

SERRE'S GENERALIZATION OF NAGAO'S THEOREM: AN ELEMENTARY APPROACH

A. W. MASON

ABSTRACT. Let C be a smooth projective curve over a field k . For each closed point Q of C let $\mathcal{C} = \mathcal{C}(C, Q, k)$ be the coordinate ring of the affine curve obtained by removing Q from C . Serre has proved that $GL_2(\mathcal{C})$ is isomorphic to the fundamental group, $\pi_1(G, T)$, of a graph of groups (G, T) , where T is a tree with at most one non-terminal vertex. Moreover the subgroups of $GL_2(\mathcal{C})$ attached to the terminal vertices of T are in one-one correspondence with the elements of $\text{Cl}(\mathcal{C})$, the ideal class group of \mathcal{C} . This extends an earlier result of Nagao for the simplest case $\mathcal{C} = k[t]$.

Serre's proof is based on applying the theory of groups acting on trees to the quotient graph $\overline{X} = GL_2(\mathcal{C}) \backslash X$, where X is the associated *Bruhat-Tits building*. To determine \overline{X} he makes extensive use of the theory of vector bundles (of rank 2) over C . In this paper we determine \overline{X} using a more elementary approach which involves substantially less algebraic geometry.

The subgroups attached to the edges of T are determined (in part) by a set of positive integers S , say. In this paper we prove that S is bounded, even when $\text{Cl}(\mathcal{C})$ is *infinite*. This leads, for example, to new free product decomposition results for certain principal congruence subgroups of $GL_2(\mathcal{C})$, involving unipotent and elementary matrices.

INTRODUCTION

Let C be a smooth projective curve over a field k and let K be its function field. For each closed point Q of C let $\mathcal{C} = \mathcal{C}(C, Q, k)$ be the coordinate ring of the affine curve obtained by removing Q from C . Serre [8, Theorem 10, p.119] has proved the following result.

Theorem (Serre). *There exists a graph of groups (G, T) , where T is a tree with at most one non-terminal vertex, such that*

$$GL_2(\mathcal{C}) \cong \pi_1(G, T),$$

where $\pi_1(G, T)$ is the fundamental group of (G, T) .

Moreover, the subgroups of $GL_2(\mathcal{C})$ attached to the terminal vertices of T are in one-one correspondence with the elements of $\text{Cl}(\mathcal{C})$, the ideal class group of \mathcal{C} .

This extends a previous result of Nagao for the case $\mathcal{C} = k[t]$. (See [8, Proposition 3, p.88].) (In this case C is the projective line over k , Q is its point at infinity and T consists of 2 vertices and a single edge. The group $GL_2(k[t])$ is then a (proper) amalgamated product of a pair of groups.)

Received by the editors March 25, 1999.

2000 *Mathematics Subject Classification*. Primary 20H25; Secondary 20E08, 14H05.

Key words and phrases. General linear group, tree, algebraic function field.

Serre's theorem has a number of important consequences. For example, when k is *finite*, \mathcal{C} is an *arithmetic* Dedekind domain, and this result enables Serre [8, Theorem 12, p.124] to solve the *Congruence Subgroup Problem* for $GL_2(\mathcal{C})$. To prove the theorem Serre [8, Theorem 9, p.106] determines the structure of the quotient graph $\overline{X} = GL_2(\mathcal{C}) \backslash X$, where X is the *Bruhat-Tits tree* associated with $GL_2(K)$, and then applies the fundamental theorem [8, Theorem 13, p.55] of the theory of groups acting on trees. To determine \overline{X} he identifies each of its vertices with a certain equivalence class of vector bundles of rank 2 over \mathcal{C} and then makes extensive use of the machinery of algebraic geometry. (See [8, pp.96-108].) In this paper we determine the structure of \overline{X} in a more elementary way which (unlike Serre) refers explicitly to matrices. The only non-elementary result we require from algebraic geometry is (the standard function field version of) the Riemann-Roch theorem. The intention is to provide a proof of Serre's theorem which is accessible to a larger part of the mathematical community.

Our proof contains an additional feature. The subgroups of $GL_2(\mathcal{C})$ attached to the terminal vertices of T are determined (in part) by a set of positive integers \mathcal{S} , say. In this paper we prove that \mathcal{S} is *bounded*. (This is obvious when $\text{Cl}(\mathcal{C})$ is finite, which is the case, for example, when k is finite.) We use the existence of this bound to prove decomposition theorems more precise than the above for normal subgroups of $GL_2(\mathcal{C})$ contained in certain principal congruence subgroups. For the case where $\text{Cl}(\mathcal{C})$ is finite, versions of these results have appeared in previous papers [4], [5] of the author.

Radtke [7] has provided an alternative proof of Serre's theorem by considering the action of $GL_2(\mathcal{C})$, as a group of linear fractional transformations, on the so-called "algebraist's upper half plane", $\check{K} \backslash K$, where \check{K} is the completion of K with respect to the discrete valuation of K determined by Q . This is analogous to the classical approach of Ford towards the structure of discrete subgroups of $PSL_2(\mathbb{R})$, via their action on the complex upper half plane. However Radtke only deals with the case where k is finite.

In [1] Lubotzky considers a special type of discrete subgroup Γ (called a *lattice*) of a rank one semi-simple algebraic group G defined over a local field F . By using the theory of *Schottky groups* applied to the action of Γ on T , the *Bruhat-Tits tree* associated with G , he determines the structure of $\Gamma \backslash T$. This provides a more general version of Serre's result [8, Theorem 9, p.106] but again *only* applies to the case where k is finite. In this paper we are concerned with all k .

1. DEDEKIND DOMAINS IN FUNCTION FIELDS

We begin with a description of those parts of the theory of function fields which are essential for our purposes. Given that this paper is not written primarily for specialists in algebraic geometry, it seems appropriate to make this account reasonably detailed. We make use of the very accessible book [9] of Stichtenoth, adopting his terminology.

As usual $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and \mathbb{C} denote the sets of natural numbers, rational integers, rational numbers, real numbers and complex numbers, respectively. We denote the set of units of a ring R (with identity) by R^* .

Let k be a field. An *algebraic function field* K/k of *one variable over* k is a field K containing k such that K is a finite, separable extension of $k(x)$, for some $x \in K$, *transcendental* over k . Let \check{k} be the algebraic closure of k in K . It is known

[9, I.1.15, p.6] that \check{k} is a *finite* extension of k . From now on we assume that $\check{k} = k$, in which case k is called the *full constant field* of K .

A *valuation ring* \mathcal{O}_0 of K/k is a proper subring of K , properly containing k , with the property that, for all $z \in K^*$, either $z \in \mathcal{O}_0$ or $z^{-1} \in \mathcal{O}_0$. It can be shown [9, I.1.5, p.2] and [9, I.1.6, p.3] that \mathcal{O}_0 is a local ring whose maximal ideal P is principal. In addition, every non-zero \mathcal{O}_0 -ideal is a power of P . It is known [9, I.1.5(b), p.2] that \mathcal{O}_0 is determined by its maximal ideal. For this reason we denote \mathcal{O}_0 by \mathcal{O}_P . The maximal ideal P is called a *place* of K/k , and the set of all places is denoted by \mathbb{P}_K . There is a one-one correspondence [9, I.1.12, p.5] between \mathbb{P}_K and the set of all *discrete valuations* of K/k which are trivial on k . For each $P \in \mathbb{P}_K$ we denote its corresponding valuation by v_P . By definition v_P is (in part) a multiplicative map

$$v_P : K \rightarrow \mathbb{Z} \cup \{\infty\},$$

which is trivial on k^* .

For each $P \in \mathbb{P}_K$ it can be shown [9, I.1.14, p.6] that the *residue class field* of P , \mathcal{O}_P/P , is a *finite* extension of k . We denote the degree of this extension by $\deg P$.

A *divisor* D is a formal sum of the type

$$D = \sum_{P \in \mathbb{P}_K} \alpha_P P,$$

where $\alpha_P \in \mathbb{Z}$ and $\alpha_P = 0$, for all but finitely many P . We put $v_P(D) = \alpha_P$. The integer

$$\deg D := \sum_{P \in \mathbb{P}_K} \alpha_P \deg P$$

is called the *degree* of D . Under the natural definition of addition the set of divisors becomes [9, p.15] a group, the *divisor group* \mathcal{D}_K . By [9, I.3.4, p.14] there is a natural map from K to \mathcal{D}_K . Let $x \in K^*$. We define

$$(x) := \sum_{P \in \mathbb{P}_K} v_P(x) P.$$

Our next definition leads to the Riemann-Roch theorem. For each $A \in \mathcal{D}_K$, we define

$$\mathcal{L}(A) := \{x \in K : v_P(x) \geq -v_P(A), \text{ for all } P \in \mathbb{P}_K\}.$$

It is known [9, I.4.9., p.18] that $\mathcal{L}(A)$ is a *finite-dimensional* vector space over k . The integer

$$\dim A := \dim_k(\mathcal{L}(A))$$

is called the *dimension* of A . We recall [9, p.21] the definition of the non-negative integer referred to as the *genus* g of K/k . We now state two celebrated results of Riemann and Roch.

(a) **(Riemann)** $\dim A \geq \deg A + 1 - g$.

(b) **(Riemann-Roch)** If $\deg A \geq 2g - 1$, then

$$\dim A = \deg A + 1 - g.$$

Part (a) is *Riemann's Theorem* [9, I.4.17, p.21]. Part (b) is an immediate consequence of the *Riemann-Roch Theorem* [9, I.5.17, p.29].

From now on we fix a place Q of \mathbb{P}_K . We denote its valuation ring and discrete valuation by \mathcal{O} and v , respectively, and we put $d = \deg Q$. Let

$$\mathcal{C} = \bigcap_{P \neq Q} \mathcal{O}_P = \{x \in K : v_P(x) \geq 0, \text{ for all } P \neq Q\}.$$

Then \mathcal{C} is a *Dedekind* domain whose quotient field is K . See [9, III.2.5, p.68]. We record some elementary properties of \mathcal{C} .

Lemma 1.1. *Let $x \in \mathcal{C}$, where $x \neq 0$. Then:*

- (i) $v(x) \leq 0$,
- (ii) $v(x) = 0 \Leftrightarrow x \in k^*$,
- (iii) $\mathcal{C}^* = k^*$.

Proof. Part (i) follows from the “product formula” [9, I.4.11, p.18]. Part (ii) follows from [9, I.1.19, p.8] (since we are assuming k is *algebraically closed* in K). Part (iii) is then immediate. \square

Let $P \in \mathbb{P}_K$, where $P \neq Q$. The map

$$P \mapsto \mathcal{C} \cap P$$

defines a one-one correspondence.

$$\mathbb{P}_K - \{Q\} \leftrightarrow \text{Spec } \mathcal{C},$$

where $\text{Spec } \mathcal{C}$ is the set of all maximal (equivalently, non-zero, prime) \mathcal{C} -ideals. Let $x \in \mathcal{C}$, where $x \neq 0$. The \mathcal{C} -ideal $x\mathcal{C}$ is uniquely expressible as a product of maximal ideals. Let $P \in \mathbb{P}_K$, where $P \neq Q$, and let $\mathfrak{p} = \mathcal{C} \cap P$. Under the above correspondence it can be shown [9, III.2.9, p.70] that

$$v_P(x) = \text{ord}_{\mathfrak{p}}(x\mathcal{C}).$$

We now introduce what for our purposes is a particularly important set of finite-dimensional k -spaces contained in \mathcal{C} .

Definition. For each $n \in \mathbb{N} \cup \{0\}$, let

$$\mathcal{C}(n) := \{x \in \mathcal{C} : v(x) \geq -n\}.$$

Clearly $\mathcal{C}(n)$ is a vector space over k . By Lemma 1.1 it follows that $\mathcal{C}(0) = k$. Let \mathfrak{q} be a non-zero, proper \mathcal{C} -ideal. Then

$$\mathfrak{q} = \prod_{i=1}^t \mathfrak{p}_i^{\alpha_i},$$

for some (distinct) $\mathfrak{p}_i \in \text{Spec } \mathcal{C}$ and $\alpha_i \in \mathbb{N}$ ($1 \leq i \leq t$). Now there exist $P_i \in \mathbb{P}_K$, where $P_i \neq Q$, such that

$$\mathfrak{p}_i = \mathcal{C} \cap P_i.$$

We define the *degree* of \mathfrak{q} , $\deg \mathfrak{q}$, by

$$\deg \mathfrak{q} := \sum_{i=1}^t \alpha_i d_i,$$

where $d_i = \deg P_i$ ($1 \leq i \leq t$).

In addition we define

$$\deg \mathcal{C} := 0.$$

By [9, III.2.9, p.70] it follows that

$$\deg \mathfrak{q} = \dim_k(\mathcal{C}/\mathfrak{q}).$$

Lemma 1.2. *Let \mathfrak{q} be a non-zero \mathcal{C} -ideal and let $n \in \mathbb{N}$. Then $\mathfrak{q} \cap \mathcal{C}(n)$ is a finite-dimensional vector space over k , and*

$$\dim_k(\mathfrak{q} \cap \mathcal{C}(n)) \geq nd - \deg \mathfrak{q} + 1 - g.$$

Moreover,

$$\dim_k(\mathfrak{q} \cap \mathcal{C}(n)) = nd - \deg \mathfrak{q} + 1 - g,$$

whenever

$$nd \geq \deg \mathfrak{q} + 2g - 1.$$

Proof. We note that $\mathfrak{q} \cap \mathcal{C}(n) = \mathcal{L}(D)$, where

$$D = \begin{cases} nQ - \sum_{i=1}^t \alpha_i P_i, & \mathfrak{q} \neq \mathcal{C}, \\ nQ, & \mathfrak{q} = \mathcal{C}. \end{cases}$$

The proof follows from the Riemann–Roch theorem. \square

2. THE IDEAL CLASS GROUP

At this point we introduce the *ideal class group* of \mathcal{C} , $\text{Cl}(\mathcal{C})$, which plays an important role in Serre's theorem. We recall the definition. Non-zero \mathcal{C} -ideals $\mathfrak{q}, \mathfrak{q}'$ are said to be *equivalent* if and only if there exists $\mu \in K^*$ such that $\mathfrak{q}' = \mu\mathfrak{q}$. This is an equivalence relation. Let $[\mathfrak{q}]$ denote the equivalence class containing \mathfrak{q} . The set of equivalence classes forms a group, $\text{Cl}(\mathcal{C})$, under the natural definition of multiplication, whose identity is the class consisting of the principal ideals.

By Lemma 1.1(i) we know that if $x \in \mathcal{C}$ and $x \neq 0$, then $v(x) \leq 0$. In this section we show that it is possible to represent the elements of $\text{Cl}(\mathcal{C})$ by \mathcal{C} -ideals \mathfrak{q}_ω ($\omega \in \Omega$), say, such that, for each $\omega \in \Omega$, there exists a non-zero $x_\omega \in \mathfrak{q}_\omega$ with the property that $v(x_\omega) \geq L$, where L is a constant. This, of course, is obvious when $\text{Cl}(\mathcal{C})$ is finite. It is known that $\text{Cl}(\mathcal{C})$ is finite, for example, when k is finite. (See [5, Theorem 3.3].) In this paper however we are concerned with all k . It is known that, when k is infinite, $\text{Cl}(\mathcal{C})$ can be finite or infinite. (See, for example, [6].)

The existence of L will be used later to prove, for example, a decomposition theorem for principal congruence subgroups of $GL_2(\mathcal{C})$ which involves unipotent matrices.

Definition. Let \mathfrak{q} be a non-zero \mathcal{C} -ideal. We define

$$\max(\mathfrak{q}) := \max\{v(x) : x \in \mathfrak{q}, x \neq 0\}.$$

By Lemma 1.1(ii) it follows that

$$\max(\mathfrak{q}) = 0 \Leftrightarrow \mathfrak{q} = \mathcal{C}.$$

Lemma 2.1. *Let \mathfrak{q} be a non-zero \mathcal{C} -ideal such that*

$$\deg \mathfrak{q} \geq d + g.$$

Then there exists $\mathfrak{q}_0 \in [\mathfrak{q}]$ such that

$$\max(\mathfrak{q}_0) > \max(\mathfrak{q}).$$

Proof. Let

$$\mathfrak{q} = \prod_{i=1}^t \mathfrak{p}_i^{\alpha_i}$$

be the primary decomposition of \mathfrak{q} , where $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ are distinct and $\alpha_i \in \mathbb{N}$ ($1 \leq i \leq t$). We consider the divisor

$$D = \sum_{i=1}^t \alpha_i P_i - Q,$$

where $\mathcal{C} \cap P_i = \mathfrak{p}_i$ ($1 \leq i \leq t$).

By Riemann's theorem [9, I.4.17, p.21] it follows that

$$\dim D \geq \deg D + 1 - g = \deg \mathfrak{q} - d + 1 - g \geq 1.$$

Choose non-zero $\lambda \in \mathcal{L}(D)$. Then

$$(i) \quad \lambda \mathfrak{q} \leq \mathcal{C}$$

and

$$(ii) \quad \max(\lambda \mathfrak{q}) \geq 1 + \max(\mathfrak{q}).$$

We take $\mathfrak{q}_0 = \lambda \mathfrak{q}$. □

Lemma 2.2. *Let \mathfrak{q} be a non-zero \mathcal{C} -ideal and let*

$$n_0 = \min\{n \in \mathbb{N} : n \geq 1 + (\deg \mathfrak{q} + 2g - 1)/d\}.$$

Then there exists a non-zero $x \in \mathfrak{q}$ such that

$$v(x) = -n_0.$$

Proof. By Lemma 1.2 and the definition of n_0 it follows that

$$\dim_k(\mathfrak{q} \cap \mathcal{C}(n_0)) = n_0 d - \deg \mathfrak{q} + 1 - g$$

and that

$$\dim_k(\mathfrak{q} \cap \mathcal{C}(n_0 - 1)) = (n_0 - 1)d - \deg \mathfrak{q} + 1 - g.$$

We choose $x \in \mathfrak{q} \cap \mathcal{C}(n_0)$ with $x \notin \mathfrak{q} \cap \mathcal{C}(n_0 - 1)$. □

We now come to the principal result in this section.

Theorem 2.3. *Let $[\mathfrak{q}]$ be any element of $\text{Cl}(\mathcal{C})$. Then there exists $\mathfrak{q}_0 \in [\mathfrak{q}]$ such that*

$$\max(\mathfrak{q}_0) > -(3d + 3g - 1)/d.$$

Proof. We choose $\mathfrak{q}_0 \in [\mathfrak{q}]$ such that

$$\max(\mathfrak{q}_0) = \max\{\max(\mathfrak{q}') : \mathfrak{q}' \in [\mathfrak{q}]\}.$$

By Lemma 2.1 it follows that

$$\deg \mathfrak{q}_0 < d + g.$$

We now apply Lemma 2.2 to \mathfrak{q}_0 . There exists a non-zero $x \in \mathfrak{q}_0$ such that

$$v(x) = -n_0,$$

where

$$n_0 = \min\{n \in \mathbb{N} : n \geq (d + \deg \mathfrak{q}_0 + 2g - 1)/d\}.$$

Since $\deg \mathfrak{q}_0 < d + g$, then

$$d + \deg \mathfrak{q}_0 + 2g - 1 < 2d + 3g - 1.$$

We conclude that

$$n_0 < (3d + 3g - 1)/d. \quad \square$$

3. STABILIZERS OF VERTICES

The group $GL_2(K)$ acts on a *tree* X , called its *Bruhat-Tits building*. From the structure of the quotient graph $GL_2(\mathcal{C}) \backslash X$ it is possible to prove a decomposition theorem for $GL_2(\mathcal{C})$, using the Bass-Serre theory of groups acting on trees. Such a theorem involves the stabilizers of the vertices X .

We recall [9, I.1.6, p.3] that the maximal ideal Q of \mathcal{O} is principal. We fix a \mathcal{O} -generator π of Q . Let $x \in K^*$. Then $x = \pi^n y$, where $n = v(x)$ and $v(y) = 0$. By definition it follows that

$$\mathcal{O} = \{x \in K : v(x) \geq 0\}, \quad \pi\mathcal{O} = \{x \in K : v(x) > 0\}, \quad \mathcal{O}^* = \{x \in K^* : v(x) = 0\}.$$

We put

$$k_d := \mathcal{O}/\pi\mathcal{O}.$$

Then, by definition, k_d is a finite extension of k and

$$[k_d : k] = d.$$

We recall also the definition of X . (See [8, pp. 69-72].) Let $V = K^2$. A *lattice* L of V is an \mathcal{O} -submodule of V which is free of rank 2. The group $GL_2(K)$ acts on the set of lattices in the natural way. Lattices L, L' are said to be *equivalent*, written

$$L \equiv L',$$

if and only if $L = \mu L'$, for some $\mu \in K^*$. The equivalence class containing L , Λ , is called a *lattice class*, and the vertices of X are the lattice classes. The edges of X are defined in the following way. Let $\Lambda, \Lambda' \in X$. Then Λ, Λ' are *adjacent* if and only if, for all $L \in \Lambda$, there exists a (unique) $L' \in \Lambda'$ such that $L' \leq L$ and

$$L/L' \cong k_d.$$

Then, with respect to these definitions, X is a tree [8, Theorem 1, p.70]. The group $GL_2(K)$ acts on X . Moreover, if $g \in GL_2(K)$ and $\det g \in k^*$, then g acts *without inversion* on X . (See [8, Corollary, p.75].)

At this point we simplify our notation. We put

$$G := GL_2(\mathcal{C}) \quad \text{and} \quad \Gamma := SL_2(\mathcal{C}).$$

Definition. Let $\Lambda \in X$ and $L \in \Lambda$. The stabilizer of Z in G is

$$S(Z) := \{g \in G : g(Z) = Z\},$$

where $Z = L$ or Λ .

It is known [8, Lemma 1, p.76] that

$$S(\Lambda) = S(L).$$

In this paper unipotent matrices are particularly important. We recall that a matrix $U \in GL_2(K)$ is *unipotent* if and only if $(U - I_2)^2 = 0$ (equivalently, $\det U = 1$ and $\text{tr } U = 2$).

Definition. Let $\Lambda \in X$ and $L \in \Lambda$. We put

$$U(\Lambda) = U(L) = \{U \in S(\Lambda) : U \text{ is unipotent}\}.$$

We make frequent use of the following matrix. For each $s \in K$, we put

$$g_s := \begin{bmatrix} 0 & -1 \\ 1 & -s \end{bmatrix}.$$

We introduce the *standard basis* $\{\mathbf{e}_1, \mathbf{e}_2\}$ of V , where

$$\mathbf{e}_1 = (1, 0) \text{ and } \mathbf{e}_2 = (0, 1).$$

We now define some special lattices.

Definition. Let $s \in K$ and $n \in \mathbb{N} \cup \{0\}$. We put

- (i) $L_n(\infty) := \mathcal{O}\mathbf{e}_1 + \mathcal{O}\pi^n\mathbf{e}_2$, and
- (ii) $L_n(s) := \mathcal{O}(s\mathbf{e}_1 + \mathbf{e}_2) + \mathcal{O}\pi^n\mathbf{e}_1$.

We denote the corresponding lattice classes by $\Lambda_n(\infty)$ and $\Lambda_n(s)$. It can be easily shown that these account for almost all lattice classes.

Lemma 3.1. *Let $\Lambda \in X$. Then either Λ or $g_0(\Lambda)$ lies in the set*

$$\{\Lambda_n(\infty), \Lambda_n(s) : s \in K, n \in \mathbb{N} \cup \{0\}\}.$$

Proof. We can represent Λ by a lattice generated by

$$\alpha\mathbf{e}_1 + \beta\mathbf{e}_2 \text{ and } \gamma\mathbf{e}_1 + \delta\mathbf{e}_2,$$

say, where $\alpha, \beta, \gamma, \delta \in \mathcal{O}$ and *not all* $\alpha, \beta, \gamma, \delta \in \pi\mathcal{O}$. We may assume then that either $\alpha \in \mathcal{O}^*$ or $\beta \in \mathcal{O}^*$. The result follows by a “rearrangement” of generators. \square

It is convenient to simplify our notation. We put

$$\begin{aligned} S_n(s) &:= S(\Lambda_n(s)), & S_n(\infty) &:= S(\Lambda_n(\infty)), \\ U_n(s) &:= U(\Lambda_n(s)), & U_n(\infty) &:= U(\Lambda_n(\infty)). \end{aligned}$$

We now show that for “sufficiently large” n , the stabilizers $S_n(s)$ and $S_n(\infty)$ have a simple structure. We begin with the easy cases.

Lemma 3.2. *Let $s \in k$ and $n \in \mathbb{N}$. Then $g_s \in \Gamma$ and*

$$g_s S_n(s) g_s^{-1} = S_n(\infty) = \left\{ \begin{bmatrix} \alpha & b \\ 0 & \beta \end{bmatrix} : \alpha, \beta \in k^*, b \in \mathcal{C}(n) \right\}.$$

Proof. Let $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then it is easily verified that $g \in S_n(\infty)$ if and only if $v(a), v(d) \geq 0, v(b) \geq -n$ and $v(c) \geq n$. By Lemma 1.1 it follows that $c = 0$ and that $a, d \in k^*$. The rest is obvious. \square

An immediate consequence of Lemma 3.2 is the following.

Lemma 3.3. *Let $s \in k$ and $n \in \mathbb{N}$. Then*

$$U_n(s) \cong U_n(\infty) \cong (\mathcal{C}(n))^+.$$

The situation when $s \notin k$ is more complicated. An important role is played by the following \mathcal{C} -ideal. For each $s \in K^*$ we define

$$\mathfrak{q}_s := \mathcal{C} \cap s^{-1}\mathcal{C} \cap s^{-2}\mathcal{C}.$$

Lemma 3.4. *Let $s \in K$, where $s \notin k$. If $nd > \deg \mathfrak{q}_s$, then $g \in S_n(s)$ if and only if*

$$g = \begin{bmatrix} \alpha + sc & (\beta - \alpha)s - s^2c \\ c & \beta - sc \end{bmatrix},$$

where

- (i) $\alpha, \beta \in k^*$,
- (ii) $c \in \mathcal{C}(n) \cap \mathcal{C}s^{-1} \cap ((\beta - \alpha)s^{-1} + \mathcal{C}s^{-2})$,
- (iii) $\det g = \alpha\beta$.

Proof. We note that the hypothesis on s ensures that $\mathfrak{q}_s \neq \mathcal{C}$. Let

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then, by [8, Lemma 1, p.76], $g \in S_n(s)$ if and only if

$$g_s g g_s^{-1}(L_n(\infty)) = L_n(\infty).$$

Let

$$g_s g g_s^{-1} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}.$$

Then it is easily verified that

$$a' = d + cs, \quad b' = -c, \quad c' = -b + s(d - a) + s^2c, \quad d' = a - cs,$$

and hence that $g \in S_n(s)$ if and only if

- (a) $v(a'), v(d') \geq 0$,
- (b) $v(b') \geq -n$,
- (c) $v(c') \geq n$.

Let $s = x/y$, where $x, y \in \mathcal{C}$. We note that

$$\mathfrak{q}_s = (\mathcal{C} + s\mathcal{C} + s^2\mathcal{C})^{-1} = y^2(\overline{\mathfrak{q}}_s)^{-1},$$

where

$$\overline{\mathfrak{q}}_s = (x\mathcal{C} + y\mathcal{C})^2.$$

Hence

$$\mathfrak{q}_s \overline{\mathfrak{q}}_s = y^2\mathcal{C},$$

and so

$$\deg \mathfrak{q}_s + \deg \overline{\mathfrak{q}}_s = -2v(y)d,$$

by the “product formula” [9, I.4.11, p.18].

Suppose now that $v(c') \geq n$, for some *non-zero* c' . Then $c' = zy^{-2}$, for some non-zero $z \in \overline{\mathfrak{q}}_s$. By the hypothesis on n , it follows that

$$v(z) > (\deg \mathfrak{q}_s)/d + 2v(y) = -(\deg \overline{\mathfrak{q}}_s)/d.$$

On the other hand, $z \in \overline{\mathfrak{q}}_s$, and so (again by [9, I.4.11, p.18])

$$-v(z)d \geq \deg \overline{\mathfrak{q}}_s,$$

which yields the desired contradiction, unless $\overline{\mathfrak{q}}_s = \mathcal{C}$.

When $\bar{\mathfrak{q}}_s = \mathcal{C}$, then $\mathfrak{q}_s = v^2\mathcal{C}$, and so

$$v(z) > 0,$$

which contradicts Lemma 1.1. We conclude that $c' = 0$.

It follows that a', d' are the *eigenvalues* of g . Then $a' + d' = a + d \in \mathcal{C} \cap \mathcal{O} = k$ and $\det g = a'd' \in k^*$. (See Lemma 1.1.) As k is algebraically closed in K , the eigenvalues a', d' lie in k^* . The rest follows. \square

Our next result is an immediate consequence.

Lemma 3.5. *Let $s \in K$, where $s \notin k$. If $nd > \deg \mathfrak{q}_s$, then*

$$U_n(s) = \left\{ \begin{bmatrix} 1 + cs & -cs^2 \\ c & 1 - cs \end{bmatrix} : c \in \mathcal{C}(n) \cap \mathfrak{q}_s \right\} \cong (\mathcal{C}(n) \cap \mathfrak{q}_s)^+.$$

The remaining results in this section will be used to determine the structure of the quotient graph $G \backslash X$.

Definition. We define the *neighbourhood* of a lattice L to be

$$N(L) := \{L', \text{ lattice} : L' \leq L, L/L' \cong k_d\}.$$

If Λ is the lattice class containing L , it is clear that the elements of $N(L)$ are in one-one correspondence with those vertices of X *adjacent* to Λ (and hence, since X is a tree, with those edges of X incident with Λ). It is also clear that if $g \in GL_2(K)$ stabilizes L , then g acts on $N(L)$.

Lemma 3.6. *Let $n \in \mathbb{N}$ and, for each $\alpha \in k_d$, let $K_n(\alpha)$ be the lattice generated by*

$$\pi \mathbf{e}_1 \text{ and } \alpha \mathbf{e}_1 + \pi^n \mathbf{e}_2.$$

Then

$$N(L_n(\infty)) = \{L_{n+1}(\infty)\} \cup \{K_n(\alpha) : \alpha \in k_d\}.$$

Proof. Let $L \in N(L_n(\infty))$. Then L is generated by

$$\beta \mathbf{e}_1 + \gamma \pi^n \mathbf{e}_2 \text{ and } \delta \mathbf{e}_1 + \varepsilon \pi^n \mathbf{e}_2,$$

say, where $\beta, \gamma, \delta, \varepsilon \in \mathcal{O}$ and $v(\beta\varepsilon - \gamma\delta) = 1$. It follows that either $\beta \in \mathcal{O}^*$ or $\gamma \in \mathcal{O}^*$. The result follows from a “rearrangement of the generators”. \square

We now come to the equivalence relation which is central to the definition of $G \backslash X$.

Definition. Let L, L' be lattices with corresponding classes Λ, Λ' , respectively, and let H be a subgroup of $GL_2(K)$.

Let $Z = L$ or Λ . We say that Z and Z' are *H-equivalent*, written

$$Z \sim_H Z',$$

if and only if

$$Z' = h(Z),$$

for some $h \in H$.

Lemma 3.7. *Let V be a finite-dimensional vector space over k , where, for some $n \in \mathbb{N}$,*

$$(a) \quad k \leq V \leq \mathcal{C}(n)$$

and

$$(b) \quad \dim_k(V/V \cap \mathcal{C}(n-1)) = d.$$

Let

$$H = \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} : c \in V \right\}.$$

Then

$$H \text{ stabilizes } L_n(\infty).$$

Moreover, for all $L \in N(L_n(\infty))$,

$$\text{either } L_{n+1}(\infty) \sim_H L \quad \text{or} \quad \pi L_{n-1}(\infty) \sim_H L.$$

Proof. The first part is obvious. For the second part,

$$\text{either } L = L_{n+1}(\infty) \text{ or } L = K_n(\alpha),$$

for some $\alpha \in k_d$, by Lemma 3.6. Now H stabilizes $L_{n+1}(\infty)$. The hypothesis on the k -dimension ensures that

$$\pi^n V + \pi \mathcal{O} = \mathcal{O}.$$

It follows that, for all $\alpha \in k_d$, there exists an $h \in H$ such that

$$h(K_n(\alpha)) = \pi L_{n-1}(\infty). \quad \square$$

4. CUSPS

From now on we denote the quotient graph $G \backslash X$ by \overline{X} and the image in \overline{X} of the lattice class Λ by $\overline{\Lambda}$. In this section we prove that \overline{X} is (in part) made up of a set of pairwise disjoint *paths of infinite length* which are in one-one correspondence with the elements of $\text{Cl}(\mathcal{C})$, the ideal class group of \mathcal{C} . We denote the *projective line over K* , $\mathbb{P}_1(K) = K \cup \{\infty\}$, by \hat{K} .

We recall that, for each $s \in K^*$,

$$\mathfrak{q}_s = \mathcal{C} \cap \mathcal{C}s^{-1} \cap \mathcal{C}s^{-2}.$$

It is convenient to extend this definition to \hat{K} . If $\sigma \in \{0, \infty\}$, we define

$$\mathfrak{q}_\sigma := \mathcal{C}.$$

The following set of positive integers will play an important role in the structure of \overline{X} .

Let $\sigma \in \hat{K}$. We define n_σ to be the *least* integer $n \in \mathbb{N}$ for which

$$d(n-1) \geq \deg \mathfrak{q}_\sigma + 2g - 1, \text{ when } g \neq 0,$$

and

$$d(n-1) > \deg \mathfrak{q}_\sigma, \text{ when } g = 0.$$

The structure of \overline{X} involves subgraphs of the following type.

For each $\sigma \in \hat{K}$, let $C(\sigma)$ be the subgroup of \overline{X} induced by the vertices

$$\overline{\Lambda}_n(\sigma), \text{ where } n \geq n_\sigma.$$

It is clear that the vertex $\overline{\Lambda}_n(\sigma)$ is adjacent (in \overline{X}) to $\overline{\Lambda}_{n-1}(\sigma)$ and $\overline{\Lambda}_{n+1}(\sigma)$, when $n \geq n_\sigma$. We now prove that these are the *only* vertices of \overline{X} adjacent to $\overline{\Lambda}_n(\sigma)$.

At this point it is convenient to introduce the following notation. For each $\sigma \in \hat{K}$ and $n \in \mathbb{N}$, we put

$$\overline{U}_n(\sigma) := \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} : c \in \mathfrak{q}_\sigma \cap \mathcal{C}(n) \right\}.$$

We begin this section with a useful lemma.

Lemma 4.1. *Let $\sigma, \tau \in \hat{K}$ and suppose that*

$$\overline{\Lambda}_n(\sigma) = \overline{\Lambda}_m(\tau),$$

where $n \geq n_\sigma - 1$ and $m \geq n_\tau - 1$. Then

$$nd - \deg \mathfrak{q}_\sigma = md - \deg \mathfrak{q}_\tau.$$

Proof. There exists $g \in G$ such that

$$g(\Lambda_n(\sigma)) = \Lambda_m(\tau)$$

By Lemmas 3.2 - 3.5 it follows that

$$h(\overline{U}_n(\sigma)) = \overline{U}_m(\tau),$$

where $h = g_\tau g g_\sigma^{-1}$. The $(2, 1)$ -entry of h is therefore zero, and so

$$\lambda(\mathfrak{q}_\sigma \cap \mathcal{C}(n)) = \mathfrak{q}_\tau \cap \mathcal{C}(m),$$

for some $\lambda \in K^*$. We now apply Lemma 1.2. □

We can now determine the structure of $C(\sigma)$.

Theorem 4.2. *For all $\sigma \in \hat{K}$, the subgraph $C(\sigma)$ of \overline{X} is a tree whose vertices are $\overline{\Lambda}_n(\sigma)$, where $n \geq n_\sigma$.*

Moreover,

- (i) $\overline{\Lambda}_{n_\sigma}(\sigma)$ is a terminal vertex, and
- (ii) all other vertices have degree 2.

Proof. By Lemma 4.1, the vertices

$$\overline{\Lambda}_n(\sigma),$$

where $n \geq n_\sigma - 1$, are distinct.

It is clear that the edges of \overline{X} incident with a vertex $\overline{\Lambda}_n(\sigma)$ of $C(\sigma)$ are in one-one correspondence with the orbits of the action of $S_n(\sigma)$ on the neighbourhood $N(L_n(\sigma))$ of $L_n(\sigma)$. This action is obviously equivalent to that of $H = g_\sigma(S_n(\sigma))g_\sigma^{-1}$ on $N(L_n(\infty))$. By Lemmas 3.3 and 3.5,

$$\overline{U}_n(\sigma) \leq H.$$

We now apply Lemmas 1.2 and 3.7. □

The graph $C(\sigma)$ is a *path of infinite length with origin* $\overline{\Lambda}_{n_\sigma}(\sigma)$ and is called a *cuspid*, after Serre [8, p.104]. The cusps have the following intersection property.

Lemma 4.3. *Let $\sigma, \tau \in \hat{K}$ and suppose that*

$$\overline{\Lambda}_n(\sigma) = \overline{\Lambda}_m(\tau),$$

for some $n \geq n_\sigma$ and $m \geq n_\tau$. Then

$$\overline{\Lambda}_{n+t}(\sigma) = \overline{\Lambda}_{m+t}(\tau),$$

for all $t \in \mathbb{N}$.

Proof. We only have to consider the case $t = 1$. By Theorem 4.2,

$$\overline{\Lambda}_{m+1}(\tau) = \overline{\Lambda}_{n+1}(\sigma) \quad \text{or} \quad \overline{\Lambda}_{n-1}(\sigma).$$

Suppose that

$$\overline{\Lambda}_{m+1}(\tau) = \overline{\Lambda}_{n-1}(\sigma).$$

By Lemma 4.1 it follows that

$$nd - \deg \mathfrak{q}_\sigma = md - \deg \mathfrak{q}_\tau$$

and

$$(n-1)d - \deg \mathfrak{q}_\sigma = (m+1)d - \deg \mathfrak{q}_\tau.$$

The result follows, since $d \neq 0$. □

The group $GL_2(K)$ acts on \hat{K} as a group of linear fractional transformations in the usual way. Let $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $GL_2(K)$ and let $z \in K$. Then

$$g(z) = \frac{az + b}{cz + d},$$

unless $c \neq 0$ and $z = -dc^{-1}$, in which case $g(z) = \infty$. In addition, $g(\infty) = ac^{-1}$ (resp. ∞), when $c \neq 0$ (resp. $c = 0$).

By Lemmas 3.2 and 3.4 it is clear that, for all $\sigma \in \hat{K}$ and all $n \geq n_\sigma$,

$$S_n(\sigma) \leq S_{n+1}(\sigma).$$

We now define two subgroups determined by the cusp $C(\sigma)$. We put

$$(a) \quad S(\sigma) := \bigcup_{n \geq n_\sigma} S_n(\sigma)$$

and

$$(b) \quad U(\sigma) := \bigcup_{n \geq n_\sigma} U_n(\sigma).$$

By Lemmas 3.2 and 3.3 it follows that

$$S(\infty) = \left\{ \begin{bmatrix} \alpha & c \\ 0 & \beta \end{bmatrix} : \alpha, \beta \in k^*, c \in \mathcal{C} \right\}$$

and

$$U(\infty) = \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} : c \in \mathcal{C} \right\}.$$

In addition,

$$S(0) = S(\infty)^T \quad \text{and} \quad U(0) = U(\infty)^T.$$

By Lemmas 3.4 and 3.5 it follows that, if $s \in K^*$, then

$$S(s) = \left\{ \begin{bmatrix} \alpha + sc & b \\ c & \beta - sc \end{bmatrix} : \alpha, \beta \in k^*, c \in \mathcal{C} \cap \mathcal{C}s^{-1}, b \in \mathcal{C}, b = (\beta - \alpha)s - cs^2 \right\}$$

and that

$$U(s) = \left\{ \begin{bmatrix} 1 + cs & -cs^2 \\ c & 1 - sc \end{bmatrix} : c \in \mathfrak{q}_s \right\}.$$

Lemma 4.4. *For all $\sigma \in \hat{K}$,*

$$(a) \quad S(\sigma) = \{g \in G : g(\sigma) = \sigma\}$$

and

$$(b) \quad U(\sigma) = \{g \in G : g, \text{ unipotent}, g(\sigma) = \sigma\}.$$

Proof. This follows from the above together with [3, Theorem 2.1]. \square

These subgroups are closed under conjugation. Combining Lemma 4.4 and [3, Lemma 1.3], we have

Lemma 4.5. *Let $\sigma \in \hat{K}$ and $g \in G$. Then*

$$gS(\sigma)g^{-1} = S(\sigma') \quad \text{and} \quad gU(\sigma)g^{-1} = U(\sigma'),$$

where $\sigma' = g(\sigma)$.

At this point we reintroduce the ideal class group of \mathcal{C} . Let $z \in K$. Then $z = xy^{-1}$, for some $x, y \in \mathcal{C}$. Since every \mathcal{C} -ideal is generated by two elements, there is a well-defined surjective map

$$\phi : K \rightarrow \text{Cl}(\mathcal{C}),$$

given by

$$\phi(z) = [\mathfrak{q}'],$$

where $\mathfrak{q}' = x\mathcal{C} + y\mathcal{C}$. The map ϕ extends to \hat{K} by defining $\phi(\infty)$ to be the identity. It is a classical result that, for all $\sigma, \tau \in \hat{K}$,

$$\phi(\sigma) = \phi(\tau) \Leftrightarrow \sigma = g(\tau), \text{ for some } g \in \Gamma.$$

(See, for example, [3, Theorem 3.3].) This gives rise to the following one-one correspondences:

$$\Gamma \backslash \hat{K} \leftrightarrow G \backslash \hat{K} \leftrightarrow \text{Cl}(\mathcal{C}).$$

From now on

$$\mathcal{S} = \{\infty\} \cup \{s_\omega : \omega \in \Omega\}$$

will denote a complete set of representatives of the orbits of the action of Γ on \hat{K} . Since $g_s(s) = \infty$ we may assume that $s_\omega \notin \mathcal{C}$. We now show that the cusps $C(\sigma)$, where $\sigma \in \mathcal{S}$, can be used to partition \overline{X} .

Lemma 4.6. *Let $\sigma, \tau \in \mathcal{S}$. If $\sigma \neq \tau$, then*

$$C(\sigma) \cap C(\tau) = \emptyset.$$

Proof. We prove this only for cases where $\sigma, \tau \neq \infty$. The other cases are similar. Suppose that

$$C(\sigma) \cap C(\tau) \neq \emptyset.$$

Then, for some $n \geq n_\sigma$ and $m \geq n_\tau$,

$$\overline{\Lambda}_{n+t}(\sigma) = \overline{\Lambda}_{m+t}(\tau),$$

for all $t \in \mathbb{N} \cup \{0\}$, by Lemma 4.3. By considering stabilizer subgroups it is clear that there exist $g, h \in G$ such that

$$U_n(\sigma) = gU_m(\tau)g^{-1} \quad \text{and} \quad U_{n+1}(\sigma) = hU_{m+1}(\tau)h^{-1}.$$

Then

$$jU_m(\tau)j^{-1} \leq U_{m+1}(\tau),$$

where $j = h^{-1}g$, and so

$$j_0 \overline{U}_m(\tau) j_0^{-1} \leq \overline{U}_{m+1}(\tau),$$

where $j_0 = g_\tau j g_\tau^{-1}$. Let

$$j_0 = \begin{bmatrix} e & f \\ e' & f' \end{bmatrix}.$$

Then $e' = 0$, and so e and f' are the *eigenvalues* of j . Since $e, f' \in K$ and \mathcal{C} is a *Dedekind* domain (and hence integrally closed), it follows that $e, f' \in \mathcal{C}$. But $ef' = \det j \in k^*$. Now, by Lemma 1.1, $\mathcal{C}^* = k^*$ and so $e, f' \in k^*$. We deduce that

$$j_0 \overline{U}_r(\tau) j_0^{-1} = \overline{U}_r(\tau),$$

for all $r \geq m$. We have thus proved that

$$U_{n+t}(\sigma) = gU_{m+t}(\tau)g^{-1},$$

for all $t \in \mathbb{N} \cup \{0\}$, from which it follows that

$$U(\sigma) = \bigcup_{t \geq 0} (U_{n+t}(\sigma)) = \bigcup_{t \geq 0} (gU_{m+t}(\tau)g^{-1}) = gU(\tau)g^{-1} = U(g(\tau)),$$

by Lemma 4.5.

Now choose

$$u = \begin{bmatrix} 1 + c\sigma & -c\sigma^2 \\ c & 1 - c\sigma \end{bmatrix} \in U(\sigma),$$

where $c \in \mathcal{C}$ and $c \neq 0$. Now $u(\tau') = \tau'$, where $\tau' = g(\tau)$. It follows that $\sigma = g(\tau)$ and hence (since $\sigma, \tau \in \mathcal{S}$) that $\sigma = \tau$. \square

Lemma 4.6 enables us to provide an alternative proof of a structure theorem of Serre [8, Theorem 9, p.106].

Theorem 4.7 (Serre). *With the above notation, there exists a connected subgraph Y of \overline{X} such that*

- (a) $\overline{X} = \left(\bigcup_{\sigma \in \mathcal{S}} C(\sigma) \right) \cup Y$,
- (b) $\text{vert}(Y) \cap \text{vert}(C(\sigma)) = \{\overline{\Lambda}_{n_\sigma}(\sigma)\} \quad (\sigma \in \mathcal{S})$,
- (c) $\text{edge}(Y) \cap \text{edge}(C(\sigma)) = \emptyset \quad (\sigma \in \mathcal{S})$.

5. SERRE'S DECOMPOSITION THEOREM

As outlined by Serre [8, p.117], we can use the fundamental theorem of the theory of groups acting on trees [8, Theorem 13, p.55] to infer from the structure of \overline{X} a decomposition theorem for G .

We choose a maximal tree T of \overline{X} and a *lift*

$$j : T \rightarrow X,$$

which we extend to a map

$$j : \text{edge}(\overline{X}) \rightarrow \text{edge}(X).$$

By Theorems 4.2 and 4.7 the tree T contains each $C(\sigma)$, and so there exists $g_\sigma \in G$ such that $j(C(\sigma))$ is the *path of infinite length* in X with vertices $g_\sigma(\Lambda_n(\sigma))$, $n \geq n_\sigma$, and *origin* $g_\sigma(\Lambda_{n_\sigma}(\sigma))$. We recall that $S_n(\sigma) \leq S_{n+1}(\sigma)$, for all $n \geq n_\sigma$, and that the stabilizer in G of $g_\sigma(\Lambda_n(\sigma))$ is $g_\sigma(\Lambda_n(\sigma))g_\sigma^{-1}$. The decomposition theorem follows from [8, Theorem 13, p.55] applied to j .

We call a combinatorial graph R a *star* if and only if R is a tree with *no more than one* non-terminal vertex.

Theorem 5.1 (Serre). *With the above notation,*

$$G \cong \pi_1(\overline{G}, T_0),$$

the fundamental group of a star of groups (\overline{G}, T_0) defined as follows.

(i) T_0 is a star with terminal vertices v_σ , vertex v^* and edges e_σ , where e_σ joins v^* and v_σ ($\sigma \in \mathcal{S}$).

(ii) The assignment of groups to the terminal vertices and edges of T_0 provided by \overline{G} is given by

$$(a) \quad \overline{G}_{v_\sigma} = g_\sigma(S(\sigma))g_\sigma^{-1}$$

and

$$(b) \quad \overline{G}_{e_\sigma} = \overline{G}_{v^*} \cap \overline{G}_{v_\sigma} = g_\sigma(S_{n_\sigma}(\sigma))g_\sigma^{-1}.$$

Notes. (i) Serre's proof of this result [8, Theorem 10, p.119] is based on a different proof [8, Theorem 9, p.106] of Theorem 4.7. In Serre's terminology G is the "sum of the subgroups \overline{G}_{v^*} and \overline{G}_{v_σ} ($\sigma \in \mathcal{S}$), amalgamated along their common subgroups $\overline{G}_{v^*} \cap \overline{G}_{v_\sigma}$."

(ii) For the definitions of a graph of groups and its fundamental group, see [8, Definition 8, p.37] and [8, p.42], respectively.

We devote the remainder of the paper to showing how the results of §2 can be used to impose an upper bound on the set of integers $\{n_\sigma : \sigma \in \mathcal{S}\}$. We conclude with two consequences of the existence of such a bound. We require two further lemmas.

Lemma 5.2. *There exists a complete set of representatives of the orbits of G on \hat{K} ,*

$$\mathcal{S}' = \{\infty\} \cup \{s'_\omega : \omega \in \Omega\},$$

say, with the property that, for all $\sigma' \in \mathcal{S}'$,

$$n_{\sigma'} \leq n^*,$$

where $n^ = n^*(d, g)$ is a constant dependent only on d and g .*

Proof. For each $t \in \mathbb{R}$, let $\{t\}$ denote the *least* integer $n \geq t$. By definition it is clear that $n_\infty = \{(d + 2g - 1)/d\}$ when $g \neq 0$, and that $n_\infty = 2$ when $g = 0$.

By the “3/2-transitivity” property of the generators of ideals in a Dedekind domain, together with Theorem 2.3, we can choose

$$s'_\omega = x_\omega y_\omega^{-1},$$

where $x_\omega, y_\omega \in \mathcal{C}$, and

$$v(y_\omega) > -(3d + 3g - 1)/d.$$

Let $\sigma' = s'_\omega$ and $y = y_\omega$. Then $\mathfrak{q}_{\sigma'}$ contains the principal ideal $y^2\mathcal{C}$. By the “product formula” [8, I.4.11, p.18],

$$\deg(y^2\mathcal{C}) = -2dv(y).$$

It follows that

$$\deg \mathfrak{q}_{\sigma'} < 6d + 6g - 2.$$

By definition, when $g \neq 0$, $n_{\sigma'}$ is the *least* positive integer n with the property that

$$d(n - 1) \geq \deg \mathfrak{q}_{\sigma'} + 2g - 1.$$

We conclude that

$$n_{\sigma'} \leq \{(10d + 8g - 3)/d\}.$$

A similar bound holds when $g = 0$. □

We now introduce *congruence subgroups*. For each \mathcal{C} -ideal \mathfrak{q} , we put

$$\Gamma(\mathfrak{q}) := \{X \in \Gamma : X \equiv I_2 \pmod{\mathfrak{q}}\}.$$

An immediate consequence of Lemma 5.2 is the following.

Lemma 5.3. *With the above notation, there exist infinitely many \mathcal{C} -ideals \mathfrak{q} such that*

$$\Gamma(\mathfrak{q}) \cap S_{n_{\sigma'}}(\sigma') = \{I_2\},$$

for all $\sigma' \in S'$.

Proof. Let \mathfrak{q} be any proper \mathcal{C} -ideal. We consider first the case where $\sigma' \neq \infty$. Let $X \in \Gamma(\mathfrak{q}) \cap S_{n_{\sigma'}}(\sigma')$. By Lemma 3.4 it follows that

$$X = \begin{bmatrix} \alpha + sc & * \\ c & \beta - sc \end{bmatrix},$$

where $\alpha, \beta \in k^*$, $\det X = \alpha\beta = 1$ and $s = \sigma'$. By considering the trace of X it is clear that

$$\alpha + \beta \equiv 2 \pmod{\mathfrak{q}},$$

and so

$$\alpha + \beta = 2.$$

It follows that $\alpha = \beta = 1$, in which case

$$c \in \mathfrak{q} \cap \mathfrak{q}_{\sigma'} \cap \mathcal{C}(n_{\sigma'}),$$

by Lemma 3.5.

By Lemma 3.2, if $X \in \Gamma(\mathfrak{q}) \cap S_{n_\sigma}(\infty)$, then

$$X = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix},$$

where $b \in \mathcal{C}(n_\infty)$.

Now $\mathcal{C}(n^*)$ is a *finite-dimensional* vector space over k (Lemma 1.2), and so by [2, Lemma 3.1] there exist infinitely many \mathfrak{q} such that

$$\mathfrak{q} \cap \mathcal{C}(n^*) = \{0\}.$$

We now apply Lemma 5.2. □

Definition. For each \mathcal{C} -ideal \mathfrak{q} , let $U(\mathfrak{q})$ (resp. $NE(\mathfrak{q})$) be the subgroup (resp. *normal* subgroup) of G generated by the unipotent (resp. elementary) matrices in $\Gamma(\mathfrak{q})$.

It is clear that

$$NE(\mathfrak{q}) \leq U(\mathfrak{q}) \leq \Gamma(\mathfrak{q}).$$

We conclude with two applications of Lemmas 5.2 and 5.3. Our first shows that, for infinitely many \mathfrak{q} , the subgroups $NE(\mathfrak{q})$ and $U(\mathfrak{q})$ of $\Gamma(\mathfrak{q})$ are determined by factors in a free product decomposition of $\Gamma(\mathfrak{q})$.

Theorem 5.4. *For infinitely many \mathfrak{q} ,*

$$\Gamma(\mathfrak{q}) = E(\mathfrak{q}) * F(\mathfrak{q}) * W,$$

where

- (i) *the normal subgroup of $\Gamma(\mathfrak{q})$ generated by $E(\mathfrak{q})$ is $NE(\mathfrak{q})$, and*
- (ii) *the normal subgroup of $\Gamma(\mathfrak{q})$ generated by $E(\mathfrak{q})$ and $F(\mathfrak{q})$ is $U(\mathfrak{q})$.*

Proof. This follows from Theorem 5.1 and Lemma 5.3 as in the proof of [5, Theorem 3.1]. □

Our final result shows that, for infinitely many \mathfrak{q} , $U(\mathfrak{q}) \neq NE(\mathfrak{q})$.

Theorem 5.5. *Let V be a vector space of countably infinite dimension over k . For infinitely many \mathfrak{q} , there exist non-empty index sets Δ and Δ_0 , where $\Delta_0 \subseteq \Delta$ and $\Delta_0 \neq \Delta$, such that*

$$(i) \quad U(\mathfrak{q}) = \bigstar_{\delta \in \Delta} W_\delta$$

and

$$(ii) \quad U(\mathfrak{q})/NE(\mathfrak{q}) \cong \bigstar_{\delta \in \Delta_0} W_\delta,$$

where

$$W_\delta \cong V^+ \quad (\delta \in \Delta).$$

Proof. This follows from Theorem 5.1 and Lemma 5.3 as in the proof of [4, Corollary 2.5]. □

Theorem 5.4 (resp. 5.5) has been proved [5, Theorem 3.1] (resp. [4, Corollary 2.5]) for the case where $\text{Cl}(\mathcal{C})$ is *finite* (in which case the existence of an upper bound for \mathcal{S} is obvious). It is known that $\text{Cl}(\mathcal{C})$ is finite when, for example, k is finite or g is zero. However, there are many \mathcal{C} for which $\text{Cl}(\mathcal{C})$ is infinite. (See, for example, [6].)

REFERENCES

- [1] A. Lubotzky. Lattices in rank one Lie groups over local fields. *Geom. and Func. Analysis* **4** (1991), 405-431. MR **92k**:22019
- [2] A.W. Mason. Free Quotients of Congruence Subgroups of SL_2 over a Coordinate Ring. *Math. Z.* **198** (1988), 39-51. MR **89b**:20107
- [3] A.W. Mason. Groups generated by elements with rational fixed points. *Proc. Edinburgh Math. Soc.* **40** (1997), 19-30. MR **98a**:20055
- [4] A.W. Mason. Unipotent Matrices, Modulo Elementary Matrices, in SL_2 over a Coordinate Ring. *J. Algebra* **203** (1998), 134-155. MR **99f**:20080
- [5] A.W. Mason. Free quotients of congruence subgroups of the Serre groups and unipotent matrices. *Comm. Algebra* **27** (1999), 335-356. MR **2000a**:20110
- [6] A.W. Mason and R.W.K. Odoni. Ideal class groups of Dedekind domains contained in function fields. *Proc. Roy. Irish Acad.* **97A** (1997), 155-162. MR **99h**:13011
- [7] W. Radtke. Diskontinuierliche arithmetische Gruppen im Funktionenkörperfall. *J. Reine Angew. Math.* **363** (1985), 191-200. MR **87g**:11065
- [8] J-P. Serre. *Trees* (Springer-Verlag, 1980). MR **82c**:20083
- [9] H. Stichtenoth. *Algebraic Function Fields and Codes* (Springer-Verlag, 1993). MR **94k**:14016

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW G12 8QW, SCOTLAND,
UNITED KINGDOM

E-mail address: awm@maths.gla.ac.uk