# Decomposing some finitely generated groups into free products with amalgamation

V.V. Benyash-Krivetz
Institute of Mathematics,
National Academy of Sciences of Belarus,
Surganova str., 11
220072, Minsk
Belarus

**Abstract**

In this paper we study the problem of decomposing finitely generated groups into non-trivial free products with amalgamation. We prove that if $\dim X^s(\Gamma) \geq 2$, where $X^s(\Gamma)$ is the character variety of irreducible representations of $\Gamma$ into $\mathrm{SL}_2(\mathbb{C})$, then $\Gamma$ is a non-trivial free product with amalgamation. We also consider a generalized triangle group $\Gamma = \langle a, b \mid a^n = b^k = R^m(a, b) \rangle$. It is proved that if one of the generators of $\Gamma$ has an infinite order, then $\Gamma$ is a non-trivial free product with amalgamation. In general case we find some sufficient conditions under which $\Gamma$ is a non-trivial free product with amalgamation.

# Introduction

We say that a group $G$ is a non-trivial free product with amalgamation if $G = G_1 *_A G_2$, where $G_1 \neq A \neq G_2$ (see [1]). Wall [2] posed the following question:

*Which one-relator groups are non-trivial free products with amalgamation?*

Let $G = \langle g_1, \dots, g_m \mid R_1 = \dots = R_n = 1 \rangle$ be a group with $m$ generators and $n$ relations. If $\operatorname{def} G = m - n \geq 2$, then it is proved in [4] that $G$ is a non-trivial free product with amalgamation; in particular, any group $G$ with $m \geq 3$ generators and one relation is a non-trivial free product with amalgamation. The case of groups with two generators and one relation is more complicated. For example, obviously, a free abelian group $G = \langle a, b \mid [a, b] = 1 \rangle$ of rank 2, where $[a, b] = aba^{-1}b^{-1}$, is not a non-trivial free product with amalgamation. Other examples are given by groups $G_n = \langle a, b \mid aba^{-1} = b^n \rangle$. Clearly, $G_n$ is solvable for any $n$ and bearing in mind results in [3], it is easy to show that $G_n$ is not a non-trivial free product with amalgamation for $n \neq -1$. The following conjecture was stated in [4].

Conjecture 1 *Let $G = \langle a, b \mid R^m(a, b) = 1 \rangle$, $m \geq 2$, be a group with two generators and one relation with torsion. Then $G$ is a non-trivial free product with amalgamation.*

Zieschang [5] studied the problem of decomposing discontinuous groups of transformations of the plane into non-trivial free products with amalgamation. He has given a complete answer to the question when such a group is a non-trivial free product with amalgamation in all cases except for the groups $H_1 = \langle a, b \mid [a, b]^n = 1 \rangle$ and $H_2 = \langle a, b \mid a^2 = [a, b]^n = 1 \rangle$, $n \geq 2$. Rosenberger [6] has proved that the groups $H_1$ and $H_2$ are non-trivial free products with amalgamation if $n$ is not a power of 2. In the recent papers [7, 8] it is proved that $H_1$ is a non-trivial free product with amalgamation for arbitrary $n \geq 2$. An independent proof of this fact was given in [9, 10].

In the present paper we study a more general case. Namely, we consider the so-called *generalized triangle groups* $G$ having a presentation of the form

$$G = \langle a, b \mid a^m = b^n = R^l(a, b) = 1 \rangle,$$

where $l \geq 2$, $R(a, b)$ is a cyclically reduced word in the free group on $a$, $b$. Not all of these groups are non-trivial free products with amalgamation. For example, Zieschang [5] has proved that *the ordinary triangle group*

$$T(m, n, l) = \langle a, b \mid a^m = b^n = (ab)^l = 1 \rangle$$

with $m, n, l \geq 2$ is not a non-trivial free product with amalgamation. On the other hand, it is shown in [10] that a group $G = \langle a, b \mid a^{2m} = R^l(a, b) = 1 \rangle$, where $m = 0$ or

$m \geq 1$ and $l \geq 2$, is a free product with amalgamation. In Theorems 2 and 3 we prove more general results about decomposing generalized triangle groups into non-trivial free products with amalgamation.

Theorem 1 states that a finitely generated group $\Gamma$ is a non-trivial free product with amalgamation if the dimension of some algebraic variety (the so-called character variety of irreducible representations of $\Gamma$ into $\mathrm{SL}_2(\mathbb{C})$) is more than 1. To formulate this result, we recall some notations and facts from the geometric representation theory (see also [11, 12, 13, 14]).

Let $\Gamma = \langle g_1, \ldots, g_m \rangle$ be a finitely generated group and let $G \subset \mathrm{GL}_n(K)$ be a connected linear algebraic group defined over an algebraically closed field $K$ of characteristic zero. Obviously, for each homomorphism $\rho : \Gamma \to G(K)$ the set of elements

$$(\rho(g_1), \ldots, \rho(g_m)) \in G(K) \times \cdots \times G(K)$$

satisfies all defining relations of $\Gamma$. So the correspondence $\rho \to (\rho(g_1), \ldots, \rho(g_m))$ is a bijection between the set $\mathrm{Hom}\,(\Gamma, G(K))$ and the set of $K$-points of some affine $K$-variety $R(\Gamma, G) \subset G^m$. The variety $R(\Gamma, G)$ is usually called *the representation variety* of the group $\Gamma$ into the algebraic group $G$.

The group $G$ acts on $R(\Gamma, G)$ in a natural way (by simultaneous conjugation of components) and its orbits are in one to one correspondence with the equivalence classes of representations of $\Gamma$. In the general case the orbits of the group $G$ under this action are not necessarily closed and hence the variety of orbits (the geometric quotient) is not an algebraic variety. However, if $G$ is a reductive group, then one can consider the categorical quotient $X(\Gamma, G) = R(\Gamma, G)/G$ (see [15]). Its points parametrize closed $G$-orbits. In the case $G = \mathrm{GL}_n(K)$ or $G = \mathrm{SL}_n(K)$ an orbit of $G$ is closed if and only if the corresponding representation is completely reducible. Therefore, in this case points of the variety $X(\Gamma, G)$ are in one to one correspondence with the equivalence classes of completely reducible representations of $\Gamma$ into $G$ or, in other words, with characters of representations of $\Gamma$ into $G$.

Throughout this paper we consider only the case $G = \mathrm{SL}_2(K)$ and for brevity we put $R(\Gamma, \mathrm{SL}_2(K)) = R(\Gamma)$ and $X(\Gamma, \mathrm{SL}_2(K)) = X(\Gamma)$. All information about varieties $R(\Gamma)$, $X(\Gamma)$ used in the paper can be found in [12, 16, 17, 18]. We set

$$R^s(\Gamma) = \{\rho \in R(\Gamma) \mid \rho \text{ is irreducible}\}, \qquad X^s(\Gamma) = \pi(R^s(\Gamma)),$$

where $\pi : R(\Gamma) \to X(\Gamma)$ is the canonical projection. It is shown in [12] that $R^s(\Gamma)$ and $X^s(\Gamma)$ are open in Zariski topology subsets of $R(\Gamma)$ and $X(\Gamma)$ respectively. The aim of the present paper is to prove the following theorems.

THEOREM 1 *Let $\Gamma$ be a finitely generated group such that* $\dim X^s(\Gamma) \geq 2$. *Then $\Gamma$ is a non-trivial free product with amalgamation.*

Theorem 2 *Let $\Gamma_n = \langle a, b \mid a^n = b^k = R^m(a,b) = 1\rangle$, where $n, k, m \in \mathbb{Z}$, $n, k, m \geq 2$, and $R(a,b) = a^{u_1}b^{v_1}\dots a^{u_s}b^{v_s}$ is a cyclically reduced word on the free product on $a, b$ such that $0 < u_i < n$, $0 < v_i < k$, and $s \geq 1$. Suppose that there exists $i \in \{1, \dots, s\}$ such that $u_i \geq 2$ and $n = u_i p f$, where $f \in \mathbb{Z}$, $p$ is a prime and $u_i p$ does not divide $u_j$ for $j \neq i$. Then in the following cases the group $\Gamma_n$ is a non-trivial free product with amalgamation:*

*1) $m = 2$, $p$ does not belong to a certain finite set $S$ of primes, which is completely determined by the exponent $k$ and the word $R$;*

*2) $m = 3$ or $m = 2^l > 3$, $p \neq 2$;*

*3) $m > 3$ and $m \neq 2^l$.*

Note that the condition $u_i p \nmid u_j$ for $j \neq i$ in Theorem 2 holds automatically if $u_i = \max_{1 \leq j \leq s} u_j \geq 2$ or $u_i \nmid u_j$ for each $j \neq i$.

Theorem 3 *Let $\Gamma = \langle a, b \mid a^n = R^m(a,b) = 1\rangle$, where $n = 0$ or $n \geq 2$, $m \geq 2$, and $R(a,b) = a^{u_1}b^{v_1}\dots a^{u_s}b^{v_s}$ is a cyclically reduced word on the free product on $a, b$, $s \geq 1$, $0 < u_i < n$. Then $\Gamma$ is a non-trivial free product with amalgamation.*

As a direct consequence of Theorem 3, we obtain the proof of Conjecture 1.

Corollary 1 *Let $\Gamma = \langle a, b \mid R^m(a,b) = 1\rangle$, $m \geq 2$, be a group with two generators and one relation with torsion. Then $\Gamma$ is a non-trivial free product with amalgamation.*

At the end of Section 2 we verify that the group $\Gamma$ introduced in Corollary 1 satisfies the assumptions of Theorem 1, i.e. $\dim X_2^s(\Gamma) = 2$ and therefore we obtain an another proof of Conjecture 1.

Corollary 2 *Fuchsian groups $H_1 = \langle a, b \mid [a,b]^n = 1\rangle$ and $H_2 = \langle a, b \mid a^2 = [a,b]^n = 1\rangle$, $n \geq 2$, are non-trivial free products with amalgamation.*

**Acknowledgments.** This research was carried out with the financial support of the Institute of Mathematics of the National Academy of Sciences of Belarus in the framework of the State Basic Research Programme "Mathematical Structures". This paper was written while the author was visiting the University of Bielefeld as a guest of SFB 343 "Diskrete Strukturen in der Mathematik". I gratefully acknowledge the support and the hospitality of the University of Bielefeld.

# 1. Proof of Theorem 1

In what follows we denote the field of $p$-adic numbers by $\mathbb{Q}_p$, the ring of $p$-adic integers by $\mathbb{Z}_p$, the group of $p$-adic units in $\mathbb{Z}_p$ by $\mathbb{Z}_p^*$ , the $p$-adic valuation by $|\ |_p$, the trace of a matrix $A$ by $\operatorname{tr} A$, and the identity $2 \times 2$ matrix by $E$.

We recall some facts about the character variety $X(\Gamma)$ of representations of a finitely generated group $\Gamma$ into $\mathrm{SL}_2(\mathbb{C})$ (see [12]). For an arbitrary element $g \in \Gamma$ the regular function

$$\tau_g : R(\Gamma) \to \mathbb{C}, \qquad \tau_g(\rho) = \operatorname{tr} \rho(g),$$

is called, usually, *the Fricke character* of the element $g$. It is known that the $\mathbb{Z}$-algebra $T(\Gamma)$ generated by all functions $\tau_g$, $g \in \Gamma$, is finitely generated. If $\tau_{g_1}, \ldots, \tau_{g_s}$ are generators of $T(\Gamma)$, then the $\mathbb{C}$-algebra of $\mathrm{SL}_2(\mathbb{C})$-invariant regular functions $\mathbb{C}[R(\Gamma)]^{\mathrm{SL}_2(\mathbb{C})}$ coincides with $\mathbb{C}[\tau_{g_1}, \ldots, \tau_{g_s}]$. Consider the morphism

$$\pi : R(\Gamma) \to \mathbb{A}^s, \qquad \pi(\rho) = (\tau_{g_1}(\rho), \ldots, \tau_{g_s}(\rho)).$$

It is shown in [12] that the image $\pi(R(\Gamma))$ is closed in $\mathbb{A}^s$. Since $X(\Gamma)$ and $\pi(R(\Gamma))$ are biregularly isomorphic, we will identify $X(\Gamma)$ and $\pi(R(\Gamma))$.

The idea of the proof of Theorem 1 is to construct a representation $\rho : \Gamma \to \mathrm{SL}_2(\mathbb{Q}_p)$ for some prime $p$ such that the group $\rho(\Gamma)$ is dense in $\mathrm{SL}_2(\mathbb{Q}_p)$ in $p$-adic topology. If we do so, Theorem 1 will follows from the following well-known facts:

1) If $H$ is a subgroup of $\mathrm{SL}_2(\mathbb{Q}_p)$ dense in the $p$-adic topology, then $H$ is a non-trivial free product with amalgamation (see [19]).

2) If $f : G_1 \to G_2$ is an epimorphism of groups and $G_2$ is a non-trivial free product with amalgamation, then $G_1$ is such product as well.

Lemma 1 *Let $H$ be a subgroup of $\mathrm{SL}_2(\mathbb{Q}_p)$. Then $H$ is dense in $\mathrm{SL}_2(\mathbb{Q}_p)$ in the $p$-adic topology if and only if $H$ is absolutely irreducible (that is, irreducible over the algebraic closure of $\mathbb{Q}_p$), unbounded, and non-discrete.*

**Proof.** If $H$ is dense in $\mathrm{SL}_2(\mathbb{Q}_p)$, then, obviously, $H$ is absolutely irreducible, unbounded, and non-discrete. Conversely, we first claim that there exists an element $h \in H$ such that $|\operatorname{tr} h|_p > 1$. Indeed, otherwise the traces of all elements of $H$ belong to $\mathbb{Z}_p$, whence the group $H$ is conjugate to a subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ (see [20] or [12, Lemma I.4.3]). This implies that $H$ is bounded which contradicts to our assumptions.

Let $\operatorname{tr} h = p^{-s}\alpha$, where $\alpha \in \mathbb{Z}_p^*$, $s > 0$. The characteristic polynomial of $h$ is of the form $f(y) = y^2 - p^{-s}\alpha y + 1$ and its discriminant is equal to $D = p^{-2s}\alpha^2 - 4 = p^{-2s}(\alpha^2 - 4p^{2s})$. Thus, $D$ is a square in $\mathbb{Q}_p$, whence the roots of $f(y)$ belong to $\mathbb{Q}_p$. It follows that $h$ is conjugate in $\mathrm{SL}_2(\mathbb{Q}_p)$ to a diagonal matrix of the form

$$\operatorname{diag}(\lambda, \lambda^{-1}), \quad \lambda = p^{-s}\gamma, \quad s \geq 0, \quad \gamma \in \mathbb{Z}_p^*. \tag{1}$$

Conjugating $H$, if necessary, we can suppose that $h = \mathrm{diag}(\lambda, \lambda^{-1}) \in H$. Clearly, the unipotent subgroups of $\mathrm{SL}_2(\mathbb{Q}_p)$

$$U_1 = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \Big| a \in \mathbb{Q}_p \right\}, \qquad U_2 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \Big| a \in \mathbb{Q}_p \right\}.$$

generate $\mathrm{SL}_2(\mathbb{Q}_p)$. Therefore, it suffices to show that $U_1, U_2 \subset \overline{H}$, where $\overline{H}$ is the closure of $H$ in the $p$-adic topology.

Take, for example, $U_1$ and let us prove that $U_1 \subset \overline{H}$. To this end, first we show that $\overline{H}$ contains a non-trivial unipotent element $u = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \in \mathbb{Q}_p^*$. Let

$$\Gamma_j = \left\{ \begin{pmatrix} 1+p^j a & p^j b \\ p^j c & 1+p^j d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q}_p) \;\Big|\; a,b,c,d \in \mathbb{Z}_p \right\}$$

be the principal congruence subgroup of the level $j$ in $\mathrm{SL}_2(\mathbb{Q}_p)$. The groups $\Gamma_j$, $j \geq 1$, form a base for the neighborhoods of the identity in $\mathrm{SL}_2(\mathbb{Q}_p)$. The non-discreteness of $H$ implies that for each $j > 0$ there exists an element $E \neq x_j \in H \cap \Gamma_j$. Let

$$x_j = \begin{pmatrix} 1+p^j a_j & p^j b_j \\ p^j c_j & 1+p^j d_j \end{pmatrix},$$

where $a_j, b_j, c_j, d_j \in \mathbb{Z}_p$. Then $\lim_{j\to\infty} x_j = E$. Since $H$ is an absolutely irreducible subgroup of $\mathrm{SL}_2(\mathbb{Q}_p)$, without loss of generality we can assume that almost all elements $b_j$, $c_j$ (with the exception of a finite number) are not equal to 0 (otherwise one can conjugate all $x_j$ by a suitable element $y$ from $H$ and again $\lim_{j\to\infty} y x_j y^{-1} = E$).

Let $c_j = p^{k_j}\varepsilon_j$, where $k_j \geq 0$, $\varepsilon_j \in \mathbb{Z}_p^*$, and let $t_j = [(k_j+j)/(2s)]$ be the integer part of the number $(k_j+j)/(2s)$, where $s$ is defined in (1). Then we have $r_j = k_j + j - 2st_j \in \{0, 1, \ldots, 2s-1\}$. Now consider the following sequence $\{x'_j\}$ of elements of $H$:

$$x'_j = h^{-t_j} x_j h^{t_j} = \begin{pmatrix} 1+p^j a_j & p^{j+2st_j}\gamma^{-2t_j} b_j \\ p^{r_j}\gamma^{2t_j}\varepsilon_j & 1+p^j d_j \end{pmatrix}. \tag{2}$$

The infinite sequence $\{p^{r_j}\gamma^{2t_j}\varepsilon_j\}$ is contained in $\mathbb{Z}_p$; in particular, it is bounded. Therefore, it contains a convergent subsequence

$$a_{j_m} = p^{r_{j_m}}\gamma^{2t_{j_m}}\varepsilon_{j_m}.$$

Since $|a_{j_m}|_p = p^{-r_{j_m}} \geq p^{-2s+1}$, we have $\lim_{j_m\to\infty} a_{j_m} = a \neq 0$. Thus it follows from (2) that

$$\lim_{j_m\to\infty} x'_{j_m} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = u \in \overline{H}.$$

Conjugating $u$ by a suitable power of $h$, we can suppose that $a \notin \mathbb{Z}_p$. Since $u^n = \begin{pmatrix} 1 & 0 \\ an & 1 \end{pmatrix}$ for arbitrary $n \in \mathbb{Z}$ and the closure of $a\mathbb{Z}$ in $\mathbb{Q}_p$ contains $\mathbb{Z}_p$, the group $\overline{H}$

contains $U_1' = \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \Big| x \in \mathbb{Z}_p \right\}$. Furthermore, let $u_1 = \begin{pmatrix} 1 & 0 \\ p^{-r}\beta & 1 \end{pmatrix} \in U_1$ be an element such that $r > 0$ and $\beta \in \mathbb{Z}_p^*$. Choose an integer $m$ such that $2sm - r \geq 0$. Then $h^m u_1 h^{-m} \in U_1'$, whence $u_1 \in \overline{H}$. Thus, we obtain $U_1 \subset \overline{H}$. Similarly, one can prove that $U_2 \subset \overline{H}$. it follows that $\overline{H} = \mathrm{SL}_2(\mathbb{Q}_p)$. Lemma 1 is proved.

Lemma 2 *Let $X$ and $Y$ be irreducible $\mathbb{Q}$-defined affine varieties,* $\dim Y \geq 1$, *and let $f : X \to Y$ be a dominant $\mathbb{Q}$-defined regular morphism. Then there exists a prime $p \neq 2$ and $x \in X(\mathbb{Q}_p)$ such that not all coordinates of the image $f(x) \in Y(\mathbb{Q}_p)$ belong to $\mathbb{Z}_p$.*

*Proof.* Let $K$ be an algebraic closure of $\mathbb{Q}$, $D$ be an arbitrary irreducible curve in $Y(K)$, and let $L$ be an arbitrary irreducible curve such that $L \subset f^{-1}(D)$ and $f(L)$ is dense in $D$. Let $\overline{D}$ and $\overline{L}$ be the projective closures of $D$ and $L$, respectively, and let $\widetilde{L}$ be the smooth projective model of $\overline{L}$. The regular morphism $f : L \to D$ determines a rational morphism $\widetilde{f} : \widetilde{L} \to \overline{D}$. Since any rational morphism from a smooth curve to a projective variety is regular and the image of a projective variety under regular map is closed (see [21]), $\widetilde{f}$ is a regular surjective morphism.

Let $v \in \overline{D} \backslash D$ be a point at infinity on $\overline{D}$ and $w \in \widetilde{f}^{-1}(v)$. The coordinates of both points $v$ and $w$ generate the finite extension $K_1/\mathbb{Q}$. By Chebotarev's density theorem, there exist infinitely many prime numbers $p$ such that $K_1 \subset \mathbb{Q}_p$. Choose one of them. Then $w \in \widetilde{L}(\mathbb{Q}_p)$, $v \in \overline{D}(\mathbb{Q}_p)$. Since $w$ is a non-singular point on $\widetilde{L}$, $w$ has a $p$-adic neighborhood $W \subset \widetilde{L}(\mathbb{Q}_p)$ such that $W$ is homeomorphic to an area in $\mathbb{Q}_p$ (see [21, chapter II]). This means that there exists an infinite sequence of elements $w_i \in W$ such that $w_i \in L(\mathbb{Q}_p)$ and $\lim_{i \to \infty} w_i = w$ in the $p$-adic topology. Then by continuity of $\widetilde{f}$, we have $\lim_{i \to \infty} \widetilde{f}(w_i) = v$. Since $v \in \overline{D}(\mathbb{Q}_p)$ is a point at infinity, the sequence of elements $f(w_i) = \widetilde{f}(w_i) \in D(\mathbb{Q}_p)$ is not bounded. Therefore, there exists $i$ such that not all of the coordinates of the point $f(w_i)$ belong to $\mathbb{Z}_p$. Lemma 2 is proved.

**Proof of Theorem 1.** Let $g_1 \ldots, g_s \in \Gamma$ be elements such that the functions $\tau_{g_1}, \ldots, \tau_{g_s}$ generate the ring $T(\Gamma)$. Then the projection $\pi : R(\Gamma) \to X(\Gamma)$ is defined by the formula $\pi(\rho) = (\tau_{g_1}(\rho), \ldots, \tau_{g_s}(\rho))$. Since, by the assumptions of Theorem 1, we have $\dim X^s(\Gamma) \geq 2$, there exists an irreducible component $Z$ of the variety $X(\Gamma)$ such that $\dim Z \geq 2$ and $U = Z \cap X^s(\Gamma) \neq \varnothing$.

Let $p_i : Z \to \mathbb{A}^1$ be the projection defined by the formula $p_i(z_1, \ldots, z_s) = z_i$. Since $\dim Z \geq 2$, at least for one $i$ the projection $p_i$ is dominant. Therefore, there exists an integer $n > 2$ such that $n \in p_i(U)$. Let $Y = p_i^{-1}(n) \subset Z$. Then, by the Dimension Theorem, $\dim Y \geq \dim Z - 1 \geq 1$ and $Y \cap U \neq \varnothing$. Furthermore, let $X$ be an irreducible component of $\pi^{-1}(Y)$ such that $\pi(X))$ is dense in $Y$. Applying Lemma 2 to the varieties $X$, $Y$, and the morphism $\pi$, we obtain that for some prime $p$ the set $X(\mathbb{Q}_p)$ contains a representation $\rho$ with the following property: $\rho$ is irreducible and not all coordinates of the point $\pi(\rho)$ belong to $\mathbb{Z}_p$. The latter means that there exists $j$ such that $\tau_{g_j}(\rho) = \mathrm{tr}\,\rho(g_j) \notin \mathbb{Z}_p$, implying $\rho(\Gamma)$ is an unbounded subgroup of $\mathrm{SL}_2(\mathbb{Q}_p)$.

It also follows from the construction of the representation $\rho$ that $\tau_{g_i}(\rho) = \operatorname{tr}\rho(g_i) = n > 2$. Therefore, the cyclic subgroup of $\rho(\Gamma)$ generated by $\rho(h_i)$ is infinite and bounded, whence $\rho(\Gamma)$ is a non-discrete subgroup of $\mathrm{SL}_2(\mathbb{Q}_p)$. By Lemma 1, $\rho(\Gamma)$ is dense in $\mathrm{SL}_2(\mathbb{Q}_p)$ in the $p$-adic topology. As we have noted above, this fact implies that $\rho(\Gamma)$ (and therefore $\Gamma$) is a non-trivial free product with amalgamation. Theorem 1 is proved.

# 2. Some auxiliary results

In this section we prove some auxiliary results used in the proofs of Theorems 2 and 3. In what follows we denote the ring of algebraic integers in $\mathbb{C}$ by $\mathcal{O}$, the group of units in $\mathcal{O}$ by $\mathcal{O}^*$, the free group of rank 2 with generators $g$ and $h$ by $F_2 =< g, h >$, and the greatest common divisor of integers $a$ and $b$ by $(a, b)$. If $K \supset L$ is a finite extension of fields and $x \in K$, then we denote the norm of the element $x$ by $N_{K/L}(x)$. The following lemma characterizes elements of a finite order in $\mathrm{SL}_2(\mathbb{C})$.

Lemma 3 *Let $2 < m \in \mathbb{Z}$ and $\pm E \neq X \in \mathrm{SL}_2(\mathbb{C})$. Then $X^m = E$ if and only if* $\operatorname{tr} X = \varepsilon + \varepsilon^{-1}$, *where $\varepsilon^m = 1$, $\varepsilon \neq \pm 1$ (in other words,* $\operatorname{tr} X = 2\cos(2r\pi/m)$ *for some $r \in \{1, \dots, m-1\}$). In particular, if* $\operatorname{tr} X = 0$, *then $X^2 = -E$.*

*Proof.* If $X^m = E$, then the assertion is obvious. Conversely, let $\operatorname{tr} X = \varepsilon + \varepsilon^{-1}$. Then $\varepsilon, \varepsilon^{-1}$ are the eigenvalues of the matrix $X$. It follows that $X$ is conjugate to the matrix $\operatorname{diag}(\varepsilon, \varepsilon^{-1})$, whence $X^m = E$, as required.

Obviously, the representation variety $R(F_2)$ of the free group $F_2 = \langle g, h\rangle$ coincides with $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$. It is known that the ring $T(F_2)$ is generated by the functions $\tau_g, \tau_h, \tau_{gh}$ (see [12, 16, 17]). Recall that for an element $u \in F_2$ the function $\tau_u$ called the Fricke character of the element $u$.

Lemma 4 *For all $\alpha, \beta, \gamma \in \mathbb{C}$ there exist matrices $A, B \in \mathrm{SL}_2(\mathbb{C})$ such that $\tau_g(A, B) =$* $\operatorname{tr} A = \alpha, \quad \tau_h(A, B) = trB = \beta, \quad \tau_{gh}(A, B) = \operatorname{tr} AB = \gamma.$

This lemma can be easily proved by straightforward computations.

Lemma 4 implies that $X(F_2) = \pi(R(F_2)) = \mathbb{A}^3$ and that the functions $\tau_g, \tau_h, \tau_{gh}$ are algebraically independent over $\mathbb{C}$. So for all $u \in F_2$ we have

$$\tau_u = Q_u(\tau_g, \tau_h, \tau_{gh}),$$

where $Q_u \in \mathbb{Z}[x, y, z]$ is a uniquely determined polynomial with integer coefficients. The polynomial $Q_u$ is usually called the Fricke polynomial of the element $u$. The following relations for Fricke characters follows immediately from the relations between traces of arbitrary matrices in $\mathrm{SL}_2(\mathbb{C})$:

$$1)\tau_{u^{-1}} = \tau_u; \quad 2)\tau_{uv} = \tau_{vu}; \quad 3)\tau_{vuv^{-1}} = \tau_u; \quad 4)\tau_{uv} = \tau_u\tau_v - \tau_{uv^{-1}}. \tag{3}$$

Furthermore, we need a more detailed information on the Fricke polynomials (see [22]). Consider polynomials $P_n(\lambda)$ satisfying the initial conditions $P_{-1}(\lambda) = 0$ and $P_0(\lambda) = 1$ and the recurrence relation

$$P_n(\lambda) = \lambda P_{n-1}(\lambda) - P_{n-2}(\lambda).$$

If $n < 0$, we set $P_n(\lambda) = -P_{|n|-2}(\lambda)$. The degree of the polynomial $P_n(\lambda)$ is equal to $n$ if $n > 0$ and to $|n| - 2$ if $1n < 0$. It is easy to verify, by induction on $n$, that

$$P_n(2\cos(\varphi)) = \frac{\sin((n+1)\varphi)}{\sin(\varphi)}. \tag{4}$$

It follows from (4) that

$$\lambda_{n,k} = 2\cos(\tfrac{k\pi}{n+1}), \qquad k = 1, 2, \ldots, n. \tag{5}$$

are $n$ zeros of the polynomial $P_n(\lambda)$, $n \geq 1$. It is easy also to verify, by induction, that for $n \geq 0$ we have

$$\begin{aligned} P_{2n}(\lambda) &= \lambda^{2n} + \cdots + (-1)^n \\ P_{2n-1}(\lambda) &= \lambda(\lambda^{2n-2} + \cdots + (-1)^{n-1}n). \end{aligned} \tag{6}$$

Let now $w = g^{\alpha_1}h^{\beta_1}\ldots g^{\alpha_s}h^{\beta_s}$ be a cyclically reduced word in $F_2$ and let $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$. Let us treat the Fricke polynomial $Q_w(x, y, z)$ as a polynomial in $z$. We may write

$$Q_w(x, y, z) = M_n(x, y)z^n + M_{n-1}(x, y)z^{n-1} + \ldots + M_0(x, y).$$

Lemma 5 ([22]) *The degree of the Fricke polynomial $Q_w(x, y, z)$ with respect to $z$ is equal to $s$, that is, the number of blocks of the form $g^{\alpha_i}h^{\beta_i}$ in $w$. The leading coefficient $M_s(x, y)$ of the polynomial $Q_w(x, y, z)$ has the following form*

$$M_s(x, y) = \prod_{i=1}^{s} P_{\alpha_i - 1}(x))P_{\beta_i - 1}(y). \tag{7}$$

The following lemma plays an important role in the proofs of Theorems 2 and 3. Let $\Gamma = \langle a, b \mid a^n = R^m(a, b) = 1\rangle$, where $n = 0$ or $n \geq 2$, $m \geq 2$, $R(a, b)$ is a cyclically reduced word containing $b$ in the free group on $a$ and $b$. Assume that there exists matrices $A, B \in \mathrm{SL}_2(\mathbb{C})$ such that $\operatorname{tr} A = \alpha = 2\cos(t\pi/n)$ for some $t \in \{1, \ldots, n-1\}$ and $\operatorname{tr} R(A, B) = Q_R(\alpha, y, z) = c$, where $Q_R$ is the Fricke polynomial of the element $R(g, h) \in F_2$, $c = 2\cos(r\pi/m)$ for some $r \in \{1, \ldots, m-1\}$, $y = \operatorname{tr} B$, $z = \operatorname{tr} AB$.

LEMMA 6 (a) *Let* $H =< A, B >$ *be the group generated by matrices* $A$ *and* $B$. *Assume that the following two conditions hold:*

1) *there exists a unipotent element (or an element of a finite order)* $W \in H$ *of the form* $W = A^{\alpha_1}B^{\beta_1}\dots A^{\alpha_s}B^{\beta_s}$, *where* $\alpha_i, \beta_i \neq 0$ *for* $i = 1, \dots, s$, *such that* $l = \sum_{i=1}^{s} \beta_i \neq 0$.

2) *There exists an element* $h \in H$ *such that* $\operatorname{tr} h \notin \mathcal{O}$.

*Then the group* $\Gamma$ *is a non-trivial free product with amalgamation.*

(b) *Suppose that instead of the condition 1) the following condition holds:*

1′) $B$ *has a finite order, that is,* $\operatorname{tr} B = 2\cos(k_1\pi/k)$ *for some* $k \geq 2$, $(k_1, k) = 1$.

*Then for any integer* $v$ *the group* $\Gamma_1 = \langle a, b \mid a^n = b^{kv} = R^m(a, b) = 1\rangle$ *is a non-trivial free product with amalgamation.*

The proof of this lemma is based on the Bass classification of finitely generated subgroups in $\mathrm{SL}_2(\mathbb{C})$ [23].

PROPOSITION 1 ([23]) *Let* $H \subset \mathrm{GL}_2(\mathbb{C})$ *be a finitely generated subgroup. Then one of the following cases occur:*

1) *there exists an epimorphism* $f : H \to \mathbb{Z}$ *such that* $f(u) = 0$ *for all unipotent elements* $u \in H$*;*

2) $\operatorname{tr} h \in \mathcal{O}$ *for every element* $h \in H$*;*

3) $H$ *is a non-trivial free product with amalgamation.*

*Proof of Lemma 6.* First we show that the group $H$ does not satisfy the condition 1) of Proposition 1. Indeed, assume that $f : H \to \mathbb{Z}$ is an epimorphism such that $f(z) = 0$ for all unipotent elements $z \in H$. Then $f(A) = 0$ because $A^{2n} = E$, by Lemma 3. Furthermore, $f(u) = lf(B) = 0$, whence $f(B) = 0$ because, by the assumptions, $u$ is either unipotent or has a finite order and $l \neq 0$. Therefore, $f(H) = \{0\}$ – a contradiction.

Thus, by Proposition 1, $H$ is a non-trivial free product with amalgamation, that is, $H = H_1 *_F H_2$, where $H_1 \neq F \neq H_2$. Let $\overline{A}$, $\overline{B}$, $\overline{H}$, $\overline{H}_1$, $\overline{H}_2$, $\overline{F}$ be the images of $A$, $B$, $H$, $H_1$, $H_2$, $F$ in $\mathrm{PSL}_2(\mathbb{C})$, respectively. If $-E \notin H$, then the groups $H$ and $\overline{H}$ are isomorphic. If $-E \in H$, then $-E$ belongs to the centre of $H$, hence $-E \in F$. In all these cases $\overline{H}_1 \neq \overline{F} \neq \overline{H}_2$ and therefore $\overline{H} = \overline{H}_1 *_{\overline{F}} \overline{H}_2$ is a non-trivial free product with amalgamation.

By Lemma 3, the conditions $\operatorname{tr} A = \alpha$ and $Q_R(\alpha, y, z) = c$ imply that $A^{2n} = R^{2m}(A, B) = E$. Hence $\overline{A}^n = R^m(\overline{A}, \overline{B}) = 1$ in $\mathrm{PSL}_2(\mathbb{C})$. It follows that $\overline{H}$ is an epimorphic image of $\Gamma$ and therefore $\Gamma$ is a non-trivial free product with amalgamation as well.

Furthermore, if we replace the condition 1) by 1′), then again the group $\overline{H}$ is a non-trivial free product with amalgamation. Moreover, we have $\overline{A}^n = \overline{B}^k = R^m(\overline{A}, \overline{B}) = 1$

in $\mathrm{PSL}_2(\mathbb{C})$. It follows that $\overline{H}$ is an epimorphic image of $\Gamma_1$, whence $\Gamma_1$ is a non-trivial free product with amalgamation. Lemma 6 is proved.

Lemma 7 1) *Let $r, s \in \mathbb{Z}$, where $s \geq 3$ and $(r, s) = 1$. Then $\cos(r\pi/s) \notin \mathcal{O}$.*

2) *Let $s \in \mathbb{Z}$, $s \geq 1$, and $r \not\equiv 0 \pmod{2s+1}$. Then $2\cos(r\pi/(2s+1)) \in \mathcal{O}^*$.*

3) *Let $0 \neq u \in \mathbb{Z}$, $p$ be a prime, and let $\varepsilon$ be a primitive root of unity of degree $4pu$. Set*

$$x_r = 2\cos(\tfrac{r\pi}{2pu}), \quad y_r = 2\sin(\tfrac{r\pi}{2pu}), \quad K = \mathbb{Q}(\varepsilon).$$

*Then there exist $r, r_1 \not\equiv 0 \pmod{p}$ such that $p$ divides both of the integers $N_{K/\mathbb{Q}}(x_r)$ and $N_{K/\mathbb{Q}}(y_{r_1})$. In particular, $x_r, y_{r_1} \notin \mathcal{O}^*$.*

4) *Let $u, c \in \mathbb{Z}$, $|u| \geq 2$, $c \neq 0$, and let $p$ be a prime not dividing $c$. Set $x_0 = -2\cos(\pi/u)$, $x_r = 2\cos(r\pi/(pu))$. Then there exists $r \not\equiv 0 \pmod{p}$ such that $c/(x_r - x_0) \notin \mathcal{O}$.*

5) *Let $p > 2$ be a prime. Then for each $r \not\equiv 0 \pmod{p}$ and $s \geq 1$ we have $\sin(r\pi/p^s) \notin \mathcal{O}^*$.*

6) *Let $t \geq 1$. Then for each odd $r$ we have $2sin(r\pi/2^t) \notin \mathcal{O}^*$.*

*Proof.* 1) Assume that $\cos(r\pi/s) \in \mathcal{O}$. Then for every $d \in \mathbb{Z}$ we have $\cos(dr\pi/s) \in \mathcal{O}$. Since, by the assumptions, $(r, s) = 1$, for every integer $l$ there exists $d$ such that $dr \equiv l \pmod{s}$. Therefore, for all integers $l$ we have $\cos(l\pi/s) \in \mathcal{O}$. By (5), the polynomial $P_{s-1}(\lambda)$ has the roots $2\cos(l\pi/s)$, $l = 1, \ldots, s-1$. Therefore, the polynomial $P_{s-1}(2\lambda)$ has the roots $\cos(l\pi/s)$, $l = 1, \ldots, s-1$.

If $s = 2s_1 + 1$ is odd, then, by (6), we have $P_{2s_1}(2\lambda) = 2^{2s_1}\lambda^{2s_1} + \cdots + (-1)^{s_1}$. Since $1/2^{2s_1} \notin \mathbb{Z}$, the polynomial $P_{2s_1}(2\lambda)$ has a root not belonging to $\mathcal{O}$, that is, there exists $l$ such that $\cos(l\pi/s) \notin \mathcal{O}$ – a contradiction. If $s = 2s_1$ is even, then it follows from (6) that $P_{2s_1-1}(2\lambda) = 2\lambda(2^{2s_1-2}\lambda^{2s_1-2} + \cdots + (-1)^{s_1-1}s_1)$. By the assumptions, $s \geq 3$, hence $s_1 \geq 2$. Then $s_1/2^{2s_1-2} \notin \mathbb{Z}$ and $P_{2s_1-1}(2\lambda)$ has a root not belonging to $\mathcal{O}$. We obtain again a contradiction proving item 1).

2) By (5) and (6), the number $2\cos(r\pi/(2s+1))$ is a root of the polynomial $P_{2s}(\lambda) = \lambda^{2s} + \cdots + (-1)^s$ and therefore it belongs to $\mathcal{O}^*$.

3) Since $y_r = 2\cos((pu - r)\pi/(2pu)) = x_{pu-r}$, it suffices to prove the assertion for $x_r$. Let $u = p^f u'$, where $f \geq 0$ and $p \nmid u'$. Set $r = r_1 u'$, where $p \nmid r_1$. Then $x_r = 2\cos(r_1\pi/(2p^{f+1}))$. By (5) and (6), the polynomial

$$P_{2p^{f+1}-1}(\lambda) = \lambda(\lambda^{2p^{f+1}-2} + \cdots + (-1)^{p^{f+1}-1}p^{f+1})$$

has the roots $2\cos(r'\pi/(2p^{f+1}))$, $r' = 1, \ldots, 2p^{f+1} - 1$, and the polynomial

$$P_{2p^f-1}(\lambda) = \lambda(\lambda^{2p^f-2} + \cdots + (-1)^{p^f-1}p^f)$$

has the roots $2\cos(r'\pi/(2p^f))$, $r' = 1, \ldots, 2p^f - 1$. Therefore, the polynomial $P_{2p^f-1}(\lambda)$ divides the polynomial $P_{2p^{f+1}-1}(\lambda)$. Let

$$P_{2p^{f+1}-1}(\lambda) = P_{2p^f-1}(\lambda)F(\lambda), \tag{8}$$

where $F(\lambda)$, as it is easy to see, is a polynomial of degree $2(p^{f+1} - p^f)$ with the leading coefficient 1 and the constant term $p$. The roots of $F(\lambda)$ are the numbers $2\cos(r'\pi/(2p^{f+1}))$, $r' \not\equiv 0 \,(\mathrm{mod}\, p)$. It is easy to see that there exists $r_1 \not\equiv 0 \,(\mathrm{mod}\, p)$ such that $N_{K/\mathbb{Q}}(2\cos(r_1\pi/(2p^{f+1}))) = \pm p^s$ for some $s \geq 1$, as required.

4) We note that

$$x_r - x_0 = 2\cos(\tfrac{r\pi}{pu}) + 2\cos(\tfrac{\pi}{u}) = \left(2\cos(\tfrac{(r+p)\pi}{2pu})\right)\left(2\cos(\tfrac{(r-p)\pi}{2pu})\right).$$

So it suffices to show that for some $r \not\equiv 0 \,(\mathrm{mod}\, p)$ we have $c/\alpha_r \notin \mathcal{O}$, where $\alpha_r = 2\cos((r+p)\pi/(2pu))$. Let $K_r = \mathbb{Q}(\alpha_r)$ and $[K_r : \mathbb{Q}] = d$. By item 3), there exists $r \not\equiv 0$ $(\mathrm{mod}\, p)$ such that $p$ divides $N_{K_r/\mathbb{Q}}(\alpha_r)$. Then

$$N_{K_r/\mathbb{Q}}\left(\frac{c}{\alpha_r}\right) = \frac{c^d}{N_{K_r/\mathbb{Q}}(\alpha_r)} \notin \mathbb{Z},$$

because, by the assumptions, $p \nmid c$. Hence $c/\alpha_r \notin \mathcal{O}$, as required.

5) Note that $1/\sin(r\pi/p^s) = 2/(2\cos((p^s - 2r)\pi/(2p^s)))$. It follows from the proof of item 4) that there exists $r_0 \not\equiv 0 \,(\mathrm{mod}\, p)$ such that

$$\frac{2}{2\cos((p^s - 2r_0)\pi/(2p^s))} \notin \mathcal{O}.$$

Now we show that for every $r \not\equiv 0 \,(\mathrm{mod}\, p)$ we have $\sin(r\pi/p^s) \notin \mathcal{O}$. Assume the contrary. Let $1/\sin(r\pi/p^s) \in \mathcal{O}$ for some $r$ with $(r,p) = 1$. Since $p \nmid (p^s - 2r_0)$, there exists $d$ such that $r \equiv d(p^s - 2r_0) \,(\mathrm{mod}\, p^s)$. Then, by (4), we have

$$P_d\left(2\cos(\tfrac{(p^s-2r_0)\pi}{p^s})\right) = \frac{\sin(d(p^s - 2r_0)\pi/p^s)}{\sin((p^s - 2r_0)\pi/p^s)} = \pm\frac{\sin(r\pi/p^s)}{\sin((p^s - 2r_0)\pi/p^s)}.$$

This means that

$$\frac{1}{\sin((p^s - 2r_0)\pi/p^s)} = \pm\frac{1}{\sin(r\pi/p^s)}P_d\left(2\cos(\tfrac{(p^s-2r_0)\pi}{p^s})\right) \in \mathcal{O}$$

which is impossible.

6) For $t = 1$ the assertion is obvious. Suppose that $t > 1$. By item 3), there exists odd $r_0$ such that $2\sin(r_0\pi/2^t) \notin \mathcal{O}^*$. We claim that for every odd $r$ we have $2\sin(r\pi/2^t) \notin \mathcal{O}^*$. Assume the contrary, i.e. for some odd $r$ we have $2\sin(r\pi/2^t) \in \mathcal{O}^*$. Obviously, there exists an integer $d$ such that $r \equiv dr_0 \,(\mathrm{mod}\, 2^t)$. Then, by (4), we have

$$P_d\left(2\cos(\tfrac{r_0\pi}{2^t})\right) = \pm\frac{2\sin(r\pi/2^t)}{2\sin(r_0\pi/2^t)},$$

whence $2\sin(r_0\pi/2^t) \in \mathcal{O}^*$ – a contradiction. Lemma 7 is proved.

LEMMA 8 1) *Let $s,t \geq 0$. Then*

$$P_s(\lambda)P_t(\lambda) = \sum_{i=0}^{t} P_{s-t+2i}(\lambda). \tag{9}$$

2) *The polynomial $P_s(\lambda) - P_{s-1}(\lambda)$ has the roots $\lambda_r = 2\cos((2r+1)\pi/(2s+1))$, $r \in \{0,1,\ldots,s-1\}$.*

3) *If $\gamma = 2\cos(2r\pi/(2s+1))$, where $s \geq 1$, $r \in \{1\ldots,s\}$, and $(r,2s+1)=1$, then $P_s(\gamma) - P_{s-1}(\gamma) \notin \mathcal{O}^*$.*

4) *If $\gamma = 2\cos((2r+1)\pi/(2s))$, where $s \geq 2$ and $(s,2r+1)=1$, then $0 \neq P_{s-1}(\gamma) \notin \mathcal{O}^*$.*

*5) Let $\gamma \in \mathcal{O}$. Assume that $\gamma$ is not equal to $2\cos(r\pi/s)$, where $r,s \in \mathbb{Z}$. Then there exists an integer $l > 0$ such that $P_l(\gamma) \notin \mathcal{O}^*$.*

*Proof.* 1) We fix $s$ and proceed by induction on $t$. If $t=0$, then $P_s(\lambda)P_0(\lambda) = P_s(\lambda)$. If $t=1$, then, by definition, $P_s(\lambda)P_1(\lambda) = P_s(\lambda)\lambda = P_{s+1}(\lambda) + P_{s-1}(\lambda)$. Furthermore, we have by induction

$$\begin{aligned} P_s(\lambda)P_t(\lambda) &= P_s(\lambda)(\lambda P_{t-1}(\lambda) - P_{t-2}(\lambda)) = \lambda \sum_{i=0}^{t-1} P_{s-t+1+2i}(\lambda) - \sum_{i=0}^{t-2} P_{s-t+2+2i}(\lambda) \\ &= \sum_{i=0}^{t-1}(P_{s-t+2+2i}(\lambda) + P_{s-t+2i}(\lambda)) - \sum_{i=0}^{t-2} P_{s-t+2+2i}(\lambda) \\ &= P_{s+t}(\lambda) + \sum_{i=0}^{t-1} P_{s-t+2i}(\lambda) = \sum_{i=0}^{t} P_{s-t+2i}(\lambda) \end{aligned}$$

as required.

2) Bearing in mind (4), we obtain

$$P_s(\lambda_r) - P_{s-1}(\lambda_r) = \frac{\sin((2r+1)(s+1)\pi/(2s+1)) - \sin((2r+1)s\pi/(2s+1))}{\sin((2r+1)\pi/(2s+1))} = 0.$$

3) Taking into account (4), we have

$$\frac{1}{P_{s+1}(\gamma) - P_s(\gamma)} = \frac{\sin(2r\pi/(2s+1))}{2\sin(r\pi/(2s+1))\cos(r\pi)} = \pm\cos(\tfrac{r\pi}{2s+1}) \notin \mathcal{O},$$

by item 1) of Lemma 7.

4) Using (4), we obtain

$$\frac{1}{P_{s-1}(\gamma)} = \frac{\sin((2r+1)\pi/(2s))}{\sin((2r+1)\pi/2)} = (-1)^r \cos\left(\tfrac{(s-2r-1)\pi}{2s}\right) \notin \mathcal{O},$$

by item 1) of Lemma 7.

5) Since, by (5), the polynomial $P_l(\lambda)$ has the roots $2\cos(r\pi/(l+1))$, $r = 1, \dots, l$, we can write $P_l(\gamma) = \prod_{r=1}^{l}(\gamma - 2\cos(r\pi/(l+1)))$. Hence it suffices to prove that $\gamma - (\varepsilon + \varepsilon^{-1}) \notin \mathcal{O}^*$, where $\varepsilon \neq \pm 1$ is a root of 1.

Let $f(\lambda) \in \mathbb{Q}[\lambda]$ be an irreducible polynomial such that $f(\gamma) = 0$. We denote by $K_0$ the splitting field of $f(\lambda)$ and put $K_1 = K_0(x_0)$, where $x_0$ is a root of the equation $x + x^{-1} = \gamma$. Let $Z_1$ be the integer closure of $\mathbb{Z}$ in $K_1$ and let $p \neq 2$ be a prime. Take a prime ideal $\mathfrak{p}_1$ in $Z_1$ lying above $(p)$. Then $k_1 = Z_1/\mathfrak{p}_1 \supset \mathbb{Z}/p\mathbb{Z} = k$ is a finite extension of fields. Clearly, we have $x_0, y_0 \in Z_1$. Denote by $\overline{x}_0$ and $\overline{\gamma}$ the images of $x_0$ and $\gamma$, respectively, in the field $k_1$. Then the following equality holds

$$\overline{x}_0 + \overline{x}_0^{-1} = \overline{\gamma}.$$

If $l = |k_1^*|$ is the order of the multiplicative group of $k_1$, then $\overline{x}_0^l = 1$ in $k_1$. Consider the field $K_2 = K_1(\xi)$, where $\xi$ is a primitive root of 1 of degree $l$ in $\mathbb{C}$. Let $Z_2$ be the integer closure of $Z_1$ in $K_2$ and $\mathfrak{p}_2$ be a prime ideal of $Z_2$ lying above $\mathfrak{p}_1$. We set $k_2 = Z_2/\mathfrak{p}_2 \supset k_1$. Let $\Delta$ be the group of roots of 1 of degree $l$ in $K_2$ and $\overline{\Delta}$ be its image in $k_2$.

We show that $\overline{\Delta} = k_1^*$. Assume the contrary, i.e. $\overline{\Delta} \neq k_1^*$. Then for some integer $r$, $0 < r < l$, we have $\overline{\xi}^r = 1$, where $\overline{\xi}$ is the image of $\xi$ in $k_2$. Then $(1+y)^l = 1$, that is, $1 + C_l^1 y + \dots + C_l^l y^l = 1$, where $C_l^i$ is the corresponding binomial coefficient. Hence $y(l + yy_1) = 0$, where $y_1 = C_l^2 y + \dots + C_l^l y^{l-1}$. Since $y \neq 0$, we obtain $l \in \mathfrak{p}_2 \cap \mathbb{Z} = (p)$. But $l = |k_1^*| = p^t - 1$ for some $t$ – a contradiction. Thus, there exists a root $\varepsilon$ of 1 of degree $l$ such that $\overline{\varepsilon} = \overline{x}_0$. This means that $\gamma - (\varepsilon + \varepsilon^{-1}) \in \mathfrak{p}_2$ and hence $\gamma - (\varepsilon + \varepsilon^{-1})$ is not a unit in the ring $\mathcal{O}$. Lemma 8 is proved.

Lemma 9 *Let $F_2 = \langle g, h \rangle$ be the free group with generators $g$ and $h$. Set $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$, and $t = \tau_{ghg^{-1}h^{-1}}$. Then the following assertions hold.*

1) $t = x^2 + y^2 + z^2 - xyz - 2$.

2) *Let $R = gh(ghg^{-1}h^{-1})^s$. Then*

$$\tau_R = (P_s(t) - P_{s-1}(t))z.$$

3) *Let $T = (gh)^{-1}(ghg^{-1}h^{-1})^s(gh)^2(ghg^{-1}h^{-1})^s$. Then*

$$\tau_T = (t-2)P_{s-1}(t)^2 z^3 + (2 - P_{2s-1}(t) + P_{2s-2}(t))z.$$

*Proof.* 1) This can be proved by straightforward computations using relations (3) (see [16]).

2) Let $u$ and $v$ be arbitrary elements in $F_2$. Then using induction and the relations (3), one easily shows that for arbitrary integers $p$ and $q$

$$\tau_{u^p v^q} = P_{p-1}(\tau_u)P_{q-1}(\tau_v)\tau_{uv} - P_{p-2}(\tau_u)P_q(\tau_v) - P_p(\tau_u)P_{q-2}(\tau_v). \qquad (10)$$

Now set $u = gh$ and $v = ghg^{-1}h^{-1}$. Then $\tau_u = z$, $\tau_v = t$, and $\tau_{uv} = \tau_{gh(ghg^{-1}h^{-1})} = zt - \tau_{g^{-1}h^{-1}} = z(t-1)$. Hence

$$\begin{aligned}\tau_{uv^s} &= P_{s-1}(\tau_v)\tau_{uv} - P_{s-2}(\tau_v)\tau_u = P_{s-1}(t)(t-1)z - P_{s-2}(t)z \\ &= z(tP_{s-1}(t) - P_{s-1}(t) - P_{s-2}(t)) = z(P_s(t) + P_{s-2}(t) - P_{s-1}(t) - P_{s-2}(t)) \\ &= z(P_s(t) - P_{s-1}(t)).\end{aligned}$$

3) Let $u$ and $v$ be such as above. Then using the relations (3) and (10), we have

$$\begin{aligned}\tau_{u^{-1}v^s} &= \tau_{u^{-1}}\tau_{v^s} - \tau_{uv^s} = z(P_s(t) - P_{s-2}(t)) - z(P_s(t) - P_{s-1}(t)) \\ &= z(P_{s-1}(t) - P_{s-2}(t)); \\ \tau_{u^2v^s} &= \tau_u\tau_{uv^s} - \tau_{v^s} = z^2(P_s(t) - P_{s-1}(t)) - P_s(t) + P_{s-2}(t); \\ \tau_{u^3} &= z^3 - 3z.\end{aligned}$$

Hence

$$\begin{aligned}\tau_{u^{-1}v^su^2v^s} &= \tau_{u^{-1}v^s}\tau_{u^2v^s} - \tau_{u^3} = z^3((P_s(t) - P_{s-1}(t))(P_{s-1}(t) - P_{s-2}(t)) - 1) \\ &\quad + z(3 - (P_{s-1}(t) - P_{s-2}(t))(P_s(t) - P_{s-2}(t))).\end{aligned}$$

Using (9), we simplify the last expression. First consider the coefficient at $z^3$.

$$\begin{aligned}&(P_s(t) - P_{s-1}(t))(P_{s-1}(t) - P_{s-2}(t)) - 1 = P_s(t)P_{s-1}(t) + P_{s-1}(t)P_{s-2}(t) \\ &- P_s(t)P_{s-2}(t) - P_{s-1}(t)^2 - 1 = P_{s-1}(t)(P_s(t) + P_{s-2}(t)) - \sum_{i=1}^{s-1} P_{2i}(t) - P_0(t) \\ &- P_{s-1}(t)^2 = tP_{s-1}(t)^2 - 2P_{s-1}(t)^2 = (t-2)P_{s-1}(t)^2.\end{aligned}$$

Now consider the coefficient at $z$.

$$\begin{aligned}&3 - (P_{s-1}(t) - P_{s-2}(t))(P_s(t) - P_{s-2}(t)) = 3 - P_s(t)P_{s-1}(t) + P_{s-1}(t)P_{s-2}(t) \\ &+ P_s(t)P_{s-2}(t) - P_{s-2}(t)^2 = 3 - \sum_{i=1}^{s} P_{2i-1}(t) + \sum_{i=1}^{s-1} P_{2i-1}(t) + \sum_{i=1}^{s-1} P_{2i}(t) - \sum_{i=0}^{s-2} P_{2i}(t) \\ &= 2 - P_{2s-1}(t) + P_{2s-2}(t).\end{aligned}$$

Lemma 9 is proved.

We close this section by deducing Corollary 1 from Theorem 1 and thus obtaining another proof of Conjecture 1. Let $\Gamma = \langle a, b \mid R^m(a,b) = 1\rangle$, where $m \geq 2$, $R(a,b) = a^{u_1}b^{v_1}\dots a^{u_s}b^{v_s}$, $u_i, v_i \neq 0$, $s \geq 1$, and $R(a,b)$ is not a proper power.

First consider the case $m \geq 3$. We need to prove that $\dim X^s(\Gamma) \geq 2$. In the character variety $X(F_2) = \mathbb{A}^3$ of the free group $F_2 = \langle g, h\rangle$ consider the hypersurface $V$ given by the equation

$$\tau_{R(g,h)}(x,y,z) = 2\cos(\tfrac{2\pi}{m}), \tag{11}$$

where $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$. By Lemma 5, we can rewrite (11) in the form

$$f(x,y,z) = M_s(x,y)z^s + \cdots + M_0(x,y) - 2\cos(\tfrac{2\pi}{m}) = 0. \tag{12}$$

We claim that $V \subset X(\Gamma)$. Indeed, let $v = (x_0, y_0, z_0) \in V$ and let $A, B \in \mathrm{SL}_2(\mathbb{C})$ be matrices such that $\operatorname{tr} A = x_0$, $\operatorname{tr} B = y_0$, $\operatorname{tr} AB = z_0$. Then, by Lemma 3, we have $R^m(A,B) = E$. Hence the pair of matrices $(A,B)$ determines a representation $\rho$ of the group $\Gamma$ into $\mathrm{SL}_2(\mathbb{C})$. The image of $\rho$ in $X(\Gamma)$ coincides with $v$. Hence, $v \in X(\Gamma)$.

Furthermore, let $V_1, \ldots, V_r$ be the irreducible components of $V$. Obviously (see [21]), $\dim V_i = 2$ for each $i$. It remains to show that $V \cap X^s(\Gamma) \neq \varnothing$. Let us assume the contrary. Then all representations corresponding to points of $V$ are reducible. This means that the regular function $\tau_{ghg^{-1}h^{-1}} - 2$ is identically equal to 0 on $V$. Hence, by item 1 of Lemma 9, we have

$$g(x,y,z) = x^2 + y^2 + z^2 - xyz - 4 \equiv 0$$

on $V$ and so

$$f(x,y,z) = g(x,y,z)^d \tag{13}$$

for some $d \geq 1$.

If $|u_i| \geq 2$ or $|v_i| \geq 2$ for some $i$, then by Lemma 5, the leading coefficient $M_s(x,y)$ in (12) is not a constant and the equality (13) is impossible. So $|u_i| = |v_i| = 1$ for $i = 1, \ldots, s$. If for some $i$ we have $u_i = u_{i+1}$ or $v_i = v_{i+1}$ ($u_1 = u_s$ or $v_1 = v_s$ for $i = s$), then we can consider new generators of the group $\Gamma$. Namely, assume, for example, that $u_1 = u_2$. We set $a_1 = a^{u_1}b^{v_1}$, $b_1 = b$. Then $\Gamma = \langle a_1, b_1 \mid R_1^m(a_1,b_1) = 1\rangle$, where $R_1^m(a_1,b_1) = a_1^{u_1'}b_1^{v_1'} \ldots a_1^{u_r'}b_1^{v_r'}$, $u_i', v_i' \neq 0$, $r \geq 1$, and $u_1' \geq 2$. This case was considered above.

Thus we can assume without loss of generality that $u_{i+1} = -u_i$, $v_{i+1} = -v_i$. Since, by the assumptions, $R(a,b)$ is not a proper power, we have for $R(a,b)$ only two possibilities up to cyclic rearrangement: $R(a,b) = aba^{-1}b^{-1}$ or $R(a,b) = ab^{-1}a^{-1}b$. In both cases we have

$$f(x,y,z) = x^2 + y^2 + z^2 - xyz - 2 - 2\cos(\tfrac{2\pi}{m}) = g(x,y,z) + 2 - 2\cos(\tfrac{2\pi}{m}).$$

Since $2 - 2\cos(\frac{2\pi}{m}) \neq 0$, obviously, $g(x,y,z)$ has no zeros on $V$ – a contradiction.

Let now $m = 2$. In this case one can consider a group $\Gamma_1 = \langle a, b \mid R^4(a,b) = 1\rangle$. We have proved above that $\dim X_2^s(\Gamma_1) \geq 2$. Then it follows from the proof of Theorem 1 that there exists a representation $\rho : \Gamma_1 \to \mathrm{SL}_2(\mathbb{Q}_p)$ for some prime $p$ such that $\rho(\Gamma_1)$ is a non-trivial free product with amalgamation. Let $G$ be the image of $\rho(\Gamma_1)$ in $\mathrm{PSL}_2(\mathbb{Q}_p)$. Then $G$ is an epimorphic image of $\Gamma$. Obviously, $G$, and therefore $\Gamma$, is a non-trivial free product with amalgamation as well.

## 3. Proof of Theorem 2

1) Let $\Gamma_n = \langle a, b \mid a^n = b^k = R^2(a,b) = 1\rangle$ and let $F_2 = \langle g, h\rangle$ be the free group with generators $g$ and $h$. Set $x = \tau_g$, $\beta = \tau_h = 2\cos(\pi/k)$, and $z = \tau_{gh}$. Consider the equation

$$Q_{R(g,h)}(x, \beta, z) = 0, \tag{14}$$

where $Q_{R(g,h)}$ is the Fricke polynomial of the element $R(g,h) \in F_2$. By Lemma 5, we can rewrite (14) in the form

$$A_0(x)z^s + \cdots + A_s(x) = 0, \tag{15}$$

where $A_0(x) = \prod_{i=1}^{s} P_{u_i-1}(x)P_{v_i-1}(\beta)$. Since, by the assumptions, there exists $i$ such that $|u_i| \geq 2$, we have $\deg P_{u_i-1}(x) \geq 1$. Let $x_0 = -2\cos(\pi/u_i)$ be one of the roots of $P_{u_i-1}(x)$. Then $x - x_0$ divides $A_0(x)$. Let $A_0(x) = (x - x_0)B_0(x)$, where $B_0(x) \in \mathcal{O}[x]$. Write (15) in the form

$$(x - x_0)B_0(x)z^s + \cdots + A_s(x) = 0. \tag{16}$$

First we assume that all polynomials $A_1(x), \ldots, A_s(x)$ are divisible by $x - x_0$. Then (16) can be written in the form

$$(x - x_0)f(x, z) = 0, \tag{17}$$

where $f(x, z)$ is some polynomial in $x$ and $z$. Let $z_0$ be an arbitrary non-integer element of $\mathbb{C}$, that is, $z_0 \notin \mathcal{O}$, and let $A, B \in \mathrm{SL}_2(\mathbb{C})$ be matrices with $\operatorname{tr} A = x_0$, $\operatorname{tr} B = \beta$, and $\operatorname{tr} AB = z_0$. By construction, the pair of matrices $(A, B)$ determines a representation of the group $\Gamma_n$ into $\mathrm{PSL}_2(\mathbb{C})$. Applying Lemma 6, we obtain that $\Gamma_n$ is a non-trivial free product with amalgamation.

Assume now that not all polynomials $A_1(x), \ldots, A_s(x)$ are divisible by $x - x_0$. Let, for example, $A_1(x)$ is not divisible by $x - x_0$ and let $0 \neq \delta = A_1(x_0) \in \mathcal{O}$ be the residue of $A_1(x)$ modulo $x - x_0$. Set $c = N_{\mathbb{Q}(\delta)/\mathbb{Q}}(\delta) \in \mathbb{Z}$. Take a finite set of primes $S = \{p \in \mathbb{Z} \mid p \text{ divides } c\}$ from the assertion of the theorem. Assume that $n = u_i p f$ for some integer $f$ and prime $p \notin S$, where $u_i p \nmid u_j$ for $j \neq i$. Let $x_r = 2\cos(r\pi/(pu_i))$ for some $r \not\equiv 0 \pmod{p}$ and let $K_r = \mathbb{Q}(\delta, x_r - x_0)$. By item 3) of Lemma 7, one can choose $r$ such that $p$ divides $N_{K_r/\mathbb{Q}}(x_r - x_0) \in \mathbb{Z}$. Since, by construction, $p$ does not divide $c$, we have $N_{K_r/\mathbb{Q}}(\delta/(x_r - x_0)) \notin \mathbb{Z}$, hence $\delta/(x_r - x_0) \notin \mathcal{O}$. Thus we have

$$\frac{A_1(x_r)}{x_r - x_0} \notin \mathcal{O}.$$

Furthermore, since $p \nmid r$ and $pu_i \nmid u_j$ for each $j \neq i$, we have $B_0(x_r) \neq 0$. Now set $x = x_r$ and write the equation (16) in the form

$$z^s + \tfrac{A_1(x_r)}{(x_r - x_0)B_0(x_r)} z^{s-1} + \cdots + \tfrac{A_s(x_r)}{(x_r - x_0)B_0(x_r)} = 0. \tag{18}$$

Clearly, we have $A_1(x_r)/((x_r-x_0)B_0(x_r)) \notin \mathcal{O}$ because $B_0(x_r) \in \mathcal{O}$. Hence the equation (18) has a root $z_0 \notin \mathcal{O}$. Consider matrices $A, B \in \mathrm{SL}_2(\mathbb{C})$ such that

$$\operatorname{tr} A = x_r, \qquad \operatorname{tr} B = \beta, \qquad \operatorname{tr} AB = z_0.$$

By construction, the pair of matrices $(A, B)$ determines a representation of the group $\Gamma_n$ into $\mathrm{PSL}_2(\mathbb{C})$. Applying Lemma 6, we obtain that $\Gamma_n$ is a non-trivial free product with amalgamation.

2) We keep the notation of item 1). Consider the equation

$$Q_{R(g,h)}(x, \beta, z) = \gamma_t, \tag{19}$$

where $\gamma_t = 2\cos(t\pi/m)$ and $m \nmid t$. By Lemma 5, we can rewrite (19) in the form

$$(x - x_0)B_0(x)z^s + \cdots + A_s(x) - \gamma_t = 0. \tag{20}$$

Let $x_r = 2\cos(r\pi/(pu_i))$, where $r \not\equiv 0 \pmod{p}$. We claim that there exist $t$ and $r$ such that $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathcal{O}$. Indeed, let us assume the contrary.

First, consider the case $m = 3$. Then $\gamma_1 = 1$, $\gamma_2 = -1$. Since both of the numbers $(A_s(x_r)-1)/(x_r-x_0)$ and $(A_s(x_r)+1)/(x_r-x_0)$ belong to $\mathcal{O}$, their difference $2/(x_r-x_0) \in \mathcal{O}$ for each $r \not\equiv 0 \pmod{p}$. By the assumptions, $p \neq 2$, which contradicts item 4) of Lemma 7.

Now let $m = 2^l$. Then $\gamma_{2^{l-1}} = 0$, $\gamma_{2^{l-2}} = \sqrt{2}$. Since both of the numbers $A_s(x_r)/(x_r - x_0)$ and $(A_s(x_r) - \sqrt{2})/(x_r - x_0)$ belong to $\mathcal{O}$, we have $\sqrt{2}/(x_r - x_0) \in \mathcal{O}$ and therefore $2/(x_r - x_0) \in \mathcal{O}$. Again this contradicts item 4) of Lemma 7.

Thus, there exist $t$ and $r$ such that $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathcal{O}$. Since $p \nmid r$ and $pu_i \nmid u_j$ for each $j \neq i$, we have $B_0(x_r) \neq 0$. Set $x = x_r$ and write (20) in the form:

$$z^s + \cdots + \tfrac{A_s(x_r)-\gamma_t}{(x_r-x_0)B_0(x_r)} = 0. \tag{21}$$

By construction, $(A_s(x_r) - \gamma_t))/((x_r - x_0)B_0(x_r)) \notin \mathcal{O}$ whence (21) has a root $z_0 \notin \mathcal{O}$. Consider matrices $A, B \in \mathrm{SL}_2(\mathbb{C})$ such that

$$\operatorname{tr} A = x_r, \qquad \operatorname{tr} B = \beta, \qquad \operatorname{tr} AB = z_0.$$

By construction, these matrices determine a representation of $\Gamma_n$ into $\mathrm{PSL}_2(\mathbb{C})$. Applying Lemma 6, we obtain that the group $\Gamma_n$ is a non-trivial free product with amalgamation.

3) Let $m > 3$ and $m \neq 2^l$. We keep the notation of item 2). Show that there exist $t \not\equiv 0 \pmod{m}$ and $r \not\equiv 0 \pmod{p}$ such that $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathcal{O}$. Indeed, let us assume the contrary. Suppose that for each $t \not\equiv 0 \pmod{m}$ and each $r \not\equiv 0 \pmod{p}$ we have $(A_s(x_r) - \gamma_t)/(x_r - x_0) \in \mathcal{O}$.

First consider the case, where $m$ is odd and $m$ is divisible by an integer of the form $4g+1$, $g \geq 1$, that is, $m = (4g+1)m_1$. Consider the numbers $\delta_t = \gamma_{2tm_1} = 2\cos(2t\pi/(4g+1))$, $t = 1, ..., 2g$. Then $1 + \sum_{i=1}^{2g} \delta_i = 0$, as the sum of all roots of 1 of degree $4g+1$. Note that $-\delta_t = \gamma_{(4g+1-2t)m_1}$. Let $C_i = (A_s(x_r) - (-1)^i \delta_i)/(x_r - x_0)$. Then we have

$$\sum_{i=1}^{2g} (-1)^i C_i = -\sum_{i=1}^{2g} \frac{\delta_i}{x_r - x_0} = \frac{1}{x_r - x_0} \in \mathcal{O}$$

for each $r \not\equiv 0 \,(\mathrm{mod}\ p)$ which contradicts item 4) of Lemma 7.

Now suppose that $m$ is odd and $m$ does not have divisors of the form $4g+1$, $g \geq 1$. Then $m = 4g+3$ with $g \geq 1$. We have $1 + \sum_{i=1}^{2g+1} \gamma_{2i} = 0$, as the sum of all roots of 1 of degree $4g+3$. Set $C_0 = (A_s(x_r) + \gamma_1)/(x_r - x_0)$ and $C_i = (A_s(x_r) - (-1)^i \gamma_{2i})/(x_r - x_0)$ for $i = 1, ..., 2g+1$. Then

$$C_0 + \sum_{i=1}^{2g+1} (-1)^i C_i = \frac{\gamma_1 - 1}{x_r - x_0} \in \mathcal{O}. \tag{22}$$

We show that $\gamma_1 - 1 \in \mathcal{O}^*$. Since $\gamma_1$ is a root of the polynomial $P_{4g+2}(\lambda)$, we have that $\gamma_1 - 1$ is a root of the polynomial $P_{4g+2}(\lambda + 1)$. Its constant term is equal to

$$P_{4g+2}(1) = P_{4g+2}(2\cos(\frac{\pi}{3})) = \frac{\sin((4g+3)\pi/3)}{\sin(\pi/3)} \in \{-1, 1, 0\}.$$

Note that $P_{4g+2}(1) = 0$ if and only if $4g+3$ is divisible by 3, i.e. $g$ is divisible by 3. Let $g = 3g_1$. Then $4g+3 = 12g_1 + 3 = 3(4g_1 + 1)$, whence $m$ is divisible by $4g_1 + 1$. This contradicts our assumptions. Hence $P_{4g+2}(1) = \pm 1$ and $\gamma_1 - 1 \in \mathcal{O}^*$. Then it follows from (21) that for each $r \not\equiv 0 \pmod p$ we have $1/(x_r - x_0) \in \mathcal{O}$. We obtain again a contradiction to item 4) of Lemma 7.

Finally, consider the case, where $m$ is even. Let $m = m_1 2^g$, where $g \geq 1$ and $m_1 > 1$ is odd. Consider the numbers $\gamma_{i2^g} = 2\cos(i\pi/m_1)$. Arguing just as in the case of odd $m$ above, we obtain a contradiction to item 4) of Lemma 7.

Thus, there exist $t$ and $r$ such that $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathcal{O}$. Then the constant term in the equation (21) does not belong to $\mathcal{O}$ and (21) has a root $z_0 \notin \mathcal{O}$. Let $A, B \in \mathrm{SL}_2(\mathbb{C})$ be matrices such that

$$\mathrm{tr}\, A = x_r, \qquad \mathrm{tr}\, B = \beta, \qquad \mathrm{tr}\, AB = z_0.$$

By construction, they determine a representation of the group $\Gamma_n$ into $\mathrm{PSL}_2(\mathbb{C})$. Applying Lemma 6, we complete the proof of Theorem 2.

*Remark.* In several cases one can obtain a more precise information on decomposing a generalized triangle group $\Gamma$ into a non-trivial free product with amalgamation. For example, consider the following group $\Gamma_k = \langle a, b \mid a^2 = b^k = (ab^2)^3 = 1\rangle$. Then it follows from Theorem 2 that $\Gamma_k$ is a non-trivial free product with amalgamation if $k = 2k_1$, where $1 < k_1 \neq 2^l$. However, it is easy to see that for $k_1 = 2^l$, $l \geq 1$, the group $\Gamma_k$ is a non-trivial free product with amalgamation as well. Indeed, let $F_2 = \langle g, h \rangle$ be a free group and let $x = \tau_g = 0$, $y = \tau_h$, and $z = \tau_{gh}$. Consider the equation

$$Q_{gh^2}(0, y, z) = yz = 2\cos(\pi/3) = 1.$$

Let $y = y_r = 2\cos(r\pi/2^{l+1})$. By item 6) of Lemma 7, we have $z_r = 1/y_r \notin \mathcal{O}$ for each odd $r$. Then Lemma 6 implies that $\Gamma_k$ is a non-trivial free product with amalgamation.

# 4. Proof of Theorem 3

First, assume that the word $R(a, b) = a^{u_1}b^{v_1} \dots A^{u_s}b^{v_s}$ satisfies the condition $v = \max_{1\leq i\leq s} |v_i| \geq 2$. Then, by Theorem 2, there exists a prime $p$ such that the group $\Gamma_1 = \langle a, b \mid a^n = b^{pv} = R^m(a, b) = 1\rangle$ is a non-trivial free product with amalgamation. Since $\Gamma_1$ is an epimorphic image of $\Gamma$, the group $\Gamma$ is a non-trivial free product with amalgamation as well.

Thus we can assume that

$$R(a, b) = a^{u_1}b^{v_1} \dots a^{u_s}b^{v_s},$$

where $v_i \in \{-1, 1\}$, $i = 1, \dots, s$. Suppose for a moment that either $v_i = v_{i+1}$ for some $i < s$ or $v_1 = v_s$. Let, for example, $v_1 = v_2$. Then we consider the new generators of the group $\Gamma$: $a_1 = a$, $b_1 = a^{u_2}b^{v_1}$. It is easy to see that $\Gamma = \langle a_1, b_1 \mid a_1^n = R_1^m(a_1, b_1) = 1\rangle$, where $R_1(a_1, b_1) = a_1^{u_1'}b_1^{v_1'} \dots A_1^{u_l'}b_1^{v_l'}$, $0 < u_i' < n$, and $v_i' \neq 0$ for $i = 1, \dots, l$. In addition, we have $v' = \max_{1\leq i\leq l} |v_i'| \geq 2$, thus reducing this case to the previous one.

Thus without loss of generality we can assume that

$$R(a, b) = a^{u_1}ba^{u_2}b^{-1} \dots a^{u_{2k-1}}ba^{u_{2k}}b^{-1},$$

where $k \geq 1$ and $0 < u_i < n$ for $i = 1, \dots, 2k$. Set $c = ba^{-1}b^{-1}$. Then

$$R(a, b) = a^{u_1}c^{-u_2} \dots a^{u_{2k-1}}c^{-u_{2k}} = R_1(a, c).$$

Let $F_2 = \langle g, h \rangle$ be a free group of rank 2 and $f = hg^{-1}h^{-1}$. Set $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$, and $t = \tau_{gf}$. Then $\tau_f = \tau_g = x$ and $t = \tau_{gf} = \tau_{ghg^{-1}h^{-1}} = x^2 + y^2 + z^2 - xyz - 2$, by item 1 of Lemma 9. Consider the element $R_1(g, f) \in F_2$ as a word in $g$ and $f$. Let $q(x, t)$ be the Fricke polynomial of $R_1(g, f)$, i.e.

$$q(x, t) = Q_{R_1(g,f)}(\tau_g, \tau_f, \tau_{gf}) = Q_{R_1(g,f)}(x, x, t).$$

Since $R_1(g,f)$ contains $k$ blocks of the form $g^{u_j}f^{-u_{j+1}}$, by Lemma 5, the degree of the polynomial $q(x,t)$ with respect to $t$ is equal to $k$ and the leading coefficient of $q(x,t)$ is equal to $(-1)^k\prod_{i=1}^{2k}P_{u_i-1}(x)$. Since by construction $R(g,h)=R_1(g,f)$, we have

$$Q_{R(g,h)}(x,y,z)=q(x,t)=q(x,x^2+y^2+z^2-xyz-2). \tag{23}$$

For numbers $r\not\equiv 0\,(\mathrm{mod}\ n)$, $l\not\equiv 0\,(\mathrm{mod}\ m)$ we set $x=\tau_g=\alpha_r=2\cos(r\pi/n)$, $\gamma_l=2\cos(l\pi/m)$ and consider the equation

$$Q_{R(g,h)}(\alpha_r,y,z)=\gamma_l. \tag{24}$$

By (23), we can rewrite (24) in the form

$$q(\alpha_r,t)=\gamma_l. \tag{25}$$

Lemma 10 *There exist $r,l\in\mathbb{Z}$, where $r\not\equiv 0\,(\mathrm{mod}\ n)$ and $l\not\equiv 0\,(\mathrm{mod}\ m)$ such that $P_{u_i-1}(\alpha_r)\neq 0$ for $i=1,\dots,2k$ and the equation (25) has a root $t=t_0\neq 2$.*

*Proof.* First let $m\geq 3$. In this case $\gamma_1\neq\gamma_2$. Set $r=1$. Then the degree of the polynomial $q(\alpha_1,t)$ is equal to $k$. Obviously, at least one of the equations $q(\alpha_1,t)=\gamma_1$ and $q(\alpha_1,t)=\gamma_2$ has a root $t_0\neq 2$.

Next assume $m=2$. Suppose that the equation $q(\alpha_r,t)=0$ has the unique root $t=2$. This means that for arbitrary matrices $A,B\in\mathrm{SL}_2(\mathbb{C})$ such that $\mathrm{tr}\,A=\mathrm{tr}\,B=\alpha_r$, the condition $\mathrm{tr}\,R_1(A,B)=\mathrm{tr}\,A^{u_1}B^{-u_2}\dots A^{u_{2k-1}}B^{-u_{2k}}=0$ implies that $\mathrm{tr}\,AB=2$. So to obtain a contradiction, it suffices to find matrices $A,B\in\mathrm{SL}_2(\mathbb{C})$ satisfying the conditions:

1) $\mathrm{tr}\,A=\mathrm{tr}\,B=\alpha_r$;
2) $\mathrm{tr}\,AB\neq 2$;
3) $\mathrm{tr}\,R_1(A,B)=\mathrm{tr}\,A^{u_1}B^{-u_2}\dots A^{u_{2k-1}}B^{-u_{2k}}=0$.

We find $A$ and $B$ in the form

$$A=\begin{pmatrix}\varepsilon_r & w\\ 0 & \varepsilon_r^{-1}\end{pmatrix},\qquad B=\begin{pmatrix}\varepsilon_r & 0\\ w & \varepsilon_r^{-1}\end{pmatrix},$$

where $\varepsilon_r+\varepsilon_r^{-1}=\alpha_r=2\cos(r\pi/n)$ and $w$ is a variable. It is easy to see that $\mathrm{tr}\,AB=w^2+\varepsilon_r^2+\varepsilon_r^{-2}$. The condition $\mathrm{tr}\,AB\neq 2$ is equivalent to $w^2+\varepsilon_r^2+\varepsilon_r^{-2}\neq 2$, i.e.

$$w^2\neq 2-(\varepsilon_r^2+\varepsilon_r^{-2})=2-2\cos(\tfrac{2r\pi}{n})=4\sin^2(\tfrac{r\pi}{n}).$$

It is easy to verify by induction that

$$A^i=\begin{pmatrix}\varepsilon_r^i & P_{i-1}(\alpha_r)w\\ 0 & \varepsilon_r^{-i}\end{pmatrix},\qquad B^i=\begin{pmatrix}\varepsilon_r^i & 0\\ P_{i-1}(\alpha_r)w & \varepsilon_r^{-i}\end{pmatrix},$$

and

$$R_1(A,B) = \begin{pmatrix} \varepsilon_r^d + C_1(\alpha_r)w^2 + \cdots + C_k(\alpha_r)w^{2k} & wf_1(w) \\ wf_2(w) & \varepsilon_r^{-d} + D_1(\alpha_r)w^2 + \cdots + D_{k-1}(\alpha_r)w^{2k-2} \end{pmatrix}$$

where $d = \sum_{i=1}^{2k} u_i$, $C_k(\alpha_r) = (-1)^k \prod_{i=1}^{2k} P_{u_i-1}(\alpha_r)$, $f_1(w)$ and $f_2(w)$ are some polynomials in $w$. Hence

$$\operatorname{tr} R_1(A,B) = C_k(\alpha_r)w^{2k} + \cdots + (C_1(\alpha_r) + D_1(\alpha_r))w^2 + (\varepsilon_r^d + \varepsilon_r^{-d}) = g(w^2).$$

We claim that there exists $r$, where $1 \le r < n$ such that $C_k(\alpha_r) \neq 0$ and the polynomial $g(w^2)$ has a root $w_0$ with $w_0^2 \neq 4\sin^2(r\pi/n)$. Assume the contrary. Suppose that for each $r$ such that $C_k(\alpha_r) \neq 0$ we have

$$g(w) = C_k(\alpha_r)(w - 4\sin^2(\tfrac{r\pi}{n}))^k. \tag{26}$$

Comparing the constant terms in the left and right parts of (26) and taking into account the expression for $C_k(\alpha_r)$, we obtain

$$\left(\prod_{i=1}^{2k} P_{u_i-1}(2\cos(\tfrac{r\pi}{n}))\right) 4^k \left(\sin(\tfrac{r\pi}{n})\right)^{2k} = 2\cos(\tfrac{dr\pi}{n}). \tag{27}$$

By (4), we have $P_{u_i-1}(2\cos(r\pi/n)) = \sin(u_i r\pi/n)/\sin(r\pi/n)$. Let $u_i/n = u_i'/n_i$, where $(u_i', n_i) = 1$. Then (27) has the form

$$\prod_{i=1}^{2k} \left(2\sin\left(\tfrac{u_i' r\pi}{n_i}\right)\right) = 2\cos(\tfrac{dr\pi}{n}). \tag{28}$$

On the other hand, we show that the assumption that (28) holds for each $r$ such that the left part of (28) is non-zero leads to a contradiction.

First consider the case, where $n$ is odd. Let $n_0 = \min_j n_j$ and let, say, $n_0 = n_1$. Then $n_1$ is odd. Let $p > 2$ be a prime divisor of $n_1$. Set $r = n_1/p$. Then $2\sin(u_1' r\pi/n_1) = 2\sin(u'1\pi/p)$. If $j > 1$, then $2\sin(u_j' r\pi/n_j) = 2\sin(u_j' n_1\pi/(pn_j)) \neq 0$ because, by construction, $pn_j$ does not divide $u_j' n_1$. It follows from (28) that

$$\prod_{i=2}^{2k} \left(2\sin\left(\tfrac{u_i' n_1\pi}{pn_i}\right)\right) = \frac{2\cos(dn_1\pi/(pn))}{\sin(u_1'\pi/p)} \in \mathcal{O}. \tag{29}$$

If $dn_1$ is divisible by $pn$, then $2\cos(dn_1\pi/(pn)) = \pm 1$. Otherwise, $2\cos(dn_1\pi/(pn)) \in \mathcal{O}^*$, by item 2 of Lemma 7. It follows from (29) that in both cases $1/(2\sin(u_1'\pi/p)) \in \mathcal{O}$, which contradicts item 5 of Lemma 7.

Now let $n = 2^l n'$, where $l \ge 1$ and $n'$ is odd. Set $n_i = 2^{l_i} n_i'$, where $l_i \ge 0$ and $n_i'$ is odd. Let $n_0' = \min_j n_j'$.

If $n_0' > 1$, then we set $r = 2^l r'$, where $r' \not\equiv 0 \,(\mathrm{mod}\ n')$. Then (28) has the form

$$\prod_{i=1}^{2k} \left( 2\sin\left(\tfrac{u_i' 2^{l-l_i} r' \pi}{n_i'}\right)\right) = 2\cos(\tfrac{dr'\pi}{n'}), \tag{30}$$

where $n'$ is odd. But we have proved above that there exists $r'$ such that the left part of (30) is non-zero and the equality (30) is not valid.

Now let $n_0' = 1$. Set

$$I = \{i \mid n_i' = 1\}, \qquad l_0 = \min_{i \in I} l_i, \qquad I_0 = \{i \in I \mid l_i = l_0\}.$$

Furthermore, we set $r = 2^{l_0 - 1} r'$, where $r'$ is odd. Then for $i \in I_0$, we have

$$2\sin\left(\tfrac{u_i' r\pi}{n_i}\right) = 2\sin\left(\tfrac{u_i' 2^{l_0-1} r'\pi}{2^{l_0}}\right) = 2\sin\left(\tfrac{u_i' r'\pi}{2}\right) = \pm 2.$$

It follows that the equality (28) can be rewritten in the form:

$$\prod_{i \notin I_0} \left( 2\sin\left(\tfrac{u_i' r'\pi}{2^{l_i - l_0 + 1} n_i'}\right)\right) = \pm \tfrac{1}{2^{|I_0|-1}} \cos(\tfrac{dr'\pi}{2^{l-l_0+1} n'}). \tag{31}$$

Choose $r'$ such that the left part of (31) is non-zero. Then the right part of (31) should be non-zero as well. If $|I_0| > 1$ or $|I_0| = 1$ and $\cos(dr'\pi/(2^{l-l_0+1}n')) \neq \pm 1$, then the left part of (31) belongs to $\mathcal{O}$. But by item 1) of Lemma 7, the right part of (31) does not belong to $\mathcal{O}$ – a contradiction.

So it remains to consider the case $|I_0| = 1$ and $\cos(dr'\pi/(2^{l-l_0+1}n')) = \pm 1$. In this case (31) has the form

$$\prod_{i \neq i_0} \left( 2\sin\left(\tfrac{u_i' r'\pi}{2^{l_i - l_0 + 1} n_i'}\right)\right) = \pm 1. \tag{32}$$

If $|I| > 1$ and $i_0 \neq i \in I$, then $l_i > l_0$ and $n_i = 1$. Hence for each odd $r'$, the left part of (32) is non-zero and it follows from (32) that $1/(2\sin(u_i' r'\pi/(2^{l_i - l_0 + 1}))) \in \mathcal{O}$. This contradicts to item 5 of Lemma 7.

Now let $I = I_0 = \{i_0\}$. Set

$$n_{j_0} = \min_{j \neq i_0} n_j \geq 3, \qquad J = \{j \mid n_j = n_{j_0}\}, \qquad l_{j_0} = \min_{j \in J} l_j.$$

If $l_{j_0} - l_0 + 1 > 0$, then we put $r' = n_{j_0}$. It is easy to see that in this case the left part of (32) is not equal to 0 and it follows from (32) that $1/(2\sin(u_{j_0}'\pi/2^{l_{j_0} - l_0 + 1})) \in \mathcal{O}$, which is impossible, by item 6 of Lemma 7.

Finally, if $l_{j_0} - l_0 + 1 \leq 0$, then we take an arbitrary prime divisor $p \geq 3$ of $n_{j_0}$ and set $r' = n_{j_0}/p$. Then, as above, the left part of (32) is not equal to 0 and we obtain, by (32), that

$$2\sin\left(\tfrac{u_{j_0}' r'\pi}{2^{l_{j_0} - l_0 + 1} n_{j_0}'}\right) = 2\sin\left(\tfrac{u_{j_0}' 2^{-l_{j_0} + l_0 - 1}\pi}{p}\right) \in \mathcal{O}^*.$$

This contradicts to item 5 of Lemma 7. Lemma 10 is proved.

Now we can complete the proof of Theorem 3. By Lemma 10, one can choose $r, l$ such that the equation (25) has a root $t_0 \neq 2$. Since, by construction, $t = x^2+y^2+z^2-xyz-2$ and $x = \alpha_r$, it follows that $y$, $z$ satisfy the equation

$$y^2 + z^2 - \alpha_r yz + \alpha_r^2 - 2 - t_0 = 0. \tag{33}$$

Let $(y_0, z_0)$ be some solution of (33) and let $A, B \in \mathrm{SL}_2(\mathbb{C})$ be matrices such that $\operatorname{tr} A = \alpha_r$, $\operatorname{tr} B = y_0$, and $\operatorname{tr} AB = z_0$. Then, by construction, $\operatorname{tr} ABA^{-1}B^{-1} = t_0$, $\operatorname{tr} R(A, B) = \gamma_l$, and the pair of matrices $(A, B)$ determines a representation of the group $\Gamma$ into $\mathrm{PSL}_2(\mathbb{C})$. Note that this representation is irreducible because $t_0 \neq 2$.

Lemma 6 shows that to complete the proof it suffices to find a a solution $(y_0, z_0)$ of the equation (33) with the following properties.

1) There exists an element of finite order $W_1(A, B) = A^{\alpha_1}B^{\beta_1} \dots A^{\alpha_g}B^{\beta_g}$ such that $\alpha_i, \beta_i \neq 0$ for $i = 1, \dots, g$ and $\sum_{i=1}^{g} \beta_g \neq 0$.
2) $z_0 = \operatorname{tr} AB \notin \mathcal{O}$.

The rest of the proof depends on the form of $t_0$. We consider the following cases:
1) $t_0 \notin \mathcal{O}$;
2) $t_0 = 2\cos((2k + 1)\pi/(2s + 1))$, where $s \geq 1$ and $(2k + 1, 2s + 1) = 1$;
3) $t_0 = 2\cos(2k\pi/(2s + 1))$, where $s \geq 1$ and $(k, 2s + 1) = 1$;
4) $t_0 = 2\cos((2k + 1)\pi/(2s))$, where $s \geq 1$ and $(2k + 1, s) = 1$;
5) $t_0 \in \mathcal{O}$ and $t_0 \neq 2\cos(k\pi/s)$ for arbitrary integers $k$ and $s$.

Case 1. Set $y_0 = 0$ and $W_1(A, B) = B$. Then $W_1(A, B) = B$ has order 4. Since $t_0 \notin \mathcal{O}$, the equation (33) has a solution $(0, z_0)$ such that $z_0 \notin \mathcal{O}$.

Case 2. Set $W_1(A, B) = AB(ABA^{-1}B^{-1})^s$. Combining Lemmas 8 and 9, we obtain

$$\operatorname{tr} W_1(A, B) = (P_{s+1}(t_0) - P_s(t_0))z_0 = 0 \cdot z_0 = 0.$$

Hence $W_1(A, B)$ has order 4. Now we can take an arbitrary solution $(y_0, z_0)$ of the equation (33) with $z_0 \notin \mathcal{O}$.

Case 3. Set $W_1(A, B) = AB(ABA^{-1}B^{-1})^s$ and assume that

$$\operatorname{tr} W_1(A, B) = 2\cos(\pi/3) = 1.$$

Then $W_1(A, B)$ has order 6 and it follows from item 2 of Lemma 9 that

$$\operatorname{tr} W_1(A, B) = (P_{s+1}(t_0) - P_s(t_0))z_0 = 1.$$

Hence, by item 3 of Lemma 8, we have $z_0 = 1/(P_{s+1}(t_0) - P_s(t_0)) \notin \mathcal{O}$. and so we can take any solution $(y_0, z_0)$ of (33).

Case 4. Set $W_1(A,B) = (AB)^{-1}(ABA^{-1}B^{-1})^s(AB)^2(ABA^{-1}B^{-1})^s$ and assume that

$$\operatorname{tr} W_1(A,B) = 2\cos(\pi/3) = 1. \tag{34}$$

Then $W_1(A,B)$ has order 6 and, by item 3 of Lemma 9, we can write (34) in the form

$$(t_0-2)P_{s-1}(t_0)^2 z_0^3 + (2 - P_{2s-1}(t_0) + P_{2s-2}(t_0))z_0 - 1 = 0. \tag{35}$$

By item 4 of Lemma 8, we have $0 \neq P_{s-1}(t_0) \notin \mathcal{O}^*$, whence

$$1/((t_0-2)P_{s-1}(t_0)^2) \notin \mathcal{O}.$$

It follows that (35) has a root $z_0 \notin \mathcal{O}$ and again we can take any solution $(y_0, z_0)$ of (33).

Case 5. Since $t_0 \in \mathcal{O}$ and $t_0 \neq 2\cos(k\pi/s)$ for arbitrary integers $k$ and $s$, by item 5 of Lemma 8, there exists an integer $l > 0$ such that $0 \neq P_l(t_0) \notin \mathcal{O}^*$. Set $W_1(A,B) = (AB)^{-1}(ABA^{-1}B^{-1})^{l+1}(AB)^2(ABA^{-1}B^{-1})^{l+1}$ and assume that (34) holds. Then $W_1(A,B)$ has order 6 and, by item 3 of Lemma 9 we can write (34) in the form

$$(t_0-2)P_l(t_0)^2 z_0^3 + (2 - P_{2l+1}(t_0) + P_{2l}(t_0))z_0 - 1 = 0. \tag{36}$$

Since by construction, $1/((t_0-2)P_l(t_0)^2) \notin \mathcal{O}$, we obtain that (36) has a root $z_0 \notin \mathcal{O}$. So any solution $(y_0, z_0)$ of (33) is as required. Theorem 3 is proved.

## References


[1] R.C. Lyndon and P.E. Schupp, “Combinatorial group theory”, Springer-Verlag, Berlin–Heidelberg–New York, 1977.

[2] C.T.C. Wall (editor), “Homological group theory” (Proceedings of a conference in Durham), *London Math. Soc. Lecture Notes.* **36** (1977).

[3] G. Baumslag, and P.B. Shalen,“ Amalgamated products and finitely presented groups”, *Comment. Math. Helv.* **65** (1990), 243–254.

[4] B. Fine, F. Levin, and G. Rosenberger, “Free subgroups and decompositions of one-relator products of cyclics; Part 2: Normal torsion free subgroups and FPA decompositions”, *J. of Indian Math. Soc.* **49** (1985), 237–247.

[5] H. Zieschang, “On decompositions of discontinuous groups of the plane”, *Math. Zeit.* **151** (1976), 165–188.

[6] G. Rosenberger, “Bemerkungen zu einer Arbeit von H. Zieschang”, *Arch. der Math.* **29** (1977), 623–627.

[7] D.D. Long, C. Maclachlan, and A.W. Reid, “Splitting groups of signature $(1, n)$”, *J. of Algebra.* **185** (1996), 329–341.

[8] M.J. Dunwoody and M. Sageev, “Splittings of certain Fuchsian groups”, *Proc. of the Amer. Math. Soc.* **125**:7 (1997), 1953–1954.

[9] V.V. Benyash-Krivets, “Decomposing one-relator products of cyclic groups into free products with amalgamation”, *Sbornik: Mathematics,* **189**:8 (1998), 1125–1137.

[10] V.V. Benyash-Krivets, “On decomposing some $F$-groups into free products with amalgamation” (in Russian), *Dokl. Akad. Nauk Belarus* , **41**:6 (1997), 1–4.

[11] A. Lubotzky and A. Magid, “Varieties of representations of finitely generated groups”, *Memoirs AMS.* **58** (1985), 1–116.

[12] M. Culler and P. Shalen, “Varieties of group representations and splittings of 3 manifolds”, *Ann. of Math.* **117** (1983), 109–147.

[13] A.S. Rapinchuk, V.V. Benyash-Krivets, and V.I. Chernousov, “Representation varieties of the fundamental groups of compact orientable surfaces”, *Israel J. Math.* **93** (1996), 29–71.

[14] V.V. Benyash-Krivets and V.I. Chernousov, "Representation varieties of the fundamental groups of compact non-orientable surfaces", *Sbornik: Mathematics,* **188**:7 (1997), 997–1039.

[15] D. Mumford, "Geometric invariant theory", Springer-Verlag, Berlin–Heidelberg–New York, 1965.

[16] R. Horowitz, "Characters of free groups represented in the two dimensional linear group", *Comm. Pure. Appl. Math.* **25** (1972), 635–649.

[17] H. Helling, "Diskrete Untergruppen von $\mathrm{SL}_2(\mathbb{R})$", *Invent. Math.* **17** (1972), 217–229.

[18] W. Magnus, "The uses of 2 by 2 matrices in combinatorial group theory", *Result. der Math.* **4**:2 (1981), 171–192.

[19] J.-P. Serre, "Arbres, amalgames, $\mathrm{SL}_2$", *Astérisque* , **42** (1977).

[20] E.B. Vinberg, "Rings of definition of dense subgroups of semisimple linear groups", Math. USSR Izvestiya, **5**:1 (1971), 45–55.

[21] I.R. Shafarevich, "Basic algebraic geometry", Springer-Verlag, Berlin–Heidelberg–New York, 1974.

[22] C. Traina, "Trace polynomial for two generated subgroups of $\mathrm{SL}_2(\mathbb{C})$", *Proc. Amer. Math. Soc.* **79** (1980), 369–372.

[23] H. Bass, "Finitely generated subgroups of $\mathrm{GL}_2(\mathbb{C})$", *in "The Smith Conjecture"*, Wiley, New York, 1984, pp. 127–136.