FINITE QUOTIENTS OF RINGS AND APPLICATIONS TO SUBGROUP SEPARABILITY OF LINEAR GROUPS

EMILY HAMILTON

Abstract. In this paper we apply results from algebraic number theory to subgroup separability of linear groups. We then state applications to subgroup separability of free products with amalgamation of hyperbolic 3-manifold groups.

1. Introduction

Definition 1.1. (1) Let \( H \) be a subgroup of a group \( G \). \( H \) is separable in \( G \) if, given any element \( g \in G \setminus H \), there is a finite index subgroup \( K \subset G \), such that \( H \subset K \) but \( g \notin K \).

(2) A group \( G \) is residually finite if the subgroup consisting of the identity element is separable in \( G \). Equivalently \( G \) is residually finite if for any non-trivial element \( g \) of \( G \), there is a homomorphism \( \phi \) of \( G \) to a finite group with \( \phi(g) \) non-trivial.

(3) A group \( G \) is subgroup separable, or LERF (locally extended residually finite), if every finitely generated subgroup of \( G \) is separable in \( G \).

Subgroup separability is a powerful property. If a finitely presented group \( G \) is subgroup separable, then, given a finitely generated subgroup \( H \) of \( G \), there is an algorithm to decide in a finite number of steps whether or not a given word in \( G \) belongs to \( H \) \[14\]. In geometric topology, subgroup separability is interesting since it allows certain immersions to lift to embeddings in finite sheeted covering spaces \[19\]. This is often used in low-dimensional topology and especially in the theory of 3-manifolds.

This paper was motivated by the study of subgroup separability of fundamental groups of hyperbolic 3-manifolds, and free products with amalgamation of these groups. Suppose that \( \Gamma \) is the fundamental group of an orientable hyperbolic 3-manifold \( M \). Then there exists a discrete faithful representation from \( \Gamma \) into \( \text{SL}(2, \mathbb{C}) \). If \( M \) has finite volume, then we may view \( \Gamma \subset \text{SL}(2, \mathbb{R}) \), where \( \mathbb{R} \) is a finitely generated ring in a number field \( k \). Proving that subgroups of \( \Gamma \) are separable involves finding group homomorphisms from \( \Gamma \) into finite groups. To construct these homomorphisms, we can work with the ring \( \mathbb{R} \). A ring homomorphism from \( \mathbb{R} \) into a finite ring \( S \) induces a group homomorphism from \( \Gamma \) into the finite group \( \text{SL}(2, S) \). To find these ring homomorphisms, we may apply results from algebraic...
number theory. For example, let $h$ be an element of $\Gamma$ of the form

$$h = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad |\lambda| \neq 1,$$

and let $a, b \in \mathbb{Z}$ with $a \nmid b$. Suppose that we want to find a subgroup $K$ of finite index in $\Gamma$ that contains $\langle h^a \rangle$ but not $h^b$. To do this, we first apply a result from algebraic number theory, Corollary 2.5 of this paper, to find a ring homomorphism from $R$ into a finite field $F$ such that the multiplicative order of the image of $\lambda$ is divisible by $a$. If $\phi : \Gamma \subset \text{SL}(2, R) \rightarrow \text{SL}(2, F)$ is the induced group homomorphism and $N$ is the kernel of $\phi$, then $K = \langle h^a \rangle N$ satisfies the required conditions. As this example indicates, problems involving subgroup separability of fundamental groups of hyperbolic 3-manifolds can be reduced to algebraic problems involving finitely generated rings in number fields. The point of this paper is to prove a few of these algebraic results and then to describe some applications.

This paper is organized as follows. In section 2, we prove algebraic results regarding finite quotients of finitely generated rings in number fields. In section 3, we apply these results to subgroup separability of linear groups. In section 4, we mention some applications to subgroup separability of free products with amalgamation of hyperbolic 3-manifold groups.

2. Finite quotients of rings

In this section we collect results on finite quotients of finitely generated rings contained in number fields. We assume standard terminology and results of algebraic number theory. For reference see [11].

**Notation 2.1.**

1. By a number field we mean a finite field extension of $\mathbb{Q}$. If $k$ is a number field, let $\mathcal{O}_k$ denote the ring of algebraic integers of $k$. If $p$ is a non-zero prime ideal of $\mathcal{O}_k$, then we complete $k$ at $p$ to obtain the local field $k_p$, with ring of algebraic integers $\mathcal{O}_{k_p}$. The ring $\mathcal{O}_{k_p}$ has a unique maximal ideal. The quotient of $\mathcal{O}_{k_p}$ by this maximal ideal is called the residue class field of $\mathcal{O}_{k_p}$. The quotient map is called the residue class field map with respect to $p$.

2. Given a non-zero prime ideal $p$ of $\mathcal{O}_k$, let $\nu_p$ denote the exponential $p$-adic valuation of $k$. We say $p$ divides a non-zero element $x \in k$, and write $p | x$, if $\nu_p(x) \neq 0$. If $x$ and $y$ are non-zero elements of $k$, then we say $(x, y) = 1$ in $\mathcal{O}_k$ if no prime ideal $p$ of $\mathcal{O}_k$ divides both $x$ and $y$.

3. Facts: (i) $x \in \mathcal{O}_{k_p}$ iff $\nu_p(x) \geq 0$, (ii) $x$ is contained in the unique maximal ideal of $\mathcal{O}_{k_p}$ iff $\nu_p(x) > 0$, and (iii) $x$ is a unit in $\mathcal{O}_{k_p}$ iff $\nu_p(x) = 0$.

4. We denote a primitive $r$th root of unity by $\zeta_r$.

5. For any field $F$, we denote the group of $n$th powers of non-zero elements of $F$ by $F^n$.

We begin with a theorem due to Postnikova and Schinzel [16, 18]. From this result we prove a theorem and two corollaries. The corollaries have applications to subgroup separability of linear groups. The first corollary follows immediately from the proof of Proposition 1 of [1] or Proposition 5 of [9]. We give an alternative proof in this paper. This corollary is an integral part of the proof from [1] that abelian subgroups of finitely generated discrete subgroups of $\text{PSL}(2, \mathbb{C})$ are separable. Both corollaries will be used in section 3 of this paper.
Theorem 2.2. Let $a$ and $b$ be non-zero algebraic integers of a number field $L$ such that $(a,b) = 1$ in $\mathcal{O}_L$ and $a/b$ is not a root of unity. Let $t$ be a positive integer. A non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ is called a primitive divisor of $a^t - b^t$ if $\mathfrak{P} \mid (a^t - b^t)$ but $\mathfrak{P} \nmid (a^s - b^s)$ for all positive integers $s$ that are less than $t$. Then there exists a positive integer $r$ such that $a^t - b^t$ has a primitive divisor in $\mathcal{O}_L$ for all $t \geq r$.

From Theorem 2.2 we prove the following.

Theorem 2.3. Let $k$ be a number field and let $\delta$ be a non-zero element of $k$ that is not a root of unity. Let $S$ be a finite set of prime ideals of $\mathcal{O}_k$. Then there exists a positive integer $n$ with the following property. For each integer $m \geq n$, there exists a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$, lying outside of $S$, such that $\delta \in \mathcal{O}_k$, and the multiplicative order of the image of $\delta$ in the residue class field of $\mathcal{O}_k$, is equal to $m$.

Proof. We claim that there exists a finite field extension $L$ of $k$ and elements $a, b \in \mathcal{O}_L$ such that $\delta = a/b$ and $(a, b) = 1$ in $\mathcal{O}_L$. Since $k$ is the quotient field of $\mathcal{O}_k$, there exist elements $x, y \in \mathcal{O}_k$ such that $\delta = x/y$. Let $x\mathcal{O}_k$ and $y\mathcal{O}_k$ denote the principal ideals in $\mathcal{O}_k$ generated by $x$ and $y$, respectively. Since $\mathcal{O}_k$ is a Dedekind domain, every non-zero ideal of $\mathcal{O}_k$ has a unique factorization as a product of prime ideals. We say a prime ideal $\mathfrak{p}$ divides a non-zero ideal $\mathfrak{a}$ if $\mathfrak{p}$ appears in this factorization. Express $x\mathcal{O}_k = ab_1$ and $y\mathcal{O}_k = ab_2$, where $a, b_1$ and $b_2$ are ideals of $\mathcal{O}_k$, and no prime ideal of $\mathcal{O}_k$ divides both $b_1$ and $b_2$. By the Principal Ideal Theorem, there exists a finite field extension $L$ of $k$, namely the Hilbert class field of $k$, such that every ideal of $\mathcal{O}_k$ becomes principal when extended to an ideal of $\mathcal{O}_L$. Given an ideal $\mathfrak{a}$ of $\mathcal{O}_k$, let $\mathfrak{a}^e$ denote the extension of $\mathfrak{a}$ to $\mathcal{O}_L$; that is, the ideal in $\mathcal{O}_L$ generated by $a$. Then

$$x\mathcal{O}_L = (x\mathcal{O}_k)^e = (ab_1)^e = a^e b_1^e = (z\mathcal{O}_k)(w_1\mathcal{O}_L) = (zw_1)\mathcal{O}_L \text{ and}$$

$$y\mathcal{O}_L = (y\mathcal{O}_k)^e = (ab_2)^e = a^e b_2^e = (z\mathcal{O}_k)(w_2\mathcal{O}_L) = (zw_2)\mathcal{O}_L,$$

where $z, w_1$ and $w_2$ are generators of the principal ideals $a^e$, $b_1^e$ and $b_2^e$, respectively. It follows that $x = zw_1w_2$ and $y = zw_2w_1$, where $w_1$ and $w_2$ are units in $\mathcal{O}_L$. Let $a = w_1w_2$ and $b = w_2w_1$. Then $a$ and $b$ are elements of $\mathcal{O}_L$ and $\delta = a/b$. Moreover, $a\mathcal{O}_L = w_1\mathcal{O}_L = b_1^e$ and $b\mathcal{O}_L = w_2\mathcal{O}_L = b_1^e$. If a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ divides $b_1^e$, then the prime ideal $\mathfrak{P} \cap \mathcal{O}_k$ of $\mathcal{O}_k$ divides $b_1$. Similarly for $b_2$. By construction, no prime ideal of $\mathcal{O}_k$ divides both $b_1$ and $b_2$. Therefore, no prime ideal of $\mathcal{O}_L$ divides both $a\mathcal{O}_L$ and $b\mathcal{O}_L$. Equivalently, $(a, b) = 1$ in $\mathcal{O}_L$. This proves the claim.

By Theorem 2.2 there exists a primitive divisor $t$ such that $a^t - b^t$ has a primitive divisor in $\mathcal{O}_L$ for all $t \geq r$. Let $\mathfrak{P}_r, \mathfrak{P}_{r+1}, ...$ be primitive divisors in $\mathcal{O}_L$ of $a^r - b^r, a^{r+1} - b^{r+1}, ...$, respectively. By the definition of a primitive divisor, the primes $\mathfrak{P}_r, \mathfrak{P}_{r+1}, ...$ are distinct. Given a prime $\mathfrak{p}$ of $\mathcal{O}_k$, there exist finitely many primes $\mathfrak{P}$ of $\mathcal{O}_L$ such that $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_k$. It follows that each prime of $S$ appears on the list $\mathfrak{P} \cap \mathcal{O}_k, (\mathfrak{P}_{r+1} \cap \mathcal{O}_k), ...$ at most finitely many times. Therefore, there exists a positive integer $m \geq r$ such that $\{ \mathfrak{P}_m \cap \mathcal{O}_k, (\mathfrak{P}_{m+1} \cap \mathcal{O}_k), ... \} \cap S = \emptyset$. Fix $m \geq n$. To simplify notation, let $\mathfrak{P}$ denote the primitive divisor $\mathfrak{P}_m$ of $a^m - b^m$. Since $\mathcal{O}_L \subset \mathcal{O}_L^\mathfrak{p}$, $a$ and $b$ are elements of $\mathcal{O}_{L^\mathfrak{p}}$. If $\mathfrak{P} \mid b$, then, since $\mathfrak{P} \mid (a^m - b^m)$, $\mathfrak{P} \mid a^m$. Since $\mathfrak{P}$ is prime, this implies that $\mathfrak{P} \mid a$. However, this contradicts the assumption that $(a, b) = 1$ in $\mathcal{O}_L$. We conclude that $\mathfrak{P} \nmid b$. Therefore, $b$ is a unit in $\mathcal{O}_{L^\mathfrak{p}}$, and so $\delta = a/b \in \mathcal{O}_{L^\mathfrak{p}}$. Let $E_{\mathfrak{P}}$ denote the residue class field of $\mathcal{O}_{L^\mathfrak{p}}$ and let $\eta_{\mathfrak{P}} : \mathcal{O}_{L^\mathfrak{p}} \to E_{\mathfrak{P}}$ denote the residue class field map with respect to $\mathfrak{P}$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Since $\mathfrak{P} \mid (a^m - b^m)$, $\eta_{\mathfrak{P}}(a^m - b^m) = 0$. Since $b$ is a unit in $O_{L_{\mathfrak{p}}}$, this implies that $\eta_{\mathfrak{P}}(a/b)^m = 1$. If $\eta_{\mathfrak{P}}(a/b)^s = 1$, for some positive integer $s$ less than $m$, then $\eta_{\mathfrak{P}}(a^s - b^s) = 0$. This means that $\mathfrak{P} \mid (a^s - b^s)$. But this contradicts the fact that $\mathfrak{P}$ is a primitive divisor of $a^m - b^m$. We conclude that the multiplicative order of $\eta_{\mathfrak{P}}(\delta)$ is equal to $m$.

Let $p = \mathfrak{P} \cap O_k$, let $F_p$ denote the residue class field of $O_{k_p}$, and let $\eta_p : O_{k_p} \to F_p$ denote the residue class field map with respect to $p$:

\[
\begin{array}{c|c|c|c|c|c|c}
\mathfrak{P} & O_L & L & L_{\mathfrak{p}} & L_{\mathfrak{p}} & O_{L_{\mathfrak{p}}} & E_{\mathfrak{p}} \\
p & O_k & k & k_{\mathfrak{p}} & k_{\mathfrak{p}} & O_{k_{\mathfrak{p}}} & F_p
\end{array}
\]

By construction, $p$ is a prime ideal of $O_k$ lying outside of $S$. Since $O_{k_p} = O_{L_{\mathfrak{p}}} \cap k_{\mathfrak{p}}$, $\delta \in O_{k_p}$. Moreover, since $\eta_p$ is the restriction of $\eta_{\mathfrak{P}}$ to $O_{k_p}$, the multiplicative order of $\eta_p(\delta)$ is equal to $m$.

**Corollary 2.4.** Let $m \in \mathbb{N}$. Let $k$ be a number field and let $\delta$ be a non-zero element of $k$ that is not a root of unity. Then there exist infinitely many prime ideals $p$ of $O_k$ such that $\delta \in O_{k_p}$ and the multiplicative order of the image of $\delta$ in the residue class field of $O_{k_p}$ is divisible by $m$.

**Proof.** This follows immediately from Theorem 2.3. □

**Corollary 2.5.** Let $R$ be a finitely generated ring in a number field $k$, let $\delta$ be a non-zero element of $R$ that is not a root of unity, and let $x_1, x_2, \ldots, x_j$ be non-zero elements of $R$. Then there exists a positive integer $n$ with the following property. For each integer $m \geq n$, there exist a finite field $F$ and a ring homomorphism $\eta : R \to F$ such that the multiplicative order of $\eta(\delta)$ is equal to $m$ and $\eta(x_i) \neq 0$, for each $1 \leq i \leq j$.

**Proof.** Fix a finite generating set $G$ of $R$. Let $S$ denote the finite set of prime ideals of $O_k$ which divide an element of $\{G, x_1, x_2, \ldots, x_j\}$. By Theorem 2.3 there exists a positive integer $n$ with the following property. For each integer $m \geq n$ there exists a non-zero prime ideal $p$ of $O_k$, lying outside of $S$, such that $\delta \in O_{k_p}$ and the multiplicative order of the image of $\delta$ in the residue class field of $O_{k_p}$ is equal to $m$. Fix $m \geq n$ and let $p \subset O_k$ be the corresponding prime ideal. Let $F$ denote the residue class field of $O_{k_p}$ and let $\eta : O_{k_p} \to F$ denote the residue class field map with respect to $p$. Since $p \notin S$, $R \in O_{k_p}$ and $x_1, x_2, \ldots, x_j$ are units in $O_{k_p}$. Therefore, the restriction of $\eta$ to $R$ satisfies the conclusion of the corollary. □

We conclude this section with a theorem that can be interpreted as a cyclic subgroup separability result for rings.

**Notation 2.6.** Given a number field $k$ and a non-zero prime ideal $p$ of $O_k$, let $\eta_p$ denote the residue class field map with respect to $p$.

**Theorem 2.7.** Let $k$ be a number field. Let $\lambda$ and $\omega$ be non-zero elements of $k$ such that $\lambda$ is not a multiplicative power of $\omega$. Let $P$ be a finite set of prime ideals of $O_k$. Then there exist primes $p$ and $q$, lying outside of $P$, such that $\lambda, \omega \in O_{k_p} \cap O_{k_q}$ and $(\eta_p \times \eta_q)(\lambda)$ is not a multiplicative power of $(\eta_p \times \eta_q)(\omega)$.

**Proof.** First assume that $\omega$ is a root of unity. Let $r$ be a natural number such that $\omega^r = 1$. Consider the set $X = \{\lambda^{-1} \omega - 1, \lambda^{-1} \omega^2 - 1, \ldots, \lambda^{-1} \omega^r - 1\}$. Since $\lambda$ is not a multiplicative power of $\omega$, each element of $X$ is non-zero. A non-zero element of
$k$ is a unit in $\mathcal{O}_k$ for all but finitely many prime ideals $p$ of $\mathcal{O}_k$. Therefore, there exists a prime ideal $p$ of $\mathcal{O}_k$, lying outside of $P$, such that $\lambda, \omega$ and each element of $X$ is a unit in $\mathcal{O}_k$. Thus, the image under $\eta_p$ of each element of $X$ is non-zero in the residue class field of $\mathcal{O}_k$. It follows that $\eta_p(\lambda)$ is not a multiplicative power of $\eta_p(\omega)$, as required.

For the remainder of the proof, we assume that $\omega$ is not a root of unity. Let $G$ be the subgroup of $k^* = k \setminus \{0\}$ generated by $\lambda$ and $\omega$. By assumption, $\omega$ has infinite order in $G$. Therefore, either $G$ is free abelian of rank 1 or 2, or $G \cong \mathbb{Z} \oplus \mathbb{Z}/a\mathbb{Z}$ for some integer $a > 1$.

**Case 1.** $G \cong \mathbb{Z}$.

Let $\delta$ be a generator of $G$. Write $\omega = \delta^m$ and $\lambda = \delta^n$, $m, n \in \mathbb{Z}$. Since $\lambda$ is not a multiplicative power of $\omega$, $m \nmid n$. By Corollary 2.4 there exist infinitely many prime ideals $p$ of $\mathcal{O}_k$ such that $\delta \in \mathcal{O}_k_p$ and the multiplicative order of $\eta_p(\delta)$ is divisible by $m$. Fix one such prime $p$ lying outside of $P$. If there exists an integer $x$ such that $\eta_p(\lambda) = \eta_p(\omega)^x$, then $\eta_p(\delta)^{m^2-n} = 1$. Hence $m | (mx - n)$, a contradiction. We conclude that $\eta_p(\lambda)$ is not a multiplicative power of $\eta_p(\omega)$. Therefore, $(\eta_p \times \eta_p)(\lambda)$ is not a multiplicative power of $(\eta_p \times \eta_p)(\omega)$.

**Case 2.** $G \cong \mathbb{Z} \oplus \mathbb{Z}$.

Note that, in this case, $\lambda$ is not a root of unity. We claim that $\lambda \in (k(\zeta_q))^q$ for at most finitely many primes $q \in \mathbb{Z}$. To see this, fix a prime $q$, let $s$ be the degree of $k(\zeta_q)$ over $k$, and let

$$N : k(\zeta_q) \to k$$

denote the norm map. Suppose $\lambda = u^q$, for some $u \in k(\zeta_q)$. Then $\lambda^s = N(\lambda) = N(u)^q$. Since $s \leq q - 1$, $s$ and $q$ are relatively prime. Therefore, there exist integers $x$ and $y$ such that $xq + y = 1$. This implies that $\lambda = N(u)^q \lambda^y \in k^s$. We conclude that if $\lambda \in k(\zeta_q)^q$, then $\lambda \in k^s$. Thus, it suffices to prove that $\lambda \in k^q$ for at most finitely many primes $q \in \mathbb{Z}$. Suppose there exists a non-zero prime ideal $p$ of $\mathcal{O}_k$ such that $\nu_p(\lambda) \neq 0$. Fix such a prime $p$, and set $m = \nu_p(\lambda)$. If there exists an element $y \in k$ such that $\lambda = y^q$, then $m = \nu_p(\lambda) = \nu_p(y^q) = q
\nu_p(y)$. Therefore, $\lambda \in k^q$ only if $q$ is a prime divisor of $m$. Now suppose that $\nu_p(\lambda) = 0$ for every non-zero prime ideal $p$ of $\mathcal{O}_k$. Then $\lambda$ is a unit in $\mathcal{O}_k$. By the Unit Theorem [11], there exist units $u_1, u_2, \ldots, u_r$ in $\mathcal{O}_k$ such that every unit in $\mathcal{O}_k$ can be uniquely expressed as

$$zu_1^{a_1}u_2^{a_2}\ldots u_r^{a_r},$$

where $z$ is a root of unity and $a_i \in \mathbb{Z}$. Write $\lambda = zu_1^{a_1}u_2^{a_2}\ldots u_r^{a_r}$. Since $\lambda$ is not a root of unity, $a_1 \neq 0$, for at least one $i$. For simplicity, assume that $a_1 \neq 0$. If there exists an element $y \in k$ such that $\lambda = y^q$, then $q \mid a_1$. Therefore, $\lambda \in k^q$ only if $q$ is a prime divisor of $a_1$. This proves the claim.

Let $S$ be the finite set of prime ideals of $\mathcal{O}_k$ dividing $\lambda$ or $\omega$, together with the infinite primes of $k$. Then if $p \not\in S$, both $\lambda$ and $\omega$ are units in $\mathcal{O}_k$. Let

$$U_S = \{ x \in k^* \mid \nu_p(x) = 0, \ \forall p \not\in S \}$$

denote the set of $S$-units of $k^*$. By the $S$-Unit Theorem [11], $U_S$ is a finitely generated abelian group. Let $t$ be the order of the torsion subgroup of $U_S/G$. Choose a prime $q \in \mathbb{Z}$ such that $q \nmid t$ and $\lambda \not\in k(\zeta_q)^s$, and set $K = k(\zeta_q)$. Let $s$ be the degree of $K$ over $k$ and let

$$N : K \to k$$
Denote the norm map. Let \( L \) be the splitting field of \( x^q - \lambda \) over \( K \). Since \( \lambda \notin K^q \), the polynomial \( x^q - \lambda \) is irreducible over \( K \). Hence \( L \) is a cyclic extension of \( K \) of degree \( q \). Let \( M \) be the splitting field of \( x^q - \omega \) over \( K \). Then either \( M = K \), or \( M \) is a cyclic extension of \( K \) of degree \( q \). Suppose that \( L = M \). Then by the classification of Kummer \( q \)-extensions, there exist an element \( v \in K \) and an integer \( r \), relatively prime to \( q \), such that \( \lambda = \omega^rv^q \). Thus \( \lambda^q = N(\lambda) = N(\omega^rv^q) = \omega^{rs}N(v)^q \), and so \( N(v)^q \in G \). If \( N(v) \in G \), then \( N(v) = \lambda^q = \omega^{rs} \), for some \( c \in \mathbb{Z} \). Hence \( \lambda^{s - q} = \omega^{rs + q} \). Since \( G \cong \mathbb{Z} \oplus \mathbb{Z} \), this implies that \( \lambda^{s - q} = id \). Thus \( s = q \), a contradiction since \( s < q \). Therefore, \( N(v) \) is an element of order \( q \) in \( U_S \). But this contradicts the fact that \( q \mid t \). We conclude that \( L \neq M \), and so \( L \cap M = K \). Therefore, the compositum \( LM \) is a Galois extension of \( K \) and the map 

\[
Gal(LM/K) \to Gal(L/K) \times Gal(M/K)
\]

\[
\gamma \to (\gamma|_L, \gamma|_M)
\]

is an isomorphism. Let \( \sigma \) be a generator of \( Gal(L/K) \), let \( \tau \) be the identity element of \( Gal(M/K) \), and consider \( (\sigma, \tau) \in Gal(LM/K) \).

By the Tchebotarev Density Theorem, there exist infinitely many primes \( p \) of \( K \) with unramified extension \( \mathfrak{P} \) in \( LM \) whose Frobenius automorphism is \( (\sigma, \tau) \). Fix one such prime \( p \) such that (i) \( O_K \cap \mathfrak{P} \) lies outside of \( S \cup P \), and (ii) the characteristic of the residue class field of \( O_K \) is not equal to \( q \). Since \( (\sigma, \tau) \) is the Frobenius automorphism of \( LM/K \) with respect to \( \mathfrak{P}/\mathfrak{p} \), \( Gal((LM)_{\mathfrak{P}}/K_{\mathfrak{p}}) = \langle (\sigma, \tau)^r \rangle \) where \( (\sigma, \tau)^r = (\sigma, \tau) \). Let \( \lambda^{1/q} \) be a root of \( x^q - \lambda \). Since \( \lambda^{1/q} \notin L \), \( (\sigma, \tau)(\lambda^{1/q}) = (\sigma, \tau)^r \). Since \( \lambda^{1/q} \notin K \) and \( Gal(L/K) \cong \langle \sigma \rangle \), \( \sigma(\lambda^{1/q}) \neq \lambda^{1/q} \). We conclude that \( \sigma(\lambda^{1/q}) \neq \lambda^{1/q} \) and thus that \( \lambda^{1/q} \notin K_{\mathfrak{p}} \). Hence the polynomial \( x^q - \lambda \) is irreducible over \( K_{\mathfrak{p}} \). Similarly, \( (\sigma, \tau)(\omega^{1/q}) = (\sigma, \tau)(\omega^{1/q}) = \tau(\omega^{1/q}) = \omega^{1/q} \), and thus \( \omega^{1/q} \in K_{\mathfrak{p}} \). By our choice of \( \mathfrak{p}, \omega \) and \( \lambda \) are units in \( O_K \). Hence \( \omega^{1/q} \in O_K \), meaning that \( \omega \in O_{K^q} \). Let \( F \) denote the residue class field of \( O_K \), and let \( \phi: O_K \to F \)

denote the residue class field map. Since \( \lambda \) is a unit in \( O_K \), \( \phi(\lambda) \neq 0 \). Therefore, since the characteristic of \( F \) is not equal to \( q \), the polynomial \( x^q - \phi(\lambda) \) has no multiple roots in \( F \). Hensel’s Lemma then implies that \( x^q - \phi(\lambda) \) is irreducible over \( F \). It follows that \( \phi(\lambda) \notin F^q \). However, since \( \omega \in O_{K^q} \), \( \phi(\omega) = F^q \). We conclude that \( \phi(\lambda) \) is not a multiplicative power of \( \phi(\omega) \). Let \( q = \mathfrak{p} \cap O_{K^q} \). Since \( \eta_q \) and \( \phi \) agree on \( O_{K^q} \), \( \eta_q(\lambda) \) is not a multiplicative power of \( \eta_q(\omega) \). Therefore, \( (\eta_q \times \eta_q)(\lambda) \) is not a multiplicative power of \( (\eta_q \times \eta_q)(\omega) \).

Case 3. \( G \cong \mathbb{Z} \oplus \mathbb{Z}/a\mathbb{Z} \), for some integer \( a > 1 \).

Choose integers \( c \) and \( d \) such that \( \alpha = \lambda^c \omega^d \) has order \( a \) in \( G \). We claim that there exist primes \( \mathfrak{p} \) and \( q \) lying outside of \( P \cup S \) such that \( (\eta_\mathfrak{p} \times \eta_q)(\alpha) \) is not a multiplicative power of \( (\eta_\mathfrak{p} \times \eta_q)(\omega) \). If there exists a prime \( \mathfrak{p} \notin (P \cup S) \) such that \( \eta_\mathfrak{p}(\alpha) \) is not a multiplicative power of \( \eta_\mathfrak{p}(\omega) \), then the claim follows. Therefore, we assume that for every prime \( \mathfrak{p} \notin (P \cup S) \), \( \eta_\mathfrak{p}(\alpha) \) is a multiplicative power of \( \eta_\mathfrak{p}(\omega) \). Fix a prime \( \mathfrak{p} \notin (P \cup S) \) such that \( \eta_\mathfrak{p}(\alpha) \neq id \). By assumption, there exists an integer \( s_1 \) such that \( \eta_\mathfrak{p}(\alpha) = \eta_\mathfrak{p}(\omega)^{s_1} \). Let \( o_1 \) denote the multiplicative order of \( \eta_\mathfrak{p}(\omega) \). Since \( \eta_\mathfrak{p}(\alpha) \neq id \), \( o_1 \mid s_1 \). Thus there is a positive integer \( r \) such that \( r \mid o_1 \), but \( r \nmid s_1 \). By Corollary, there exist infinitely many prime ideals \( \mathfrak{q} \) of \( O_K \) such that \( \omega \in O_{K_{\mathfrak{q}}} \) and the multiplicative order of \( \eta_q(\omega) \) is divisible by \( ar \). Fix one such prime \( \mathfrak{q} \) lying
outside of \( P \cup S \). Let \( s_2 \) be the integer such that \( \eta_q(\alpha) = \eta_q(\omega)^{s_2} \), and let \( o_2 \) be the multiplicative order of \( \eta_q(\omega) \). Suppose that \( (\eta_p \times \eta_q)(\alpha) = (\eta_p \times \eta_q)(\omega)^s \), for some integer \( s \). Then
\[
\eta_p(\alpha) = \eta_p(\omega)^s, \quad \text{and} \quad \eta_q(\alpha) = \eta_q(\omega)^s
\]
\[
\implies s \equiv s_1 \mod o_1, \quad \text{and} \quad s \equiv s_2 \mod o_2
\]
\[
\implies s = s_1 + o_1n_1 = s_2 + o_2n_2, \quad \text{for some} \quad n_1, n_2 \in \mathbb{Z}
\]
\((*)\)

Since \( \eta_q(\omega)^{as_2} = \eta_q(\alpha)^a = \text{id}, \quad o_2 \mid as_2 \). By our choice of \( q \), \( ar \mid o_2 \). It follows that \( r \mid s_2 \). We have established that \( r \) divides \( o_1, o_2, \) and \( s_2 \). Therefore, by equation \((*)\), \( r \) divides \( s_1 \), a contradiction. We conclude that \((\eta_p \times \eta_q)(\alpha)\) is not a multiplicative power of \((\eta_p \times \eta_q)(\omega)\), as claimed. If \((\eta_p \times \eta_q)(\lambda) = (\eta_p \times \eta_q)(\omega)^s\), for some integer \( x \), then \((\eta_p \times \eta_q)(\alpha) = (\eta_p \times \eta_q)(\omega)^{sx+d}\), a contradiction. Hence \((\eta_p \times \eta_q)(\lambda)\) is not a multiplicative power of \((\eta_p \times \eta_q)(\omega)\).

As an immediate corollary we have:

**Corollary 2.8.** Let \( R \) be a finitely generated ring in a number field \( k \). Let \( \lambda \) and \( \omega \) be non-zero elements of \( R \) such that \( \lambda \) is not a multiplicative power of \( \omega \). Then there exist a finite ring \( S \) and a ring homomorphism \( \eta : R \rightarrow S \) such that \( \eta(\lambda) \) is not a multiplicative power of \( \eta(\omega) \).

**Proof.** By Theorem 2.7, there exist two infinite collections of prime ideals, \( P \) and \( Q \), such that for each \( p \in P \) and \( q \in Q \):

1. \( \lambda, \omega \in \mathcal{O}_{k_p} \cap \mathcal{O}_{k_q} \); and
2. \( (\eta_p \times \eta_q)(\lambda) \) is not a multiplicative power of \((\eta_p \times \eta_q)(\omega)\).

Each element of \( k \) is contained in \( \mathcal{O}_{k_p} \) for all but finitely many prime ideals \( p \) of \( \mathcal{O}_k \). Therefore, since \( R \) is finitely generated, we may choose primes \( p \in P \) and \( q \in Q \) such that \( R \subset \mathcal{O}_{k_p} \cap \mathcal{O}_{k_q} \). Let \( F_p \) and \( F_q \) denote the residue class fields of \( \mathcal{O}_{k_p} \) and \( \mathcal{O}_{k_q} \), respectively. Then the finite ring \( S = F_p \times F_q \) and the composition
\[
R \xrightarrow{\eta} \mathcal{O}_{k_p} \cap \mathcal{O}_{k_q} \xrightarrow{\eta_p \times \eta_q} F_p \times F_q
\]
satisfy the conclusion of the lemma. \( \square \)

### 3. Subgroup separability of linear groups

In this section we apply the results of section 2 to prove theorems about separability of linear groups and free products with amalgamation of linear groups.

**Theorem 3.1.** Let \( \Gamma \) be a finitely generated subgroup of \( SL(2, \mathbb{C}) \) whose traces consist of algebraic numbers. Let \( h \) be an element of \( \Gamma \) such that \( tr^2(h) \neq 4 \). Then the cyclic subgroup of \( \Gamma \) generated by \( h \) is separable in \( \Gamma \).

**Remark 3.2.** If \( \Gamma \) is a discrete subgroup of \( SL(2, \mathbb{C}) \), then this follows from Theorem 1 of [1].

**Proof.** Fix \( \Gamma \) and \( h \) as above. Let \( \mathbb{Q}(tr \Gamma) \) denote the field obtained by adjoining the traces of the elements of \( \Gamma \) to \( \mathbb{Q} \). Since \( \Gamma \) is finitely generated and the traces of \( \Gamma \) consist of algebraic numbers, \( \mathbb{Q}(tr \Gamma) \) is a number field. By Proposition 2.4(e) of [3], we may conjugate \( \Gamma \) in \( GL(2, \mathbb{C}) \) to lie in a finite field extension of \( \mathbb{Q}(tr \Gamma) \). Therefore, we view \( \Gamma \subset SL(2, k) \), for some number field \( k \). Let \( L \) be the field
obtained by adjoining the eigenvalues of $h$ to $k$. Since the eigenvalues of $h$
are algebraic numbers, $L$ is a number field. The element $h$ is diagonalizable over $L$.
Therefore, after conjugating $\Gamma$ in $GL(2, L)$, we may assume that

$$\Gamma \subset SL(2, L) \text{ and } h = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \text{ for some } \omega \in \mathbb{C}.$$

Let $R$ be the ring generated by the coefficients of the generators of $\Gamma$ over $\mathbb{Z}$. Then
$\Gamma \subset SL(2, R) \subset SL(2, L)$. 

Let $H = \langle h \rangle$ and let $A$ be the maximal abelian subgroup of $\Gamma$ containing $h$.
Since $\Gamma$ is a finitely generated subgroup of $GL(2, \mathbb{C})$, it is residually finite \cite{2}. By
Proposition 1 of \cite{12}, a maximal abelian subgroup of a residually finite group is
separable. Therefore, $A$ is a separable subgroup of $\Gamma$. Let $g$ be an element of $\Gamma \setminus H$.
If $g \notin A$, then, since $A$ is separable, there exists a subgroup $K$ of finite index in $\Gamma$
that contains $H$ but not $g$. Therefore, we assume $g \in A \setminus H$. This implies that

$$g = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \text{ for some } \lambda \in \mathbb{C}.$$ 

Since $g \notin H$, $\lambda$ is not a multiplicative power of $\omega$. Therefore, by Corollary 2.5
there exist a finite ring $S$ and a ring homomorphism $\eta : R \rightarrow S$ such that $\eta(\lambda)$ is
not a multiplicative power of $\eta(\omega)$. This ring homomorphism induces a group homomorphism
$\psi : SL(2, R) \rightarrow SL(2, S)$. Let $N$ denote the kernel of the composition

$$\phi : \Gamma \xrightarrow{\eta} SL(2, R) \xrightarrow{\psi} SL(2, S).$$

Since $SL(2, S)$ is a finite group, $K = HN$ is a subgroup of finite index in $\Gamma$ containing $H$. Since $\eta(\lambda)$ is not a multiplicative power of $\eta(\omega)$, $g \notin K$. \hfill $\Box$

**Theorem 3.3.** Let $\Gamma_1$ and $\Gamma_2$ be finitely generated subgroups of $SL(2, \mathbb{C})$, whose
traces consist of algebraic numbers. Let $\gamma_1$ and $\gamma_2$ be elements of infinite order
in $\Gamma_1$ and $\Gamma_2$, respectively, such that $tr^2(\gamma_1) \neq 4$ and $tr^2(\gamma_2) \neq 4$. Suppose that
$\{g \in \Gamma_1 \mid g\gamma_1 = \gamma_1 g\} = \langle \gamma_1 \rangle$ and $\{g \in \Gamma_2 \mid g\gamma_2 = \gamma_2 g\} = \langle \gamma_2 \rangle$. Let

$$\Gamma = \Gamma_1 \ast \Gamma_2$$

be the free product with amalgamation obtained by identifying $\gamma_1$ with $\gamma_2$. If $H$ is a
separable subgroup of $\Gamma_1$, then $H$ is a separable subgroup of $\Gamma$.

**Proof.** As in the proof of Theorem 4.1 we may view $\Gamma_1$ and $\Gamma_2$ in $SL(2, L)$, where
$L$ is a number field containing the eigenvalues of $\gamma_1$ and $\gamma_2$. After conjugating $\Gamma_1$
and $\Gamma_2$ (individually) in $SL(2, L)$, we may assume that

$$\gamma_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^{-1} \end{pmatrix} \text{ and } \gamma_2 = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2^{-1} \end{pmatrix}, \text{ for some } \lambda_1, \lambda_2 \in L.$$ 

Since $\gamma_1$ and $\gamma_2$ have infinite order, $\lambda_1$ and $\lambda_2$ are not roots of unity. Let $R$ denote
the ring generated by the coefficients of the generators of $\Gamma_1$ and $\Gamma_2$ over $\mathbb{Z}$. Then
$\Gamma_1, \Gamma_2 \subset SL(2, R) \subset SL(2, L)$.

Let $H \subset \Gamma_1$ be given and let $g \in \Gamma \setminus H$.

**Case 1.** $g \in \Gamma_1$.

By assumption, $H$ is a separable subgroup of $\Gamma_1$. Therefore, there exists a
subgroup $K_1$ of finite index in $\Gamma_1$ containing $H$ but not $g$. The subgroup $K_1$
contains a normal subgroup $N_1$ of finite index in $\Gamma_1$. Let $\pi$ denote the quotient
map from $\Gamma_1$ onto $\Gamma_1/N_1$. Then $\pi(g) \notin \pi(H)$. Let $n$ be the order of $\pi(\gamma_1)$. By Corollary 2.5, there exist a positive integer $m$ divisible by $n$, finite fields $S$ and $T$, and ring homomorphisms $\rho_1 : R \to S$ and $\rho_2 : R \to T$ such that the multiplicative orders of $\rho_1(\lambda_1)$ and $\rho_2(\lambda_2)$ are equal to $m$. These ring homomorphisms induce group homomorphisms

$$\phi_1 : \Gamma_1 \subset \text{SL}(2, R) \to \text{SL}(2, S) \quad \text{and}$$

$$\phi_2 : \Gamma_2 \subset \text{SL}(2, R) \to \text{SL}(2, T)$$

such that the orders of $\phi_1(\gamma_1)$ and $\phi_2(\gamma_2)$ are equal to $m$. Let $G_1 = \Gamma_1/N_1 \times \text{SL}(2, S)$, $G_2 = \text{SL}(2, T)$, and $\phi_1' : \pi \times \phi_1 : \Gamma_1 \to G_1$. Note that $\phi_1'(g) \notin \phi_1'(H)$ and the order of $\phi_1'(\gamma_1)$ is equal to $m$. Let

$$G = G_1 \ast_{\mathbb{Z}/m\mathbb{Z}} G_2$$

be the free product with amalgamation obtained by identifying $\phi_1'(\gamma_1)$ with $\phi_2(\gamma_2)$. By the universal property of free products with amalgamation, there exists a group homomorphism $\eta : \Gamma \to G$ such that $\eta$ restricted to $\Gamma_1$ is equal to $\phi_1'$. Hence $\eta(g) \notin \eta(H)$.

By the proof of Theorem 2 of [5], the free product with amalgamation of two finite groups contains a subgroup of finite index that is free. Since free groups are subgroup separable [8] and finite extensions of subgroup separable groups are subgroup separable [19], this implies that $G$ is subgroup separable. Therefore, there exists a finite group $F$ and a group homomorphism $\psi : G \to F$ such that $\psi(\eta(g)) \notin \psi(\eta(H))$. Let $K$ be the kernel of the composition $\psi \eta$. Then $KH$ is a subgroup of finite index in $\Gamma$ that contains $H$ but not $g$.

**Case 2.** $g \notin \Gamma_1$.

Express $g$ in normal form. Suppose that

$$g = a_1b_1a_2b_2 \ldots a_nb_n c,$$

$$a_i \in \Gamma_1 \setminus \langle \gamma_1 \rangle, \quad b_i \in \Gamma_2 \setminus \langle \gamma_2 \rangle, \quad c \in \langle \gamma_1 \rangle.$$

Write

$$a_i = \begin{pmatrix} w_i & x_i \\ y_i & z_i \end{pmatrix}, \quad b_i = \begin{pmatrix} r_i & s_i \\ t_i & u_i \end{pmatrix},$$

for some $w, x, y, z, r, s, t, u \in L$. Since $a_i \notin \langle \gamma_1 \rangle$ and $\{g \in \Gamma_1 \mid g\gamma_1 = \gamma_1 g\} = \langle \gamma_1 \rangle$, $a_i$ and $\gamma_1$ do not commute. It follows that either $x_i \neq 0$ or $y_i \neq 0$. After relabeling, if necessary, we assume that $x_i \neq 0$ for each $1 \leq i \leq n$. Similarly, we may assume that $s_i \neq 0$ for each $1 \leq i \leq n$.

By Corollary 2.5, there exist a positive integer $m$, finite fields $S$ and $T$, and ring homomorphisms $\rho_1 : R \to S$ and $\rho_2 : R \to T$ such that (i) $\rho_1(x_i) \neq 0$ for all $1 \leq i \leq n$, (ii) $\rho_2(s_i) \neq 0$ for all $1 \leq i \leq n$, and (iii) the multiplicative orders of $\rho_1(\lambda_1)$ and $\rho_2(\lambda_2)$ are equal to $m$. These ring homomorphisms induce group homomorphisms

$$\phi_1 : \Gamma_1 \subset \text{SL}(2, R) \to \text{SL}(2, S), \quad \text{and}$$

$$\phi_2 : \Gamma_2 \subset \text{SL}(2, R) \to \text{SL}(2, T),$$

such that (i) $\phi_1(a_i) \notin \langle \phi_1(\gamma_1) \rangle$ for all $1 \leq i \leq n$, (ii) $\phi_2(b_i) \notin \langle \phi_2(\gamma_2) \rangle$ for all $1 \leq i \leq n$, and (iii) the orders of $\phi_1(\gamma_1)$ and $\phi_2(\gamma_2)$ are equal to $m$. 
Set \( G_1 = \text{SL}(2, S) \) and \( G_2 = \text{SL}(2, T) \), and let
\[
G = G_1 \ast_{\mathbb{Z}/m\mathbb{Z}} G_2
\]
be the free product with amalgamation obtained by identifying \( \phi_1(\gamma_1) \) with \( \phi_2(\gamma_2) \). By the universal property of free products with amalgamation, there exists a group homomorphism \( \eta : \Gamma \to G \) that extends both \( \phi_1 \) and \( \phi_2 \). Since \( \phi_1(a_i) \notin \langle \phi_1(\gamma_1) \rangle \) for all \( 1 \leq i \leq n \), and \( \phi_2(b_i) \notin \langle \phi_2(\gamma_2) \rangle \) for all \( 1 \leq i \leq n \), \( \eta(g) \notin G_1 \). In particular, \( \eta(g) \notin \eta(H) \). As mentioned above, the free product with amalgamation of two finite groups is subgroup separable. Therefore, there exist a finite group \( F \) and a group homomorphism \( \psi : G \to F \) such that \( \psi(\eta(g)) \notin \psi(\eta(H)) \). Let \( K \) be the kernel of the composition \( \psi \eta \). Then \( HK \) is a subgroup of finite index in \( \Gamma \) that contains \( H \) but not \( g \).

This completes the proof in this case where \( g \) is of the form \( a_1b_1a_2b_2 \ldots a_nb_nc \). There are other possible cases for the normal form of \( g \). For example, \( g \) could be of the form \( b_2a_2b_2 \ldots a_nb_nc \). The proof in each case is similar to the proof above. The important point is that, since \( g \notin \Gamma_1 \), there is a letter \( b_i \) in the normal form of \( g \). Hence, we can construct \( \eta \) such that \( \eta(g) \notin \eta(H) \).

Since finitely generated subgroups of \( \text{SL}(2, \mathbb{C}) \) are residually finite [2], Theorem 3.3 implies the following.

**Corollary 3.4.** The group \( \Gamma \), as defined in Theorem 3.3, is residually finite.

4. **Applications to hyperbolic 3-manifold groups**

In this section we apply the results of sections 2 and 3 to subgroup separability of free products with amalgamation of hyperbolic 3-manifold groups. We begin by recalling some basic notions. For reference, see [4] or [11].

**Notation 4.1.**

1. A (complete) hyperbolic 3-orbifold is the quotient space \( M = \mathbb{H}^3/\Gamma \), where \( \mathbb{H}^3 \) denotes hyperbolic 3-space, and \( \Gamma \) is a discrete group of isometries of \( \mathbb{H}^3 \). If \( \Gamma \) is torsion free, then \( M = \mathbb{H}^3/\Gamma \) is a hyperbolic 3-manifold with fundamental group \( \Gamma \). \( M \) is orientable if \( \Gamma \) consists of orientation preserving isometries. The group of orientation preserving isometries of \( \mathbb{H}^3 \) can be identified with \( \text{PSL}(2, \mathbb{C}) \). Two orientable, hyperbolic 3-orbifolds \( \mathbb{H}^3/\Gamma, \mathbb{H}^3/\Gamma' \) are isometric by an orientation-preserving isometry (and will be identified) if and only if \( \Gamma \) and \( \Gamma' \) are conjugate in \( \text{PSL}(2, \mathbb{C}) \). Thus to an orientable, hyperbolic 3-orbifold \( M = \mathbb{H}^3/\Gamma \) we can associate a discrete, faithful representation from \( \Gamma \) into \( \text{PSL}(2, \mathbb{C}) \), which is well defined up to conjugation. By fixing such a representation, we view \( \Gamma \) as a discrete subgroup of \( \text{PSL}(2, \mathbb{C}) \).

2. Let \( M = \mathbb{H}^3/\Gamma \) be an orientable, hyperbolic 3-orbifold. We say an element \( g \in \Gamma \) is loxodromic if \( g \) is conjugate in \( \text{PSL}(2, \mathbb{C}) \) to a matrix of the form
\[
\pm \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \ |\lambda| \neq 1.
\]

We first state a result that was motivated by the following question. Let \( M_1 \) and \( M_2 \) be compact orientable 3-manifolds with non-empty boundary whose interiors admit complete hyperbolic structures of finite volume. Fix boundary components \( T_1 \in \partial M_1 \) and \( T_2 \in \partial M_2 \), and let \( f : T_1 \to T_2 \) be a homeomorphism. Let \( M \) be the manifold obtained by identifying \( M_1 \) and \( M_2 \) along the fixed boundary components...
Theorem 4.2. Let $M_1$ and $M_2$ be compact orientable 3-manifolds with non-empty boundary whose interiors admit complete hyperbolic structures of finite volume. Fix boundary components $T_1 \in \partial M_1$ and $T_2 \in \partial M_2$, and let $f : T_1 \to T_2$ be a homeomorphism. Let $M$ be the manifold obtained by identifying $M_1$ and $M_2$ along the fixed boundary components via $f$. If $\alpha \in \pi_1(M_1)$ and $\beta \in \pi_2(M_2)$ are loxodromic elements, then $\langle \alpha, \beta \rangle$ is a separable subgroup of $\pi_1(M)$.

Theorem 4.2 involves subgroup separability of free products with $\mathbb{Z} \oplus \mathbb{Z}$ amalgamation of two hyperbolic 3-manifold groups. We now consider free products with $\mathbb{Z}$ amalgamation. There are interesting results on this subject in the literature. For example, in [6] it is shown that the free product with $\mathbb{Z}$ amalgamation of two free groups is subgroup separable. A similar statement is true for two finitely generated Fuchsian groups [13]. Free groups and finitely generated Fuchsian groups are subgroup separable [8], [18]. Therefore, given these examples, one might expect that the free product with $\mathbb{Z}$ amalgamation of two subgroup separable groups is subgroup separable. However, this is not the case in general. Explicit examples are constructed in [13]. Little is known about subgroup separability of free products with $\mathbb{Z}$ amalgamation of two hyperbolic 3-orbifold groups. But we can say the following.

Theorem 4.3. Let $M_1 = \mathbb{H}^3/\Gamma_1$ and let $M_2 = \mathbb{H}^3/\Gamma_2$ be hyperbolic 3-orbifolds of finite volume, and let $\gamma_1$ and $\gamma_2$ be primitive loxodromic elements of $\Gamma_1$ and $\Gamma_2$, respectively. Let

$$\Gamma = \Gamma_1 \ast_2 \Gamma_2$$

be the free product with amalgamation obtained by identifying $\gamma_1$ with $\gamma_2$. If $H$ is a separable subgroup of $\Gamma_1$, then $H$ is a separable subgroup of $\Gamma$. In particular, $\Gamma$ is residually finite.

Proof. The identity representations $\Gamma_1 \to \text{PSL}(2, \mathbb{C})$ and $\Gamma_2 \to \text{PSL}(2, \mathbb{C})$ may be lifted to representations in $\text{SL}(2, \mathbb{C})$ [7]. Therefore, we view $\Gamma_1$ and $\Gamma_2$ as a discrete subgroups of $\text{SL}(2, \mathbb{C})$. Since $M_1$ and $M_2$ have finite volume, $\Gamma_1$ and $\Gamma_2$ are finitely generated. Moreover, by Mostow Rigidity, the traces of $\Gamma_1$ and $\Gamma_2$ consist of algebraic numbers [20]. By assumption, $\gamma_1$ and $\gamma_2$ are elements of infinite order such that $\text{tr}^2(\gamma_1) \neq 4$ and $\text{tr}^2(\gamma_2) \neq 4$. Since $\gamma_1$ and $\gamma_2$ are primitive loxodromic elements and $\Gamma_1$ and $\Gamma_2$ are discrete groups, $\{g \in \Gamma_1 | g\gamma_1 = \gamma_1g\} = \langle \gamma_1 \rangle$ and $\{g \in \Gamma_2 | g\gamma_2 = \gamma_2g\} = \langle \gamma_2 \rangle$. The result then follows from Theorem 4.3 of section 3.

If $M_1 = \mathbb{H}^3/\Gamma_1$ is a hyperbolic 3-orbifold, with $\Gamma$ finitely generated, then abelian subgroups of $\Gamma_1$ are separable in $\Gamma_1$ [1]. Therefore, Theorem 4.3 implies:

Corollary 4.4. Let $M_1 = \mathbb{H}^3/\Gamma_1$ and $M_2 = \mathbb{H}^3/\Gamma_2$ be hyperbolic 3-orbifolds of finite volume, and let $\gamma_1$ and $\gamma_2$ be primitive loxodromic elements of $\Gamma_1$ and $\Gamma_2$, respectively. Let

$$\Gamma = \Gamma_1 \ast_2 \Gamma_2$$
be the free product with amalgamation obtained by identifying $\gamma_1$ with $\gamma_2$. Then abelian subgroups of $\Gamma_1$ are separable in $\Gamma$.

This completes the section on applications to hyperbolic manifolds. However, one could use the techniques developed in this paper to analyze separability of more general subgroups of free products with $\mathbb{Z}$ or $\mathbb{Z} \oplus \mathbb{Z}$ amalgamation of two hyperbolic 3-manifold groups.

ACKNOWLEDGMENT

I thank Jonathan Sands and Farshid Hajir for assistance with number theory. In particular, Sands provided key ideas in the proof of Case 2 of Theorem 2.7 and Hajir helped clarify a point in the proof of Theorem 2.3.

REFERENCES


DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EMORY UNIVERSITY, ATLANTA, GEORGIA 30322