Applications and Applied Mathematics: An International Journal (AAM)

Volume 14
Issue 3 *Special Issue No. 3*

Article 2

2-2019

Elliptic Elements of a Subgroup of the Normalizer and Circuits in Orbital Graphs

Nazlı Y. Gözütok
Karadeniz Technical University

Bahadır Ö. Güler
Karadeniz Technical University

Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Applications and Applied Mathematics:
An International Journal
(AAM)

Special Issue No. 3 (February 2019), pp. 11 – 21

Elliptic Elements of a Subgroup of the Normalizer and Circuits in Orbital Graphs

[1]Nazlı Yazıcı Gözütok, [2]Bahadır Özgür Güler

Department of Mathematics
Karadeniz Technical University
Trabzon, Turkey
[1]nazliyazici@ktu.edu.tr, [2]boguler@ktu.edu.tr

Received: August 8, 2018; Accepted: November 3, 2018

Abstract

In this study, we investigate suborbital graphs $G_{u,N}$ of the normalizer $\Gamma_B(N)$ of $\Gamma_0(N)$ in $PSL(2,\mathbb{R})$ for $N = 2^\alpha 3^\beta > 1$ where $\alpha = 0, 2, 4, 6$, and $\beta = 0, 2$. In these cases the normalizer becomes a triangular group. We first define an imprimitive action of $\Gamma_B(N)$ on $\hat{Q}$ using the group $\Gamma_C^0(N)$ and then obtain some properties of the suborbital graphs arising from this action. Finally we define suborbital graphs $F_{u,N}$ and investigate their properties. As a consequence, we find some certain relationships between the lengths of circuits in suborbital graphs $F_{u,N}$ and the periods of the group $\Gamma_C^0(N)$.

Keywords: Normalizer; Congruence Subgroup; Suborbital Graphs

MSC 2010 No.: 20H10; 05C25

1. Introduction

Orbital graphs, also called suborbital graphs, were introduced into the theory of permutation groups (especially finite permutation groups) by Sims (1967). In their paper, Jones et al. (1991) investigate the concept in the relation to the modular group Γ acting on the projective line $PG(1,\mathbb{Q})$ over the field of rational numbers. This is an interesting infinite permutation group that, for well over a century, has played an important role in number theory, in the theory of binary quadratic forms, and in the theory of modular forms and automorphic functions.

The group $SL(2,\mathbb{Z})$, the group of 2×2 matrices of determinant 1 with integer entries, has a natural action by Mobius transformations on $PG(1,\mathbb{Q})$, given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d} \text{ for } z \in \mathbb{Q} \cup \{\infty\}.$$

The kernel of this action is $I_2, -I_2$ and Γ is $PSL(2,\mathbb{Z})$, the quotient of $SL(2,\mathbb{Z})$ by this kernel, that is, it is the induced permutation group. It is natural to identify elements of Γ with the associated 2×2 matrices X, although one must always appreciate that X and $-X$ represent the same member of Γ. The modular group has a wealth of subgroups, among which the congruence subgroups are perhaps the most important and certainly the best known. Of the congruence subgroups, the groups $\Gamma_0(N)$ have been studied extensively, especially, by Klein, Fricke, and many others, and are basic to the theory of the elliptic modular functions (Schoeneberg (1974)).

The normalizer $\Gamma_B(N)$ of $\Gamma_0(N)$ in $PSL(2,\mathbb{R})$ has acquired significance because it is related to the Monster simple group Conway and Norton (1977), Chua and Lang (2004). As in Akbaş (1989), $\Gamma_B(N)$ consists exactly of the matrices

$$\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix},$$

where all parameters are integers, $e||\frac{N}{h^2}$ and h is the largest divisor of 24 for which $h^2|N$ with understanding that the determinant e of the matrix is positive, and that $r||s$ means that $r|s$ and $(r, r/s) = 1$. It has also played an important role in work on Weierstrass points on Riemann surfaces associated to $\Gamma_0(N)$ by Lehner and Newman (1964). $\Gamma_C(N)$ is one of the important subgroups of the normalizer which is the set of transformations of determinant one. Another subgroup of $\Gamma_B(N)$ is the set $\Gamma_C^0(N)$ which consists of the matrices

$$\begin{pmatrix} a & b/h \\ cN & d \end{pmatrix},$$

with determinant 1. It is easily seen that $\Gamma_C^0(N) \le \Gamma_C(N) \le \Gamma_B(N)$.

Akbaş and Singerman (1990) shows that $\Gamma_0(N)$ contains an elliptic element of order $2(3)$ if and only if there exists a unit u in the group U_N of units $(\text{mod } N)$ such that $F_{u,N}$ contains a two-gon (triangle), respectively. This is important taking into account that the order of the elliptic elements is one of invariants in the signature of Fuchsian groups. In this study, examining the suborbital graphs of $\Gamma_B(N)$ in the cases where the normalizer is a triangle group, we calculate the order of the elliptic element of the group $\Gamma_C^0(N)$.

2. The Action of $\Gamma_B(N)$ on $\hat{\mathbb{Q}}$

In this section, we describe transitive and imprimitive action of $\Gamma_B(N)$. Hence we can apply Sim's theory to obtain suborbital graphs in the next section.

Every element of $\hat{\mathbb{Q}}$ can be represented as a reduced fraction $\frac{x}{y}$, with $x, y \in \mathbb{Z}$ and $(x,y) = 1$. Since $\frac{x}{y} = \frac{-x}{-y}$ this representation is not unique. We represent ∞ as $\frac{1}{0} = \frac{-1}{0}$. The action of the matrix

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on $\frac{x}{y}$ is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \frac{x}{y} \to \frac{ax+by}{cx+dy}.$$

Remark.

It is easily seen that if the determinant of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is 1 and if $\frac{x}{y} \in \hat{\mathbb{Q}}$ then, since $c(ax+by) - a(cx+dy) = -y$ and $d(ax+by) - b(cx+dy) = x$, $(ax+by, cx+dy) = 1$.

In this paper, we study suborbital graphs $G_{u,N}$ of the normalizer $\Gamma_B(N)$ for $N = 2^\alpha 3^\beta > 1$ where $\alpha = 0, 2, 4, 6$, $\beta = 0, 2$. With this purpose in mind, from now on, unless otherwise stated explicitly, N will denote an integer such that $N = 2^\alpha 3^\beta > 1$ where $\alpha = 0, 2, 4, 6$, and $\beta = 0, 2$.

Theorem 2.2.

$\Gamma_B(N)$ acts transitively on $\hat{\mathbb{Q}}$.

Proof:

It is enough to prove that the orbit containing ∞ is $\hat{\mathbb{Q}}$. Let $\frac{x}{y} \in \hat{\mathbb{Q}}$, $(y,h) = k$ and $y = y_1 k$, $h = h_1 k$, since $(y,h) = k$, $(y_1, h_1) = 1$. Also since $(x,y) = 1$, and $(x, y_1) = 1$. Thus $(xh_1, y_1) = 1$, follows that there are integers $a, b \in \mathbb{Z}$ such that $axh_1 - by_1 = 1$. Therefore,

$$T = \begin{pmatrix} xh_1 & b/h \\ y_1 h & a \end{pmatrix} \in \Gamma_B(N),$$

and $T(\infty) = \frac{x}{y}$. This completes the proof. ∎

Theorem 2.3.

The stabilizer of ∞ is the group $\Gamma_B(N)_\infty$ whose elements are of the form

$$\begin{pmatrix} 1 & b/h \\ 0 & 1 \end{pmatrix}, b \in \mathbb{Z}.$$

Proof:

The stabilizer of ∞ is the set $\Gamma_B(N)_\infty = \{T \in \Gamma_B(N) : T(\infty) = \infty\}$.

We obtain $T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for $T = \begin{pmatrix} a & b/h \\ ch & d \end{pmatrix} \in \Gamma_B(N)$. Then we have $a = 1$ and $c = 0$. Since $ad - bc = 1$, we have $d = 1$. Therefore, T has the form

$$\begin{pmatrix} 1 & b/h \\ 0 & 1 \end{pmatrix}, \ b \in \mathbb{Z}.$$

∎

Now we consider the imprimitivity of the action of $\Gamma_B(N)$ on $\hat{\mathbb{Q}}$, hence we start with a general discussion of primitivity of permutation groups.

Let (G, Δ) be a transitive permutation group, consisting of a group G acting on a set Δ transitively. An equivalence relation $\approx$ on Δ is called *G-invariant* if, whenever $\alpha, \beta \in \Delta$ satisfy $\alpha \approx \beta$, then $g(\alpha) \approx g(\beta)$ for all $g \in G$.

The equivalence classes are called blocks, and the block containing α is denoted by $[\alpha]$.

We call (G, Δ) *imprimitive* if Δ admits some G-invariant equivalence relation different from

(i) the identity relation, $\alpha \approx \beta$ if and only if $\alpha = \beta$;
(ii) the universal relation, $\alpha \approx \beta$ for all $\alpha, \beta \in \Delta$.

Otherwise (G, Δ) is called *primitive*. These two relations are supposed to be trivial relations. Clearly, a primitive group must be transitive, for if not the orbits would form a system of blocks. The converse is false, but we have the following useful result.

Lemma 2.4 (Biggs and White (1979)).

Let (G, Δ) be a transitive permutation group. (G, Δ) is primitive if and only if G_α the stabilizer of $\alpha \in \Delta$, is a maximal subgroup of G for each $\alpha \in \Delta$.

From the above lemma we see that whenever for some α, $G_\alpha \lneqq H \lneqq G$, then Ω admits some G-invariant equivalence relation other than the trivial cases. Because of the transitivity, every element of Ω has the form $g(\alpha)$ for some $g \in G$. Thus one of the non-trivial G-invariant equivalence relation on Ω is given as follows:

$$g(\alpha) \approx g'(\alpha) \text{ if and only if } g' \in gH.$$

If we set $G = \Gamma_B(N)$, $\Delta = \hat{\mathbb{Q}}$, $H = \Gamma_C^0(N)$ and $G_\alpha = \Gamma_B(N)_\infty$, then we clearly see that $\Gamma_B(N)_\infty \lneqq \Gamma_C^0(N) \lneqq \Gamma_B(N)$. By Lemma 2.4, $\Gamma_B(N)$ acts imprimitively on $\hat{\mathbb{Q}}$.

We define the following $\Gamma_B(N)$ invariant equivalence relation " $\approx$ " on $\hat{\mathbb{Q}}$. Since $\Gamma_B(N)$ acts transitively on $\hat{\mathbb{Q}}$, every element of $\hat{\mathbb{Q}}$ has the form $g(\infty)$ for some $g \in \Gamma_B(N)$. So, it is easily seen that

$$g(\infty) \approx g'(\infty) \Longleftrightarrow g' \in g\Gamma_B(N),$$

gives a $\Gamma_B(N)-$invariant imprimitive equivalence relation.

Let $v = \frac{r}{s}, w = \frac{x}{y} \in \hat{\mathbb{Q}}$ such that $(s, h) = h_1$ and $(y, h) = h_2$. If $s = s_1 h_1$, $y = y_1 h_2$ and $h_1' = \frac{h}{h_1}$, $h_2' = \frac{h}{h_2}$, then since $(s, h) = h_1$ and $h_1' = \frac{h}{h_1}$ we have $(s_1, h_1') = 1$. Also since $(r, s) = 1$, $(r, s_1) = 1$. Thus $(rh_1', s_1) = 1$, follows that there are integers $a, b \in \mathbb{Z}$ such that $arh_1' - bs_1 = 1$. Therefore,

$$g = \begin{pmatrix} rh_1' & b/h \\ s_1 h & a \end{pmatrix} \in \Gamma_B(N),$$

and $g(\infty)=\frac{r}{s}$. Similarly it is obtained that $(xh'_2, y_1)=1$. There are integers $a', b' \in \mathbb{Z}$ such that $a'xh'_2 - b'y_1 = 1$. Therefore,

$$g' = \begin{pmatrix} xh'_2 & b'/h \\ y_1 h & a' \end{pmatrix} \in \Gamma_B(N),$$

and $g'(\infty)=\frac{x}{y}$. Since

$$g^{-1}g' = \begin{pmatrix} a & -b/h \\ -s_1 h & rh'_1 \end{pmatrix} \begin{pmatrix} xh'_2 & b'/h \\ y_1 h & a' \end{pmatrix} = \begin{pmatrix} * & * \\ (ry_1h'_1 - xs_1h'_2)h & * \end{pmatrix},$$

$g^{-1}g' \in \Gamma_C^0(N)$ if and only if $ry_1h'_1 - xs_1h'_2 \equiv 0 \pmod h$. Thus we obtain the block condition as

$$v \approx w \iff ry_1h'_1 - xs_1h'_2 \equiv 0 \pmod h. \tag{1}$$

By our general discussion of imprimitivity, the number of blocks under $\approx$ is given by the index $|\Gamma_B(N) : \Gamma_C^0(N)|$.

Lemma 2.5.

The index of $\Gamma_0(N)$ in $\Gamma_C^0(N)$ is equal to h, where h is the largest divisor of 24 for which $h^2|N$.

Proof:

We can easily verify that

$$\Gamma_0(N/h) = \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix} \Gamma_C^0(N) \begin{pmatrix} 1 & 0 \\ 0 & h \end{pmatrix},$$

that is to say that $\Gamma_C^0(N)$ is a conjugate of $\Gamma_0(N/h)$ by $\begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix}$. Thus we get

$$\begin{aligned} |\Gamma_C^0(N) : \Gamma_0(N)| &= |\Gamma_0(N/h) : \Gamma_0(N)| \\ &= \frac{|\Gamma : \Gamma_0(N))|}{|\Gamma : \Gamma_0(N/h)|} \\ &= \frac{N\prod_{p|N}\left(1+\frac{1}{p}\right)}{N/h\prod_{p|N/h}\left(1+\frac{1}{p}\right)} = h. \end{aligned}$$

■

Lemma 2.6 (Akbaş (1989)).

$|\Gamma_B(N) : \Gamma_0(N)| = 2^\rho h^2 \tau$ where h is the largest divisor of 24 for which $h^2|N$, ρ is the number of distinct prime factors of N/h^2 and

$$\tau = \prod_{p|N}(1+\frac{1}{p}) / \prod_{p|N/h^2}(1+\frac{1}{p}).$$

Theorem 2.7.

The number of blocks arising from the imprimitive action of $\Gamma_B(N)$ by above relation is equal to $2^\rho h\tau$.

Proof:

The number of blocks arising from the imprimitive action of $\Gamma_B(N)$ by above relation is the index $|\Gamma_B(N) : \Gamma_C^0(N)|$. By using Lemma 2.5 and Lemma 2.6, we have

$$|\Gamma_B(N) : \Gamma_C^0(N)| = \frac{|\Gamma_B(N) : \Gamma_0(N)|}{|\Gamma_C^0(N) : \Gamma_0(N)|} = 2^\rho h\tau. \qquad \blacksquare$$

3. Suborbital graphs for $\Gamma_B(N)$

Sims (1967) introduced the idea of the suborbital graphs of a permutation group G acting on a set Δ. These are graphs with vertex-set Δ, on which G induces automorphisms. We summarize Sims' theory as follow: Let (G, Δ) be a transitive permutation group. Then G acts on $\Delta \times \Delta$ by $g(\alpha, \beta) = (g(\alpha), g(\beta))$, $(g \in G, \alpha, \beta \in \Delta)$. The orbits of this action are called *suborbitals* of G. The orbit containing (α, β) is denoted by $O(\alpha, \beta)$. From $O(\alpha, \beta)$ we can form a *suborbital graph* $G(\alpha, \beta)$: its vertices are the elements of Δ, and there is a directed edge from γ to δ if $(\gamma, \delta) \in O(\alpha, \beta)$. A directed edge from γ to δ is denoted by $(\gamma \to \delta)$. If $(\gamma, \delta) \in O(\alpha, \beta)$, then we say that there exists an edge $(\gamma \to \delta)$ in $G(\alpha, \beta)$.

If $\alpha = \beta$, then the corresponding suborbital graph $G(\alpha, \alpha)$, called the trivial suborbital graph, is *self-paired*: it consists of a loop based at each vertex $\alpha \in \Delta$. By a *circuit* of length *m* (or a closed edge path), we mean a sequence $v_1 \to v_2 \to \ldots \to v_m \to v_1$ such that $v_i \neq v_j$ for $i \neq j$, where $m \geq 3$. If $m = 3$ or 4 then the circuit is called a triangle or rectangle.

In this study, G is $\Gamma_B(N)$ and Δ is $\hat{\mathbb{Q}}$. We now consider the suborbital graphs for the action $\Gamma_B(N)$ on $\hat{\mathbb{Q}}$. Since $\Gamma_B(N)$ acts transitively on $\hat{\mathbb{Q}}$, each suborbital contains a pair $(\infty, \frac{u}{N})$ for some $\frac{u}{N} \in \hat{\mathbb{Q}}$ such that $(u, N) = 1$. We denote this suborbital by $O(u, N)$ and corresponding suborbital graph $G(u, N)$ by $G_{u,N}$.

Theorem 3.1 (Edge condition).

$\frac{r}{s} \longrightarrow \frac{x}{y}$ is an edge in $G_{u,N}$ if and only if there exists an integer h_1 with $h_1 | h$, $h/h_1 | s$ and if $h = h_1 h_1'$ then either

(i) $x \equiv ur \pmod{h_1'}$, $y \equiv us \pmod{h_1' h}$, and $ry - sx = h_1'^2$, or
(ii) $x \equiv -ur \pmod{h_1'}$, $y \equiv -us \pmod{h_1' h}$, and $ry - sx = -h_1'^2$.

Proof:

Let $\frac{r}{s} \longrightarrow \frac{x}{y} \in G_{u,N}$, then there exists a transformation $\begin{pmatrix} a & b/h \\ ch & d \end{pmatrix}$ in $\Gamma_B(N)$ which sends $\frac{1}{0}$ to $\frac{r}{s}$ and $\frac{u}{N}$ to $\frac{x}{y}$, therefore $\frac{a}{ch} = \frac{r}{s}$ and $\frac{au+bN/h}{cuh+dN} = \frac{au+bh}{cuh+dN} = \frac{x}{y}$. Let $(a, h) = h_1$, and let $a = a_1 h_1$, $h = h_1 h_1'$.

Thus $(a_1, h_1') = 1$ and $\frac{a}{ch} = \frac{a_1}{ch_1'}$. Since the determinant $ad - bc = 1$, $(a, c) = 1$ follows $(a_1, ch_1') = 1$. Then we have $a_1 = r$ and $ch_1' = s$. The last equation leads to $h/h_1 = h_1'|s$. We know that $(u, N) = 1$, thus $(u, N/h) = 1$, that is, $(u, h) = 1$. Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant 1, then using Remark 2.1 we see that $(au + bh, cu + dh) = 1$. Hence we will have the following matrix equation:

$$\begin{pmatrix} a & b/h \\ ch & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} a & au + bh \\ ch & cuh + dN \end{pmatrix} = \begin{pmatrix} a_1h_1 & h_1(a_1u + bh_1') \\ ch_1h_1' & h_1h_1'(cu + dh) \end{pmatrix} = \begin{pmatrix} (-1)^i h_1 r & (-1)^j h_1 x \\ (-1)^i h_1 s & (-1)^j h_1 y \end{pmatrix}, \tag{2}$$

where $i, j = 0, 1$. If $i = j = 0$ then $a_1h_1 = rh_1$, $h_1(a_1u + bh_1') = h_1x$, $ch_1h_1' = h_1s$, $h_1h_1'(cu + dh) = h_1y$. That is, $x = ur + bh_1'$ and $y = us + dh_1'h$. Hence it is obtained that $x \equiv ur \pmod{h_1'}$ and $y \equiv us \pmod{h_1'h}$. Taking determinants in Equation 2 we see that $ry - sx = h_1'^2$, so (i) holds. Similarly if $i = 1$ and $j = 0$, we obtain (ii). If $i = j = 1$, then again (i) holds. If, finally, $i = 0$ and $j = 1$, then (ii) holds.

Conversely, if (i) holds, then there exist integers b, d such that $x = ur + bh_1'$ and $y = us + dh_1'h$. Let $s = s_1h_1'$. Then the element $\begin{pmatrix} rh_1 & b/h \\ sh_1 & d \end{pmatrix}$ belongs to $\Gamma_B(N)$ and sends ∞ to $\frac{r}{s}$ and $\frac{u}{N}$ to $\frac{x}{y}$. For (ii), the result is obtained in a similar way. ∎

Corollary 3.2.

Let $uv \equiv -1 \pmod{h_1'h}$, then the suborbital graph $G_{u,N}$ is paired with $G_{v,N}$.

Proof:

We will observe that $\frac{r}{s} \to \frac{x}{y}$ in $G_{u,N}$ if and only if $\frac{x}{y} \to \frac{r}{s}$ in $G_{v,N}$. Since $\frac{r}{s} \to \frac{x}{y}$ in $G_{u,N}$, using Theorem 3.1, we have that there exists an integer h_1 with $h_1|h$, $h/h_1|s$ and $h = h_1h_1'$ such that either $x \equiv ur \pmod{h_1'}$, $y \equiv us \pmod{h_1'h}$, and $ry - sx = h_1'^2$, or $x \equiv -ur \pmod{h_1'}$, $y \equiv -us \pmod{h_1'h}$, and $ry - sx = -h_1'^2$.

Suppose that the former holds, then $xs - ry = -h_1'^2$ and $vx \equiv ruv \pmod{h_1'}$, $vy \equiv suv \pmod{h_1'h}$. Since $uv \equiv -1 \pmod{h_1'h}$, we have $xs - yr = -h_1'^2$ and $r \equiv -rx \pmod{h_1'}$, $s \equiv -vy \pmod{h_1'h}$, that is, $\frac{x}{y} \to \frac{r}{s}$ in $G_{v,N}$. ∎

Corollary 3.3.

$G_{u,N}$ is self-paired if and only if $u^2 \equiv -1 \pmod{h}$.

Proof:

Suppose $G_{u,N}$ is self paired. So the pair $(\infty, u/N)$ is sent to $(u/N, \infty)$ by $\Gamma_B(N)$. It is easily seen that such elements of $\Gamma_B(N)$ must be of the form $\begin{pmatrix} u & b/h \\ N & -u \end{pmatrix}$, where the determinant is 1. Therefore $u^2 \equiv -1 \pmod{h}$.

Conversely, let $u^2 \equiv -1 \pmod h$. Since $u^2 \equiv -1 \pmod h$, then there exists an integer b such that $-u^2 + bh = 1$. Therefore the element $\begin{pmatrix} u & b/h \\ N & -u \end{pmatrix}$ is in $\Gamma_B(N)$ and satisfies the required properties. ■

4. Properties of The Graphs $F_{u,N}$ and $G_{u,N}$

Since the action of $\Gamma_B(N)$ on $\hat{\mathbb{Q}}$ is transitive, $\Gamma_B(N)$ permutes the blocks transitively; so the subgraphs are all isomorphic. Hence it is sufficient to study only one block. On the other hand, it is clear that each non-trivial suborbital graph contains a pair $(\infty, \frac{u}{N})$ for some $\frac{u}{N} \in \hat{\mathbb{Q}}$ where $(u, N) = 1$. Therefore, we study on the following case: We denote by $F_{u,N}$ the subgraph of $G_{u,N}$ such that its vertices are in the block $[\infty]$.

Theorem 4.1.

$\frac{r}{s} \to \frac{x}{y}$ in $F_{u,N}$ if and only if $ry - sx = 1$ or $ry - sx = -1$.

Proof:

From Equation 1, it is easily seen that $[\infty] = \left\{\frac{x}{y} \,:\, y \equiv 0 \pmod{h^2}\right\}$. Since $\frac{r}{s}, \frac{x}{y} \in [\infty]$, the proof is obvious by Theorem 3.1. ■

Theorem 4.2.

$\Gamma_C^0(N)$ permutes the vertices and edges of $F_{u,N}$ transitively.

Proof:

Let $\frac{k}{l}, \frac{m}{n} \in [\infty]$ be two vertices of the graph $F_{u,N}$. Since $\Gamma_B(N)$ acts transitively on $\hat{\mathbb{Q}}$, there exists an element $T = \begin{pmatrix} a & b/h \\ ch & d \end{pmatrix} \in \Gamma_B(N)$ such that

$$\begin{pmatrix} a & b/h \\ ch & d \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} m \\ n \end{pmatrix}.$$

This yields $ckh + dl = n$. Since $n - dl \equiv 0 \pmod{h^2}$ we obtain $ckh \equiv 0 \pmod{h^2}$. We know that $(k, h) = 1$, therefore $c \equiv 0 \pmod h$. Thus we have $T \in \Gamma_C^0(N)$.

Let $x_1 \longrightarrow y_1$ and $x_2 \longrightarrow y_2$ be two edges in $F_{u,N}$. Since $\Gamma_B(N)$ acts transitively on the edges of $F_{u,N}$, there exists an element $S = \begin{pmatrix} p & r/h \\ qh & s \end{pmatrix} \in \Gamma_B(N)$ such that $S(x_1 \longrightarrow y_1) = S(x_2 \longrightarrow y_2)$. Thus we have $S(x_1) = S(x_2)$ and $S(y_1) = S(y_2)$, giving

$$\begin{pmatrix} p & r/h \\ qh & s \end{pmatrix} \begin{pmatrix} p_1 \\ q_1 \end{pmatrix} = \begin{pmatrix} p & r/h \\ qh & s \end{pmatrix} \begin{pmatrix} p_2 \\ q_2 \end{pmatrix}$$

and

$$\begin{pmatrix} p & r/h \\ qh & s \end{pmatrix} \begin{pmatrix} r_1 \\ s_1 \end{pmatrix} = \begin{pmatrix} p & r/h \\ qh & s \end{pmatrix} \begin{pmatrix} r_2 \\ s_2 \end{pmatrix}.$$

From second equation above, we obtain $q \equiv 0 \pmod{h}$. Thus, $S \in \Gamma_C^0(N)$. ■

Theorem 4.3.

If $F_{u,N}$ is self-paired, then the corresponding map to any circuit in $F_{u,N}$ is an elliptic element of order 2 in $\Gamma_C^0(N)$.

Proof:

Since $F_{u,N}$ is self-paired, $u^2 \equiv -1 \pmod{h}$. Therefore, there exists an element $k \in \mathbb{Z}$ such that $-u^2 + kh = 1$. Then we obtain

$$A = \begin{pmatrix} u & -k/h \\ N & -u \end{pmatrix} \in \Gamma_C^0(N).$$

Since $A^2 = I$, A is of order 2. ■

Theorem 4.4.

Let $\frac{a}{b} \rightarrow \frac{c}{d} \rightarrow \frac{e}{f} \rightarrow \frac{a}{b}$ be a triangle in $F_{u,N}$. Then there exists a unique elliptic element $T \in \Gamma_C^0(N)$ of order 3 such that $T(\frac{a}{b}) = \frac{c}{d}$, $T(\frac{c}{d}) = \frac{e}{f}$, $T(\frac{e}{f}) = \frac{a}{b}$.

Proof:

Since $\frac{a}{b} \rightarrow \frac{c}{d} \in F_{u,N}$, by Theorem 4.1, we have $ad - bc = \mp 1$ and for all $\Phi \in \Gamma_C^0(N)$, $\frac{a_1}{b_1} = \Phi(\frac{a}{b}) \rightarrow \Phi(\frac{c}{d}) = \frac{c_1}{d_1}$, $a_1 d_1 - b_1 c_1 = \mp 1$. By Theorem 4.2, there exists an element $K \in \Gamma_C^0(N)$ such that $K(\frac{a}{b}) = \infty$ and $K(\frac{c}{d}) = \frac{u}{N}$. Since $\frac{c_1}{d_1} \rightarrow K(\frac{e}{f}) = \frac{e_1}{f_1}$ and $c_1 f_1 - e_1 d_1 = \mp 1$, we obtain $\frac{e_1}{f_1} = \frac{u \mp 1}{1}$, that is, K transforms the triangle $\frac{a}{b} \rightarrow \frac{c}{d} \rightarrow \frac{e}{f} \rightarrow \frac{a}{b}$ to the triangle $\infty \rightarrow \frac{u}{N} \rightarrow \frac{u \mp 1}{N} \rightarrow \infty$. Then

$$S = \begin{pmatrix} -u & \dfrac{u^2 \mp u + 1}{N} \\ -N & u \mp 1 \end{pmatrix}$$

is an elliptic element of order 3 in $\Gamma_C^0(N)$. If we set $T = K^{-1} S K$, then $T \in \Gamma_C^0(N)$ is an elliptic element of order 3. ■

5. Conclusion

Actually, the suborbital graphs of the normalizer has been studied under restrictions by Keskin (2006), Keskin and Demirturk (2009), Köroglu et al. (2017), Güler et al. (2011), and Kader (2017). It is known that using different subgroups for the imprimitive action, the characters of the subgraphs are changed (Jones et al. (1991)). The purpose of our work is related to these choices. We recall that Akbaş found certain relationship between the lengths of circuits in suborbital graphs of the modular group and periods of elliptic elements of the group $\Gamma_0(N)$. He used the relation $\Gamma_\infty < \Gamma_0(N) < \Gamma$ for imprimitive action as in Jones et al. (1991). This is an important result, taking into account that the orders of the elliptic elements are one of the invariants of the group. Hence, suborbital graphs can be viewed as a tool to investigate permutation groups in terms of combinatorics. Then the authors changed the relation as $\Gamma_\infty < \Gamma_1(N) < \Gamma$ and found aforementioned relationship between the newly constructed subgraphs and the group $\Gamma_1(N)$. Hence, one can apply this method to other finitely generated Fuchsian groups. The modular group has a wealth of subgroups, among which the congruence subgroups are perhaps the most important and the certainly the best known. The normalizers of the congruence subgroups have also special interest because of their importance in number theory and group theory. One of the most remarkable of them is the normalizer of $\Gamma_0(N)$ in $PSL(2, \mathbb{R})$ as mentioned in introduction part. Akbaş and Singerman describe some important subgroups of $\Gamma_B(N)$ which will enable us to understand its structure. One of them is the Atkin-Lehner group $\Gamma_W(N)$ (Köroglu et al. (2017)). Another is the group $\Gamma_C(N)$ which is denoted by the set of transformations of the normalizer $\Gamma_B(N)$ where determinant of matrix equals to 1. In this study, $\Gamma_C^0(N)$ is defined as a congruence subgroup of $\Gamma_B(N)$ and then is examined by orbital graphs. In order to calculate the order of elliptic elements, this paper utilizes the Fuchsian group action on the upper half plane and their graphs properties.

Acknowledgement:

The first author would like to thank TUBITAK (The Scientific and Technological Research Council of Turkey) for their financial supports during her doctorate studies.

REFERENCES

Akbaş, M. (1989). *The Normalizer of Modular Subgroups*, PhD Thesis, University of Southampton.

Akbaş, M. and Singerman, D. (2001). The normalizer of $\Gamma_0(N)$ in $PSL(2, R)$, Glasgow Math., Vol. 32, pp. 317–327.

Biggs, N.L. and White, A.T. (1979). *Permutation groups and combinatorial structures*, London Mathematical Society Lecture Note Series, 33rd edn. CUP, Cambridge.

Chua, K.S. and Lang, M.L. (2004). Congruence subgroups associated to the monster, Experiment. Math., Vol. 13, No. 3, pp. 343–360.

Conway, J.H. and Norton, S.P. (1977). Monstrous Moonshine, Bull. London Math. Soc., Vol. 11, pp. 308–339.

Güler, B.Ö., Beşenk, M., Değer, A.H., and Kader, S. (2011). Elliptic elements and circuits in suborbital graphs, Hacet. J. Math. Stat., Vol. 40, No. 2, pp. 203–210.

Jones, G.A., Singerman, D. and Wicks, K. (1991). The modular group and generalized Farey graphs, London Math. Soc., Vol. 160, pp. 316–338.

Kader, S. (2017). Circuits in suborbital graphs for the normalizer, Graphs and Combinatorics, Vol. 33, No. 6, pp. 1531–1542.

Keskin, R. (2006). Suborbital graphs for the normalizer of $\Gamma_0(m)$, European J Combin., Vol. 27, No. 2, pp. 193–206.

Keskin, R. and Demirturk, B. (2009). On suborbital graphs for the normalizer of $\Gamma_0(N)$, Electron J Combin., Vol. 16, No. 1, pp. 116–133.

Köroglu, T., Güler, B.Ö. and Şanlı, Z. (2017). Suborbital graphs for the Atkin-Lehner group, Turk J Math., Vol. 41, pp. 235–243.

Lehner, J. and Newman, M. (1964). Weierstrass points of $\Gamma_0(N)$, Annals of Mathematics, Vol. 79, No. 2, pp. 360–368.

Schoeneberg, B. (1974). *Elliptic Modular Functions*, Springer Verlag.

Sims, C.C. (1967). Graphs and finite permutation groups, Math. Z., Vol. 95, pp. 76–86.