Profinite surface groups and the congruence kernel of arithmetic lattices in $\mathbf{SL}_2(\mathbf{R})$

P. A. Zalesskii*

Abstract

Let X be a proper, nonsingular, connected algebraic curve of genus g over the field $\mathbf{C}$ of complex numbers. The algebraic fundamental group $\Gamma = \pi_1(X)$ in the sense of SGA-1 [1971] is the profinite completion of the fundamental group $\pi_1^{top}(X)$ of a compact oriented 2-manifold. We prove that every projective normal (respectively, caracteristic, accessible) subgroup of Γ is isomorphic to a normal (respectively, caracteristic, accessible) subgroup of a free profinite group. We use this description to give a complete solution of the congruence subgroup problem for aritmetic lattices in $\mathrm{SL}_2(\mathbf{R})$.

Introduction

Let X be a proper, nonsingular, connected algebraic curve of genus g over the field $\mathbf{C}$ of complex numbers. As a topological space X is a compact oriented 2-manifold and is simply a sphere with g handles added. The group $\Pi = \pi_1^{top}(X)$ is called a surface group and has $2g$ generators a_i, b_i $(i = 1, \dots, g)$ subject to one relation $[a_1, b_1][a_2, b_2] \cdots [a_g, b_g] = 1$. The subgroup structure of Π is well known. Namely, if H is a subgroup of Π of finite index n, then H is again a surface group of genus $n(g-1)+1$. If n is infinite, then H is free.

The algebraic fundamental group $\Gamma = \pi_1(X)$ in the sense of SGA-1 [1971] is the profinite completion of the fundamental group $\pi_1^{top}(X)$ in the topological sense (see Exp. 10, p. 272 in [SGA-1]). It follows that the *profinite surface group* $\pi_1(X)$ has exactly the same presentation. However, the subgroup structure of Γ has not been described. First note that subgroups of a free profinite group are not necessarily free; they are so called projective groups or equivalently profinite groups of cohomological dimension 1. It is possible to characterize projective subgroups of Γ in terms of their index. Indeed, a subgroup H of Γ is projective if and only if $[G : H]$ viewing as supernatural number $\prod p^{n_p}$ has infinite p-component for every p (see Proposition 2 below), so that the situation here is somewhat similar to the discrete one. However, this is as far as we can go: there is no satisfactory description of projective profinite groups.

The situation with normal subgroups of a free profinite group is much better. O.V. Melnikov [M] described normal subgroups of free profinite groups up to isomorphism (see also Chapter 8 in [RZ]). So it is natural to ask whether every projective normal subgroup is isomorphic to a normal subgroup of a free profinite group. The objective of this paper is to answer this positively. In fact, we prove this also for characteristic subgroups.

Theorem Let $\Gamma = \Gamma_g$ be a profinite surface group of genus g and N be a projective normal (resp. characteristic) subgroup of Γ. Then N is isomorphic to a normal (resp. characteristic) subgroup of a free profinite group of countable rank.

Actually we prove the result first for so called accessible subgroups (i.e., subgroups which are subnormal in every finite image). Then using Melnikov's description of them we prove the theorem above. We do not know whether this theorem holds if the characteristic is positive.

This theorem allows us to give the complete solution of the congruence subgroup problem for aritmetic lattices in $\mathrm{SL}_2(\mathbf{R})$. Namely we prove in Section 3 that the congruence kernel of any such arithmetic group is isomorphic to a free profinite group of countable rank.

Section 1. Projective subgroups

We collect in the next lemma some properties of a profinite surface group.

* Supported by CNPq.

Lemma 1.1. *Let $\Gamma = \Gamma_g$ be the profinite completion of the fundamental group Π of a compact surface M of genus g, where $g > 0$ if the surface is orientable and $g > 1$ if not. Let p be a prime. Then:*

(i) The maximal pro-p quotient $\Gamma(p)$ of Γ is the pro-p completion of Π and $\Gamma(p)$ is a Demushkin group.

(ii) If L is an open subgroup of Γ of index divided by p then the restriction

$$Res\colon H^2(\Gamma, \mathbf{F}_p) \longrightarrow H^2(L, \mathbf{F}_p)$$

is the zero map.

Proof: (i) It is easy to see that $\Gamma(p)$ is the pro-p completion of Π. By Exer. 2, p. 43 [Serre] $\Gamma(p)$ is a Demushkin group.

(ii) The natural embedding $L \longrightarrow \Pi$ corresponds to the finite covering $\eta\colon S \longrightarrow M$ and so the corestriction of homology groups

$$Cor\colon H_2(L \cap \Pi, \mathbf{F}_p) \longrightarrow H_2(\Pi, \mathbf{F}_p)$$

coincides with the homomorphism

$$H_2(S, \mathbf{F}_p) \longrightarrow H_2(M, \mathbf{F}_p)$$

induced by η. Therefore it is just multiplication by the index $[\Pi : (\Pi \cap L] = [\Gamma : L]$ and so is the zero map. Hence, the dual map $Res\colon H^2(\Pi, \mathbf{F}_p) \longrightarrow H^2(\Pi \cap L, \mathbf{F}_p)$ is the 0-map. Consider a commutative diagram

$$\begin{tikzcd}
H^2(\Gamma, \mathbf{F}_p) \arrow[r, "Res"] \arrow[d] & H^2(L, \mathbf{F}_p) \arrow[d] \\
H^2(\Pi, \mathbf{F}_p) \arrow[r, "Res"] & H^2(L \cap \Pi, \mathbf{F}_p)
\end{tikzcd} .$$

By Lemma 5.12 (iii) in [EHKZ] the vertical maps are bijective. Therefore, the upper horizontal map is the 0-map as well.

Proposition 1.2. *Let $\Gamma = \Gamma_g$ be a profinite surface group of genus g and L be a subgroup of Γ. Then L is projective if and only if the index $[\Gamma : L]$ (as a supernatural number) has infinite p-component for every prime p.*

Proof: Put $\Gamma = \widehat{\Pi}$, where Π is the corresponding surface group. Let $\mathcal{U}$ be the family of all open subgroups of Γ containing L. Recall that L is the intersection of all $U \in \mathcal{U}$ and hence can be regarded as the inverse limit $L = \varprojlim_{U \in U} U$. Therefore $H^2(L, \mathbf{F}_p) = \varinjlim_{U \in U} H^2(U, \mathbf{F}_p)$, the direct limit.

Consider $U_2 \subset U_1$ in $\mathcal{U}$. If $[U_1 : U_2]$ is divided by p, then by Lemma 1.1 (ii) the restriction $H^2(U_1, \mathbf{F}_p) \longrightarrow H^2(U_2, \mathbf{F}_p)$ is the zero map. Therefore, if the index $[\Gamma : L]$ (as a supernatural number) has infinite p-component, we can choose a cofinal subfamily $\mathcal{V} \subseteq \mathcal{U}$ such that all maps in the direct limit $\varinjlim_{U \in V} H^2(U, \mathbf{F}_p)$ are 0-maps and so $H^2(L, \mathbf{F}_p) = 0$.

On the other hand, if the index $[\Gamma : L]$ (as a supernatural number) has finite p-component then there exists an open subgroup $U \in \mathcal{U}$ such that a Sylow subgroup L_p of L is also a Sylow subgroup of U. But any subgroup of finite index of Π is also a surface group. Therefore any open subgroup U of Γ is the profinite completion of the surface group $U \cap \Pi$. Hence, by Lemma 1.1 (ii) $H_2(U, \mathbf{F}_p) \neq 0$. But the restriction $H^2(U, \mathbf{F}_p) \longrightarrow H^2(L_p, \mathbf{F}_p)$ is an injection (see Corollary 6.7.7 in [RZ]), so $H^2(L_p, \mathbf{F}_p) \neq 0$. It follows that $H^2(L, \mathbf{F}_p) \neq 0$.

Since L is projective if and only if $H^2(L, \mathbf{F}_p) = 0$ for every p the result follows.

Note that a similar description of projective subgroups in terms of index holds also for absolute Galois group of $\mathbf{Q}_p$ (see [R, p. 291, Corollary 7.4).

Section 2. Normal projetive subgroups

For the reader convinience we begin this section with Melnikov's characterization of accessible, normal and characteristic subgroups of free profinite groups. We shall do it for second countable profinite groups only (i.e. groups that has countable base of open subsets), since this is sufficient for our purpose and simplifies the terminology.

A closed subgroup H of a profinite group G is said to be *accessible* if there exists a chain of closed subgroups of G

$$H = G_\mu \leq \cdots \leq G_\lambda \leq \cdots \leq G_2 \leq G_1 = G, \tag{1}$$

indexed by the ordinals smaller than a certain ordinal μ, such that

(i) $G_{\lambda+1} \triangleleft G_\lambda$ for all ordinals $\lambda \leq \mu$, and

(ii) if ν is a limit ordinal such that $\nu \leq \mu$, then $G_\nu = \bigcap_{\lambda \leq \nu} G_\lambda$.

Observe that H is accessible if and only if the image of H is subnormal in every finite quotient of G.

For a group G denote by $M(G)$ the intersection of maximal normal subgroups of G and by $R_p(G)$ the kernel of the epimorphism to the maximal pro-p quotient.

If S is a finite simple group $M_S(G)$ will denote the kernel of the epimorphism to the maximal direct power of S; if S is a finite p-group we shall use the notation $M_p(G)$.

A second countable profinite group is said to be homogeneous if any embedding problem:

$$\begin{tikzcd} & G \arrow[d, "f"] \\ A \arrow[r, two heads, "\alpha"] & B \end{tikzcd} \qquad (1),$$

is solvable for A, B finite, $K := \mathrm{Ker}(\alpha)$ minimal normal and $K \leq M(A)$ (this means to find an epimorphism $G \longrightarrow A$ that makes the diagram commutative).

The next theorem collects facts originally proved by Melnikov about homogeneous profinite groups that also can be found in Chapter 8 of [RZ].

Theorem 2.1. *Let G be a second countable profinite group.*
Then

(i)
G is homogeneous if and only if it is isomorphic to an accessible subgroup of free profinite group of countable rank;

(ii) G is isomorphic to a normal subgroup of a free profinite group of countable rank if and only if G is homogeneous and $G/M_p(G)$ is either trivial or infinite for every p;

(iii) G is isomorphic to a caracteristic subgroup of a free profinite group if and only if G is homogeneous and $G/M_S(G)$ is either trivial or infinite for every finite simple group S.

Theorem 2.2. *Let $\Gamma = \Gamma_g$ be a profinite surface group of genus g and N a projective accessible subgroup of Γ.*

Then N is isomorphic to an accessible subgroup of infinite index of a free profinite group.

Proof:

By Theorem 2.1 we need to solve the following embedding problem for N:

$$\begin{tikzcd} & N \arrow[d, "f"] \\ A \arrow[r, two heads, "\alpha"] & B \end{tikzcd} \qquad (1),$$

where A, B are finite, $K := \mathrm{Ker}(\alpha)$ is minimal normal and $K \leq M(A)$. If α does not split, then any homomorphism $N \longrightarrow A$ that makes (1) commutative is an epimorphism and so the result follows from the projectivity of N. Thus we may assume that $A = K \rtimes B$.

By Lemma 8.3.8 in [RZ-2000] there exists an open subgroup U of Γ_g containing N and an epimorphism $\varphi : U \longrightarrow B$ such that $\varphi_{|N} = f$. Since an open subgroup of Γ_g is again a profinite surface group, replacing Γ_g by U we may assume the existence of the following commutative diagram:

$$\begin{tikzcd} & N \arrow[r] \arrow[d, "f"] & \Gamma_g \arrow[dl, "\varphi"] \\ A \arrow[r, two heads, "\alpha"] & B & \end{tikzcd} \qquad (2),$$

where the top horizontal map is the natural inclusion. Moreover, as N is projective, 2 divides $[\Gamma_g : N]$ and so passing to an open subgroup of index 2 containing N if necessary, we may assume to be in oriented case. Let U_i be the family of all open subgroups of Γ_g containing N. Then $\varphi_i := \varphi_{|U_i}$ is an epimorphism for every i. Note that every U_i is again a profinite surface group and so has a presentation $U_i = \langle x_1, y_1, \ldots x_{g_i}, y_{g_i} \mid \prod_{j=1}^{g_i}[x_i, y_i]\rangle$, where the genus g_i of U_i can be computed by the formular $g_i - 1 = [\Gamma_g : U_i](g-1)$. This means that we can choose i with the number of generators of U_i sufficiently large, so that there exists i such that reordering generators x_j, y_j of U_i if necessary, we have $\varphi(x_1) = \varphi(x_{j_1}) = \cdots = \varphi(x_{j_n})$ and $\varphi(y_1) = \varphi(y_{j_1}) = \cdots = \varphi(y_{j_n})$, where $n = |A|$ and $j_l > j_k$ whenever $l > k$. We shall use the notation x^y for $y^{-1}xy$ in the argument to follow. Suppose $j_1 \neq 2$. Then $\prod_{j=1}^{g_i}[x_j, y_j] = [x_1, y_1][x_{j_1}, y_{j_1}]([x_2, y_2] \cdots [x_{j-1}, y_{j-1}])^{[x_{j_1}, y_{j_1}]}[x_{j+1}, y_{j+1}] \cdots [x_{g_i}, y_{g_i}]$ so replacing the generators $x_2, y_2, \ldots, x_{j-1}, y_{j-1}$ by $x_2^{[x_{j_1}, y_{j_1}]}, y_2^{[x_{j_1}, y_{j_1}]}, \ldots x_{j-1}^{[x_{j_1}, y_{j_1}]}, y_{j-1}^{[x_{j_1}, y_{j_1}]}$ we may assume that $j_1 = 2$. Continuing similarly, we in fact may assume that $j_2 = 3, \ldots j_n = n+1$. Let η be a map the sends $x_1, x_2, \ldots x_n$ to $\varphi(x_1)k$ for some $1 \neq k \in K$ and coincides with φ on the other generators. Then η extends to a homomorphism if

$$[\eta(x_1), \eta(y_1)] \ldots [\eta(x_{g_i}), \eta(y_{g_i})] = 1$$

(since this would mean that the homomorphism from a free profinite group $F(x_1, y_1, \ldots, x_{g_i}, y_{g_i}) \longrightarrow A$ extending η factors through U_i). Now putting

$$k_0 := k^{-\varphi([x_1 y_1])} k^{\varphi(y_1)}$$

one has

$$\begin{aligned} &[\eta(x_1), \eta(y_1)] \cdots [\eta(x_{g_i}), \eta(y_{g_i})] = \\ &([\varphi(x_1)k, \varphi(y_1)])^n [\varphi(x_{n+1}), \varphi(y_{n+1})] \cdots [\varphi(x_{g_i}), \varphi(y_{g_i})] = \\ &([\varphi(x_1), \varphi(y_1)]k_0)^n [\varphi(x_{n+1}), \varphi(y_{n+1})] \cdots [\varphi(x_{g_i}), \varphi(y_{g_i})] \end{aligned}$$

Then putting $b = [\varphi(x_1), \varphi(y_1)]$ and taking into account that $b = [\varphi(x_i), \varphi(y_i)]$ for all $i = 1, \ldots, n$ one has

$$\begin{aligned} &[\eta(x_1), \eta(y_1)] \cdots [\eta(x_{g_i}), \eta(y_{g_i})] = \\ &b k_0 k_0^{b^{-1}} k_0^{b^{-2}} \cdots k_0^{b^{-n}} b^{n-1} [\varphi(x_{n+1}), \varphi(y_{n+1})] \cdots [\varphi(x_{g_i}), \varphi(y_{g_i})]. \end{aligned}$$

Let $m = |B|$ and $t = |K|$, so that $n = mt$. Then

$$k_0 k_0^{b^{-1}} k_0^{b^{-2}} \cdots k_0^{b^{-n}} = (k_0 k_0^{b^{-1}} k_0^{b^{-2}} \cdots (k_0^{b^{-m+1}}))^t = 1$$

so that

$$\begin{aligned} &[\eta(x_1), \eta(y_1)] \cdots [\eta(x_{g_i}), \eta(y_{g_i})] = [\varphi(x_1), \varphi(y_1)] \cdots [\varphi(x_{g_i}), \varphi(y_{g_i})] = \\ &b^n \varphi([x_{n+1}, y_{n+1}] \cdots [x_{g_i}, y_{g_i}]) = \varphi([x_1, y_1] \cdots [x_{g_i}, y_{g_i}]) = 1 \end{aligned}$$

as needed.

Thus there exists a homomorphism $\psi\colon U_i \longrightarrow A$ such that $\varphi = \alpha\psi$. But K is minimal normal and $\psi(x_1^{-1}x_{n+1}) = k \neq 1$ so ψ is an epimorphism. Now $\alpha(\psi(N) = B$ and so $\psi(N)M(A) = A$. Since $\psi(N)$ is a subnormal subgroup of A by Proposition 8.3.6 in [RZ] $\psi(N) = A$ as needed. □

Corollary 2.3.

(i) An accessible projective subgroup of a profinite surface group is a virtually free profinite group.

(ii) two accessible projective subgroups G_1 and G_2 of profinite surface groups Γ_{g_1} and Γ_{g_2} are isomorphic if and only if $G_1/M_S(G_1) \cong G_2/M_S(G_2)$ for every finite simple group S.

(iii) An accessible projective subgroup of a profinite surface group is a free profinite group of countable rank if and only if $G/M_S(G)$ is infinite for every finite simple group S.

Proof: Theorem 2.2 together with Corollary 8.5.8 in [RZ] implies (i) and together with Theorem 8.5.2 in [RZ] implies (ii). Item (iii) is a consequence of (ii) and Theorem 2.2. □

Theorem 2.4. *Let $\Gamma = \Gamma_g$ be a profinite surface group of genus g and N a projective normal subgroup of Γ. Then N is isomorphic to a normal subgroup of a free profinite group of countable rank.*

Proof: By Theorem 2.2 N is isomorphic to an accessible subgoup of infinite index of a free profinite group. Therefore, by Theorem 2.1 we just need to show that the maximal elementary abelian pro-p quotient $N/M_p(N)$ of N is infinite or trivial.

Suppose $N/M_p(N)$ is finite. Then $M_p(N)$ is open in N and therefore there exists an open subgroup U of Γ such that $M_p(U) \cap N = M_p(N)$. Moreover, N is the intersection of such Us. Put $\bar{U} := U/R_p(U)$, $\bar{N} = NR_p(U)/R_p(U)$. We shall show that $[\bar{U} : \bar{N}]$ is infinite.

Since U is a profinite surface group of genus $g_U = [\Gamma : U](g-1)+1$, when $[\Gamma : U]$ growes, g_U also growes and so $U/M_p(U)$ growes as well. It means that $[U/M_p(U) : NM_p(U)/M_p(U)]$ growes when U tends to N, since $NM_p(U)/M_p(U)$ is bounded by $N/M_p(N)$. But $[\bar{U} : \bar{N}]$ is not less than $[U/M_p(U) : NM_p(U)/M_p(U)]$ which implies that it is infinite.

Since $\bar{U}$ is a Demushkin group (see Lemma 1.1 (i)), by Exercies 5 on p. 44 in [Serre] $\bar{N}$ is free pro-p.

Note that $|\bar{N}/M_p(\bar{N})| \leq |N/N_p(M)| < \infty$ and the abelianization $\bar{U}/\bar{U}'$ is a free abelian pro-p group of rank $2g_U$. Since the rank of $\bar{N}/\bar{N}'$ is not bigger than the rank of $\bar{N}$ we can choose U such that $\bar{N}\bar{U}'/\bar{U}'$ has rank smaller than rank$(\bar{U}/\bar{U}') - 2$. Pick $x \in \bar{U} \setminus \bar{N}$ such that $x\bar{U}'$ is a generator of $\bar{U}/\bar{U}'$ lying outside of $\bar{N}\bar{U}'/\bar{U}'$. Then $x\bar{U}' \cap \bar{N}\bar{U}'/\bar{U}' = \bar{U}'$ and $U/\langle x, \bar{N}\rangle U'$ is infinite procyclic. It follows that $\langle x\rangle \cap \bar{N} = 1$ and $[\bar{U} : \langle x, \bar{N}\rangle]$ is infinite. But infinity of $[\bar{U} : \langle x, \bar{N}\rangle]$ implies that $\bar{N}$ is free pro-p by Exercies 5 on p. 44 in [Serre]. On the other hand, if $\bar{N}$ is non-trivial $\langle x, \bar{N}\rangle = \bar{N} \rtimes \langle x\rangle$ has cohomological dimension 2, because as rank of $\bar{N}$ is finite it is the sum of cohomological dimensions of $\bar{N}$ and $\langle x\rangle$ (see [RZ, p. 275 Prop. 7.4.2. This proves that $\bar{N}$ is trivial and therefore so is $N/M_p(N)$ as required.

Thus $\bar{N}$ is free pro-p of infinite rank and the theorem is proved. □

Theorem 2.4 together with Theorem 8.7.1 in [RZ] implies the following

Corollary 2.5. *Every proper open subgroup of N is a free profinite group.*

Theorem 2.6. *Let $\Gamma = \Gamma_g$ be a profinite surface group of genus g and N a projective characteristic subgroup of Γ. Then N is isomorphic to a normal characteristic subgroup of a free profinite group of countable rank.*

Proof: Let S be a finite simple group. By Theorem 2.1 (iii) we just need to show that $N/M_S(N)$ is infinite or trivial. As 2 divides $[\Gamma : N]$ by Proposition 1.2, passing to an open subgroup of index 2 containing N, we may assume that we are in orientable case. Note that an oriented surface group of genus g can be mapped onto free group of rank g (just identify generators x_i with y_i) and therefore a free profinite group F_g of rank g is an epimorphic image of Γ_g. It follows that $F_g/M_S(F_g)$ is a quotient of $\Gamma_g/M_S(\Gamma_g)$. We conclude that if g is growing the order of $\Gamma_g/M_S(\Gamma_g)$ goes to infinity.

Suppose now that $N/M_S(N)$ is finite non-trivial. Then there exists a proper open normal subgroup U of Γ_g such that $M_S(U) \cap N = M_S(N)$. Moreover, we can choose U having this property of as large index as we wish, so that we may assume that the order of $U/M_S(U)$ is bigger than the order of $N/M_S(N)$. But $N/M_S(N)$ is characteristic in $U/M_S(U)$ so $N/M_S(N) = 1$ because $U/M_S(U) \cong \prod S$. □

Following [LS] we shall call a group G to be an F-group if G has presentation

$$\begin{aligned} G =&\langle a_1, b_1, \dots, a_n, b_n, c_1, \dots c_t, d_1, \dots d_s | \\ &c_1^{\gamma_1}, \dots, c_t^{\gamma_t}, d_1^{-1} \cdots d_s^{-1} c_1^{-1} \cdots c_t^{-1} [a_1, b_1] \cdots [a_n, b_n]\rangle \end{aligned}$$

where $n, s, t \geq 0$, and $\gamma_i > 1$.

By Proposition III.7.4 in [LS] any subgroup of finite index of an F-group is again an F-group and so a torsion free subgroup of an F-group of finite index is a surface group. Using this we can deduce the following

Corollary 2.7. *Let G be a profinite F-group, i.e. the profinite completion of an F-group. Then a projective accessible (resp. normal, characteristic) subgroup U of G is isomorphic to an accessible (resp. normal, characteristic) subgroup of a free profinite group.*

Proof: First note that the subset of torsion elements of G is closed. Indeed, this is true for every profinite group that has open torsion free subgroup L, since in this case the order of torsiont elements is bounded by $[G : L]$ and the limit of any converegent sequence of non-trivial torsion elements is again a non-trivial torsion element. By Proposition III.7.12 in [LS], an F-group contains a torsion free subgroup of finite index, therefore so is G.

Now since U is projective, it is torsion free. Since U is the intersection of all open subgroups of G containing U, there exists a torsion free open subgroup of G containing U. Now use the fact just mentioned before the statement of the corollary. □

Remark. The results of this paper are valid also for pro-$\mathcal{C}$ groups, where $\mathcal{C}$ is a class of finite groups closed for normal subgroups, extensions and quotients. If $\mathcal{C}$ is the class of finite p-groups, then Γ is a Demushkin group for which the results of the paper are known. Otherwise, $\mathcal{C}$ involves at least two primes and all the proofs are the same except the case when $\mathcal{C}$ does not contain 2-groups. In the latter case the proofs of Theorem 2.2 and 2.6 have to be adapted for non-oriented case, since one can not pass to the orientable case.

The proof of Theorem 2.2 can be performed similarly using a presentation $\langle x_1, \dots, x_g \mid x_1^2 x_2^2 \cdots x_g^2 \rangle$.

For the proof of Theorem 2.6 note that Γ is prosolvable in this case and so one needs to show that $\Gamma/M_p(\Gamma)$ is infinite or trivial. But this is exactly what is done in the proof of Theorem 2.4.

Section 3. The congruence kernel of arithmetic groups in $\mathbf{SL}_2(\mathbf{R})$

Let k be a global field and $\mathbf{G}$ be a connected, simply-connected algebraic group over k. We denote the set of k-rational points, $\mathbf{G}(k)$, by G. Let $\mathbf{G}(\mathcal{O})$ be the group of S-integral poins in G, where $\mathcal{O} = \mathcal{O}(S)$ is the *ring of S-integers* in k, for some non-empty, finite set S of places k, containing all the archimedean places. Define two tologies on $\mathbf{G}(\mathcal{O})$, the profinite topology and the congruence topology. These two topologies are defined by taking as basis of neighbourhoods of the identity all subgroups of finite index and the congruence subgroups $\mathbf{G}(\mathfrak{a}) = \{g \in \mathbf{G}(\mathcal{O})\} \mid g \equiv 1 (\mathrm{mod}\ \mathfrak{a})\}$ corresponding to non-zero ideals $\mathfrak{a}$ of $\mathcal{O}(\mathcal{S})$. Note that every congruence subgroup has finite index in $\mathbf{G}(\mathcal{O})$. The congruence kernel $C = C(G)$ is the kernel of the natural epimorphism $\widehat{\mathbf{G}(\mathcal{O})} \longrightarrow \bar{\mathbf{G}}(\mathcal{O})$, where $\widehat{\mathbf{G}(\mathcal{O})}$ is the completion with respect to the topology of all subgroups of finite index of $\mathbf{G}(\mathcal{O})$ and $\overline{\mathbf{G}(\mathcal{O})}$ is the completions of $\mathbf{G}(\mathcal{O})$ with respect to the topology of the congruence subgroups. The congruence subgroup problem, in its modern interpretation (see [Mar] p. 268), consists of describing of the congruence kernel C.

An *arithmetic* subgroup Γ of G is a subgroup commensurable with $\mathbf{G}(\mathcal{O}(S))$ for a suitable ring $\mathcal{O}(S)$, i.e. a subgroup that has a common subgroup of finite index with $\mathbf{G}(\mathcal{O}(S))$. Then the congruence subgroup problem may also be considered for Γ. Indeed, a congruence subgroups of Γ are $\Gamma(\mathfrak{a}) := \Gamma \cap \mathbf{G}(\mathfrak{a})$ and the congruence completion of Γ is $\bar{\Gamma} = \varprojlim_{\mathfrak{a}} \Gamma/\Gamma(\mathfrak{a})$. Then one has the natural epimorphism $\widehat{\Gamma} \longrightarrow \bar{\Gamma}$ and the congruence kernel of Γ is the kernel of this homomorphism. Note that the closure of $\Gamma(\mathfrak{a})$ in $\widehat{\Gamma}$ coincides with the profinite completion $\widehat{\Gamma(\mathfrak{a})}$ and coincides with the preimage in $\widehat{\Gamma}$ of the closure of $\Gamma(\mathfrak{a})$ in $\bar{\Gamma}$. Therefore, $\widehat{\Gamma(\mathfrak{a})}$ contains the congruence kernel for every $\mathfrak{a}$.

Our aim is to describe the congruence kernel for arithmetic groups in $SL_2(\mathbf{R})$. We remind the construction of an arithmetic group in our situation.

Let k be a totally real number field. Set $[k : \mathbf{Q}] = r$ and let $\sigma_1, \dots, \sigma_r : k \longrightarrow \mathbf{R}$ be the r distinct embeddings of k in $\mathbf{R}$. Let D be a quaternion algebra over k such that $D_{\sigma_1} = D \otimes_k^{\sigma_1} \mathbf{R} \cong M_2(\mathbf{R})$ and for $i = 2, \dots, r$ the algebra $D_{\sigma_i} = D \otimes_k^{\sigma_i} \mathbf{R}$ is the (division) algebra of Hamiltonian quaternions. Let $\mathcal{O}$ be the ring of integers of k and $\mathcal{O} \longrightarrow \mathbf{R} \times \cdots \times \mathbf{R}$ defined by $a \longrightarrow (\sigma_1(a), \dots, \sigma_r(a))$. Consider $\mathbf{G} = SL_1(D)$, the algebraic k-group associated with the group of elements in D having reduced norm 1.

Note that $SL_1((D_{\sigma_1}(\mathbf{R})) = SL_2(\mathbf{R})$ and $SL_1(D_{\sigma_i}(\mathbf{R}))$ is compact for all $i \geq 2$. The group $\mathbf{G}(\mathcal{O})$ of integral points is $SL_1(A)$, where A is an order of D (see Chapter IV, §1 in [V]). Then we have a diagonal embedding $\mathbf{G}(\mathcal{O}) \longrightarrow SL_2(\mathbf{R}) \times SL_1(D_{\sigma_2}(\mathbf{R})) \times \cdots \times SL_1(D_{\sigma_r}(\mathbf{R}))$. The projection of the image of $\mathbf{G}(\mathcal{O})$ on the first coordinate gives an arithmetic group in $SL_2(\mathbf{R})$ and all arithmetic groups in $SL_2(\mathbf{R})$ are obtained in this manner. The set S in this case consists of all archimedean places. Observe that $\prod_{v \in S} \mathbf{G}(\mathcal{O}_v)$ is not compact and so by Theorem 7.12 in [PR] the strong approximation holds for $\mathbf{G}$ with respect to S, i.e. $\overline{\mathbf{G}(\mathcal{O})} = \prod_{v \notin S} \mathbf{G}(\mathcal{O}_v)$. The congruence kernel C then is the kernel of the natural epimorphism $\widehat{\mathbf{G}(\mathcal{O})} \longrightarrow \mathbf{G}(\hat{\mathcal{O}}) = \prod_{v \notin S} \mathbf{G}(\mathcal{O}_v)$, where $\hat{\mathcal{O}} = \prod_{v \notin S} O_v$ is the profinite completion of $\mathcal{O}$. Note that in fact, $\mathbf{G}(\mathcal{O}_v) \cong SL_2(\mathcal{O}_v)$ for almost all v. Indeed, $A_v = A \otimes_{\mathcal{O}} \mathcal{O}_v$ is a maximal order in $D_v = D \otimes_k k_v$ for almost all v (see Section 1.5 in [PR]). On the other hand, $\mathbf{G}(k_v) = SL_2(k_v)$ for almost all v (see [V], p. 104), so by Theorem 2.3 in [V] $\mathbf{G}(\mathcal{O}_v) \cong SL_2(\mathcal{O}_v)$ for almost all v.

An arithmetic group Γ in $SL_2(\mathbf{R})$ is a *Fuchsian* group, i.e. a discrete subgroup in $SL_2(\mathbf{R})$. Moreover, it is of finite covolume in $SL_2(\mathbf{R})$, see Theorem 5.7 in [PR]. Therefore by the Fricke-Klein theorem (see Proposition 2.4 in [I]) Γ is an F-group and so we have the following presentation

$$\begin{aligned}\Gamma = &\langle a_1, b_1, \dots, a_n, b_n, c_1, \dots c_t, d_1, \dots d_s \mid \\ & c_1^{\gamma_1}, \dots, c_t^{\gamma_t}, d_1^{-1} \cdots d_s^{-1} c_1^{-1} \cdots c_t^{-1} [a_1, b_1] \cdots [a_n, b_n] \rangle\end{aligned}$$

If Γ is torsion-free then c_i are missing in the presentation above, so in this case the group G is either a surface group (when d_i are missing in the presentation) or a free group (when d_i are present there). The main result of this section is the following

Theorem 3.1. *Let Γ be an arithmetic group in $SL_2(\mathbf{R})$. Then the congruence kernel $C = C(\Gamma)$ is a free profinite group of countable rank.*

Proof: As was mentioned at the end of the second paragraph of the section, the profinite completion of any congruence subgroup contains the congruence kernel, so passing to a suitable congruence subgroup of Γ we may assume that Γ is torsion-free and is a subgroup of $\mathbf{G}(\mathcal{O})$. Then as was observed above Γ is either free or a surface group. As explained above $SL_2(\mathcal{O}_v) \cong \mathbf{G}(\mathcal{O}_v) \leq \bar{\Gamma}$ for almost all v. It follows that $\bar{\Gamma}$ contains central subgroup C of order 2, namely the group generated by the matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

in $SL_2(\mathcal{O}_v)$. Let N be its preimage in $\widehat{\Gamma}$. Then C is subgroup of N of index 2. The congruence completion $\bar{\Gamma}$ has an infinite Sylow p-subgroup for every p, because $\mathbf{G}(\mathcal{O}_v)$ has, where v is a p-adic valuation. Hence the index $[\widehat{\Gamma} : N] = |\bar{\Gamma}/C|$ as supernatural number has infinite p-component for every prime p. Therefore by Proposition 1.2, N is a projective normal subgroup of Γ. Now we can apply Corollary 2.5 to deduce that C is a free profinite group of countable rank.

Aknowledgement. The author expresses special thanks to Alex Lubotzky for discussions that led to results of Section 3. The author is also very grateful to Moshe Jarden for reading the paper and giving helpful comments for revising it and to Andrei Rapinchuk and Alexei Krassilnikov for fruitful discussions.

REFERENCES

[EHKZ] A. Engler, D. Haran, D. Kochloukova, P.A. Zalesskii, Normal Subgroups of Profinite Groups of Finite Cohomological Dimension, *J. London Math. Soc.* **69** (2004) 317-332.
[I] H. Iwaniec, Topics in Classical Automorphic Forms, Graduate Studies in Math., **17**, AMS, Rhode Island 1997.
[LS] R.S. Lyndon, P.E. Schupp, Combinatorial Group theory, Springer-Verlag, Berlin 1977.
[Mar] G.A. Margulis, Discrete Subgroups of Semisimple Lie Groups, Springer, 1991.
[M] O. V. Mel'nikov, Normal subgroups of free profinite groups, *Izv. Akad. Nauk*, **42** (1978) 3–25. English transl.: *Math. USSR Izvestija*, **12** (1978) 1–20.
[PR] V.P. Platonov and A.S. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1994.
[R] L. Ribes, Introduction to Profinite Groups and Galois Cohomology, Queens Papers Pure Appl. Math., 24, Kingston, Canada 1970.
[RZ] L. Ribes and P.A. Zalesskii, Profinite Groups. Springer 2000.
[Serre] J.-P. Serre, Galois Cohomology, Springer-Verlag, Berlin, 1997.
[SGA-1] Revêtements Étales et Groupe Fondamental, Lect. Notes Math., **224**, Springer 1971, Berlin.
[V] M.-F. Vingéras, Arithmétique des Algébres de Quaternions. Lect. Notes in Math. **800**, Berlin 1980.

Departamento de Matemática
Universidade de Brasília
70910-900 Brasília-DF
Brazil

pz@mat.unb.br