}-G_2^{(0,4)\,(\mathrm{mod}\,9)}}$
10	$N(j_{1,10}(z)) = \frac{-1}{W_{10}(j_{1,10}(z))-1} - 2$	$j_{1,10}(z) = \frac{G_2^{(0,1)\,(\mathrm{mod}\,10)}-G_2^{(0,2)\,(\mathrm{mod}\,10)}}{G_2^{(0,1)\,(\mathrm{mod}\,10)}-G_2^{(0,4)\,(\mathrm{mod}\,10)}}$
12	$N(j_{1,12}(z)) = \frac{2}{j_{1,12}(z)-1}$	$j_{1,12}(z) = \frac{\theta_3(2z)}{\theta_3(6z)}$

References

[1] I. Chen and N. Yui, *Singular values of Thompson series*, in: Groups, Difference Sets and the Monster, K. T. Arasu *et al.* (eds.), de Gruyter, 1996, 255–326.

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

[3] D. A. Cox, *Primes of the Form* $x^2 + ny^2$, Wiley, 1989.

[4] K. Harada, *Moonshine of Finite Groups*, lecture note, Ohio State Univ.

[5] C. H. Kim and J. K. Koo, *Arithmetic of the modular function* j_4, J. Korean Math. Soc. 36 (1999), 707–724.

[6] —, —, *Arithmetic of the modular function* $j_{1,4}$, Acta Arith. 84 (1998), 129–143.

[7] —, —, *Arithmetic of the modular function* $j_{1,8}$, Ramanujan J., to appear.

[8] — —, *Arithmetic of the modular functions* $j_{1,5}$ *and* $j_{1,6}$, in preparation.

[9] —, —, *Arithmetic of the modular functions* $j_{1,2}$ *and* $j_{1,3}$, in preparation.

[10] —, —, *Generation of Hauptmoduln of* $\Gamma_1(7)$, $\Gamma_1(9)$ *and* $\Gamma_1(10)$, in preparation.

[11] —, —, *On the Hauptmodul of* $\Gamma_1(12)$, preprint.

[12] C. H. Kim and J. K. Koo, *On the genus of some modular curve of level N*, Bull. Austral. Math. Soc. 54 (1996), 291–297.
[13] —, —, *The normalizer of $\Gamma_1(N)$ in $PSL_2(\mathbb{R})$*, Comm. Algebra, to appear.
[14] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, 1984.
[15] S. Lang, *Algebraic Number Theory*, Springer, 1994.
[16] —, *Elliptic Functions*, Springer, 1987.
[17] R. Rankin, *Modular Forms and Functions*, Cambridge Univ. Press, Cambridge, 1977.
[18] B. Schoeneberg, *Elliptic Modular Functions*, Springer, 1973.
[19] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan 11, Princeton, 1971.
[20] —, *On modular forms of half-integral weight*, Ann. of Math. 97 (1973), 440–481.
[21] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

Department of Mathematics
Korea Advanced Institute of Science and Technology
Taejon 305-701, South Korea
E-mail: hkj@math.kaist.ac.kr
jkkoo@math.kaist.ac.kr

Received on 10.11.1998
and in revised form on 16.12.1999 (3504)