TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 302, Number 2, August 1987

THE NORMAL SUBGROUP STRUCTURE OF THE PICARD GROUP

BENJAMIN FINE AND MORRIS NEWMAN

ABSTRACT. The Picard group Γ is $PSL_2(Z[i])$, the group of linear fractional transformations with Gaussian integer coefficients. We examine the structure of the normal subgroups of Γ. In particular we give a complete classification of the normal subgroups for indices less than 60 and show that beyond this there are large gaps in the possible indices. This classification depends on the structure of the derived series. Finally we give examples of normal noncongruence subgroups.

1. Introduction. The Picard group Γ is $PSL_2(Z[i])$, the group of linear fractional transformations $z' = (az+b)/(cz+d)$ with $ad-bc = \pm 1$ and a, b, c, d Gaussian integers. Γ has been extensively studied both as an abstract group and in automorphic function theory [**1**, **3**, **8**]. In both its general structure and in the structure of its principal congruence subgroups, Γ has been shown to be similar to the modular group $M = PSL_2(Z)$ [**3**, **4**]. Recently Brunner, Lee, Frame and Wielenberg [**1**] developed an effective procedure for classifying the torsion-free subgroups of Γ. This classification was caried out for small indices using a computer search. Further Fine [**5**] has shown that for a nonfree Fuchsian group to be embedded in Γ, it must have a special intersection property with the modular group.

In this paper we examine properties of the normal subgroup and congruence subgroup lattice in Γ. In particular we give a complete classification of the normal subgroups for indices less than 60. Further if $d(n)$ represents the number of normal subgroups of index n in Γ, we show that $d(n) = 0$ for a wide collection of n's. Finally we show that a theorem of Wohlfahrt's concerning congruence subgroups in the modular group carries over with only minor modification to Γ. This is utilized to present examples of noncongruence subgroups.

2. The derived series of Γ. Our techniques rely heavily on the structure of the derived series. We first present some notation, terminology and necessary results.

For future reference we identify the following transformations:

$$a\colon z' = -1/z, \quad t\colon z' = z+1, \quad u\colon z' = z+i, \quad l\colon z' = -z.$$

It is known [**3**] that a presentation for Γ is given by

$$(1) \quad \Gamma = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (at)^3 = (ual)^3 = [t, u] = 1\rangle.$$

Received by the editors August 12, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20G20; Secondary 20H05, 20H10.
Key words and phrases. Picard group, congruence subgroup, derived series.

It was shown by Fine [**3**, p. 481] that Γ decomposes as a free product with amalgamation of the following form:

$$\Gamma = G_1 *_H G_2 \quad \text{with } G_1 = S_3 *_{Z_3} A_4, G_2 = S_3 *_{Z_2} D_2$$

and $H = PSL_2(Z)$. (S_3 is the symmetric group on three symbols, A_4 the alternating group on four symbols and D_2 the Klein 4-group.) This decomposition will play a role in the discussion of the congruence subgroups and also appears in the derived series.

The elements of Γ can also be considered as $\pm\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad - bc = 1$ and $a, b, c, d \in Z[i]$. If $\alpha \in Z[i]$ the *principal congruence subgroup* mod(α) denoted $\Gamma(\alpha)$ consists of those matrices

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod(\alpha)$$

elementwise. $\Gamma(\alpha) \triangleleft \Gamma$ and each principal congruence subgroup has finite index. A congruence subgroup is any subgroup of finite index containing a principal congruence subgroup.

Finally if $H \subset \Gamma$, $N(H)$ is the normal closure of H in Γ. $N(g_1, g_2, \ldots, g_k)$ denotes the normal closure of the subgroup generated by $\{g_1, g_2, \ldots, g_k\}$.

First we prove

THEOREM 1. (a) Γ' *has index* 4. *Further* $\Gamma' = H_1 *_H H_2$ *where*

$$H_1 \simeq H_2 = A_4 *_{Z_2} A_4 \quad \textit{and} \quad H = Z_3 * Z_3.$$

(b) Γ'' *has index* 12. *Further* $\Gamma'' = K_1 *_K K_2$ *where*

$$K_1 \simeq K_2 = D_2 * D_2 \quad \textit{and} \quad K = Z * Z.$$

(c) Γ''' *has index* 768. Γ''' *is an HNN group whose base is a tree product of free groups each of rank* 9.

(d) *For* $n > 3$, $|\Gamma : \Gamma^{(n)}| = \infty$.

PROOF. The proof involves several lengthy but straightforward computations involving the Reidemeister-Schreier process. We outline the procedure for Γ'.

For the presentation (1) we have

$$\Gamma = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (at)^3 = (ual)^3 = [t, u] = 1 \rangle.$$

Abelianizing this gives us

$$\Gamma^{\text{ab}} = \langle a, l; a^2 = l^2 = (al)^2 = 1 \rangle = Z_2 \times Z_2.$$

Therefore $|\Gamma : \Gamma'| = 4$. Choosing coset representatives $1, a, l, al$ for Γ' in Γ and applying the Reidemeister-Schreier process we get as generators for Γ' $\{A, B, C, D, E, F, G, H\}$ with $A = ta$, $B = ual$, $C = at$, $D = aul$, $E = t^{-1}a$, $F = lua$, $G = at^{-1}$, $H = alu$. A complete set of relations is given by

$$A^3 = B^3 = C^3 = D^3 = E^3 = F^3 = G^3 = H^3 = AG = CE = BD$$
$$= FH = ADG^{-1}B^{-1} = CBE^{-1}D^{-1} = EHC^{-1}F^{-1} = GFA^{-1}H^{-1}.$$

Eliminating generators and simplifying we obtain

$$(2) \quad \Gamma' = \langle A, B, C, F; A^3 = B^3 = C^3 = F^3 = (AB^{-1})^2 = (CB)^2 = (CF)^2 = (A^{-1}F)^2 = 1 \rangle.$$

Now let

$$H_1 = \langle A, B, F; A^3 = B^3 = F^3 = (AB^{-1})^2 = (A^{-1}F)^2 = 1\rangle$$

and

$$H_2 = \langle C, B, F; C^3 = B^3 = F^3 = (CF)^2 = (CB)^2 = 1\rangle.$$

Then Γ' is generated by H_1 and H_2 with the identifications $B = B$ and $F = F$.

From the symmetry of the presentations it is clear that $H_1 \simeq H_2$ and $H = \langle B, F\rangle_{H_1} \longleftrightarrow \langle B, F\rangle_{H_2}$ is a subgroup isomorphism. Therefore

$$\Gamma' = H_1 *_H H_2.$$

What is left to show is that H_1 and H have the indicated structure. In H_1, let

$$H_{11} = \langle A, B; A^3 = B^3 = (AB^{-1})^2 = 1\rangle = A_4,$$
$$H_{12} = \langle A, F; A^3 = F^3 = (A^{-1}F)^2 = 1\rangle = A_4.$$

Then $H_1 = H_{11} * H_{12}$ with the identification $A = A$. This induces a subgroup isomorphism so $H_1 = A_4 *_{Z_3} A_4$. H in Γ' is then $\langle B, F\rangle = \langle B\rangle * \langle F\rangle = Z_3 * Z_3$.

The remainder of the theorem is handled in the same manner. Abelianizing presentation (2) for Γ' gives $(\Gamma')^{ab} = \langle A; A^3 = 1\rangle$ and so $|\Gamma' : \Gamma''| = 3$. It follows then that $|\Gamma'' : \Gamma'| = 12$.

Using coset representatives $1, A, A^2$ for Γ'' in Γ' and again applying the Reidemeister-Schreier process we obtain as generators for Γ'' $\{\alpha, \beta, \gamma, \delta, \varepsilon, \phi, \rho, \sigma, \tau\}$ with $\alpha = BA^{-1}$, $\beta = A^{-1}B$, $\gamma = ABA$, $\delta = CA$, $\varepsilon = A^{-1}CA^{-1}$, $\phi = AC$, $\rho = FA^{-1}$, $\sigma = A^{-1}F$ and $\tau = AFA$. A complete set of relations for Γ'' is

$$\alpha^2 = \beta^2 = \gamma^2 = \rho^2 = \sigma^2 = \tau^2 = (\delta\beta)^2 = (\varepsilon\gamma)^2$$
$$= (\phi\alpha)^2 = (\delta\sigma)^2 = (\varepsilon\tau)^2 = (\phi\rho)^2 = \alpha\gamma\beta = \delta\varepsilon\phi = \rho\tau\sigma = 1.$$

Eliminating $\gamma = \alpha\beta$, $\varepsilon = \delta^{-1}\phi^{-1}$ and $\tau = \rho\sigma$ and then simplifying and renaming the generators as $x_1 = \alpha$, $x_2 = \beta$, $x_3 = \rho$, $x_4 = \sigma$, $x_5 = \delta$, $x_6 = \phi$ we arrive at the following presentation for Γ'':

$$(3)\quad \Gamma'' = \langle x_1, x_2, x_3, x_4, x_5, x_6; x_1^2 = x_2^2 = x_3^2 = x_4^2 = (x_1x_2)^2$$
$$= (x_2x_5)^2 = (x_1x_6)^2 = (x_4x_5)^2 = (x_3x_6)^2$$
$$= (x_1x_6x_5x_2)^2 = (x_6x_5x_4x_3)^2 = 1\rangle.$$

Now let

$$K_1 = \langle x_1, x_2, x_5, x_6; x_1^2 = x_2^2 = (x_1x_2)^2 = (x_1x_6)^2 = (x_2x_5)^2 = (x_1x_6x_5x_2)^2 = 1\rangle$$

and

$$K_2 = \langle x_3, x_4, x_5, x_6; x_3^2 = x_4^2 = (x_3x_4)^2 = (x_3x_6)^2 = (x_4x_5)^2 = (x_6x_5x_4x_3)^2 = 1\rangle.$$

From presentation (3) it is seen that Γ'' is generated by K_1 and K_2 with the identifications $x_5 = x_5$ and $x_6 = x_6$. Further from the symmetry of the presentations for K_1 and K_2 it is clear that $K_1 \simeq K_2$ and the identifications yield subgroup isomorphisms. Therefore we have

$$\Gamma'' = K_1 *_K K_2 \quad \text{with } K = \langle x_5, x_6\rangle.$$

In K_1 let $u = x_1x_6$ and $v = x_5x_2$. Using these to eliminate x_6 and x_1 and rewriting we obtain for K_1

$$K_1 = \langle x_1, x_2, u, v; x_1^2 = x_2^2 = (x_1x_2)^2 = u^2 = v^2 = (uv)^2 = 1\rangle.$$

This is a free product of two Klein 4-groups D_2. Therefore

$$K_1 \simeq K_2 \simeq D_2 * D_2.$$

Fron this we have that

$$K = \langle x_5, x_6\rangle = \langle x_1u, x_2v\rangle = Z * Z, \quad \text{free of rank 2.}$$

Abelianizing Γ'' we get that

$$(\Gamma'')^{\text{ab}} = \langle x_1, x_2, x_3, x_4, x_5, x_6; x_i^2 = 1, i = 1, \ldots, 6 \text{ and } [X, Y] = 1\rangle = (Z_2)^6.$$

Therefore $|\Gamma'' : \Gamma'''| = 64$ and so $|\Gamma : \Gamma'''| = (12)(64) = 768$.

Applying the Reidemeister-Schreier process again to presentation (3) for Γ'' and using the 64 generators of $(Z_2)^6$ (actually the images of x_1 through x_6 in $(Z_2)^6$) as coset representatives we get a huge presentation for Γ''' on 384 generators. Taking relations and abelianizing we find that the resulting quotient is infinite. If follows that $\Gamma^{(4)}$ has infinite index in Γ'''. Further since this has infinite index it follows that the derived series from this point on has infinite index.

To see the structure of Γ''' we note that since Γ'' is a free product with amalgamation, Γ''' is an HNN group. This follows from the Karrass-Solitar subgroup theorems [**6**]. Since $\Gamma'' = K_1 *_K K_2$ the factors in the base group of Γ''' are conjugates of subgroups of K_1 and K_2. Since $K_1 \simeq K_2$ we have from a result of Takahasi [**15**] that K_1 is a retract of Γ'' and so $(\Gamma'')' \cap K_1 = K_1'$. But $K_1 = D_2 * D_2$ and so $K_1' = (D_2 * D_2)'$ which is free of rank 9. Therefore each factor in the base group is a free group of rank 9.

The sequence of indices 4,12,768 will play a prominent role in our classification of normal subgroups.

3. Normal subgroup classification. A result of Brunner, Frame, Lee and Wielenberg [**1**, p. 214] states that torsion-free subgroups of Γ must have indices divisible by 12 while from a theorem of Fine [**3**, p. 484] a normal subgroup with torsion must have index dividing 24. Thus the possible indices for proper normal subgroups are 2,3,4,6,8,12,24 and $12n$ (for $n > 2$).

We first give a complete classification for indices less than 60 and then prove several results showing that many other indices are impossible.

Note the similarity to the situation in the modular group M. A proper normal subgroup with torsion in M must have index 2 or 3 while torsion-free subgroups have indices divisible by 6 [**11**, p. 145]. The normal subgroups of the modular group have been classified with respect to index, genus, and parabolic class number [**11–14**].

We prove

THEOREM 2. *In the Picard group* Γ:

(1) *There are exactly* 3 *normal subgroups of index* 2. *Explicitly these are* $N(t)$, $N(u)$, *and* $N(t^2, u^2, at, tu)$.

(2) Γ' *is the only normal subgroup of index* 4.

(3) $\Gamma(1 + i)$ *is the only normal subgroup of index* 6.

(4) Γ'' *is the only normal subgroup of index* 12.

(5) *There are exactly* 3 *normal subgroups of index* 24. *Specifically* $N(l)$ *which has torsion and* $N(t^4, tu)$, $N(t^4, tu^{-1})$ *which are torsion-free. The latter two are isomorphic and faithfully represent* B_1 *the fundamental group of the Boromean rings.*

(6) *There are* 6 *normal subgroups of index* 48. *Explicitly these are*

(i) $N(t^2, u^2)$—*which is the principal congruence subgroup* $\Gamma(2)$,

(ii) $N(t^4, u^4, t^2u^2, (at^2)^2)$,

(iii) $N(t^4, u^4, t^2u^2, at^2altu)$,

(iv) $N(t^4, u^4, t^2u^2, at^2altu^{-1})$,

(v) $N(t^2, u^4, (au^2)^2)$,

(vi) $N(t^4, u^2, (at^2)^2)$.

The above are the only normal subgroups of index less than 60.

PROOF. We handle each part of the theorem separately. As remarked earlier the possible indices below 60 are 2,3,4,6,8,12,24,36,48. We first show that 3 and 8 are impossible.

PROPOSITION 1. Γ *has no normal subgroups of index* 3 *or of index* 8.

PROOF. Suppose $G \triangleleft \Gamma$ with $|\Gamma : G| = 3$. Let $A = \Gamma/G$ and so $|A| = 3$ and thus A is abelian. Therefore $G \supset \Gamma'$ which is impossible since $|\Gamma : \Gamma'| = 4$.

Next suppose that $G \triangleleft \Gamma$ with $|\Gamma : G| = 8$ and let $A = \Gamma/G$. Since $|A| = 8$, A is solvable and thus A has a normal subgroup of index 2 or 4.

If $|A : \overline{A}| = 2$ then $\overline{A}$ pulls back to a normal subgroup $\overline{G}$ of Γ of index 2 containing G, $\Gamma \supset \overline{G} \supset G$. Now $|\Gamma : \overline{G}| = 2$ so $\Gamma/\overline{G}$ is abelian $\rightarrow \Gamma' \subset \overline{G}$.

Since $|G : \overline{G}| = 4$, $\overline{G}/G$ is abelian and so $\overline{G}' \subset G$. But from $\Gamma' \subset \overline{G}$ it follows that $\Gamma'' \subset \overline{G}' \subset G$ which is impossible since $|\Gamma : \Gamma''| = 12$ and $|\Gamma : G| = 8$.

If $|A : \overline{A}| = 4$ then $\overline{A}$ pulls back to a normal subgroup $\overline{G}$ of index 4 in Γ. Then $|\Gamma/\overline{G}| = 4 \rightarrow \Gamma/\overline{G}$ is abelian and so $\Gamma' \subset \overline{G}$. But $|\Gamma : \Gamma'| = 4$ so $\Gamma' = \overline{G}$. But then $\Gamma \subset \Gamma' \subset G$ so $G \triangleleft \Gamma'$ with $|\Gamma' : G| = 2$. It follows that if Γ'/G is abelian $\Gamma'' \subset G$ which is impossible from above. Thus 3 and 8 are impossible indices for normal subgroups.

Embodied in the proof of Proposition 1 is the proof of

PROPOSITION 2. *If* $G \triangleleft \Gamma$ *and* $|\Gamma : G| = 4$ *then* $G = \Gamma'$ (*this is part* (2) *of the theorem*).

PROPOSITION 3. *There are exactly* 3 *normal subgroups of index* 2 *in* Γ.

PROOF. Let $G \triangleleft \Gamma$ with $|\Gamma : G| = 2$. Since Γ/G is abelian we have $\Gamma \supset G \supset \Gamma'$.

Now $\Gamma/\Gamma' = Z_2 \times Z_2 = D_2$, a Klein 4-group. This has exactly 3 normal subgroups of index 2. Therefore these pull back to exactly 3 normal subgroups of index 2 in Γ containing Γ'. Since G contains Γ', G must be one of these.

COROLLARY. *The* 3 *normal subgroups of index* 2 *are*

$$N(t), \qquad N(u), \qquad N(t^2, u^2, at, tu).$$

PROOF.

$$\Gamma/N(t) = \langle a, l, t, u \colon a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (ual)^3 = (at)^3 = [t, u] = t = 1 \rangle$$
$$= \langle u; u^2 = 1 \rangle$$

and so $|\Gamma : N(t)| = 2$. Further $N(t) \neq N(u)$ since $u \in N(t)$ but $u \notin N(u)$. Similarly $|\Gamma : N(u)| = 2$ and $|\Gamma : N(t^2, u^2, at, tu)| = 2$.

Now $tu \in N(t^2, u^2, at, tu)$ but $tu \notin N(t)$ and $tu \notin N(u)$. Therefore the three subgroups given above are 3 distinct normal subgroups of index 2.

PROPOSITION 4. *Γ'' is the only normal subgroup of index 12.*

PROOF. Suppose $G \triangleleft \Gamma$ with $|\Gamma : G| = 12$. Let $A = \Gamma/G$ so $|A| = 12 = 2^2 \cdot 3$. If A had only one 2-sylow subgroup it would be normal of index 3. This would pull back to a normal subgroup of index 3 in Γ which is impossible from Proposition 1. Thus A has more than one 2-sylow subgroup.

The number of 3-sylow subgroups is 1 or 4. If there were 4, since they intersect trivially, they cover 9 elements in A giving only one possible 2-sylow subgroup. Therefore A has only one 3-sylow subgroup which is normal of index 4. This pulls back to a normal subgroup of index 4 in Γ containing G. From Proposition 2 this must be Γ'. Therefore we have $\Gamma \supset \Gamma' \supset G$.

Now $|\Gamma' : G| = 3$ and $G \triangleleft \Gamma'$ so Γ'/G is abelian and $\Gamma'' \subset G$. But $|\Gamma : \Gamma''| = 12$ and $|\Gamma : G| = 12$ and so $\Gamma'' = G$ completing the proof of Proposition 4.

We have classified the indices 2, 4 and 12 and shown that 3 and 8 are impossible. We can now show that index 36 is also impossible.

PROPOSITION 5. *Γ has no normal subgroups of index 36.*

PROOF. Suppose $G \triangleleft \Gamma$ with $|\Gamma : G| = 36$ and let $A = \Gamma/G$. Since $|A| = 36 = 2^2 3^2$ A is solvable and nonabelian.

Let $G_0 = \Gamma' G$ = preimage of A' in Γ. Then $G_0 \triangleleft \Gamma$ and Γ/G_0 is abelian so $|\Gamma : G_0| = 2$ or 4.

If $|\Gamma : G_0| = 4$ then $G_0 = \Gamma'$ and $\Gamma \supset \Gamma' \supset G$. But then $\Gamma'/G = 9 = 3^2$ so Γ'/G is abelian and $\Gamma'' \subset G$. This is impossible since $|\Gamma : \Gamma''| = 12$.

Therefore $|\Gamma : G_0| = 2$ and $G_0 \supset \Gamma'$. It follows that $G_0' \supset \Gamma''$.

Now $|G_0/G| = 18$ so G_0/G contains a normal 3-sylow subgroup of index 2. This pulls back to a subgroup H of index 2 in G_0 giving us $G_0 \supset H \subset G$ with $|G_0 : H| = 2$ and $|H : G| = 9$. G_0/H is abelian so $H \supset G_0' \supset \Gamma'' \rightarrow |H\Gamma''| = 3$. From this it follows that $G_0' = H$ or $G_0' = \Gamma''$.

If $G_0' = H$ then H is a fully invariant subgroup of a normal subgroup of Γ and therefore H is normal in Γ. But then $|\Gamma : H| = 4$ so $H = \Gamma'$ and we have $\Gamma \supset \Gamma' \supset G$ which is impossible by the previous argument.

If $G_0' = \Gamma''$ then G_0/G_0' is abelian of order 6. An abelian group of order 6 has a unique normal subgroup of index 2. Thus there is a unique normal subgroup of index 2 in G_0 containing Γ''. Then $G_0 \supset H \subset \Gamma''$ and also $G_0 \supset \Gamma' \supset \Gamma''$. Therefore $H = \Gamma'$ which is impossible from before. This completes Proposition 5.

PROPOSITION 6. *$\Gamma(1 + i)$ is the only normal subgroup of index 6.*

PROOF. Using a formula of Newman [**11**, p. 145] we have $|\Gamma : \Gamma(1+i)| = 6$ so the proof is completed by showing that there is only one normal subgroup of index 6.

As before suppose $G \triangleleft \Gamma$, $|\Gamma : G| = 6$ and $A = \Gamma/G$. Then A is a nonabelian group of order 6 so A has a normal subgroup of index 2. Thus there is a $G_0 \triangleleft \Gamma$ with $\Gamma \supset G_0 \supset G$ and $|\Gamma : G_0| = 2$. Further $G_0 \supset \Gamma'$ so $G_0' \supset \Gamma''$.

Now $|G_0 : G| = 3$ so G_0/G is abelian giving us a series $\Gamma \supset G \supset G_0' \supset \Gamma''$.

To complete this we need the following

LEMMA. $\Gamma'' = N(ltu)$ *and* $\Gamma/\Gamma'' = S_3 \times Z_2$.

PROOF. A straightforward computation using the method of Theorem 1 gives that $ltu \in \Gamma''$ so $\Gamma'' \supset N(ltu)$. However setting $ltu = 1$ in our standard presentation for Γ we find that

$$\Gamma/N(ltu) = \langle a, t, u; a^2 = t^2 = u^2 = (at)^3 = (atu)^2 = [t,u] = 1\rangle = S_3 \times Z_2.$$

Therefore $|\Gamma : N(ltu)| = 12$, $\Gamma'' = N(ltu)$ and $\Gamma/\Gamma'' = S_3 \times Z_2$.

Now we complete the proof of Proposition 6. $\Gamma/\Gamma'' = S_3 \times Z_2$ which has a unique normal subgroup of index 6. Therefore there is a unique normal subgroup of index 6 in the series $\Gamma \supset \overline{G} \supset \Gamma''$. But $\Gamma \supset G \supset \Gamma''$ and $|\Gamma : G| = 6$. Therefore $\overline{G} = G$ completing the proof.

The two remaining cases less than 60 are 24 and 48.

PROPOSITION 7. *There are exactly* 3 *normal subgroups of index* 24. *Explicitly these are* $N(l)$ *which has torsion and* $N(t^4, tu), N(t^4, tu^{-1})$ *which are torsion-free.*

PROOF. Suppose $G \triangleleft \Gamma$ and $|\Gamma : G| = 24$. If G has torsion a theorem of Fine [**3**, p. 484] shows that G must be $N(l)$. We suppose then that G is torsion-free.

If $A = \Gamma/G$ then the image of any element of finite order in Γ has exactly the same order in A since the orders in Γ are 2 or 3 and G is torsion-free. Further if m and n are the respective orders of the images of the parabolic elements t and u in A then A is a quotient of

$$\overline{A} = \langle a, l, t, u : a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (at)^3 = (ual)^3 = t^m = u^n = [t,u] = 1\rangle.$$

The proof proceeds by showing that the only possible choices for m and n in this case are $m = n = 4$.

LEMMA. *The subgroup* $\langle t, u\rangle$ *in* A *has index at least* 6.

PROOF. We show that $1, a, l, al, ta, tal$ are all incongruent mod$\langle t, u\rangle$ in A.

(1) If $a \in \langle t, u\rangle$ then $a = t^j u^k$ so $ual = t^j u^{k+1} l$. But ual has order 3 in Γ while $t^x u^y l$ has order 2 in Γ for all choices of x, y. So $a \notin \langle t, u\rangle$.

(2) If $l \in \langle t, u\rangle$ then $l = t^j u^k$ so $l^2 = t^j u^k l = 1$. But $t^j u^k l$ has order 2 in Γ so therefore $l \notin \langle t, u\rangle$.

If $l \in a\langle t, u\rangle$ then $l = at^j u^k$. But then $al = t^j u^k$ from which it follows that $ta = t^{j-1} u^k l$. But as in the case above ta has order 3 while $t^{j-1} u^k l$ has order 2 so $l \notin a\langle t, u\rangle$.

(3) If $al \in \langle t, u\rangle$ then $al = t^j u^k$. This was impossible from the previous argument. Similarly the cases $al \in a\langle t, u\rangle$ and $al \in l\langle t, u\rangle$ are impossible.

Therefore the elements $1, a, l, al$ are all incongruent $\bmod\langle t, u\rangle$.

(4) Consider the element ta in A.

(i) If $ta \in \langle t, u\rangle$ then $a \in \langle t, u\rangle$ which was impossible from above.

(ii) If $ta \in a\langle t, u\rangle$ than $ta = at^j u^k$, $ata = t^k u^j$. But $ata = t^{-1}at^{-1}$ so then $a = t^{k+2}u^j$ which is impossible from (1).

(iii) If $ta \in l\langle t, u\rangle$. This is impossible since ta has order 3 while every element of the coset $l\langle t, u\rangle$ has order 2.

(iv) Finally if $ta \in al\langle t, u\rangle$ then $ta = alt^j u^k$ or $ata = lt^j u^k$. But then $ata = t^{-1}at^{-1} = lt^j u^k$ giving $a = lt^{j+2}u^k$ or $a \in l\langle t, u\rangle$ which is impossible.

Therefore $1, a, l, al, ta$ are all incongruent $\bmod\langle t, u\rangle$ in A. Since the index of $\langle t, u\rangle$ is greater that 4 and divides 24 it must be at least 6. Using the same type of arguments as above we can show that tal is also incongruent to $1, a, l, al, ta$.

We now proceed with the proof of Proposition 7.

Consider $\langle t, u\rangle$in $A = \Gamma/G$. This is abelian of index at least 6 in A and therefore $|\langle t, u\rangle| \leq 4$. Thus $|\langle t, u\rangle| = 2, 3, 4$. ($t = u = 1$ would make the quotient too small immediately.) Further $|\langle t\rangle| = 2, 3$ or 4 and $|\langle u\rangle| = 2, 3$ or 4. We show that if $|A| = 24$ the only possible cases are when $t^4 = u^4 = 1$ with $t = u$ or $t = u^{-1}$.

Case 1. If $t^4 = u^3 = 1$ then since $(4, 3) = 1$ it follows that $|\langle t, u\rangle| = 12$ which is impossible. Similarly $t^3 = u^4 = 1$ is impossible.

Case 2. If $t^4 = u^2 = 1$ then $|\langle t, u\rangle| = 4$ and so $u = t^2$. Then A is a quotient of

$$\begin{aligned}\overline{A} &= \langle a, l, t\colon a^2 = l^2 = (al)^2 = (tl)^2 = (t^2al)^3 = (ta)^3 = t^4 = 1\rangle \\ &= \langle a, t\colon a^2 = (at)^3 = t^4 = (t^2a)^6 = 1\rangle\end{aligned}$$

which has order 6. So this is impossible. Similarly $t^2 = u^4 = 1$ is impossible.

Case 3. If $t^3 = u^3 = 1$ then $|\langle t, u\rangle| = 3$ so $t = u$ or $t = u^{-1}$. In either case the resulting quotient has order 1 so this case is impossible.

Case 4. If $t^2 = u^2 = 1$ and $|\langle t, u\rangle| = 2$ then $u = t$ and the resulting quotient is too small. Therefore if $t^2 = u^2 = 1$ then $|\langle t, u\rangle| = 4$ and $|A\colon \langle t, u\rangle| = 6$.

Thus from Lemma $1, a, l, a, ta, tal$ give a complete set of coset representatives for $\langle t, u\rangle$ in A. However by an examination of cases identical to the proof of the lemma we can show that in this case the element ua is not congruent to any of $\{1, a, l, a, ta, tal\}$ $\bmod\langle t, u\rangle$ so this case is impossible.

Case 5. If $t^4 = u^4 = 1$ then since $|\langle t, u\rangle| \leq 4$ and $|\langle t\rangle| = 4$ it follows that $|\langle t, u\rangle| = 4$. Since $\langle t, u\rangle$ is abelian then $t = u$ or $t = u^{-1}$. But then A is a quotient of $\overline{A} = \langle a, l, t, u\colon a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (at)^3 = (ual)^3 = t^4 = u^4 = 1, u = t^{\pm 1}\rangle$.

But $\overline{A}$ has order exactly 24 so in this case $A = \overline{A}$. Since $A = \Gamma/G$ this gives two possibilities for $G \to G = N(t^4, tu)$ or $G = N(t^4, tu^{-1})$.

This completes Proposition 7.

COROLLARY. $N(t^4, tu) \simeq N(t^4, tu^{-1}) \simeq B_1$ *where* B_1 *faithfully represents the fundamental group of the Boromean rings.*

PROOF. This follows from a result of Brunner, Frame, Lee and Wielenberg which showed that up to isomorphism there is only one torsion-free normal subgroup of Γ of index 24. Further this group faithfully represents the fundamental group of the Bormean rings [**1**, p. 221].

PROPOSITION 8. *There are exactly* 6 *normal subgroups of* Γ *of index* 48. *Explicitly*:

(i) $N(t^2, u^2)$ (*which is the principal congruence subgroup* $\Gamma(2)$),
(ii) $N(t^4, u^4, t^2, u^2, (at^2)^2)$,
(iii) $N(t^4, u^4, t^2u^2, at^2altu)$,
(iv) $N(t^4, u^4, t^2u^2, at^2altu^{-1})$,
(v) $N(t^4, u^2, (at^2)^2)$,
(vi) $N(t^2, u^4, (au^2)^2)$.

PROOF. No two of the six listed subgroups coincide. The remainder of the proof involves showing that any normal subgroup of index 48 must be one of the subgroups listed above.

If $G \triangleleft \Gamma$ and $|\Gamma: G| = 48$ then G must be torsion-free. We now consider in a manner analogous to the proof of Proposition 7, a detailed analysis of the possible images of the parabolic elements t, u in the quotient Γ/G.

As in the proof of Proposition 7 if $A = \Gamma/G$ then the image of any element of finite order in G has exactly the same order in A since G is torsion-free. As before if m and n are the respective orders of the images of t and u in A then A is a quotient of

$$\overline{A} = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (at)^3 = (ual)^3 = t^m = u^n = [t, u] = 1\rangle.$$

We show first that m, n must be 2 or 4.

Now $|A| = 48 = 2^4 \cdot 3$ so A has 1 or 3 2-sylow subgroups. If there were only 1 it would be normal of index 3 which would pull back to a normal subgroup of index 3 in Γ. This is impossible from Proposition 1 so it follows that there are 3 2-sylow subgroups in A. This induces a map $f: A \to H \to S_3$ where H is a transitive subgroup of S_3. If $H = A_3$ then A has a normal subgroup of index 3 which is impossible. Therefore $H = S_3$ and A has a normal subgroup of index 6 which pulls back to a normal subgroup of index 6 in Γ which contains G. From Proposition 6 this must be the principal congruence subgroup $\Gamma(1+i)$. Thus we have $\Gamma \supset \Gamma(1+i) \supset G$ with $|\Gamma(1+i)/G| = 8$. Now $t^2, u^2 \in \Gamma(1+i)$ but $t, u \notin \Gamma(1+i)$ so in the quotient $\Gamma(1+i)/G$ the images of t^2, u^2 have order a power of 2. Therefore in $A = \Gamma/g$ the images of t, u have order a power of 2. Since $|\Gamma/G| = 48$ we then must have $m, n = 2, 4, 8, 16$ since $m = 1$ or $n = 1$ makes the resulting quotient too small.

Using exactly the same arguments as in the proof of Proposition 7 we have that in A the elements $1, a, l, al, ta, tla$ are incongruent modulo the abelian subgroup $\langle t, u\rangle$. (We now consider these elements as being in A.) Therefore $|A: \langle t, u\rangle| \geq 6$ and thus $|\langle t, u\rangle| \leq 8$. It follows that $m, n = 2, 4$ or 8.

We now show that $m \neq 8$ and $n \neq 8$ by examining the possible cases.

Case 1. $t^8 = u^8 = 1$ but no smaller powers of t or u are the identity in A. Since $|\langle t, u\rangle| \leq 8$ and t has order 8 we must have $|\langle t, u\rangle| = 8$. Then $t^8 = 1$ and $u = t^\alpha$ where t^α is a generator so $u = t^{\pm 1}$ or $u = t^{\pm 3}$.

If $u = t$ then A is a quotient of

$$\overline{A} = \langle a, l, t; a^2 = l^2 = (al)^2 = (tl)^2 = (ta)^3 = (tla)^3 = t^8 = 1\rangle.$$

Using the relation $(tla)^3 = 1$ we get that $l = tat^{-1}ata$. Eliminating l and simplifying we obtain $\overline{A} = \langle a, t; a^2 = t^4 = (ta)^3 = 1\rangle$. This is impossible since we assumed that t has order exactly 8 in A which is a quotient of $\overline{A}$. ($\overline{A}$ is the (2, 3, 4) triangle group which has order 24 making the resulting quotient too small as well.) An identical argument shows that $u = t^{-1}$ is impossible.

If $u = t^3$ then A is a quotient of

$$\overline{A} = \langle a, l, t; a^2 = l^2 = (al)^2 = (tl)^2 = t^8 = (ta)^3 = (t^3la)^3 = 1\rangle.$$

In $\overline{A}$ the same arguments used in the proof of Proposition 7 will show that the element t^2a is not congruent in $\overline{A}$ to $1, l, al, ta, tla$ modulo the subgroup $\langle t\rangle$. If further t^2a was not congruent modulo $\langle t\rangle$ to the element a then $\langle t\rangle$ would have index greater than 6. But $|\langle t\rangle| = 8$ and $|A| = 48$ so $\langle t\rangle$ has index exactly 6 and therefore t^2a must be congruent to a modulo $\langle t\rangle$. But then $t^2a = at^\alpha$ and so $at^2a = t^\alpha$. Since t has order 8, $\alpha = \pm 2$ and therefore the relation $at^2a = t^{\pm 2}$ must be in A. Thus A is a quotient of

$$\overline{\overline{A}} = \langle a, l, t; a^2 = l^2 = (al)^2 = (tl)^2 = t^8 = (ta)^3 = (t^3a)^3 = 1, at^2a = t^{\pm 2}\rangle.$$

Since $at^2a = t^{\pm 2}$ and $lt^2l = t^{-2}$ the subgroup $\langle t^2\rangle$ is normal of order 4 in $\overline{\overline{A}}$. However $\overline{\overline{A}}/\langle t^2\rangle = \langle a, l; a^2 = l^2 = (al)^2 = 1\rangle = D_2$ so $\langle t^2\rangle$ has index 4 in $\overline{\overline{A}}$. Thus $|\overline{\overline{A}}| = 16$ which is impossible since $|A| = 48$. An identical argument shows that it is also impossible if $u = t^{-3}$.

This completes Case 1 showing that in A we cannot have t and u both having order exactly 8.

Case 2. $t^8 = u^4 = 1$ and no smaller powers are the identity in A.

As in Case 1, $\langle t, u\rangle$ has index at least 6 in A. It follows that $|\langle t, u\rangle| = 8$. Therefore $\langle t, u\rangle = \langle t\rangle$ and $u = t^k$ with $k = \pm 2$. Then A is a quotient of

$$\overline{A} = \langle a, l, t; a^2 = l^2 = (al)^2 = (tl)^2 = (ta)^3 = (t^2al)^3 = t^8 = 1\rangle.$$

As in Case 1 the element t^2a in A can be shown to be shown to be incongruent modulo $\langle t\rangle$ to $1, l, al, ta, tal$ and thus must be congruent to a modulo $\langle t\rangle$. This gives us $at^2a = t^{\pm 2}$ and so $\langle t^2\rangle$ is normal of order 4 in $\overline{A}$. But $\overline{A}/\langle t^2\rangle = \langle a; a^2 = 1\rangle$. This gives that $|\overline{A}| = 8$ which is impossible since it has A as a quotient. This completes Case 2.

An identical treatment handles when u has order exactly 8 and t has order exactly 4.

Case 3. $t^8 = u^2 = 1$ and no smaller powers are the identity in A.

As in Cases 1 and 2 $|\langle t, u\rangle| = 8$ so that $\langle t, u\rangle = \langle t\rangle$ with $u = t^4$. Then A is a quotient of

$$\overline{A} = \langle a, l, t; a^2 = l^2 = (al)^2 = (tl)^2 = t^8 = (ta)^3 = (t^4al)^3 = 1\rangle.$$

Again as in the previous cases we must have $-$ since $\langle t\rangle$ has index $6 - t^2a$ congruent to the element a modulo $\langle t\rangle$. Thus $at^2a = t^{\pm 2}$ and $\langle t^2\rangle$ is normal of order 4 in A. But $\overline{A}/\langle t^2\rangle = \langle a; a^2 = 1\rangle$ giving $|\overline{A}| = 8$ which is impossible. This completes Case 3. Again an identical treatment handles the situation where $u^8 = t^2 = 1$.

Therefore we have shown that in A neither t nor u can have order $8-$ that is $m \neq 8$ and $n \neq 8$. We now consider the cases where $m = 2$ or 4 and $n = 2$ or 4.

Case 4. $t^4 = u^4 = 1$ and no smaller powers are the identity in A.

Since $\langle t, u\rangle$ has index at least 6 we must have $|\langle t, u\rangle| = 8$ or $|\langle t, u\rangle| = 4$.

Subcase (a). $|\langle t, u\rangle| = 4$. Then $\langle t, u\rangle = \langle t\rangle$ and $u = t$ or $u = t^{-1}$. In either case A is then a quotient of

$$\overline{A} = \langle a, l, t; a^2 = l^2 = (al)^2 = (tl)^2 = (ta)^3 = (tal)^3 = t^4 = 1\rangle.$$

Using the relation $(tal)^3$ to eliminate l as in Case 1 we find that $\overline{A}$ is the (2, 3, 4) triangle group which has order 24. This is too small to have A as a quotient so this subcase is impossible.

Subcase (b). $|\langle t, u\rangle| = 8$. Since $\langle t, u\rangle$ is abelian and $t^4 = u^4 = 1$ we must then have $t^2 = u^{-2}$ or $t^2u^2 = 1$. Thus in this case A is a quotient of

$$\overline{A} = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (ta)^3 = (ual)^3 = t^4 = u^4 = t^2u^2 = [t, u] = 1\rangle.$$

In A consider the element t^2a. t^2a can now be shown to be incongruent to $1, l, ta, tal$ modulo $\langle t, u\rangle$. If (1) $t^2a = t^xu^y$ then $ta = t^{x-1}u^y$. But ta has order 3 while $t^{x-1}u^y$ has order a power of 2 so this is impossible. If (2) $t^2a - lt^xu^y$ then $ta = lt^{x+1}u^y$ which is impossible since ta has order 3 but $lt^{x+1}u^y$ has order 2. If (3) $t^2a = tat^xu^y$ then $ata = t^xu^y$ so $t^{-1}at^{-1} = t^xu^y$ or $at^{-1} = t^{x+1}u^y$ which is impossible since at^{-1} has order 3. Finally if (4) $t^2a = talt^xu^y$ then $ata = lt^xu^y$ which is impossible since t has order exactly 4 while lt^xu^y has order 2. Now since $\langle t, u\rangle$ has index exactly 6 in this case t^2a must be congruent modulo $\langle t, u\rangle$ to either a or al. In the former case we would have $at^2a = t^xu^y$ while in the latter $at^2a = lt^xu^y$. Since t^2 has order exactly 2 this gives the following possibilities:

(1) $at^2a = t^2$ (which is equal to u^2),

(2) $at^2a = tu$,

(3) $at^2a = lt^xu^y$ with $x = 0, 1, 2, 3$ and $y = 0, 1, 2, 3$.

We consider all 18 possibilities and show that (1) is possible and leads to a normal subgroup of index 48, (2) is impossible while (3) is possible only if $x = 1$, $y = 1$ or $x = 1$, $y = 3$ or a pair (x, y) giving an equivalent quotient to either of the preceding 2.

First suppose that (1) holds $\rightarrow$ $at^2a = t^2$. Since $t^4 = 1$ this implies that $(at^2)^2 = 1$. Thus A is now a quotient of

$$\overline{\overline{A}} = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (ta)^3 = (ual)^3 = t^4 = u^4 = t^2u^2 = [t, u] = (at^2)^2 = 1\rangle.$$

Abelianizing $\overline{\overline{A}}$ we find that

$$\overline{\overline{A}}/\overline{\overline{A}}' = \langle a, l; a^2 = l^2 = (al)^2 = 1\rangle$$

so $\overline{\overline{A}}'$ has index 4. Applying the Reidemeister-Schreier process we discover that $\overline{\overline{A}}' \simeq A_4$ the alternating group on 4 symbols. Thus $|\overline{\overline{A}}'| = 12$ and $|\overline{\overline{A}}| = 48$. Since $|A| = 48$ and A is a quotient of $\overline{\overline{A}}$ we must have $A = \overline{\overline{A}}$. Thus the presentation for $\overline{\overline{A}}$ given above presents a quotient of Γ of order 48. This is precisely the quotient modulo the normal subgroup $N(t^4, u^4, t^2u^2, (at^2)^2)$. Thus this is one possible normal subgroup of index 48. (We note that the fact that $|\overline{\overline{A}}| = 48$ was found originally using Todd-Coxeter coset enumeration as implemented in the Cayley Group Theory Program.)

Now suppose that (2) holds so that $at^2a = tu$. Then A is a quotient of

$$\overline{A} = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (ta)^3 = (ual)^3 = t^4 = u^4 = t^2u^2 = [t, u] = 1, at^2a = tu\rangle.$$

Then $u = at^2at^{-1}$. Using $t^2 = u^2$ it is then derivable that $t^2 = 1$ contradicting the fact that t has order exactly 4. Thus this case is impossible.

Finally suppose that (3) holds. Then $at^2a = lt^xu^y$. If

(a) $x = y = 0$ then $at^2a = l$ or $t^2 = l$. Then $t = lt$ which is impossible since t has order 4 while lt has order 2.

(b) $x = 1$, $y = 0$ then $at^2a = lt$. But then $alt^2a = t$. Again this is impossible since t has order 4 while alt^2a has order 2 (being a conjugate of lt^2). The same argument shows that $x = 0$, $y = 1$ is impossible.

(c) $x = 2$, $y = 0$ then $at^2a = lt^2$. Then A is a quotient of

$$\overline{\overline{A}} = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (ta)^3 = (ual)^3 = t^4 = u^4 = t^2u^2 = [t, u] = 1, at^2a = lt^2\rangle.$$

This is found to be a group of order 96. However it has no normal subgroups of order 2 and so no quotients of size 48. To do this the Cayley Group Theory Program was used. Todd-Coxeter enumeration gave us the size of 96 while a related algorithm in Cayley produced the potential normal subgroups. Without recourse to the program the above results could also be obtained by abelianizing $\overline{\overline{A}}$ and then applying Reidemeister-Schreier. The elements of order 2 can then be enumerated and tested for normality.

Since there are no quotients of $\overline{\overline{A}}$ of size 48 this case is impossible. An identical procedure handles $x = 0, y = 2$.

(d) $x = 3$, $y = 0$ then $at^2a = lt^3$. As in the previous cases the resulting group formed by adjoining this relation to the already existing relations in A is too small to have A as a quotient. In this case the resulting group has order 2. Again an identical procedure handles $x = 0, y = 3$.

(e) $x = 1$, $y = 1$ then $at^2a = ltu$. A is then a quotient of

$$\overline{\overline{A}} = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (ta)^3 = (ual)^3 = t^4 = u^4 = t^2u^2 = [t, u] = 1, at^2a = ltu\rangle.$$

Using Todd-Coxeter coset enumeration on $\overline{\overline{A}}$ (as implemented in Cayley) we find that $|\overline{\overline{A}}| = 48$. Therefore $\overline{\overline{A}} = A$. Thus in this case

$$A = N(t^4, u^4, t^2u^2, at^2altu).$$

This gives a second potential normal subgroup of index 48.

(f) $x = 1$, $y = 3$ then $at^2a = ltu^{-1}$. As in (e) the resulting quotient obtained from adjoining this relation has order 48. This gives another normal subgroup of index 48 namely $N(t^4, u^4, t^2u^2, at^2altu^{-1})$.

The relation $at^2a = lt^{-1}u$ is equivalent in this presentation to $at^2a = ltu^{-1}$ so we get the same subgroup for $x = 3$, $y = 1$.

This completes the potential cases when t and u both have order 4.

Case 5. $t^4 = u^2 = 1$ and no smaller powers are the identity in A.

As before $|\langle t, u\rangle| = 8$ or $|\langle t, u\rangle| = 4$.

Subcase (a). $|\langle t,u\rangle| = 8$ then $\langle t,u\rangle$ has index exactly 6 and as previously we can show that t^2a is incongruent modulo $\langle t,u\rangle$ to $1, l, ta, tal$. Therefore it must be congruent to either a or al. This gives the possibilities (1) $at^2a = t^2$, (2) $at^2a = u$ or (3) $at^2a = lt^xu^y$ with $x = 0,1,2,3$ and $y = 0,1$.

If (1) holds so that $at^2a = t^2$ then $(at^2)^2 = 1$ and A is a quotient of

$$\overline{\overline{A}} = \langle a,l,t,u; a^2 = l^2 = (al)^2 = (tl)^2 = (ta)^3 = (ual)^3 = t^4 = u^2 = (at^2)^2 = [t,u] = 1\rangle.$$

Applying Todd-Coxeter we find that $|\overline{\overline{A}}| = 48$ and thus $A = \overline{\overline{A}}$. This gives the new normal subgroup $N(t^4, u^2, (at^2)^2)$.

If (2) holds so that $at^2a = u$ then $at^2at = tat^2a$. Using $(ta)^3 = 1$ we can derive that $t^2 = 1$ contradicting that the order of t is 4.

If (3) holds there are 8 separate subcases. For each pair x, y it can be shown, in the same manner as in Case 4, that the resulting group obtained by adjoining the relation $at^2a = lt^xu^y$ is too small to have A as a quotient. Therefore (3) is impossible.

Subcase (b). $|\langle t,u\rangle| = 4$. Then $u = t^2$ and A is a quotient of the group

$$\overline{\overline{A}} = \langle a,l,t; a^2 = l^2 = (al)^2 = (tl)^2 = t^4 = (ta)^3 = (t^2al)^3 = 1\rangle.$$

Using $(t^2al)^3 = 1$ we can solve for l. Thus $\overline{\overline{A}}$ is a quotient of the (2,3,4) triangle group and is too small to have A as a quotient.

Exactly the same analysis as in Case 5 handles the situation when $u^4 = t^2 = 1$ and no smaller powers. This leads to an additional normal subgroup of index 48 namely $N(t^2, u^4, (au^2)^2)$. This completes when either t or u have order 4.

Case 6. $u^2 = t^2 = 1$ with $u \neq 1$, $t \neq 1$. Then A is a quotient of

$$\overline{A} = \langle a,l,t,u; a^2 = l^2 = t^2 = u^2 = (al)^2 = (ul)^2 = (tl)^2 = (ta)^3 = (ual)^3 = [t,u] = 1\rangle.$$

This has order 48 so $\overline{A} = A$ giving the final normal subgroup of index $48 - N(t^2, u^2)$. From the formula of Newman [**11**, p. 145] we have that the principal congruence subgroup $\Gamma(2)$ has index 48. Since t^2 represents the transformation $z' = z + 2$ it follows that $t^2 \in \Gamma(2)$. Similarly u^2 represents $z' = z + 2i$ so $u^2 \in \Gamma(2)$. Therefore $\Gamma(2) \supset N(t^2, u^2)$ and since they have the same index we have $\Gamma(2) = N(t^2, u^2)$.

This completes the proof of Proposition 8 and consequently the proof of Theorem 2.

In proving Theorem 2 we showed that there are no normal subgroups of index 3, 8 or 36 and in general none of the index greater than 24 and not divisible by 12. The next result shows that there exist many other gaps in the possible indices.

THEOREM 3. *Let* $d(n)$ = *number of normal subgroups of* Γ *of index* n. *Then* $d(n) = 0$ *in all of the following cases.*

(1) $n > 12$, $n \neq 0 \bmod 12$,

(2) $n = 3$ *or* $n = 8$,

(3) $n = 12p^k$ *with* p *a prime and* $p \neq 2, 3, 5, 11$,

(4) $n = 36p^k$ *with* p *a prime and* $p \neq 2, 3, 11, 17$,

(5) $n = 12p^kq^j$ *with* p *and* q *primes satisfying* $1 + pk_1 \nmid 12q^j$ *for any* k_1 *and* $p, q \neq 2, 3, 5, 11$.

PROOF. (1) and (2) are restatements of already known results so we begin with (3).

Suppose that $G < \Gamma$ with $|\Gamma : G| = 12p^k$ with p a prime and $p \neq 2, 3, 5$ or 11. Let $A = \Gamma/G$. Since $|A| = 12p^k$ the number of p-sylow subgroups of A is of the form $1 + pk_1$ and divides 12. If $p \neq 2, 3, 5, 11$ this number must be 1 and so A has a normal p-sylow subgroup of index 12.

This will pull back to a normal subgroup of index 12 in Γ. From Theorem 2 this must be the second commutator subgroup Γ''. Thus we have $\Gamma \supset \Gamma'' \supset G$ and $|\Gamma'' : G| = p^k$.

Let $\overline{A} = \Gamma''/G$. Since $|\overline{A}| = p^k$ it follows that $\overline{A}$ is solvable. Thus there is an $\overline{A}'$ with $\overline{A}/\overline{A}'$ abelian. $\overline{A}'$ must then pull back to a subgroup $\overline{G}$ of Γ satisfying $\Gamma'' \supset \overline{G} \supset G$ and $\Gamma''/\overline{G}$ abelian.

But then $\Gamma''' \supset \overline{G}$ which is impossible since $|\Gamma'' : \Gamma'''| = 2^6$ and $|\Gamma'' : \overline{G}| = p^n$ with $p \neq 2$. Therefore there are no normal subgroups of index $12p^k$ with p satisfying the stated conditions.

Next suppose that $|\Gamma : G| = 36p^k$ with $G < \Gamma$ and p a prime and $p \neq 2, 3, 11, 17$. Let $A = \Gamma/G$. Because $p \neq 2, 3, 11, 17$ A must have a normal p-sylow subgroup of index 36. This will pull back to a normal subgroup of index 36 in Γ. From Theorem 2 there are none—thus there are no normal subgroups of index $36p^k$ with $p \neq 2, 3, 11, 17$.

Finally part (5) is essentially the same as part (3). If $G < \Gamma$ and $|\Gamma : G| = 12p^kq^j$ then under the stated conditions on the primes the quotient Γ/G must have a normal p-sylow subgroup of index $12q^j$. From part (3) Γ contains no normal subgroups of these indices so this is impossible.

We note that the process given in part (5) can be continued for strings of greater than two primes.

Besides having no normal subgroups for many indices, there are restrictions placed on the normal subgroups by the indices. The following theorem gives these and also points out the close connection with the congruence subgroups.

THEOREM 4. *Suppose* $G \triangleleft \Gamma$; *then*

(1) *If* $|\Gamma : G| = 2^k \cdot 3$ *then* $G \supset \Gamma(1 + i)$.

(2) *If* $|\Gamma : G| = 4m$ *with* $(m, 3) = 1$ *then* $G = \Gamma'$.

(3) *If* $|\Gamma : G| = 12m$ *with* $(m, 6) = 1$ *and* Γ/G *solvable then* $G = \Gamma''$.

PROOF. Part (2) is immediate. If $(m, 3) = 1$ then G must have torsion. Then $4m|24 \rightarrow m = 1$ or 2. If $m = 2$, $|\Gamma : G| = 8$ which is impossible so $m = 1$, $|\Gamma : G| = 4$ and $G = \Gamma'$.

Now suppose $|\Gamma : G| = 2^k \cdot 3$ and let $A = \Gamma/G$. If A had a normal 2-sylow subgroup this would have index 3 and pull back to a normal subgroup of index 3 in Γ which is nonexistent. Thus there are 3 2-sylow subgroups in A. This gives a map $f : A \rightarrow H \subset S_3$ where H is a transitive subgroup of S_3. Thus $H = S_3$ or $H = A_3$. If $H = A_3$ then A has a normal subgroup of index 3 which is impossible so $H = S_3$.

Therefore A has a normal subgroup of index 6 which pulls back to a normal subgroup of index 6 in Γ. Thus $\Gamma \supset \overline{G} \supset G$ with $|\Gamma : \overline{G}| = 6$. From Theorem 1 then $\overline{G} = \Gamma(1+i)$.

Finally suppose $|\Gamma : G| = 12m$ with $(m, 6) = 1$ and $\Gamma/G = A$ solvable. In A there is a normal series with abelian factors $A \supset A_1 \supset A_2 \supset \cdots \supset \{1\}$. Further the indices of the subfactors A_i/A_{i+1} must eventually not be prime to m. But this will pull back to a normal series in Γ (ending in G) with abelian factors. But the only primes dividing the indices in the derived series are 2 and 3, so $m = 1$ and $|\Gamma : G| = 12$. From Theorem 1 then $G = \Gamma''$.

COROLLARY. *The* 3 *normal subgroups of index* 24 *and the* 6 *normal subgroups of index* 48 *are all contained in* $\Gamma(1+i)$ *(in fact* $N(t^2, u^2) = \Gamma(2)$*).*

4. The normal series of powers. An interesting special case of normal subgroups are the power subgroups Γ^n—the normal subgroups of Γ generated by nth powers of elements of Γ. In the modular group it is known that $M^n = M, M^2, M^3$ if $6 \nmid n$ while the exact structure of M^{6k} is unknown if $k > 1$. M^6 is free of rank 37 [**11**]. The next result gives similar results in Γ.

THEOREM 5. (1) $\Gamma^2 = \Gamma'$,
(2) $\Gamma^3 = \Gamma$ *and* $\Gamma^n = \Gamma$ *if* $2 \nmid n$,
(3) $\Gamma^n = \Gamma^2$ *if* $2|n$ *but* $6 \nmid n$.

PROOF. The proofs are straightforward computations. We adjoin the identical relation $X^n = 1$ to the standard presentation (1) for Γ. This gives us a presentation for Γ/Γ^n—the order of this giving us the index. First if $n = 2$ we have

$$\Gamma/\Gamma^2 = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (ta)^3 = (ual)^3 = [t, u] = 1, X^2 = 1\rangle.$$

Since $(at)^3 = (at)^2 = 1$ this implies that $at = 1$ or $a = t$. Similarly $u = al$. Therefore

$$\Gamma/\Gamma^2 = \langle a, l; a^2 = l^2 = (al)^2 = 1\rangle = D_2.$$

Thus $|\Gamma : \Gamma^2| = 4$ and from Theorem 1 $\Gamma^2 = \Gamma'$.

If $n = 3$ we adjoin the identical relation $X^3 = 1$ to the presentation for Γ. From $(al)^3 = (al)^2 = 1$ we derive that $al = 1$ or $a = l$. But then $(at)^3 = (lt)^3 = (lt)^2 = 1$ so $at = 1$ and $a = t$. Similarly $(ul)^3 = (ul)^2 = 1$ implies that $u = l$ and so Γ/Γ^3 is cyclic with generator a. But $a^3 = a^2 = 1$ implies $a = 1$ so the quotient is trivial. Therefore $\Gamma = \Gamma^3$. If $2 \nmid n$ the same argument shows that Γ/Γ^n is trivial so that $\Gamma = \Gamma^n$.

If $2|n$ but $6 \nmid n$ then $(n, 3) = 1$. If we adjoin the identical relation $X^n = 1$ to Γ we have from $(ual)^3 = (ual)^n = 1$ and $(n, 3) = 1$ that $ual = 1$ or $u = al$. Similarly $a = t$. Thus $\Gamma/\Gamma^n = \langle a, l; a^2 = l^2 = (al)^2 = 1\rangle$ and $|\Gamma : \Gamma^n| = 4$. Since $\Gamma^2 = \Gamma'$ is the only normal subgroup of index 4 we have $\Gamma^n = \Gamma^2$.

As in the case of the modular group the structure of Γ^{6n} is still unknown.

There are several nice corollaries which mirror conditions in M.

COROLLARY 5.1. $\Gamma^2 \cap \Gamma^3 = \Gamma'$.

COROLLARY 5.2. (i) $(\Gamma')^2 = \Gamma'$,
(ii) $(\Gamma')^3 = \Gamma''$.

The proofs of these are just easy calculations.

5. Congruence subgroups. Closely tied to the normal subgroups are the principal congruence subgroups $\Gamma(\alpha)$. Theorem 5 actually forces many normal subgroups to lie inside $\Gamma(1+i)$. Both Drillick [**10**] and Lubotzky [**9**] have shown that Γ has *noncongruence subgroups*—that is subgroups of finite index which do not contain a principal congruence subgroup. We use a different technique to give specific examples of such noncongruence subgroups. To do this we extend a theorem of Wohlfahrt.

If $G \subset \Gamma$ and $|\Gamma : G| < \infty$ we define the *level of* G to be the least positive integer n so that $G \supset N(t^n, u^n)$.

Clearly if $|\Gamma : G| < \infty$ then G has finite level since there cannot be infinitely many distinct cosets t^n, u^n. Thus if $|\Gamma : G| < \infty$ then G must contain the free abelian group of rank 2, $N(t^n, u^n)$ for some n and thus cannot be a free group. This is a consequence quite distinct from the modular group where all torsion-free subgroups are free. We thus have

THEOREM 6. *Γ has no free subgroups of finite index. If $|\Gamma : G| < \infty$ then G contains a free abelian subgroup of rank 2.*

Using the extended concept of level defined above a theorem of Wohlfahrt [**11**, p. 149] which characterizes congruence subgroups of M can be carried over to

THEOREM 7 (WOHLFAHRT). *Let $G \subset \Gamma$ be of finite index and level n. Then G is a congruence subgroup if and only if $G \supset \Gamma(n)$.*

PROOF. If $G \supset \Gamma(n)$ then G is a congruence subgroup. Conversely if the level of G is n and G is a congruence subgroup the result follows from

LEMMA. *If $G \subset \Gamma$ and $G \supset \Gamma(\alpha n)$ and $G \supset N(t^n, u^n)$ where n is an integer and $\alpha \in Z[i]$ then $G \supset \Gamma(n)$.*

PROOF. This is essentially the argument found in Newman [**11**, p. 149]. Since $G \supset N(t^n, u^n)$ this forces the matrices

$$\pm\begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix}, \quad \pm\begin{pmatrix} 1 & 0 \\ ny & 1 \end{pmatrix} \quad \text{and} \quad \pm\begin{pmatrix} 1+nz \\ nz^2 \end{pmatrix}, \quad \begin{pmatrix} -n \\ 1-nz \end{pmatrix}$$

to be in G for any Gaussian integers x, y, z. The proof then proceeds as in [**11**].

To complete the proof of Theorem 7, suppose that G has level n and is a congruence subgroup. Thus $G \supset \Gamma(\alpha)$ for some $\alpha \in Z[i]$ and therefore $G \supset \Gamma(\alpha n)$. Since the level is n, $G \supset N(t^n, u^n)$ and so $G \supset \Gamma(n)$ from the lemma.

Using Theorem 7 we obtain sufficient conditions on a subgroup for the subgroup to contain a normal noncongruence subgroup. Since Γ is an amalgamated free product it follows from the Karrass-Solitar subgroup theorems that any subgroup of Γ is an HNN group (see [**7**] for terminology). If $|\Gamma : G| < \infty$ the *free part rank of* G is the minimum of the ranks of the free part of G when G is represented as an HNN group. The ranks are all finite and the free part rank is at least as great as the rank of the abelianization. Then

THEOREM 8. *If $|\Gamma : G| < \infty$ and the free part rank of $G \geq 2$ then G contains a normal subgroup of finite index which is a noncongruence subgroup.*

PROOF. Since the free part rank is ≥ 2, G has 2 generators g_1, g_2 which generate a free subgroup of rank 2. For any integer k let G_k be the normal subgroup of G

consisting of all words W on the generators of G such that

$$e(W, g_1) \equiv e(W, g_2) \equiv 0 \mod k,$$

where $e(W, g)$ is the exponent sum of the generator g in the word W.

Then $G_k < G$ and G/G_k is abelian of order k^2—since G mod all generators of G except g_1 and g_2 is free of rank 2. Now suppose $|\Gamma\colon G| = m$ and n is the level of G. Then $|\Gamma\colon G_k| = mk^2$. If $g \in G$ then $g^k \in G_k$ so the level of G_k is either n or nk. We show that by a proper choice of k, G_k is a noncongruence subgroup.

First choose k to be a prime and greater than $n + 1$. Then $(mn, k) = 1$ and therefore $(mnk) \not\equiv 0 \mod k^2$. Thus $G_k \not\supset \Gamma(nk)$. Since the level of G_k is n or nk this implies from Wohlfahrt's theorem that G_k is not a congruence subgroup.

COROLLARY. *The two torsion-free normal subgroups of index* 24 *contain normal noncongruence subgroups in the manner constructed above.*

PROOF. From [**1**, p. 221] the free part rank of these subgroups is 2.

A formula of Karrass-Solitar [**6**] can be used to give another criterion for normal noncongruence subgroups. Let G_1, G_3 be the factors of Γ in the amalgamated free product decomposition and let M be the modular group. Recall that M is the amalgamated subgroup. The rank of the free part is given by

$$r(G) = |\Gamma : (G, M)| - |\Gamma : (G_1, M)| - |\Gamma : (G_2, M)| + 1$$

where $|\Gamma : (G, M)|$ is the double coset index. Then

COROLLARY. *If* $r(G) \geq 2$ *then* G *contains a normal noncongruence subgroup.*

The other normal subgroup of index 24—$N(l)$—is also closely tied to the congruence subgroups. It is in fact a type of principal congruence subgroup. If $\alpha \in Z[i]$ let $\overline{\Gamma(\alpha)} = \{$linear fractional transformations congruent to $z' = z \mod \alpha\}$. Then $N(l) = \overline{\Gamma(2)}$.

We close with a result again related to the situation in the modular group M. If n is an integer $t^n \in M(n)$ so $N(t^n) \subset M(n)$. It is known that $M(n) = N(t^n)$ if and only if $1 \leq n \leq 5$ [**11**]. In Γ we obtain

THEOREM 9. *If* $\alpha \in Z[i]$ *and* $|\alpha| < 16$ *(if* $\alpha = x + yi$ *then* $|\alpha| = x^2 + y^2$*) then*
(1) *If* $\alpha \in Z$ *so that* $\alpha = x$ *then* $\Gamma(\alpha) = N(t^x, u^x)$.
(2) *If* $\alpha \notin Z$ *so* $\alpha = x + yi$ *with* $y \neq 0$ *then* $\Gamma(\alpha) = N(t^{|\alpha|}, u^{|\alpha|}, t^x u^{-y})$.

PROOF. If $\alpha \in z$ then $N(t^x, u^y) \subset \Gamma(\alpha)$ while if $\alpha = x + yi$, $y \neq 0$,

$$N(t^{|\alpha|}, u^{|\alpha|}, t^x u^{-y}) \subset \Gamma(\alpha).$$

The proof is then done by computing and comparing the corresponding indices.

If $|\alpha| < 16$ then $\alpha = 1 \pm i, 2, 2 \pm i, 1 \pm 2i, 3 \pm i, 1 \pm 3i, 3 \pm 2i, 2 \pm 3i, 3$. For each case the size of the quotient $\Gamma/N(t^x, u^x)$ or $\Gamma/N(t^{|\alpha|}, u^{|\alpha|}, t^x u^{-y})$ was computed and compared to the index of the corresponding principal congruence subgroup.

If $\mu(\alpha)$ represents the index $|\Gamma\colon \Gamma(\alpha)|$ from [**11**, Theorem VII.6] we have

$$\mu(\alpha) = |\alpha|^3 \prod_{\pi|\alpha} \left(1 - \frac{1}{|\alpha|^2}\right)$$

where π runs over the primes dividing α. We will exhibit the calculations for $\alpha = 1 + i$ and 2. The others are handled analogously.

If $\alpha = 1 + i$ this is a prime and $|\alpha| = 2$. Therefore $\mu(1 + i) = 2^3(1 - 1/2^2) = 6$. Further

$$\Gamma/N(t^2, u^2, tu^{-1}) = \langle a, t \colon a^2 = (at)^3 = t^2 = 1 \rangle = S_3.$$

Therefore $|\Gamma/N(t^2, u^2, tu^{-1})| = 6$. Since $N(t^2, u^2, tu^{-1}) \subset \Gamma(1 + i)$ they must be the same.

If $\alpha = 2$ then $|\alpha| = 4$ and the only prime dividing 2 is $1 + i$. Therefore $\mu(2) = 4^3(1 - 1/2^2) = 48$. Further $|\Gamma/N(t^2, u^2)| = 48$ and since $N(t^2, u^2) \subset \Gamma(2)$ these must be the same. The sizes of the quotient groups were computed using Todd-Coxeter coset enumeration as implemented in the Cayley Group Theory Program.

We note that the theorem may be true for larger norms.

REFERENCES

1. A. M. Brunner, M. Frame, Y. W. Lee, and N. Wielenberg, *Classifying torsion-free subgroups of the Picard group*, Trans. Amer. Math. Soc. **282** (1984), 205–235.
2. A. M. Brunner, Y. W. Lee and N. Wielenberg, *Polyhedral groups and graph amalgamation products* (to appear).
3. B. Fine, *Fuchsian subgroups of the Picard group*, Canad. J. Math. **28** (1976), 481–486.
4. ——, *Congruence subgroups of the Picard group*, Canad. J. Math. **32** (1979), 1474–1481.
5. ——, *Fuchsian embeddings in the Bianchi groups*, Canad. J. Math. (in press).
6. A. Karrass and D. Solitar, *The subgroup of a free product of two groups with an amalgamated subgroup*, Trans. Amer. Math. Soc. **150** (1970), 227–255.
7. ——, *The subgroups of* HNN *groups and groups with one defining relation*, Canad. J. Math. **23** (1971), 627–643.
8. F. Klein and R. Fricke, *Vorlesungen uber der Theorie die Modulfunktionen*, Teubner, Leipzig, 1890.
9. A. Lobotzky, *Free quotients and the congruence kernel of* SL_2, J. Algebra **77** (1982), 411–418.
10. W. Magnus, *Non-Euclidean tesselations and their groups*, Academic Press, New York, 1974.
11. M. Newman, *Integral matrices*, Academic Press, New York, 1972.
12. ——, *Normal congruence subgroups of the modular group*, Amer. J. Math. **85** (1963), 419–427.
13. ——, *Free subgroups and normal subgroups of the modular group*, Illinois J. Math. **8** (1964), 262–265.
14. ——, *A complete description of normal subgroups of genus one of the modular group*, Amer. J. Math. **86** (1964), 17–24.
15. M. Takahasi, *Note on word subgroups in free product subgroups*, J. Inst. Polytech. Osaka City Univ. Ser. A. Math. **2** (1961), 13–18.

DEPARTMENT OF MATHEMATICS, FAIRFIELD UNIVERSITY, FAIRFIELD, CONNECTICUT 06430

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CALIFORNIA 93106