

NON-NORMAL, STANDARD SUBGROUPS OF THE BIANCHI GROUPS

A. W. MASON AND R. W. K. ODONI

(Communicated by Ronald M. Solomon)

ABSTRACT. Let S be a subgroup of $SL_n(K)$, where K is a Dedekind ring, and let \mathfrak{q} be the K -ideal generated by $x_{ij}, x_{ii} - x_{jj}$ ($i \neq j$), where $(x_{ij}) \in S$. The subgroup S is called *standard* iff S contains the normal subgroup of $SL_n(K)$ generated by the \mathfrak{q} -elementary matrices. It is known that, when $n \geq 3$, S is standard iff S is normal in $SL_n(K)$. It is also known that every standard subgroup of $SL_2(K)$ is normal in $SL_2(K)$ when K is an arithmetic Dedekind domain with infinitely many units.

The ring of integers of an imaginary quadratic number field, \mathcal{O} , is one example (of three) of such an arithmetic domain with finitely many units. In this paper it is proved that every *Bianchi group* $SL_2(\mathcal{O})$ has uncountably many non-normal, standard subgroups. This result is already known for related groups like $SL_2(\mathbb{Z})$.

INTRODUCTION

Let R be a commutative ring, and let \mathfrak{q} be an R -ideal. We put $SL_n(R, \mathfrak{q}) = \text{Ker}(SL_n(R) \rightarrow SL_n(R/\mathfrak{q}))$, where $n \geq 2$. Let $U_n(R, \mathfrak{q})$ (resp. $NE_n(R, \mathfrak{q})$) be the subgroup (resp. normal subgroup) of $SL_n(R)$ generated by the unipotent (resp. elementary) matrices in $SL_n(R, \mathfrak{q})$. It is clear that $NE_n(R, \mathfrak{q})$ is a subgroup of $U_n(R, \mathfrak{q})$. We put $U_n(R, R) = U_n(R)$ and $NE_n(R, R) = NE_n(R)$. By definition we have $SL_n(R, R) = SL_n(R)$.

Let $\mathcal{O} (= \mathcal{O}_d)$ be the ring of integers of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$, where \mathbb{Q} is the set of rational numbers and d is a square-free positive integer. In this paper we prove the following result for the *Bianchi groups*, $SL_2(\mathcal{O})$.

Theorem. *For infinitely many \mathcal{O} -ideals \mathfrak{q} , $SL_2(\mathcal{O}, \mathfrak{q})/U_2(\mathcal{O}, \mathfrak{q})$ (and hence $SL_2(\mathcal{O}, \mathfrak{q})/NE_2(\mathcal{O}, \mathfrak{q})$) has a free, non-cyclic quotient.*

Our proof is based on the fundamental paper [16] of Zimmert. Central to Zimmert's approach is a special finite subset of \mathbb{N} , the set of positive integers, determined by \mathcal{O} , which is now usually referred to as the *Zimmert set*. In this paper we apply some elementary analytic number theory to the Zimmert set and then make use of a previous result [11, Theorem 4.9] of the first author.

Within the context of the class of linear groups $SL_n(A)$, where A is a *Dedekind ring of arithmetic type* [1, p. 83], our theorem represents a two-dimensional anomaly. In a celebrated paper Bass, Milnor and Serre [1, Corollary 4.3, p. 95] have proved

Received by the editors September 25, 1994.

1991 *Mathematics Subject Classification*. Primary 20H10, 11F06; Secondary 11A25, 20E05.

©1996 American Mathematical Society

that, when $n \geq 3$, the quotient group $SL_n(A, \mathfrak{q})/NE_n(A, \mathfrak{q})$ is always finite, cyclic. Liehl [4] and Vaserstein [15] have proved that this is also true for $n = 2$, provided A^* , the set of units of A , is infinite. By a classical theorem of Dirichlet, A^* is finite if and only if (i) $A = \mathcal{O}$, (ii) $A = \mathbb{Z}$, the ring of rational integers, or (iii) $A = \mathcal{C} = \mathcal{C}(C, P, k)$, the coordinate ring of the affine curve obtained by remaining a closed point P from a (suitable) projective curve C over a *finite* field k . (The simplest case of type (iii) is the polynomial ring $k[t]$.) When $A = \mathbb{Z}$ or \mathcal{C} , it is known ([9, Lemma 3.5], [7, Corollary 2.6]) that $SL_2(A, \mathfrak{q})/U_2(A, \mathfrak{q})$ has a free, non-cyclic quotient, for all but finitely many \mathfrak{q} . (Note that, as \mathbb{Z} is a principal ideal domain, $NE_2(\mathbb{Z}, \mathfrak{q}) = U_2(\mathbb{Z}, \mathfrak{q})$, for all \mathfrak{q} .)

An immediate consequence of our theorem represents another two-dimensional anomaly. A subgroup S of $SL_n(R)$ is called *standard* if and only if $NE_n(R, \mathfrak{q}_0) \leq S$, where \mathfrak{q}_0 is the R -ideal generated by $x_{ij}, x_{ii} - x_{jj}$ ($i \neq j$), for all $(x_{ij}) \in S$. Let K be a Dedekind ring (or, more generally, a Noetherian domain of Krull dimension 1). Then, by [1, Theorems 7.4, 7.5(e), p. 106] and [5, Theorem 3.2], when $n \geq 3$, a subgroup S of $SL_n(K)$ is standard if and only if S is normal in $SL_n(K)$. It is also known [6, Corollary 1.3] that every standard subgroup of $SL_2(A)$ is normal, provided A^* is infinite. The following result shows that, when A^* is finite, this situation is completely different.

Corollary. $SL_2(\mathcal{O})$ has uncountably many non-normal, standard subgroups.

This result is already known for $A = \mathcal{C}$ [7, Theorem 3.2] and for $A = \mathbb{Z}$ [8, Theorem 3].

A weaker version (in the other direction) of the above classification theorem of normal subgroups of $SL_n(K)$ says that, when $n \geq 3$, every non-central normal subgroup of $SL_n(K)$ contains $NE_n(K, \mathfrak{q}')$, for some *non-zero* K -ideal, \mathfrak{q}' . A non-central, normal subgroup N of $SL_2(K)$ is called a *normal subgroup of level zero* if and only if $NE_2(K, \mathfrak{q}) \leq N$ *only* when $\mathfrak{q} = \{0\}$. Serre [14, Proposition 2, p. 492] has proved that, when A^* is infinite, $SL_2(A)$ has no normal subgroups of level zero. Again the situation is completely different when A^* is finite. When $A = \mathbb{Z}, \mathcal{O}$ or \mathcal{C} , it is known that $SL_2(A)$ has uncountably many normal subgroups of level zero. (See [8, Theorem 1], [10, Theorem 4], [7, Theorem 3.1].)

1. ZIMMERT SETS

Let D be the discriminant of $\mathbb{Q}(\sqrt{-d})$. It is well known that $D = -4d$, unless $d \equiv 3 \pmod{4}$, in which case $D = -d$. Let

$$\omega = \begin{cases} \sqrt{-d}, & d \equiv 1, 2 \pmod{4}, \\ (1 + \sqrt{-d})/2, & d \equiv 3 \pmod{4}. \end{cases}$$

For each $m \in \mathbb{N}$ let \mathcal{O}_m be the order of index m in \mathcal{O} . It is known that

$$\mathcal{O}_m = \mathbb{Z} + m\omega\mathbb{Z}.$$

(By definition, $\mathcal{O}_1 = \mathcal{O}$.)

Definition. For each d, m the *Zimmert set* $Z(d, m)$ is the set of all $n \in \mathbb{N}$ such that

- (i) $4n^2 \leq m^2|D| - 3$.
- (ii) $(|a + m\omega|^2, n) = 1$, for all $a \in \mathbb{Z}$.
- (iii) $n \neq 2$.

(It is clear that $Z(d, m) \neq \emptyset$ iff $m^2|D| \geq 7$.) The original definition (for the case $m = 1$ only) is due to Zimmert [16]. The extended definition is due to Grunewald and Schwermer [3]. The principal purpose of Zimmert's paper [16, Satz 1(i)] is to prove that $SL_2(\mathcal{O})$ has a free quotient of rank $|Z(d, 1)|$ and this result is extended [3] (without too much difficulty) to $SL_2(\mathcal{O}_m)$ by Grunewald and Schwermer.

Notation. Let $r(d, m) = |Z(d, m)|$.

Theorem 1. For each d there exists $m_0 = m_0(d)$ such that, when $m > m_0$,

$$r(d, m) > \frac{9}{20} \frac{M}{\ln M} - \frac{\ln m}{\ln 2},$$

where $M = \frac{1}{2}\sqrt{(m^2|D| - 3)}$.

Proof. For each odd prime p and integer a , let

$$\left(\frac{a}{p}\right)$$

denote the Legendre symbol.

Let $Z^*(d, m)$ be the set of odd primes p such that

- (i) $4p^2 \leq m^2|D| - 3$.
- (ii) $(p, dm) = 1$.
- (iii) $\left(\frac{-d}{p}\right) = -1$.

It is clear that $Z^*(d, m) \subseteq Z(d, m)$. Let $r^* = |Z^*(d, m)|$. Now

$$d = 2^\varepsilon q_1 \cdots q_r,$$

where $\varepsilon = 0$ or 1 and q_1, \dots, q_r are distinct odd primes. Let

$$N = 8q_1 \cdots q_r.$$

For any odd prime p , by quadratic reciprocity,

$$\begin{aligned} \left(\frac{-d}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right)^\varepsilon \prod_{i=1}^r \left(\frac{q_i}{p}\right) \\ &= (-1)^{\binom{p-1}{4}} (-1)^{\varepsilon \binom{p^2-1}{8}} \prod_{i=1}^r \left(\frac{p}{q_i}\right)^{\binom{p-1}{2} \binom{q_i-1}{2}}. \end{aligned}$$

It follows that, if p' is any prime for which $p \equiv p' \pmod{N}$, then

$$\left(\frac{-d}{p'}\right) = \left(\frac{-d}{p}\right).$$

The condition $\left(\frac{-d}{p}\right) = -1$ is therefore equivalent to p lying in one of $\frac{1}{2}\phi(N)$ arithmetic progressions \pmod{N} , where ϕ is the Euler function.

For each $y \in \mathbb{Z}$, where $(y, N) = 1$, let $\pi(y, N; M)$ be the number of primes p such that $p \leq M$ and $p \equiv y \pmod{M}$. By the prime number theorem for arithmetic progressions,

$$\pi(y, N; M) = \frac{1}{\phi(N)} \cdot \frac{M}{\ln M} + o\left(\frac{M}{\ln M}\right).$$

(For this formulation of the theorem see, for example, [2, Theorem 3.5.1, p. 72].)

Now let $\pi(N; M)$ be the number of primes p such that $p \leq M$ and $(p, N) = 1$. It follows that there exists $m_0 = m_0(d)$ such that, when $m > m_0$,

$$\pi(N; M) > \frac{9}{10} \cdot \frac{1}{2} \cdot \frac{M}{\ln M}.$$

We deduce that, when $m > m_0$,

$$r^* > \frac{9}{20} \frac{M}{\ln M} - \omega(m),$$

where $\omega(m)$ is the number of primes dividing m . It is clear that

$$2^{\omega(m)} \leq m.$$

The result follows. \square

The following conclusion is immediate.

Corollary 2. *For each d ,*

$$r(d, m) \rightarrow \infty, \quad \text{as } m \rightarrow \infty.$$

In [12, Corollary 5] it is proved that $r(d, 1) \rightarrow \infty$, as $d \rightarrow \infty$. (This is a more difficult problem.)

2. FREE QUOTIENTS

Let F_t be the free group of rank t , where $t \geq 0$.

Theorem 3. *Given t, d , there exists an epimorphism*

$$\rho : SL_2(\mathcal{O}_m)/U_2(\mathcal{O}_m) \rightarrow F_t,$$

for all but finitely many m .

Proof. It is known [11, Theorem 4.1] that there exists an epimorphism

$$\rho : SL_2(\mathcal{O}_m)/U_2(\mathcal{O}_m) \rightarrow F_s,$$

where $s = r(d, m) - 1$. The result follows from Corollary 2. \square

When $r(d, 1) \geq 3$, it follows that $SL_2(\mathcal{O})/U_2(\mathcal{O})$ and hence $SL_2(\mathcal{O}_m)/U_2(\mathcal{O}_m)$, for all m , have a free, non-cyclic quotient. By [12, Corollary 5] it is known that $r(d, 1) \geq 3$, for all but finitely many d . (The smallest such value is $d = 67$.)

This does not (in general) happen when $r(d, 1) < 3$. For example, when $d = 1, 2, 3, 7, 11$, it is a classical result that \mathcal{O} is a Euclidean ring. For these cases $SL_2(\mathcal{O}) = U_2(\mathcal{O}) (= E_2(\mathcal{O}))$, i.e. $SL_2(\mathcal{O})$ is generated by elementary matrices.

Corollary 4. *Given t, d , there exists an epimorphism*

$$\sigma : SL_2(\mathcal{O}, \mathfrak{q})/U_2(\mathcal{O}, \mathfrak{q}) \rightarrow F_t$$

for infinitely many \mathcal{O} -ideals \mathfrak{q} .

Proof. Fix m as in Theorem 3 and let \mathfrak{q}_0 be the conductor of \mathcal{O}_m in \mathcal{O} , i.e. the largest (non-zero) \mathcal{O} -ideal contained in \mathcal{O}_m . Let \mathfrak{q} be any non-zero \mathcal{O} -ideal contained in \mathfrak{q}_0 . From Theorem 3 $SL_2(\mathcal{O}_m)$ has a normal subgroup N , containing $U_2(\mathcal{O}_m)$, such that

$$SL_2(\mathcal{O}_m)/N \cong F_t.$$

Now \mathcal{O}_m is a Noetherian domain of Krull dimension 1 and so

$$NE_2(\mathcal{O}_m) \cdot SL_2(\mathcal{O}_m, \mathfrak{q}) = SL_2(\mathcal{O}_m),$$

by [5, Theorem 3.1]. It follows that $N \cdot SL_2(\mathcal{O}_m, \mathfrak{q}) = SL_2(\mathcal{O}_m)$ and hence that

$$SL_2(\mathcal{O}_m, \mathfrak{q})/SL_2(\mathcal{O}_m, \mathfrak{q}) \cap N \cong F_t.$$

We note that $U_2(\mathcal{O}_m, \mathfrak{q}) \leq N$, $SL_2(\mathcal{O}_m, \mathfrak{q}) = SL_2(\mathcal{O}, \mathfrak{q})$ and $U_2(\mathcal{O}_m, \mathfrak{q}) = U_2(\mathcal{O}, \mathfrak{q})$. \square

Corollary 5. $SL_2(\mathcal{O})$ has 2^{\aleph_0} non-normal, standard subgroups.

Proof. Fix $\mathcal{O}, \mathfrak{q}$ as in Corollary 4 with $t \geq 2$. Let S be any subgroup of $SL_2(\mathcal{O})$ such that

$$U_2(\mathcal{O}, \mathfrak{q}) \leq S \leq SL_2(\mathcal{O}, \mathfrak{q}).$$

It is clear that the \mathcal{O} -ideal generated by $x_{ij}, x_{ii} - x_{jj}$ ($i \neq j$), where $(x_{ij}) \in S$, is \mathfrak{q} , i.e. S is standard. In the proof of [7, Theorem 3.2] it is shown that a free group of rank at least 2 contains 2^{\aleph_0} non-normal subgroups. The result follows. \square

3. CONCLUDING REMARKS

By [12, Corollary 5] a stronger version of Corollary 4 holds for all but finitely many \mathcal{O} . When $r(d, 1) \geq 3$, it is known [11, Theorem 4.1] that $SL_2(\mathcal{O})/U_2(\mathcal{O})$ has a free, non-cyclic quotient. This is also then true for $SL_2(\mathcal{O}, \mathfrak{q})/U_2(\mathcal{O}, \mathfrak{q})$, where \mathfrak{q} is any non-zero \mathcal{O} -ideal.

For the remaining \mathcal{O} however infinitely many \mathfrak{q} in general are excluded from the statement of Corollary 4. Consider for example the *Picard group*, $SL_2(\mathbb{Z}[i])$, where $i^2 = -1$. (In this case $d = 1$ and $\omega = i$.) Let p be any rational prime, where $p \equiv 1 \pmod{4}$, and let α be a quadratic residue \pmod{p} .

The \mathbb{Z} -module,

$$\mathbb{Z}(1 + \alpha i) + \mathbb{Z}pi,$$

is a prime $\mathbb{Z}[i]$ -ideal \mathfrak{p} , say, and it is clear that the *only* order in $\mathbb{Z}[i]$ containing \mathfrak{p} is $\mathbb{Z}[i]$ itself. The proof of Corollary 4 tells us nothing about the structure of $SL_2(\mathbb{Z}[i], \mathfrak{p})/U_2(\mathbb{Z}[i], \mathfrak{p})$, since $SL_2(\mathbb{Z}[i]) = U_2(\mathbb{Z}[i])$. (We recall that $\mathbb{Z}[i]$ is a Euclidean ring.)

It is likely however that restrictions of this type are merely a consequence of the method of proof. Accordingly we conclude with the following.

Conjecture. $SL_2(\mathcal{O}, \mathfrak{q})/U_2(\mathcal{O}, \mathfrak{q})$ has a free, non-cyclic quotient, for all but finitely many \mathcal{O} -ideals \mathfrak{q} .

REFERENCES

1. H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*, Inst. Hautes Études Sci. Publ. Math. **33** (1967), 59–137. MR **39**:5574
2. A. O. Gelfond and Yu. V. Linnik, *Elementary methods in analytic number theory*, George Allen and Unwin, London, 1966.
3. F. J. Grunewald and J. Schwermer, *Free non-abelian quotients of SL_2 over orders of imaginary quadratic number fields*, J. Algebra **69** (1981), 298–304. MR **82i**:10027
4. B. Liehl, *On the groups SL_2 over orders of arithmetic type*, J. Reine Angew. Math. **323** (1981), 153–171. MR **82h**:10034
5. A. W. Mason, *On the subgroups of $GL(n, A)$ which are generated by commutators II*, J. Reine Angew. Math. **322** (1981), 118–135. MR **82i**:20056
6. ———, *Standard subgroups of $GL_2(A)$* , Proc. Edinburgh Math. Soc. **30** (1987), 341–349. MR **89b**:20101

7. ———, *Free quotients of congruence subgroups of SL_2 over Dedekind rings of arithmetic type contained in a function field*, Math. Proc. Cambridge Philos. Soc. **101** (1987), 421–429. MR **88d**:11033
8. ———, *Non-standard, normal and non-normal, standard subgroups of the modular group*, Canad. Math. Bull. **32** (1989), 109–113. MR **90f**:20067
9. ———, *Congruence hulls in SL_n* , J. Pure Appl. Algebra **89** (1993), 255–272. MR **94i**:20085
10. ———, *Normal subgroups of level zero of the Bianchi groups*, Bull. London Math. Soc. **26** (1994), 263–267. CMP 94:16
11. ———, *Free quotients of Bianchi groups and unipotent matrices* (submitted).
12. A. W. Mason, R. W. K. Odoni, and W. W. Stothers, *Almost all Bianchi groups have free, non-cyclic quotients*, Math. Proc. Cambridge Philos. Soc. **111** (1992), 1–6. MR **92j**:11042
13. A. W. Mason and R. W. K. Odoni, *Free quotients of subgroups of the Bianchi groups whose kernels contain many elementary matrices*, Math. Proc. Cambridge Philos. Soc. **116** (1994), 253–273. CMP 94:14
14. J.-P. Serre, *Le problème des groupes de congruence pour SL_2* , Ann. of Math. (2) **92** (1970), 489–527. MR **42**:7671
15. L. N. Vaserstein, *On the group SL_2 over Dedekind rings of arithmetic type*, Math. USSR-Sb. **18** (1972), 321–332. MR **55**:8253
16. R. Zimmert, *Zur SL_2 der ganzen Zahlen eines imaginär-quadratischen Zahlkörpers*, Invent. Math. **19** (1973), 73–81. MR **47**:6883

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW G12 8QW, SCOTLAND
E-mail address: awm@maths.gla.ac.uk