ISRAEL JOURNAL OF MATHEMATICS 91 (1995), 77–91

QUOTIENTS OF THE CONGRUENCE KERNELS OF SL_2 OVER ARITHMETIC DEDEKIND DOMAINS

BY

A. W. MASON

Department of Mathematics
University of Glasgow, Glasgow, G12 8QW, Scotland, U.K.
e-mail: AWM@MATHS.GLA.UK.AC

ABSTRACT

Let $\mathcal{C} = \mathcal{C}(C, P, k)$ be the coordinate ring of the affine curve obtained by removing a closed point P from a (suitable) projective curve C over a *finite* field k. Let $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$ be the principal congruence subgroup of $\mathrm{SL}_2(\mathcal{C})$ and $U_2(\mathcal{C}, \mathbf{q})$ be the subgroup generated by the all unipotent matrices in $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$, where $\mathbf{q}$ is a $\mathcal{C}$-ideal. In this paper we prove that, for all but finitely many $\mathbf{q}$, the quotient $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})/U_2(\mathcal{C}, \mathbf{q})$ is a free group of finite, *unbounded* rank.

Let $C(\mathrm{SL}_2(A))$ be the congruence kernel of $\mathrm{SL}_2(A)$, where A is an arithmetic Dedekind domain with only finitely many units. (e.g. $A = \mathcal{C}$ or $\mathbb{Z}$) and let G be any finitely generated group. From the above (and previous results) we deduce that the profinite completion of $G, \hat{G}$, is a homomorphic image of $C(\mathrm{SL}_2(A))$. This is related to previous results of Lubotzky and Mel'nikov.

Introduction

Let R be an integral domain and let $\mathbf{q}$ be an R-ideal. We put $\mathrm{SL}_n(R, \mathbf{q}) = \mathrm{Ker}(\mathrm{SL}_n(R) \to \mathrm{SL}_n(R/\mathbf{q}))$, where $n \geq 2$. A subgroup S of $\mathrm{SL}_n(R)$ is called a **congruence subgroup** iff $S \geq \mathrm{SL}_n(R, \mathbf{q}')$, for some *non-zero* $\mathbf{q}'$. Let $U_2(R, \mathbf{q})$ be the subgroup of $\mathrm{SL}_2(R)$ generated by the unipotent matrices contained in $\mathrm{SL}_2(R, \mathbf{q})$. It is clear that $U_2(R, \mathbf{q}) \geq \mathrm{NE}_2(R, \mathbf{q})$, where $\mathrm{NE}_2(R, \mathbf{q})$ is the normal

Received November 16, 1993 and in revised form March 24, 1994

subgroup of $\mathrm{SL}_2(R)$ generated by the elementary matrices contained in $\mathrm{SL}_2(R, \mathbf{q})$. We put $U_2(R, R) = U_2(R)$ and $\mathrm{NE}_2(R, R) = \mathrm{NE}_2(R)$.

Let C be a smooth projective curve over a finite field k, which is absolutely connected, and let P be a closed point of C. We denote by $\mathcal{C} = \mathcal{C}(C, P, k)$ the coordinate ring of the affine curve obtained by removing P from C. See [19, p.96]. (The simplest example is $\mathcal{C} = k[t]$, the polynomial ring over k.) In this paper we begin with the following decomposition theorem for $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$.

THEOREM A: *For all but finitely many* $\mathbf{q}$,

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q}) = V(\mathbf{q}) * F,$$

where

(i) F *is a free, non-cyclic group of finite (unbounded) rank,*

(ii) $V(\mathbf{q})$ *is a subgroup of* $U_2(\mathcal{C}, \mathbf{q})$ *generated by infinitely many elements of order* p, *where* $p = \mathrm{char}\, k$,

and

(iii) *the normal subgroup of* $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$ *generated by* $V(\mathbf{q})$ is $U_2(\mathcal{C}, \mathbf{q})$.

The following consequence is immediate.

COROLLARY B: *For all but finitely many* $\mathbf{q}$, $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})/U_2(\mathcal{C}, \mathbf{q})$ *is a free, non-cyclic group of finite (unbounded) rank.*

Our proof based on a special case of a fundamental theorem of Serre [19, Theorem 10, p. 119]. Serre's theorem (which generalises an earlier result of Nagao [13] for the case $\mathcal{C} = k[t]$) is one of the first important applications of the Bass–Serre theory of groups acting on trees and enables him to solve the congruence subgroup problem for $\mathrm{SL}_2(\mathcal{C})$. (See [19, Theorem 12, p.124].) Radtke [16], [17] has provided a more elementary proof of this special case. The above corollary extends two previous results of the author. For the simplest case $\mathcal{C} = k[t]$ the corollary is proved in [7, Theorem 1.3]. (We note that since $k[t]$ is a principal ideal domain, $U_2(k[t], \mathbf{q}) = \mathrm{NE}_2(k[t], \mathbf{q})$.) In addition it is known [8, Corollary 2.3] that, for all but finitely many $\mathbf{q}$, the group $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})/\mathrm{NE}_2(\mathcal{C}, \mathbf{q})$ has a free, non-cyclic quotient. The existence of subgroups finite index in $\mathrm{SL}_2(\mathcal{C})$ (like $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$) with free quotients was first proved by Lubotzky [6]. However Lubotzky's results make no mention of unipotent matrices.

It is of interest to compare the above with other corresponding results in the class of groups $\mathrm{SL}_n(A)$, where A is a *Dedekind ring of arithmetic type* [2, p.83] and $n \geq 2$. By a classical theorem of Dirichlet it follows that A^*, the set of units of A, is finite if and only if (i) $A = \mathcal{C}$, (ii) $A = \mathbb{Z}$, the ring of rational integers, or (iii) $A = \mathcal{O}$, the ring of integers of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$, where $\mathbb{Q}$ is the set of rational numbers and d is a square-free positive integer. The groups $\mathrm{SL}_2(A)$, where $A = \mathbb{Z}, \mathcal{O}$ or $\mathcal{C}$, have a completely different normal subgroup structure from that of $\mathrm{SL}_n(A)$, where $n \geq 3$ or A^* is infinite. From results of Bass, Milnor and Serre [2], together with those of Liehl [5] and Vaserstein [20] it follows that, when A^* is infinite or $n \geq 3$, every non-central normal subgroup of $\mathrm{SL}_n(A)$ is of finite index. It follows that no non-central, normal subgroup N of such $\mathrm{SL}_n(A)$ has a free (even infinite cyclic) quotient (since the abelianization of N is then *finite*.) For these cases $\mathrm{SL}_n(A)$ has only countably many normal subgroups. For $\mathrm{SL}_2(A)$, when $A = \mathbb{Z}, \mathcal{O}$ or $\mathcal{C}$, the situation is completely different. The existence of subgroups of finite index with free, non-cyclic quotients ensures, by virtue of [14, Lemma], that $\mathrm{SL}_2(A)$ is *SQ*-universal. (See [4], [6], [15].) Consequently ([14, p.4]) $\mathrm{SL}_2(A)$ has uncountably many normal subgroups. Unlike the above Corollary the results in [4], [6], [15] are not concerned with unipotent matrices. Results corresponding to our Corollary for the modular group, $\mathrm{SL}_2(\mathbb{Z})$, and the Bianchi groups, $\mathrm{SL}_2(\mathcal{O})$, can be found in [9] and [11], respectively.

The fact that $\mathrm{SL}_2(A, \mathbf{q})/\mathrm{NE}_2(A, \mathbf{q})$, where $A = \mathbb{Z}$, $\mathcal{O}$ or $\mathcal{C}$, has a finitely generated free quotient of unbounded rank has implications for the congruence subgroup structure of $\mathrm{SL}_2(A)$. It is known [10, Theorem 3.6] that, for these cases, every finitely generated group G can be realised as a quotient C/S, where S is a subgroup of $\mathrm{SL}_2(A)$ and C is the *smallest* congruence subgroup of $\mathrm{SL}_2(A)$ containing S. (In [10] C is called the **congruence hull** of S.) Serre [18, p.491] has introduced a profinite group $C(\mathrm{SL}_2(A))$, called the **congruence kernel** of $\mathrm{SL}_2(A)$, as a "measure" of the number of non-congruence subgroups in $\mathrm{SL}_2(A)$ and he proves that $C(\mathrm{SL}_2(A))$ is infinite if and only if A^* is finite.

Let $\hat{F}_\omega$ be the free profinite group on countably many generators. Lubotzky [6] and Mel'nikov [12] have proved that $C(\mathrm{SL}_2(\mathbb{Z})) \cong \hat{F}_\omega$ and Lubotzky [6] has proved that $C(\mathrm{SL}_2(A))$ has a closed subgroup isomorphic to $\hat{F}_\omega$, when $A = \mathcal{O}$ or $\mathcal{C}$. From our results on congruence hulls we deduce the following.

THEOREM C: *Let G be any finitely generated group. When $A = \mathbb{Z}$, $\mathcal{O}$ or $\mathcal{C}$,* *there exists a continuous epimorphism*

$$\psi\colon C(\mathrm{SL}_2(R)) \to \hat{G},$$

where $\hat{G}$ is the profinite completion of G.

When $A = \mathbb{Z}$, Theorem C is implied by the results of Lubotzky [6] and Mel'nikov [12]. When $A = \mathcal{O}$ or $\mathcal{C}$, Theorem C implies the results of Lubotzky [6].

The author is grateful to Professor A. Lubotzky for a stimulating conversation which has led to much of this paper.

1. Groups acting on trees

As stated above this paper is based on a decomposition theorem of Serre [19, Theorem 10, p. 119] whose proof depends upon the Bass–Serre theory of groups acting on trees. Consequently we require a number of results from this theory. For our purposes the most convenient reference is Serre's book [19].

We begin by recalling some basic definitions. Let Y be a connected, oriented graph with vertex and edge sets $\operatorname{vert} Y$ and $\operatorname{edge} Y$, respectively. To each edge e there corresponds another edge $\bar{e}$ ($\neq e$), the so-called **inverse** of e. Let (G, Y) be a **graph** of **groups** [19, Definition 8, p. 37]. This consists of the graph Y together with groups G_v and G_e, for each $v \in \operatorname{vert} Y$ and each $e \in \operatorname{edge} Y$. In addition, for each $e \in \operatorname{edge} Y$, $G_e = G_{\bar{e}}$ and there exist monomorphisms from G_e into G_u and G_v, where u, v are the end-points of e. Associated with (G, Y) is its **fundamental group**, $\pi_1(G, Y, T)$ where T is a maximal subtree of Y. (See [19, p. 42].) It can be shown [19, Proposition 20, p. 44] that $\pi_1(G, Y, T)$ is independent of the particular choice of T and consequently it is often simply denoted by $\pi_1(G, Y)$. We require a number of results for $\pi_1(G, Y)$, where (i) Y is a finite tree or (ii) Y and all G_v are finite.

Definition: Let H be a subgroup of a group K and let $x, y \in K$. We put

$$x^y = yxy^{-1} \text{ and } H^x = xHx^{-1}.$$

Let H^K denote the **normal** subgroup of K generated by H.

THEOREM 1.1: *With the above notation, let T be a finite tree with $V = \operatorname{vert} T$, $E = \operatorname{edge} T$, and let (G,T) be a graph of groups. Let N be a normal subgroup of finite index in $\Gamma = \pi_1(G,T)$ such that*

$$N \cap G_e = \{1\}, \qquad \text{for all } e \in E.$$

Now let S_v be a (finite) system of left coset representatives for $\Gamma/N\cdot G_v$, where $v \in V$, and let

$$N(v) = \mathop{\ast}_{g\in S_v} (N \cap G_v)^g.$$

Then

$$N = \left(\mathop{\ast}_{v\in V} N(v)\right) * F,$$

where

(i) *F is a free group of finite rank,*

and

(ii) $(N(v))^N = (N \cap G_v)^\Gamma$,

for all $v \in V$.

Proof: It is part of the basic theory of groups acting on trees that Γ (and hence N) acts (without inversion) on a tree X, where

$$\operatorname{vert} X = \bigsqcup_{v\in V} (\Gamma/G_v) \text{ and } \operatorname{edge} X = \bigsqcup_{e\in E} (\Gamma/G_e).$$

(In X the edge "gG_e" joins the vertices "gG_u" and gG_v, where $u, v \in V$ are the end-points of $e \in E$.) See [19, Theorem 12, p. 52]. Let $X_\circ$ be the quotient graph $N\backslash X$. Then it is clear that

$$\operatorname{vert} X_\circ = \bigsqcup_{v\in V} (\Gamma/N\cdot G_v) \text{ and } \operatorname{edge} X_\circ = \bigsqcup_{e\in E} (\Gamma/N\cdot G_e).$$

By one of the fundamental theorems of the theory of groups acting on trees [19, Theorem 13, p. 55],

$$N = \pi_1(N^*, X_\circ),$$

where N^* assigns to the vertex "$gN\cdot G_v$" (resp. the edge "$gN\cdot G_e$") the group $(N\cap G_v)^g$ (resp. $N \cap (G_e)^g$), where $g \in \Gamma$. (We note that $N \cap (G_v)^g$ (resp. $N\cap(G_e)^g$) is the stabilizer in N of the vertex "gG_v" (resp. edge "gG_e") in X.) From the above hypothesis, we have

$$N \cap (G_e)^g = (N \cap G_e)^g = \{1\}, \qquad \text{for all } e \in E \quad \text{and all } g \in \Gamma.$$

It follows from the definition [19, p. 42] of $\pi_1(N^*, X_\circ)$ that

$$N = \left(\mathop{\ast}_{v \in V} N(v) \right) * F,$$

where F is the fundamental group (in the usual sense) of the (connected) graph $X_\circ$. Since $X_\circ$ is finite, F is a free group of finite rank. Part (i) follows.

For part (ii) it suffices to show that $gng^{-1} \in (N(v))^N$, for all $g \in \Gamma$ and all $n \in N \cap G_v$. Now

$$g = n_1 g_1 x,$$

for some $n_1 \in N, g_1 \in S_v$ and $x \in G_v$. Then

$$gng^{-1} = n_1(g_1(xnx^{-1})g_1^{-1})n_1^{-1} \in (N(v))^N,$$

since $xnx^{-1} \in N \bigcap G_v$. ∎

Remarks: (i) From the proof of Theorem 1.1 it follows that the rank of F is

$$1 + \frac{1}{2}|\operatorname{edge} X_\circ| - |\operatorname{vert} X_\circ| = 1 + \frac{1}{2}\sum_{e \in E} |\Gamma\colon N \cdot G_e| - \sum_{v \in V} |\Gamma\colon N \cdot G_v|.$$

(ii) Theorem 1.1 is also valid if T is a finite graph.

THEOREM 1.2: *Let Y be a finite connected graph and let (G,Y) be a graph of groups such that G_v is finite, for all $v \in \operatorname{vert} Y$. Let N be a normal subgroup of finite index in $\Gamma = \pi_1(G,Y)$, such that*

$$N \cap G_v = \{1\}, \qquad \text{for all } v \in \operatorname{vert} Y.$$

Then N is a free group of finite rank.

Proof: By the hypothesis,

$$N \cap (G_v)^g = (N \cap G_v)^g = \{1\},$$

for all $g \in \Gamma$. The result follows from [19, Lemma 8, p. 121]. ∎

Remark: By [19, Exercise 3, p. 123] it follows that the rank of N is

$$1 + \frac{\mu}{2}\sum_{e \in E} |G_e|^{-1} - \mu \sum_{v \in V} |G_v|^{-1},$$

where $\mu = |\Gamma\colon N|$, $E = \operatorname{edge} Y$ and $V = \operatorname{vert} Y$.

2. Principal results

Some preliminaries are required before describing Serre's theorem [19, Theorem 10, p. 119]. We shall make use of some results from Radtke's simplified proof [16].

We can represent (uniquely) the elements of the projective line $P_1(K)$, over K, where K is the quotient field of $\mathcal{C}$, by pairs (1,0) and $(s,1)$, where $s = a/b$, with $a, b \in \mathcal{C}, b \neq 0$. Clearly $\mathrm{GL}_2(\mathcal{C})$ acts on $P_1(K)$. Let Γ_∞ and Γ_s be the stabilizer of (1,0) and $(s,1)$ in $\mathrm{GL}_2(\mathcal{C})$, respectively.

LEMMA 2.1: (i)

$$\Gamma_\infty = \left\{ \begin{bmatrix} \alpha & b \\ 0 & \beta \end{bmatrix} : \alpha, \beta \in k^*, b \in \mathcal{C} \right\}.$$

(ii)

$$\Gamma_s = \left\{ \begin{bmatrix} \alpha + sx & (\beta - \alpha)s - s^2 x \\ x & \beta - sx \end{bmatrix} : \alpha, \beta \in k^*, \right.$$
$$\left. x \in \mathcal{C} \cap (\mathcal{C}s^{-1}) \cap (\mathcal{C}s^{-2} + (\beta - \alpha)s^{-1}) \right\}.$$

Proof: See [17, Lemma 2 (ii), (iii)]. ∎

Let $I(\mathcal{C})$ be the ideal class group of $\mathcal{C}$. It is well-known that $I(\mathcal{C})$ is *finite*, of order $h + 1$, say, where $h \geq 0$. The following result is an immediate consequence of the theory of ideals in Dedekind rings. (See [17, Lemma 2(i)].)

LEMMA 2.2: *There exist bijections*

$$P^1(K) \backslash \mathrm{SL}_2(\mathcal{C}) \leftrightarrow P^1(K) \backslash \mathrm{GL}_2(\mathcal{C}) \leftrightarrow I(\mathcal{C}).$$

From now on we represent the elements of $I(\mathcal{C})$ by the pairs (1,0), $(s_1, 1), \ldots, (s_h, 1)$ and for simplicity we denote these by $\infty, s_1, \ldots, s_h$, respectively, where $s_1, \ldots, s_h \in K$.

Let U be a unipotent matrix in $\mathrm{GL}_2(\mathcal{C})$. Then $\mathrm{tr}\, U = 2$, $\det U = 1$ and so either

$$U = \begin{bmatrix} 1 + xs & -s^2 x \\ x & 1 - xs \end{bmatrix} \quad \text{or} \quad U = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix},$$

for some $s \in K, x \in \mathcal{C} \cap (\mathcal{C}s^{-1}) \cap (\mathcal{C}s^{-2})$ and $y \in \mathcal{C}$.

LEMMA 2.3: *Let*

$$U = \begin{bmatrix} 1 + xs & -s^2 x \\ x & 1 - xs \end{bmatrix},$$

as above, and let $s = a/b$, *where* $a, b \in \mathcal{C}, b \neq 0$.

(i) *If* $a\mathcal{C} + b\mathcal{C}$ *is a principal* $\mathcal{C}$*-ideal, then*

$$U^g \in \Gamma_\infty,$$

for some $g \in \mathrm{SL}_2(\mathcal{C})$.

(ii) *Otherwise,*

$$U^g \in \Gamma_{s_i},$$

for some unique i, *where* $1 \leq i \leq h$, *and* $g \in \mathrm{SL}_2(\mathcal{C})$.

Proof: Obvious from Lemmas 2.1 and 2.2. ∎

We are now in a position to describe Serre's theorem.

Notation: We put $\Gamma_i = \Gamma_{s_i}$, where $1 \leq i \leq h$.

THEOREM 2.4 (Serre): *There exists a finite tree* T *with* $h+2$ *vertices,* $v_\circ, v_\infty, v_1, \ldots, v_h$ *and (oriented) edges* $e_\infty, e_1, \ldots, e_h$, *where* e_α *begins at* $v_\circ$ *and ends at* $v_\alpha, (\alpha \in \{\infty, 1, \ldots, h\})$, *together with a graph of groups* (G, T) *such that*

$$\mathrm{GL}_2(\mathcal{C}) = \pi_1(G, T),$$

with

$$G_{v_\circ} = \Lambda, \textit{say}, \textit{ and } G_{v_\alpha} = \Gamma_\alpha \quad (\alpha \in \{\infty, 1, \ldots, h\}).$$

In addition there exists a finite graph Y *and a graph of groups* (L, Y), *where each* L_v *is finite* ($v \in \mathrm{vert}\, Y$), *such that*

$$\Lambda = \pi_1(L, Y).$$

Moreover, for each $\alpha \in \{\alpha, 1, \ldots, h\}$,

$$G_{e_\alpha} = L_v, \qquad \textit{for some } v \in \mathrm{vert}\, Y.$$

Proof: For the first part see [19, Theorem 10, p. 119]. (Radtke [16] has obtained a simpler proof.)

For the second part the definition of Λ as the fundamental group of a graph of groups can be found in [19, p. 119]. By [19, Corollary 4, p. 108], Y is finite. Serre states [19, p. 124] that each L_v is finite. This follows from [19, Proposition 2, p. 76], together with [1, Theorem 2, p. 230]. For the final assertion see [19, p. 118]. ∎

Notation: Let F_t denote the free group of rank t, where $t \geq 0$.

THEOREM 2.5:

(a) *For all but finitely many $\mathcal{C}$-ideals* $\mathbf{q}$,

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q}) = V(\mathbf{q}) * F_r,$$

where

(i) $V(\mathbf{q})$ *is generated by infinitely many unipotent matrices each of order* $p = \operatorname{char} k$,

(ii) $(V(\mathbf{q}))^S = U_2(\mathcal{C}, \mathbf{q})$, *where* $S = \mathrm{SL}_2(\mathcal{C}, \mathbf{q})$,

(iii) $r = r(\mathbf{q})$ *is at least 2.*

(b) *Let* $\mathbf{p}$ *be a prime $\mathcal{C}$-ideal. Then*

$$r(\mathbf{p}) \to \infty \quad \text{as } |\mathcal{C}\colon \mathbf{p}| \to \infty.$$

Proof: With the notation of Theorem 2.4, let S be the (finite) set of all matrices, apart from I_2, in L_v, where $v \in \operatorname{vert} Y$. For each $A \in S$ choose one *non-zero* entry α, say, from those of $A - I_2$, and let $S_\circ$ be the set of all such α. Now let $\mathbf{q} \neq \{0\}$,

$$S_1 = \{\mathbf{q}\colon \mathbf{q} \neq \{0\}, \mathbf{q} \cap S_\circ = \emptyset\}.$$

Clearly S_1 contains all but finitely many $\mathcal{C}$-ideals. It is clear that $\mathcal{C} \notin S_1$.

Now choose $\mathbf{q} \in S_1$. Then $|\,\mathrm{GL}_2(\mathcal{C})\colon \mathrm{SL}_2(\mathcal{C}, \mathbf{q})| < \infty$ and

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q}) \cap G_e = \{1\},$$

for all $e \in \operatorname{edge} T$, by Theorem 2.4. Let S_β be a system of left coset representatives for $\mathrm{GL}_2(\mathcal{C}) / \mathrm{SL}_2(\mathcal{C}, \mathbf{q}) \cdot G_{v_\beta}$, where $\beta \in \{\infty, 0, 1, \ldots, h\}$. We put

$$\Delta_\circ = \mathop{\ast}_{g \in S_\circ} (\Lambda \cap \mathrm{SL}_2(\mathcal{C}, \mathbf{q}))^g,$$

and

$$\Delta_\beta = \mathop{\ast}_{g \in S_\beta} (\Gamma_\beta \cap \mathrm{SL}_2(\mathcal{C}, \mathbf{q}))^g \quad (\beta \in \{\infty, 1, \ldots, h\}).$$

Then, by Theorem 1.1 applied to Theorem 2.4,

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q}) = \left(\mathop{\ast}_{\beta \neq 0} \Delta_\beta \right) * \Delta_\circ * F_t,$$

for some t.

Now $\Lambda \cap \mathrm{SL}_2(\mathcal{C}, \mathbf{q})$ is a normal subgroup of finite index in Λ and by our choice of $\mathbf{q}$

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q}) \cap L_v = \{1\},$$

for all $v \in \operatorname{vert} Y$. We now apply Theorem 1.2 to Theorem 2.4 to conclude that $\Lambda \cap \mathrm{SL}_2(\mathcal{C}, \mathbf{q})$ is a free group of finite rank. It follows that

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q}) = \left(\mathop{\ast}_{\beta \neq 0} \Delta_\beta \right) * F_r,$$

for some r.

By Lemma 2.1,

$$\Gamma_\infty \cap \mathrm{SL}_2(\mathcal{C}, \mathbf{q}) = \left\{ \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} : q \in \mathbf{q} \right\}$$

and

$$\Gamma_i \cap \mathrm{SL}_2(\mathcal{C}, \mathbf{q}) = \left\{ \begin{bmatrix} 1 + qs_i & -s_i^2 q \\ q & 1 - qs_i \end{bmatrix} : q \in \mathbf{q} \cap (\mathbf{q}s_i^{-1}) \cap (\mathbf{q}s_i^{-2}) \right\},$$

where $1 \leq i \leq h$. Let

$$V(\mathbf{q}) = \mathop{\ast}_{\beta \neq 0} \Delta_\beta .$$

Since $\mathrm{SL}_2(\mathcal{C})$ is infinitely generated [19, Corollary, p. 119] so is $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$. Hence $V(\mathbf{q})$ is infinitely generated. The rest of part(i) and part (ii) follows from Lemma 2.3.

It has been shown [8, Corollary 2.3] that there is a constant $c_\circ$ such that, whenever $|\mathcal{C}\colon \mathbf{q}| > c_\circ$, the group $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$ has a quotient F_u, for some $u \geq 2$. Clearly the set of ideals for which $|\mathcal{C}\colon \mathbf{q}| \leq c_\circ$ is finite. Let T_1 be the set of all ideals for which $|\mathcal{C}\colon \mathbf{q}| > c_\circ$ and let $T_\circ = T_1 \cap S_1$. For each $\mathbf{q} \in T_\circ$, from the above,

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q}) = V(\mathbf{q}) * F_r,$$

and $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})$ has a quotient F_u, where $u \geq 2$. Now $V(\mathbf{q})$ is generated by element of finite order and so F_r maps onto F_u. Thus $r \geq u \geq 2$. Part(iii) follows.

The remainder follows from part(iii) of the proof of [10, Theorem 3.6] where it is shown that $\mathrm{SL}_2(\mathcal{C}, \mathbf{p})$ has a free quotient of rank $t(\mathbf{p})$ and that $t(\mathbf{p}) \to \infty$, as $|\mathcal{C}\colon \mathbf{p}| \to \infty$. It is clear that all but finitely many prime ideals $\mathbf{p} \in S_1$. For any such $\mathbf{p}$, from the above,

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{p}) = V(\mathbf{p}) * F_{r_\circ},$$

where $r_\circ = r(\mathbf{p})$ and $r_\circ \geq t(\mathbf{p})$. Hence $r_\circ \to \infty$ as $|\mathcal{C}: \mathbf{p}| \to \infty$. ∎

The following consequence is immediate.

COROLLARY 2.6: *For all but finitely many ideals* $\mathbf{q}$,

$$\mathrm{SL}_2(\mathcal{C}, \mathbf{q})/U_2(\mathcal{C}, \mathbf{q}) \cong F_r,$$

where $r \geq 2$. *Further,* r *is unbounded.*

As an illustration of our results consider the simplest case $\mathcal{C} = k[t]$. Now $k[t]$ is a Euclidean ring and hence a principal ideal domain. In Theorem 2.4 the tree T has only two vertices with vertex groups

$$\Lambda = \mathrm{SL}_2(k) \quad \text{and} \quad \Gamma_\infty = \left\{ \begin{bmatrix} \alpha & a \\ 0 & \beta \end{bmatrix} : \alpha, \beta \in k^*, a \in k[t] \right\}$$

and single edge group

$$\mathrm{SL}_2(k) \cap \Gamma_\infty = \left\{ \begin{bmatrix} \alpha & \gamma \\ 0 & \alpha^{-1} \end{bmatrix} : \alpha \in k^*, \gamma \in k \right\}.$$

Serre's theorem is a generalisation of an earlier result of Nagao [13].

Since $k[t]$ is a principal ideal domain, by Lemma 2.3(i),

$$U_2(k[t], \mathbf{q}) = \mathrm{NE}_2(k[t], \mathbf{q}),$$

for all $\mathbf{q}$. In the proof of Theorem 2.5 for this case

$$S_1 = \{\mathbf{q} \colon \mathbf{q} \neq \{0\}, k[t]\}.$$

In an earlier paper [7, Corollary 1.4] it is proved that

$$\mathrm{SL}_2(k[t], \mathbf{q})/U_2(k[t], \mathbf{q}) \cong F_r,$$

where $r \geq 2$, when $\mathbf{q} \neq \{0\}, k[t]$ and $\mathbf{q}$ is *not* generated by a polynomial of degree 1. In the excluded cases $\mathrm{SL}_2(k[t], \mathbf{q}) = U_2(k[t], \mathbf{q})$. This shows that Corollary 2.6 does not always hold for all non-zero ideals.

For some $\mathcal{C}$, however, Corollary 2.6 can hold for all $\mathbf{q} \neq \{0\}$. Serre [19, 2.4.2, p. 113] gives an example for which $\mathrm{SL}_2(\mathcal{C}, \mathbf{q})/U_2(\mathcal{C}, \mathbf{q})$ maps onto F_3, for all $\mathbf{q} \neq \{0\}$ (including $\mathbf{q} = \mathcal{C}$).

3. Congruence kernels

The congruence kernel was first introduced by Serre [18] as part of his global approach to the congruence subgroup problem for $\mathrm{SL}_2(A)$, where A is a Dedekind ring of arithmetic type [2, p. 83]. Serre's method is based on the theory of profinite groups. We recall some basic definitions. The group $\mathrm{SL}_2(A)$ is a topological group, where either (a) the normal subgroups of finite index or (b) the normal congruence subgroups are bases for the neighbourhoods of the identity. Let $\hat{\mathrm{SL}}_2(A)$ and $\tilde{\mathrm{SL}}_2(A)$ be the completions of $\mathrm{SL}_2(A)$ with respect to the topologies (a) and (b), respectively. Then $\hat{\mathrm{SL}}_2(A)$ and $\tilde{\mathrm{SL}}_2(A)$ are profinite groups containing an embedding of $\mathrm{SL}_2(A)$. For each subgroup S of $\mathrm{SL}_2(A)$ let $\hat{S}$ (resp. $\tilde{S}$) be the closure in $\hat{\mathrm{SL}}_2(A)$ (resp. $\tilde{\mathrm{SL}}_2(A)$) of the embedding of S in $\hat{\mathrm{SL}}_2(A)$ (resp. $\tilde{\mathrm{SL}}_2(A)$).

There is a continuous epimorphism

$$\phi\colon \hat{\mathrm{SL}}_2(A) \to \tilde{\mathrm{SL}}_2(A).$$

The kernel of ϕ is called the **congruence kernel** of $\mathrm{SL}_2(A)$ and is denoted by $C(\mathrm{SL}_2(A))$. Serre [18, Théorème 2, p. 498, Corollaire 2, p. 506] has shown that $C(\mathrm{SL}_2(A))$ is *finite* if and only if A^* is *infinite*. (When A^* is infinite, $C(\mathrm{SL}_2(A))$ is isomorphic to the (finite) group of roots of unity in A.) When A^* is finite, i.e. when $A = \mathbb{Z}$, $\mathcal{O}$ or $\mathcal{C}$, Mel'nikov [12] and Lubotzky [6] have thrown more light on the actual structure of $C(\mathrm{SL}_2(A))$.

In this section we show how results like Corollary 2.6 and [10, Theorem 3.6] prove that $C(\mathrm{SL}_2(A))$, where $A = \mathbb{Z}, \mathcal{O}$ or $\mathcal{C}$, has many infinite quotients. This approach to proving that $C(\mathrm{SL}_2(A))$ is infinite is different to that of Serre. In addition our results provide an alternative proof of Lubotzky's results [6, Theorem B(ii)] for $A = \mathcal{O}$ and $\mathcal{C}$.

THEOREM 3.1: *Let $A = \mathbb{Z}$, $\mathcal{O}$ or $\mathcal{C}$. Let G be any finitely generated group. There exist subgroups S, T of $\mathrm{SL}_2(A)$ with the following properties:*

(i) *$S \lhd T$;*

(ii) *$T = \mathrm{SL}_2(A) \cap \tilde{S}$;*

(iii) *T is a congruence subgroup;*

(iv) *$T/S \cong G$.*

Proof: The proof of this result is contained in [10, Theorem 3.6]. For completeness we indicate how Corollary 2.6 implies the result for the case $A = \mathcal{C}$. For the cases $A = \mathbb{Z}$ and $\mathcal{O}$, see [10, § 3].

By Corollary 2.6 there exists a $\mathcal{C}$-ideal $\mathbf{q}$ such that

$$\mathrm{SL}_2(\mathcal{C},\mathbf{q})/S \cong G,$$

where S is a (normal) subgroup of $\mathrm{SL}_2(\mathcal{C},\mathbf{q})$ containing $U_2(\mathcal{C},\mathbf{q})$. Since $\mathcal{C}$ is a Dedekind domain, the intersection of all congruence subgroups of $\mathrm{SL}_2(\mathcal{C})$ containing S is $\mathrm{SL}_2(\mathcal{C},\mathbf{q})$ (the so-called **congruence hull** [10] of S.) Take $T = \mathrm{SL}_2(\mathcal{C},\mathbf{q})$. ∎

Let H be any group. We denote by $\hat{H}$ the usual profinite completion of H, i.e. the completion of H with respect to the topology for which its normal subgroups of finite index form a basis for the neighbourhoods of the identity.

THEOREM 3.2: *Let G be any finitely generated group. When $A = \mathbb{Z}$, $\mathcal{O}$ or $\mathcal{C}$, there exists a continuous epimorphism*

$$\psi\colon C(\mathrm{SL}_2(A)) \to \hat{G}.$$

Proof: We put $C = C(\mathrm{SL}_2(A))$. Let S,T be as in Theorem 3.1. We identify them with their embeddings in $\hat{\mathrm{SL}}_2(A)$ and $\tilde{\mathrm{SL}}_2(A)$. By Theorem 3.1(ii),

$$\tilde{S} = \tilde{T}.$$

It follows that

$$C\cdot\hat{S} = C\cdot\hat{T}.$$

By Theorem 3.1(iii) we have $C \le \hat{T}$ and so

$$C/C\cap\hat{S} \cong \hat{T}/\hat{S}.$$

Now $|\hat{\mathrm{SL}}_2(A)\colon \hat{T}| < \infty$ and so the topology induced on $\hat{T}$ by $\hat{\mathrm{SL}}_2(A)$ is the usual profinite topology on $\hat{T}$. By [3, Proposition 21, p. 234],

$$C/C\cap\hat{S} \cong \hat{G}. \quad ∎$$

From Theorem 3.2 it follows in particular that $C(\mathrm{SL}_2(A))$, where $A = \mathbb{Z}$, $\mathcal{O}$ or $\mathcal{C}$, maps continuously onto $\hat{F}_t$, the free profinite group on t generators, for all t.

Let $\hat{F}_\omega$ denote the free profinite group on countably many generators. This is the completion of the free group of countably infinite rank with respect to the topology for which the basis for the neighbourhoods of the identity consists of those normal subgroups of finite index which contain all but finitely many elements of a given free generating set. Mel'nikov [12] has proved that

$$C(\mathrm{SL}_2(\mathbb{Z})) \cong \hat{F}_\omega.$$

For the case $A = \mathbb{Z}$, Corollary 3.2 is a consequence of this result. We conclude with an alternative proof of a result first established by Lubotzky [6, Theorem B(ii)].

COROLLARY 3.3: *Let $A = \mathcal{O}$ or $\mathcal{C}$. Then $C(\mathrm{SL}_2(A))$ has a closed subgroup isomorphic to $\hat{F}_\omega$.*

Proof: By Corollary 3.2 there is a continuous epimorphism

$$\psi\colon C(\mathrm{SL}_2(A)) \to \hat{F}_r,$$

for all r. Since $\hat{F}_r$ is a free profinite group ψ splits and so there exists a closed subgroup N of $C(\mathrm{SL}_2(A))$ such that

$$N \cong \hat{F}_r.$$

We now apply Lubotzky's result [6, Theorem 2.1(a)] to conclude that N and hence $C(\mathrm{SL}_2(A))$ has a closed subgroup isomorphic to $\hat{F}_\omega$. ∎

ACKNOWLEDGEMENT: The referee has pointed out that parts (a)(i) and (a)(ii) of Theorem 2.5 are a special case of a more general result of A. Lubotzky in *Lattices in rank one Lie groups over local fields*, Geometric and Functional Analysis 1 (1991), 405–431. (See Theorem 7.1, p. 427.)

References

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Nelson, London, 1968.

[2] H. Bass, J. Milnor and J-P. Serre, *Solution of the congruence subgroup problem for* $\mathrm{SL}_n (n \geq 3)$ *and* $\mathrm{Sp}_{2n} (n \geq 2)$, Publications de l'Institute de Mathématiques des Hautes Études Scientifiques **33** (1967), 59–137.

[3] N. Bourbaki, *General Topology, Part 1*, Addison-Wesley, London, 1966.

[4] F.J. Grunewald and J. Schwermer, *Free non-abelian quotients of* SL_2 *over orders of imaginary quadratic number fields*, Journal of Algebra **69** (1981), 298–304.

[5] B. Liehl, *On the groups* SL_2 *over order of arithmetic type*, Journal für die reine und angewandte Mathematik **323** (1981), 153–171.

[6] A. Lubotzky, *Free quotients and the congruence kernel of* SL_2, Journal of Algebra **77** (1982), 411–418.

[7] A. W. Mason, *Anomalous normal subgroups of* $SL_2(K[x])$, The Quarterly Journal of Mathematics. Oxford **36** (1985), 345–358.

[8] A. W. Mason, *Free quotients of congruence subgroups of* SL_2 *over a Dedekind ring of arithmetic type contained in a function field*, Mathematical Proceedings of the Cambridge Philosophical Society **101** (1987), 421–429.

[9] A. W. Mason, *Non-standard, normal subgroups and non-normal, standard subgroups of the modular group*, Canadian Mathematical Bulletin **32** (1989), 109–113.

[10] A. W. Mason, *Congruence hulls in* SL_n, Journal of Pure and Applied Algebra **89** (1993), 255–272.

[11] A. W. Mason and R. W. K. Odoni, *Non-normal, standard subgroups of the Bianchi groups*, in preparation.

[12] O. V. Mel'nikov, *The congruence kernel of* $SL_2(\mathbb{Z})$, Soviet Mathematics. Doklady **17** (1976), 867–870.

[13] H. Nagao, *On* $GL(2, K[x])$, J. Poly. Osaka Univ. **10** (1959), 117–121.

[14] P. M. Neumann, *The SQ-universality of some finitely presented groups*, Journal of the Australian Mathematical Society **16** (1973), 1–6.

[15] M. Newman, *Free subgroups and normal subgroups of the modular group*, Illinois Journal of Mathematics **8** (1964), 262–265.

[16] W. Radtke, *Diskontinuierliche arithmetische Gruppen im Funktionenkörperfall*, Dissertation, Bochum, 1984.

[17] W. Radtke, *Diskontinuierliche arithmetische Gruppen im Funktionenkörperfall*, Journal für die reine und angewandte Mathematik **363** (1985), 191–200.

[18] J-P. Serre, *Le problème des groupes de congruence pour* SL_2, Annals of Mathematics **92** (1970), 489–527.

[19] J-P. Serre, *Trees*, Springer-Verlag, Berlin, Heidelberg, New York, 1980.

[20] L. N. Vaserstein, *On the group* SL_2 *over a Dedekind rings of arithmetic type*, Mathematics of the USSR-Sbornik **18** (1972), 321–332.