Generators of function fields of the modular curves $X_1(5)$ and $X_1(6)$

by

Chang Heon Kim and Ja Kyung Koo

BK21 Research Report

09 - 09

May 29, 2009

DEPARTMENT OF MATHEMATICAL SCIENCES

한국과학기술원
Korea Advanced Institute of Science and Technology

GENERATORS OF FUNCTION FIELDS OF THE MODULAR CURVES $X_1(5)$ AND $X_1(6)$

CHANG HEON KIM[1] & JA KYUNG KOO[2]

ABSTRACT. We show that the modular functions $j_{1,5}$ and $j_{1,6}$ generate function fields of the modular curves $X_1(N)$ ($N = 5, 6$ respectively) and find some number theoretic properties of these modular functions.

1. INTRODUCTION

Let $\mathfrak{H}$ be the complex upper half plane and let $\Gamma_1(N)$ be a congruence subgroup of $SL_2(\mathbb{Z})$ whose elements are congruent to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N$ ($N = 1, 2, 3, \dots$). Since the group $\Gamma_1(N)$ acts on $\mathfrak{H}$ by linear fractional transformations, we get the modular curve $X_1(N) = \Gamma_1(N)\backslash\mathfrak{H}^*$, as the projective closure of smooth affine curve $\Gamma_1(N)\backslash\mathfrak{H}$, with genus $g_{1,N}$.

Let $r \in \mathbb{Z}$ and $r \not\equiv 0 \mod N$. For $z \in \mathfrak{H}$, Ishii ([7]) found a family of modular functions $X_r(z)$ defined by

$$X_r(z) = \exp\left(2\pi i \frac{-(r-1)(N-1)}{4N}\right) \prod_{s=0}^{N-1} \frac{K_{r,s}(z)}{K_{1,s}(z)},$$

where $K_{u,v}(z)$ are Klein forms of level N. For the Klein forms we refer to Kubert and Lang [14]. For $\zeta_N = e^{2\pi i/N}$, let $\mathfrak{F}_N$ be the field of modular functions for the principal congruence group $\Gamma(N)$ with $\mathbb{Q}(\zeta_N)$-rational Fourier coefficients at the cusp $i\infty$. Then $X_r(z) \in \mathfrak{F}_N$ (resp. $X_r(z)^{\varepsilon_N} \in \mathfrak{F}_N$) if r is odd (resp. if r is even), where ε_N is 1 or 2 according as N is odd or even. When $N \geq 7$, by utilizing such modular functions, Ishida and Ishii showed in [8] that $X_2(z)^{\varepsilon_N N}, X_3(z)^N$ are generators of function fields of the modular curves $X_1(N)$. As for the cases $N = 1, 2, 3$ we know that the elliptic modular function $j(z)$ ($N = 1$), and the Thompson series of type $2B$ ($N = 2$, Table 3 in [2]) and the Thompson series of type $3B$ ($N = 3$, Table 3 in [2]) are generators, respectively because $\overline{\Gamma}_1(2)=\overline{\Gamma}_0(2)$ and $\overline{\Gamma}_1(3)=\overline{\Gamma}_0(3)$. In the case $N = 4$,

AMS Subject Classification : 11F03, 11F06, 11F11, 14H55

[1]This work was supported by the research fund of Hanyang University (HY-2008-N).
[2]This work was partially supported by the SRC Program of KOSEF grant funded by MEST R11-2007-035-01001-0.

we refer to [10]. Thus, in order to find the rest two cases $N = 5, 6$ we use the following general fact. Since $g_{1,N} = 0$ only for the eleven cases $1 \leq N \leq 10$ and $N = 12$ ([9]), the function field $\mathbb{C}(X_1(N))$ of the curve $X_1(N)$ is a rational function field over $\mathbb{C}$ for such N.

In this article we shall find the field generators $j_{1,5}$ and $j_{1,6}$ as uniformizers of the modular curves $X_1(N)$ when $N = 5$ and 6, respectively. In §3 $j_{1,5}$ is constructed by making use of the Dedekind eta functions and Eisenstein series of weight 2. And in §4 we build up $j_{1,6}$ from the Eisenstein series of weight 2. In §5 we estimate the normalized generators (or hauptmodulus) $N(j_{1,5})$ and $N(j_{1,6})$. And, when $z \in \mathfrak{H} \cap \mathbb{Q}(\sqrt{-d})$ for a square free positive integer d, we show that $N(j_{1,N})(z)$ $(N = 5, 6)$ becomes an algebraic integer. In §6 we show that the hauptmodulus $N(j_{1,5})$ has integral Fourier coefficients. Lastly, in §7 we find certain connection between hauptmodulus $N(j_{1,N})$ and the parameter t emerging from the moduli problem of elliptic curves.

Throughout the article we adopt the following notations:

$\mathfrak{H}^*$ the extended complex upper half plane

Γ a congruence subgroup of $SL_2(\mathbb{Z})$

$\Gamma(N)$ $= \{\gamma \in SL_2(\mathbb{Z}) | \ \gamma \equiv I \mod N\}$

$\Gamma_0(N)$ the Hecke subgroup $\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) | \ c \equiv 0 \mod N\}$

$X(\Gamma) = \Gamma \backslash \mathfrak{H}^*$

$X(N) = \Gamma(N) \backslash \mathfrak{H}^*$

$X_0(N) = \Gamma_0(N) \backslash \mathfrak{H}^*$

$\mathbb{C}(X(\Gamma))$ function field of the curve $X(\Gamma)$

$\overline{\Gamma}$ the inhomogeneous group of $\Gamma (= \Gamma / \pm I)$

$\sigma_1(n) = \sum_{\substack{d|n \\ d>0}} d$ the sum of positive divisors of n

$q_h = e^{2\pi i z/h}$, $z \in \mathfrak{H}$

$f|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} = f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z)$

$f|_{[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)]_k} = (ad - bc)^{\frac{k}{2}} \cdot f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z) \cdot (cz + d)^{-k}$

$M_k(\Gamma)$ the space of modular forms of weight k with respect to the group Γ

$M_k(\Gamma_0(N),\chi) = \{f \in M_{\frac{k}{2}}(\Gamma_0(N)) \mid f(\gamma z) = \chi(d)(cz+d)^k f(z)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)\}$

$a \sim b$ means that a is equivalent to b

$z \to i\infty$ denotes that z goes to $i\infty$.

$\nu_0(F)$ the sum of orders of zeros of a modular form (or function) F

$\nu_\infty(F)$ the sum of orders of poles of a modular form (or function) F

$\sigma_\infty(\Gamma)$ the number of Γ-inequivalent cusps of Γ

We shall always take the branch of the square root having argument in $(-\frac{\pi}{2},\frac{\pi}{2}]$. Thus, $\sqrt{z}$ is a holomorphic function on the complex plane with the negative real axis $(-\infty,0]$ removed. For any integer k, we define $z^{\frac{k}{2}}$ to mean $(\sqrt{z})^k$.

2. Fundamental region of $X_1(N)$

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$.

Definition. An *(open) fundamental region* R for Γ is an open subset of $\mathfrak{H}^*$ with the properties:

1. there do not exist $\gamma \in \Gamma$ and $w, z \in R$ for which $w \neq z$ and $w = \gamma z$;
2. for any $z \in \mathfrak{H}^*$, there is $\gamma \in \Gamma$ such that $\gamma z \in \overline{R}$ the closure of R.

We will examine some necessary results about fundamental regions, which will give us useful geometric informations for the modular curve $X_1(N)$. Let $\Gamma^1(N)$ be a congruence subgroup of $SL_2(\mathbb{Z})$ whose elements are congruent to $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ mod N $(N = 1,2,3,\cdots)$. We note that the two groups $\Gamma_1(N)$ and $\Gamma^1(N)$ are conjugate:

$$\Gamma^1(N) = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \begin{pmatrix} 1/N & 0 \\ 0 & 1 \end{pmatrix}. \tag{1}$$

It turns out that the Γ^1 groups are more convenient than their Γ_1 counterparts for drawing pictures and making geometric computations. Now we will draw fundamental regions by using Ferenbaugh's idea ([4], §3). Suppose $c, r \in \mathbb{R}$ with $r > 0$. Then we define the sets

$$\text{arc}(c,r) = \{z \in \mathfrak{H}^* |\ |z-c| = r\}$$

$$\text{inside}(c,r) = \{z \in \mathfrak{H}^* |\ |z-c| < r\}$$

$$\text{outside}(c,r) = \{z \in \mathfrak{H}^* |\ |z-c| > r\}.$$

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of Γ, and assume $c \neq 0$. Then we define

$$\text{arc}(\gamma) = \text{arc}(a/c, 1/|c|),$$

$$\text{inside}(\gamma) = \text{inside}(a/c, 1/|c|) \quad \text{and}$$

$$\text{outside}(\gamma) = \text{outside}(a/c, 1/|c|).$$

If $c = 0$, γ is of the form $z \mapsto z + n$ for some integer n. We shall assume γ is not the identity, so $n \neq 0$. We then adopt the following conventions: for $n > 0$, we define

$$\text{arc}(\gamma) = \left\{z \in \mathfrak{H}^* |\ \text{Re}(z) = \frac{n}{2}\right\}$$
$$\text{inside}(\gamma) = \left\{z \in \mathfrak{H}^* |\ \text{Re}(z) > \frac{n}{2}\right\}$$
$$\text{outside}(\gamma) = \left\{z \in \mathfrak{H}^* |\ \text{Re}(z) < \frac{n}{2}\right\}.$$

As for the case $n < 0$, we define "arc" in the same way and reverse the inequalities in the definitions of "inside" and "outside". Then we have

Proposition 1. *The element $\gamma \in \Gamma - \{I\}$ sends arc(γ^{-1}) to arc(γ), inside(γ^{-1}) to outside(γ) and outside(γ^{-1}) to inside(γ).*

Proof. [4], Proposition 3.1. □

Theorem 2. *With notations as in the above, a fundamental region R for Γ is given by*

$$R = \bigcap_{\gamma \in \Gamma - \{I\}} \textit{outside}(\gamma).$$

Proof. [4], Theorem 3.3. □

Now the following theorem enables us to get the generators of the group $\overline{\Gamma}$.

Theorem 3. *Let* $\overline{\Gamma}$ *be a congruence subgroup of* $\overline{\Gamma}(1)$ *of finite index and* R *be a fundamental region for* $\overline{\Gamma}$*. Then the sides of* R *can be grouped into pairs* λ_i, λ_i' $(i = 1, 2, \cdots, s)$ *in such a way that* $\lambda_i \subseteq \overline{R}$ *and* $\lambda_i' = \gamma_i\lambda_i$ *where* $\gamma_i \in \overline{\Gamma}$ $(i = 1, 2, \cdots, s)$*.* γ_i*'s are called boundary substitutions of* R*. Furthermore,* $\overline{\Gamma}$ *is generated by the boundary substitutions* $\gamma_1, \cdots, \gamma_s$*.*

Proof. [19], Theorem 2.4.4 (or [10], Theorem 1). □

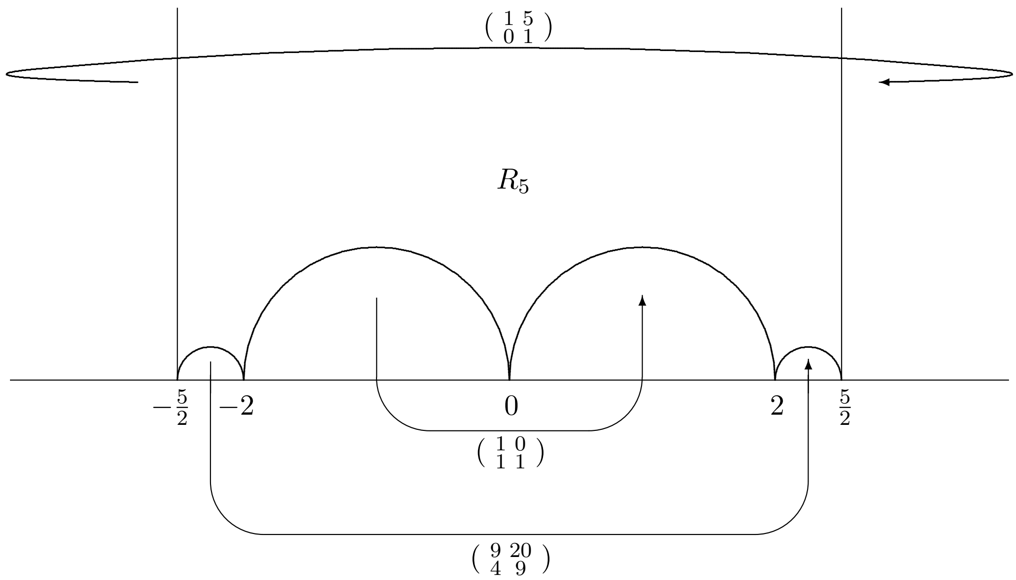
3. Modular function $j_{1,5}$

Let us take $\Gamma = \Gamma^1(5)$ and put $\gamma_1 = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}$, $\gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $\gamma_3 = \begin{pmatrix} 9 & 20 \\ 4 & 9 \end{pmatrix}$. If R_5 is a fundamental region of $\Gamma^1(5)$, then by Theorem 2 it is given by

$$R_5 = \bigcap_{i=1}^{3} outside(\gamma_i^{\pm 1})$$

and is drawn as follows.

Fundamental domain of $\Gamma^1(5)$



We denote by S_Γ the set of inequivalent cusps of Γ. Then we see from the above figure that $S_{\Gamma^1(5)} = \{\infty, 0, 2, \frac{5}{2}\}$. Furthermore it follows from Theorem 3 that $\overline{\Gamma}^1(5)$ is generated by γ_1, γ_2 and γ_3. Thus we obtain the following theorem by (1).

Theorem 4. *(i)* $S_{\Gamma_1(5)} = \{\infty, 0, \frac{2}{5}, \frac{1}{2}\}$. *All cusps of* $\Gamma_1(5)$ *are regular* ([16], [22]).
(ii) $\overline{\Gamma}_1(5)$ *is generated by* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix}$ *and* $\begin{pmatrix} 9 & 4 \\ 20 & 9 \end{pmatrix}$.

For later use we are in need of calculating the widths of the cusps of $\Gamma_1(5)$.

Lemma 5. *Let* $a/c \in \mathbb{P}^1(\mathbb{Q})$ *be a cusp with* $(a, c) = 1$. *Then the width of* a/c *in* $X_1(N)$ *is given by* $N/(c, N)$ *if* $N \neq 4$.

Proof. [11], Lemma 3. □

Therefore, we have the following table of inequivalent cusps of $\Gamma_1(5)$:

Table 1. Cusps of $\Gamma_1(5)$

cusp	∞	0	$\frac{2}{5}$	$\frac{1}{2}$
width	1	5	1	5

Let G_2 be the Eisenstein series of weight 2 defined by

$$G_2(z) = 2\zeta(2) - 8\pi^2 \sum_{n \geq 1} \sigma_1(n) q^n, \quad z \in \mathfrak{H}. \tag{2}$$

Then G_2 has the following transformation formula ([20], p.68) for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ and $z \in \mathfrak{H}$:

$$G_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 G_2(z) - 2\pi i c(cz+d). \tag{3}$$

Lemma 6. *For each prime* p, *let* $G_2^{(p)}(z) = G_2(z) - pG_2(pz)$. *Then* $G_2^{(p)}(z) \in M_2(\Gamma_0(p))$.

Proof. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\Gamma_0(p)$, then

$$\begin{aligned}
G_2^{(p)}(z)|_{[\gamma]_2} &= (cz+d)^{-2}G_2^{(p)}(\gamma z) \\
&= (cz+d)^{-2}(G_2(\gamma z) - pG_2(p\,\gamma z)) \\
&= (cz+d)^{-2}(G_2(\gamma z) - pG_2(\left(\begin{smallmatrix} a & pb \\ c/p & d \end{smallmatrix}\right)\cdot pz) \\
&\qquad \text{using } \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} a & pb \\ c/p & d \end{smallmatrix}\right) \\
&= (cz+d)^{-2}((cz+d)^2G_2(z) - 2\pi ic(cz+d) \\
&\qquad - p((\frac{c}{p}pz+d)^2G_2(pz) - 2\pi i\frac{c}{p}(\frac{c}{p}pz+d))) \quad \text{by (3)} \\
&= G_2^{(p)}(z).
\end{aligned}$$

Recall that there are 2 cusps $\infty,\ 0$ in $X_0(p)$. The q-expansion of G_2 implies the holomorphicity of $G_2^{(p)}$ at ∞. At 0

$$\begin{aligned}
G_2^{(p)}(z)|_{[\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)]_2} &= z^{-2}G_2^{(p)}(-1/z) \\
&= z^{-2}(G_2(-1/z) - pG_2(-p/z)) \\
&= z^{-2}(z^2G_2(z) - 2\pi iz - p((z/p)^2G_2(z/p) - 2\pi iz/p)) \quad \text{by (3)} \\
&= G_2(z) - 1/pG_2(z/p),
\end{aligned}$$

hence it is holomorphic there. □

Lemma 7. *For $F \in M_k(\Gamma_0(N),\chi)$, let $W_N(F)$ be the Fricke involution of F, i.e., $W_N(F) = F|_{[\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)]_k}$. Then for a quadratic character χ on $(\mathbb{Z}/N\mathbb{Z})^*$, W_N preserves $M_k(\Gamma_0(N),\chi)$.*

Proof. [13], p.145. □

Let $\eta(z) = e^{\frac{\pi iz}{12}}\prod_{n=1}^{\infty}(1-q^n),\ z \in \mathfrak{H}$ be the Dedekind eta function. It is well-known ([12], p.235) that

$$\eta(z+1) = e^{\frac{\pi i}{12}}\eta(z) \quad\text{and}\quad \eta(-1/z) = (-iz)^{\frac{1}{2}}\eta(z). \tag{4}$$

Lemma 8. *(i) $\eta^p(z)/\eta(pz) \in M_{\frac{p-1}{2}}\left(\Gamma_0(p),\left(\frac{\cdot}{p}\right)\right)$ for a prime $p > 3$.*
(ii) $W_p(\eta^p(z)/\eta(pz)) =$ constant $\times\, \eta^p(pz)/\eta(z) \in M_{\frac{p-1}{2}}\left(\Gamma_0(p),\left(\frac{\cdot}{p}\right)\right)$.

Proof. For (i) we refer to [18], p.28.

(ii)

$$\begin{aligned}
W_p(\eta^p(z)/\eta(pz)) &= \frac{\eta^p(z)}{\eta(pz)}\Big|_{[\left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)]_{\frac{p-1}{2}}} \\
&= p^{\frac{p-1}{4}}(pz)^{-\frac{p-1}{2}}\eta^p\left(-\frac{1}{pz}\right)/\eta\left(p\cdot\left(-\frac{1}{pz}\right)\right) \\
&= p^{-\frac{p-1}{4}}z^{-\frac{p-1}{2}}\frac{(-ipz)^{\frac{p}{2}}\eta^p(pz)}{(-iz)^{\frac{1}{2}}\eta(z)} \quad \text{by (4)} \\
&= \text{ constant } \times \eta^p(pz)/\eta(z).
\end{aligned}$$

Hence, this completes the proof by Lemma 7. □

Now, put $x(z) = 4\cdot\eta^5(z)/\eta(5z) + E_2^{(5)}(z)$ and $y(z) = \eta^5(5z)/\eta(z)$, where $E_2(z) = G_2(z)/(2\zeta(2))$ is the normalized Eisenstein series of weight 2 and $E_2^{(5)}(z) = E_2(z) - 5E_2(5z)$. From the q-expansions of G_2 and η it follows that

$$x(z) = -44q - 52q^2 - 56q^3 - 228q^4 + \cdots ,$$

$$y(z) = q + q^2 + 2q^3 + 3q^4 + 5q^5 + \cdots .$$

We set $j_{1,5}(z) = x(z)/y(z)$.

Theorem 9. *(a)* $x, y \in M_2(\Gamma_1(5))$.

(b) $\mathbb{C}(X_1(5))$ *is equal to* $\mathbb{C}(j_{1,5}(z))$.

(c) $j_{1,5}$ *takes the following value at each cusp:* $j_{1,5}(\infty) = -44$, $j_{1,5}(0) = -20\sqrt{5}$, $j_{1,5}(1/2) = 20\sqrt{5}$, *and* $j_{1,5}(2/5) = \infty$ *(a simple pole).*

Proof. (a) follows from Lemma 6 and 8. Next, it is clear by (a) that $j_{1,5}(z) \in \mathbb{C}(X_1(5))$. We see from the construction of x and y that both x and y vanish at ∞. Also, we know from [22], p.39 that $\nu_0(x) = \nu_0(y) = 2$. Let ∞ and z_0 (resp. z_0') be the zeros of x (resp. y). If z_0 is equivalent to z_0' under $\Gamma_1(5)$, then x/y has no poles in $X_1(5)$ so that it would be a constant. However, the q-expansions of x and y show that the quotient x/y cannot be a constant. Thus z_0 is not $\Gamma_1(5)$-equivalent to z_0'. And $\nu_0(j_{1,5}) = \nu_\infty(j_{1,5}) = 1$, which implies that $j_{1,5}$ generates $\mathbb{C}(X_1(5))$ over $\mathbb{C}$. Now we will prove (c). As mentioned in the Table 1, we note that there are 4 inequivalent cusps $\infty, 0, 1/2, 2/5$ in $X_1(5)$.

(i) $s = \infty$:

$$j_{1,5}(\infty) = \lim_{z\to i\infty} \frac{x}{y} = \lim_{q\to 0} \frac{-44q - 52q^2 - 56q^3 - 228q^4 + \cdots}{q + q^2 + 2q^3 + 3q^4 + 5q^5 + \cdots}$$
$$= -44.$$

(ii) $s = 0$: Since $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ sends ∞ to 0,

$$j_{1,5}(0) = \lim_{z\to i\infty} \left.\frac{4\cdot \eta^5(z)/\eta(5z) + E_2^{(5)}(z)}{\eta^5(5z)/\eta(z)}\right|_{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)}$$
$$= \lim_{z\to i\infty} \frac{4\cdot \eta^5(-1/z)/\eta(-5/z) + E_2^{(5)}(-1/z)}{\eta^5(-5/z)/\eta(-1/z)}$$
$$= \lim_{z\to i\infty} \frac{4\cdot(\sqrt{-iz}^5\eta^5(z))/(\sqrt{-iz/5}\ \eta(z/5)) + z^2E_2(z) - (z^2/5)E_2(z/5)}{(\sqrt{-iz/5}^5\eta^5(z/5))/(\sqrt{-iz}\ \eta(z))}$$
by (3) and (4)
$$= -20\sqrt{5}.$$

(iii) $s = 1/2$: Now that $\left(\begin{smallmatrix} 3 & 1 \\ 5 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ sends ∞ to $1/2$,

$$j_{1,5}(1/2) = \lim_{z\to i\infty} \left.\frac{4\cdot \eta^5(z)/\eta(5z) + E_2^{(5)}(z)}{\eta^5(5z)/\eta(z)}\right|_{\left(\begin{smallmatrix} 3 & 1 \\ 5 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)}$$
$$= \lim_{z\to i\infty} \left.\frac{-4\cdot \eta^5(z)/\eta(5z) + E_2^{(5)}(z)}{-\eta^5(5z)/\eta(z)}\right|_{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)} \quad \text{by Lemma 6 and 8}$$
$$= 20\sqrt{5} \quad \text{similarly to (ii).}$$

(iv) $s = 2/5$: $\left(\begin{smallmatrix} 2 & 1 \\ 5 & 3 \end{smallmatrix}\right)\infty = 2/5$.

$$j_{1,5}(2/5) = \lim_{z\to i\infty} \left.\frac{4\cdot \eta^5(z)/\eta(5z) + E_2^{(5)}(z)}{\eta^5(5z)/\eta(z)}\right|_{\left(\begin{smallmatrix} 2 & 1 \\ 5 & 3 \end{smallmatrix}\right)}$$
$$= \lim_{z\to i\infty} \frac{-4\cdot \eta^5(z)/\eta(5z) + E_2^{(5)}(z)}{-\eta^5(5z)/\eta(z)} \quad \text{by Lemma 6 and 8}$$
$$= \infty \text{ (a simple pole).}$$

□

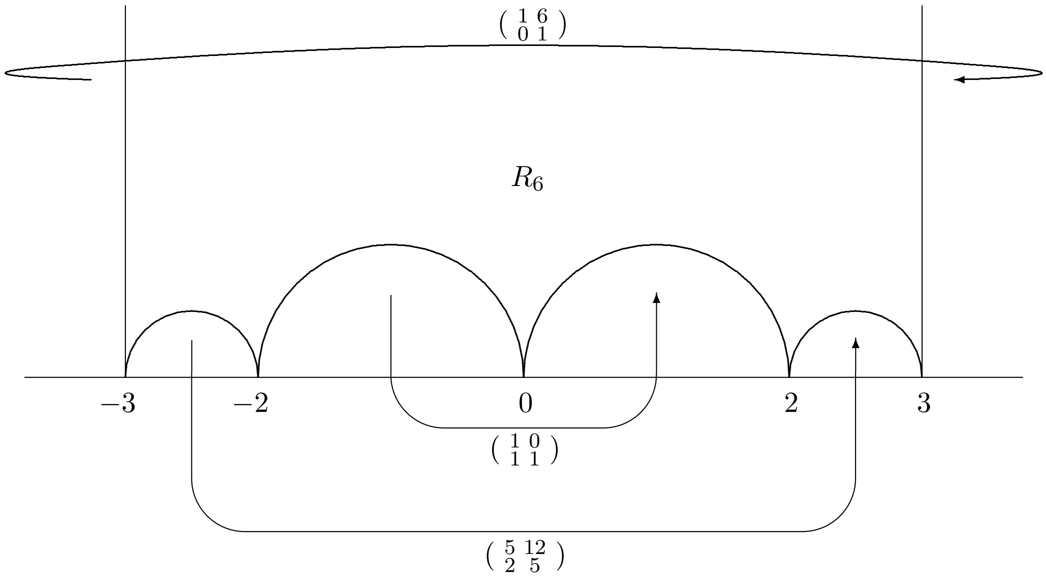
4. Modular function $j_{1,6}$

Let us take $\Gamma = \Gamma^1(6)$ and set $\gamma_1 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$, $\gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $\gamma_3 = \begin{pmatrix} 5 & 12 \\ 2 & 5 \end{pmatrix}$. If R_6 is a fundamental region of $\Gamma^1(6)$, then R_6 is described as

$$R_6 = \bigcap_{i=1}^{3} outside(\gamma_i^{\pm 1}).$$

Hence we have the following picture for R_6.

Fundamental domain of $\Gamma^1(6)$



Then as we see in the above figure $S_{\Gamma^1(6)} = \{\infty, 0, 2, 3\}$. Furthermore, it follows from Theorem 3 that $\overline{\Gamma}^1(6)$ is generated by γ_1, γ_2 and γ_3. Therefore we obtain the following theorem by (1).

Theorem 10. *(i)* $S_{\Gamma_1(6)} = \{\infty, 0, \frac{1}{3}, \frac{1}{2}\}$. *All cusps of* $\Gamma_1(6)$ *are regular (*[16], [22]*).*
(ii) $\overline{\Gamma}_1(6)$ *is generated by* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}$ *and* $\begin{pmatrix} 5 & 2 \\ 12 & 5 \end{pmatrix}$.

We then have the following table of inequivalent cusps of $\Gamma_1(6)$ in virtue of Lemma 5:

Table 2. Cusps of $\Gamma_1(6)$

cusp	∞	0	$\frac{1}{3}$	$\frac{1}{2}$
width	1	6	2	3

Let $G_2^{(p)}(z)$ be the series as in Lemma 6. Put $X(z) = G_2^{(2)}(z) - G_2^{(2)}(3z) = G_2(z) - 2G_2(2z) - G_2(3z) + 2G_2(6z)$ and $Y(z) = 2G_2^{(2)}(z) - G_2^{(3)}(z) = G_2(z) - 4G_2(2z) + 3G_2(3z)$. We set $j_{1,6}(z) = X(z)/Y(z)$.

Theorem 11. *(a)* $X, Y \in M_2(\Gamma_1(6))$.
(b) $\mathbb{C}(X_1(6))$ *is equal to* $\mathbb{C}(j_{1,6}(z))$.
(c) $j_{1,6}$ *takes the following value at each cusp:* $j_{1,6}(\infty) = 1$, $j_{1,6}(0) = 4/3$, $j_{1,6}(1/3) = 0$, *and* $j_{1,6}(1/2) = 1/3$.

Proof. By Lemma 6, $G_2^{(p)}(z) \in M_2(\Gamma_0(p))$ for a prime p. Meanwhile, the identity

$$\left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \Gamma_0(p) \left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right) \cap \Gamma_0(p) = \Gamma_0(pq)$$

allows us to have $G_2^{(p)}(qz) \in M_2(\Gamma_0(pq))$. Therefore we easily get (a), from which $j_{1,6} = X/Y \in \mathbb{C}(X_1(6))$. By the q-expansion of G_2 as in (2) we derive that

$$X(z) = -8\pi^2 \cdot (q + q^2 + 3q^3 + q^4 + 6q^5 + \cdots), \tag{5}$$

$$Y(z) = -8\pi^2 \cdot (q - q^2 + 7q^3 - 5q^4 + 6q^5 + \cdots). \tag{6}$$

Thus both X and Y vanish at ∞. And, the zero formula ([22], p.39) yields $\nu_0(X) = \nu_0(Y) = 2$. If ∞ and w_0 (resp. w_0') are the zeros of X (resp. Y), then w_0 is not $\Gamma_1(6)$-equivalent to w_0'. Therefore $\nu_0(j_{1,6}) = \nu_\infty(j_{1,6}) = 1$, which means that $j_{1,6}$ generates $\mathbb{C}(X_1(6))$ over $\mathbb{C}$. Next, as for the statement (c), we first recall that there are four $\Gamma_1(6)$-inequivalent cusps ∞, 0, 1/3 and 1/2. Put $f_1(z) = G_2^{(2)}(z)$, $f_2(z) = f_1(3z)$ and $f_3(z) = G_2^{(3)}(z)$. Then

$$X(z) = f_1(z) - f_2(z) \quad \text{and} \quad Y(z) = 2f_1(z) - f_3(z). \tag{7}$$

We shall then evaluate the values of f_i $(i = 1, 2, 3)$ at each cusp. First we note that

$$G_2^{(p)}(\infty) = \lim_{z \to i\infty} G_2^{(p)}(z) = 2\zeta(2)(1 - p) \quad \text{by (2)} \tag{8}$$

$$G_2^{(p)}(0) = \lim_{z \to i\infty} G_2^{(p)}(-1/z) = 2\zeta(2)(1 - 1/p) \quad \text{by (2) and (3).} \tag{9}$$

(i) Cusp values of f_1:

$$f_1(\infty) = G_2^{(2)}(\infty) = -2\zeta(2) \quad \text{by (8)},$$
$$f_1(0) = G_2^{(2)}(0) = \zeta(2) \quad \text{by (9)},$$
$$f_1(1/3) = f_1(0) = \zeta(2) \quad \text{since } f_1 \in M_2(\Gamma_0(2)) \text{ and } 1/3 \sim 0 \text{ under } \Gamma_0(2),$$
$$f_1(1/2) = f_1(\infty) = -2\zeta(2) \quad \text{since } 1/2 \sim \infty \text{ under } \Gamma_0(2).$$

(ii) Cusp values of f_2: Observe that $f_2(z) = f_1(3z) = \frac{1}{3} f_1|_{[\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2}$.

$$\begin{aligned}
f_2(\infty) &= \lim_{z\to i\infty} f_2(z) = \lim_{z\to i\infty} f_1(3z) = f_1(\infty) = -2\zeta(2),\\
f_2(0) &= \lim_{z\to i\infty} f_2|_{\left[\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right]_2} = \lim_{z\to i\infty} \frac{1}{3} f_1|_{[\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2\left[\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right]_2}\\
&= \lim_{z\to i\infty} \frac{1}{3} f_1|_{\left[\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right]_2[\left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right)]_2} = \frac{1}{3} f_1(0)\cdot 3 \cdot \frac{1}{9} = \frac{1}{9}\zeta(2),\\
f_2(1/3) &= \lim_{z\to i\infty} f_2|_{[\left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)]_2} = \lim_{z\to i\infty} \frac{1}{3} f_1|_{[\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2[\left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)]_2}\\
&= \lim_{z\to i\infty} \frac{1}{3} f_1|_{[\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)]_2[\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2} = \frac{1}{3} f_1(1)\cdot 3 = f_1(0) = \zeta(2),\\
f_2(1/2) &= \lim_{z\to i\infty} f_2|_{[\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)]_2} = \lim_{z\to i\infty} \frac{1}{3} f_1|_{[\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2[\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)]_2}\\
&= \lim_{z\to i\infty} \frac{1}{3} f_1|_{[\left(\begin{smallmatrix} 3 & 1 \\ 2 & 1 \end{smallmatrix}\right)]_2\left[\left(\begin{smallmatrix} 1 & -1 \\ 0 & 3 \end{smallmatrix}\right)\right]_2} = \frac{1}{3} f_1(3/2)\cdot 3 \cdot \frac{1}{9} = \frac{1}{9} f_1(1/2) = -\frac{2}{9}\zeta(2).
\end{aligned}$$

(iii) Cusp values of f_3:

$$f_3(\infty) = G_2^{(3)}(\infty) = -4\zeta(2) \quad \text{by (8)},$$
$$f_3(0) = G_2^{(3)}(0) = \frac{4}{3}\zeta(2) \quad \text{by (9)},$$
$$f_3(1/3) = f_3(\infty) = -4\zeta(2) \quad \text{since } f_3 \in M_2(\Gamma_0(3)) \text{ and } 1/3 \sim \infty \text{ under } \Gamma_0(3),$$
$$f_3(1/2) = f_3(0) = \frac{4}{3}\zeta(2) \quad \text{since } 1/2 \sim 0 \text{ under } \Gamma_0(3).$$

By (i), (ii), (iii) and (7) we conclude that

$X(\infty) = 0$, $Y(\infty) = 0$, $j_{1,6}(\infty) = 1$, (see (5) and (6))

$X(0) = \frac{8}{9}\zeta(2)$, $Y(0) = \frac{2}{3}\zeta(2)$, $j_{1,6}(0) = 4/3$,

$X(1/3) = 0$, $Y(1/3) = 6\zeta(2)$, $j_{1,6}(1/3) = 0$,

$X(1/2) = -\frac{16}{9}\zeta(2)$, $Y(1/2) = -\frac{16}{3}\zeta(2)$, $j_{1,6}(1/2) = 1/3$. □

5. Normalized generators

For a modular function f, we call f *normalized* if its q-series is

$$\frac{1}{q} + 0 + a_1 q + a_2 q^2 + \cdots .$$

Lemma 12. *The normalized generator of a genus zero function field is unique.*

Proof. [10], Lemma 8. □

We will construct the normalized generator (or the hauptmodulus) of the function field $\mathbb{C}(X_1(N))$ $(N = 5, 6)$ from the modular function $j_{1,N}$ $(N = 5, 6)$ described in Theorem 9 and Theorem 11. First, we note that

$$\begin{aligned}\frac{-8}{j_{1,5}(z) + 44} &= \frac{-8y}{x + 44y} \\ &= \frac{1}{q} + 5 + 10q + 5q^2 - 15q^3 - 24q^4 + 15q^5 + \cdots ,\end{aligned}$$

which is in $q^{-1}\mathbb{Z}[[q]]$. This will be justified later in §6. Thus let $N(j_{1,5}) = \frac{-8}{j_{1,5}+44} - 5$. As for the modular function $j_{1,6}$, we observe that

$$\begin{aligned}\frac{2}{j_{1,6} - 1} &= \frac{2Y}{X - Y} = \frac{2(G_2(z) - 4G_2(2z) + 3G_2(3z))}{2G_2(2z) - 4G_2(3z) + 2G_2(6z)} = \frac{G_2(z) - 4G_2(2z) + 3G_2(3z)}{G_2(2z) - 2G_2(3z) + G_2(6z)} \\ &= \frac{-8\pi^2 \cdot (q - q^2 + 7q^3 - 5q^4 + \cdots)}{-8\pi^2 \cdot (q^2 - 2q^3 + 3q^4 + \cdots)} \\ &= \frac{1}{q} + 1 + 6q + 4q^2 - 3q^3 - 12q^4 - 8q^5 + \cdots ,\end{aligned}$$

which is also in $q^{-1}\mathbb{Z}[[q]]$ because the q-series of $\frac{1}{-8\pi^2} \cdot (G_2(z) - 4G_2(2z) + 3G_2(3z))$ and $\frac{1}{-8\pi^2} \cdot (G_2(2z) - 2G_2(3z) + G_2(6z))$ belong to $\mathbb{Z}[[q]]$, and the leading coefficient of the latter series is 1. Define $N(j_{1,6}) = \frac{2}{j_{1,6}-1} - 1$. Then the above computation shows that $N(j_{1,5})$ and $N(j_{1,6})$ are the normalized generators of $\mathbb{C}(X_1(5))$ and $\mathbb{C}(X_1(6))$, respectively. By Theorem 9-(c) and 11-(c) we have the following tables:

Table 3. Cusp values of $j_{1,5}$ and $N(j_{1,5})$

s	∞	0	$1/2$	$2/5$
$j_{1,5}(s)$	-44	$-20\sqrt{5}$	$20\sqrt{5}$	∞
$N(j_{1,5})(s)$	∞	$\frac{1+5\sqrt{5}}{2}$	$\frac{1-5\sqrt{5}}{2}$	-5

Table 4. Cusp values of $j_{1,6}$ and $N(j_{1,6})$

s	∞	0	1/3	1/2
$j_{1,6}(s)$	1	4/3	0	1/3
$N(j_{1,6})(s)$	∞	5	-3	-4

Lemma 13. *Let N be a positive integer such that the modular curve $X_1(N)$ is of genus 0. Let t be an element of $\mathbb{C}(X_1(N))$ for which (i) $\mathbb{C}(X_1(N)) = \mathbb{C}(t)$ and (ii) t has no poles except for a simple pole at one cusp s. Let $f \in \mathbb{C}(X_1(N))$. If f has a pole of order n only at s, then f can be written as a polynomial in t of degree n.*

Proof. Take $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma\infty = s$. Let h be the width of s. Then we have

$$t|_\gamma = \frac{1}{c}\,\frac{1}{q_h} + \cdots$$

and

$$f|_\gamma = b_n\,\frac{1}{q_h^n} + \cdots$$

for some $c \neq 0$ and $b_n \neq 0$. Thus

$$(f - b_n(ct)^n)|_\gamma = \lambda_{n-1}\,\frac{1}{q_h^{n-1}} + \cdots$$

for some λ_{n-1}. And

$$(f - b_n(ct)^n - \lambda_{n-1}(ct)^{n-1})|_\gamma = \lambda_{n-2}\,\frac{1}{q_h^{n-2}} + \cdots$$

for some λ_{n-2}. In this way we can choose $\lambda_i \in \mathbb{C}$ such that

$$(f - b_n(ct)^n - \lambda_{n-1}(ct)^{n-1} - \cdots - \lambda_1(ct))|_\gamma \in \mathbb{C}[[q_h]].$$

Let $g = f - b_n(ct)^n - \lambda_{n-1}(ct)^{n-1} - \cdots - \lambda_1(ct)$. Then g has no poles in $\mathfrak{H}^*$, and so g must be a constant, say λ_0. Therefore we end up with $f = b_n c^n t^n + \lambda_{n-1}c^{n-1}t^{n-1} + \cdots + \lambda_1 ct + \lambda_0$, as desired. □

Theorem 14. *Let d be a square free positive integer and t be the hauptmodulus $N(j_{1,N})$, $(N = 5, 6)$. For $z \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$, $t(z)$ is an algebraic integer.*

Proof. Let $j(z) = \frac{1}{q} + 744 + 196884q + \cdots$ be an elliptic modular function. It is well-known that $j(z)$ is an algebraic integer for $z \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$ ([15], [22]). For algebraic proofs, see [3],

[17], [21] and [23]. Now, we view j as a function on the modular curve $X_1(N)$. Let s be a cusp of $\Gamma_1(N)$ other than ∞, whose width is h_s. Then j has a pole of order h_s at the cusp s. On the other hand, $t(z) - t(s)$ has a simple zero at s. Thus

$$j \times \prod_{s \in S_{\Gamma_1(N)} \setminus \{\infty\}} (t(z) - t(s))^{h_s}$$

has a pole only at ∞ whose degree is 12 if $N = 5$ or 6. And so by Lemma 13, it is a monic polynomial in t of degree 12, which we denote by $f(t)$. With the aid of datum from Tables 1,2,3 and 4, we can compute the product part in the above more explicitly, that is,

$$\prod_{s \in S_{\Gamma_1(N)} \setminus \{\infty\}} (t(z) - t(s))^{h_s} = \begin{cases} (t^2 - t - 31)^5 (t+5), & \text{if } N = 5 \\ (t-5)^6 (t+3)^2 (t+4)^3, & \text{if } N = 6. \end{cases}$$

Since j and t have integer coefficients in the q-expansions, $f(t)$ is a monic polynomial in $\mathbb{Z}[t]$ of degree 12. This claims that $t(z)$ is integral over $\mathbb{Z}[j(z)]$. Therefore $t(z)$ is integral over $\mathbb{Z}$ for $z \in \mathbb{Q}(\sqrt{-d}) \cap \mathfrak{H}$. $\square$

6. Integrality of Fourier coefficients of $N(j_{1,5})$

We recall that $N(j_{1,5}) = \frac{-8}{j_{1,5}+44} - 5 = \frac{-8y}{x+44y} - 5$ where $x(z) = 4 \cdot \eta^5(z)/\eta(5z) + E_2^{(5)}(z)$ and $y(z) = \eta^5(5z)/\eta(z)$. Since the q-series of $-8y$ and $x + 44y$ start with $-8(q + q^2 + \cdots)$ ($\in -8q\mathbb{Z}[[q]]$) and $-8q^2 + 32q^3 + \cdots$ ($\in q^2\mathbb{Z}[[q]]$) respectively, the q-series of $N(j_{1,5})$ is in $q^{-1}\mathbb{Z}[[q]]$ if all the Fourier coefficients of $x+44y$ is divisible by 8, in which case we simply write $8 \mid x+44y$. Then

$$\begin{aligned} 8 \mid x + 44y \Leftrightarrow 8 \mid x + 4y \Leftrightarrow 8 \mid 4 \cdot \eta^5(z)/\eta(5z) + 4 \cdot \eta^5(5z)/\eta(z) + E_2^{(5)}(z) \\ \Leftrightarrow 2 \mid \eta^5(z)/\eta(5z) + \eta^5(5z)/\eta(z) \quad \text{except the constant term} \end{aligned}$$

because $24 \mid E_2^{(5)}(z)$ except the constant term. Hence it suffices to show that $2 \mid \eta^5(z)/\eta(5z) + \eta^5(5z)/\eta(z)$ except the constant term.

Let Δ^n be the set of 2×2 integer matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $a \in 1 + N\mathbb{Z}$, $c \in N\mathbb{Z}$, and $ad - bc = n$. For $f \in M_k(\Gamma_1(N))$ we define the Hecke operator T_n by

$$(10) \qquad f|_{T_n} = n^{(k/2)-1} \sum f|_{[\alpha_j]_k}$$

where $\Gamma_1(N)\alpha_j$ runs through the right cosets of $\Gamma_1(N)$ in Δ^n. Then T_n preserves the space $M_k(\Gamma_0(N),\chi)$ for a Dirichlet character χ ([13], §5). Let $W_N(f) = f|_{\left[\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\right]_k}$ be the action of Fricke involution on f.

Lemma 15. *Let n be a positive integer prime to N and $f \in M_k(\Gamma_0(N),\chi)$ for a Dirichlet character χ. Then we have $W_N \circ T_n(f) = \chi(n) T_n \circ W_N(f)$.*

Proof. Δ^n has the following right coset decomposition: (See [13], [16], [22])

$$\Delta^n = \bigcup_{\substack{a|n \\ (a,N)=1}} \bigcup_{i=0}^{\frac{n}{a}-1} \Gamma_1(N)\sigma_a \begin{pmatrix} a & i \\ 0 & \frac{n}{a} \end{pmatrix} \tag{11}$$

where $\sigma_a \in SL_2(\mathbb{Z})$ such that $\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \mod N$. By (10) and (11),

$$T_n \circ W_N(f) = n^{(k/2)-1} \sum_{a,b} f|_{\left[\alpha_N \sigma_a \left(\begin{smallmatrix} a & b \\ 0 & n/a \end{smallmatrix}\right)\right]_k},$$

where $\alpha_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Let $\alpha_{a,b} = \sigma_n \alpha_N \sigma_a \left(\begin{smallmatrix} a & b \\ 0 & n/a \end{smallmatrix}\right) \alpha_N^{-1} \in \Delta^n$. Then it is easy to show that $\alpha_{a,b}$ are in distinct cosets of $\Gamma_1(N)$ in Δ^n, and hence form a set of representatives; so by (10),

$$\begin{aligned} T_n \circ W_N(f) &= n^{(k/2)-1} \sum_{a,b} f|_{[\alpha_{a,b}\alpha_N]_k} = n^{(k/2)-1} \sum_{a,b} f|_{\left[\sigma_n \alpha_N \sigma_a \left(\begin{smallmatrix} a & b \\ 0 & n/a \end{smallmatrix}\right)\right]_k} \\ &= \chi(n) T_n(W_N(f)) \quad \text{since } f|_{[\sigma_n]_k} = \chi(n) f. \end{aligned}$$

This completes the proof. □

Next, we observe that

$$M_2(\Gamma_1(5)) = \bigoplus_{\chi \in \widehat{(\mathbb{Z}/5\mathbb{Z})^\times}} M_2(\Gamma_0(5),\chi).$$

Since $(\mathbb{Z}/5\mathbb{Z})^\times$ is generated by $\bar{2}(= 2 \mod 5\mathbb{Z})$, any $\chi \in \widehat{(\mathbb{Z}/5\mathbb{Z})^\times}$ is determined by the value at $\bar{2}$. Let χ_1 be the character such that $\chi_1(\bar{2}) = i$. Then $\widehat{(\mathbb{Z}/5\mathbb{Z})^\times}$ is generated by χ_1 so that ${\chi_1}^4 = \chi_{triv}$ and ${\chi_1}^2 = \left(\frac{\cdot}{5}\right)$. Note that if χ is an odd character, then $M_2(\Gamma_0(5),\chi) = \{0\}$. Thus

$$M_2(\Gamma_1(5)) = M_2(\Gamma_0(5)) \bigoplus M_2(\Gamma_0(5), \left(\frac{\cdot}{5}\right)). \tag{12}$$

Now that the dimension of the space $M_2(\Gamma)$ is equal to $\sigma_\infty(\Gamma) - 1$, it follows from (12) that $M_2\left(\Gamma_0(5), \left(\frac{\cdot}{5}\right)\right)$ is two dimensional. In fact it is generated by $\eta^5(z)/\eta(5z)$ and $\eta^5(5z)/\eta(z)$.

It then follows from the proof of Lemma 8-(ii) that

$$W_5(\eta^5(z)/\eta(5z)) = -5\sqrt{5}\cdot\eta^5(5z)/\eta(z). \tag{13}$$

The fact that W_5 is an involution and (13) imply that

$$W_5(\eta^5(5z)/\eta(z)) = (-5\sqrt{5})^{-1}\cdot\eta^5(z)/\eta(5z).$$

Since T_m preserves $M_k(\Gamma_0(N),\chi)$, we may set

$$T_m(\eta^5(z)/\eta(5z)) = p_m\cdot\eta^5(z)/\eta(5z) + q_m\cdot\eta^5(5z)/\eta(z) \tag{14}$$

and

$$T_m(\eta^5(5z)/\eta(z)) = r_m\cdot\eta^5(z)/\eta(5z) + s_m\cdot\eta^5(5z)/\eta(z) \tag{15}$$

for $p_m, q_m, r_m, s_m \in \mathbb{C}$. Here, we recall from [13], p.163 that if $f(z) = \sum a_n q^n$ and $T_m(f(z)) = \sum b_n q^n$,

$$b_n = \sum_{\substack{d|(m,n)\\ d>0}} \chi(d)d^{k-1}a_{mn/d^2}.$$

If we compare the constant terms in (15), we get $r_m = 0$. In like manner, from (14) we have

$$p_m = \sum_{\substack{d|m\\ d>0}} \left(\frac{d}{5}\right) d^{k-1}\cdot 1. \tag{16}$$

When $(m,5) = 1$, by Lemma 15 we obtain

$$T_m\circ W_5\left(\frac{\eta^5(z)}{\eta(5z)}\right) = \left(\frac{m}{5}\right) W_5\circ T_m\left(\frac{\eta^5(z)}{\eta(5z)}\right).$$

Then, by (13) the LHS of the above is equal to $-5\sqrt{5}\cdot T_m\left(\frac{\eta^5(5z)}{\eta(z)}\right) = -5\sqrt{5}\left(s_m\cdot\frac{\eta^5(5z)}{\eta(z)}\right)$. On the other hand the RHS is equal to

$$\begin{aligned}\text{RHS} &= \left(\frac{m}{5}\right) W_5\left(p_m\cdot\frac{\eta^5(z)}{\eta(5z)} + q_m\cdot\frac{\eta^5(5z)}{\eta(z)}\right)\\ &= \left(\frac{m}{5}\right)\left[-5\sqrt{5}\cdot p_m\cdot\frac{\eta^5(5z)}{\eta(z)} + (-5\sqrt{5})^{-1}q_m\cdot\frac{\eta^5(z)}{\eta(5z)}\right].\end{aligned}$$

Hence, by equating both sides we deduce that $q_m = 0$ and $s_m = \left(\frac{m}{5}\right)p_m = \left(\frac{m}{5}\right)\cdot\sum_{\substack{d|m\\ d>0}}\left(\frac{d}{5}\right)d^{k-1}$ by (16). Therefore for each positive integer m prime to 5, it holds that

$$T_m\left(\frac{\eta^5(z)}{\eta(5z)}\right) = p_m\cdot\frac{\eta^5(z)}{\eta(5z)} \tag{17}$$

and

$$T_m\left(\frac{\eta^5(5z)}{\eta(z)}\right) = \left(\frac{m}{5}\right) p_m \cdot \frac{\eta^5(5z)}{\eta(z)}. \tag{18}$$

Let $\frac{\eta^5(z)}{\eta(5z)} = \sum c_m q^m$ and $\frac{\eta^5(5z)}{\eta(z)} = \sum d_m q^m$. If we compare the q^1-coefficients in (17) and (18), then we get

$$c_m = -5 \cdot p_m,\ \ d_m = \left(\frac{m}{5}\right) p_m \quad \text{for } (m,5)=1. \tag{19}$$

Now, let $m = 5$. It then follows from (16) that $p_5 = 1$. Moreover in (17) and (18) by comparing the q^1-coefficients, we have $q_5 = 0$ and $s_5 = 5$. More generally, we take $m = 5^l \cdot m_0$ with $l \geq 0$ and $5 \nmid m_0$. Then

(20)

$$\begin{aligned} T_{5^l\cdot m_0}\left(\frac{\eta^5(z)}{\eta(5z)}\right) &= T_{5^l}\circ T_{m_0}\left(\frac{\eta^5(z)}{\eta(5z)}\right) = T_{5^l}\left(p_{m_0}\cdot\frac{\eta^5(z)}{\eta(5z)}\right) \quad \text{by (19)} \\ &= (T_5)^l\left(p_{m_0}\cdot\frac{\eta^5(z)}{\eta(5z)}\right) = p_{m_0}\cdot {p_5}^l\cdot\frac{\eta^5(z)}{\eta(5z)} = p_{m_0}\cdot\frac{\eta^5(z)}{\eta(5z)} \quad \text{since } p_5 = 1. \end{aligned}$$

Similarly,

$$T_{5^l\cdot m_0}\left(\frac{\eta^5(5z)}{\eta(z)}\right) = \left(\frac{m_0}{5}\right)\cdot p_{m_0}\cdot 5^l\cdot\frac{\eta^5(5z)}{\eta(z)}. \tag{21}$$

In the equations (20) and (21), if we compare the q^1-coefficients, we obtain

$$c_{5^l\cdot m_0} = -5\cdot p_{m_0} \quad \text{and} \quad d_{5^l\cdot m_0} = 5^l\cdot\left(\frac{m_0}{5}\right)\cdot p_{m_0}$$

with $p_{m_0} = \sum_{\substack{d|m_0 \\ d>0}} \left(\frac{d}{5}\right) d^{k-1}$. And, it is clear that 2 divides $c_{5^l\cdot m_0} + d_{5^l\cdot m_0}$, hence we conclude that

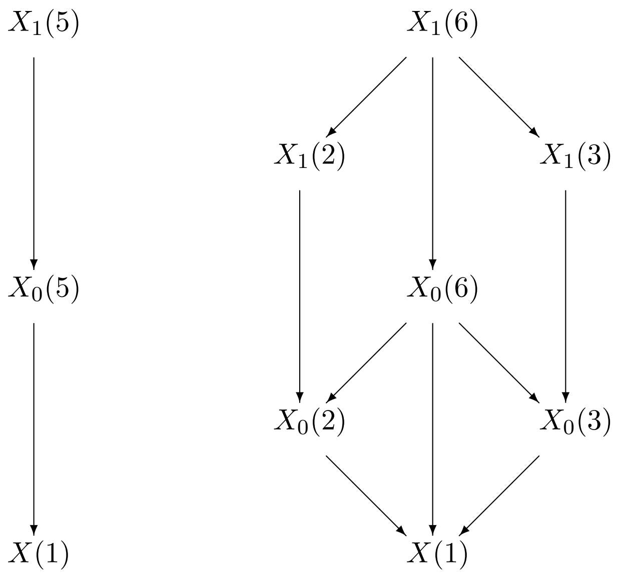
$$2 \mid \frac{\eta^5(z)}{\eta(5z)} + \frac{\eta^5(5z)}{\eta(z)}$$

except the constant term.

7. Relationship with moduli of elliptic curves

When k is a field of characteristic prime to N, the k-rational points on the curve $X_0(N)$ ($X_1(N)$, respectively) parametrize pairs (E, C) (pairs (E, P), respectively) - modulo equivalence over an algebraic closure k^{alg} - of elliptic curves E with a k-rational cyclic subgroup C (k-rational point P, respectively) of order N. There are "forgetful" maps $X_1(N)$ to $X_0(N)$

which send $(E, P) \to (E, C)$ in terms of the subgroup $C = \{P, [2]P, \ldots, [N]P\}$. There are two diagrams of interest coming from these "forgetful" maps:



All of these curves have genus zero, but some of theses modular curves are easier to describe than others. For example, there is a canonical bijection $\mathbb{P}^1 \to X(1)$ of the "j-line" which sends $j \mapsto (E_j, O_j)$ in terms of the normal form

$$E_j : y^2 + xy = x^3 - \frac{36}{j - 1728} x - \frac{1}{j - 1728}$$

with a specified base point $O_j = (0 : 1 : 0)$. Clearly the function field of $X(1)$ is $k(j)$.

Similarly, there are canonical bijections $\mathbb{P}^1 \to X_1(N)$ which send $t \mapsto (E_t, P_t)$ in terms of the Tate normal forms

$$E_t : \begin{cases} y^2 = x^3 + 2x^2 + tx, & \text{if } N = 2; \\ y^2 + 3xy + ty = x^3, & \text{if } N = 3; \\ y^2 + (1+t)xy + ty = x^3 + tx^2, & \text{if } N = 5; \\ y^2 + (1+t)xy + (t - t^2)y = x^3 + (t - t^2)x^2, & \text{if } N = 6; \end{cases} \tag{22}$$

each with a specified point $P_t = (0 : 0 : 1)$ of order N. Such formulas can be found in [6, pp.94-95]. Using the "forgetful" maps $X_1(N)$ to $X(1)$, one has the expressions

$$j = \begin{cases} 64(4 - 3t)^3/(t^2(1 - t)), & \text{if } N = 2; \\ 27(9 - 8t)^3/(t^3(1 - t)), & \text{if } N = 3; \\ (1 - 12t + 14t^2 + 12t^3 + t^4)^3/(t^5(1 - 11t - t^2)), & \text{if } N = 5; \\ ((1 - 3t)(1 - 9t + 3t^2 - 3t^3))^3/(t^6(1 - t)^3(1 - 9t)), & \text{if } N = 6. \end{cases}$$

Clearly the function field of $X_1(N)$ is $k(t)$ in these cases; it may be thought of as an algebraic extension of $k(j)$. When the parameter t is interpreted as a modular function $t(z)$, we can find the following identities between our modular function $N(j_{1,N})(z)$ and $t(z)$.

Theorem 16. *(i)* $N(j_{1,5})(z) + 5 = \frac{\varepsilon^5 t(z)+1}{-t(z)+\varepsilon^5}$.
(ii) $N(j_{1,6})(z) + 1 = 6\frac{1+3t(z)}{1-9t(z)}$.
Here we set $\varepsilon = \zeta_5 + \zeta_5^{-1}$.

Proof. (i) First we note that ε satisfies $\varepsilon^2 + \varepsilon - 1 = 0$. Since $\varepsilon = 2\cos(2\pi/5) > 0$, we have $\varepsilon = \frac{-1+\sqrt{5}}{2}$ and hence $\varepsilon^5 = \frac{-11+5\sqrt{5}}{2}$. Let $f(z) = N(j_{1,5})(z) + 5$. The values of $f(z)$ at the cusps (obtained from Table 3) are:

s	∞	$2/5$	$1/2$	0
$f(s)$	∞	0	$-\varepsilon^5$	ε^{-5}

Since $\Delta(E_t) = -t^5(t^2 + 11t - 1)$ from the equation of E_t in (22), the set of possible values of $t(z)$ at the cusps are $\{\infty, 0, \varepsilon^5, -\varepsilon^{-5}\}$. Since $t(z)$ is a fractional linear transformation of $f(z)$, we come up with

$$[f(\infty), f(2/5), f(1/2), f(0)] = [t_1, t_2, t_3, t_4]$$
$$[\infty, 0, -\varepsilon^5, f(z)] = [t_1, t_2, t_3, t(z)]$$

where $t_1 = t(\infty), t_2 = t(2/5), t_3 = t(1/2), t_4 = t(0)$. Thus we obtain that

$$\frac{(t(z)-t_1)(t_2-t_3)}{(t(z)-t_3)(t_2-t_1)} = \frac{\varepsilon^5}{f(z)+\varepsilon^5}. \tag{23}$$

Suppose $t(z)$ has a pole or zero at a cusp s. Let h be the width of the cusp s. Considering the q_h-expansion of $t(z)$ at s we see from the identity

$$j = \frac{(1 - 12t + 14t^2 + 12t^3 + t^4)^3}{t^5(1 - 11t - t^2)}$$

that $\frac{1}{q} + O(1) = \frac{1}{q_h^5} + O(1)$. This yields $h = 5$. It then follows from Table 1 that $s = 1/2$ or $s = 0$. This means that $t_3, t_4 \in \{\infty, 0\}$ and so $t_1, t_2 \in \{\varepsilon^5, -\varepsilon^{-5}\}$. There are four possibilities for the cusp values $t(s)$:

Case (i). $t_1 = \varepsilon^5, t_2 = -\varepsilon^{-5}, t_3 = 0, t_4 = \infty$

Case (ii). $t_1 = \varepsilon^5, t_2 = -\varepsilon^{-5}, t_3 = \infty, t_4 = 0$

Case (iii). $t_1 = -\varepsilon^{-5}, t_2 = \varepsilon^5, t_3 = 0, t_4 = \infty$

Case (iv). $t_1 = -\varepsilon^{-5}, t_2 = \varepsilon^5, t_3 = \infty, t_4 = 0$

We see by routine check that only the second and third case satisfy the identity (23), from which we conclude that $t(z)$ should be either

$$u(z) = \frac{\varepsilon^5 f(z) - 1}{f(z) + \varepsilon^5} \quad \text{or} \quad v(z) = \frac{f(z) + \varepsilon^5}{-\varepsilon^5 f(z) + 1}.$$

Now we consider the elliptic curve $E_1 : y^2 + 2xy + y = x^3 + x^2$. By making appropriate change of variables we achieve the elliptic curve

$$E : y^2 = 4x^3 - \frac{4}{3}x + \frac{19}{27}$$

which is isomorphic to E_1. We note that under this isomorphism the point $P_1 = (0,0) \in E_1$ is sent to $(2/3, -1) \in E$. The period lattice L of E is given by $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with

$$\omega_1 = 6.3460465213977671084439730837727365260 87\cdots\ ,$$

$$\omega_2 = 3.1730232606988835542219865418863682630438\cdots$$
$$+ 1.4588166169384952293308896129036752571 58\cdots i$$

from which we can estimate that

$$g_2(L) = 1.33333\cdots\ ,\ g_3(L) = -0.703703703\cdots\ ,$$

$$\mathcal{P}(\omega_1/5, L) = 0.66666\cdots\ ,\ \mathcal{P}'(\omega_1/5, L) = -1.00000\cdots\ .$$

Here $\mathcal{P}(z, L)$ stands for the Weierstrass $\mathcal{P}$-function attached to the lattice L. Thus it turns out that the point of $X_1(5)$ corresponding to the pair (E_1, P_1) is ω_2/ω_1. Using the Fourier expansion of $f(z)$ we can find $u(\omega_2/\omega_1) = 1.00000\cdots$ and $v(\omega_2/\omega_1) = -1.00000\cdots$. Therefore we are forced to have $t(z) = u(z)$.

(ii) Let $g(z) = N(j_{1,6})(z) + 1$. Then it is immediate from Table 4 that the values of $g(z)$ at the cusps of $X_1(6)$ are as follows:

s	∞	0	1/3	1/2
$g(s)$	∞	6	-2	-3

Since $\Delta(E_t) = (t-1)^3 t^6 (9t-1)$ from the equation of E_t in (22), the set of possible values of $t(z)$ at the cusps are $\{\infty, 1, 0, 1/9\}$. Since $t(z)$ is a fractional linear transformation of $g(z)$, we have the equality

$$[g(\infty), g(0), g(1/3), g(1/2)] = [t_1, t_2, t_3, t_4]$$
$$[\infty, 6, -2, g(z)] = [t_1, t_2, t_3, t(z)]$$

where $t_1 = t(\infty), t_2 = t(0), t_3 = t(1/3), t_4 = t(1/2)$. Thus we establish

$$\frac{(t(z)-t_1)(t_2-t_3)}{(t(z)-t_3)(t_2-t_1)} = \frac{8}{g(z)+2}. \tag{24}$$

Suppose $t(s) = \infty$ for some cusp s. We let h be the width of the cusp s and consider the q_h-expansion of $t(z)$ at s. We choose an element $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma\infty = s$. It then follows that $t|_\gamma = \frac{c}{q_h} + O(1)$ for some $c \in \mathbb{C}$. Now, from the identity

$$j = \frac{((1-3t)(1-9t+3t^2-3t^3))^3}{t^6(1-t)^3(1-9t)}$$

we see that $\frac{1}{q} + O(1) = \frac{1}{q_h^2} + O(1)$. This yields $h = 2$. It then follows from Table 2 that $s = 1/3$ and hence $t_3 = t(1/3) = \infty$. Similarly if $t(s) = 0$, then we come up with $\frac{1}{q} + O(1) = \frac{1}{q_h^6} + O(1)$. Thus we have $h = 6$ and $s = 0$. And we deduce that $t_2 = t(0) = 0$. Therefore, the identity (24) is simplified to

$$\frac{t(z)-t_1}{-t_1} = \frac{8}{g(z)+2}. \tag{25}$$

Here we have two choices for the values t_1 and t_4: $t_1 = 1$ and $t_4 = 1/9$, or $t_1 = 1/9$ and $t_4 = 1$. Only the latter case fits the identity (25), from which we get the assertion as desired. □

According to the referee's comment we can have canonical bijections $\mathbb{P}^1 \to X_0(N)$ which send $r \mapsto (E_r, C_r)$ in terms of the normal forms

$$E_r : \begin{cases} y^2 = x^3 + \frac{2(r+64)}{r^2}x^2 + \frac{r+64}{r^3}x, & \text{if } N = 2; \\ y^2 + \frac{3(r+27)}{r}xy + \frac{(r+27)^2}{r^2}y = x^3, & \text{if } N = 3; \\ y^2 + \frac{2(2r+25)}{r}xy + \frac{4(r^2+22r+125)}{r^2}y = x^3 + \frac{r+10}{r}x^2, & \text{if } N = 5; \\ y^2 + \frac{5r+36}{r}xy + \frac{9(r+8)(r+9)}{r^2}y = x^3 + \frac{2(r+9)}{r}x^2, & \text{if } N = 6; \end{cases}$$

and cyclic subgroups $C_r =< (x : y : 1) \mid \psi_r(x) = 0 >$ of order N which are generated by the roots of certain divisors of the division polynomials:

$$\psi_r(x) = \begin{cases} x & \text{if } N = 2; \\ x & \text{if } N = 3; \\ 5x^2 - \frac{4(r^2+22r+125)}{r^2} & \text{if } N = 5; \\ x & \text{if } N = 6. \end{cases}$$

Using the "forgetful" maps $X_1(N) \to X_0(N)$, one has the expressions

$$r = \begin{cases} 64t/(1-t), & \text{if } N = 2; \\ 27t/(1-t), & \text{if } N = 3; \\ 125t/(1-11t-t^2), & \text{if } N = 5; \\ 72t/(1-9t), & \text{if } N = 6. \end{cases}$$

Clearly the function field of $X_0(N)$ is $k(r)$ in these cases; it may be thought of as an algebraic extension of $k(j)$ which is contained in $k(t)$. These curves are chosen on the parameter r. For $z \in \mathfrak{H}^*$, define the hauptmoduli

$$r(z) = \begin{cases} \left(\frac{\eta(z)}{\eta(2z)}\right)^{24} = \frac{1}{q} - 24 + 276q - 2048q^2 + \cdots & \text{if } N = 2; \\ \left(\frac{\eta(z)}{\eta(3z)}\right)^{12} = \frac{1}{q} - 12 + 54q - 76q^2 + \cdots & \text{if } N = 3; \\ \left(\frac{\eta(z)}{\eta(5z)}\right)^{6} = \frac{1}{q} - 6 + 9q + 10q^2 + \cdots & \text{if } N = 5; \\ \frac{\eta(z)^5\eta(3z)}{\eta(2z)\eta(6z)^5} = \frac{1}{q} - 5 + 6q + 4q^2 + \cdots & \text{if } N = 6, \end{cases}$$

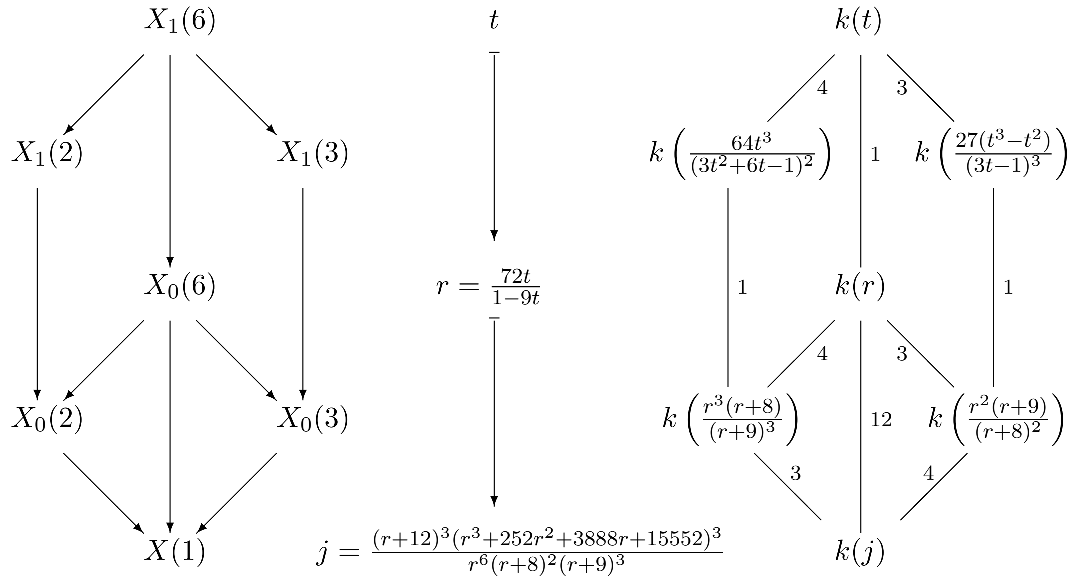
in terms of the Dedekind eta function

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \qquad \text{for } q = e^{2\pi i z}.$$

We may summarize all of this discussion in a lattice diagram of function fields. As for $X_1(5)$, the "forgetful" maps correspond to the following for a field of k of characteristic not dividing 5:

$$\begin{array}{ccc} X_1(5) & t & k(t) \\ \downarrow & \downarrow & \big| \, 2 \\ X_0(5) & r = \frac{125t}{1-11t-t^2} & k(r) \\ \downarrow & \downarrow & \big| \, 6 \\ X(1) & j = \frac{(r^2+250r+3125)^3}{r^5} & k(j) \end{array}$$

For $X_1(6)$, the "forgetful" maps correspond to the following for a field of k of characteristic not dividing 6:



Acknowledgement. We appreciate the referee for his valuable and prudent comments and suggestions which enabled us to add the last section on certain connection with moduli of elliptic curves. It definitely makes our work be better one.

References

[1] Borcherds, R.E., Monstrous moonshine and monstrous Lie superalgebras, Invent. math. 109, 405-444, 1992.
[2] Conway, J.H. and Norton, S.P., Monstrous Moonshine, Bull. London Math. Soc., 11, 308-339, 1979.
[3] Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg 14, 197-272, 1941.
[4] Ferenbaugh, C.R., The genus-zero problem for $n|h$-type groups, Duke Math. Journal, Vol. 72, No. 1, 31-63, 1993.
[5] Harada, K., Moonshine of Finite Groups, Ohio State University, (Lecture Note).
[6] Husemöller, D., Elliptic Curves (Second Edition), Springer-Verlag, 2004.
[7] Ishii, N., Construction of generators of modular function fields, Math. Japon. 28, 655-681, 1983.
[8] Ishida, N. and Ishii, N., The equation for the modular curve $X_1(N)$ derived from the equation for the modular curve $X(N)$, Tokyo J. Math. 22, 167-175, 1999.
[9] Kim, C.H. and Koo, J.K., On the genus of some modular curve of level N, Bull. Australian Math. Soc., 54, 291-297, 1996.
[10] ______________________, Arithmetic of the modular function $j_{1,4}$, Acta Arith. 84, 129-143, 1998.
[11] ______________________, Arithmetic of the modular function $j_{1,8}$, Ramanujan J., 4, 317-338, 2000.
[12] Knapp, A.W., Elliptic Curves, Mathematical Notes 40, Princeton University Press, 1992.
[13] Koblitz, N., Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, 1984.
[14] Kubert, D. and Lang, S., Units in the modular function fields, Math. Ann. 218, 175-189, 1975.
[15] Lang, S., Elliptic Functions, Springer-Verlag, 1987.
[16] Miyake, T., Modular Forms, Springer-Verlag, 1989.
[17] Néron, A., Modeles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I.H.E.S. no.21, 5-128, 1964.

[18] Ogg, A., Survey of Modular Functions of One Variable, Lecture Notes in Mathematics 320, 1-36, Springer-Verlag 1986.
[19] Rankin, R., Modular Forms and Functions, Cambridge: Cambridge University press 1977.
[20] Schoeneberg, B., Elliptic Modular Functions, Springer-Verlag, 1973.
[21] Serre, J.-P. and Tate, J., Good reduction of abelian varieties, Ann. Math. 88, 492-517, 1968.
[22] Shimura, G., Introduction to the Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan, No.11. Tokyo Princeton, 1971.
[23] Silverman, J.H., Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994
[24] Thompson, J.G., Some numerology between the Fischer-Griess monster and the elliptic modular function, Bull. London Math. Soc. 11, 352-353, 1979.

[1]Department of Mathematics, Hanyang University, Seoul, 133-791 Korea
E-mail address: `chhkim@hanyang.ac.kr`

[2]Korea Advanced Institute of Science and Technology, Department of Mathematical Sciences, Daejeon, 305-701 Korea
E-mail address: `jkkoo@math.kaist.ac.kr`