NORMALIZERS OF THE CONGRUENCE SUBGROUPS OF THE HECKE GROUP \(G_5\) II

MONG-LUNG LANG AND SER-PEOW TAN

(Communicated by Ronald M. Solomon)

Abstract. Let \(\lambda = 2 \cos(\pi/5)\). Let \((\tau)\) be an ideal of \(\mathbb{Z}[\lambda]\) and let \((\tau_0)\) be the maximal ideal of \(\mathbb{Z}[\lambda]\) such that \((\tau_0^2) \subseteq (\tau)\). Then \(N(G_0(\tau)) \leq G_0(\tau_0)\). In particular, if \(\tau\) is square free, then \(G_0(\tau)\) is self-normalized in \(PSL_2(\mathbb{R})\).

1. Introduction

In this paper, we continue our study into the extent to which properties of the modular group hold for the Hecke groups; see [CLLT], [LLT1], [LLT2], [LT1], [LT2] for some previous results. We are in particular interested in the Hecke group \(G_5\) which we denote by \(G\) and its congruence subgroups \(G_0(\tau)\). Our main results are:

(i) **Theorem 8.** Let \(\lambda = 2 \cos(\pi/5) = (1 + \sqrt{5})/2\). Let \((\tau)\) be an ideal of \(\mathbb{Z}[\lambda]\) and let \((\tau_0)\) be the maximal ideal of \(\mathbb{Z}[\lambda]\) such that \((\tau_0^2) \subseteq (\tau)\). Then \(N(G_0(\tau)) \leq G_0(\tau_0)\).

(ii) **Main Theorem.** Let \((\tau)\) be an ideal of \(\mathbb{Z}[\lambda]\). Suppose that \(\tau\) is square free. Then \(G_0(\tau)\) is self-normalized in \(PSL_2(\mathbb{R})\).

This contrasts with the cases of the congruence subgroups of the modular group \(\Gamma\) which admit Atkin-Lehner involutions, so have strictly larger normalizers ([AL], [C], [LN]).

We recall the following definitions, notation and results. For \(q \geq 4\), the Hecke groups \(G_q\) are the (discrete) subgroups \(\langle w, u_q \rangle\) of \(PSL_2(\mathbb{Z}[\lambda_q])\), where \(\lambda_q = 2 \cos(\pi/q)\) and

\[
    w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad u_q = \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix}.
\]

When \(q = 3\), we recover the modular group \(\Gamma\) so the above can be thought of as a natural generalization of \(\Gamma\). Alternatively, we can interpret the generalization as \(G_q\) being maximal discrete subgroups whose entries are in some extension of \(\mathbb{Z}\). Finally, we have the geometric interpretation: \(\Gamma\) is a \((2, 3, \infty)\) triangle group and the Hecke group \(G_q\) is a \((2, q, \infty)\) triangle group.
Let \( \mathcal{A} \) be an ideal of \( \mathbb{Z}[\lambda_q] \). We define

\[
G_0(\mathcal{A}) = \{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_q \mid c \in \mathcal{A} \}.
\]

Again, this is a natural generalization of the congruence subgroups \( \Gamma_0(n) \) of \( \Gamma \).

Recall that \( G_q \) is commensurable with \( \text{PSL}_2(\mathbb{Z}) \) if and only if \( q = 4 \) or 6. The elements of such groups are completely known; see [P], for example. Suppose \( G_q \) is not commensurable with \( \text{PSL}_2(\mathbb{Z}) \). By the results of Leutbecher, [L1], [L2], \( \mathbb{Q}(\lambda) \cup \{\infty\} \) is the set of cusps of \( G_q \) if and only if \( q = 5 \). Also, 5 is the only \( q \) other than 4, 6 for which \( \mathbb{Q}(\lambda) \) is a quadratic field. For all other \( q \)'s, the degree is \( > 2 \). As a consequence, \( q = 5 \) is the next most workable and interesting \( q \).

Some of the classical results on the modular group can be generalized to \( G = G_5 \) ([CLLT], [LLT2]). From now on \( q = 5 \), so \( \lambda_q = (1 + \sqrt{5})/2 \).

The main facts used in the proof of our main theorem are:

(a) \( \mathbb{Z}[\lambda] \) is a principal ideal domain.

(b) The set of cusps of \( G \) is \( \mathbb{Q}(\lambda) \cup \{\infty\} \) ([L1], [L2]). Furthermore, if \( x \in \mathbb{Q}(\lambda) \) is a cusp, \( x \) has a unique reduced form \( x = \frac{a}{b} \) (\( \mathbb{R} \)). By definition, this means that \( a, b \in \mathbb{Z}[\lambda] \) with \( b > 0 \) and there exists \( c, d \in \mathbb{Z}[\lambda] \) such that \( \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G \).

Clearly, \( (a, b) = 1 \) so that if \( x = \frac{a}{b} \) with \( (a', b') = 1 \), then \( a = \mu a' \), \( b = \mu b' \) where \( \mu \) is a unit in \( \mathbb{Z}[\lambda] \).

(c) (Proposition 6 of [LLT1]) Suppose \( x_i, x_j \) are members in \( \mathbb{Q}(\lambda) \cup \{\infty\} \) with reduced form \( a_i/b_i \) and \( a_j/b_j \) respectively, and suppose that \( x_i < x_j \). Then the following statements are equivalent:

(i) \( \begin{pmatrix} a_j & a_i \\ b_j & b_i \end{pmatrix} \in G \);

(ii) \( (x_i, x_j) \) is an even line, that is, it is the image of the complete hyperbolic geodesic with ends at 0 and \( \infty \) under the action of some \( \mathcal{A} \in G \);

(iii) \( a_j b_i - a_i b_j = 1 \).

(d) The even lines give a tessellation of \( \mathbb{H} \) (the upper half plane) into ideal pentagons, that is, hyperbolic 5-gons whose vertex angles are all zero ([K], [LLT1]).

(e) \( \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G \) if and only if \( b = m\lambda, m \in \mathbb{Z} \) (\( \mathbb{R} \)). Similarly, \( \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in G \) if and only if \( c = n\lambda, n \in \mathbb{Z} \). (This result is well known, a proof of this result can be found in Corollary 5 of [LLT1].)

The rest of the paper is organized as follows. In Sections 2 and 3, we study the reduced forms of \( \mathbb{Q}(\lambda) \). Facts about reduced forms that are useful in the determination of \( N(G_0(\tau)) \) are given in Corollary 3 and Lemma 4. The next two sections are devoted to the reduction of the supergroups of \( N(G_0(\tau)) \) (a group \( S \) is a supergroup of \( N(G_0(\tau)) \) if \( N(G_0(\tau)) \) is a subgroup of \( S \)). In Section 6, we complete the proof of our main theorem.

Throughout the paper, \( \lambda = 2\cos(\pi/5) \), \( (\tau) \) is an ideal of \( \mathbb{Z}[\lambda] \), and \( N(G_0(\tau)) \) is the normalizer of \( G_0(\tau) \) in \( \text{PSL}_2(\mathbb{R}) \).
2. Reduced forms

Recall first that $a/b$ is a reduced form if

(i) $a, b \in \mathbb{Z}[\lambda]$ with $b > 0$,

(ii) there exist $c, d \in \mathbb{Z}[\lambda]$ such that \[
\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G.
\]

Let $x/y = (x_1 + x_2 \lambda)/(y_1 + y_2 \lambda) > 0$ be a reduced form. Since $\lambda^2 = \lambda + 1$, we may assume that $x_1, x_2, y_1, y_2$ are nonnegative rational integers (LLT1).

The following lemmas must be well known among the experts. For the reader’s convenience, the proof is included.

Lemma 1. Let $x/y > 0$ ($y > 0$) be a reduced form. Then $y \in \mathbb{N}$ if and only if $y = 1$.

Proof. Let $a/b$ and $c/d$ ($0 \leq a/b < c/d$) be reduced forms such that $(a/b, c/d)$ is an even line. The vertices of the ideal pentagon lying below $(a/b, c/d)$ are given by

\[
\left\{ (a/b, (\lambda a + c)/(\lambda b + d), \lambda(a + c)/(\lambda(b + d)), (a + \lambda c)/(b + \lambda d), c/d \right\}.
\]

Since $x/y$ is a reduced form, $x/y$ is a vertex of an ideal pentagon $I$. Suppose that $I$ lies below $(a/b, c/d)$. As $x/y \notin \{0, \infty\}$, we may assume that

\[
x/y \in \left\{ (\lambda a + c)/(\lambda b + d), \lambda(a + c)/(\lambda(b + d)), (a + \lambda c)/(b + \lambda d) \right\}.
\]

Let $a = a_1 + a_2 \lambda$, $b = b_1 + b_2 \lambda$, $c = c_1 + c_2 \lambda$, and $d = d_1 + d_2 \lambda$. Note that we may assume that $a_1, a_2, b_1, b_2, c_1, c_2, d_1,$ and $d_2$ are nonnegative rational integers.

Suppose that $y \in \mathbb{N}$.

Case 1. $x/y = (\lambda a + c)/(\lambda b + d)$. It follows that $b_1 + b_2 + d_2 = 0$ and $b_2 + d_1 = y$. Hence $b_1 = b_2 = d_2 = 0$. As a consequence, $b = 0$ and $d = y$. This is a contradiction ($0 \leq a/b < c/d$).

Case 2. $x/y = (a + \lambda c)/(b + \lambda d)$. It follows that $b_2 + d_1 + d_2 = 0$ and $b_1 + d_2 = y$. Hence $b_2 = d_1 = d_2 = 0$. As a consequence, $b = y$, $d = 0$, and $(a/b, c/d) = (a/y, 1/0)$. By Proposition 6 (iii) of [LLT1], $y = 1$.

Case 3. $x/y = \lambda(a + c)/(\lambda(b + d))$. It follows that $b_1 + b_2 + d_1 + d_2 = 0$ and $b_2 + d_2 = y$ is an integer. It follows that $b_1 = b_2 = d_1 = d_2 = 0$. This is a contradiction.

This completes the proof of the lemma.

Lemma 2. Let $m$ be a positive rational integer. Then the only reduced forms between 0 and $\lambda$ with denominator $m\lambda$ are $1/m\lambda$ and $\lambda - 1/m\lambda = (m\lambda^2 - 1)/m\lambda = (m\lambda + (m - 1))/m\lambda$.

Proof. Let $0 < x/m\lambda < \lambda$ be a reduced form. Similar to Lemma 1, we may assume that

\[
x/y \in \{ (\lambda a + c)/(\lambda b + d), \lambda(a + c)/(\lambda(b + d)), (a + \lambda c)/(b + \lambda d) \}
\]

for some even line $(a/b, c/d)$. Let $a = a_1 + a_2 \lambda$, $b = b_1 + b_2 \lambda$, $c = c_1 + c_2 \lambda$, and $d = d_1 + d_2 \lambda$. Note that we may assume that $a_1, a_2, b_1, b_2, c_1, c_2, d_1,$ and $d_2$ are nonnegative rational integers.

Suppose that $x/m\lambda = (\lambda a + c)/(\lambda b + d)$. It follows that $b_1 + b_2 + d_2 = m$ and $b_2 + d_1 = 0$. Hence $b_2 = d_1 = 0$. This implies that $b = b_1 \in \mathbb{N}$. Since $a/b$ is a reduced form, $b = b_1 = 1$ (Lemma 1). By Corollary 5 of [LLT1], $a = k\lambda$ for some
$k \in \mathbb{Z}$. Since $0 \leq a/b < \lambda$, $a = 0$. It follows that $d = (m - 1)\lambda$. By Proposition 6 (iii) of \cite{LT1}, $c = 1$. Hence $x/m\lambda = (\lambda a + c)/(\lambda b + d) = 1/m\lambda$.

Suppose that $x/m\lambda = (a + \lambda c)/(b + \lambda d)$. It follows that $b_2 + d_1 + d_2 = m$ and $b_1 + d_2 = 0$. Hence $b_1 = d_2 = 0$. This implies that $d = d_1 \in \mathbb{N} \cup \{0\}$. Since $c/d$ is a reduced form, $d = d_1 = 1$ (Lemma 1). Applying Corollary 5 of \cite{LT1}, $c = 0$ or $k\lambda$, where $k \in \mathbb{Z}$. Since $0 \leq a/b < c/d \leq \lambda$, $c = \lambda$. Since $c/d = 1/k, b_2 = (m - 1)\lambda$. By Proposition 6 (iii) of \cite{LT1}, $a = -1 + (m - 1)\lambda^2$. Hence $x/m\lambda = (\lambda a + c)/(\lambda b + d) = (m\lambda^2 - 1)/m\lambda$.

Suppose that $x/m\lambda = \lambda(a + c)/\lambda(b + d)$. It follows that $b_2 = d_2 = 0$. This implies that $b = b_1 \in \mathbb{N}$, $d = d_1 \in \mathbb{N} \cup \{0\}$, and $b_1 + d_1 = m$. By Lemma 1, $b = b_1 = 1$ and $d = d_1 = 0$. It follows that $m = 1$. Since $1/\lambda$ and $\lambda/\lambda = \lambda - 1/\lambda$ are the only reduced forms between 0 and $\lambda$ with denominator $\lambda$, the lemma holds.

In summary, the only reduced forms between 0 and $\lambda$ with denominator $m\lambda$ are $1/m\lambda$ and $(m\lambda^2 - 1)/m\lambda$.

Applying Lemma 2, we have the following.

**Corollary 3.** Let $m$ be a positive rational integer. Then $x/m\lambda$ is a reduced form if and only if $x = km\lambda^2 \pm 1$, where $k \in \mathbb{Z}$. Further, if $x/m\lambda$ and $y/m\lambda$ are reduced forms such that $x/m\lambda - y/m\lambda = 2/m\lambda$, then $x/m\lambda = k\lambda + 1/m\lambda$ and $y/m\lambda = k\lambda - 1/m\lambda$.

**Proof.** By Lemma 2, the reduced forms with denominator $m\lambda$ are given by $k\lambda \pm (1/m\lambda)$. This completes the proof of the corollary.

### 3. Pseudo-Euclidean Algorithm and Reduced Forms

Let $a, b \in \mathbb{Z}[\lambda] \setminus \{0\}$. There exists a unique rational integer $q$ such that

(i) $a = (q\lambda)b + r,
(ii) |r| = |a - (q\lambda)b| \leq |a - (x\lambda)b|$ for all $x \in \mathbb{Z}.

We call such a division algorithm *pseudo-Euclidean* (see \cite{R} for more details). In terms of matrices, the above can be written as

$$
\begin{pmatrix}
1 & -q\lambda \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
a \\
b
\end{pmatrix} = 
\begin{pmatrix}
r
\end{pmatrix}.
$$

Note that \(\begin{pmatrix}
1 & -q\lambda \\
0 & 1
\end{pmatrix} \in G\). Let $n \in \mathbb{N}$. Applying the pseudo-Euclidean algorithm repeatedly, one has,

\[
\begin{align*}
n &= (q_1\lambda)1 + r_1, \\
1 &= (q_2\lambda)r_1 + r_2, \\
r_1 &= (q_2\lambda)r_2 + r_3, \\
&\vdots \\
r_k &= (q_{k+1}\lambda)r_{k+1} + r_{k+2}, \\
r_{k+1} &= (q_{k+2}\lambda)r_{k+2} + 0.
\end{align*}
\]
The finiteness of the algorithm is governed by the fact that the set of cusps of $G$ is \( \mathbb{Q}(\lambda) \cup \{\infty\} \). Note that in terms of matrices, the above can be written as

\[
\begin{pmatrix} n \\ 1 \end{pmatrix} = A \begin{pmatrix} r_{k+2} \\ 0 \end{pmatrix},
\]

where $A \in G$. It is clear that

\[ \gcd(n, 1) = \gcd(1, r_1) = \cdots = \gcd(r_{k+1}, r_{k+2}) = r_{k+2} \]

is a unit. As

(i) $|r_{k+2}| < 1$,

(ii) $\lambda$ is a primitive unit,

there exists $e(n) \in \mathbb{N}$ such that

\[ |r_{k+2}| = \lambda^{-e(n)}. \]

Multiplying (3.1) by $\lambda^{e(n)}$, one has

\[
\begin{pmatrix} n \lambda^{e(n)} \\ \lambda^{e(n)} \end{pmatrix} = A \begin{pmatrix} \pm 1 \\ 0 \end{pmatrix}.
\]

Since $A \in G$ and $\pm 1/0$ is a reduced form, we conclude that $n\lambda^{e(n)}/\lambda^{e(n)}$ is the reduced form of $n$. Consequently, $-\lambda^{e(n)}/n\lambda^{e(n)}$ is the reduced form of $-1/n$. Note that since the reduced form is unique, $e(n)$ is the unique rational integer such that $-\lambda^{e(n)}/n\lambda^{e(n)}$ and $n\lambda^{e(n)}/\lambda^{e(n)}$ are reduced forms.

**Lemma 4.** Let $m \geq 1$ and $x > 1$ be rational integers. Then there exists $f \in \mathbb{N}$ such that $e(mx^{f+1}) > e(mx^f)$.

**Proof.** Let $s, t \in \mathbb{N} \cup \{0\}$. Applying the pseudo-Euclidean algorithm, one has

\[ mx^s = (qs)\lambda + r_s \]

and

\[ mx^t = (qt)\lambda + r_t. \]

Suppose that $r_s = r_t$. It follows that

\[ mx^s - mx^t = (qs - qt)\lambda. \]

As $\lambda$ is irrational, the above implies that $mx^s = mx^t$. Consequently, $r_s \neq r_t$ if and only if $s \neq t$. Therefore, $mx^s$ is not congruent to $mx^t$ modulo $\lambda$ if and only if $s \neq t$. This implies that

\[ \Omega = \{ mx^s \lambda^{e(mx^s)}/\lambda^{e(mx^s)} \mod \lambda : s \in \mathbb{N} \cup \{0\} \} \]

is infinite. Let

\[ mx^s \lambda^{e(mx^s)}/\lambda^{e(mx^s)} = k_s \lambda + mx^s \lambda^{e(mx^s)}/\lambda^{e(mx^s)} \mod \lambda, \]

where $k_s \in \mathbb{Z}$. It follows that

\[
\begin{pmatrix} 1 & -k_s \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} mx^s \lambda^{e(mx^s)} \\ \lambda^{e(mx^s)} \end{pmatrix} = \begin{pmatrix} mx^s \lambda^{e(mx^s)} - \lambda^{e(mx^s)}/k_s \lambda \\ \lambda^{e(mx^s)} \end{pmatrix}.
\]
As $mx^s x^{e(mx^s)} / x^{e(mx^s)}$ is in reduced form, (3.2) implies that
\[(mx^s x^{e(mx^s)} - x^{e(mx^s)}) / x^{e(mx^s)} = mx^s x^{e(mx^s)} / x^{e(mx^s)} \pmod{\lambda}\]
is also in reduced form. Hence every element in $\Omega$ is in reduced form. Since
(i) $\Omega$ is infinite,
(ii) there exist only finitely many cusps $u/v$ (in reduced form) in $[0, \lambda]$ such that $v \leq x^{e(m)}$,
there exists some $s$ such that
\[x^{e(mx^s)} > x^{e(m)}\].
Hence there exists some $f \in \mathbb{N}$ such that $e(mx^{f+1}) > e(mx^f)$. \(\square\)

4. First reduction

Throughout this section, $(\tau)$ is a nontrivial ideal of $\mathbb{Z}[[\lambda]]$ and $m$ is the smallest positive rational integer in $(\tau)$. Let $PGL_2^+(\mathbb{Q}(\lambda)) = \{ A \in PGL_2(\mathbb{Q}(\lambda)) : \det A > 0 \}$. A matrix $M$ in $PGL_2^+(\mathbb{Q}(\lambda))$ is said to be primitive if
(i) all the entries of $M$ are members of $\mathbb{Z}[\lambda]$,
(ii) the greatest common divisor of the entries of $M$ is 1.

Denote by $N(G_0(\tau))$ the normalizer of $G_0(\tau)$ in $PSL_2(\mathbb{R})$. The purpose of this section is to show that every element in $N(G_0(\tau))$ is of the form $\pi A'$, where $\pi \in \mathbb{Q}(\lambda)^{1/2} = \{ z \in \mathbb{R} : z^2 \in \mathbb{Q}(\lambda) \}$ and $A' \in PGL_2^+(\mathbb{Q}(\lambda))$ is primitive.

For any
\[A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N(G_0(\tau)),\]
we have
\begin{align*}
(4.1) & \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - ac\lambda & a^2\lambda \\ -c^2\lambda & 1 + ac\lambda \end{pmatrix} \in G_0(\tau), \\
(4.2) & \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 + dc\lambda & d^2\lambda \\ -c^2\lambda & 1 - dc\lambda \end{pmatrix} \in G_0(\tau), \\
(4.3) & \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ m\lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 + bdm\lambda & -b^2m\lambda \\ d^2m\lambda & 1 - bdm\lambda \end{pmatrix} \in G_0(\tau), \\
(4.4) & \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ m\lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 - abm\lambda & -b^2m\lambda \\ a^2m\lambda & 1 + abm\lambda \end{pmatrix} \in G_0(\tau).
\end{align*}

Case 1. Suppose $c = 0$. By (4.1), we have $a = \pm \sqrt{m^2}$ and $d = \pm 1/\sqrt{m^2}$ ($ad = 1$),
where $m \in \mathbb{Z}[\lambda]$. By (4.4), $abm \in \mathbb{Z}[\lambda]$. Hence $b = \pm n_3/m\sqrt{n_2}$, where $n_3 \in \mathbb{Z}[\lambda]$. As a consequence,
\[A = \pm \begin{pmatrix} \sqrt{m^2} & n_3/m\sqrt{n_2} \\ 0 & 1/\sqrt{n_2} \end{pmatrix}.\]
It follows that $A = \pi A'$, where $\pi \in \mathbb{Q}(\lambda)^{1/2} = \{ z \in \mathbb{R} : z^2 \in \mathbb{Q}(\lambda) \}$ and $A' \in PGL_2^+(\mathbb{Q}(\lambda))$ is primitive.
Case 2. Suppose \( c \neq 0 \). By (4.1), \( c = \pm \sqrt{tn_1} \), where \( n_1 \in \mathbb{Z}[\lambda] \). Since \( 1 - ac \lambda \in \mathbb{Z}[\lambda] \), \( a = \pm n_3/\sqrt{tn_1} \), where \( n_3 \in \mathbb{Z}[\lambda] \). By (4.2), \( 1 - dc \lambda \in \mathbb{Z}[\lambda] \). Hence \( d = \pm n_4/\sqrt{tn_1} \), where \( n_4 \in \mathbb{Z}[\lambda] \). Since the determinant of \( A \) is 1, we conclude that

\[
b = \pm (n_3 n_4 / \sqrt{tn_1} - 1) / \sqrt{tn_1}.
\]

Similar to Case 1, \( A = \pi A' \), where \( \pi \in \mathbb{Q}(\lambda)^{1/2} = \{ z \in \mathbb{R} : z^2 \in \mathbb{Q}(\lambda) \} \) and \( A' \in PGL_2^+(\mathbb{Q}(\lambda)) \) is primitive.

Remark. Applying the proof we presented in this section, one can show that every member of the normalizer of \( G_0 \) of \( G_q \), \( q \geq 4 \), is of the form \( A = \pi A' \), where \( \pi \in \mathbb{Q}(\lambda)^{1/2} = \{ z \in \mathbb{R} : z^2 \in \mathbb{Q}(\lambda) \} \) and \( A' \in PGL_2^+(\mathbb{Q}(\lambda)) \) is primitive.

5. Second reduction: \( N(G_0(\tau)) \leq G_5 \)

Throughout this section, \( m \) is the smallest positive rational integer in the nontrivial ideal \( (\) \) and \( A = A_0 \in N(G_0(\tau)) \), where \( A \in PGL_2^+(\mathbb{Q}(\lambda)) \) is primitive. The main purpose of this section is to show that \( A \) is a member of \( G = G_5 \).

For each

\[
A = \pi A' = \pi \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N(G_0(\tau)),
\]

let \( a'/c' \) be the reduced form of \( a/c \). Proposition 6 of \([\text{LLT1}]\) implies that \( G \) contains an element of the form

\[
B^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.
\]

It follows that

\[
u(A) = BA = \pi BA' = \pi \begin{pmatrix} x & y \\ 0 & z \end{pmatrix},
\]

where \( x, y, z \in \mathbb{Z}[\lambda] \). Note that since \( B \in G \) and \( A' \) is primitive, \( \gcd(x, y, z) = 1 \). Furthermore, since \( B \in G \) and \( A \in N(G_0(\tau)) \),

\[
u(A) \sigma u(A)^{-1} = BA \sigma (BA)^{-1} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in G
\]

for every \( \sigma \in G_0(\tau) \). In particular, \( r/t \) and \( s/u \) are in reduced form.

Lemma 5. \( x/z \) is a rational integer and \( m \) is a multiple of \( x/z \).

Proof. Let \( \sigma = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \). It follows by applying (5.1) that

\[
u(A) \sigma u(A)^{-1} = \begin{pmatrix} 1 & x \lambda / z \\ 0 & 1 \end{pmatrix} \in G.
\]

By Corollary 5 of \([\text{LLT1}]\), \( x/z \in \mathbb{Z} \). This completes the proof of the first part of the lemma. Let \( \sigma = \begin{pmatrix} 1 & m \lambda \\ 0 & 1 \end{pmatrix} \). It follows that

\[
u(A) \sigma u(A)^{-1} = \begin{pmatrix} 1 + m y \lambda / x & -m y^2 \lambda / x z \\ m z \lambda / x & 1 - m y \lambda / x \end{pmatrix} \in G.
\]
Hence $mz\lambda/x \in \mathbb{Z} \llbracket \lambda \rrbracket$. Since

(i) $mz\lambda/x \in \mathbb{Z} \llbracket \lambda \rrbracket$,
(ii) both $x/z$ and $m$ are rational integers,

$m$ is a multiple of $x/z$. This completes the proof of the lemma. 

Lemma 6. $z = \pm 1$.

Proof. Replacing $x$ by $-x$ if necessary, we may assume that $mz/x > 0$. By (5.2),

\[
(1 + my\lambda/x)/(mz\lambda/x) \quad \text{and} \quad (-1 + my\lambda/x)/(mz\lambda/x)
\]

are reduced forms (recall that the denominator of a reduced form is nonnegative). Note that

\[
(1 + my\lambda/x)/(mz\lambda/x) - (-1 + my\lambda/x)/(mz\lambda/x) = 2/(mz\lambda/x)
\]

By Corollary 3, we have

(i) $(1 + my\lambda/x)/(mz\lambda/x) = k\lambda + 1/(mz\lambda/x)$,
(ii) $(-1 + my\lambda/x)/(mz\lambda/x) = k\lambda - 1/(mz\lambda/x)$,

where $k \in \mathbb{Z}$. Hence $y = kz$. Using Lemma 5, we conclude that both $x$ and $y$ are multiples of $z$. Since $\gcd(x, y, z) = 1$, the above implies that $z = \pm 1$. 

Applying Lemmas 5 and 6 to $u(A)$, we have (replace $B$ by $-B$ if necessary)

\[
u(A) = BA = \pi BA' = \pi \begin{pmatrix} x & k\lambda \\ 0 & 1 \end{pmatrix},
\]

where $x, k \in \mathbb{Z}$. Multiplying $u(A)$ by

\[
\begin{pmatrix} 1 & -k\lambda \\ 0 & 1 \end{pmatrix} \in G,
\]

one has

\[
d(A) = \begin{pmatrix} 1 & -k\lambda \\ 0 & 1 \end{pmatrix} u(A) = \pi \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.
\]

Note that since $A \in N(G_0(\tau))$,

\[
d(A)\sigma d(A)^{-1} = \begin{pmatrix} r' & s' \\ t' & u' \end{pmatrix} \in G
\]

for every $\sigma$ in $G_0(\tau)$. In particular, $r'/t'$ and $s'/u'$ are reduced forms.

Lemma 7. Let $(\tau)$ be a nontrivial ideal of $\mathbb{Z} \llbracket \lambda \rrbracket$. Then $N(G_0(\tau)) \leq G = G_5$.

Proof. Let $A = \pi A' \in N(G_0(\tau))$, where $\pi \in \mathbb{Q}(\lambda)^{1/2}$ and $A' \in PGL_2^+(\mathbb{Q}(\lambda))$ is primitive. Since

(i) $d(A) = \pi \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$,

(ii) $A$ and $d(A)$ have the same determinant,

\[
det A = \pi^2 x.
\]

It follows that $det A' = x$. Since $x/z \in \mathbb{Z}$ (Lemma 5) and $z = \pm 1$ (Lemma 6), $x \in \mathbb{Z}$. As members in $PGL_2^+(\mathbb{Q}(\lambda))$ admit positive determinant, $det A' = x \in \mathbb{N}$. Suppose that $x \geq 2$. By Lemma 4, there exists some $f$ such that $e(mx^{f+1}) > e(mx^f)$ ($m$ is the smallest positive rational integer in $(\tau)$). Let $n = x^{f+1}$. Since $-\lambda^{e(mn)}/\lambda^{e(mn)} mn$ is in reduced form (Section 3), by Proposition 6 of [LTT], $G_0(\tau)$ has an element of the form

\[
\sigma = \begin{pmatrix} -\lambda^{e(mn)} \\ \lambda^{e(mn)} mn \end{pmatrix} \in G_0(\tau).
\]
By (5.3),
\[ d(A)d(A)^{-1} = \begin{pmatrix} -\lambda^e(mn) & \ast \\ \lambda^e(mn)mn/x & \ast \end{pmatrix} \in G. \]
It follows that
\[ -\lambda^e(mn)/(\lambda^e(mn)mn/x) \]
is in reduced form. This is a contradiction \((e(mn) = e(mx^f+1) > e(mx^f) = e(mn/x))\). Hence \(x = 1\). As a consequence,
\[ A = B^{-1} \begin{pmatrix} 1 & k\lambda \\ 0 & 1 \end{pmatrix} \in G. \]
Since \(1 = \det A = \pi^2 \det A' = \pi^2\) and \(\pi \in \mathbb{Q}(\lambda)^{1/2}\), we conclude that \(\pi = \pm 1\). Hence \(A = \pm A'\). Since \(A' \in G\), \(A = \pm A' \in G = G_5\). This implies that \(N(G_0(\tau)) \leq G = G_5\).

6. The main theorem

**Theorem 8.** Let \((\tau)\) be an ideal of \(\mathbb{Z}[\lambda]\) and let \((\tau_0)\) be the maximal ideal of \(\mathbb{Z}[\lambda]\) such that \((\tau^2_0) \subseteq (\tau)\). Then \(N(G_0(\tau)) \leq G_0(\tau_0)\).

**Proof.** Let \(A \in N(G_0(\tau))\). By Lemma 7, \(A \in G\). The theorem now follows by applying (4.1).

**Main Theorem.** Let \((\tau)\) be an ideal of \(\mathbb{Z}[\lambda]\). Suppose that \(\tau\) is square free. Then \(G_0(\tau)\) is self-normalized in \(\text{PSL}_2(\mathbb{R})\).

**Proof.** Since \(\tau\) is square free, \((\tau) = (\tau_0)\) in Theorem 8. This completes the proof of the theorem.

**References**


Department of Mathematics, National University of Singapore, Singapore 119260, Republic of Singapore

E-mail address: matlm1@math.nus.edu.sg

E-mail address: mattansp@nus.edu.sg