Normal congruence subgroups of the Bianchi groups and related groups

by

Robert M Scarth

A thesis submitted to
The Department of Mathematics
in the Faculty of Science
at the University of Glasgow
for the degree of
Doctor of Philosophy

April 21, 1999

Summary

Let $\mathcal{O}$ be an order in an imaginary quadratic number field. This thesis is mainly concerned with normal subgroups of $SL_2(\mathcal{O})$ and of $PSL_2(\mathcal{O})$. Suppose that $\mathcal{O}$ is a maximal order then $\mathcal{O}$ is the ring of integers in the number field and the group $PSL_2(\mathcal{O})$ is a *Bianchi group*. In chapter one we discuss the geometric background of these groups and introduce some fundamental algebraic concepts; those of order and level. We also discuss the Congruence subgroup problem. Chapter two is a discussion of the fundamental theorem of Zimmert [93]. In chapter three we discuss $PSL_2(\mathcal{O})$ where $\mathcal{O}$ is not a maximal order. We derive a formula for their index in the Bianchi groups and presentations for some of these groups. In particular we derive a presentation for $PSL_2(\mathbb{Z}\left[\sqrt{-3}\right])$ and using this presentation get a partial classification of the normal subgroups of $PSL_2(\mathbb{Z}\left[\sqrt{-3}\right])$.

Chapter four generalizes a result of Mason and Pride [62] about $SL_2(\mathbb{Z})$ to all but finitely many $SL_2(\mathcal{O})$. This result shows that for an arbitrary normal subgroup of $N \lhd SL_2(\mathcal{O})$ there is no relationship between the order and level of N. This is in distinction to the groups $SL_n(\mathcal{O})$, $n \geqslant 3$, where the order and level of a normal subgroup coincide. This answers a question of Lubotzky's.

Let $\mathcal{O}$ be an order in an imaginary quadratic number field. Then $\mathcal{O}$ is a Noetherian domain of Krull dimension one and has characteristic zero. Chapter five discusses SL_2 over the class of all Noetherian domains of Krull dimension one, including those of non-zero characteristic. In particular we generalize the work of Mason [58] and derive a relationship between the order and level of a normal congruence subgroup of $SL_2(K)$ for any Noetherian domain of Krull dimension one, K. In chapter six we apply this work to $SL_2(\mathcal{O})$ and construct a new and vast class of normal non-congruence subgroups of $SL_2(\mathcal{O})$. Finally we take a closer look at some particular $PSL_2(\mathcal{O})$.

"Results! Why man, I have gotten a lot of results. I know several thousand things that don't work."

- Thomas Edison [50] p.121.

List of Notation

R	A Ring.	
R^*	The group of units in the ring R.	
$char R$	The characteristic of R.	
L	A Local Ring.	
u	A unit in a ring R.	
$\mathbb{F}_q$	The field of q elements.	
d	A positive square-free integer.	p.4
m	A positive integer.	p.4
$\mathcal{O}_d$	The ring of integers in the imaginary quadratic number field $\mathbb{Q}\left(\sqrt{-d}\right)$.	p.4
$\mathcal{O}_{d,m}$	The Order of index m in $\mathcal{O}_d$.	p.4
ω	$\begin{cases} \frac{1+i\sqrt{d}}{2} & \text{if } d \equiv 3 \pmod 4 \\ i\sqrt{d} & \text{else} \end{cases}$	p.4
D	The discriminant of $\mathbb{Q}\left(\sqrt{-d}\right)$.	p.21
$\mathfrak{q}$	An ideal in a ring R.	
e_{ij}	The matrix with a 1 in the $(i,j)^{th}$ position and zero's elsewhere.	p.9
$E_{ij}(r)$	Denotes $I + re_{ij}$.	
E_{ij}	An elementary matrix; $E_{ij}(1)$.	
$E(x)$	Denotes the matrix $\begin{pmatrix} x & 1 \\ -1 & 0 \end{pmatrix}$.	p.43
$D(\mu)$	Denotes the matrix $\begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}$.	p.43
$SL_n(R)$	The group of $n \times n$ matrices over R with determinant 1.	
$PSL_n(R)$	$SL_n(R)$ with the centre factored out.	
$GL_n(R)$	The group of $n \times n$ matrices over R with non-zero determinant.	
$PSL_2(\mathbb{Z})$	The Modular group.	p.2

$PSL_2(\mathcal{O}_d)$	The Bianchi groups.	p.4
A	The matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(R)$.	p.4
T	The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(R)$.	p.4
U	The matrix $\begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix} \in SL_2(\mathcal{O}_{d,m})$.	p.4
a, t, u	The images of A, T, and U in $PSL_2(R)$, or $PSL_2(\mathcal{O}_{d,m})$.	p.4
M	An arbitrary 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.	
trM	The trace of the matrix M, ie $a + d$.	p.5
$detM$	The determinant of M, ie $ad - bc$.	
$E_n(R)$	The subgroup of $SL_n(R)$ generated by the elementary matrices.	p.9
$U_n(R)$	The normal subgroup of $SL_n(R)$ generated by the unipotent matrices.	p.24
$E_n(R, \mathfrak{q})$	The subgroup of $E_n(R)$ generated by the $\mathfrak{q}$-elementary matrices.	p.10
$H_n(R, \mathfrak{q})$	The subgroup of $SL_n(R)$ consisting of the $\mathfrak{q}$-scalar matrices.	p.10
$SL_n(R, \mathfrak{q})$	The principal congruence subgroup of level $\mathfrak{q}$.	p.11
$PSL_n(R, \mathfrak{q})$	The principal congruence subgroup of level $\mathfrak{q}$ in $PSL_2(R)$.	p.108
$H(\mathfrak{q})$	Alternative notation to $H_n(R, \mathfrak{q})$.	
$\Gamma(\mathfrak{q})$	Alternative notation to $SL_n(R, \mathfrak{q})$.	
$\Delta(\mathfrak{q})$	Alternative notation to $E_n(R, \mathfrak{q})$.	p.70
$U_n(R, \mathfrak{q})$	The normal subgroup of $SL_n(R)$ generated by the unipotent matrices in $SL_n(R, \mathfrak{q})$.	p.30
$o(S)$	The order of the subgroup S.	p.11
$l(S)$	The level of the subgroup S.	p.10
$\mathcal{E}_0\,(2, R; \mathfrak{q})$	The set of normal subgroups of $SL_2(R)$ of level zero and order $\mathfrak{q}$.	p.55
$Z(d, m)$	The Zimmert Set.	p.21
$r(d, m)$	The cardinality of $Z(d, m)$.	p.21
$\rho(d, m)$	The largest rank of a free quotient of $\Gamma_{d,m}$.	p.32
$\mathcal{N}_{d,m}(n)$	The number of normal congruence subgroups of $\Gamma_{d,m}$ of index exactly n.	p.110
G	An arbitrary group.	
F_r	The free group of rank r.	

$[x, y]$	The commutator of x and y, ie $x^{-1}y^{-1}xy$.	
G'	The commutator subgroup of G.	
G^{ab}	The abelianization of G, ie G/G'.	
N	An arbitrary normal subgroup of G.	
$N(x_1, \ldots)$	The normal closure in G of the elements $x_1, \ldots$.	p.97
$a_n(G)$	The number of subgroups of G of index exactly n.	p.97
$\gcd(x, y)$	The greatest common divisor of x and y.	
$\mathbb{H}^2$	Hyperbolic 2-space.	p.1
$\mathbb{H}^3$	Hyperbolic 3-space.	p.3

Contents

Acknowledgements

I would like to thank my supervisor, Dr. Alec Mason, for his patience, kindness and encouragement during the last three and a half years. I would also like to thank everyone at the Department of Mathematics at the University of Glasgow for contributing to a friendly and stimulating environment. Thanks also to the EPSRC for giving me financial support between October 1995 and September 1998, the Department of Mathematics here at Glasgow for giving my funding to attend various conferences, and my parents for paying my rent while I completed this work.

I would like to thank Andy, Iain, Mark Brightwell, Mark Ratter, Mohammad, and Stephen for the many interesting and stimulating discussions we had about Politics, Football, Philosophy, Theology, and even some Mathematics. I'd have learnt a lot less without you.

Finally, I would like to thank my family,especially my parents, for their unfailing support and belief throughout 21 years of education.

Statement

This thesis is submitted in accordance with the regulations for the degree of Doctor of Philosophy in the University of Glasgow.

Chapter one provides some motivation and introduces some fundamental concepts. Chapter two is a discussion of Zimmert's theorem [93]. Chapters three and six and the independent work of the author and chapters four and five are the joint work of the author and his supervisor. References are given throughout.

Chapter 1

Introduction

1.1 Geometric Background

We are interested in groups acting on Hyperbolic space. Hyperbolic geometry is the best known example of a non-Euclidean geometry. The importance of the parallel axiom and the development of non-Euclidean geometry in the history of Mathematics, indeed the history of Western thought cannot be overstated. See [41, 67, 82] for brief and accesible accounts.

1.1.1 Hyperbolic geometry

Let

$$\mathbb{H}^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

and equip $\mathbb{H}^2$ with the following metric

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y}$$

We now have the Poincaré half plane model for two dimensional hyperbolic geometry. The geodesics in $\mathbb{H}^2$ are straight lines and semicircles orthogonal to the real axis. The historical point is that given a geodesic L and a point P not on L there are infinitely many geodesics passing through P which do not intersect L. That is Euclids parallel axiom does not hold. We are interested in distance preserving maps, or rigid motions. The hyperbolic distance between $z_1, z_2 \in \mathbb{H}^2$ shall be denoted $\rho(z_1, z_2)$.

Definition. A function from $\mathbb{H}^2$ onto itself which preserves hyperbolic distance is called an *isometry.* The group of isometries is denoted $Isom(\mathbb{H}^2)$.

Consider the following set

$$\mathcal{M} = \left\{ z \mapsto \frac{az+b}{cz+d} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

this is the set of *Moebius transformations* of $\mathbb{C}$. They map $\mathbb{H}^2$ onto itself and are all isometries. $\mathcal{M}$ can be identified with the group $PSL_2(\mathbb{R})$ via the obvious map.

Theorem. *([38] theorem* 1.3.1*)* $Isom(\mathbb{H}^2)$ *is generated by* $PSL_2(\mathbb{R})$ *and the map* $z \mapsto -\overline{z}$. $PSL_2(\mathbb{R})$ *is of index* 2 *in* $Isom(\mathbb{H}^2)$.

Let X be a metric space and G a group acting on X.

Definition. A family $\{M_\alpha : \alpha \in A\}$ of subsets of X is called *locally finite* if for any compact set $K \subset X$ we have $M_\alpha \cap K \neq \emptyset$ for only finitely many $\alpha \in A$.

Definition. We say that a group G acts *properly discontinuously* on X if the G-orbit of any point $x \in X$ is locally finite.

Definition. A closed connected $F \subset X$, with $int(F) \neq \emptyset$, is a *fundamental region* for G if

1. $GF = X$.
2. $int(F) \cap g(int(F)) = \emptyset \ \forall \, 1 \neq g \in G$.

The existence of a fundamental region allows us, in particular to find a presentation for the group (see [49]).

Definition. $G \leqslant PSL_2(\mathbb{C})$ is said to be *discrete* if it contains no sequence of matrices converging elementwise to the identity. Discrete subgroups of $PSL_2(\mathbb{R})$ are called *Fuchsian groups.*

Example 1.1.1. $PSL_2(\mathbb{Z})$ is obviously discrete and therefore a Fuchsian group.

Suppose that $G \leqslant PSL_2(\mathbb{R})$ is not discrete. So G contains a sequence $\{g_n\}$ such that $g_n \to I$. Suppose that G has a fundamental region $F \subset \mathbb{H}^2$ and let $x \in int(F)$. Then $g_n x \to x$ as $n \to \infty$. So $\exists N$ such that $\forall \, n > N \ int(F) \cap g_n(int(F)) \neq \emptyset$. Contradiction. Hence G cannot have a fundamental region.

Let Γ be a Fuchsian group. Let $p \in \mathbb{H}^2$ be not fixed by any non-trivial element of Γ. The *Dirichlet fundamental polygon* for Γ centred at p is

$$D_p(\Gamma) = \left\{z \in \mathbb{H}^2 : \rho(z,p) \leqslant \rho(Tz,p) \ \forall T \in \Gamma\right\}$$

Theorem. *([38] theorem 3.2.2) For every Fuchsian group Γ and every $p \in \mathbb{H}^2$ not fixed by a non-trivial element of Γ, $D_p(\Gamma)$ is a connected convex fundamental region for Γ.*

Example 1.1.2. Let $\Gamma = PSL_2(\mathbb{Z})$. The set

$$F = \left\{z \in \mathbb{H}^2 : |z| \geqslant 1, |\mathrm{Re}(z)| \leqslant \frac{1}{2}\right\}$$

is a Dirichlet region for Γ centred at ki, some $k > 1$.

The theory of Fuchsian groups is of great interest and has been extensively studied. See [6, 7, 38].

1.1.2 Hyperbolic 3-space

The upper half-space in Euclidean three-space gives a convenient model of 3-dimensional hyperbolic space

$$\mathbb{H}^3 = \{(z,r) \in \mathbb{C} \times \mathbb{R} : r > 0\}$$

which we equip with the hyperbolic metric

$$ds^2 = \frac{dx^2 + dy^2 + dr^2}{r^2}$$

The group $PSL_2(\mathbb{C})$ acts on $\mathbb{H}^3$ in the following way. Let $M \in PSL_2(\mathbb{C})$ where

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

Then

$$M(z,r) = \left(\frac{(\bar{\delta} - \bar{\gamma}\bar{z})(\alpha z - \beta) - r^2\bar{\gamma}\alpha}{\tau}, \frac{r}{\tau}\right)$$

where

$$\tau = |\gamma z - \delta|^2 + r^2|\gamma|^2$$

Under this action the hyperbolic metric is $PSL_2(\mathbb{C})$-invariant. $SL_2(\mathbb{C})$ acts on $\mathbb{H}^3$ in exactly the same way. As above we want a class of discrete subgroups of $PSL_2(\mathbb{C})$. We make use of the following

Proposition. *[19] Let A be a discrete subring of $\mathbb{C}$ with a one then $SL_2(A)$ is a discrete subgroup of $SL_2(\mathbb{C})$.*

Proposition. *[19] The discrete subrings of $\mathbb{C}$ with a one are*

1. $\mathbb{Z}$.

2. *The ring of integers $\mathcal{O}_d = \mathbb{Z} + \omega\mathbb{Z}$ in an imaginary quadratic number field.*

3. *The orders $\mathcal{O}_{d,m} = \mathbb{Z} + m\omega\mathbb{Z}$ in an imaginary quadratic number field.*

where d is a positive square-free integer, m is a positive integer, and

$$\omega = \begin{cases} \frac{1+i\sqrt{d}}{2} & \textit{if } d \equiv 3 \pmod 4 \\ i\sqrt{d} & \textit{else} \end{cases}$$

This gives us a class of discrete subgroups of $SL_2(\mathbb{C})$ and of $PSL_2(\mathbb{C})$. We have already met the group $PSL_2(\mathbb{Z})$. It is known as the *Modular group.* It was Picard who, in 1883, first studied $PSL_2(\mathbb{Z}[i])$, and this group is known as the *Picard group* [67, 73]. The groups $PSL_2(\mathcal{O}_d)$ are called the *Bianchi groups.* They were first studied by Bianchi in the 1890s [8, 9] as a natural class of discrete subgroups of $PSL_2(\mathbb{C})$. See [23] chapter 7 for a discussion of their action on $\mathbb{H}^3$ and [25] for a discussion of their algebraic properties. The groups $PSL_2(\mathcal{O}_{d,m})$ are of finite index in the Bianchi groups. See [23] for a general treatment of discrete subgroups of $PSL_2(\mathbb{C})$ acting on $\mathbb{H}^3$. The Modular group and the Bianchi groups are the first arithmetic examples of such groups and are of great interest in number theory. We take the opportunity here to introduce three matrices which will be very important in what follows. Let R be any commutative ring with a one and let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(R)$$

We will also need the following

$$U = \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix} \in SL_2(\mathcal{O}_{d,m}).$$

We denote the corresponding matrices in PSL_2 by a, t, u. This will be a general convention.

A description of a fundamental region for the Bianchi groups in $\mathbb{H}^3$ can be found in [23] section 7.3. Swan [84] has used this to derive presentations for the group $SL_2(\mathcal{O}_d)$ for $d = 1, 2, 3, 7, 11, 5, 6, 15, 19$. It is then easy to derive a presentation for $PSL_2(\mathcal{O}_d)$.

We now look at matrices of finite order in $SL_2(\mathbb{C})$ and $SL_2(\mathcal{O}_{d,m})$. The results are well known but the presentation is our own. Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{C})$$

and let $tr = a + d$ be the trace of M. Recall that conjugate matrices have the same trace.

Lemma 1.1.1. *If $tr = \pm 2$ and $M \neq I$ then M is conjugate to $\pm T$ and so is of infinite order.*

Proof. We can suppose that

$$M = \begin{pmatrix} 1+\alpha & \beta \\ \gamma & 1-\alpha \end{pmatrix}$$

Now

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{pmatrix}$$

So letting $a = \sqrt{\beta}$, and $c = i\sqrt{\gamma}$ and then choosing b, d, so that $ad - bc = 1$ we get the result. □

Lemma 1.1.2. *If $tr^2 \neq 4$ (ie $tr \neq \pm 2$) then M is conjugate to*

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

for some $\alpha \in \mathbb{C}$.

Proof. Suppose that $z \in \mathbb{C}$ is a fixed point of M ie

$$\frac{az+b}{cz+d} = z$$

So $cz^2 + (d-a)z - b = 0$. The discriminant of this quadratic is $(d-a)^2 + 4bc = (a+d)^2 - 4(ad-bc) = tr^2 - 4$. Now $tr^2 \neq 4$ so M has two distinct fixed points z_1, and z_2. Let $w = (z_2 - z_1)^{-1}$ and consider

$$\begin{pmatrix} 1 & -z_2 \\ w & -z_1 w \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -z_2 \\ w & -z_1 w \end{pmatrix}^{-1}$$

Using the fact that $cz_i^2 + (d-a)z_i - b = 0$, for $i = 1, 2$, we can show that this matrix is equal to

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

for some $\alpha \in \mathbb{C}$. □

Lemma 1.1.3. *If $|tr| > 2$ then M is of infinite order.*

Proof. Clearly $tr^2 \neq 4$, so M is conjugate to

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

for some $\alpha \in \mathbb{C}$. Suppose that $|\alpha| = 1$, so $|\alpha^{-1}| = 1$ and $|tr| = |\alpha + \alpha^{-1}| \leqslant |\alpha| + |\alpha^{-1}| = 2$. So $|tr| \leqslant 2$. Contradiction. So $|\alpha| \neq 1$, so $|\alpha| > 1$, or $|\alpha^{-1}| > 1$. So $|\alpha^n| \to \infty$, or $|\alpha^{-n}| \to \infty$ as $n \to \infty$. Now

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}^n = \begin{pmatrix} \alpha^n & 0 \\ 0 & \alpha^{-n} \end{pmatrix}.$$

So $M^n \neq I$ for every $n \in \mathbb{Z}$. □

Lemma 1.1.4. *If $|tr| = 2$ and $tr^2 \neq 4$ then M is of infinite order.*

Proof. Now $tr^2 \neq 4$ so M is conjugate to

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

for some $\alpha \in \mathbb{C}$. As above if $|\alpha| \neq 1$ then M is of infinite order. So suppose that $|\alpha| = 1$, so $\alpha^{-1} = \overline{\alpha}$. So $\alpha + \alpha^{-1} = \alpha + \overline{\alpha} = 2\mathrm{Re}(\alpha)$. So $2 = |tr| = |\alpha + \alpha^{-1}| = 2|\mathrm{Re}(\alpha)|$, so $\mathrm{Re}(\alpha) = 1$. Hence $\alpha = \alpha^{-1} = 1$ and $M = I$. Contradiction. □

Lemma 1.1.5. *Suppose that $|tr| < 2$. Then if $tr \notin \mathbb{R}$ then M is of infinite order.*

Proof. $tr^2 \neq 4$ so M is conjugate to

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

for some $\alpha \in \mathbb{C}$ and where $\alpha + \alpha^{-1} = tr$. Now if $|\alpha| \neq 1$ then, as above, M is of infinite order. So suppose that $|\alpha| = 1$ then $\alpha^{-1} = \overline{\alpha}$ so $tr = \alpha + \overline{\alpha} = 2\mathrm{Re}(\alpha) \in \mathbb{R}$. □

Lemma 1.1.6. *If $tr = 0$ then $M^2 = -I$.*

Proof. Now M is conjugate to

$$X = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$$

some $\alpha \in \mathbb{C}$ such that $\alpha + \alpha^{-1} = 0$. So $\alpha^2 + 1 = 0$, so $\alpha = \pm i$. It is then easy to verify that $X^2 = -I$. □

Lemma 1.1.7. *If $tr = 1$ then $M^3 = -I$ and if $tr = -1$ then $M^3 = I$.*

Proof. Now M is conjugate to

$$X = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$$

for some $\alpha \in \mathbb{C}$ such that $\alpha + \alpha^{-1} = tr$. First suppose that $tr = -1$. Then $\alpha^2 + \alpha + 1 = 0$, so $\alpha(\alpha^2 + \alpha + 1) = 0$ and so $\alpha^3 = 1$. Thus $X^3 = I$ and so $M^3 = I$. Similarly if $tr = 1$ then $\alpha^3 = -1$ and so $X^3 = -I$. Hence result. □

Theorem 1.1.8. *Let $I \neq M \in SL_2(\mathcal{O}_{d,m})$. Then M is of finite order if and only if $tr = 0$, or ± 1.*

Proof. Now $tr \in \mathcal{O}_{d,m}$ so $|tr|^2 \in \mathbb{Z}$. First, if $|tr|^2 \geqslant 4$ then M is of infinite order. Suppose that $|tr|^2 < 4$, so $|tr|^2 = 0$, 1, 2, or 3, but if M is of finite order $tr \in \mathcal{O}_{d,m} \cap \mathbb{R} = \mathbb{Z}$, so $|tr| = 0$, or 1. Now if $|tr| = 0$ then $tr = 0$ and so $M^2 = -I$. If $|tr|^2 = 1$ then $tr = \pm 1$, so $M^6 = I$. □

1.2 The normal subgroups of $SL_n(R)$

Let R be a ring, with a one. Let $n \in \mathbb{N}$, $n \geqslant 2$, and form the group $SL_n(R)$. It is natural to ask the following

Question. What are the normal subgroups of $SL_n(R)$?

The case where R is a field is simple; literally:

Theorem. *[21] Let $\mathbb{F}$ be any field, $n \in \mathbb{N}$, $n \geqslant 2$. Then $PSL_n(\mathbb{F})$ is simple with two exceptions:*

$$PSL_2(\mathbb{F}_2) \cong S_3 \text{ and } PSL_2(\mathbb{F}_3) \cong A_4$$

where $\mathbb{F}_d$ denotes the field of d elements.

By another result of Dieudonné [21] $SL_2(\mathbb{F})' = SL_2(\mathbb{F})$, and so the only non-trivial normal subgroup of $SL_2(\mathbb{F})$ is $\{\pm I\}$. Note that the exceptions are both two dimensional linear groups. We shall see that the two dimensional case is, in general, more complicated than the higher dimensional cases. Further, when investigating normal subgroups of $SL_2(R)$ one finds that ideals of index 2 or 3 in R play an important role. When we pass from fields to rings we no longer have simplicity.

Example 1.2.1. Let $m \in \mathbb{Z}$. Consider the following subgroup

$$\Gamma(m) = \{M \in SL_2(L) : M \equiv I \pmod{m}\}$$

This is clearly a non-trivial normal subgroup of $SL_2(L)$. It is called the *Principal congruence subgroup of level* m, and is a member of a very important class of normal subgroups, as we shall see later on.

1.2.1 SL_n over a local ring

The next easiest case after that of a field is a local ring,so let $R = L$, be a commutative local ring, with maximal ideal $\mathfrak{m}$, and let $N\mathfrak{m} = |L : \mathfrak{m}|$. We introduce two classes of normal subgroup of $SL_2(L)$. Let $\mathfrak{q} \lhd L$ be an ideal in L, then define

$$\Gamma(\mathfrak{q}) = \{M \in SL_2(L) : M \equiv I \pmod{\mathfrak{q}}\}$$

this is the kernel of the natural map $SL_n(L) \longrightarrow SL_n(L/\mathfrak{q})$ and let

$$H(\mathfrak{q}) = \{M \in \Gamma : M \equiv kI \pmod{\mathfrak{q}}, k \in L\}$$

$H(\mathfrak{q})/\Gamma(\mathfrak{q})$ is the centre of $SL_2(L)/\Gamma(\mathfrak{q})$. Let $S \leqslant SL_2(L)$, by the *level* of S, denoted $l(S)$, we mean the largest ideal, $\mathfrak{q}$ of L such that $\Gamma(\mathfrak{q}) \leqslant S$, and by the *order* of S, denoted $o(S)$, we mean the smallest ideal, $\mathfrak{q}$ of L such that $S \leqslant H(\mathfrak{q})$. Since $\Gamma(\mathfrak{q}) \leqslant H(\mathfrak{q})$ we have $l(S) \leqslant o(S)$.

The first attempt to classify the Normal subgroups of $SL_2(L)$ was in 1961 by Klingenberg.

Theorem. *[42] Let $N \leqslant SL_2(L)$ be of order $\mathfrak{q}$. Then $N \lhd SL_2(L) \Leftrightarrow l(N) = o(N)$ where, for $n = 2$ we assume $N\mathfrak{m} \neq 3$, and 2 is a unit.*

Lacroix, in 1966 [43], dropped the condition that 2 was a unit and included the case where $N\mathfrak{m} = 3$ but was unable to deal with the case $N\mathfrak{m} = 2$:

Theorem. *Suppose that $N\mathfrak{m} > 2$, and let $N \leqslant SL_2(L)$ be of order $\mathfrak{q}$. Then $N \lhd SL_2(L) \Leftrightarrow o(N) = l(N)$ unless $N\mathfrak{m} = 3$, and $o(N) = L$. If $N\mathfrak{m} = 3$ and $N \lhd SL_2(L)$, $o(N) = L$ then $N = SL_2(L)$, or $N = SL_2(L)'$.*

However Lacroix provided examples of non-normal subgroups of $SL_2(L)$ of order L.

The case where $N\mathfrak{m} = 2$ appears to be very complicated in general (see [43]). Mason [57] has investigated the case where $N\mathfrak{m} = 2$, $\mathfrak{m}$ is principal and every ideal of L is a power of $\mathfrak{m}$. In section (5.3) we investigate the normal subgroups of $SL_2(L)$ and introduce techniques which allow us to deal with the case $N\mathfrak{m} = 2$ and $\mathfrak{m}$ nilpotent.

Klingenberg showed (roughly) that $N \lhd SL_n(L) \Leftrightarrow l(N) = o(N)$. This leads to the following

Definition. Let $S \leqslant SL_n(L)$. If $l(S) = o(S)$ we say that S is *standard.*

This gives rise to the *standard criterion*:

$$N \lhd SL_n(L) \Leftrightarrow N \text{ is standard}$$

With slight modification these concepts carry over to the case of an arbitrary ring. We remark that Costa and Keller [18] have characterized the normal subgroups of $GL_2(A)$ for an arbitrary commutative local ring A in terms of certain commutator groups. Their solution reduces to that of Klingenberg and Lacroix in the relevant cases. We mention it only in passing here because we are mainly interested in the standard criterion, or, where that fails the relationship between the order and level of a normal subgroup.

1.2.2 SL_n over an arbitrary ring

We introduce the following subgroup of $SL_n(R)$:

$$E_n(R) =< I + re_{ij} : r \in R, i \neq j >$$

It is well known that when $R = F$ is a field, $SL_n(F) = E_n(F)$. This remains true for some rings. Firstly, in light of the previous section

Proposition. *([3] corollary 5.9.2) Let L be a semilocal ring. Then $\forall n \geqslant 2$ $E_n(L) = SL_n(L)$.*

Proposition. *([33] proposition 2.4) Let R be a euclidean ring. Then $\forall n \geqslant 2$ $E_n(R) = SL_n(R)$.*

As $\mathbb{Z}$ is euclidean we have

Proposition. *([51] lemma* 3.1*) $SL_2(\mathbb{Z}) = E_2(\mathbb{Z})$.*

Let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{-d})$. The *Bianchi groups* are the groups $PSL_2(\mathcal{O}_d)$, we have already mentioned them in section (1.1.2). Now $\mathcal{O}_d$ has a euclidean algorithm $\Leftrightarrow d = 1, 2, 3, 7, 11$ ([13] p.21), so if $d = 1, 2, 3, 7, 11$ then $SL_2(\mathcal{O}_d) = E_2(\mathcal{O}_d)$. In fact

Proposition. *([14] Theorem 6.1)*

$$SL_2(\mathcal{O}_d) = E_2(\mathcal{O}_d) \Leftrightarrow d = 1, 2, 3, 7, 11$$

The groups $PSL_2(\mathcal{O}_d)$, $d = 1, 2, 3, 7, 11$ are called the *Euclidean Bianchi groups.* We can now ask the following which is obviously related to our original question

Question. What are the $E_n(R)$-normalized subgroups of $SL_n(R)$?

We now introduce an important concept, the *SR_n-condition.* Let R be a ring. If $a_1, \ldots, a_n \in R$ such that $\sum Ra_i = R$ then $\exists b_1, \ldots, b_{n-1} \in R$ such that $\sum R(a_i + b_i a_n) = R$ then we say that R has *stable range n*, and we write $SR_n(R)$ or say R has SR_n. The SR_2-condition is particularly important so we describe it separately: If $Ra_1 + Ra_2 = R$ then $\exists t \in R$ such that $a_1 + ta_2$ is a unit. See [16, 29, 85, 87, 88] for examples of rings with SR_2.

Proposition. *([3] Proposition* 5.3.4*) Semilocal rings are SR_2-rings.*

Proposition. *[3] If R is an SR_2-ring then $SL_2(R) = E_2(R)$.*

We remark that Dedekind domains have SR_3 ([3] theorem 3.5 page 239). We must also modify our concept of level because, famously, in general not every normal subgroup of $SL_n(R)$ contains a principal congruence subgroup. Let $\mathfrak{q} \lhd R$. Let

$$E_n(R, \mathfrak{q}) =< I + \alpha e_{ij} : \alpha \in \mathfrak{q}, 1 \leqslant i, j \leqslant n, i \neq j >^{E_n(R)}$$

$$H_n(R, \mathfrak{q}) = \{M \in SL_n(R) : M \equiv kI \pmod{\mathfrak{q}}, k \in R\}$$

Let $S \leqslant SL_n(R)$. By the *level* of S, denoted $l(S)$, we mean the largest $\mathfrak{q} \lhd R$ such that $E_n(R, \mathfrak{q}) \leqslant S$. This is well defined because $E_n(R, \mathfrak{q}_1)E_n(R, \mathfrak{q}_2) = E_n(R, \mathfrak{q}_1 + \mathfrak{q}_2)$. By the *order* of S, denoted $o(S)$ we mean the smallest $\mathfrak{q} \lhd R$ such that $S \leqslant H_n(R, \mathfrak{q})$. As before, we say S is *standard* if $l(S) = o(S)$. We define a *Principal congruence subgroup* as before

$$SL_n(R, \mathfrak{q}) = \{M \in SL_n(R) : M \equiv I \pmod{\mathfrak{q}}\}$$

clearly $E_n(R, \mathfrak{q}) \leqslant SL_n(R, \mathfrak{q})$. As in the case of a local ring $H_n(R, \mathfrak{q})/SL_n(R, \mathfrak{q})$ is the centre of $SL_n(R)/SL_n(R, \mathfrak{q})$. In the case of a local ring our two concepts of level are the same because:

Proposition. *([3] corollary 5.9.2) Let L be a local ring. Then $\forall n \geqslant 2$ $E_n(L, \mathfrak{q}) = SL_n(L, \mathfrak{q})$.*

Any subgroup of $SL_n(R)$ which contains a principal congruence subgroup is known as a *congruence subgroup*. The question of whether every subgroup of finite index in $SL_n(R)$ is a congruence subgroup or not is of great interest and is known as the *Congruence Subgroup Problem*. We discuss it in the next section.

Most attempts to understand the normal subgroups of $SL_n(R)$ are centred round the standard criterion, and we now describe some of these attempts.

Theorem. *Let $H \leqslant GL_n(A)$. Then for $n \geqslant 3$, if A has SR_2 [3], or is commutative [86], or is a Banach algebra [88], or is von-Neumann regular [89] then*

$$H \textit{ is } E_n(A)\textit{-normalized} \Leftrightarrow H \textit{ is standard}$$

We remark that there exist examples of rings for which the standard criterion fails for $n \geqslant 3$ (See [28, 90]). We now focus exclusively on commutative rings and ask how are the $E_2(R)$-normalized subgroups and the standard subgroups related? It turns out that the answer depends very much on R.

Theorem. *[3] IF R has SR_2 and $S \leqslant SL_2(R)$ then S standard $\Rightarrow$ S is $E_2(R)$-normalized.*

Costa and Keller ([17] theorem 2.6) have provided a partial converse

Theorem. *Let R be an SR_2 ring with $6 \in R^*$. Then $N \lhd SL_2(R) \Rightarrow N$ is standard.*

The cases $R = F_2$, or F_3 show that $6 \in R^*$ is necessary. Suppose now that A is a Dedekind domain of arithmetic type (see the section at the end of this chapter on number theory) so A has SR_3, and suppose that A has infinitely many units. Serre has shown ([80] Prop 2 p. 492)

Theorem. *Let A be a Dedekind domain of arithmetic type and suppose that A^* is infinite. Then $SL_2(A)$ has no $E_2(A)$-normalized subgroups of level zero and non-zero order.*

Mason has proved the following

Theorem. *[55] Let A be a Dedekind domain of arithmetic type with infinitely many units then every standard subgroup of $SL_2(A)$ is $E_2(A)$-normalized.*

we also have

Theorem. *[75] Let A be a Dedekind domain of arithmetic type with infinitely many units. Then the $E_2(A)$-normalized subgroups of $SL_2(A)$ are precisley the standard subgroups if and only if the following three conditions hold for A:*

1. *All residue class fields of A have more than 3 elements.*
2. *$2 \in A^*$ or 2 is unramified in A.*
3. *$E_2(A, \mathfrak{a}) = [E_2(A), E_2(A, \mathfrak{a})]$ for every $\mathfrak{a} \lhd A$.*

However Mason has shown that when A^* is infinite the order and level of an $E_2(A)$-normalized subgroup are closely related.

Theorem. *([58]) Let $N \leqslant SL_2(A)$ be $E_2(A)$-normalized. Let $\mathfrak{q} = o(N)$, and $\mathfrak{q}^* = l(N)$. Then*

1. *If A is contained in a number field and is not totally imaginary then $12\mathfrak{q} \leqslant \mathfrak{q}^*$.*
2. *If A is contained in a number field and is totally imaginary then $12\mathfrak{u}_0\mathfrak{q} \leqslant \mathfrak{q}^*$.*
3. *If A is contained in a function field in one variable over a finite field then $\mathfrak{q}^3 \leqslant \mathfrak{q}^*$.*

where $\mathfrak{u}_0$ is defined as follows. Let m be the total number of roots of unity in A, and let $\mathfrak{u}$ be the A-ideal generated by $u^2 - 1$ where $u \in A^*$. If $m = 2$ Let $\mathfrak{u}_0 = \mathfrak{u} + 2A$ and if $m > 2$ then let $\mathfrak{u}_0 = \mathfrak{u}$.

So we can see that in the two dimensional case the unit structure becomes important. What happens to the standard criterion when the unit group is finite? Consider first the group $SL_2(\mathbb{Z})$, here we see that not only does the standard criterion fail but it fails badly:

Theorem. *[56, 62] The group $SL_2(\mathbb{Z})$ has $2^{\aleph_0}$ non-normal standard subgroups and $2^{\aleph_0}$ non-standard normal subgroups.*

In fact a more precise result is achieved. Let let $\mathcal{E}_0(2,\mathbb{Z};\mathfrak{q})$ denote the set of normal subgroups of $SL_2(\mathbb{Z})$ of level zero, and order $\mathfrak{q}$.

Theorem. *[62] Let $0 \neq \mathfrak{q} \lhd \mathbb{Z}$ then $|\mathcal{E}_0(2,\mathbb{Z};\mathfrak{q})| = 2^{\aleph_0}$.*

The situation in the groups $SL_2(\mathcal{O}_d)$ is similar

Theorem. *[60] For every positive square-free integer d, the group $SL_2(\mathcal{O}_d)$ has $2^{\aleph_0}$ non-normal standard subgroups.*

The obvious question now is

Question. Does every group $SL_2(\mathcal{O}_d)$ have $2^{\aleph_0}$ non-standard normal subgroups?

Mason has shown

Theorem. *[59] For every positive square-free integer d, the group $SL_2(\mathcal{O}_d)$ has $2^{\aleph_0}$ normal subgroups of level zero.*

The only normal subgroup of $SL_2(\mathcal{O}_d)$ with order $\{0\}$ is the trivial subgroup. Thus there are uncountably many non-standard normal subgroups in the groups $SL_2(\mathcal{O}_d)$. Later we extend this to show that for all but finitely many (d,m), and all $0 \neq \mathfrak{q} \lhd \mathcal{O}_{d,m}$, $|\mathcal{E}_0(2,\mathcal{O}_{d,m};\mathfrak{q})| = 2^{\aleph_0}$. The exceptions are almost certainly due to an inadequacy in our proof. Mason has obtained similar results in the final case. Let $\mathcal{C}$ be a Dedekind domain of arithmetic type contained in a function field and with finitely many units. Let $\Gamma = SL_2(\mathcal{C})$.

Theorem. *([53] theorem 3.1) There exist $2^{\aleph_0}$ normal subgroups of finite index in Γ which have level zero.*

Theorem. *([53] theorem 3.2) Let $\mathfrak{q} \lhd \mathcal{C}$ be such that $N\mathfrak{q} > c_0$, some constant c_0. Then Γ contains $2^{\aleph_0}$ non-normal standard subgroups of level $\mathfrak{q}$.*

1.2.3 The Congruence Subgroup Problem

Let R be a commutative ring with a one.

Congruence Subgroup Problem. Does every subgroup of $SL_n(R)$ of finite index contain a principal congruence subgroup?

This question can, with some care, be made to make sense in $PSL_n(R)$, the details can be found in section (6.4). The Congruence Subgroup Problem has a long history and has its origins in the work of Fricke and Klein, and Pick in the 19th century (see [34] section 4.3 and [11] chapter I.6 section B). Klein [39] pointed out, at a meeting of the Munich Academy on 6th December 1879, that the Modular Group, $PSL_2(\mathbb{Z})$, contains subgroups of finite index which do not contain a principal congruence subgroup. This was later proven simultaneously and independently by Fricke [27] and Pick [74]. We outline the proof, which can be found in [51]. Chandler and Magnus [11] assert, without any evidence, that it may be pre-1914.

Lemma.

$$\frac{PSL_2(\mathbb{Z})}{PSL_2(\mathbb{Z}, n\mathbb{Z})} \cong PSL_2(\mathbb{Z}_n)$$

Where $\mathbb{Z}_n$ denotes the ring of integers mod n.

Lemma. *The only non-abelian quotient groups that can appear in a composition series of $PSL_2(\mathbb{Z}_n)$ are the groups $PSL_2(\mathbb{Z}_p)$, where p is prime.*

Lemma. *A_{11} is a quotient of $PSL_2(\mathbb{Z})$, and A_{11} is not isomorphic to any of the groups $PSL_2(\mathbb{Z}_p)$.*

The kernel of the map $PSL_2(\mathbb{Z}) \twoheadrightarrow A_{11}$ is then a normal non-congruence subgroup of $PSL_2(\mathbb{Z})$. It is then a simple matter to see that $SL_2(\mathbb{Z})$ must also contain non-congruence subgroups. The positive solution of the problem in the $n \geqslant 3$ case was proved simultaneously in 1965 by Mennicke [66] and Bass-Lazard-Serre [4] in the context of $SL_2(\mathbb{Z})$:

Theorem. *Let $n \geqslant 3$. If $H \leqslant SL_n(\mathbb{Z})$ is of finite index then $SL_2(\mathbb{Z}, n\mathbb{Z}) \leqslant H$ for some $n \neq 0$.*

Again we see that in the two dimensional case the normal subgroup structure of $SL_n(\mathbb{Z})$ is much more complicated than the higher dimensional cases. In fact the situation is a lot more complicated than may at first appear because "most" subgroups of the Modular group are non-congruence subgroups. We now outline two different ways in which this idea is made precise.

The Modular group has the following presentation $PSL_2(\mathbb{Z}) =< a, t; a^2, (at)^3 >\cong C_2 * C_3$ [25, 51, 70, 81]. Newman [71] has derived an asymptotic formula for the number of subgroups of a given index in the free product of finitely many cyclic groups. Applied to the Modular group we get

Theorem. *[71] Let $a_n(G)$ denote the number of subgroups of G of index n. Then*

$$a_n(PSL_2(\mathbb{Z})) \sim (12\pi e^{1/2})^{-1/2} \exp\left(\frac{n\log n}{6} - \frac{n}{6} + n^{\frac{1}{2}} + n^{\frac{1}{3}} + \frac{\log n}{2}\right)$$

Now let $\gamma_n(PSL_2(\mathbb{Z}))$ denote the number of congruence subgroups of $PSL_2(\mathbb{Z})$ of index at most n. A special case of a theorem of Lubotzky [47] is

Theorem. *There exists positive constants C_1, C_2 such that*

$$n^{C_1 \log n/\log\log n} \leqslant \gamma_n(PSL_2(\mathbb{Z})) \leqslant n^{C_2 \log n/\log\log n}.$$

So it can be seen that

$$\frac{\gamma_n(PSL_2(\mathbb{Z}))}{a_n(PSL_2(\mathbb{Z}))} \longrightarrow 0 \text{ as } n \longrightarrow \infty$$

and in this sense most subgroups of the modular group are non-congruence subgroups. Again it is now simple to see that in $SL_2(\mathbb{Z})$ most subgroups are non-congruence. We now outline another interpretation. Let

$$\mathcal{F} = \{S \leqslant SL_2(\mathbb{Z}) : |SL_2(\mathbb{Z}) : S| < \infty\}$$

and

$$\mathcal{C} = \{C \leqslant SL_2(\mathbb{Z}) : C \text{ a congruence subgroup}\}$$

These constitute bases for neighbourhoods of the identity for two topologies on $SL_2(\mathbb{Q})$. Let $\widehat{SL_2(\mathbb{Q})}$ be the completion relative to $\mathcal{F}$ and let $\overline{SL_2(\mathbb{Q})}$ be the completion relative to $\mathcal{C}$. Since $\mathcal{C} \subseteq \mathcal{F}$ we have a natural surjection

$$\Pi : \widehat{SL_2(\mathbb{Q})} \longrightarrow \overline{SL_2(\mathbb{Q})}$$

We denote the kernel of this map by $C(SL_2, \mathbb{Z})$ and call it the *non-congruence kernel.* The Congruence Subgroup Problem now becomes the following

Question. Is $C(SL_2, \mathbb{Z})$ trivial?

Theorem. *[45]*

$$C(SL_2, \mathbb{Z}) = \hat{F}_\omega$$

where $\hat{F}_\omega$ is the free profinite group of countable rank.

That is the congruence kernel is enormous, and so again most subgroups of $SL_2(\mathbb{Z})$ are non-congruence. It is simple to see that the same is true in the modular group $PSL_2(\mathbb{Z})$. So far we have looked at the congruence subgroup problem in $SL_n(\mathbb{Z})$. What about more general rings?

Let K be a global field (see section on number theory at the end of this chapter), $S_\infty \subseteq S \subseteq \Omega$, $S \neq \emptyset$ and $\mathcal{O} = \mathcal{O}_S$ the ring of S-integers. Form the group $SL_n(\mathcal{O})$. Clearly the congruence subgroup problem makes sense in this group and we can construct the congruence kernel $C(SL_n, \mathcal{O})$ in exactly the same way as $C(SL_2, \mathbb{Z})$. The congruence subgroup problem then becomes to determine the structure of $C(SL_n, \mathcal{O})$. Bass-Milnor-Serre [5] proved the following

Theorem. *With the above notation suppose that $\mathcal{O}$ is a Dedekind domain of arithmetic type, and $n \geqslant 3$. Then $C(SL_n, \mathcal{O}) = 1$ unless K is a number field which is totally complex and $\mathcal{O}$ is the ring of integers, in which case $C(SL_n, \mathcal{O}) \cong \mu(K)$, the (finite cyclic) group of all roots of unity in K.*

The $n = 2$ case was dealt with by Serre [80].

Theorem. *With the above notation and $n = 2$ then*

1. *If $|S| \geqslant 2$ and it is not the case that K is a totally complex number field and $\mathcal{O}$ its ring of integers then $C(SL_2, \mathcal{O}) = 1$.*
2. *If $|S| \geqslant 2$ and K is a totally complex number field and $\mathcal{O}$ is its ring of integers then $C(SL_2, \mathcal{O}) \cong \mu(K)$.*
3. *If $|S| = 1$ then $C(SL_2, \mathcal{O})$ is infinite.*

Thus the Congruence Subgroup Problem fails completely only in the case where $n = 2$ and $|S| = 1$. So again we see that the two dimensional case is more complicated than the higher dimensional cases, and in the two dimensional case the unit structure of the ring becomes important. There are three families of rings $\mathcal{O}$ for which $|S| = 1$: $\mathbb{Z}$, $\mathcal{O}_d$, and $\mathcal{C}$ (see section on number theory). We have already seen Lubotzky's characterization of $C(SL_2, \mathbb{Z})$. He also proved

Theorem. *[45] With the above notation let $\mathcal{O} = \mathcal{O}_d$, or $\mathcal{C}$. Then $C(SL_2, \mathcal{O})$ contains $\hat{F}_\omega$, the free profinite group of countable rank, as a closed subgroup.*

So the Modular group and the Bianchi groups contain a great many non-congruence subgroups. We have already mentioned that Fricke [27] and Pick [74] gave examples of non-congruence subgroups of the modular group (see also [40]). Reiner [77] generalized their construction and many authors have produced classes of non-congruence subgroups (see [37] and [70]). Stothers has shown [83] that the minimal index of a non-congruence subgroup in the Modular group is 7. McQuillan has classified the normal congruence subgroups of the Modular group [65]. Drillick [22] has adapted the approach in Magnus [51] outlined earlier to the Bianchi group $PSL_2(\mathcal{O}_1)$, known as the *Picard Group.* Britto [10] generalized Drillicks arguments to construct an infinite family of non-congruence subgroups in $PSL_2(\mathcal{O}_d)$ for $d = 1, 2, 3, 7, 11, 5, 6, 15$. Since the basis of this construction is a surjection of $PSL_2(\mathcal{O}_d)$ onto A_n, $n \geqslant 7$, all of the normal non-congruence subgroups constructed by these methods are of index $6k$, for some $k \in \mathbb{N}$. It is also the case that these normal non-congruence subgroups are torsion free.

In chapter five we extend the work of Mason in [58] and derive a relationship between the order and level of a normal congruence subgroup of $PSL_2(\mathcal{O}_{d,m})$. We then use this relationship in chapter six to show that nearly every normal subgroup in $PSL_2(\mathcal{O}_{d,m})$ of index not divisible by 6 is a non-congruence subgroup. Further they all have torsion. Thus our normal non-congruence subgroups are all different from those constructed by Drillick and Britto.

1.3 Some Number Theory

For more information see [34] section 2.2E and the references therein.

Let K be any field. Let

$$v : K \longrightarrow \mathbb{R}$$

Consider the following four conditions:

1. $v(a) \geqslant 0$, and $v(a) = 0 \Leftrightarrow a = 0$.

2. $v(ab) = v(a)v(b)$.

3. $v(a + b) \leqslant v(a) + v(b)$.

4. $v(a + b) \leqslant \max(v(a), v(b))$.

Clearly 1 and 4 $\Rightarrow$ 3. If v satisfies $1, 2$, and 3 we say v is a *valuation on* K. If v also satisfies 4, v is *non-Archimedean*, and if not it is *Archimedean.* If $v(a) = 1\ \forall a \in K - \{0\}$ then v is the *trivial valuation.* We say that a field is *global* if it is a finite separable extension of $\mathbb{Q}$ or of the quotient field of a polynomial ring $\mathbb{F}_d[X]$, where $\mathbb{F}_d$ is a finite field of order d. In the first case K is a *number field*, in the second a *function field.* We say that two valuations v_1, and v_2 are *equivalent* if for every $a \in K$ we have $v_1(a) < 1 \Leftrightarrow v_2(a) < 1$. Let K be a global field. Let Ω be a complete set of inequivalent non-trivial valuations on K and let $S_\infty \subseteq \Omega$ be the set of Archimedean valuations. Suppose $S_\infty \subseteq S \subseteq \Omega$ and $S \neq \emptyset$ then

$$\mathcal{O}_S = \{x \in K : v(x) \leqslant 1\ \forall v \notin S\}$$

is called the *ring of S-integers* of K. $\mathcal{O}_S$ is a Dedekind domain. If S is finite then we say $\mathcal{O}_S$ is a *Dedekind domain of arithmetic type.* If K is a number field and $S = S_\infty$ then $\mathcal{O}_S$ is the *ring of integers* of K.

The completion of K with respect to an Archimedean valuation, v, is isomorphic (as a topological field) to $\mathbb{R}$, or $\mathbb{C}$ and we say v is *real* or *complex* accordingly. The number field K is *totally real* if all valuations in S_∞ are real, and *totally complex* if they are all complex.

Theorem. *Let $\mathcal{O} = \mathcal{O}_S$ be a Dedekind domain of arithmetic type. Suppose $|S| = 1$ then one of the following is the case*

1. $\mathcal{O} = \mathbb{Z}$.

2. $\mathcal{O} = \mathcal{O}_d$ *the ring of integers in* $\mathbb{Q}(\sqrt{-d})$, d *a positive square free integer.*

3. $\mathcal{O} = C$, *the coordinate ring of an affine curve obtained by removing a point from a projective curve defined over a finite field.*

farther these are precisely the Dedekind domains of arithmetic type with finitely many units.

Example 1.3.1. Let $d \in \mathbb{N}$ be square free. Let $\mathcal{O}$ be the ring of integers in $\mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}$ is a Dedekind domain of arithmetic type, and by [13] theorem 11.4, $\mathcal{O}^*$ is infinite.

Chapter 2

Zimmert's Theorem

In this chapter we describe a topological method invented by Zimmert [93] and its extension due to Grunewald and Schwermer [32]. It concerns the action of $SL_2(R)$ on hyperbolic 3-space $\mathbb{H}^3$, where R is an order in an imaginary quadratic number field. See also [23] chapter 7 section 5 for a discussion of this method.

Recall that the Bianchi groups are $PSL_2(\mathcal{O}_d)$ where $\mathcal{O}_d$ is the ring of integers in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$, and recall that

$$\mathcal{O}_d = \mathbb{Z} + \omega\mathbb{Z} \text{ where } \omega = \begin{cases} \frac{1+i\sqrt{d}}{2} & \text{if } d \equiv 3 \pmod 4 \\ i\sqrt{d} & \text{else} \end{cases}$$

and where d is a positive square-free integer. Now let $m \in \mathbb{N}$ and let

$$\mathcal{O}_{d,m} = \mathbb{Z} + m\omega\mathbb{Z}$$

where ω is as above. The $\mathcal{O}_{d,m}$ are the *orders* in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$. It is clear that $\mathcal{O}_d = \mathcal{O}_{d,1}$ and that $|\mathcal{O}_d : \mathcal{O}_{d,m}| = m$. We can form the groups $SL_2(\mathcal{O}_{d,m})$. Since $m\mathcal{O}_d \subseteq \mathcal{O}_{d,m}$ we have $SL_2(\mathcal{O}_d, m\mathcal{O}_d) \leqslant SL_2(\mathcal{O}_{d,m})$ so that $SL_2(\mathcal{O}_{d,m})$ is of finite index in $SL_2(\mathcal{O}_d)$. Similar comments can be made to show that $PSL_2(\mathcal{O}_{d,m})$ is of finite index in $PSL_2(\mathcal{O}_d)$. The aim of Zimmert's method is to prove the following

Theorem. *For every d there exists m such that $SL_2(\mathcal{O}_{d,m})$ has a free non-abelian quotient.*

As $PSL_2(\mathcal{O}_{d,m}) = SL_2(\mathcal{O}_{d,m})/ < -I >$ the following theorem is clear

Theorem. *For every d there exists an m such that $PSL_2(\mathcal{O}_{d,m})$ has a free non-abelian quotient.*

We say that a group G is *SQ-Universal* if every countable group can be embedded in a quotient of G. It follows from a result of P. M. Neumann [69] and the above theorem that

Theorem. *[32] Every Bianchi group $PSL_2(\mathcal{O}_d)$ is SQ-universal.*

Thus the Bianchi groups may be considered "large" [76]. It follows from SQ-Universality that every Bianchi group has $2^{\aleph_0}$ normal subgroups [69] and it is this that is the source of the extremely complicated normal subgroup structure described in the previous chapter.

2.1 Hyperbolic 3-space

The upper half-space in Euclidean three-space gives a convenient model of 3-dimensional hyperbolic space

$$\mathbb{H}^3 = \{(z, r) \in \mathbb{C} \times \mathbb{R} : r > 0\}$$

which we equip with the hyperbolic metric

$$ds^2 = \frac{dx^2 + dy^2 + dr^2}{r^2}$$

The group $SL_2(\mathbb{C})$ acts on $\mathbb{H}^3$ in the following way. Let $M \in SL_2(\mathbb{C})$ where

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

Then

$$M(z, r) = \left(\frac{(\bar{\delta} - \bar{\gamma}\bar{z})(\alpha z - \beta) - r^2\bar{\gamma}\alpha}{\tau}, \frac{r}{\tau} \right)$$

where

$$\tau = |\gamma z - \delta|^2 + r^2|\gamma|^2$$

Under this action the hyperbolic metric is $SL_2(\mathbb{C})$-invariant. The group $SL_2(\mathbb{C})$ is generated by the matrices

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

where $a \in \mathbb{C}$. These generators operate on $\mathbb{H}^3$ in the following way

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} (z, r) = (z + a, r), \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (z, r) = \left(\frac{-\bar{z}}{|z|^2 + r^2}, \frac{r}{|z|^2 + r^2} \right).$$

2.2 Zimmert's Method

Let D be the discriminant of $\mathbb{Q}(\sqrt{-d})$. It is well known that [52]

$$D = \begin{cases} -d & \text{if } d \equiv 3 \pmod 4 \\ -4d & \text{else} \end{cases}$$

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

1. $4n^2 \leqslant m^2|D| - 3$.
2. D is a quadratic non-residue modulo all the odd prime divisors of n, and if $D \not\equiv 5 \pmod 8$ then n is odd.
3. $n > 0$, $\gcd(n, m) = 1$ and $n \neq 2$.

It is easy to prove that $Z(d, m) = \emptyset \Leftrightarrow (d, m) = (1, 1)$, or $(3, 1)$, and if $Z(d, m) \neq \emptyset$ then $1 \in Z(d, m)$. We let $r(d, m) = |Z(d, m)|$. Zimmert's theorem is

Theorem. *[32] $SL_2(\mathcal{O}_{d,m})$ has a free quotient of rank $r(d, m)$.*

Zimmert [93] proved the $m = 1$ case. We now outline the proof. Let

$$B_{d,m} = \left\{(z, r) \in \mathbb{H}^3 : \tau \geqslant 1 \ \forall \text{ coprime } \gamma, \delta \in \mathcal{O}_{d,m}\right\}$$

where, γ, δ coprime means that $\gamma\mathcal{O}_{d,m} + \delta\mathcal{O}_{d,m} = \mathcal{O}_{d,m}$, and, as before

$$\tau = |\gamma z - \delta|^2 + r^2|\gamma|^2$$

Every point of $\mathbb{H}^3$ is equivalent to a point of $B_{d,m}$ under the action of $SL_2(\mathcal{O}_{d,m})$ and so the natural map

$$B_{d,m} \longrightarrow SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3$$

is surjective. Let

$$D = \{(s_1 + s_2 m\omega, r) \in B_{d,m} : s_1, s_2 \in [0, 1]\}$$

D is a fundamental domain for $SL_2(\mathcal{O}_{d,m})$ [84, 93].

Proposition 2.2.1. *([84] Proposition 3.9) Every $h \in \mathbb{H}^3$ has a neighbourhood U such that $\sigma U \cap D \neq \emptyset$ for only finitely many $\sigma \in SL_2(\mathcal{O}_{d,m})$.*

Let $n \in Z(d,m)$, $t \in \mathbb{Z}$ such that $(n,t) = 1$. Let

$$F_{n,t} = \left\{(z,r) \in B_{d,m} : \left|\mathrm{Im}\left(z - \frac{tm\omega}{n}\right)\right| \leqslant \frac{1}{m^4|D|^2}\right\}$$

By condition 1 in the definition of the Zimmert set we have $F_{n_1,t_2} \cap F_{n_2,t_2} \neq \emptyset \Leftrightarrow n_1 = n_2$, and $t_1 = t_2$.

Lemma 2.2.2. *([93] Hilfssatz 1) Let $(z,r) \in F_{n,t}$, let $\sigma \in SL_2(\mathcal{O}_{d,m})$ such that $\sigma(z,r) = (z',r') \in B_{d,m}$. Then $\exists t' \in \mathbb{Z}$ such that* $\gcd(n,t') = 1$ *and*

$$Im\left(z - \frac{tm\omega}{n}\right) = Im\left(z' - \frac{t'm\omega}{n}\right).$$

Further

$$r \geqslant \frac{5}{2m^2|D|}$$

Now for each $n \in Z(d,m)$ define $\varphi_n : B_{d,m} \to S^1$, where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, by

$$\varphi_n(z,r) = \begin{cases} 1 & \text{if } (z,r) \notin \bigcup_{(n,t)=1} F_{n,t} \\ exp2\pi i\left(\frac{1}{2} + \frac{m^4|D|^2}{2} Im\left(z - \frac{tm\omega}{n}\right)\right) & \text{if } (z,r) \in F_{n,t} \end{cases}$$

There is a unique factorization of φ_n over $SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3$ by a continuous map

$$f_n : SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3 \longrightarrow S^1$$

This is well defined by lemma (2.2.2) and continuous by proposition (2.2.1). Suppose that $Z(d,m) = \{n_1, \ldots, n_r\}$. Let Y denote the one point union of $r(d,m)$ copies of S^1 with base point 1 ie

$$Y = \left\{(z_1, \ldots, z_r) \in S^1 \times \cdots \times S^1 : z_i \neq 1 \text{ for at most one } i\right\}$$

Now define

$$f : SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3 \longrightarrow Y$$

by

$$(z,r) \longmapsto (f_1(z,r), \ldots, f_r(z,r))$$

where f_i denotes f_{n_i}. Now f induces a homomorphism

$$f_* : \pi_1\left(SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3\right) \longrightarrow \pi_1(Y,1)$$

Now let $g \in SL_2(\mathcal{O}_{d,m})$ and let $h_0 \in \mathbb{H}^3$. Let P be any path from h_0 to gh_0. The image of P in $SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3$ is a loop and therefore represents some $\alpha_g \in \pi_1\left(SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3\right)$. Define

$$\theta : SL_2(\mathcal{O}_{d,m}) \longrightarrow \pi_1\left(SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3\right)$$

by $g \mapsto \alpha_g$. This map is well defined. We now have

$$\sigma : SL_2(\mathcal{O}_{d,m}) \longrightarrow \pi_1\left(SL_2(\mathcal{O}_{d,m})\backslash\mathbb{H}^3\right) \longrightarrow \pi_1(Y) \cong F_r$$

where $r = r(d,m)$. Now consider the natural map

$$\psi : F_r \twoheadrightarrow \mathbb{Z}^r$$

Zimmert shows ([93] Satz $2(i)$) that $\sigma\psi$ is surjective. So $1 \neq \text{im}\sigma \leqslant F_r$, also $SL_2(\mathcal{O}_{d,m})$ is finitely generated, so imσ is a free group of rank s, where $r \leqslant s < \infty$ and so maps onto a free group of rank r. Thus

Theorem 2.2.3. *$SL_2(\mathcal{O}_{d,m})$ maps onto a free group of rank $r(d,m)$.*

so clearly

Theorem 2.2.4. *$PSL_2(\mathcal{O}_{d,m})$ maps onto a free group of rank $r(d,m)$.*

2.3 Explicit result about the free generators

We have just seen that

$$\sigma : SL_2(\mathcal{O}_{d,m}) \twoheadrightarrow \pi_1(Y) \cong F_r$$

where r is the order of the Zimmert Set.

Lemma 2.3.1. *The image, under σ, of the matrix*

$$U = \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix}$$

can be taken as a free generator of $\pi_1(Y)$.

Proof. Let $z_0 = \frac{-i}{m^4|D|^2}, z_1 = z_0 + m\omega$, and let $h_i = (z_i, 1)$. So $uh_0 = h_1$. Now define a path P from h_0 to h_1 by $P = \{(z(s), 1) : s \in [0,1]\}$, where $z(s) = (1-s)z_0 + sz_1 = z_0 + sm\omega$. Now

$$P \cap \left(\bigcup_{t \in \mathbb{Z}} F_{1,t} \right) = (P \cap F_{1,0}) \cup \{h_1\}$$

and $h_1 \in F_{1,1}$. So $f_1(P) = S^1$. Now recall that

$$Y = \left\{ (z_1, \ldots, z_r) \in S^1 \times \cdots \times S^1 : z_i \neq 1 \text{ for at most one } i \right\}$$

Let S_i^1 denote the i^{th} circle of Y. Then S_i^1 gives rise to $g_i \in \pi_1(Y)$ and $\{g_1, \ldots, g_r\}$ is a set of free generators of $\pi_1(Y) \cong F_r$. So

$$f_*(\sigma(u)) = g_1 g_0 = x$$

where $g_0 \in < g_2, \ldots, g_r >$. By Tietze transformations we can take $\{x, g_2, \ldots, g_r\}$ to be a set of free generators of $\pi_1(Y)$, as required. □

Lemma 2.3.2. *$\sigma(u)$ is a free generator of imσ.*

Proof. Clearly $\sigma(u) \in \text{im}\sigma$. We can then apply Proposition 2.10 on page 8 of [48] to get the result. □

2.4 Unipotent matrices

Let R be any commutative ring with a one. Recall that a matrix $M \in GL_2(R)$ is *unipotent* if $(M - I)^2 = 0$. Let $U_2(R)$ denote the normal subgroup of $SL_2(R)$ generated by the unipotent matrices. Clearly $E_2(R) \leqslant U_2(R)$ and so $NE_2(R)$, the *normal* subgroup generated by the elementary matrices is contained in $U_2(R)$.

Lemma 2.4.1. *Let $M \in GL_2(R)$. Then*

$$\begin{aligned} M \textit{ is unipotent } &\Leftrightarrow \det M = 1 \textit{ and } trM = 2 \\ &\Leftrightarrow M = \begin{pmatrix} 1+\alpha & \gamma \\ \beta & 1-\alpha \end{pmatrix} \textit{ where } \alpha^2 + \beta\gamma = 0, \alpha, \beta, \gamma \in R. \end{aligned}$$

Proof. Let

$$I \neq M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R)$$

be unipotent. Let $t = \mathrm{tr} M = a + d$. Then

$$0 = (M - I)^2 = \begin{pmatrix} (a-1)^2 + bc & b(t-2) \\ c(t-2) & (d-1)^2 + bc \end{pmatrix}$$

Now suppose that $t \neq 2$, so $b = c = 0$, so $(a-1)^2 + bc = (a-1)^2 = 0$, so $a = 1$, similarly $d = 1$, so $M = I$. Contradiction. So $t = 2$, and $d = 2 - a$, so $\det M = a(2-a) - bc = -(a^2 - 2a + 1) + 1 - bc = -((a-1)^2 + bc) + 1 = 1$.

Conversely suppose that $\det M = 1$ and $\mathrm{tr} M = 2$. So

$$M = \begin{pmatrix} a & b \\ c & 2-a \end{pmatrix}$$

so

$$(M - I)^2 = \begin{pmatrix} (a-1)^2 + bc & 0 \\ 0 & (1-a)^2 + bc \end{pmatrix}$$

and $(a-1)^2 + bc = a^2 - 2a + 1 - bc = -(a(2-a) - bc) + 1 = -1 + 1 = 0$. So M is unipotent.

Now suppose that $\det M = 1$ and $\mathrm{tr}\ M = 2$. It is clear that M can be written in the form

$$\begin{pmatrix} 1+\alpha & \gamma \\ \beta & 1-\alpha \end{pmatrix}$$

where $\alpha^2 + \beta\gamma = 0$, some $\alpha, \beta, \gamma \in R$. So conversely suppose that M is of this form. Then

$$(M - I)^2 = \begin{pmatrix} \alpha^2 + \beta\gamma & \alpha\gamma - \alpha\gamma \\ \alpha\beta - \alpha\beta & \alpha^2 + \beta\gamma \end{pmatrix} = 0$$

so M is unipotent. □

Lemma 2.4.2. *Let $\delta \in R$. Then every conjugate of*

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

in $SL_2(R)$ is unipotent.

Proof.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 - ac\delta & a^2\delta \\ -c^2\delta & 1 + ac\delta \end{pmatrix}$$

□

Lemma 2.4.3. *Suppose that R is an integral domain and let $\alpha, \beta \in R$ then $\alpha R + \beta R$ is principal if and only if $\exists \alpha', \beta' \in R$ such that α', and β' are coprime and $\alpha\alpha' + \beta\beta' = 0$.*

Proof. Suppose first that $\alpha R + \beta R = \delta R$. So $\alpha = \delta r_1$, $\beta = \delta r_2$, $\delta = \alpha r_3 + \beta r_4$, where $r_i \in R$, $i = 1, 2, 3, 4$. So $\delta = \delta(r_1 r_3 + r_2 r_4)$, and because R is an integral domain and $\delta \neq 0$, we have $r_1 r_3 + r_2 r_4 = 1$. Let $\alpha' = r_2$, and $\beta' = -r_1$. So α', and β' are coprime, and $\alpha\alpha' + \beta\beta' = 0$.

Conversely suppose that $\exists$ coprime $\alpha', \beta' \in R$ such that $\alpha\alpha' + \beta\beta' = 0$. Now $\alpha\alpha' = -\beta\beta'$, and α' and β' are coprime, so $\alpha = \beta'\beta''$, and $\beta = \alpha'\alpha''$. So $0 = \alpha\alpha' + \beta\beta' = \alpha'\beta'(\alpha'' + \beta'')$, and as R is an integral domain and $\alpha' \neq 0 \neq \beta'$ we have $\alpha'' = -\beta''$. So $\alpha R + \beta R = \beta'\beta'' R + \alpha'\alpha'' R = \alpha''(\alpha' R + \beta' R) = \alpha'' R$. □

Lemma 2.4.4. *Suppose that R is an integral domain and let*

$$M = \begin{pmatrix} 1+\alpha & \gamma \\ \beta & 1-\alpha \end{pmatrix}$$

be unipotent. Then M is conjugate in $SL_2(R)$ to

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

if and only if $\alpha R + \beta R$ is principal.

Proof. Suppose that

$$\begin{pmatrix} 1+ac\delta & a^2\delta \\ -c^2\delta & 1-ac\delta \end{pmatrix} = \begin{pmatrix} 1+\alpha & \gamma \\ \beta & 1-\alpha \end{pmatrix}.$$

So $\alpha = ac\delta$, $\beta = -c^2\delta$, $\gamma = a^2\delta$. Clearly $\alpha R + \beta R \subseteq c\delta R$. Now let $x \in R$ and consider $c\delta x$.

$$\begin{aligned} c\delta x &= c\delta x(ad - bc) && \text{as } ad - bc = 1 \\ &= ac\delta xd - c^2\delta bx \\ &= \alpha xd + \beta bx && \text{as } \alpha = ac\delta, \beta = -c^2\delta \\ &\in \alpha R + \beta R \end{aligned}$$

So $\alpha R + \beta R = \delta c R$, ie is a principal ideal.

Conversely suppose that $\alpha R + \beta R$ is principal. Now

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1+\alpha & \gamma \\ \beta & 1-\alpha \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} =$$

$$\begin{pmatrix} 1+\frac{1}{\beta}(a\alpha+b\beta)(c\alpha+d\beta) & \frac{-1}{\beta}(a\alpha+b\beta)^2 \\ \frac{1}{\beta}(c\alpha+d\beta)^2 & \frac{-1}{\beta}(a\alpha+b\beta)(c\alpha+d\beta) \end{pmatrix} = Y$$

and $\alpha R+\beta R$ is principal so, by (2.4.3), $\exists \alpha', \beta' \in R$ such that α', and β' are coprime and $\alpha'\alpha+\beta'\beta=0$. Let $c=\alpha'$, and $d=\beta'$ so $\exists a, b$ such that $ad-bc=1$ and $c\alpha+d\beta=0$, so

$$Y = \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}$$

where $\delta = \frac{-1}{\beta}(a\alpha+b\beta)^2$. □

Having set out the basics that we require in the context of an arbitrary commutative ring we now turn to the case where $R = \mathcal{O}_{d,m}$ is an order in an imaginary quadratic number field. Let r be the order of the Zimmert Set and

$$\sigma : SL_2(\mathcal{O}_{d,m}) \longrightarrow F_r$$

be the map given in the previous section. Let $K = \ker \sigma$.

Lemma 2.4.5. *([93] Hilfssatz 2) Let $\mathcal{O} = \mathcal{O}_{d,m}$ and let $M \in SL_2(\mathcal{O})$, and $\alpha, \beta \in \mathcal{O}$ such that $\alpha\mathcal{O}+\beta\mathcal{O}$ is not a principal ideal. Let $\epsilon, t \in \mathbb{R}$ such that $0 < \epsilon \leqslant 1$, and $|t| \leqslant \epsilon$. Let*

$$h' = (z, r) = \left(\frac{-\alpha+t}{\beta}, \frac{1}{|\beta|}\sqrt{2\epsilon-\epsilon^2} \right)$$

and suppose that $Mh' = (z', r')$. Then

$$r' \leqslant |\beta|\sqrt{2\epsilon-\epsilon^2}$$

Proof. Suppose that

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

so $r' = r/\tau$, where $\tau = |cz-d|^2 + r^2|c|^2$. Now

$$\tau = \left| c\frac{-\alpha+t}{\beta} - d \right|^2 + \left(\frac{1}{|\beta|}\sqrt{2\epsilon-\epsilon^2} \right)^2 |c|^2 \geqslant \frac{1}{|\beta|^2}$$

For equivalently

$$|(c-\alpha-\beta d)+ct|^2+\left(2\epsilon-\epsilon^2\right)|c|^2\geqslant 1$$

Now c and d are coprime and $\beta\mathcal{O}+\alpha\mathcal{O}$ is not a principal ideal so, by (2.4.3), $0\neq -c\alpha-\beta d\in\mathcal{O}$, so $|-c\alpha-\beta d|\geqslant 1$. Thus

$$|(-c\alpha-\beta d)+ct|^2+\left(2\epsilon-\epsilon^2\right)|c|^2\geqslant(1-|ct|)^2+\left(2\epsilon-\epsilon^2\right)|c|^2$$

Suppose that $|ct|\geqslant 1$. Clearly $(1-|ct|)^2\geqslant 0$. Also $|c|\geqslant 1/|t|\geqslant 1/\epsilon$ and so $(2\epsilon-\epsilon^2)|c|^2=\left(\frac{2}{\epsilon}-1\right)|c|^2\epsilon^2\geqslant\frac{2}{\epsilon}-1\geqslant 1$. Now suppose that $|ct|\leqslant 1$. First of all observe that $2\epsilon-\epsilon^2\geqslant 2|t|-|t|^2\Leftrightarrow(\epsilon-|t|)(2-\epsilon-|t|)\geqslant 0$, and as $0<|t|\leqslant\epsilon\leqslant 1$, this is true, so $2\epsilon-\epsilon^2\geqslant 2|t|-|t|^2$. Now

$$\begin{aligned}(1-|ct|)^2+(2\epsilon-\epsilon^2)|c|^2=1-2|ct|+|ct|^2+(2\epsilon-\epsilon^2)|c|^2\geqslant 1\\ \Leftrightarrow |ct|^2-2|ct|+(2\epsilon-\epsilon^2)|c|^2\geqslant 0\end{aligned}$$

Now if $|c|=0$ then this is certainly true, so suppose that $|c|\neq 0$, so as $c\in\mathcal{O}$ we have $|c|\geqslant 1$. Now

$$\begin{aligned}&|ct|^2-2|ct|+(2\epsilon-\epsilon^2)|c|^2\\ =&|c|\left(|c||t|^2-2|t|+(2\epsilon-\epsilon^2)|c|\right)\\ \geqslant&|c|\left(|c||t|^2-2|t|+(2|t|-|t|^2)|c|\right)\\ =&2|c||t|(|c|-1)\geqslant 0.\end{aligned}$$

So $r'=r/\tau\leqslant|\beta|^2(1/|\beta|)\sqrt{2\epsilon-\epsilon^2}=|\beta|\sqrt{2\epsilon-\epsilon^2}$. □

Theorem 2.4.6. *([93] Satz 2(ii)) Let $\alpha,\beta,\gamma\in\mathcal{O}_{d,m}$ such that $\alpha^2+\beta\gamma=0$ and $\alpha\mathcal{O}_{d,m}+\beta\mathcal{O}_{d,m}$ is not principal. Then*

$$M=\begin{pmatrix}1+\alpha & \gamma\\ \beta & 1+\alpha\end{pmatrix}\in K$$

Proof. Let $\epsilon\in\mathbb{R}$ and let

$$h_1=(z_1,r_1)=\left(\frac{-\alpha+\epsilon}{\beta},\frac{1}{|\beta|}\sqrt{2\epsilon-\epsilon^2}\right)$$

and suppose that $Mh_1 = h_2 = (z_2, r_2)$. Now

$$\begin{aligned}\tau &= \left|\beta\frac{-\alpha+\epsilon}{\beta} - (1-\alpha)\right|^2 + \frac{1}{|\beta|^2}\left(2\epsilon-\epsilon^2\right)|\beta|^2 \\ &= |-\alpha+\epsilon-1+\alpha|^2 + 2\epsilon-\epsilon^2 \\ &= (\epsilon-1)^2 + 2\epsilon - \epsilon^2 \\ &= 1\end{aligned}$$

So $r_2 = r_1$, and

$$z_2 = \left(\overline{1-\alpha} - \overline{\beta}\frac{\overline{-\alpha+\epsilon}}{\overline{\beta}}\right)\left((1+\alpha)\frac{-\alpha+\epsilon}{\beta} + \frac{\alpha^2}{\beta}\right) - \frac{1}{|\beta|}\left(2\epsilon-\epsilon^2\right)\overline{\beta}(1+\alpha)$$

After some algebraic manipulation we see that

$$z_2 = \frac{-\alpha-\epsilon}{\beta}$$

so

$$h_2 = \left(\frac{-\alpha-\epsilon}{\beta}, \frac{1}{|\beta|}\sqrt{2\epsilon-\epsilon^2}\right)$$

Now let

$$P = \left\{h' = \left(\frac{-\alpha+t}{\beta}, \frac{1}{|\beta|}\sqrt{2\epsilon-\epsilon^2}\right) \in \mathbb{H}^3 : t \in \mathbb{R}, -\epsilon \leqslant t \leqslant \epsilon\right\}$$

so P is a path in $\mathbb{H}^3$ from h_1 to h_2. Let $h' \in P$ and $M_2 \in SL_2(\mathcal{O})$. Then, by (2.4.5), if $M_2h' = (z', r')$ we have $r' \leqslant |\beta|\sqrt{2\epsilon-\epsilon^2}$. Now choose ϵ so that $|\beta|\sqrt{2\epsilon-\epsilon^2} < 5/(2m^2|D|)$. So, by (2.2.2), $M_2h' \notin F_{n,t}$ for every $n \in Z(d,m)$ and $t \in \mathbb{Z}$ coprime to n. Thus $\varphi_n(h') = 1$ and it follows that M is in the kernel of the Zimmert map. □

Theorem 2.4.7. *With the above notation, there exists an epimorphism*

$$\tau : \frac{SL_2(\mathcal{O}_{d,m})}{U_2(\mathcal{O}_{d,m})} \longrightarrow F_s$$

where $s = r - 1$.

Proof. We have already seen, in the previous section that $SL_2(\mathcal{O}_{d,m})$ has a free quotient of rank $s+1$ where

$$U = \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix}$$

can be taken as a free generator. Now consider a unipotent matrix

$$M = \begin{pmatrix} 1+\alpha & \gamma \\ \beta & 1-\alpha \end{pmatrix}$$

where $\alpha^2 + \beta\gamma = 0$. Now either $\alpha R + \beta R$ is principal or it isn't. If it is not principal then, by theorem (2.4.6), $M \in K$. If $\alpha R + \beta R$ is principal then, by lemma (2.4.4), M is conjugate, in $SL_2(\mathcal{O}_{d,m})$ to

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

for some $\delta \in \mathcal{O}_{d,m}$. Now$\delta = z_1 + m\omega z_2$, $z_i \in \mathbb{Z}$, but $T \in SL_2(\mathbb{Z}) \leqslant K$, so we can suppose that M is conjugate to some power of U. So either M is in the kernel of the map $SL_2(\mathcal{O}_{d,m}) \twoheadrightarrow F_r$ or it is conjugate to a power of U, which can be taken as a free generator of F_r. So clearly

$$\frac{SL_2(\mathcal{O}_{d,m})}{U_2(\mathcal{O}_{d,m})} \twoheadrightarrow \frac{< u, x_2, \ldots, x_r; >}{< u >} \cong < x_2, \ldots x_r; > = F_s$$

□

Corollary 2.4.8.

$$\frac{SL_2(\mathcal{O}_{d,m})}{NE_2(\mathcal{O}_{d,m})}$$

has a free quotient of rank $s = r - 1$.

Let R be any commutative ring and let $\mathfrak{q} \lhd R$. Then let

$$SL_n(R, \mathfrak{q}) = \ker(SL_n(R) \to SL_n(R/\mathfrak{q}))$$

and let $U_n(R, \mathfrak{q})$ be the normal subgroup of $SL_n(R)$ generated by all unipotent matrices in $SL_n(R, \mathfrak{q})$, let $E_n(R, \mathfrak{q})$ denote the normal subgroup of $E_n(R)$ generated by all $\mathfrak{q}$ elementary matrices and $NE_n(R, \mathfrak{q})$ denote the normal subgroup of $SL_n(R)$ generated by $\mathfrak{q}$ elementary matrices.

Corollary 2.4.9. *Let* $0 \neq \mathfrak{q} \lhd \mathcal{O}_{d,m}$. *Then*

$$\frac{SL_2(\mathcal{O}_{d,m}, \mathfrak{q})}{U_2(\mathcal{O}_{d,m}, \mathfrak{q})}$$

has a free quotient of rank $s = r - 1$.

Proof. Now

$$SL_2(\mathcal{O}_{d,m},\mathfrak{q})U_2(\mathcal{O}_{d,m}) \geqslant SL_2(\mathcal{O}_{d,m},\mathfrak{q})E_2(\mathcal{O}_{d,m}) = SL_2(\mathcal{O}_{d,m})$$

so

$$\frac{SL_2(\mathcal{O}_{d,m},\mathfrak{q})}{U_2(\mathcal{O}_{d,m}) \cap SL_2(\mathcal{O}_{d,m},\mathfrak{q})} \cong \frac{SL_2(\mathcal{O}_{d,m})}{U_2(\mathcal{O}_{d,m})} \twoheadrightarrow F_s$$

thus

$$\frac{SL_2(\mathcal{O}_{d,m},\mathfrak{q})}{U_2(\mathcal{O}_{d,m},\mathfrak{q})} \twoheadrightarrow F_s$$

□

2.5 Computation of Zimmert Sets

Given the definition of the Zimmert Set $Z(d,m)$ it is a simple matter to write a computer program to calculate any Zimmert Set. We have written such a program in GAP [24]. Since we are interested in free non-abelian quotients it would be useful to know values of (d,m) such that $r(d,m) \leqslant 1$. Consider first the Zimmert sets $Z(d,1)$ which we denote $Z(d)$, let $r(d) = r(d,1)$. Mason, Odoni and Stothers [61] have proved

Theorem. *For all but finitely many d* $r(d) \geqslant 2$.

Obviously we would like a list of the d such that $r(d) = 1$. By means of a computer search Mason et al [61] establish that up to 2×10^{13} the only values of d for which $r(d) = 1$ are: 2, 5, 6, 7, 11, 14, 15, 17, 19, 21, 23, 26, 29, 30, 31, 35, 39, 41, 47, 51, 59, 66, 69, 71, 87, 89, 95, 101, 105, 110, 111, 119, 129, 159, 161, 191, 194, 209, 215, 230, 231, 255, 285, 311, 321, 335, 341, 374, 399, 426, 455, 479, 546, 591, 615, 671, 831, 959, 1095, 1119, 1239, 2415 and they conjecture that these are the only values of d for which $r(d) = 1$. Recall that $r(1) = r(3) = 0$.

We extended this work by using our computer program to calculate pairs (d,m) such that $r(d,m) = 1$. For every square free $d \in \mathbb{N}$ and every $m \in \mathbb{N}$ we checked every pair (d,m) such that $m^2|D| \leqslant 10^7$ and found 104 pairs (d,m) such that $r(d,m) = 1$. Excluding those mentioned above these are : $(1,2)$, $(1,3)$, $(1,6)$, $(2,2)$, $(2,3)$, $(3,2)$, $(3,3)$, $(3,4)$, $(3,10)$, $(5,2)$, $(5,3)$, $(5,4)$, $(6,2)$, $(6,3)$, $(6,4)$, $(6,5)$, $(7,2)$, $(7,3)$, $(10,3)$, $(11,2)$, $(11,4)$, $(14,2)$, $(15,2)$, $(15,3)$, $(21,2)$, $(23,2)$, $(26,2)$, $(31,3)$, $(35,2)$, $(35,4)$, $(35,6)$, $(39,2)$, (41, 2), (55, 3), (59, 2), (66, 2), (111, 2), (119, 2), (131, 2), (195, 2), (231, 2), (341, 2). Notice that, perhaps surprisingly, $r(d,1) > 1$ does not imply $r(d,m) > 1$, for $m > 1$; for example $r(10,1) = 2$, yet $r(10,3) = 1$. It seems very reasonable to make the following

Conjecture. The only pairs (d,m) such that $r(d,m) = 1$ are those listed above.

It can be seen from the data above that for most d such that $r(d) = 1$, $r(d,2) > 1$, so that Zimmert's theorem only just fails to give a free non-abelian quotient. However Zimmert's theorem is not best possible; for $r(5) = 1$ yet $PSL_2(\mathcal{O}_5)$ has a free quotient of rank 2. With this in mind make the following

Definition. Let $\rho(d,m)$ be the largest rank of a free quotient of $SL_2(\mathcal{O}_{d,m})$.

$\rho(d,m)$ is well defined as $PSL_2(\mathcal{O}_{d,m})$ is finitely generated. Let $\rho(d) = \rho(d,1)$. Clearly $\rho(d,m) \geqslant r(d,m)$. If we have a presentation for $PSL_2(\mathcal{O}_{d,m})$ we can compute $\rho(d,m)$:

Theorem. *([61] theorem 6, and [78])*

$\rho(d)$	0	1	2	3	5	7	8
d	1, 3	2, 7, 11, 19	5, 6, 15, 43	10, 13, 67	22	21, 163	37

Mason et al [61] have the following

Conjecture. $\rho(d) > 1$ for all $d > 19$.

We have no reason to doubt this. The only square free $d \leqslant 19$ missing from the above are 14, and 17, we partially close this gap

Proposition 2.5.1. $4 \leqslant \rho(14) \leqslant 5$

Proof. The following presentation for $PSL_2(\mathcal{O}_{14})$ can be found in [30] Proposition 3.5.

$$\begin{aligned} < g_1, g_2, g_3, g_4, g_5, g_6, g_7 \,;\, & g_1^2, (g_1g_2)^3, g_1g_3g_1^{-1}g_3^{-1}, g_2g_4g_2^{-1}g_4^{-1}, \\ & g_5g_6^{-1}g_7g_3^{-1}g_6g_5^{-1}g_3g_7^{-1}, g_6g_4g_1g_3^{-1}g_6g_1g_6^{-1}g_3g_4^{-1}g_1g_6^{-1}g_1, \\ & g_1g_6g_1g_2g_6^{-1}g_1g_6^{-1}g_3g_1g_2^{-1}g_3^{-1}g_6, \\ & g_2^{-1}g_7^{-1}g_6g_2^{-1}g_1g_6^{-1}g_1g_5g_2g_6^{-1}g_7g_2g_1g_3^{-1}g_6g_1g_5^{-1}g_3 > \end{aligned}$$

From this it is easy to compute that $PSL_2(\mathcal{O}_{14})^{ab} \cong \mathbb{Z}_6 \times \mathbb{Z}^5$, and so $\rho(14) \leqslant 5$. It is also easy to see that by setting $g_1 = g_2 = g_5g_6^{-1} = 1$ we get the free group of rank 4. So $\rho(14) \geqslant 4$. □

Proposition 2.5.2. $\rho(1,2) = \rho(3,2) = 1$.

Proof. We have the following presentations from (3.5.1) and (3.3.1)

$$PSL_2(\mathcal{O}_{1,2}) =< a, t, z, w; a^2, z^2, (at)^3, (atz)^2, [t, w], (atw^{-1}zw)^2 >$$

$$PSL_2(\mathcal{O}_{3,2}) =< a, t, w; a^2, (at)^3, (w^{-1}awa)^3, [t, w] >$$

from which it is easy to see $PSL_2(\mathcal{O}_{1,2})^{ab} = \mathbb{Z}_2 \times \mathbb{Z}$, and $PSL_2(\mathcal{O}_{3,2})^{ab} = \mathbb{Z}_6 \times \mathbb{Z}$. So $\rho(1,2) = \rho(3,2) = 1$. □

Proposition 2.5.3. $\rho(7,2) = 2$.

Proof. We have from section (3.5)

$$PSL_2(\mathcal{O}_{7,2}) =< a, t, w, x, y \,;\, a^2, x^2, [t, w], (ax)^3, (at)^3, y = txyxt^{-1}, (ytay^{-1}x)^2,$$
$$xyat^{-1}y^{-1}wt^{-1}aw^{-1}t >$$

Now suppose that $PSL_2(\mathcal{O}_{7,2})/N$ is free then N contains the normal closure of all elements in $PSL_2(\mathcal{O}_{7,2})$ of finite order, so $N(a, x, t) \leqslant N$. It is easy to calculate that $PSL_2(\mathcal{O}_{7,2})/N(a, x, t) \cong F_2$. So $\rho(7,2) = 2$. □

Proposition 2.5.4. $3 \leqslant \rho(11,2) \leqslant 4$.

Proof. We have from section (3.5)

$$PSL_2(\mathcal{O}_{11,2}) =< a, t, w, k, l, m, n \,;\, a^2, k^2, [m, n], [t, w], (at)^3, tklkt^{-1}l^{-1},$$
$$km^{-1}ltat^{-1}l^{-1}m, nlat^{-1}l^{-1}n^{-1}mwaw^{-1}tm^{-1},$$
$$m^{-1}tklt^{-1}l^{-1}mwt^{-1}aw^{-1}t >$$

so the kernel of a free quotient of $PSL_2(\mathcal{O}_{11,2})$ must contain a, k, t. It is easy to compute that $PSL_2(\mathcal{O}_{11,2})/N(a, k, t) =< z, l, m, n; [m, n] >$. This maps onto the free group of rank 3, so $\rho(11,2) \geqslant 3$, and it abelianization is $\mathbb{Z}^4$ so $\rho(11,2) \leqslant 4$. □

Given the evidence presented above it seems reasonable to make the following

Conjecture. The only values of (d, m) for which $PSL_2(\mathcal{O}_{d,m})$ does not have a free non-abelian quotient are: $(1,1)$, $(1,2)$, $(2,1)$, $(3,1)$, $(3,2)$, $(7,1)$, $(11,1)$, $(19,1)$.

There are results later on in this thesis which depend on the fact that $PSL_2(\mathcal{O}_{d,m})$ has a free non-abelian quotient. Usually we then attempt to deal with the cases mentioned in the conjecture. We are quite certain that the conjecture is true and so the idea is that we have a proved a theorem (or a version of it) for all Bianchi groups. For example it is not yet proven that $PSL_2(\mathcal{O}_{2,2})$ has a free non-abelian quotient, so strictly speaking our theorem which depends on $PSL_2(\mathcal{O}_{d,m})$ having a free non-abelian quotient has not been proved for $PSL_2(\mathcal{O}_{2,2})$, although we are quite certain that it is true and all that is required is a presentation of $PSL_2(\mathcal{O}_{2,2})$ to verify it. Contrast this with $PSL_2(\mathcal{O}_2)$ where a slightly different technique may be required or with $PSL_2(\mathcal{O}_3)$ where a radically different technique is perhaps needed. For this reason we do not consider $PSL_2(\mathcal{O}_{2,2})$ to be a "true" exception and we refer to the pairs mentioned in the conjecture as the "true exceptions". The conjecture could (and probably will) be proved by means of a computer search. See the comments at the end of section (3.5).

Recall theorem (2.4.7). To get a free non-abelian quotient we require that $r(d,m) \geqslant 3$. In exactly the same way as above we have used our `GAP` [24] program to get a list of pairs (d,m) such that $r(d,m) = 2$. Again for every square free $d \in \mathbb{N}$ and every $m \in \mathbb{N}$ we checked every pair (d,m) such that $m^2|D| \leqslant 10^7$ and found 215 pairs (d,m) such that $r(d,m) = 2$. These are: $(1,4)$, $(1,5)$, $(1,7)$, $(1,9)$, $(2,4)$, $(2,5)$, $(2,7)$, $(3,5)$, $(3,6)$, $(3,8)$, $(3,12)$, $(5,5)$, $(6,6)$, $(7,5)$, $(7,6)$, $(7,9)$, $(10,1)$, $(10,2)$, $(10,6)$, $(10,9)$, $(11,3)$, $(11,6)$, $(13,1)$, $(13,3)$, $(13,6)$, $(14,3)$, $(14,4)$, $(15,4)$, $(15,5)$, $(17,2)$, $(17,3)$, $(17,4)$, $(17,5)$, $(19,2)$, $(19,3)$, $(19,4)$, $(19,6)$, $(19,12)$, $(21,3)$, $(21,4)$, $(21,5)$, $(21,6)$, $(22,1)$, $(26,3)$, $(29,2)$, $(29,3)$, $(30,2)$, $(30,3)$, $(30,7)$, $(31,2)$, $(33,1)$, $(33,2)$, $(33,5)$, $(34,1)$, $(38,1)$, $(38,5)$, $(39,3)$, $(39,4)$, $(39,5)$, $(41,1)$, $(43,1)$, $(46,1)$, $(47,2)$, $(47,3)$, $(51,2)$, $(51,4)$, $(51,6)$, $(51,8)$, $(55,1)$, $(55,2)$, $(55,6)$, $(61,1)$, $(62,1)$, $(62,2)$, $(65,1)$, $(65,2)$, $(66,3)$, $(69,2)$, $(69,3)$, $(70,1)$, $(71,2)$, $(74,1)$, $(77,1)$, $(77,2)$, $(79,1)$, $(79,3)$, $(83,1)$, $(83,2)$, $(86,1)$, $(87,2)$, $(87,3)$, $(87,4)$, $(94,3)$, $(95,2)$, $(95,3)$, $(101,2)$, $(105,2)$, $(110,2)$, $(114,1)$, $(129,2)$, $(131,1)$, $(134,1)$, $(138,1)$, $(143,1)$, $(143,2)$, $(145,3)$, $(146,1)$, $(149,1)$, $(151,1)$, $(155,1)$, $(159,2)$, $(165,1)$, $(167,1)$, $(167,2)$, $(173,1)$, $(179,1)$, $(182,1)$, $(183,1)$, $(185,1)$, $(186,1)$, $(195,1)$, $(195,4)$, $(199,1)$, $(206,1)$, $(215,2)$, $(222,1)$, $(230,2)$, $(231,3)$, $(237,1)$, $(239,1)$, $(251,1)$, $(251,2)$, $(255,2)$, $(266,1)$, $(269,1)$, $(271,1)$, $(285,2)$, $(287,1)$, $(290,1)$, $(299,2)$, $(314,1)$, $(327,1)$, $(329,1)$, $(339,2)$, $(359,1)$, $(383,1)$, $(390,1)$, $(395,2)$, $(399,2)$, $(431,1)$, $(446,1)$, $(447,1)$, $(455,2)$, $(458,1)$, $(471,1)$, $(494,1)$, $(497,1)$, $(503,1)$, $(506,1)$,

$(519,1)$, $(545,1)$, $(551,1)$, $(563,2)$, $(569,1)$, $(623,1)$, $(654,1)$, $(659,2)$, $(689,1)$, $(699,2)$, $(705,1)$, $(719,1)$, $(755,2)$, $(759,1)$, $(770,1)$, $(789,1)$, $(791,1)$, $(815,1)$, $(831,2)$, $(854,1)$, $(887,1)$, $(935,1)$, $(1031,1)$, $(1055,1)$, $(1151,1)$, $(1169,1)$, $(1190,1)$, $(1199,1)$, $(1209,1)$, $(1223,1)$, $(1271,1)$, $(1326,1)$, $(1335,1)$, $(1407,1)$, $(1511,1)$, $(1551,1)$, $(1599,1)$, $(1751,1)$, $(1767,1)$, $(1823,1)$, $(1895,1)$, $(1959,1)$, $(1991,1)$, $(2015,1)$, $(2159,1)$, $(2435,2)$, $(2639,1)$, $(2679,1)$, $(2735,1)$, $(3119,1)$, $(3311,1)$, $(3471,1)$, $(4479,1)$, $(6215,1)$, $(6815,1)$, $(8655,1)$. Again it seems reasonable to make the following

Conjecture. The only pairs (d,m) such that $r(d,m)=2$ are those listed above.

Chapter 3

The groups $PSL_2(\mathcal{O}_{d,m})$

In chapter two we saw that almost all of the groups $PSL_2(\mathcal{O}_{d,m})$ had a free non-abelian quotient. In this chapter we take a closer look at these groups. For completeness we restate the definition.

Let $m, d \in \mathbb{N}$, d square-free then the orders in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$ are

$$\mathcal{O}_{d,m} = \mathbb{Z} + m\omega\mathbb{Z} \text{ where } \omega = \begin{cases} \frac{1+i\sqrt{d}}{2} & \text{if } d \equiv 3 \pmod 4 \\ i\sqrt{d} & \text{else} \end{cases}$$

The maximal order $\mathcal{O}_{d,1}$ is the ring of integers in $\mathbb{Q}(\sqrt{-d})$ and is denoted $\mathcal{O}_d$. $\mid \mathcal{O}_d : \mathcal{O}_{d,m} \mid = m$. We are considering the groups $PSL_2(\mathcal{O}_{d,m})$. Since $m\mathcal{O}_d \subseteq \mathcal{O}_{d,m}$, we have $PSL_2(\mathcal{O}_d, m\mathcal{O}_d) \leqslant PSL_2(\mathcal{O}_{d,m})$, so $PSL_2(\mathcal{O}_{d,m})$ is of finite index in $PSL_2(\mathcal{O}_d)$. We now compute this index.

3.1 Computation of $|PSL_2(\mathcal{O}_d) : PSL_2(\mathcal{O}_{d,m})|$

First observe that

$$|PSL_2(\mathcal{O}_d) : PSL_2(\mathcal{O}_{d,m})| = |PSL_2(\mathcal{O}_d) : PSL_2(\mathcal{O}_{d,p_1})| \dots |PSL_2(\mathcal{O}_{d,p_1 \dots p_{r-1}}) : PSL_2(\mathcal{O}_{d,m})|$$

where $m = p_1 \dots p_r$ and p_i are not necessarily distinct primes. So for $m, p \in \mathbb{N}$, p prime, we compute $|PSL_2(\mathcal{O}_{d,m}) : PSL_2(\mathcal{O}_{d,mp})|$. We need the following well known lemma.

Lemma 3.1.1. *Let R be any commutative ring. Let $\mathfrak{q} \lhd R$ such that $R/\mathfrak{q}$ is an SR_2-ring. Then the natural map*

$$SL_2(R) \longrightarrow SL_2(R/\mathfrak{q})$$

is onto.

Proof. $R/\mathfrak{q}$ is SR_2 so $SL_2(R/\mathfrak{q}) = E_2(R/\mathfrak{q})$ and clearly

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \longmapsto \begin{pmatrix} 1+\mathfrak{q} & \alpha+\mathfrak{q} \\ \mathfrak{q} & 1+\mathfrak{q} \end{pmatrix}.$$

So the map is onto. □

Lemma 3.1.2. *For any* $d, m, p \in \mathbb{N}$ *such that* d *is square free, and* p *is prime*

$$|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,mp})| = |PSL_2(\mathcal{O}_{d,m}) : PSL_2(\mathcal{O}_{d,mp})|$$

and so

$$|SL_2(\mathcal{O}_{d}) : SL_2(\mathcal{O}_{d,m})| = |PSL_2(\mathcal{O}_{d}) : PSL_2(\mathcal{O}_{d,m})|$$

Proof. First observe that

$$|PSL_2(\mathcal{O}_{d,m}) : PSL_2(\mathcal{O}_{d,mp})| = \frac{|PSL_2(\mathcal{O}_{d,m}) : PSL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|}{|PSL_2(\mathcal{O}_{d,mp}) : PSL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|}$$

Now

$$|PSL_2(\mathcal{O}_{d,m}) : PSL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})| = \left| PSL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d.m}}\right)\right|$$

Now, for any ring R and any ideal $\mathfrak{q}$ of R such that $R/\mathfrak{q}$ is finite, we have $|PSL_2(R/\mathfrak{q})| = \rho|SL_2(R/\mathfrak{q})|$, where $\rho = 1$ if $2 \in \mathfrak{q}$ and $\rho = 1/2$ if $2 \notin \mathfrak{q}$. So

$$\left| PSL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}\right)\right| = \rho \left| SL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}\right)\right|$$

where $\rho = 1$ if $p = 2$ and $\rho = 1/2$ if $p \neq 2$. Also, as $|\mathcal{O}_{d,mp} : p\mathcal{O}_{d,m}| = p$,

$$|PSL_2(\mathcal{O}_{d,mp}) : PSL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})| = |PSL_2(\mathbb{F}_p)| = \rho|SL_2(\mathbb{F}_p)|$$

where ρ is as above (this follows from [79] theorem 8.14). Thus

$$\begin{aligned} \frac{|PSL_2(\mathcal{O}_{d,m}) : PSL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|}{|PSL_2(\mathcal{O}_{d,mp}) : PSL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|} &= \frac{\rho|SL_2(\mathcal{O}_{d,m}/p\mathcal{O}_{d,m})|}{\rho|SL_2(\mathbb{F}_p)|} \\ &= \frac{|SL_2(\mathcal{O}_{d,m}/p\mathcal{O}_{d,m})|}{|SL_2(\mathbb{F}_p)|} \\ &= \frac{|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|}{|SL_2(\mathcal{O}_{d,mp}) : SL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|} \\ &= |SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,mp})| \end{aligned}$$

□

In what follows we work with SL_2 as it makes the proofs a little simpler. Observe that

$$|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,mp})| = \frac{|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|}{|SL_2(\mathcal{O}_{d,mp}) : SL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})|}$$

Lemma 3.1.3. $|SL_2(\mathcal{O}_{d,mp}) : SL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})| = |SL_2(\mathbb{F}_p)| = p(p^2-1)$.

Proof. Observe that $|\mathcal{O}_{d,mp} : p\mathcal{O}_{d,m}| = p$ so

$$\frac{SL_2(\mathcal{O}_{d,mp})}{SL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})} \cong SL_2(\mathbb{F}_p).$$

This group has the required order by [79] theorem 8.8 and 8.14 □

Now

$$|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,m}, p\mathcal{O}_{d,m})| = \left|SL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}\right)\right|$$

So we need to have some understanding of the structure of $\mathcal{O}_{d,m}/p\mathcal{O}_{d,m}$.

Lemma 3.1.4. *If $p \mid m$ then $\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}$ is local with maximal ideal $\mathfrak{m} = (m\omega)$.*

Proof. Let $R = \mathcal{O}_{d,m}/p\mathcal{O}_{d,m}$. We compute R^*. Now

$$R = \{r + m\omega s : r, s = 0, 1, \ldots, p-1\}$$

Let $u_i = r_i + m\omega s_i \in R$, $i = 1, 2$. Then

$$u_1u_2 = r_1r_2 + (r_1s_2 + r_2s_1)m\omega + m^2\omega^2 s_1s_2$$

suppose first that $d \equiv 1, 2 \pmod 4$, so $\omega^2 = -d$. Then

$$\begin{aligned} u_1u_2 &= r_1r_2 - dm^2 s_1s_2 + (r_1s_2 + r_2s_1)m\omega \\ &= r_1r_2 + (r_1s_2 + r_2s_1)m\omega \end{aligned}$$

since $p \mid m$. Now suppose that $d \equiv 3 \pmod 4$, so $\omega^2 = \omega - (d+1)/4$. Then

$$\begin{aligned} u_1u_2 &= r_1r_2 - m^2\frac{d+1}{4}s_1s_2 + (r_1s_2 + r_2s_1 + ms_1s_2)m\omega \\ &= r_1r_2 + (r_1s_2 + r_2s_1)m\omega \end{aligned}$$

again as $p \mid m$. Now suppose that $r_1 \neq 0$ and let $r_2 = r_1^{-1}$, $s_2 = -r_1^{-2}s_1$, so $u_1u_2 = 1$. So $r_1 \neq 0 \Rightarrow u_1^{-1}$ exists. Hence $\{r + m\omega s : r \neq 0\} \subseteq R^*$. But if $r_1 = 0$ then $u_1u_2 = r_2s_1m\omega \neq 1$. So $r_1 = 0 \Rightarrow u_1$ is not a unit. Hence

$$R^* = \{r + m\omega s : r \neq 0\}$$

We now show that $R-R^* = \{m\omega s : s = 0, 1, \ldots, p-1\} = (m\omega)$. Clearly $R-R^* \subseteq (m\omega)$. Now if $d \equiv 1, 2 \pmod 4$ then

$$\begin{aligned} m\omega(r + m\omega s) &= rm\omega + m^2\omega^2 s \\ &= rm\omega - dm^2 s \\ &= rm\omega \in R - R^* \end{aligned}$$

similarly if $d \equiv 3 \pmod 4$ then

$$\begin{aligned} m\omega(r + m\omega s) &= rm\omega + m^2\omega^2 s \\ &= rm\omega + m^2 s\left(\omega - \frac{d+1}{4}\right) \\ &= (r + ms)m\omega - m^2 s\frac{d+1}{4} \\ &= rm\omega \in R - R^* \end{aligned}$$

Hence $R - R^* = (m\omega)$. So R is a local ring with maximal ideal $\mathfrak{m} = (m\omega)$ of index p. □

Lemma 3.1.5. *If $p \nmid m$ then*

$$\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}} \cong \frac{\mathcal{O}_d}{p\mathcal{O}_d}$$

and the isomorphism is given by

$$r + (m\omega)s \longmapsto r + (ms)\omega$$

Proof. It is a trivial matter to verify that the map is a homomorphism. Now let $r + s\omega \in \mathcal{O}_d/p\mathcal{O}_d$. As $p \nmid m$, m^{-1} exists and $r + (m^{-1}s)m\omega \mapsto r + s\omega$. So the map is onto. Now suppose that $r + m\omega s \mapsto 1$, so $r + (ms)\omega = 1$ in $\mathcal{O}_d/p\mathcal{O}_d$, so $r = 1$ and $ms \equiv 0 \pmod p$. But $p \nmid m$, so $s = 0$. So $r + m\omega s = 1$. So the map is injective. Hence result. □

The structure of $\mathcal{O}_d/p\mathcal{O}_d$ is well known and can be found in any book on algebraic number theory. See, for example, [52] page 108. First recall the definition of the discriminant of $K = \mathbb{Q}(\sqrt{-d})$:

$$D = \begin{cases} -d & \text{if } d \equiv 3 \pmod 4, \\ -4d & \text{else.} \end{cases}$$

Now χ_K, the *quadratic character* of K is defined as follows. If $p \mid D$ then $\chi_K(p) = 0$,

$$\chi_K(2) = \begin{cases} 1 & \text{if } D \equiv 1 \pmod 8, \\ -1 & \text{if } D \equiv 5 \pmod 8). \end{cases}$$

and if $p \neq 2$ then

$$\chi_K(p) = \begin{cases} 1 & \text{if } D \equiv x^2 \pmod p, \\ -1 & \text{else.} \end{cases}$$

Theorem. *[52] Let $p \in \mathbb{Z}$ be prime then*

$$p\mathcal{O}_d = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \textit{for } \chi_K(p) = 1, \\ \mathfrak{p} & \textit{for } \chi_K(p) = -1, \\ \mathfrak{p}^2 & \textit{for } \chi_K(p) = 0. \end{cases}$$

where $\mathfrak{p}, \mathfrak{p}_i$ are prime ideals of $\mathcal{O}_d$.

Lemma 3.1.6. *If $p \mid m$ then $|SL_2(\mathcal{O}_{d,m}/p\mathcal{O}_{d,m})| = p^3|SL_2(\mathbb{F}_p)|$.*

Proof. Now $\mathcal{O}_{d,m}/p\mathcal{O}_{d,m}$ is local with maximal ideal $\mathfrak{m}$, of index p, so

$$\left|SL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}\right)\right| = \left|SL_2\left(\frac{\mathcal{O}_{d,m}}{\mathfrak{m}}\right)\right| \left|SL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}, \frac{\mathfrak{m}}{p\mathcal{O}_{d,m}}\right)\right|.$$

and $|SL_2(\mathcal{O}_{d,m}/\mathfrak{m})| = |SL_2(\mathbb{F}_p)|$, and by lemma (4.2.9) $\left|SL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}, \frac{\mathfrak{m}}{p\mathcal{O}_{d,m}}\right)\right| = p^3$. □

Thus

Lemma 3.1.7. *If $p \mid m$ then*

$$|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,mp})| = p^3$$

Lemma 3.1.8. *If $p \nmid m$ then*

$$\left|SL_2\left(\frac{\mathcal{O}_{d,m}}{p\mathcal{O}_{d,m}}\right)\right| = \begin{cases} p^2(p^2-1)^2 & \textit{if } \chi_K(p) = 1, \\ p^4(p^2-1) & \textit{if } \chi_K(p) = 0, \\ p^2(p^4-1) & \textit{if } \chi_K(p) = -1. \end{cases}$$

Proof. If $\chi_K(p) = -1$ then $\mathcal{O}_{d,m}/p\mathcal{O}_{d,m} \cong \mathbb{F}_{p^2}$ and $|SL_2(\mathbb{F}_{p^2})| = p^2(p^4-1)$, by [79] theorem 8.8 and the comments at the bottom of p.157. Now suppose that $\chi_K(p) = 1$, so that $R = \mathcal{O}_{d,m}/p\mathcal{O}_{d,m}$ has two ideals $\mathfrak{m}_1$, and $\mathfrak{m}_2$ of index p. So, by (6.4.4), $SL_2(R) = SL_2(R/\mathfrak{m}_1) \times SL_2(R/\mathfrak{m}_2)$ and $|SL_2(R)| = |SL_2(\mathbb{F}_p)|^2 = p^2(p^2-1)^2$, by [79] theorem 8.8 and the comments at the bottom of p.157. Finally suppose that $\chi_K(p) = 0$, so $L = \mathcal{O}_{d,m}/p\mathcal{O}_{d,m}$ is a local ring and, as before $|SL_2(L)| = p^3|SL_2(\mathbb{F}_p)| = p^4(p^2-1)$. □

Thus

Lemma 3.1.9. *Suppose that $p \nmid m$ then*

$$|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,mp})| = \begin{cases} p(p^2-1) & \textit{if } \chi_K(p) = 1, \\ p^3 & \textit{if } \chi_K(p) = 0, \\ p(p^2+1) & \textit{if } \chi_K(p) = -1. \end{cases}$$

Now observe that, from the above, if $p \nmid m$

$$|SL_2(\mathcal{O}_{d,m}) : SL_2(\mathcal{O}_{d,mp^\alpha})| = |SL_2(\mathcal{O}_d : SL_2(\mathcal{O}_{d,p^\alpha})|$$

so that

$$|SL_2(\mathcal{O}_d) : SL_2(\mathcal{O}_{d,m})| = \prod_{i=1}^{r} |SL_2(\mathcal{O}_d) : SL_2(\mathcal{O}_{d,p_i^{\alpha_i}})|$$

where $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ and

$$\begin{aligned} |SL_2(\mathcal{O}_d) : SL_2(\mathcal{O}_{d,p^\alpha})| &= |SL_2(\mathcal{O}_d) : SL_2(\mathcal{O}_{d,p})||SL_2(\mathcal{O}_{d,p}) : SL_2(\mathcal{O}_{d,p^\alpha})| \\ &= p^{3(\alpha-1)}|SL_2(\mathcal{O}_d) : SL_2(\mathcal{O}_{d,p})|. \end{aligned}$$

Thus

Theorem 3.1.10.

$$|PSL_2(\mathcal{O}_d) : PSL_2(\mathcal{O}_{d,m})| = m^3 \prod_{i=1}^{r} \frac{1}{p_i^3} \, |PSL_2(\mathcal{O}_d) : PSL_2(\mathcal{O}_{d,p})| \, ,$$

where $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, and

$$|PSL_2(\mathcal{O}_d) : PSL_2(\mathcal{O}_{d,p})| = \begin{cases} p(p^2-1) & \textit{if } \chi_K(p) = 1, \\ p^3 & \textit{if } \chi_K(p) = 0, \\ p(p^2+1) & \textit{if } \chi_K(p) = -1. \end{cases}$$

3.2 A miscellany of results

Theorem 3.2.1. *Let $m_1, m_2 \in \mathbb{N}$ be distinct, and suppose $m_2 \mid m_1$, so $PSL_2(\mathcal{O}_{d,m_1}) \leqslant PSL_2(\mathcal{O}_{d,m_2})$. Then $PSL_2(\mathcal{O}_{d,m_1}) \ntriangleleft PSL_2(\mathcal{O}_{d,m_2})$.*

Proof. Let

$$X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL_2(\mathcal{O}_{d,m_2}),$$

and let

$$M = \begin{pmatrix} 1 & 1+m_1\omega \\ 0 & 1 \end{pmatrix} \in PSL_2(\mathcal{O}_{d,m_1})$$

so

$$XMX^{-1} \equiv \begin{pmatrix} 1-\alpha\gamma & \alpha^2 \\ -\gamma^2 & 1+\alpha\gamma \end{pmatrix} \pmod{m_1\omega M_2(\mathcal{O}_d)}.$$

Now suppose that $d \equiv 1,2 \pmod 4$. Let p be a rational prime such that $p \nmid d$ and $p \nmid m_1$, so $p \nmid dm_2^2$. So $\exists x, y \in \mathbb{Z}$ such that $px + dm_2^2 y = 1$ ie $px + m_2\omega(-\omega m_2 y) = 1$. Let $\alpha = m_2\omega$, $\gamma = p$ then

$$X = \begin{pmatrix} m_2\omega & -x \\ p & -m_2\omega y \end{pmatrix} \in PSL_2(\mathcal{O}_{d,m_2})$$

and $XMX^{-1} \notin PSL_2(\mathcal{O}_{d,m_1})$

Now suppose that $d \equiv 3 \pmod 4$, so $\omega^2 = \omega - (d+1)/4$, so $(d+1)/4 = \omega(1-\omega)$. Let p be a rational prime such that $p \nmid (d+1)/4$ and $p \nmid m_1$, so $p \nmid m_2^2(d+1)/4$. So $\exists x, y \in \mathbb{Z}$ such that $px + m_2^2 y(d+1)/4 = 1$ ie $px + m_2\omega(m_2 y(1-\omega)) = 1$. Then

$$X = \begin{pmatrix} m_2\omega & -x \\ p & (1-\omega)m_2 y \end{pmatrix} \in PSL_2(\mathcal{O}_{d,m_2})$$

and $XMX^{-1} \notin PSL_2(\mathcal{O}_{d,m_1})$. Hence result. □

Theorem 3.2.2. *Let $N \lhd PSL_2(\mathcal{O}_{d,m})$ be of index n. Then if $6 \nmid n$ then $o(N) = \mathcal{O}_{d,m}$ and N has torsion.*

Proof. Suppose that $6 \nmid n$, so $2 \nmid n$ or $3 \nmid n$. If $2 \nmid n$ then

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in N,$$

and $a^2 = 1$ so N has torsion. Also $a \equiv kI \pmod{\mathfrak{q}} \Rightarrow 1 \in \mathfrak{q}$ ie $\mathfrak{q} = \mathcal{O}_{d,m}$, so $o(N) = \mathcal{O}_{d,m}$. If $3 \nmid n$ then

$$at = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in N$$

so, as above N has torsion and $o(N) = \mathcal{O}_{d,m}$. □

3.3 A presentation for $SL_2(\mathbb{Z}\left[\sqrt{-3}\right])$

Dennis has shown [19]

Theorem. $SL_2(\mathbb{Z}\left[\sqrt{-3}\right]) = E_2(\mathbb{Z}\left[\sqrt{-3}\right])$.

Following Fine [25] we apply the following, due to Cohn [15]

Theorem. *Let R be a subring of $\mathbb{C}$ with the usual absolute valuation. Suppose that if $\alpha \in R$, and $|\alpha| \lnsim 2$ then $\alpha = 0$, or $|\alpha| = 1$, or $|\alpha| = \sqrt{p}$, where $p = 2, 3$. Then $E_2(R)$ is generated by $E(x)$ with the following complete set of relations:*

1. $E(x)E(0)E(y) = -E(x+y)$
2. $E(x)D(\mu) = D(\mu^{-1})E(\mu x \mu)$
3. $(E(\overline{\alpha})E(\alpha))^p = -I$ $\forall \alpha \in R$ *such that* $|\alpha| = \sqrt{p}$, *where* $p = 2, 3$.
4. $E(\mu)E(\mu^{-1})E(\mu) = D(-\mu)$

Where $x, y \in R$, $\mu \in R^*$, and

$$E(x) = \begin{pmatrix} x & 0 \\ -1 & 0 \end{pmatrix}, D(\mu) = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}.$$

Let $\mathcal{O} = \mathbb{Z} + i\sqrt{3}\mathbb{Z}$. Now $\mathcal{O}^* = \{\pm 1\}$, and the only elements of norm between 1 and 2 are $\pm i\sqrt{3}$. So we get for $SL_2(\mathbb{Z}\left[\sqrt{-3}\right])$

Generators:

$$E(x), \text{ where } x \in R$$

Relators:

$$E(x)E(0)E(y) = -E(x+y), \tag{3.1}$$

$$-I \text{ central}, \ (-I)^2 = I, \tag{3.2}$$

$$(E(i\sqrt{3})E(-i\sqrt{3}))^3 = -I, \tag{3.3}$$

$$E(1)^3 = -I, E(-1)^3 = I. \tag{3.4}$$

Using (3.1) we can reduce the generators to $E(0), E(\pm 1), E(\pm i\sqrt{3})$, as follows. Let $z \in \mathbb{Z}$, and suppose $z \geqslant 0$. Then

$$E(z) = -E(z-1)E(0)E(1),$$

and

$$E(iz\sqrt{3}) = -E(i(z-1)\sqrt{3})E(0)E(i\sqrt{3}).$$

We get similar formulas for $z \leqslant 0$. Putting these together we get

$$E(z_1 + iz_2\sqrt{3}) = -E(z_1)E(0)E(iz_2\sqrt{3}).$$

If $x, y = 0$ then it is easy to see

$$E(O)^2 = -I \Leftrightarrow E(x)E(0)E(y) = -E(x+y) \tag{3.5}$$

and (3.1) certainly implys the following

$$E(1)E(0)E(i\sqrt{3}) = E(i\sqrt{3})E(0)E(1) \tag{3.6}$$

$$E(1)E(0)E(-i\sqrt{3}) = E(-i\sqrt{3})E(0)E(1) \tag{3.7}$$

$$E(-1)E(0)E(i\sqrt{3}) = E(i\sqrt{3})E(0)E(-1) \tag{3.8}$$

$$E(-1)E(0)E(-i\sqrt{3}) = E(-i\sqrt{3})E(0)E(-1) \tag{3.9}$$

and we also get

$$E(-1) = -E(0)E(1)^{-1}E(0)^{-1} \tag{3.10}$$

$$E(-i\sqrt{3}) = -E(0)E(i\sqrt{3})^{-1}E(0)^{-1} \tag{3.11}$$

Using (3.10), and (3.11) we can eliminate the generators $E(-1)$, and $E(-i\sqrt{3})$, so $SL_2(\mathbb{Z}\left[\sqrt{-3}\right])$ is generated by $E(0), E(1)$, and $E(i\sqrt{3})$. We can show that (3.7), (3.8), (3.9) can be deduced from (3.6) as follows. RTP

$$E(1)E(0)E(-i\sqrt{3}) = E(-i\sqrt{3})E(0)E(1)$$

now, using (3.10), and (3.11)

$$\begin{aligned} LHS &= E(1)E(0)(-E(0)E(i\sqrt{3})^{-1}E(0)^{-1}) \\ &= E(1)E(i\sqrt{3})^{-1}E(0)^{-1} \end{aligned}$$

and

$$\begin{aligned} RHS &= -E(0)E(i\sqrt{3})^{-1}E(0)^{-1}E(0)E(1) \\ &= -E(0)E(i\sqrt{3})^{-1}E(1) \end{aligned}$$

now

$$\begin{aligned}
&E(1)E(i\sqrt{3})^{-1}E(0)^{-1}(-E(0)E(i\sqrt{3})^{-1}E(1))^{-1}\\
=&-E(1)E(i\sqrt{3})^{-1}E(0)^{-1}E(1)^{-1}E(i\sqrt{3})E(0)^{-1}\\
=&-E(1)E(1)^{-1}E(0)^{-1}E(i\sqrt{3})^{-1}E(i\sqrt{3})E(0)^{-1}\\
=&-E(0)^{-2}=I
\end{aligned}$$

and so $LHS = RHS$. The others are done in a similar manner.

And so a presentation for $SL_2(\mathbb{Z}\left[\sqrt{-3}\right])$ is:

Generators:

$$E(0), E(1), E(i\sqrt{3}), -I$$

Relators:

$$E(1)^3 = -I$$
$$E(0)^2 = -I$$
$$-I \text{ central, } (-I)^2 = I$$
$$(E(i\sqrt{3})E(0)E(i\sqrt{3})^{-1}E(0)^{-1})^3 = I$$
$$E(1)E(0)E(i\sqrt{3}) = E(i\sqrt{3})E(0)E(1)$$

Letting

$$A = E(0) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = E(0)E(1)^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$U = -E(0)E(1)^{-1}E(0)E(i\sqrt{3})^{-1} = \begin{pmatrix} 1 & 2\omega \\ 0 & 1 \end{pmatrix}.$$

We get

Generators:

$$A, T, U, J$$

Relators:

$$A^2 = (AT)^3 = J,$$
$$J \text{ central, } J^2 = I$$
$$(U^{-1}TAT^{-1}UA^{-1})^3 = [T, U] = I$$

Let $W = T^{-1}U$ and set $J = I$ to get

Theorem 3.3.1.

$$PSL_2(\mathcal{O}_{3,2}) = PSL_2(\mathbb{Z}\left[\sqrt{-3}\right]) =< a,t,w; a^2, (at)^3, (w^{-1}awa)^3, [t,w] >$$

3.4 The Group $PSL_2(\mathcal{O}_{3,2})$

First of all observe

Theorem 3.4.1.

$$PSL_2(\mathcal{O}_{3,2})^{ab} =< t,w; t^6, [t,w] >\cong \mathbb{Z}_6 \times \mathbb{Z}$$

Letting $N = N(w)$, the normal closure of w in $PSL_2(\mathcal{O}_{3,2})$, we see that $l(N) = 0$ and

$$\frac{PSL_2(\mathcal{O}_{3,2})}{N} =< a,t; a^2, (at)^3 >= M.$$

We aim to decompose $PSL_2(\mathcal{O}_{3,2})$ as a non-trivial free product with amalgamation and as an HNN group. We do here for $PSL_2(\mathcal{O}_{3,2})$ what Fine did in [25] for $PSL_2(\mathcal{O}_2)$, $PSL_2(\mathcal{O}_7)$, $PSL_2(\mathcal{O}_{11})$.

3.4.1 HNN and amalgam decomposition

Theorem 3.4.2. *$PSL_2(\mathcal{O}_{3,2})$ is an HNN extension of $K_{3,2}$ with the Modular group associated, where $K_{3,2} = S_3 *_{\mathbb{Z}_3} D(3,3,3)$, and $D(3,3,3) =< x,y; x^3, y^3, (xy)^3 >$ is one of von Dyck's groups (see [36]).*

Proof. We start with the presentation

$$< a,t,w; a^2, (at)^3, (w^{-1}awa)^3, [t,w] >$$

Letting $v = w^{-1}aw$, the presentation becomes

$$< a,t,v,w; a^2, (at)^3, (av)^3, v^2, (tv)^3, t = w^{-1}tw, v = w^{-1}aw >$$

Let

$$K_{3,2} =< a,t,v; a^2, (at)^3, (av)^3, v^2, (tv)^3 >$$

We claim that $PSL_2(\mathcal{O}_{3,2})$ is an HNN extension of $K_{3,2}$ with $< a,t >\cong M \cong< v,t >$ associated. First of all we show that $< a,t >\cong M$. Now as $a^2 = (at)^3 = 1$ it is clear that

$M \twoheadrightarrow < a, t >$. But $< a, t > \leqslant K_{3,2}$, and $K_{3,2} \twoheadrightarrow M$ via the map $t \mapsto t$, $a \mapsto a$, and $v \mapsto a$. We see from this that $< a, t > \twoheadrightarrow M$, and so that $M \cong < a, t >$. We can show that $< v, t > \cong M$ in exactly the same way. Let θ be the automorphism of $K_{3,2}$ given by $a \mapsto v$, $v \mapsto a$, and $t \mapsto t$. We must show that $\theta(< a, t >) = < v, t >$. Now $\theta(a) = v \in < v, t >$, and $\theta(t) = t \in < v, t >$, so clearly $\theta(< a, t >) \leqslant < v, t >$. Similarly $\theta(< v, t >) \leqslant < a, t >$. Now $< v, t > = \theta(\theta(< v, t >)) \leqslant \theta(< a, t >)$, and so $\theta(< a, t >) = < v, t >$.

Now consider $K_{3,2}$ and let $s = at$, $m = av$, so $t = as$, and $v = am$. Thus

$$K_{3,2} = < a, s, m; a^2, s^3, m^3, (am)^2, (sm^2)^3 >$$

Recall that

$$< a, m; a^2, m^3, (am)^2 > \cong S_3$$

and

$$< s, \overline{m}; s^3, \overline{m}^3, (s\overline{m}^{-1})^3 > \cong D(3,3,3)$$

So

$$K_{3,2} = S_3 *_{m=\overline{m}} D(3,3,3)$$

□

We have the following theorem

Theorem 3.4.3. *[48] If G maps onto a free product then G can be decomposed as an amalgamated free product. More precisely if $\theta : G \twoheadrightarrow A * B$ and $H = \theta^{-1}(A) \cap \theta^{-1}(B)$, G_A and G_B are disjoint copies of $\theta^{-1}(A)$ and $\theta^{-1}(B)$ respectively and H_A, H_B are copies of H in G_A and G_B respectively Then G is isomorphic to the amalgamated free product $G_A *_{H_A=H_B} G_B$.*

As $PSL_2(\mathcal{O}_{3,2})$ maps onto $PSL_2(\mathbb{Z})$ which is the free product of a 2-cycle and a 3-cycle, we immediately get that $PSL_2(\mathcal{O}_{3,2})$ is an amalgamated free product. However if we do some direct calculations we get a nice decomposition.

Theorem 3.4.4.

$$PSL_2(\mathcal{O}_{3,2}) = G_1 *_H G_2$$

where G_1 is an HNN extension of S_3, G_2 is an HNN extension of $D(3,3,3)$, and $H = \mathbb{Z} * \mathbb{Z}_3$.

Proof. We start with the presentation

$$< a, t, w; a^2, (at)^3, (w^{-1}awa)^3, [t, w] >$$

Letting $t = as$, $x = w^{-1}sw$, $m = w^{-1}aw$ the presentation becomes

$$< a, w, s, x, m; a^2, s^3, (am)^3, x = w^{-1}sw, m = w^{-1}aw, am = sx^{-1}, x^3, m^2, (sx^{-1})^3 >$$

Now let

$$G_1 =< a, m, w; a^2, m^2, (am)^3, m = w^{-1}aw >$$

and

$$G_2 =< \overline{w}, s, x; s^3, x^3, (sx^{-1})^3, x = \overline{w}^{-1}s\overline{w} >$$

and

$$H_1 =< w, am >\leqslant G_1$$

and

$$H_2 =< \overline{w}, sx^{-1} >\leqslant G_2$$

Using the normal form theorem for HNN extensions ([12] chapter 1 theorem 31) it can be shown that $H_1 \cong H_2 \cong \mathbb{Z} * \mathbb{Z}_3$. We can now combine the presentation for G_1 and G_2, adding the relations $w = \overline{w}$ and $am = sx^{-1}$, to get

$$< a, m, w, s, x, \overline{w}; a^2, m^2, (am)^3, m = w^{-1}aw, s^3, x^3, (sx^{-1})^3, x = \overline{w}^{-1}s\overline{w} >$$

after applying Tietze transformations to eliminate $\overline{w}$ we get the earlier presentation for $PSL_2(\mathcal{O}_{3,2})$. Thus

$$PSL_2(\mathcal{O}_{3,2}) = G_1 *_H G_2$$

Now recall that

$$S_3 =< x, y; x^2, y^2, (xy)^3 >$$

It is clear that

$$< a, m; a^2, m^2, (am)^3 >\leqslant G_1$$

and that $< a >\cong \mathbb{Z}_2 \cong < m >$. It is very easy to see that under the automorphism, θ, of S_3 where $\theta : a \mapsto m$ and $\theta : m \mapsto a$, we have $\theta(< a >) =< m >$ and so G_1 is an HNN extension of S_3 with two 2-cycles associated. Again it is easy to see that

$$D(3,3,3) =< s, x; s^2, x^3, (sx^{-1})^3 > \leqslant G_2$$

and that under that automorphism of $D(3,3,3)$ given by $\varphi : s \mapsto x$, and $\varphi : x \mapsto s$, we have $\varphi(< s >) =< x >\cong \mathbb{Z}_3$ and so G_2 is an HNN extension of $D(3,3,3)$ with two 3-cycles associated. □

Now recall that $PSL_2(\mathcal{O}_3)$ does not decompose as a non-trivial free product with amalgamation or as an HNN group. However the above gives us a natural example of a subgroup of finite index in $PSL_2(\mathcal{O}_3)$ which does. Hence

Theorem 3.4.5. *$PSL_2(\mathcal{O}_3)$ is virtually a non-trivial product with amalgamation and virtually an HNN group. More precisely $|PSL_2(\mathcal{O}_3) : PSL_2(\mathcal{O}_{3,2})| = 10$ and $PSL_2(\mathcal{O}_{3,2})$ decomposes as a non-trivial free product with amalgamation and as an HNN group.*

Contrast this with Fine's [25] rather artificial construction of a subgroup of index 144 which decomposes as a non-trivial free product with amalgamation. We can pose the following

Question. Is 10 the least index of a subgroup of $PSL_2(\mathcal{O}_3)$ which decomposes as a free product with amalgamation or as an HNN group?

3.4.2 Some Consequences

First recall that in an HNN group a torsion element must be conjugate to a torsion element in the base ([12] chapter 1 exercise 22). We need the following

Lemma 3.4.6. *Every element of finite order in $D(3,3,3)$ is conjugate to one of:*

$$x, x^2, y, y^2, xy, (xy)^2$$

all of which have order 3.

Proof. This is easy to see by making $D(3,3,3)$ act on the infinite lattice in Euclidean 2-space made up of regular hexagons and triangles as given in [36] p.93. □

Theorem 3.4.7. *In $PSL_2(\mathcal{O}_{3,2})$ every element of finite order is conjugate to one of:*

$$a, at, (at)^2, aw^{-1}aw, (aw^{-1}aw)^2, w^{-1}awt, w^{-1}awt^{-1}$$

where a has order 2 and the rest have order 3

Proof. Recall that $PSL_2(\mathcal{O}_{3,2})$ is an HNN extension of $K_{3,2}$ and $K_{3,2} = S_3 *_{\mathbb{Z}_3} D(3,3,3)$. Let $g \in PSL_2(\mathcal{O}_{3,2})$ be of finite order. So g is conjugate to an element of finite order in $K_{3,2}$ and so g is conjugate to an element of finite order in S_3 or $D(3,3,3)$. Now suppose that g has order 2, then, as all the elements of finite order in $D(3,3,3)$ have order 3, g is conjugate to an element of order 2 in S_3, recall

$$S_3 =< a, m; a^2, m^3, (am)^2 >$$

and S_3 has exactly one conjugacy class of order 2. So g is conjugate to a.

Now suppose that g has order 3, so as S_3 has only one conjugacy class of order 3 and it is represented by m we have that g is conjugate to one of:

$$s, s^2, m, m^2, sm^{-1}, s^{-1}m$$

The result follows, as $s = at$, and $m = aw^{-1}aw$. □

Theorem 3.4.8. *Let $\tau \in PSL_2(\mathcal{O}_{3,2})$ be a torsion element. Write $x \sim y$ if x and y are conjugate. Then*

1. *If $\tau \sim at, (at)^2, w^{-1}awt, w^{-1}awt^{-1}$ then $\frac{PSL_2(\mathcal{O}_{3,2})}{N(\tau)} \cong \mathbb{Z}_2 \times \mathbb{Z}$*

2. *If $\tau \sim a$ then $\frac{PSL_2(\mathcal{O}_{3,2})}{N(\tau)} \cong \mathbb{Z}_3 \times \mathbb{Z}$*

3. *If $\tau \sim aw^{-1}aw, (aw^{-1}aw)^2$ then $\frac{PSL_2(\mathcal{O}_{3,2})}{N(\tau)} \cong \mathbb{Z} \times M$*

Proof. Recall

$$PSL_2(\mathcal{O}_{3,2}) =< a, t, w; a^2, (at)^3, [t, w], (w^{-1}awa)^3 >$$

set $a = 1$, so $t^3 = 1$, so we get

$$\frac{PSL_2(\mathcal{O}_{3,2})}{N(a)} =< t, w; t^3, [t, w] >\cong \mathbb{Z}_3 \times \mathbb{Z}$$

The others are similar □

Theorem 3.4.9. *Let T be the set of all torsion elements in $PSL_2(\mathcal{O}_{3,2})$. Then $N(T) = N(M)$.*

Proof. $N(T) = N(a, at, aw^{-1}aw, w^{-1}awt, w^{-1}awt^{-1})$, and $N(M) = N(a,t)$. Clearly $N(M) \subseteq N(T)$. Now suppose that $a = t = 1$. So $a = at = aw^{-1}aw = w^{-1}awt = w^{-1}awt^{-1} = 1$. So $N(T) \subseteq N(M)$. □

Lemma 3.4.10. *Let $N \lhd \mathbb{Z}_p \times \mathbb{Z} =< x, y >$, be of index n , where p is a rational prime. Then if $p \nmid n$ then*

$$N = N(x, y^n)$$

if $p \mid n$ then

$$N = N(x, y^n), N(x^m y^k)$$

where $n = pk$, and $m = 0, 1, \ldots, p-1$.

Proof. Suppose $p \nmid n$. Then $x \in N$ and it is clear that $N = N(x, y^n)$.

Suppose that $p \mid n$, so $n = pk$, say. If, as above $x \in N$ then $N = N(x, y^n)$ so suppose that $x \notin N$. Let l be the order of y mod N, so $l \mid pk$. Suppose that $l \mid k$, and $l \neq k$, so $y^l = 1$, and $l < k$, but then there are $< pk$ distinct cosets of N. Contradiction. So if $l \mid k$ then $l = k$, and as $l \mid pk$ we must have $l = k$, or pk.

Suppose that $l = k$. Then $N(y^k) \leqslant N$. But $N(y^k)$ is of index $pk = n$, so $N = N(y^k) = N(x^0 y^k)$. Now suppose that $l = pk$. So $y, y^2, \ldots, y^{pk}$ are $pk = n$ distinct cosets representatives of N. Now $x \notin N$, so $x = y^r$ some r, $1 \leqslant r \leqslant pk$, and $1 = x^p = y^{pr}$, so $pk \mid pr$ so $k \mid r$, so $r = k, 2k, \ldots, pk$. If $r = pk$ then $x = y^{pk} = 1$. Contradiction, as $x \notin N$. So $r \neq pk$, so $x = y^k, y^{2k}, \ldots, y^{(p-1)k}$. Hence, using the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field $y^k = x^m$ where $m = 1, \ldots, p-1$. So $N(x^m y^k) \leqslant N$. But $N(x^m y^k)$ is of index n, so $N = N(x^m y^k)$.

We now show that these groups are distinct. Suppose that

$$N(x, y^n) = N(x^m y^k)$$

then $y^k \in N(x, y^{pk})$. Contradiction. Suppose that

$$N(x^{m_1} y^k) = N(x^{m_2} y^k) = N$$

where $0 \leqslant m_1, m_2 \leqslant p-1$. Then $x^{m_1} y^k y^{-k} x^{-m_2} \in N$, so $x^{m_1 - m_2} \in N$, so $m_1 \equiv m_2 \pmod{p}$ so $m_1 = m_2$. Hence all the groups are distinct. □

Theorem 3.4.11. *Let $N \lhd PSL_2(\mathcal{O}_{3,2})$ be of index n. Then if $(n,6)=1$*

$$N = N(a,t,w^n)$$

if $2 \mid n$, and $3 \nmid n$ then N is one of

$$N(a,t,w^n), N(at, w^{n/2}), N(at, aw^{n/2})$$

if $2 \nmid n$, and $3 \mid n$ then N is one of

$$N(a,t,w^n), N(a, w^{n/3}), N(a, tw^{n/3}), N(a, t^2w^{n/3})$$

Proof. Suppose that $(n,6)=1$, so working $\mod N$, $a = at = w^{-1}awa = 1$, so $a = t = 1$, so $N = N(a,t,w^n)$. Now suppose that $2 \nmid n$, and $3 \mid n$, so $a = 1$. So $PSL_2(\mathcal{O}_{3,2})/N$ is a factor of $< t, w; t^3, tw = wt > \cong \mathbb{Z}_3 \times \mathbb{Z}$. So, by (3.4.10), $N = N(a,t,w^n)$, $N(a, w^{n/3})$, $N(a, tw^{n/3})$, $N(a, t^2w^{n/3})$. Now suppose $2 \mid n$, and $3 \nmid n$, so $at = w^{-1}awa = 1$. So $PSL_2(\mathcal{O}_{3,2})/N$ a factor of $< a, w; a^2, aw = wa > \cong \mathbb{Z}_2 \times \mathbb{Z}$. So, by (3.4.10), $N = N(a,t,w^n)$, $N(at, w^{n/2})$, $N(at, aw^{n/2})$. □

Theorem 3.4.12. *Let $n \in \mathbb{N}$. Let $H = PSL_2(\mathcal{O}_{3,2})/PSL_2(\mathcal{O}_{3,2})^n$. Then*

1. *If $(n,6)=1$ then $H \cong \mathbb{Z}_n$ and $PSL_2(\mathcal{O}_{3,2})^n = N(a,t,w^n)$.*

2. *If $3 \nmid n$ and $2|n$ then $H \cong \mathbb{Z}_2 \times \mathbb{Z}_n$ and $PSL_2(\mathcal{O}_{3,2})^n = N(at, w^n)$.*

3. *If $2 \nmid n$ and $3|n$ then $H \cong \mathbb{Z}_3 \times \mathbb{Z}_n$ and $PSL_2(\mathcal{O}_{3,2})^n = N(a, w^n)$.*

Proof. Recall

$$PSL_2(\mathcal{O}_{3,2}) =< a, t, w; a^2, (at)^3, [t,w], (w^{-1}awa)^3 >$$

Suppose that $(n,6)=1$ then, working $\mod PSL_2(\mathcal{O}_{3,2})^n$, $a = at = 1$, so $a = t = 1$, and $w^n = 1$. So $H \cong \mathbb{Z}_n$. Now suppose that $3 \nmid n$ and $2 \mid n$ then $at = 1$, so $a = t$, and $(w^{-1}awa) = 1$ so $[a,w] = 1$, and $w^n = 1$, so $H \cong \mathbb{Z}_2 \times \mathbb{Z}_n$. Suppose that $2 \nmid n$ and $3 \mid n$ then $a = 1$ so $t^3 = 1$, and $w^n = 1$. So $H \cong \mathbb{Z}_3 \times \mathbb{Z}_n$. □

Theorem 3.4.13.

$$PSL_2(\mathcal{O}_{3,2})' < PSL_2(\mathcal{O}_{3,2})^2 \cap PSL_2(\mathcal{O}_{3,2})^3$$

Proof. Obviously $PSL_2(\mathcal{O}_{3,2})' \leqslant PSL_2(\mathcal{O}_{3,2})^2 \cap PSL_2(\mathcal{O}_{3,2})^3$. Consideration of index shows that the inclusion is strict. □

Remark. It is well known [70] that, in the Modular group $PSL_2(\mathbb{Z})' = PSL_2(\mathbb{Z})^2 \cap PSL_2(\mathbb{Z})^3$. Fine ([25] Corollary 4.5.4.3) shows that if $d = 2, 7, 11$ then $PSL_2(\mathcal{O}_d)' < PSL_2(\mathcal{O}_d)^2 \cap PSL_2(\mathcal{O}_d)^3$.

3.5 Presentations for some other $PSL_2(\mathcal{O}_{d,m})$.

Using GAP [24] we find the following presentation for a subgroup of $PSL_2(\mathcal{O}_1)$ of index 8

$$< a, t, w, z; a^2, z^2, (at)^3, (atz)^2, [t, w], (atw^{-1}zw)^2 >$$

where

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, w = \begin{pmatrix} 1 & 2i \\ 0 & 1 \end{pmatrix},$$

$$z = (uat)a(uat)^{-1} = \begin{pmatrix} 1-2i & 1-2i \\ -2 & 2i-1 \end{pmatrix}.$$

Since all the generators lie in $PSL_2(\mathcal{O}_{1,2})$, and, by (3.1.10), $|PSL_2(\mathcal{O}_1) : PSL_2(\mathcal{O}_{1,2})| = 8$, the group given by this presentation must be $PSL_2(\mathcal{O}_{1,2})$. Hence

Theorem 3.5.1.

$$PSL_2(\mathcal{O}_{1,2}) =< a, t, w, z; a^2, z^2, (at)^3, (atz)^2, [t, w], (atw^{-1}zw)^2 >$$

We can show that $PSL_2(\mathcal{O}_{1,2})$ decomposes as an HNN group and as a non-trivial amalgamated free product in the same way as we did for $PSL_2(\mathcal{O}_{3,2})$.

Using GAP [24] we find the following presentation for a subgroup of $PSL_2(\mathcal{O}_{11})$ of index 10

$$< a, t, w, k, l, m, n; a^2, (at)^3, k^2, [m, n], [t, w], tklkt^{-1}l^{-1}, km^{-1}ltat^{-1}l^{-1}m,$$
$$nlat^{-1}l^{-1}n^{-1}mwaw^{-1}tm^{-1}, m^{-1}tklt^{-1}l^{-1}mwt^{-1}aw^{-1}t >$$

Where

$$w = \begin{pmatrix} 1 & 2\omega \\ 0 & 1 \end{pmatrix}, k = (uat)a(uat)^{-1} = \begin{pmatrix} -1+2\omega & 5 \\ 2 & 1-2\omega \end{pmatrix},$$

$$l = (ua)u^2(ua)^{-1} = \begin{pmatrix} -7+2\omega & 6+4\omega \\ 2\omega & 5-2\omega \end{pmatrix},$$

$$m = (uaua)u(uaua)^{-1} = \begin{pmatrix} -8+6\omega & 21+6\omega \\ 3+2\omega & 10-6\omega \end{pmatrix},$$

$$n = (ua)uuatat^{-1}au^{-1}t^{-1}(ua)^{-1} = \begin{pmatrix} 7+6\omega & 26-14\omega \\ 6-2\omega & -5-6\omega \end{pmatrix}.$$

Since all the generators lie in $PSL_2(\mathcal{O}_{11,2})$, and, by (3.1.10), $|PSL_2(\mathcal{O}_{11}) : PSL_2(\mathcal{O}_{11,2})| = 10$, the group given by this presentation must be $PSL_2(\mathcal{O}_{11,2})$.

Again using GAP [24] wefind the following presentation for a subgroup of index 6 in $PSL_2(\mathcal{O}_7)$:

$$< a, t, w, x, y\, ;\, a^2, x^2, [t, w]\,, (ax)^3, (at)^3, y = txyxt^{-1}, (ytay^{-1}x)^2,$$
$$xyat^{-1}y^{-1}wt^{-1}aw^{-1}t >$$

where

$$w = \begin{pmatrix} 1 & 2\omega \\ 0 & 1 \end{pmatrix}, x = (uat)a(uat)^{-1} = \begin{pmatrix} 1-2\omega & -3 \\ -2 & -1+2\omega \end{pmatrix},$$

$$y = (ua)u^2(ua)^{-1} = \begin{pmatrix} -5+2\omega & -4-2\omega \\ 2\omega & 3-2\omega \end{pmatrix}.$$

Since all the generators lie in $PSL_2(\mathcal{O}_{7,2})$ and, by (3.1.10), $|PSL_2(\mathcal{O}_7) : PSL_2(\mathcal{O}_{7,2})| = 6$ the group given by this presentation must be $PSL_2(\mathcal{O}_{7,2})$.

The method of this section ie getting GAP [24] to list all subgroups of Γ_d of the relevent index and then labouriously checking whether the generators for each lay in $PSL_2(\mathcal{O}_{d,m})$ is very unsophisticated and consequently of use in only very few cases. Swan [84] has developed a method for computing presentations for $PSL_2(\mathcal{O}_d)$ which can easily be extended to the $PSL_2(\mathcal{O}_{d,m})$ ([78] page 628). However the computations rapidly become unwieldy as d becomes large. Riley [78] developed a computer package (written in Fortran) called the *Poincaré File* which he used to find presentations for $PSL_2(\mathcal{O}_d)$ for $10 < d < 37$ and $d = 43, 67, 163$. Such an approach can be used to find presentations for $PSL_2(\mathcal{O}_{d,m})$. The implementation of this in GAP [24] could be an interesting future project.

Chapter 4

Non-standard normal subgroups of $SL_2(\mathcal{O}_{d,m})$

Let R be a commutative ring with a one. Let $n \in \mathbb{N}$ such that $n \geqslant 2$. Let $1 \leqslant i,j \leqslant n$ then e_{ij} denotes the $n \times n$ matrix with a 0 in every position except (i,j), where it has a 1.

$$E_n(R) =< I + re_{ij} : 1 \leqslant i,j \leqslant n, i \neq j >$$

Let $\mathfrak{q} \lhd R$

$$E_n(R,\mathfrak{q}) =< I + \alpha e_{ij} : \alpha \in \mathfrak{q}, 1 \leqslant i,j \leqslant n, i \neq j >^{E_n(R)}$$

the largest $\mathfrak{q}$ such that $E_n(R,\mathfrak{q}) \leqslant S$ is the *level* of S and is denoted $l(S)$. This is well defined because $E_n(R,\mathfrak{q}_1)E_n(R,\mathfrak{q}_2) = E_n(R,\mathfrak{q}_1 + \mathfrak{q}_2)$.

$$H_n(R,\mathfrak{q}) = \{M \in SL_n(R) : M \equiv kI \pmod{\mathfrak{q}}, \text{ some } k \in R\}$$

the smallest $\mathfrak{q}$ such that $S \leqslant H_n(R,\mathfrak{q})$ is the *order* of S and is denoted $o(S)$. $S \leqslant SL_n(R)$ is said to be *standard* if $l(S) = o(S)$.

$$\mathcal{E}_0(2,R;\mathfrak{q}) = \{N \lhd SL_2(R) : o(N) = \mathfrak{q}, l(N) = 0\}$$

4.1 Non-standard normal subgroups of $SL_2(\mathbb{Z})$

Here we describe the proof of the following theorem, mentioned in chapter one. This proof appeared in [62].

Theorem. *Let* $0 \neq \mathfrak{q} \lhd \mathbb{Z}$ *then* $|\mathcal{E}_0(2,\mathbb{Z};\mathfrak{q})| = 2^{\aleph_0}$.

First recall that the Modular group, $PSL_2(\mathbb{Z})$, has the presentation $< x, y; x^2, y^3 >$ (see [81]).

Theorem. *[62] Every countable group can be embedded in an infinite simple group generated by* x, y *of order* $2, 3$ *respectively, and where* xy *has infinite order.*

Corollary. *[62]* $\exists 2^{\aleph_0}\ N \lhd SL_2(\mathbb{Z})$ *such that* $SL_2(\mathbb{Z})/N$ *is simple, and* $l(N) = 0$.

Lemma 4.1.1. *[62] Let* X, Y *be sets,* X *infinite. Let* $f : X \longrightarrow Y$ *be a surjection. For* $y \in Y$ *let* $c_y = |f^{-1}(y)|$. *Then if* $\exists c_0$ *such that* $c_y \leqslant c_0 \lneq |X|\ \forall y \in Y$ *then* $|X| = |Y|$.

Proof. Obviously $|Y| \leqslant |X|$. Now $|X| = \sum_{y \in Y} c_y \leqslant |Y|c_y \leqslant |Y|c_0$, and $c_o \lneq |X|$ so $|X| \leqslant |Y|$. □

Theorem. *[62] Let* $0 \neq \mathfrak{q} \lhd \mathbb{Z}$ *then* $|\mathcal{E}_0(2,\mathbb{Z};\mathfrak{q})| = 2^{\aleph_0}$.

Proof. Let

$$\mathcal{S} = \{N \lhd SL_2(\mathbb{Z}) : l(N) = 0, SL_2(\mathbb{Z})/N \text{ simple } \}$$

so $|\mathcal{S}| = 2^{\aleph_0}$. We show that if $N \in \mathcal{S}$ then $o(N) = \mathbb{Z}$ and so $|\mathcal{E}_0(2,\mathbb{Z},\mathbb{Z})| = |\mathcal{S}| = 2^{\aleph_0}$. Let $N \in \mathcal{S}$, let $\mathfrak{q}_0 = o(N)$. So, since $N \leqslant H(\mathfrak{q}_0) \lhd SL_2(\mathbb{Z})$ $H(\mathfrak{q}_0) = N$ or $SL_2(\mathbb{Z})$. Suppose $H(\mathfrak{q}_0) = N$ then $\mathfrak{q}_0 = l(H(\mathfrak{q}_0)) = l(N) = 0$ so $o(N) = 0$, but $o(N) = 0 \Leftrightarrow N = 1$ or $\{I, -I\}$ and $PSL_2(\mathbb{Z})$ is not simple, so $o(N) \neq 0$. Hence $H(\mathfrak{q}_0) = SL_2(\mathbb{Z})$ so $\mathfrak{q}_0 = l(H(\mathfrak{q}_0)) = l(SL_2(\mathbb{Z})) = \mathbb{Z}$ i.e. $o(N) = \mathbb{Z}$.

Now suppose $\mathfrak{q} \neq \mathbb{Z}$. Let $\mathcal{S}_1 = \{H(\mathfrak{q}) \cap N : N \in \mathcal{S}\}$. Define $\rho : \mathcal{S} \longrightarrow \mathcal{S}_1$ by $\rho(N) = H(\mathfrak{q}) \cap N$. Let $X \in \mathcal{S}_1$, and let $\mathcal{S}_2 = \rho^{-1}(X) \subseteq \mathcal{S}$. Suppose $Y \in \mathcal{S}_2$ so $SL_2(\mathbb{Z})/Y$ is simple and $o(Y) = \mathbb{Z}$. Now $YH(\mathfrak{q}) = Y$, or $SL_2(\mathbb{Z})$. Suppose that $YH(\mathfrak{q}) = Y$, so $H(\mathfrak{q}) \leqslant Y$. So $\mathfrak{q} \leqslant l(Y) = 0$. Contradiction. Hence $YH(\mathfrak{q}) = SL_2(\mathbb{Z})$, so

$$|Y : X| = |Y : H(\mathfrak{q}) \cap Y| = |SL_2(\mathbb{Z}) : H(\mathfrak{q})| \lneq \infty$$

so $|\mathcal{S}_2| \leqslant \aleph_0$. Now $\mathcal{S}$ is infinite, ρ is a surjection and $|\mathcal{S}_2| \leqslant \aleph_0 \lneq 2^{\aleph_0} = |\mathcal{S}|$, so by the lemma $|\mathcal{S}_1| = |\mathcal{S}| = 2^{\aleph_0}$.

We now show that if $M \in \mathcal{S}_1$ then $l(M) = 0$ and $o(M) = \mathfrak{q}$, and so $|\mathcal{E}_0(2,\mathbb{Z};\mathfrak{q})| = 2^{\aleph_0}$, as required. Let $M \in \mathcal{S}_1$, so $M = H(\mathfrak{q}) \cap N$, some $N \in \mathcal{S}$. Now $M \leqslant N$, so $l(M) \leqslant$

$l(N) = 0$, so $l(M) = 0$. Let $\mathfrak{q}_1 = o(M)$. Now $M \leqslant H(\mathfrak{q})$ so $o(M) = \mathfrak{q}_1 \leqslant \mathfrak{q}$. Let $\hat{N}$ be the image of N in $PSL_2(\mathbb{Z})$, so, as $-I \in N$

$$\frac{SL_2(\mathbb{Z})}{N} \cong \frac{PSL_2(\mathbb{Z})}{\hat{N}}$$

since $\hat{N}$ is of infinite index in $PSL_2(\mathbb{Z})$, $\hat{N}$ is free and so contains elements of infinite order. So N contains elements of infinite order. Now, as before

$$|N : M| = |N : H(\mathfrak{q}) \cap N| = |SL_2(\mathbb{Z}) : H(\mathfrak{q})| < \infty$$

so M contains elements of infinite order, so $\mathfrak{q}_1 = o(M) \neq 0$. Now, as before, $NH(\mathfrak{q}_1) = SL_2(\mathbb{Z})$, so

$$\begin{aligned} H(\mathfrak{q}) &= H(\mathfrak{q}) \cap NH(\mathfrak{q}_1) \\ &= H(\mathfrak{q}_1)(N \cap H(\mathfrak{q})) \\ &= H(\mathfrak{q}_1)M \\ &= H(\mathfrak{q}_1). \end{aligned}$$

so $\mathfrak{q}_1 = \mathfrak{q}$. Hence result. □

4.2 Non-standard normal subgroups of $SL_2(\mathcal{O}_{d,m})$

In this section we aim to extend the results proved above to the groups $SL_2(\mathcal{O}_d)$. This answers a question of Lubotzky's (MR92c : 20088). In fact we extend it to all $SL_2(\mathcal{O}_{d,m})$ with a free non-abelian quotient, more precisely what we require is that the group maps onto the Modular group, M in a "nice" way. Recall from chapter two that it is conjectured that the only $SL_2(\mathcal{O}_{d,m})$ which do not have a free non-abelian quotient are $SL_2(\mathcal{O}_1)$, $SL_2(\mathcal{O}_{1,2})$, $SL_2(\mathcal{O}_2)$, $SL_2(\mathcal{O}_3)$, $SL_2(\mathcal{O}_{3,2})$, $SL_2(\mathcal{O}_7)$, $SL_2(\mathcal{O}_{11})$, and $SL_2(\mathcal{O}_{19})$. We show that in fact $SL_2(\mathcal{O}_{1,2})$, $SL_2(\mathcal{O}_2)$, and $SL_2(\mathcal{O}_{3,2})$ map onto the Modular group in a "nice" way and so the result goes though for these groups as well, leaving only 5 true exceptions. We prove an unsatisfactory version of the result for $SL_2(\mathcal{O}_7)$, $SL_2(\mathcal{O}_{11})$, and $SL_2(\mathcal{O}_{19})$ (which relies on the fact that they have an infinite cyclic quotient) but we were unable to make any progress with $SL_2(\mathcal{O}_1)$ and $SL_2(\mathcal{O}_3)$.

Lemma 4.2.1. *Let $N \lhd SL_2(\mathcal{O}_{d,m})$. Then*

$$l(N) = 0 \Leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix} \text{ has infinite order mod } N.$$

Proof. Suppose that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix}$$

have finite order mod N i.e.

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & tm\omega \\ 0 & 1 \end{pmatrix} \in N, \text{ some } s, t \in \mathbb{N}.$$

Let $M = st$, let $\mathfrak{q} = (M) \lhd \mathcal{O}_{d,m}$, so $\mathfrak{q} \neq 0$. Let $\alpha \in \mathfrak{q}$, so

$$\alpha = (z_1 + m\omega z_2)M = z_1 M + m\omega z_2 M,$$

some $z_1, z_2 \in \mathbb{Z}$. So

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & M \\ 0 & 1 \end{pmatrix}^{z_1} \begin{pmatrix} 1 & m\omega M \\ 0 & 1 \end{pmatrix}^{z_2} \in N.$$

Hence $E_2(\mathcal{O}_{d,m}, \mathfrak{q}) \leqslant N$, so $l(N) \neq 0$.

Conversely suppose $l(N) \neq 0$. So $E_2(\mathcal{O}_{d,m}, \mathfrak{q}) \leqslant N$, some $\mathfrak{q} \neq 0$. Now $|\mathcal{O}_{d,m} : \mathfrak{q}| \lneqq \infty$, and so $1 + \mathfrak{q}$ has finite (additive) order i.e. $s \in \mathfrak{q}$, some $s \in \mathbb{N}$. Similarly $tm\omega \in \mathfrak{q}$, some $t \in \mathbb{N}$. So

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & tm\omega \\ 0 & 1 \end{pmatrix} \in N$$

i.e.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$$

have finite order mod N. □

Recall the following result from lemma (2.3.2).

Theorem 4.2.2. *Suppose $r = r(d, m) \geqslant 1$ then there exists a surjective homomorphism*

$$\rho : SL_2(\mathcal{O}_{d,m}) \longrightarrow F_r =< x_1, \ldots, x_r >$$

such that

$$\rho \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix} = x_1$$

Now consider the case $r(d,m) > 1$.

Lemma 4.2.3. *If $r(d,m) > 1$ then $\exists 2^{\aleph_0} N \lhd SL_2(\mathcal{O}_{d,m})$ such that $SL_2(\mathcal{O}_{d,m})/N$ is simple, $l(N) = 0$, and N contains elements of infinite order.*

Proof. We have

$$\varphi : SL_2(\mathcal{O}_{d,m}) \twoheadrightarrow F_r \twoheadrightarrow < x_1, x_2; x_2^2, (x_1x_2)^3 > \cong PSL_2(\mathbb{Z})$$

and

$$u = \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix} \mapsto x_1 \mapsto t$$

Now by a result of Mason and Pride [62] mentioned in the previous section the Modular group $PSL_2(\mathbb{Z})$ has $2^{\aleph_0}$ normal subgroups N such that $PSL_2(\mathbb{Z})/N$ is simple and t has infinite order mod N. Pulling these subgroups back to $SL_2(\mathcal{O}_{d,m})$ we get $2^{\aleph_0}$ normal subgroups N of $SL_2(\mathcal{O}_{d,m})$ such that $SL_2(\mathcal{O}_{d,m})/N$ is simple and u has infinite order mod N. Further, as $\ker \varphi$ contains $SL_2(\mathbb{Z})$, N contains elements of infinite order. Hence result. □

We can now generalize almost word for word the corresponding proof for the Modular group.

Theorem 4.2.4. *Suppose $r(d,m) > 1$ and let $0 \neq \mathfrak{q} \lhd \mathcal{O}_{d,m}$ then $|\mathcal{E}_0(2, \mathcal{O}_{d,m}; \mathfrak{q})| = 2^{\aleph_0}$.*

Proof. Let

$$\mathcal{S} = \{N \lhd SL_2(\mathcal{O}_{d,m}) : l(N) = 0, SL_2(\mathbb{Z}) \leqslant N, SL_2(\mathcal{O}_{d,m})/N \text{ simple } \}$$

so, by (4.2.3), $|\mathcal{S}| = 2^{\aleph_0}$. We show that if $N \in \mathcal{S}$ then $o(N) = \mathcal{O}_{d,m}$ and so $|\mathcal{E}_0(2, \mathcal{O}_{d,m}, \mathcal{O}_{d,m})| = |\mathcal{S}| = 2^{\aleph_0}$. Let $N \in \mathcal{S}$, let $\mathfrak{q}_0 = o(N)$. So, since $N \leqslant H(\mathfrak{q}_0) \lhd SL_2(\mathcal{O}_{d,m})$ we have $H(\mathfrak{q}_0) = N$ or $SL_2(\mathcal{O}_{d,m})$. Suppose $H(\mathfrak{q}_0) = N$ then $\mathfrak{q}_0 = l(H(\mathfrak{q}_0)) = l(N) = 0$ so $o(N) = 0$, but $o(N) = 0 \Leftrightarrow N = 1$ or $\{I, -I\}$ and $PSL_2(\mathcal{O}_{d,m})$ is not simple, so $o(N) \neq 0$. Hence $H(\mathfrak{q}_0) = SL_2(\mathcal{O}_{d,m})$ so $\mathfrak{q}_0 = l(H(\mathfrak{q}_0)) = l(SL_2(\mathcal{O}_{d,m})) = \mathcal{O}_{d,m}$ i.e. $o(N) = \mathcal{O}_{d,m}$.

Now suppose $\mathfrak{q} \neq \mathcal{O}_{d,m}$. Let $\mathcal{S}_1 = \{H(\mathfrak{q}) \cap N : N \in \mathcal{S}\}$. Define $\rho : \mathcal{S} \longrightarrow \mathcal{S}_1$ by $\rho(N) = H(\mathfrak{q}) \cap N$. Let $X \in \mathcal{S}_1$, and let $\mathcal{S}_2 = \rho^{-1}(X) \subseteq \mathcal{S}$. Suppose $Y \in \mathcal{S}_2$ so $SL_2(\mathcal{O}_{d,m})/Y$ is simple and $o(Y) = \mathcal{O}_{d,m}$. So $YH(\mathfrak{q}) = Y$, or $SL_2(\mathcal{O}_{d,m})$. Suppose that

$YH(\mathfrak{q}) = Y$, so $H(\mathfrak{q}) \leqslant Y$, so $\mathfrak{q} \leqslant l(Y) = 0$. Contradiction. Hence $YH(\mathfrak{q}) = SL_2(\mathcal{O}_{d,m})$. Now

$$|Y : X| = |Y : H(\mathfrak{q}) \cap Y| = |SL_2(\mathcal{O}_{d,m}) : H(\mathfrak{q})| \lneq \infty$$

so $|\mathcal{S}_2| \leqslant \aleph_0$. Now $\mathcal{S}$ is infinite, ρ is a surjection and $|\mathcal{S}_2| \leqslant \aleph_0 \lneq 2^{\aleph_0} = |\mathcal{S}|$, so by lemma (4.1.1), $|\mathcal{S}_1| = |\mathcal{S}| = 2^{\aleph_0}$.

We now show that if $M \in \mathcal{S}_1$ then $l(M) = 0$ and $o(M) = \mathfrak{q}$, and so $|\mathcal{E}_0(2, \mathcal{O}_{d,m}; \mathfrak{q})| = 2^{\aleph_0}$, as required. Let $M \in \mathcal{S}_1$, so $M = H(\mathfrak{q}) \cap N$, some $N \in \mathcal{S}$. Now $M \leqslant N$, so $l(M) \leqslant l(N) = 0$, so $l(M) = 0$. Let $\mathfrak{q}_1 = o(M)$. Now $M \leqslant H(\mathfrak{q})$ so $o(M) = \mathfrak{q}_1 \leqslant \mathfrak{q}$. Now N contains elements of infinite order. So, as before,

$$|N : M| = |N : H(\mathfrak{q}) \cap N| = |SL_2(\mathcal{O}_{d,m}) : H(\mathfrak{q})| < \infty$$

so M contains elements of infinite order, so $\mathfrak{q}_1 = o(M) \neq 0$. As before, $NH(\mathfrak{q}_1) = SL_2(\mathcal{O}_{d,m})$, so

$$\begin{aligned} H(\mathfrak{q}) &= H(\mathfrak{q}) \cap NH(\mathfrak{q}_1) \\ &= H(\mathfrak{q}_1)(N \cap H(\mathfrak{q})) \\ &= H(\mathfrak{q}_1)M \\ &= H(\mathfrak{q}_1). \end{aligned}$$

so $\mathfrak{q}_1 = \mathfrak{q}$. Hence result. □

We have already seen in chapter two that when $r(d,m) = 1$ we may still have a free

r**Lemma 4.2.5.** *For $(d,m) = (5,1)$, $(6,1)$, $(15,1)$, $(14,1)$, $(7,2)$, $(11,2)$, $SL_2(\mathcal{O}_{d,m})$ has a free quotient of rank 2 and the image of*

Lemma 4.2.5. *For $(d,m) = (5,1)$, $(6,1)$, $(15,1)$, $(14,1)$, $(7,2)$, $(11,2)$, $SL_2(\mathcal{O}_{d,m})$ has a free quotient of rank 2 and the image of*

$$\begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix}$$

can be taken as a free generator. Further the kernel of this map contains an element of infinite order.

Proof. Here we work with the presentations for $PSL_2(\mathcal{O}_{d,m})$, as these are a homomorphic images of $SL_2(\mathcal{O}_{d,m})$ this is sufficient. In the following the presentations for $d = 5, 6, 15$

are taken from [84], and for $d = 14$ from [30]. The presentations for $PSL_2(\mathcal{O}_{7,2})$ and $PSL_2(\mathcal{O}_{11,2})$ can be found in (3.5). a, t, u have the usual meanings.

$$PSL_2(\mathcal{O}_5) =< a,t,u,b,c; a^2, (at)^3, [t,u], b^2, (ab)^2, (aubu^{-1})^2, aca = tct^{-1}, ubu^{-1}cb = tct^{-1} >$$

so $PSL_2(\mathcal{O}_5)/N(a,t,b) =< u,c; >\cong F_2$.

$$PSL_2(\mathcal{O}_6) =< a,t,u,b,c; a^2, (at)^3, [t,u], b^2, [a,c], (atb)^3, t^{-1}ctubu^{-1} = bc, (atubu^{-1})^3 >$$

so $PSL_2(\mathcal{O}_6)/N(a,t,b) =< u,c; >\cong F_2$.

$$PSL_2(\mathcal{O}_{15}) =< a,t,u,c; a^2, (at)^3, [t,u], [a,c], ucuat = taucu >$$

so $PSL_2(\mathcal{O}_{15})/N(a,t) =< u,c; >\cong F_2$.

$$\begin{aligned} PSL_2(\mathcal{O}_{14}) =< a,t,u,b,c,d,e; a^2, (at)^3, [t,u], [a,b], & cd^{-1}eb^{-1}dc^{-1}be^{-1}, \\ & dau^{-1}b^{-1}dad^{-1}baud^{-1}a, \\ & adtad^{-1}ad^{-1}bt^{-1}ab^{-1}d, \\ & at^{-1}ae^{-1}dat^{-1}d^{-1}acatad^{-1}eatb^{-1}dac^{-1}b > \end{aligned}$$

after some calculation we see that $PSL_2(\mathcal{O}_{14})/N(a,t,b,e,d) =< u,c; >\cong F_2$.

$$\begin{aligned} PSL_2(\mathcal{O}_{11,2}) =< a,t,w,k,l,m,n; a^2, (at)^3, k^2, [m,n], [t,w], tklkt^{-1}l^{-1}, km^{-1}ltat^{-1}l^{-1}m, \\ nlat^{-1}l^{-1}n^{-1}mwaw^{-1}tm^{-1}, m^{-1}tklt^{-1}l^{-1}mwt^{-1}aw^{-1}t > \end{aligned}$$

so $PSL_2(\mathcal{O}_{11,2})/N(a,k,t,m,n) =< w,l; >\cong F_2$.

$$\begin{aligned} PSL_2(\mathcal{O}_{7,2}) =< a,t,w,x,y\,; a^2, x^2, [t,w], (ax)^3, (at)^3, y = txyxt^{-1}, (ytay^{-1}x)^2, \\ xyat^{-1}y^{-1}wt^{-1}aw^{-1}t > \end{aligned}$$

so $PSL_2(\mathcal{O}_{7,2})/N(a,x,t) =< w,y; >\cong F_2$. □

It is clear from the proof of theorem (4.2.4) that it is sufficient for $SL_2(\mathcal{O}_{d,m})$ to map onto the Modular group with kernel of level zero. We remark that $PSL_2(\mathcal{O}_5)/N(b,c,u) \cong PSL_2(\mathcal{O}_6)/N(b,c,u) = < a,t; a^2, (at)^3 >= PSL_2(\mathbb{Z})$.

Lemma 4.2.6.

$$\frac{PSL_2(\mathcal{O}_2)}{N(u)} =< a, t; a^2, (at)^3 >\cong PSL_2(\mathbb{Z})$$

$$\frac{PSL_2(\mathcal{O}_{3,2})}{N(w)} =< a, t; a^2, (at)^3 >\cong PSL_2(\mathbb{Z})$$

$$\frac{PSL_2(\mathcal{O}_{1,2})}{N(a, t, (zw)^3)} =< z, w; z^2, (zw)^3 >\cong PSL_2(\mathbb{Z})$$

Clearly the kernels contain elements of infinite order.

Proof. This is obvious given the following presentations

$$PSL_2(\mathcal{O}_2) =< a, t, u; a^2, (at)^3, (u^{-1}aua)^2, [t, u] >$$

$$PSL_2(\mathcal{O}_{3,2}) =< a, t, w; a^2, (at)^3, (w^{-1}awa)^3, [t, w] >$$

$$PSL_2(\mathcal{O}_{1,2}) =< a, t, w, z; a^2, z^2, (at)^3, (atz)^2, [t, w], (atw^{-1}zw)^2 >$$

The presentation for $PSL_2(\mathcal{O}_2)$ can be found in [25]. The presentation for $PSL_2(\mathcal{O}_{1,2})$ can be found in (3.5.1) and for $PSL_2(\mathcal{O}_{3,2})$ in (3.3.1). □

Thus we have

Proposition 4.2.7. *Let* $(d, m) = (1, 2), (2, 1), (3, 2), (5, 1), (6, 1), (14, 1), (15, 1)$. *Let* $0 \neq \mathfrak{q} \lhd \mathcal{O}_{d,m}$ *then* $|\mathcal{E}_0(2, \mathcal{O}_{d,m}; \mathfrak{q})| = 2^{\aleph_0}$.

The only "true exceptions" not covered above are $SL_2(\mathcal{O}_1)$, $SL_2(\mathcal{O}_3)$, $SL_2(\mathcal{O}_7)$, $SL_2(\mathcal{O}_{11})$, and $SL_2(\mathcal{O}_{19})$. The results we can achieve are very unsatisfactory. When we have an infinite cyclic quotient we get the following result

Theorem 4.2.8. *Suppose* $SL_2(\mathcal{O}_{d,m})/K \cong \mathbb{Z}$ *and* $l(K) = 0$ *then* $\forall\, 0 \neq \mathfrak{q} \lhd \mathcal{O}_{d,m}$ $\exists N \lhd SL_2(\mathcal{O}_{d,m})$ *such that* $l(N) = 0$ *and* $o(N) = \mathfrak{q}$.

The following lemma was proved in [63] as Theorem 4.1 for any $n \geqslant 2$ and any Dedekind domain of arithmetic type, A.

Lemma 4.2.9. *Let R be a commutative ring with a one, $\mathfrak{q}_1, \mathfrak{q}_2 \lhd R$ such that $R/\mathfrak{q}_2$ is an SR_2-ring $\mathfrak{q}_2 \leqslant \mathfrak{q}_1$. Then*

$$\frac{SL_2(R,\mathfrak{q}_1)}{SL_2(R,\mathfrak{q}_2)} \text{ is abelian } \Leftrightarrow \mathfrak{q}_1^2 \leqslant \mathfrak{q}_2$$

Furthermore, if $SL_2(R,\mathfrak{q}_1)/SL_2(R,\mathfrak{q}_2)$ is abelian then $SL_2(R,\mathfrak{q}_1)/SL_2(R,\mathfrak{q}_2) \cong \mathfrak{a}^3$, where $\mathfrak{a} = \mathfrak{q}_1/\mathfrak{q}_2$, and the isomorphism is given by:

$$\begin{pmatrix} 1+z & x \\ y & 1-z \end{pmatrix} \longleftrightarrow (x,y,z).$$

Proof. Denote $SL_2(R,\mathfrak{q}_i)$ by $\Gamma(\mathfrak{q}_i)$. Now suppose that $\mathfrak{q}_1^2 \leqslant \mathfrak{q}_2$ and let $X, Y \in \Gamma(\mathfrak{q}_1)$. Then $X - I, Y - I \equiv 0 \pmod{\mathfrak{q}_1}$ and so we have

$$(X-I)(Y-I) \equiv (Y-I)(X-I) \equiv 0 \pmod{\mathfrak{q}_1^2}$$

It follows that $XY \equiv YX \pmod{\mathfrak{q}_2}$ and so $\Gamma(\mathfrak{q}_1)' \subseteq \Gamma(\mathfrak{q}_2)$. Conversely suppose that $\Gamma(\mathfrak{q}_1)\ /\ \Gamma(\mathfrak{q}_2)$ is abelian. Let $x, y \in \mathfrak{q}_1$ then

$$[I + xe_{12}, I + ye_{21}] = \begin{pmatrix} * & * \\ * & 1-xy \end{pmatrix} \equiv I \pmod{\mathfrak{q}_2}$$

and so $xy \in \mathfrak{q}_2$ hence $\mathfrak{q}_1^2 \subseteq \mathfrak{q}_2$.

Recall that by lemma (3.1.1), $\varphi : SL_2(R) \longrightarrow SL_2(R/\mathfrak{q}_2)$ is surjective, and $\Gamma(\mathfrak{q}_2) = \mathrm{Ker}\varphi$. Let $\gamma(\mathfrak{q}_1) = \varphi(\Gamma(\mathfrak{q}_1))$ and observe that $\gamma(\mathfrak{q}_1) \cong \Gamma(\mathfrak{q}_1)/\Gamma(\mathfrak{q}_2)$. We show that $\gamma(\mathfrak{q}_1) \cong \mathfrak{a}^3$. Define $\theta : \mathfrak{a}^3 \longrightarrow SL_2(R/\mathfrak{q}_2)$ by

$$(x,y,z) \longmapsto \begin{pmatrix} 1+z & x \\ y & 1-z \end{pmatrix}.$$

We first show that θ is a homomorphism. Let $x_i, y_i, z_i \in \mathfrak{a}$ where $i = 1, 2$. Then since $\mathfrak{q}_1^2 \leqslant \mathfrak{q}_2$,

$$\theta\,(x_1,y_1,z_1)\,\theta\,(x_2,y_2,z_2) = \begin{pmatrix} 1+z_1+z_2 & x_1+x_2 \\ y_1+y_2 & 1-z_1-z_2 \end{pmatrix} = \theta\,(x_1+x_2, y_1+y_2, z_1+z_2)$$

So θ is a homomorphism.

We now show that θ is injective. Suppose that $\theta\,(x,y,z) = 1$ i.e.

$$\begin{pmatrix} 1+z & x \\ y & 1-z \end{pmatrix} \equiv I \pmod{\mathfrak{q}_2}$$

so $(x, y, z) = 0$ and so θ is injective.

We now show that $im\theta = \gamma(\mathfrak{q}_1)$. Let $X \in im\theta$. Since $X \in SL_2(R/\mathfrak{q}_2)$ and φ is surjective $\exists Y \in SL_2(R)$ such that $\varphi(Y) = X$. We show $Y \in \Gamma(\mathfrak{q}_1)$ and so $X = \varphi (Y) \in \gamma(\mathfrak{q}_1)$. Now $X \in im\theta$ so

$$X = \begin{pmatrix} 1+z & x \\ y & 1-z \end{pmatrix}$$

some $x, y, z \in \mathfrak{a}$. Let

$$Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $a, b, c, d \in R$. So $a \in 1 + z$, $b \in x$, $c \in y$, $d \in 1 - z$, so $a, d \equiv 1 \pmod{\mathfrak{q}_1}$ and $b, c \equiv 0 \pmod{\mathfrak{q}_1}$, so $Y \equiv I \pmod{\mathfrak{q}_1}$ i.e. $Y \in \Gamma(\mathfrak{q}_1)$. Hence $im\theta \subseteq \gamma(\mathfrak{q}_1)$.

Now we show that $\gamma(\mathfrak{q}_1) \subseteq im\theta$. Let $X \in \gamma(\mathfrak{q}_1)$, so $X = \varphi(Y)$ some $Y \in \Gamma(\mathfrak{q}_1)$. RTP

$$X = \begin{pmatrix} 1+z & x \\ y & 1-z \end{pmatrix}$$

some $x, y, z \in \mathfrak{a}$. Let

$$Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $a, b, c, d \in R$. Now $Y \equiv I \pmod{\mathfrak{q}_1}$ so $a, d \equiv 1 \pmod{\mathfrak{q}_1}$ and $b, c \equiv 0 \pmod{\mathfrak{q}_1}$. Let $x = b + \mathfrak{q}_2$, $y = c + \mathfrak{q}_2$ so that $x, y \in \mathfrak{a}$. Now let $z = \zeta + \mathfrak{q}_2 = (a-1) + \mathfrak{q}_2$ and since $a \equiv 1 \pmod{\mathfrak{q}_1}$ we have $z \in \mathfrak{a}$. We show that $d + \mathfrak{q}_2 = 1 - z$. Now $(a-1)(d-1) \in \mathfrak{q}_1^2 \leqslant \mathfrak{q}_2$ and so $a + d \equiv 2 \pmod{\mathfrak{q}_2}$. So now $1 - z = 1 - \zeta + \mathfrak{q}_2 = 1 - (a-1) + \mathfrak{q}_2 = 2 - a + \mathfrak{q}_2 = d + \mathfrak{q}_2$. Hence

$$X = \varphi(Y) = \begin{pmatrix} a+\mathfrak{q}_2 & b+\mathfrak{q}_2 \\ c+\mathfrak{q}_2 & d+\mathfrak{q}_2 \end{pmatrix} = \begin{pmatrix} 1+z & x \\ y & 1-z \end{pmatrix}$$

some $x, y, z \in \mathfrak{a}$. Hence $\gamma(\mathfrak{q}_1) \subseteq im\theta$. Hence result. □

Theorem 4.2.10. *Suppose that $SL_2(\mathcal{O}_{d,m})/K \cong \mathbb{Z}$ and $l(K) = 0$. Then $\forall\ 0 \neq \mathfrak{q} \lhd \mathcal{O}_{d,m}$ $\exists N \lhd SL_2(\mathcal{O}_{d,m})$ such that $l(N) = 0$ and $o(N) = \mathfrak{q}$.*

Proof. Let $0 \neq \mathfrak{q}_1 \lhd \mathcal{O}_{d,m}$ and consider $H(\mathfrak{q}_1) \cap K$. Let $\mathfrak{q}_2 = o(H(\mathfrak{q}_1) \cap K)$, so $\mathfrak{q}_2 \leqslant \mathfrak{q}_1$. Clearly $l(H(\mathfrak{q}_1) \cap K) = 0$. We show $\mathfrak{q}_1 = \mathfrak{q}_2$. Suppose not. Now $\Gamma/K \cong \mathbb{Z}$ so

$H(\mathfrak{q}_1) \;/\; H(\mathfrak{q}_2)$ is cyclic, so $\Gamma(\mathfrak{q}_1)/\Gamma(\mathfrak{q}_1)\cap H(\mathfrak{q}_2)$ is cyclic. Also $\Gamma(\mathfrak{q}_1)\cap H(\mathfrak{q}_2)/\Gamma(\mathfrak{q}_2)$ is central in $\Gamma(\mathfrak{q}_1)/\Gamma(\mathfrak{q}_2)$. So $\Gamma(\mathfrak{q}_1)/\Gamma(\mathfrak{q}_2)$ is central by cyclic, and so abelian. Hence $\mathfrak{q}_1^2 \leqslant \mathfrak{q}_2$. Let $\mathfrak{a} = \mathfrak{q}_1/\mathfrak{q}_2$. So $\Gamma(\mathfrak{q}_1)/\Gamma(\mathfrak{q}_2) \cong \mathfrak{a}^3$. Where

$$\begin{pmatrix} 1+z & x \\ y & 1-z \end{pmatrix} \longleftrightarrow (x,y,z)$$

We show $\mathfrak{a}^2 \hookrightarrow \Gamma(\mathfrak{q}_1)/\Gamma(\mathfrak{q}_1)\cap H(\mathfrak{q}_2)$. Define

$$\varphi : \mathfrak{a}^2 \longrightarrow \frac{\Gamma(\mathfrak{q}_1)}{\Gamma(\mathfrak{q}_1)\cap H(\mathfrak{q}_2)}$$

by

$$\varphi(x,y) = \begin{pmatrix} 1 & x \\ y & 1 \end{pmatrix}.$$

φ is clearly a homomorphism. Now suppose that $\varphi(x,y) = 1$. So

$$\begin{pmatrix} 1 & x \\ y & 1 \end{pmatrix} \in \Gamma(\mathfrak{q}_1)\cap H(\mathfrak{q}_2),$$

so $x, y \in \mathfrak{q}_2$, so $(x,y) = 0$ in $\mathfrak{a}^2$, hence φ is injective. So $\mathfrak{a}^2$ is cyclic, so $\mathfrak{a}$ is trivial i.e. $\mathfrak{q}_1 = \mathfrak{q}_2$. □

The only (d,m) excluded from the above theorem are $(1,1)$, and $(3,1)$. Neither $SL_2(\mathcal{O}_1)$ nor $SL_2(\mathcal{O}_3)$ have infinite cyclic quotients and so using the above techniques we are unable to say anything about $\mathcal{E}_0(2,\mathcal{O}_d;\mathfrak{q})$ for $d = 1,3$.

However despite the difficulties mentioned above we feel confident in making the following

Conjecture. $\forall (d,m)$ and $\forall\, 0 \neq \mathfrak{q} \lhd \mathcal{O}_{d,m}$, $|\mathcal{E}_0(2,\mathcal{O}_{d,m};\mathfrak{q})| = 2^{\aleph_0}$.

Chapter 5

Order and level of a normal congruence subgroup

We have seen that in general there is no relationship between the order and level of a normal subgroup of $SL_2(\mathcal{O}_{d,m})$. However if we restrict ourselves to normal *congruence* subgroups we do find a nice relationship. Mason [58] has proved

Theorem. *Let $N \lhd SL_2(\mathcal{O}_d)$ be a congruence subgroup of level $\mathfrak{q}^*$ and order $\mathfrak{q}$. Then* $12\mathfrak{q} \leqslant \mathfrak{q}^*$.

Suppose that $N \lhd SL_2(\mathcal{O}_d)$ is a congruence subgroup of order $\mathcal{O}_d$ then $SL_2(\mathcal{O}_d, 12\mathcal{O}_d) \leqslant N$. We use this fact to show that a large class of subgroups of the $SL_2(\mathcal{O}_d)$ are non-congruence subgroups. First of all we aim to extend the above results to $SL_2(\mathcal{O}_{d,m})$. In fact we extend it to SL_2 over a larger class of rings. The material in this chapter is the most technically complex and perhaps the hardest to follow in this thesis, so we apologize to the reader for the Cimmerian night which is about to descend.

5.1 Primary decomposition in Noetherian domains

The material in this section has been lifted from chapters four, seven, and eleven of Atiyah and MacDonald [2]. Let A be any commutative ring.

Definition. $\mathfrak{q} \lhd A$ is *primary* if $\mathfrak{q} \neq A$ and $xy \in \mathfrak{q} \Rightarrow x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$, some $n \geqslant 0$.

Definition. Let $\mathfrak{q} \lhd A$. Then the *radical* of $\mathfrak{q}$ is

$$r(\mathfrak{q}) = \{x \in A : x^n \in \mathfrak{q}, \text{some } n \geqslant 0\}$$

Proposition 5.1.1. *([2] Proposition 1.14) The radical of $\mathfrak{q} \lhd A$ is the intersection of all prime ideals which contain $\mathfrak{q}$.*

Proposition 5.1.2. *([2] Exercise 1.13) Let $\mathfrak{a}, \mathfrak{b} \lhd A$. Then*

$$r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$$

Proposition 5.1.3. *([2] Proposition 4.1) Let $\mathfrak{q} \lhd A$ be primary. Then $r(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.*

Definition. Let $\mathfrak{a} \lhd A$. A primary decomposition of $\mathfrak{a}$ is

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

where $\mathfrak{q}_i \lhd A$ is primary.

Definition. If $\mathfrak{p} = r(\mathfrak{q})$ we say that $\mathfrak{q}$ is $\mathfrak{p}$-primary.

Lemma 5.1.4. *([2] Lemma 3.1) Let $\mathfrak{q}_i \lhd A$, $1 \leqslant i \leqslant n$ be $\mathfrak{p}$-primary. Then $\mathfrak{q} = \cap_{i=1}^{n} \mathfrak{q}_i$ is $\mathfrak{p}$-primary.*

If in a primary decomposition, all the $r(\mathfrak{q}_i)$ are distinct and $\cap_{i \neq j} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$, $i = 1, \ldots, n$ then we say that the decomposition is minimal. All primary decompositions discussed here shall be minimal.

Recall that a ring A is *Noetherian* if it satisfies three equivalent conditions:

1. Every nonempty set of ideals in A has a maximal element.

2. Every ascending chain of ideals in A is stationary.

3. Every ideal in A is finitely generated.

From now on let A be Noetherian.

Definition. We say that $\mathfrak{a} \lhd A$ is irreducible if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow \mathfrak{a} = \mathfrak{b}$, or $\mathfrak{c}$.

Lemma 5.1.5. *([2] Lemma 7.11) Every ideal in A is a finite intersection of irreducible ideals.*

Definition. Let $x \in A$. Then the *annihilator* of x is $Ann(x) = \{a \in A : ax = 0\}$.

Lemma 5.1.6. *([2] Lemma 7.12) Every irreducible ideal in A is primary.*

Thus we have proved the following

Theorem 5.1.7. *([2] Theorem 7.13) In a Noetherian ring, every ideal has a primary decomposition.*

Proposition 5.1.8. *([2] Proposition 7.14) In a Noetherian ring A, every ideal contains a power of its radical.*

Let R be a commutative ring. A proper chain of prime ideals

$$0 \lhd \mathfrak{p}_1 \lhd \cdots \lhd \mathfrak{p}_n \lhd R$$

is of *length* n. The *Krull dimension* of R is the maximum length of chains of prime ideals in R. Thus a domain is of Krull dimension one, if and only if all non-zero prime ideals are maximal. From now on K shall denote a Noetherian domain of Krull dimension one.

Theorem 5.1.9. *Let K be a Noetherian domain of Krull dimension one. Let $0 \neq \mathfrak{q} \lhd K$. Then*

$$\mathfrak{q} = \mathfrak{p}_1 \dots \mathfrak{p}_t$$

where $\mathfrak{p}_i$ is a primary ideal. Furthermore, for each i, $r(\mathfrak{p}_i) = \mathfrak{m}_i$, a maximal ideal; $\mathfrak{m}_i^{n_i} \leqslant \mathfrak{p}_i$, for some n_i; and $\mathfrak{p}_i + \mathfrak{p}_j = K$, for $i \neq j$.

Proof. The radical of a primary ideal is prime, and so, as K is of Krull dimension one, is maximal. Suppose that

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

is a minimal primary decomposition. Now $r(\mathfrak{p}_i) = m_i$ is maximal and, as the decomposition is minimal, $\mathfrak{m}_i \neq \mathfrak{m}_j$ if $i \neq j$. Further $m_i^{n_i} \leqslant \mathfrak{p}_i$, as every ideal contains a power of its radical. Thus $\mathfrak{p}_i + \mathfrak{p}_j = K$ if $i \neq j$. So $\mathfrak{q}$ is an intersection of coprime ideals. Hence a product

$$\mathfrak{q} = \mathfrak{p}_i \dots \mathfrak{p}_t$$

□

Lemma 5.1.10. *Let K be a Noetherian domain of Krull dimension one. Let $\mathfrak{q}^* \leqslant \mathfrak{q}$ be ideals in K such that $0 \neq \mathfrak{q}^* \neq K$. Suppose that $\mathfrak{q}^* = \mathfrak{p}_1^* \dots \mathfrak{p}_t^*$ is a primary decomposition. Then $\mathfrak{q} = \mathfrak{p}_1 \dots \mathfrak{p}_t$ where $\mathfrak{p}_i = K$ or $r(\mathfrak{p}_i) = r(\mathfrak{p}_i^*)$ and $\mathfrak{p}_i^* \leqslant \mathfrak{p}_i$.*

Proof. If $\mathfrak{q} = K$ then the result is trivial, so suppose that $K \neq \mathfrak{q} = \mathfrak{p}_1 \dots \mathfrak{p}_s$ is a primary decomposition. We can suppose that $r(\mathfrak{p}_1) = r(\mathfrak{p}_1^*) = \mathfrak{m}_1$. Let $\mathfrak{q}_0^* = \mathfrak{p}_2^* \dots \mathfrak{p}_t^*$, $\mathfrak{q}_0 = \mathfrak{p}_2 \dots \mathfrak{p}_s$. So $\mathfrak{q}^* = \mathfrak{p}_1^* \mathfrak{q}_0^*$, and $\mathfrak{q} = \mathfrak{p}_1 \mathfrak{q}_0$. Now $\mathfrak{p}_1^* + \mathfrak{q}_0^* = K = \mathfrak{p}_1 + \mathfrak{q}_0$. Since $r(\mathfrak{p}_1^*) = r(\mathfrak{p}_1)$ we have $\mathfrak{p}_1 + \mathfrak{q}_0^* = K$. So $\mathfrak{p}_1^*(\mathfrak{p}_1 + \mathfrak{q}_0^*) = \mathfrak{p}_1^*$, so $\mathfrak{p}_1^*\mathfrak{p}_1 + \mathfrak{p}_1^*\mathfrak{q}_0^* = \mathfrak{p}_1^*$. Now $\mathfrak{p}_1^*\mathfrak{q}_0^* = \mathfrak{q}^* \leqslant \mathfrak{q} \leqslant \mathfrak{p}_1$, and $\mathfrak{p}_1^*\mathfrak{p}_1 \leqslant \mathfrak{p}_1$, so $\mathfrak{p}_1^* \leqslant \mathfrak{p}_1$. Now for those $\mathfrak{p}_i^*$ which have a radical distinct from all the $r(\mathfrak{p}_j)$ we let $\mathfrak{p}_i = K$. □

Example 5.1.1. Let D be a Dedekind domain. Then by definition ([2] chapter 9) D is a Noetherian domain of Krull dimension one. In this case every primary ideal is a prime power.

Example 5.1.2. Let $\mathcal{O}_{d,m} = \mathbb{Z} + m\omega\mathbb{Z}$ be an order in an imaginary quadratic number field. Then $\mathcal{O}_{d,m}$ is a $\mathbb{Z}$-module of finite rank and so, by Hilbert's basis theorem (see [2] Theorem 7.5) is Noetherian. Now $\mathcal{O}_{d,m}$ is of finite index in $\mathcal{O}_d$ and $\mathcal{O}_d$ is a Dedekind domain and so a Noetherian domain of Krull dimension one. Thus by theorem 20(1) on page 81 of [64], $\mathcal{O}_{d,m}$ is a Noetherian domain of Krull dimension one, it is clearly of characteristic zero. Note that maximal orders are Dedekind domains. However in non-maximal orders not every primary ideal is a power of a prime ideal.

For example consider the order $\mathcal{O}_{3,2} = \mathbb{Z} + i\sqrt{3}\mathbb{Z}$. Let $\mathfrak{m} = (2, 1 + i\sqrt{3})$. Then $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}_{3,2}$ of index 2 and $\mathfrak{m}^2 < 2\mathcal{O}_{3,2} < \mathfrak{m}$. So the ideal $2\mathcal{O}_{3,2}$ is a primary ideal which is not a power of a prime ideal.

Example 5.1.3. Let $p \in \mathbb{Z}$ be a rational prime and let $K = \mathbb{Z}/p\mathbb{Z}$. Let $R = K[X]$ and let $\mathfrak{q} \lhd R$ be of finite index. R is Noetherian by Hilbert's basis theorem. Consider the subring $S = K + \mathfrak{q}$, of R. We show that S is a Noetherian domain of Krull dimension one. By theorem 20(1) on page 81 of [64], if S is Noetherian then it is of Krull dimension one, so it suffices to show that S is Noetherian. Now R is a PID so $\mathfrak{q} = (f)$ where $\deg f = d$. Let $g = \sum a_i X^i \in R$ and consider $fg = b_0 f + \dots + b_t X^t f$, which is in the K-module generated by $fK, XfK, \dots, X^t fK$. Suppose that $t \geqslant d$, so $\deg X^t f \geqslant 2d = \deg f^2$. So, as R has a Euclidean algorithm, $X^t f = hf^2 + r$, where $\deg r < \deg f^2 = 2d$, and $\deg h \leqslant \deg X^t f - 2d < \deg X^t f$. So that fg is in the K-module generated by $fK, XfK, \dots, X^{t-1} fK$. Repeat the above until we see that fg is in the K-module generated by $fK, XfK, \dots, X^{d-1} fK$. So $S = K + \mathfrak{q}$ is generated as a K-module by $K, fK, XfK, \dots, X^{d-1} fK$ and so is Noetherian, by Hilbert's basis theorem. S is thus an example of a Noetherian domain of Krull dimension one and non-zero characteristic.

5.2 Wohlfahrt's Theorem

Wohlfahrt [91] showed that if S is a subgroup of $SL_2(\mathbb{Z})$, of level m then S is a congruence subgroup if and only if $SL_2(\mathbb{Z}, m\mathbb{Z}) \leqslant S$. That is he extended Klein's concept of the level of a congruence subgroup of the Modular group to an arbitrary subgroup of the Modular group. This concept of level and Wohlfahrt's theorem have been of great use in the construction of non-congruence subgroups of the Modular group. We have seen how the concept of level can be extended to $SL_n(R)$ where R is any ring with a one. In this section we extend Wohlfahrt's theorem to all Noetherian domains of Krull dimension one.

Definition. R is said to be an *SR_2-ring* if $a, b \in R$ such that $\gcd(a,b) = 1 \Rightarrow \exists t \in R$ such that $a + tb \in R^*$.

Lemma 5.2.1. *Let A be any commutative ring with a one. Let $a, b \in A$ such that $\gcd(a,b) = 1$. Let $\mathfrak{q} \lhd A$ such that $\overline{A} = A/\mathfrak{q}$ is an SR_2-ring. Then $\exists t \in A$ such that $(a + bt)A + \mathfrak{q} = A$.*

Proof. As a, b are coprime $\exists s, t \in A$ such that $as + bt = 1$. Now $\overline{1} = \varphi(1) = \varphi(as + bt) = \overline{as} + \overline{bt}$, where $\varphi : A \to \overline{A}$ is the natural homomorphism. So $\overline{a}, \overline{b}$ are coprime. So, as $\overline{A}$ is an SR_2-ring $\exists \overline{t} \in \overline{A}$ such that $(\overline{a} + \overline{bt}) = \overline{u}$, where $\overline{u} \in \overline{A}^*$, so $(a + bt) \equiv u \pmod{\mathfrak{q}}$, so $u = (a + bt) - q$, some $q \in \mathfrak{q}$. Hence $(a + bt)A + \mathfrak{q} = A$. □

Theorem 5.2.2. *Let A be any commutative ring. Let $\mathfrak{q}_i \lhd A$, $i = 1, 2$. Suppose that $\overline{A} = A/\mathfrak{q}_1$ is an SR_2-ring. Then*

$$SL_2(A, \mathfrak{q}_2) \leqslant E_2(A, \mathfrak{q}_2) SL_2(A, \mathfrak{q}_1)$$

Proof. Denote $SL_2(A, \mathfrak{q}_i)$ by $\Gamma(\mathfrak{q}_i)$ and $E_2(A, \mathfrak{q}_i)$ by $\Delta(\mathfrak{q}_i)$. Let

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(\mathfrak{q}_2).$$

Now $ad - bc = 1$ so a, b are coprime, and $\overline{A}$ is an SR_2-ring, so by the lemma (5.2.1) $\exists t \in A$ such that $(a + bt)A$ is prime to $\mathfrak{q}_1$. Let

$$T = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \in \Delta(A)$$

so

$$T^{-1}XT = \begin{pmatrix} a+bt & * \\ * & * \end{pmatrix} \in \Gamma(\mathfrak{q}_2)$$

so wlog aA and $\mathfrak{q}_1$ are coprime. Let $x \in A$ such that $ax \equiv 1 \pmod{\mathfrak{q}_1}$. Now let

$$T_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, X_1 = \begin{pmatrix} 1 & x(1-a-b) \\ 0 & 1 \end{pmatrix},$$

$$X_2 = \begin{pmatrix} 1 & a-1 \\ 0 & 1 \end{pmatrix}.$$

$a \equiv 1 \pmod{\mathfrak{q}_2}$, so $X_2 \in \Delta(\mathfrak{q}_2)$, and $1-a, b \in \mathfrak{q}_2$ so $X_1 \in \Delta(\mathfrak{q}_2)$. Now

$$T_1^{-1}XX_1T_1X_2 \equiv \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \pmod{\mathfrak{q}_1}$$

where $q \in \mathfrak{q}_2$. So $T_1^{-1}XX_1T_1X_2 \in \Delta(\mathfrak{q}_2)\Gamma(\mathfrak{q}_1)$. Hence $X \in \Delta(\mathfrak{q}_2)\Gamma(\mathfrak{q}_1)$, as $X_1, X_2 \in \Delta(\mathfrak{q}_2)$, and $T_1 \in \Delta(A)$, and $\Delta(\mathfrak{q}_2) \lhd \Delta(A)$. □

The following corollary is the classical form of Wohlfahrt's theorem and is equivalent to the theorem.

Corollary 5.2.3. *Let $G \leqslant SL_2(A)$ have level $\mathfrak{q}$. Then G is a congruence subgroup if and only if $SL_2(A, \mathfrak{q}) \leqslant G$.*

Corollary 5.2.4. *Let A be an SR_2-ring. Let $\mathfrak{q} \lhd A$. Then $SL_2(A, \mathfrak{q}) = E_2(A, \mathfrak{q})$. So in particular $SL_2(A) = E_2(A)$.*

Proof. Take $\mathfrak{q}_1 = 0$ in the theorem. □

Corollary 5.2.5. *Let A be any commutative ring. Let $\mathfrak{q}_i \lhd A$, $i = 1, 2$. Suppose that $\overline{A} = A/\mathfrak{q}_2$ is an SR_2-ring. Then*

$$SL_2(A, \mathfrak{q}_1 + \mathfrak{q}_2) = E_2(A, \mathfrak{q}_1)SL_2(A, \mathfrak{q}_2)$$

Proof. Obviously $\Gamma(\mathfrak{q}_1)\Gamma(\mathfrak{q}_2) \leqslant \Gamma(\mathfrak{q}_1 + \mathfrak{q}_2)$. Then

$$\begin{aligned} \Gamma(\mathfrak{q}_1 + \mathfrak{q}_2) &\leqslant \Delta(\mathfrak{q}_1 + \mathfrak{q}_2)\Gamma(\mathfrak{q}_2) && \text{by theorem (5.2.2)} \\ &= \Delta(\mathfrak{q}_1)\Delta(\mathfrak{q}_2)\Gamma(\mathfrak{q}_2) \\ &\leqslant \Delta(\mathfrak{q}_1)\Gamma(\mathfrak{q}_2) \end{aligned}$$

□

Lemma 5.2.6. *[3] Semilocal rings are SR_2 rings.*

Proof. Let R be a semilocal ring,and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ be the maximal ideals of R. Let $a, b \in R$ such that $gcd(a, b) = 1$. RTP $\exists t \in R$ such that $a + tb \in R^*$.

$\forall i = 1, \ldots, t$ suppose

$$\forall s \in R, \quad a + bs \equiv 0 \pmod{\mathfrak{m}_i}$$

Then, taking $s = 0$, we get $a \in \mathfrak{m}_i$, and, taking $s = 1$, we get $b \in \mathfrak{m}_i$. But a, b are coprime. Contradiction. So $\forall i \, \exists t_i$ such that $a + t_i b \not\equiv 0 \pmod{\mathfrak{m}_i}$. Then, by the Chinese Remainder Theorem, $\exists t \in R$ such that $t \equiv t_i \pmod{\mathfrak{m}_i} \, \forall i$. So

$$a + tb \equiv a + t_i b \not\equiv 0 \pmod{\mathfrak{m}_i} \, \forall i$$

So $a + tb \in R^*$, as required. □

Lemma 5.2.7. *Let K be a Noetherian domain of Krull dimension one. Let $0 \neq \mathfrak{q} \lhd K$. Then $K/\mathfrak{q}$ is semilocal and therefore an SR_2-ring.*

Proof. As K is Noetherian we have a primary decomposition $\mathfrak{q} = \cap_{i=1}^{t} \mathfrak{p}_i$. As K has dimension one this is a product $\mathfrak{p}_i \ldots \mathfrak{p}_t$ and $r(\mathfrak{p}_i)$ is maximal. Let $\mathfrak{m}_i = r(\mathfrak{p}_i)$. So $\forall i \, \exists n_i \in \mathbb{N}$ such that $\mathfrak{m}_i^{n_i} \leqslant \mathfrak{p}_i$. So $\mathfrak{m}_1^{n_1} \ldots \mathfrak{m}_t^{n_t} \leqslant \mathfrak{q}$. Now suppose that $\hat{\mathfrak{m}} \lhd K/\mathfrak{q}$ is a maximal ideal. So $\hat{\mathfrak{m}} = \mathfrak{m}/\mathfrak{q}$, some maximal ideal $\mathfrak{m} \geqslant \mathfrak{q}$. Suppose that $\mathfrak{m} \neq \mathfrak{m}_i \, \forall i$. Then $\mathfrak{m} + \mathfrak{m}_1^{n_1} \ldots \mathfrak{m}_t^{n_t} = K$, but $\mathfrak{m}_1^{n_1} \ldots \mathfrak{m}_t^{n_t} \leqslant \mathfrak{q}$, so $\mathfrak{m} + \mathfrak{q} = K$. Contradiction. Hence $K/\mathfrak{q}$ has only finitely many maximal ideals and so is semilocal and therefore SR_2. □

Thus

Theorem 5.2.8. *Let K be a Noetherian domain of Krull dimension one. Let $\mathfrak{q}_i \lhd K$, $i = 1, 2$, $\mathfrak{q}_1 \neq 0$. Then*

$$SL_2(K, \mathfrak{q}_1 + \mathfrak{q}_2) = E_2(K, \mathfrak{q}_2) SL_2(K, \mathfrak{q}_1)$$

$$SL_2(K, \mathfrak{q}_1 + \mathfrak{q}_2) = SL_2(K, \mathfrak{q}_1) SL_2(K, \mathfrak{q}_2)$$

Let $\mathcal{O}$ be an order of an imaginary quadratic number field. So $\mathcal{O}$ is a Noetherian domain of Krull dimension one, so we have a Wohlfahrt theorem in these rings. We remark that maximal orders are Dedekind domains and in this case the result has already been proved [63].

5.3 Preliminary results about $SL_2(L)$

Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Let $N \lhd SL_2(L)$. Let $o(N) = \mathfrak{q}$, and $l(N) = \mathfrak{q}^*$. We are interested in how $\mathfrak{q}$ and $\mathfrak{q}^*$ are related. It will turn out that whether 2 is a unit or not is of critical importance. The case $2 \in L^*$ is easier to handle than $2 \notin L^*$. When $2 \notin L^*$ we have two cases, $o(N) = L$ and $o(N) \neq L$ both of which split into two subcases, $|L : \mathfrak{m}| > 2$ and $|L : \mathfrak{m}| = 2$, with the latter case being the most difficult. Here we present a complete account; the results up to lemma (5.3.15) are known.

Lemma 5.3.1. *[3] Let L be a commutative local ring and let $\mathfrak{q} \lhd L$. Then*

$$SL_2(L, \mathfrak{q}) = E_2(L, \mathfrak{q})$$

and so, in particular

$$SL_2(L) = E_2(L)$$

Proof. This follows from (5.2.4) and (5.2.6) □

Lemma 5.3.2. *Let $N \lhd SL_2(L)$. Then $o(N)$ is generated by*

$$\left\{ c \in L : \begin{pmatrix} * & * \\ c & * \end{pmatrix} \in N \right\}$$

Proof. $o(N)$ is generated by $b, c, a - d$ for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N.$$

The result follows as

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in N$$

and

$$VT^{-1}XTV^{-1} = \begin{pmatrix} d & -c \\ d - a + c - b & a - c \end{pmatrix} \in N$$

where

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, V = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

□

Corollary 5.3.3. *Let L be any local ring. Let $N \lhd SL_2(L)$ such that $o(N) = L$. Then* $\exists X = \begin{pmatrix} * & * \\ c & * \end{pmatrix} \in N$, *such that c is a unit.*

We make use of the following notation.

$$E_{12}(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, E_{21}(y) = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$$

The following lemma is a slight generalization of lemme 3.3 part (ii) of [44].

Lemma 5.3.4. *Let A be a commutative ring. Let $t \in A$, and $u \in A^*$, and let*

$$Y = \begin{pmatrix} u & t \\ 0 & u^{-1} \end{pmatrix} \in N \lhd SL_2(A).$$

Then $E_{12}((u - u^{-1})\alpha) \in N \ \forall \alpha \in A$.

Proof.

$$\begin{pmatrix} 1 & (u-u^{-1})\alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -u^{-1}\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & t \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} 1 & u^{-1}\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & -t \\ 0 & u \end{pmatrix} \in N$$

□

Lemma 5.3.5. *([54] lemma 1.1) Let A be a commutative ring. Let $N \lhd SL_2(A)$ and suppose that*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N.$$

Then $\forall u \in A^*$ such that $u^2 \equiv 1 (\mod c)$, $u^4 - 1 \in l(N)$.

Proof. Let

$$M_2 = \begin{pmatrix} u & t \\ 0 & u^{-1} \end{pmatrix}$$

where $u \in A^*$ such that $u^2 \equiv 1 (\mod c)$, and $t \in A$. Then

$$[M_2, M] = M_2^{-1} M^{-1} M_2 M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where

$$\alpha = (u^{-1}d + ct)(ua + tc) - u^{-1}c(bu^{-1} + at),$$

$$\gamma = ac - u^2ac - utc^2,$$

$$\delta = ad - u^2bc - utcd.$$

Now if $a - u^2a - utc = 0$ then $\gamma = 0$ and $a - u^2a - utc = 0 \Leftrightarrow a(1 - u^2) = utc$. Since $u^2 \equiv 1(\mod c)$, $u^2 - 1 = kc$, some $k \in A$. So let $t = u^{-1}ak$, so $\gamma = 0$. Now $tc = u^{-1}a(1 - u^2)$, substituting this into the expressions for α and δ and simplifying we see that $\alpha - \delta = u^4 - 1$ and so by (5.3.4) we get $u^4 - 1 \in l(N)$. □

Lemma 5.3.6. *Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Let $N \lhd SL_2(L)$, $o(N) = \mathfrak{q} \leqslant \mathfrak{m}$. Then $8\mathfrak{q} \leqslant l(N)$.*

Proof. Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N$$

by (5.3.2) it is enough to show that $8c \in l(N)$. Let $u_1 = 1 + c$, $u_2 = 1 - c$. As $o(N) \neq L$, $u_i \in L^*$, and $u_i^2 \equiv 1(\mod c)$, so by (5.3.5) $u_i^4 - 1 \in l(N)$, so $(u_1^4 - 1) - (u_2^4 - 1) = 8c(c^2 + 1) \in l(N)$, and $1 + c^2 \in L^*$ so $8c \in l(N)$. □

Lemma 5.3.7. *Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Let $N \lhd SL_2(L)$. Suppose that $2 \in L^*$ and $o(N) \neq L$. Then $o(N) = l(N)$.*

Proof. As $2 \in L^*$, $8 \in L^*$ and so this follows from (5.3.6). □

Lemma 5.3.8. *Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Suppose that $2 = 0$. Let $N \lhd SL_2(L)$ and suppose that $o(N) = \mathfrak{q} \leqslant \mathfrak{m}$. Then*

$$\mathfrak{q}^{(4)} =< \alpha^4 : \alpha \in \mathfrak{q} > \leqslant l(N)$$

Proof. Consider

$$\begin{pmatrix} * & * \\ c & * \end{pmatrix} \in N$$

as $o(N) \neq L$, $c \in \mathfrak{m}$. Let $u_1 = 1 + xc$, $u_2 = 1 + yc$, some $x, y \in L$. Now, as $2 = 0$, $c^4(x^4 - y^4) = u_1^4 - u_2^4 \in l(N)$, by (5.3.5). Pick $x, y \in L$ such that $x = y + 1$, so $x^4 - y^4 = 1$. Hence result. □

When $|L : \mathfrak{m}| > 2$ we can improve the above results. First we need Whitehead's lemma

Lemma 5.3.9. *Let R be any commutative ring with a one. Let $u \in R^*$. Then*

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \in E_2(R).$$

Proof. Let $u \in R^*$. Then

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -u^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & u \\ -u^{-1} & 0 \end{pmatrix} \in E_2(R).$$

Now $u^2, -u \in R^*$, so

$$\begin{pmatrix} 0 & u^2 \\ -u^2 & 0 \end{pmatrix} \begin{pmatrix} 0 & -u \\ u^{-1} & 0 \end{pmatrix} = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \in E_2(R)$$

□

Lemma 5.3.10. *([43] Proposition* 1.3.6 *) Let A be any commutative ring. Let $\mathfrak{q} \lhd A$. Let $\Gamma = SL_2(A)$, $\Delta = E_2(A)$, $\Delta(\mathfrak{q}) = E_2(A, \mathfrak{q})$, $\Gamma(\mathfrak{q}) = SL_2(A, \mathfrak{q})$, $H(\mathfrak{q}) = H_2(A, \mathfrak{q})$. Then*

$$[\Gamma, H(\mathfrak{q})] \leqslant \Gamma(\mathfrak{q})$$

$$[\Delta, \Delta(\mathfrak{q})] \leqslant \Delta(\mathfrak{q})$$

and if $\exists u \in A^*$ such that $u^2 - 1 \in A^*$ then

$$[\Delta, \Delta(\mathfrak{q})] = \Delta(\mathfrak{q})$$

Proof. Let $M_1 \in \Gamma$, $M_2 \in H(\mathfrak{q})$. So $[M_1, M_2] = M_1 M_2 M_1^{-1} M_2^{-1} \equiv M_1 k I M_1^{-1} k^{-1} I \equiv I$ mod $\mathfrak{q}$. So $[\Gamma, H(\mathfrak{q})] \in \Gamma(\mathfrak{q})$. Now, as $\Delta, \Delta(\mathfrak{q})$ are both normal in Δ, $[\Delta, \Delta(\mathfrak{q})] \leqslant \Delta \cap \Delta(\mathfrak{q}) = \Delta(\mathfrak{q})$.

Now let $t \in A$ and suppose that $u \in A^*$ such that $u^2 - 1 \in A^*$ and consider

$$\left[\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (u^2-1)t \\ 0 & 1 \end{pmatrix}$$

By Whitehead's lemma (5.3.9)

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \in \Delta$$

Now let $\alpha \in \mathfrak{q}$ and let $t = (u^2-1)^{-1}\alpha \in \mathfrak{q}$, so that

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (u^2-1)t \\ 0 & 1 \end{pmatrix} \in [\Delta, \Delta(\mathfrak{q})]$$

□

Lemma 5.3.11. *([54] lemma 1.2) Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Suppose that $|L : \mathfrak{m}| > 2$ and $2 \notin L^*$. Let $N \lhd SL_2(L)$ have order $\mathfrak{q} \leqslant \mathfrak{m}$. Let*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N.$$

Then $2c^2, c^4 \in l(N) \Rightarrow 2c, c^2 \in l(N)$.

Proof. Now

$$M_2 = MT^{-1}M^{-1}T = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in N$$

where $e = 1 + ac$ and $g = c^2$. Note that $2g$, and $g^2 \in l(N) = \mathfrak{q}$. Now let

$$M_3 = M_2T(-t)M_2^{-1}T(t) = \begin{pmatrix} 1 + get & t(1 - e^2 + get) \\ g^2t & 1 - get + g^2t^2 \end{pmatrix}$$

where $t \in L$. Let $r = 1 + get$ and $s = t(1 - e^2) + get^2$. So

$$D(r,r)T(r^{-1}s) = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & r^{-1}s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix}$$

and $g^2, 2g \in \mathfrak{q}$ so

$$M_3 \equiv D(r,r)T(r^{-1}s)(\mod \mathfrak{q})$$

Let $q = 1 - r^2 \in \mathfrak{q}$ and let

$$M_4 = \begin{pmatrix} r(1+q) & q \\ -q & r \end{pmatrix}$$

then $\det M_4 = r^2(1+q) + q^2 = r^2(2-r^2) + (1-r^2)^2 = 1$, so $M_4 \in SL_2(L)$. Clearly $M_4 \in H(\mathfrak{q})$. Now

$$M_4M_3 \equiv \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} = \begin{pmatrix} r^2 & rs \\ 0 & r^2 \end{pmatrix} (\mod \mathfrak{q})$$

and $q = 1-r^2 \in \mathfrak{q}$, so $r^2 \equiv 1(\mod \mathfrak{q})$. Now $rs = s+tegs = s+t^2eg(1-e^2)+t^3e^2g^2$, and $g^2 \in \mathfrak{q}$, so $t^3e^2g^2 \in \mathfrak{q}$. Also $1-e^2 = -(2ac+a^2g)$, so $t^2eg(1-e^2) = -t^2e(2gac+a^2g^2)$, and $2g, g^2 \in \mathfrak{q}$, so $rs \equiv s(\mod \mathfrak{q})$. Hence $SR \equiv T(s)(\mod \mathfrak{q})$. So $T(s) = T(t(1-e^2))T(t^2eg) \in NH(\mathfrak{q})$. Now

$$\begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} = \begin{pmatrix} e & u^{-2}f \\ u^2g & h \end{pmatrix} \in N$$

and repeat the above argument with this matrix to get $T(t(1-e^2))T(t^2eu^2g) \in NH(\mathfrak{q})$, $\forall u \in L^*$ $\forall t \in L$.

Now, as $|L : \mathfrak{m}| > 2$ we can find $v \in L^*$ such that $v-1 \in L^*$. Now consider the above with $u = v, v-1$. So

$$T(t(1-e^2))T(t^2ev^2g) \in NH(\mathfrak{q})$$

and

$$T(t(1-e^2))T(t^2eg)T(t^2egv^2)T(-t^2e2gv) \in NH(\mathfrak{q})$$

Now $2g \in \mathfrak{q}$, so $T(-2t^2e2gv) \in NH(\mathfrak{q})$ and so it follows from the above that

$$T(t(1-e^2)) \in NH(\mathfrak{q})$$

$\forall t \in L$. Hence $e^2-1 \in l(NH(\mathfrak{q}))$. Now $e^2-1 = (1+ac)^2-1 = a(2c+ac^2)$, and $ad-bc = 1$, $c \in \mathfrak{m}$, so $a, d \in L^*$, so $2c+ac^2 \in l(NH(\mathfrak{q}))$. Now, again using the fact that $|L : \mathfrak{m}| > 2$, let $w \in L^*$ such that $w^2-1 \in L^*$, so

$$\begin{pmatrix} w^{-1} & 0 \\ 0 & w \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} = \begin{pmatrix} a & w^{-2}b \\ w^2c & d \end{pmatrix}$$

Repeating the above argument we see that $2w^2c+aw^4c^2 = w^2(2c+aw^2c^2) \in l(NH(\mathfrak{q}))$. So, as $w^2 \in L^*$, $2c+aw^2c^2 \in l(NH(\mathfrak{q}))$. So $2c+aw^2c^2-(2c+ac^2) = ac^2(w^2-1) \in l(NH(\mathfrak{q}))$, and $a, w^2-1 \in L^*$, so $c^2 \in l(NH(\mathfrak{q}))$, and $2c \in l(NH(\mathfrak{q}))$.

So $\Gamma(2c+c^2) \leqslant NH(\mathfrak{q})$. Let $\mathfrak{q}_0 = (2c)+(c^2)$. Now

$$\begin{aligned}
\Gamma(\mathfrak{q}_0) &= [\Gamma, \Gamma(\mathfrak{q}_0)] && \text{by (5.3.10) and (5.3.1)}\\
&\leqslant [\Gamma, NH(\mathfrak{q})] && \text{as } \Gamma(\mathfrak{q}_0) \leqslant NH(\mathfrak{q}_0)\\
&\leqslant [\Gamma, N]\,[\Gamma, H(\mathfrak{q})] &&\\
&\leqslant N\Gamma(\mathfrak{q}) && \text{by (5.3.10)}\\
&\leqslant N && \text{as } \Gamma(\mathfrak{q}) \leqslant N
\end{aligned}$$

□

Lemma 5.3.12. *([54] theorem* 1.3 *) Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Suppose that $|L:\mathfrak{m}| > 2$, $2 \notin L^*$, and $2 \neq 0$. Let $N \lhd SL_2(L)$, $o(N) = \mathfrak{q} \leqslant \mathfrak{m}$. Then $2\mathfrak{q} \leqslant l(N)$.*

Proof. We show that $2c^4, c^8 \in l(N)$ and apply (5.3.11). Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N$$

so $c \in \mathfrak{m}$. Let $x, y \in L$ and consider $1+xc, 1+yc \in L^*$, so by (5.3.5),

$$\begin{aligned}
(1+xc)^4-(1+yc)^4 &= 4c(x-y)+6c^2(x^2-y^2)+4c^3(x^3-y^3)+c^4(x^4-y^4)\\
&= (x-y)c\,(2+(x+y)c)\,\big(2+2(x+y)c+(x^2+y^2)c\big) \in l(N)
\end{aligned}$$

Now, using the fact that $|L:\mathfrak{m}| > 2$ choose $x=u$, $y=v$ such that $u, v \in L^*$, $u+v=1$, so $u-v = 1-2v \in L^*$, as $2 \notin L^*$. So

$$c(2+c)(2+2c+(1-2uv)c^2) \in l(N)$$

Choosing $x=1, y=0$, we see that

$$c(2+c)(2+2c+c^2) \in l(N)$$

so that

$$2c^3(2+c) \in l(N)$$

Now, again using the fact that $|L:\mathfrak{m}| > 2$ choose $u \in L^*$ such that $u^2-1 \in L^*$. Conjugating X by $D(u,u^{-1})$ and repeating the above argument shows that

$$2c^3(2+u^2c) \in l(N)$$

so, since $u^2 - 1 \in l(N)$, we see that

$$2c^4 \in l(N)$$

Now, with $x = 1, y = 0$, we see that

$$c^4 + 4c^3 + 6c^2 + 4c \in l(N)$$

so, multiplying by c^4 we get

$$c^8 + 4c^7 + 6c^6 + 4c^5 = c^8 + 2c^4(2c^3 + 3c^2 + 2c) \in l(N)$$

so

$$c^8 \in l(N)$$

Hence result. □

Lemma 5.3.13. *([54] theorem* 1.3 *) Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Suppose that $|L : \mathfrak{m}| > 2$, and $2 = 0$. Let $N \lhd SL_2(L)$ and suppose that $o(N) = \mathfrak{q} \leqslant \mathfrak{m}$. Then $\mathfrak{q}^{(2)} \leqslant l(N)$.*

Proof. By (5.3.8) $2c^4, c^4 \in l(N)$. Hence by (5.3.11), $2c, c^2 \in l(N)$. Clearly $2c = 0$. Hence result. □

Lemma 5.3.14. *Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Let $N \lhd SL_2(L)$. Suppose that $o(N) = L$ and $|L : \mathfrak{m}| > 3$. Then $l(N) = L$.*

Proof. Let

$$\begin{pmatrix} * & * \\ c & * \end{pmatrix} \in N$$

such that $c \in L^*$. Now let $u \in L^*$, so $u^2 - 1 = cc^{-1}(u^2 - 1)$, so $u^2 \equiv 1(\mod c)$. So by (5.3.5) $u^4 - 1 \in l(N)$. Now if $\forall u \in L^*$ $u^4 - 1 \in \mathfrak{m}$, $|L : \mathfrak{m}| \leqslant 5$. So if $|L : \mathfrak{m}| > 5$ then we are done.

Suppose that $|L : \mathfrak{m}| = 5$. Let $\alpha \in \mathfrak{m}$, and let $u_1 = 1 + \alpha$, $u_2 = 1 - \alpha$, so $u_i \in L^*$ and $u_i^2 \equiv 1 \pmod{c}$, so, by (5.3.5), $8\alpha(1 + \alpha^2) = u_1^4 - u_2^4 \in l(N)$. Now $|L : \mathfrak{m}| = 5$ so $2 \in L^*$, so $8 \in L^*$, and $1 + \alpha^2 \in L^*$, so $\alpha \in l(N)$, hence $\mathfrak{m} \leqslant l(N)$. Now let $M \lhd SL_2(\mathbb{F}_5)$ be the image of N under the natural map $SL_2(L) \twoheadrightarrow SL_2(\mathbb{F}_5)$, so $o(M) = \mathbb{F}_5$, $M \neq \{\pm I\}$, and as $PSL_2(\mathbb{F}_5)$ is simple, $M\{\pm I\} = SL_2(\mathbb{F}_5)$. So M is of index 1 or 2 in $SL_2(\mathbb{F}_5)$ but $SL_2(\mathbb{F}_5)' = SL_2(\mathbb{F}_5)$ [72], so $M = SL_2(\mathbb{F}_5)$. So $N = SL_2(L)$ and $l(N) = L$. Now suppose that $|L : \mathfrak{m}| = 4$. Let $u \in L^* - \{1\}$. Then $u^4 - 1 = u - 1 \notin \mathfrak{m}$, so $l(N) = L$. □

Lemma 5.3.15. *Let L be a commutative local ring with maximal ideal $\mathfrak{m}$. Let $N \lhd SL_2(L)$. Suppose that $o(N) = L$ and $|L : \mathfrak{m}| = 3$. Then $\mathfrak{m} \leqslant l(N)$.*

Proof. As $o(N) = L$, by (5.3.3),

$$\exists \begin{pmatrix} * & * \\ c & * \end{pmatrix} \in N$$

such that $c \in L^*$. Let$\alpha \in \mathfrak{m}$ and let $u_1 = 1 + \alpha$, $u_2 = 1 - \alpha$, so $u_i \in L^*$ and $u_i^2 \equiv 1($ mod $c)$. So $8\alpha(1 + \alpha^2) = u_1^4 - u_2^4 \in l(N)$ by (5.3.5). As $|L : \mathfrak{m}| = 3$, 2 is a unit and, as $\alpha \in \mathfrak{m}$, $1 + \alpha^2$ is also a unit. So $\alpha \in l(N)$. Hence $\mathfrak{m} \leqslant l(N)$. □

Lemma 5.3.16. *Let L be a commutative local ring with nilpotent maximal ideal $\mathfrak{m}$ of index 2. Then $|SL_2(L)| = 2^\alpha 3$.*

Proof. Let $n \in \mathbb{N}$ be minimal such that $\mathfrak{m}^n = 0$. Let $\Gamma = SL_2(L)$, and $\Gamma(i) = SL_2(L, \mathfrak{m}^i)$. Then

$$|\Gamma| = |\Gamma : \Gamma(1)||\Gamma(1) : \Gamma(2)| \dots |\Gamma(n-2) : \Gamma(n-1)||\Gamma(n-1) : \Gamma(n)|$$

First, as $\mathfrak{m}$ of index 2, $\Gamma/\Gamma(1) \cong PSL_2(\mathbb{F}_2) \cong S_3$, so $|\Gamma : \Gamma(1)| = 6$. Now, $\Gamma(i-1)/\Gamma(i) \cong \mathbb{Z}_2^3$ by lemma (4.2.9), so $|\Gamma(i-1) : \Gamma(i)| = 8$. Hence $|\Gamma| = 2^{3(n-1)+1}3$. Hence result. □

Lemma 5.3.17. *Let L be a commutative local ring with nilpotent maximal ideal $\mathfrak{m}$ of index 2. Let $N \lhd SL_2(L)$. Then*

$$o(N) = L \Leftrightarrow |SL_2(L) : N| = 2^\alpha$$

Proof. Let Γ denote $SL_2(L)$. Suppose first that $o(N) = L$. If $\Gamma(\mathfrak{m}) \leqslant N$ then, as $\Gamma/\Gamma(\mathfrak{m}) \cong S_3$, $|\Gamma : N| = 1$, or 2. So suppose that $\Gamma(\mathfrak{m}) \nleqslant N$ and suppose that $3 \mid |\Gamma : N|$. Now $N\Gamma(\mathfrak{m}) = \Gamma$, or is of index 2 in Γ so $3 \mid |N\Gamma(\mathfrak{m}) : N|$ and $3 \mid |N\Gamma(\mathfrak{m}) : \Gamma(\mathfrak{m})|$ so $9 \mid |\Gamma : N \cap \Gamma(\mathfrak{m})|$. So $9 \mid |\Gamma|$, contradicting lemma (5.3.16). So $3 \nmid |\Gamma : N|$ ie $|\Gamma : N| = 2^\alpha$.

Now suppose that $o(N) \neq L$. So $N \leqslant H(\mathfrak{m}) = \Gamma(\mathfrak{m})$ and $|\Gamma : \Gamma(\mathfrak{m})| = 6$, so $3 \mid |\Gamma : N|$. Hence result. □

Now observe the following consequence of (5.3.17)

Corollary 5.3.18. *Let L be a commutative local ring with maximal nilpotent ideal $\mathfrak{m}$ of index 2. Let $N \lhd SL_2(L)$, $o(N) = L$ and $M \in SL_2(L)$ of order 3. Then $M \in N$.*

Lemma 5.3.19. *Let L be a commutative local ring with nilpotent maximal ideal $\mathfrak{m}$ of index 2. Let $N \lhd SL_2(L)$, $o(N) = L$. Then $T^4 \in N$, and $T^2 \in N \Leftrightarrow -I \in N$.*

Proof. AT is of order 3 so $AT \in N$, so $A \equiv T^{-1}(\mod N)$, and $A^4 = I$, so $T^4 \in N$. Also $A^2 = -I$ so $T^2 \equiv -I(\mod N)$. □

Lemma 5.3.20. *Let $a \in L$, $u \in L^*$. Then*

$$\begin{pmatrix} a & u \\ -cu^{-1} & -(1+a) \end{pmatrix}$$

is of order 3, where $c = a^2 + a + 1 \in L^*$.

Proof. Tedious calculation. □

Lemma 5.3.21. *Let L be a commutative local ring with nilpotent maximal ideal $\mathfrak{m}$, of index 2. Let $\alpha \in \mathfrak{m}$ and Let $N \lhd SL_2(L)$ be of order L. Then*

$$\begin{pmatrix} 1 & 4\alpha \\ 0 & 1 \end{pmatrix} \in N.$$

Proof. By lemma (5.3.20)

$$\begin{pmatrix} 1 & u \\ -3u^{-1} & -2 \end{pmatrix} \in N$$

for every unit u. Let $\alpha \in \mathfrak{m}$, $u = 1+\alpha$, and suppose that $u^{-1} = 1+\beta$, some $\beta \in \mathfrak{m}$. Now

$$\begin{pmatrix} 1 & u \\ -3u^{-1} & -2 \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & 3u \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & -u^{-1} \\ 0 & 1 \end{pmatrix} A^{-1}$$

$$= \begin{pmatrix} 1 & 1+\alpha \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & 1+\beta \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & 3+3\alpha \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & -1-\beta \\ 0 & 1 \end{pmatrix} A^{-1}$$

$$= T \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} AT \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} A^{-1}T^3 \begin{pmatrix} 1 & 3\alpha \\ 0 & 1 \end{pmatrix} AT^{-1} \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} A^{-1}$$

and $AT \in N$, $A^{-1}T^3 \equiv A^{-1}T^{-1} \equiv I(\mod N)$, $AT^{-1} \equiv ATT^{-2} \equiv T^{-2}(\mod N)$, so

$$T \begin{pmatrix} 1 & 4\alpha+\beta \\ 0 & 1 \end{pmatrix} T^{-2} \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} A^{-1} \in N.$$

so

$$\begin{pmatrix} 1 & 4\alpha \\ 0 & 1 \end{pmatrix} A^{-1}T^{-1} \in N$$

and $A^{-1}T^{-1} \in N$. Hence

$$\begin{pmatrix} 1 & 4\alpha \\ 0 & 1 \end{pmatrix} \in N$$

as required. □

Theorem 5.3.22. *Let L be a commutative local ring with nilpotent maximal ideal $\mathfrak{m}$ of index 2. Let $N \lhd SL_2(L)$ be of order L. Then $4L \leqslant l(N)$.*

Proof. We show $E_2(L, 4L) \leqslant N$. Recall that $E_2(L, 4L)$ is generated by conjugates of

$$E_{12}(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

where $x \in 4L$. Let $x \in 4L$, so $x = 4y$, some $y \in L$. Now $y \in L^*$ or $y \in \mathfrak{m}$. Suppose that $y \in L^*$, so $y = 1 + \alpha$, where $\alpha \in \mathfrak{m}$. So $x = 4y = 4 + 4\alpha$, so

$$E_{12}(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 4\alpha \\ 0 & 1 \end{pmatrix} \in N.$$

If $y \in \mathfrak{m}$ then similarly $e_{12}(x) \in N$. So $E_2(L, 4L) \leqslant N$, as required. □

Since we are also interested in $PSL_2(R)$, for commutative rings R we consider normal subgroups of SL_2 which contain $-I$.

Lemma 5.3.23. *Let L be a commutative local ring with nilpotent maximal ideal $\mathfrak{m}$ of index 2. Let $N \lhd SL_2(L)$ have order L and let $\alpha \in \mathfrak{m}$. Suppose that $-I \in N$. Then*

$$\begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix} \in N$$

and so $2L \leqslant l(N)$.

Proof. $-I \in N$ so by (5.3.19), $T^2 \in N$. Now, by (5.3.20), $\forall u \in L^*$,

$$\begin{pmatrix} 0 & u \\ -u^{-1} & -1 \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & 2u \\ 0 & 1 \end{pmatrix} \in N$$

Let $\alpha \in \mathfrak{m}$, let $u = 1+\alpha \in L^*$ and suppose that $u^{-1} = 1+\alpha'$, $\alpha' \in \mathfrak{m}$. So that

$$\begin{pmatrix} 1 & 1+\alpha \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & 1+\alpha' \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & 2+2\alpha \\ 0 & 1 \end{pmatrix} \in N$$

so

$$T \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} AT \begin{pmatrix} 1 & \alpha' \\ 0 & 1 \end{pmatrix} A^{-1}T^2 \begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix} \in N$$

but, as AT, $T^2 \in N$,

$$\begin{pmatrix} 1 & \alpha+\alpha' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix} \in N$$

Now, by (5.3.20), and since $-I \in N$,

$$\begin{pmatrix} 1 & u \\ -u^{-1} & 0 \end{pmatrix} = A \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in N$$

so

$$A \begin{pmatrix} 1 & 1+\alpha' \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & 1+\alpha \\ 0 & 1 \end{pmatrix} \in N$$

ie

$$AT \begin{pmatrix} 1 & \alpha' \\ 0 & 1 \end{pmatrix} A^{-1}T \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in N$$

hence, as $AT, T^2 \in N$, we have

$$\begin{pmatrix} 1 & \alpha+\alpha' \\ 0 & 1 \end{pmatrix} \in N.$$

Hence

$$\begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix} \in N.$$

Now using the fact that $T^2 \in N$ and arguing in exactly the same way as in theorem (5.3.22), we see that $E_2(L, 2L) \leqslant N$, ie $2L \leqslant l(N)$. □

Lemma 5.3.24. *Let L be a commutative local ring with maximal nilpotent ideal $\mathfrak{m}$ of index 2 and suppose that $2 = 0$ in L. Let $N \lhd SL_2(L)$ have order L. Then*

$$\mathfrak{m}^{(2)} =< \alpha^2 : \alpha \in \mathfrak{m} >\leqslant l(N)$$

Proof. By lemma (5.3.20), and since $2 = 0$,

$$\begin{pmatrix} a & u \\ -cu^{-1} & 1+a \end{pmatrix} \in N$$

and this matrix equals

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & au \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & -au^{-1} \\ 0 & 1 \end{pmatrix} A^{-1}$$

Now let $\alpha, \beta \in \mathfrak{m}$, let $u = 1+\alpha$, $a = 1+\beta$, and suppose that $u^{-1} = 1+\alpha'$, where $\alpha' \in \mathfrak{m}$. Then $au = 1+\alpha+\beta+\alpha\beta$, and $au^{-1} = 1+\alpha'+\beta+\alpha'\beta$, and so

$$\begin{pmatrix} 1 & 1+\alpha \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & 1+\alpha' \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & 1+\alpha+\beta+\alpha\beta \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & -(1+\alpha'+\beta+\alpha'\beta) \\ 0 & 1 \end{pmatrix} A^{-1}$$

lies in N, and so, as $AT \in N$, and $2 = 0$, we get

$$\begin{pmatrix} 1 & (\alpha-\alpha')\beta \\ 0 & 1 \end{pmatrix} \in N$$

Now $(1+\alpha)(1+\alpha') = 1$, so $\alpha+\alpha'+\alpha\alpha' = 0$, so, as $2 = 0$, $\alpha-\alpha' = \alpha\alpha'$, and $\alpha' = \alpha(1+\alpha')$, so $\alpha-\alpha' = \alpha^2u^{-1}$. So

$$\begin{pmatrix} 1 & \alpha^2u^{-1}\beta \\ 0 & 1 \end{pmatrix} \in N$$

Now let $x \in L$, if $x \in \mathfrak{m}$ then

$$\begin{pmatrix} 1 & \alpha^2(1+\alpha)^{-1}x \\ 0 & 1 \end{pmatrix} \in N.$$

Now if $x \notin \mathfrak{m}$ then $x = 1+\beta$, some $\beta \in \mathfrak{m}$, and

$$\begin{pmatrix} 1 & \alpha^2(1+\alpha)^{-1}x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha^2(1+\alpha)^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha^2(1+\alpha)^{-1}\beta \\ 0 & 1 \end{pmatrix}$$

Now

$$\begin{pmatrix} 1 & u \\ -u^{-1} & 0 \end{pmatrix} = A \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in N$$

by lemma (5.3.20). So using the fact that $u = 1+\alpha$, $u^{-1} = 1+\alpha'$, and $AT \in N$ we get

$$\begin{pmatrix} 1 & \alpha+\alpha' \\ 0 & 1 \end{pmatrix} \in N$$

and so, as $\alpha + \alpha' + \alpha\alpha' = 0$ we get

$$\begin{pmatrix} 1 & \alpha^2(1+\alpha)^{-1} \\ 0 & 1 \end{pmatrix} \in N$$

and so

$$\begin{pmatrix} 1 & \alpha^2(1+\alpha)^{-1}x \\ 0 & 1 \end{pmatrix} \in N.$$

Hence $\alpha^2(1+\alpha)^{-1} \in l(N)$ $\forall \alpha \in \mathfrak{m}$, and so $\alpha^2 \in l(N)$ $\forall \alpha \in \mathfrak{m}$. Hence result. □

5.4 Order and level of a normal congruence subgroup

Throughout this section K shall be a Noetherian domain of Krull dimension one, so K has primary decomposition and a Wohlfahrt theorem. Let $N \lhd SL_2(K)$, and suppose N is a congruence subgroup. Let $\mathfrak{q}^* = l(N) \neq 0$, and $\mathfrak{q} = o(N)$. We ask how $\mathfrak{q}^*$ and $\mathfrak{q}$ are related. We are particularly interested in the case where $\mathfrak{q} = K$. The following 3 lemmas can be proved using elementary group theory.

Lemma 5.4.1. *Let G be any group and let $A, B, C \lhd G$. Then $[BA, CA] \leqslant [B, C]\,A$.*

Lemma 5.4.2. *Let $A, B \lhd G$. Then $[A, B] \leqslant A \cap B$.*

Lemma 5.4.3. *Let G be a group and let $A, B, C \lhd G$ where $C \leqslant A$. Then $A \cap BC = (A \cap B)(A \cap C)$.*

The following lemma is a generalization of [58] lemma 3.3.

Lemma 5.4.4. *Let $N \lhd SL_2(K) = \Gamma$, $l(N) = \mathfrak{q}^* = \mathfrak{q}_1^*\mathfrak{q}_2^* \neq 0$, where $\mathfrak{q}_1^* + \mathfrak{q}_2^* = K$, and $\mathfrak{q}_1$ is primary. Then by* (5.1.10), *$o(N) = \mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2$, where $\mathfrak{q}_1^* \leqslant \mathfrak{q}_1$. Let $N_0 = (N \cap \Gamma(\mathfrak{q}_2^*))\Gamma(\mathfrak{q}_1^*)$, $\mathfrak{q}' = l(N_0)$, and $\overline{N} = N\Gamma(\mathfrak{q}_1^*)$. Then*

1. *$o(\overline{N}) = \mathfrak{q}_1$*

2. *$[\Gamma, \overline{N}] \leqslant N_0$*

3. *$\mathfrak{q}' = \mathfrak{q}_1^*$*

Proof. Now

$$\begin{aligned} o(\overline{N}) &= o(N\Gamma(\mathfrak{q}_1^*)) \\ &= o(N) + \mathfrak{q}_1^* \\ &= \mathfrak{q} + \mathfrak{q}_1^* \\ &= \mathfrak{q}_1\mathfrak{q}_2 + \mathfrak{q}_1^* \\ &= (\mathfrak{q}_1 \cap \mathfrak{q}_2) + (\mathfrak{q}_1 \cap \mathfrak{q}_1^*) \\ &= \mathfrak{q}_1 \cap (\mathfrak{q}_2 + \mathfrak{q}_1^*) && \text{by the modular law (see [2] p.6)} \\ &= \mathfrak{q}_1 \cap K = \mathfrak{q}_1. \end{aligned}$$

Now, as K has a Wohlfahrt theorem and $\mathfrak{q}_1^*+\mathfrak{q}_2^* = K$, we have, by (5.2.8), $\Gamma = \Gamma(\mathfrak{q}_1^*+\mathfrak{q}_2^*) = \Gamma(\mathfrak{q}_1^*)\Gamma(\mathfrak{q}_2^*)$, so

$$\begin{aligned} [\Gamma, \overline{N}] &= [\Gamma(\mathfrak{q}_1^*)\Gamma(\mathfrak{q}_2^*), N\Gamma(\mathfrak{q}_1^*)] \\ &\leqslant [\Gamma(\mathfrak{q}_2^*), N]\,\Gamma(\mathfrak{q}_1^*) && \text{by lemma (5.4.1)} \\ &\leqslant N_0 && \text{by lemma (5.4.2)} \end{aligned}$$

Now $\Gamma(\mathfrak{q}_1^*) \leqslant N_0$, so $\mathfrak{q}_1^* \leqslant l(N_0) = \mathfrak{q}'$. RTP $\mathfrak{q}' \leqslant \mathfrak{q}_1^*$. Now N_0 is a congruence subgroup of level $\mathfrak{q}'$, so by Wohlfahrt (5.2.3) $\Gamma(\mathfrak{q}') \leqslant N_0$, so

$$\begin{aligned} \Gamma(\mathfrak{q}'\mathfrak{q}_2^*) &= \Gamma(\mathfrak{q}') \cap \Gamma(\mathfrak{q}_2^*) && \text{as } \mathfrak{q}' + \mathfrak{q}_2^* = K \\ &\leqslant N_0 \cap \Gamma(\mathfrak{q}_2^*) \\ &= ((N \cap \Gamma(\mathfrak{q}_2^*))\Gamma(\mathfrak{q}_1^*)) \cap \Gamma(\mathfrak{q}_2^*) \\ &= (N \cap \Gamma(\mathfrak{q}_2^*))\Gamma(\mathfrak{q}^*) && \text{by (5.4.3)} \\ &\leqslant N\Gamma(\mathfrak{q}^*) \\ &= N \end{aligned}$$

So $\mathfrak{q}'\mathfrak{q}_2^* \leqslant l(N) = \mathfrak{q}_1^*\mathfrak{q}_2^*$. Now $\mathfrak{q}' + \mathfrak{q}_2^* = \mathfrak{q}_1^* + \mathfrak{q}_2^* = K$, so $\mathfrak{q}' \cap \mathfrak{q}_2^* = \mathfrak{q}'\mathfrak{q}_2^* \leqslant \mathfrak{q}_1^*\mathfrak{q}_2^* = \mathfrak{q}_1^* \cap \mathfrak{q}_2^*$, and $\mathfrak{q}_1^* \leqslant \mathfrak{q}'$, so $\mathfrak{q}_1^* \cap \mathfrak{q}_2^* \leqslant \mathfrak{q}' \cap \mathfrak{q}_2^*$. Hence $\mathfrak{q}' \cap \mathfrak{q}_2^* = \mathfrak{q}_1^* \cap \mathfrak{q}_2^*$. So

$$\begin{aligned} \mathfrak{q}' &= \mathfrak{q}' \cap (\mathfrak{q}_1^* + \mathfrak{q}_2^*) \\ &= (\mathfrak{q}' \cap \mathfrak{q}_2^*) + \mathfrak{q}_1^* \\ &= (\mathfrak{q}_1^* \cap \mathfrak{q}_2^*) + \mathfrak{q}_1^* \\ &= \mathfrak{q}_1^*. \end{aligned}$$

□

The following lemma is a generalization of [58] lemma 3.4.

Lemma 5.4.5. *Let $N \lhd SL_2(K)$, $l(N) = \mathfrak{q}^* = \mathfrak{q}_0^*\mathfrak{p}^* \neq 0$, where $\mathfrak{p}^*$ is primary and $\mathfrak{q}_0^* + \mathfrak{p}^* = K$, so by* (5.1.10)*, $o(N) = \mathfrak{q} = \mathfrak{q}_0\mathfrak{p}$, where $\mathfrak{p}^* \leqslant \mathfrak{p}$. Let $N_0 = (N \cap \Gamma(\mathfrak{q}_0^*))\Gamma(\mathfrak{p}^*)$, and $\overline{N} = N\Gamma(\mathfrak{p}^*)$. Let L denote the local ring $K/\mathfrak{p}^*$. Let $\varphi : SL_2(K) \to SL_2(L)$ be the natural homomorphism. Let $M_0 = \varphi(N_0)$, and $\overline{M} = \varphi(\overline{N})$. Then*

1. $M_0 \lhd SL_2(L)$
2. $l(M_0) = 0$
3. $o(\overline{M}) = \mathfrak{p}/\mathfrak{p}^*$
4. $[E_2(L), \overline{M}] \leqslant M_0$

Proof. 1 is obvious. For 4 recall that $[SL_2(K), \overline{N}] \leqslant N_0$, on applying φ we see that $[SL_2(L), \overline{M}] \leqslant M_0$. Now as L is local so an SR_2-ring we have $E_2(L) = SL_2(L)$. For 3, as $\overline{M} = \varphi(\overline{N})$, and $o(\overline{N}) = \mathfrak{p}$ we get $o(\overline{M}) = \mathfrak{p}/\mathfrak{p}^*$. Now suppose that $l(M_0) = \overline{\mathfrak{a}} \neq 0$. So $E_2(L, \overline{\mathfrak{a}}) = SL_2(L, \overline{\mathfrak{a}}) \leqslant M_0$, so $E_2(K, \mathfrak{a}) \leqslant N_0$. So, as $l(N_0) = \mathfrak{p}^*$, we have $\mathfrak{a} \leqslant \mathfrak{p}^*$, so $\mathfrak{a} = \mathfrak{p}$, so $\overline{\mathfrak{a}} = 0$. Contradiction. Hence $l(M_0) = 0$. □

Lemma 5.4.6. *([57] lemma 2.1) Let L be any local ring. Let $N \lhd SL_2(L)$ such that $o(N) = L$. Then $\exists X \in N$ of the form*

$$\begin{pmatrix} * & * \\ 1 & 1 \end{pmatrix}$$

Proof. By (5.3.3)

$$\exists M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N$$

such that c is a unit. Now

$$\begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -c^{-1}d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} * & -c^{-1} \\ c & 0 \end{pmatrix} = M_2 \in N$$

Let

$$T = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}$$

Then

$$[T, M_2] = T^{-1}M_2^{-1}TM_2 = \begin{pmatrix} 1+t^2c^2 & t \\ tc^2 & 1 \end{pmatrix} \in N$$

Choose $t = c^{-2}$ to get the result. □

Let L be a local ring, with maximal ideal $\mathfrak{m}$, and residue field $K = L/\mathfrak{m}$. The following theorem is a slight generalization of [58] theorem 2.2.

Theorem 5.4.7. *Let L be a commutative local ring. Let $N \lhd SL_2(L), M \leqslant GL_2(L)$ such that $N \leqslant M$, and $[E_2(L), M] \leqslant N$. Let $\mathfrak{q} = o(N), \mathfrak{q}^* = l(N), \mathfrak{q}_0 = o(M)$, so $\mathfrak{q}^* \leqslant \mathfrak{q} \leqslant \mathfrak{q}_0$. Then $\mathfrak{q} = \mathfrak{q}_0$, unless $K = F_2$, and $\mathfrak{q}_0 \neq L$ in which case $\mathfrak{m}\mathfrak{q}_0 \leqslant \mathfrak{q} \leqslant \mathfrak{q}_0$.*

Proof. Let

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M$$

Let $\delta = ad - bc \in L^*$. Then, as $[E_2(L), M] \leqslant N$, $[T(r), X] \in N$ and so $(d^2 - \delta)r\delta^{-1} + r^2cd\delta^{-1} \in \mathfrak{q}\ \forall r \in L$. So $\forall u \in L^*$, $(d^2-\delta)\delta^{-1} + ucd\delta^{-1} \in \mathfrak{q}$, so $(u-1)cd \in \mathfrak{q}$. Suppose that $\mathfrak{q}_0 \leqslant \mathfrak{m}$. Then $c \in \mathfrak{m}$, as $o(M) = \mathfrak{q}_0$. Now $ad - bc = \delta \in L^*$ and $c \in \mathfrak{m}$, so $bc \in \mathfrak{m}$. So if a or $d \in \mathfrak{m}$ then $\delta \in \mathfrak{m}$. Contradiction. Hence $a, d \notin \mathfrak{m}$ ie $a, d \in L^*$. So, as $(u-1)cd \in \mathfrak{q}$, $(u-1)c \in \mathfrak{q}$. When $|K| > 2$ we can choose $u \in L^*$ such that $u - 1 \equiv 1 \pmod{\mathfrak{q}}$. So $c \in \mathfrak{q}$. Hence, by (5.3.2), $\mathfrak{q}_0 = o(M) \leqslant \mathfrak{q}$. So $\mathfrak{q}_0 = \mathfrak{q}$. If $|K| = 2$ then $u = 1 + \alpha$, where $\alpha \in \mathfrak{m}$, so $u - 1 = \alpha \in \mathfrak{m}$, so $\alpha c \in \mathfrak{q}$, so, by (5.3.2), $\mathfrak{m}\mathfrak{q}_0 \leqslant \mathfrak{q}$.

Now suppose that $\mathfrak{q}_0 = L$, so $\exists X_0 \in N \subseteq M$ of the form

$$\begin{pmatrix} * & * \\ 1 & 1 \end{pmatrix}$$

So$(u-1)c = u - 1 \in \mathfrak{q}\,\forall u \in L^*$. Thus if $|K| > 2$ then $\mathfrak{q} = L = \mathfrak{q}_0$. Suppose that $|K| = 2$, let $\alpha \in \mathfrak{m}$, so $u = 1 + \alpha \in L^*$, so $\alpha = u - 1 \in \mathfrak{q}$, so $\mathfrak{m} \leqslant \mathfrak{q}$. Suppose that $\mathfrak{m} = \mathfrak{q}$ and consider the natural homomorphism $f : SL_2(L) \to SL_2(\mathbb{F}_2)$. Now $o(N) = \mathfrak{q}$ so $f(N) = 1$, and $X_0 \in M$ and $[SL_2(L), M] \leqslant N$, so $f(X_0)$ is central. But $SL_2(\mathbb{F}_2)$ has trivial centre, so $f(X_0) = I$. But $X_0 = \begin{pmatrix} * & * \\ 1 & 1 \end{pmatrix}$. So, under the map $L \to \mathbb{F}_2$, $1 \mapsto 0$. Contradiction. Hence $\mathfrak{q} = L$. □

We are now in a position to address the main problem of this chapter; to derive a relationship between the order and level of a normal congruence subgroups of SL_2 over a Noetherian domain of Krull dimension one. We deal first with the case of a normal subgroup of order K. This is for two reasons, first we are able to obtain a better bound in this case, in fact our bound is best possible, and second, when we apply these results to the construction of non-congruence subgroups of the Bianchi groups we do so by showing a large class of normal subgroups has order $\mathcal{O}_{d,m}$.

Theorem 5.4.8. *Let K be a Noetherian domain of Krull dimension one and suppose that char$K \neq 2$, or 3. Let $N \lhd SL_2(K)$ be a congruence subgroup. Suppose that $o(N) = K$ and that $l(N) = \mathfrak{q}^*$. Then $12K \leqslant \mathfrak{q}^*$.*

Proof. Let $\mathfrak{q}^* = \mathfrak{p}_1^* \dots \mathfrak{p}_t^*$ be a primary decomposition. Fix $i \in \{1, \dots, t\}$ and consider p_i^*. Let $\mathfrak{q}_0^* = \cap_{j \neq i} \mathfrak{p}_j^*$, $\mathfrak{p}^* = \mathfrak{p}_i^*$, and so we can apply (5.4.5) let $\mathfrak{q}_0 = \mathfrak{p} = K$. Let $L_i = K/\mathfrak{p}_i^*$ and denote the maximal ideal of L_i by $\mathfrak{m}_i$. By an abuse of notation we also use $\mathfrak{m}_i$ to denote the corresponding maximal ideal of K, ie $r(\mathfrak{p}_i^*) = \mathfrak{m}_i$. Let $\varphi_i : SL_2(K) \to SL_2(L_i)$ be the natural homomorphism. Let $N_0 = (N \cap \Gamma(\mathfrak{q}_0^*))\Gamma(\mathfrak{p}^*)$, $\overline{N} = N\Gamma(\mathfrak{p}^*)$. Let $M_0 = \varphi_i(N_0)$, $\overline{M} = \varphi_i(\overline{N})$. Then by lemma (5.4.5) $l(M_0) = 0$, $o(\overline{M}) = \mathfrak{p}/\mathfrak{p}^* = L_i$, and $[E_2(L_i), \overline{M}] \leqslant M_0$. Now by theorem (5.4.7), as $o(N) = K$ then $o(M_0) = o(\overline{M}) = L_i$.

Suppose that $2 \in L_i^*$. Then, by (5.3.14) $o(M_0) = l(M_0)$ unless $|L_i : \mathfrak{m}_i| = 3$, in which case, by (5.3.15), $\mathfrak{m}_i \leqslant l(M_0)$. If $o(M_0) = l(M_0)$ then $L_i = 0$ and so $\mathfrak{p}_i^* = K$. If $|L_i : \mathfrak{m}_i| = 3$ and $\mathfrak{m}_i \leqslant l(M_0)$ then L_i is the field of 3 elements and $3K \leqslant \mathfrak{p}_i^*$.

Now suppose that $2 \notin L_i^*$. If $|L_i : \mathfrak{m}_i| > 3$ then, by (5.3.14), $l(M_0) = o(M_0)$ and so $\mathfrak{p}_i^* = K$. If $|L_i : \mathfrak{m}_i| = 3$ then, by (5.3.15), $\mathfrak{m}_i \leqslant l(M_0)$ and so L_i is the field of 3 elements and $3K \leqslant \mathfrak{p}_i^*$. If $|L_i : \mathfrak{m}_i| = 2$ and $2 \neq 0$ in L_i then, by (5.3.22), $4o(M_0) \leqslant l(M_0)$ and so $4K \leqslant \mathfrak{p}_i^*$. If $|L_i : \mathfrak{m}_i| = 2$ and $2 = 0$ in L_i then $2 \in \mathfrak{p}_i^*$ so $2K \leqslant \mathfrak{p}_i^*$. So, in all cases $12K \leqslant \mathfrak{p}_i^*$. Now $\mathfrak{q}^* = \mathfrak{p}_1^* \dots \mathfrak{p}_t^* = \bigcap_{i=1}^t \mathfrak{p}_i^* \geqslant 12K$. Hence result. □

Note from the proof above that the $12K$ comes from ideals of index 2 and ideals of index 3. When one or both of these are not present we get a better bound.

Corollary 5.4.9. *Let K be a Noetherian domain of Krull dimension one. Let $N \lhd SL_2(K)$ be a congruence subgroup. Suppose that $o(N) = K$ and $l(N) = \mathfrak{q}^*$. Then*

1. *If K has no ideals of index 2, then $3K \leqslant \mathfrak{q}^*$.*

2. *If K has no ideals of index* 3 *then* $4K \leqslant \mathfrak{q}^*$.

3. *If K has no ideals of index* 2 *or* 3 *then* $\mathfrak{q}^* = K$.

Corollary 5.4.10. *Let K be a Noetherian domain of Krull dimension one and suppose that $charK = 0$. Let $N \lhd SL_2(K)$ be a congruence subgroup which contains $-I$. Suppose that $o(N) = K$, and $l(N) = \mathfrak{q}^*$. Then $6K \leqslant \mathfrak{q}^*$.*

Proof. This follows from (5.4.8) and (5.3.23). □

Lemma 5.4.11. *Let K be a Noetherian domain of Krull dimension one. Let $p \in \mathbb{Z}$ be a rational prime. Then K has only finitely many maximal ideals of index p.*

Proof. Let $\mathfrak{m} \lhd K$ be a maximal ideal of index p. Now $\forall x \in K \ x^p - x \in \mathfrak{m}$. So consider the ideal

$$\mathfrak{q} = \sum_{x \in K} (x^p - x)\, K$$

So $\mathfrak{q} \leqslant \mathfrak{m}$. Now, by (5.1.9), $\mathfrak{q} = \mathfrak{p}_1 \dots \mathfrak{p}_t$, where $\mathfrak{p}_i$ is primary, $r(\mathfrak{p}_i) = \mathfrak{m}_i$, a maximal ideal; $\mathfrak{m}_i^{n_i} \leqslant \mathfrak{p}_i$, for some n_i; and $\mathfrak{p}_i + \mathfrak{p}_j = K$, for $i \neq j$. Suppose that $\mathfrak{m}$ is distinct from $\mathfrak{m}_i$, $i = 1, \dots, t$. Now $\mathfrak{m}_i^{n_i} \leqslant \mathfrak{p}_i$ so $K = \mathfrak{m}_i^{n_i} + \mathfrak{m} \leqslant \mathfrak{p}_i + \mathfrak{m}$. So $\forall i \ \ \mathfrak{p}_i + \mathfrak{m} = K$, so $\mathfrak{m} + \mathfrak{q} = \mathfrak{m} + (\mathfrak{p}_1 \dots \mathfrak{p}_t) = K$. But $\mathfrak{q} \leqslant \mathfrak{m}$. Contradiction. So $\mathfrak{m} = \mathfrak{m}_i$, some $i = 1, \dots, t$. Hence result. □

In light of this lemma make the following

Definition. Let K be a Noetherian domain of Krull dimension one. Let $p \in \mathbb{Z}$ be a rational prime. Let

$$\mathcal{M}_p = \bigcap \{\mathfrak{m} \lhd K : |K : \mathfrak{m}| = p\}$$

and if K has no ideals of index p let $\mathcal{M}_p = K$.

Lemma 5.4.12. *Let R be a commutative ring of characteristic* 2. *Let $\mathfrak{q}_1, \mathfrak{q}_2 \lhd R$. Then $(\mathfrak{q}_1\mathfrak{q}_2)^{(4)} = \mathfrak{q}_1^{(4)}\mathfrak{q}_2^{(4)}$.*

Proof. First recall that $\mathfrak{q}_i =< \alpha^4 : \alpha \in \mathfrak{q}_i >$ and $\mathfrak{q}_1^{(4)}\mathfrak{q}_2^{(4)} =< \alpha^4\beta^4 : \alpha \in \mathfrak{q}_1, \beta \in \mathfrak{q}_2 >$. Let $\alpha \in \mathfrak{q}_1$, and $\beta \in \mathfrak{q}_2$ so $\alpha^4\beta^4 = (\alpha\beta)^4 \in (\mathfrak{q}_1\mathfrak{q}_2)^{(4)}$. So $\mathfrak{q}_1^{(4)}\mathfrak{q}_2^{(4)} \leqslant (\mathfrak{q}_1\mathfrak{q}_2)^{(4)}$.

Conversely let $\gamma \in \mathfrak{q}_1\mathfrak{q}_2$, so $\gamma = \sum \alpha_i\beta_i r_i$ where $\alpha_i \in \mathfrak{q}_1, \beta_i \in \mathfrak{q}_2, r_i \in R$. So $\gamma^4 = (\sum \alpha_i\beta_i r_i)^4 = \sum \alpha_i^4\beta_i^4 r_i^4$ as R is of characteristic 2. So $\gamma^4 \in \mathfrak{q}_1^{(4)}\mathfrak{q}_2^{(4)}$. Hence result. □

Recall that if char$K = p$, some prime p then any other rational prime, q is a unit in K. Using this fact we get the following

Theorem 5.4.13. *Let K be a Noetherian domain of Krull dimension one and suppose that char$K = p$, for some prime p. Let $N \lhd SL_2(K)$ be a congruence subgroup. Suppose that $o(N) = K$ and $l(N) = \mathfrak{q}^*$. Then*

1. *If char$K > 3$ then $\mathfrak{q}^* = K$.*
2. *If char$K = 3$ then $\mathcal{M}_3 \leqslant \mathfrak{q}^*$ and if K has no ideals of index 3 then $\mathfrak{q}^* = K$.*
3. *If char$K = 2$ then $\mathcal{M}_2^2 \leqslant \mathfrak{q}^*$ and if K has no ideals of index 2 then $\mathfrak{q}^* = K$.*

Proof. Part 1 follows from (5.4.8). For part 2 consider the setup in the proof of theorem (5.4.8). As char$K = 3$ then 2 is a unit in K and L_i so, by (5.3.14), $o(M_0) = l(M_0)$ unless $|L_i : \mathfrak{m}_i| = 3$, in which case, by (5.3.15), $\mathfrak{m}_i \leqslant l(M_0)$. If $o(M_0) = l(M_0)$ then $\mathfrak{p}_i^* = K$. If $|L_i : \mathfrak{m}_i| = 3$ and $\mathfrak{m}_i \leqslant l(M_0)$ then $\mathfrak{m}_i \leqslant \mathfrak{p}_i^*$. The result follows.

For part 3 we use the same setup as theorem (5.4.8) but in this case, as char$K = 2$ then $2 \notin L_i^*$. Now if $|L_i : \mathfrak{m}_i| > 3$ then $\mathfrak{p}_i^* = K$, as before. Also $|L_i : \mathfrak{m}_i| \neq 3$ for if $|L_i : \mathfrak{m}_i| = 3$ then $3 \in \mathfrak{m}_i$ but as char$K = 2$ then 3 is a unit. Now suppose that $|L_i : \mathfrak{m}_i| = 2$, as $2 = 0$ we have, by (5.3.24) $\mathfrak{m}_i^{(2)} \leqslant l(M_0)$ and so $\mathfrak{m}_i^{(2)} \leqslant \mathfrak{p}_i^*$. The result follows. □

We now deal with case of a normal congruence subgroup of order di stinct from K.

Theorem 5.4.14. *Let K be a Noetherian domain of Krull dimension one and suppose that char$K \neq 2$, or 3. Let $N \lhd SL_2(K)$ be a congruence subgroup. Suppose that $o(N) = \mathfrak{q} \neq K$, and $l(N) = \mathfrak{q}^*$. Then $48\mathfrak{q} \leqslant \mathfrak{q}^*$.*

Proof. Let $\mathfrak{q}^* = \mathfrak{p}_1^* \dots \mathfrak{p}_t^*$ be a primary decomposition. Then, by (5.1.10) $\mathfrak{q} = \mathfrak{p}_1 \dots \mathfrak{p}_t$, where $\mathfrak{p}_i^* \leqslant \mathfrak{p}_i$. Fix $i \in \{1, \dots, t\}$ and consider p_i^*. Let $\mathfrak{q}_0^* = \cap_{j \neq i} \mathfrak{p}_j^*$, $\mathfrak{p}^* = \mathfrak{p}_i^*$, $\mathfrak{q}_0 = \cap_{j \neq i} \mathfrak{p}_j$, and let $\mathfrak{p} = \mathfrak{p}_i$. Let $L_i = K/\mathfrak{p}_i^*$ and let $\varphi_i : SL_2(K) \to SL_2(L_i)$ be the natural homomorphism. Let $N_0 = (N \cap \Gamma(\mathfrak{q}_0^*))\Gamma(\mathfrak{p}^*)$, $\overline{N} = N\Gamma(\mathfrak{p}^*)$. Let $M_0 = \varphi_i(N_0)$, $\overline{M} = \varphi_i(\overline{N})$. Then by lemma (5.4.5) $l(M_0) = 0$, $o(\overline{M}) = \mathfrak{p}/\mathfrak{p}^*$, and $[E_2(L_i), \overline{M}] \leqslant M_0$.

First suppose that $|L_i : \mathfrak{m}_i| > 2$, so by theorem (5.4.7) $o(M_0) = o(\overline{M})$. Now suppose that $2 \in L_i^*$. So, by (5.3.7), and (5.3.14), $o(M_0) = l(M_0) = 0$ unless $|L_i : \mathfrak{m}_i| = 3$ and $o(M_0) = L_i$, in which case, by (5.3.15), $\mathfrak{m}_i \leqslant l(M_0)$. If $o(M_0) = l(M_0)$ then $\mathfrak{p}_i = \mathfrak{p}_i^*$.

If $|L_i : \mathfrak{m}_i| = 3$ and $o(M_0) = L_i$ then $\mathfrak{m}_i \leqslant \mathfrak{p}_i^*$ ie $3\mathfrak{p}_i \leqslant \mathfrak{p}_i^*$. Now suppose that $2 \notin L_i^*$. If $o(M_0) = L_i$ and $|L_i : \mathfrak{m}_i| > 3$ then, by (5.3.14), $l(M_0) = L_i$ and so $\mathfrak{p}_i^* = K$. Also $|L_i : \mathfrak{m}_i| \neq 3$ for if $|L_i : \mathfrak{m}_i| = 3$ then $3 \in \mathfrak{m}_i$ and, as $2 \in \mathfrak{m}_i$, $1 = 3 - 2 \in \mathfrak{m}_i$. Suppose that $o(M_0) \neq L_i$ and $2 \neq 0$ in L_i. Then as $|L_i : \mathfrak{m}_i| > 2$, by (5.3.12), $2o(M_0) \leqslant l(M_0) = 0$, and so $2\mathfrak{p}_i \leqslant \mathfrak{p}_i^*$. Finally if $2 = 0$ in L_i then $2 \in \mathfrak{p}_i^*$, so $2\mathfrak{p}_i \leqslant \mathfrak{p}_i^*$.

Now suppose that $|L_i : \mathfrak{m}_i| = 2$. So if $o(\overline{M}) = L_i$ (ie $\mathfrak{p}_i = K$) then, by (5.4.7), $o(M_0) = o(\overline{M})$ and if $o(\overline{M}) \neq L_i$ (ie $\mathfrak{p}_i \neq K$) then, by (5.4.7), $\mathfrak{m}_i o(\overline{M}) \leqslant o(M_0)$. Now $|L_i : \mathfrak{m}_i| = 2$ so $2 \notin L_i^*$ and $2 \neq 0$. If $o(\overline{M}) = L_i$ then, by (5.4.7), $o(\overline{M}) = o(M_0)$ and, by (5.3.22), $4o(M_0) \leqslant l(M_0)$ so $4\mathfrak{p}_i \leqslant \mathfrak{p}_i^*$. If $o(\overline{M}) \neq L_i$ (and so $o(M_0) \neq L_i$) then, by (5.4.7), $\mathfrak{m}_i o(\overline{M}) \leqslant o(M_0)$ and, by (5.3.6), $8o(M_0) \leqslant l(M_0)$ so $16\mathfrak{p}_i \leqslant \mathfrak{p}_i^*$. If $2 = 0$ in L_i then $2 \in \mathfrak{p}_i^*$, so $2\mathfrak{p}_i \leqslant \mathfrak{p}_i^*$.

So in all cases $48\mathfrak{p}_i \leqslant \mathfrak{p}_i^*$ and so, as before $48\mathfrak{q} \leqslant \mathfrak{q}^*$. □

Again, when ideals of index 2 or 3 are not present we can improve the bound

Corollary 5.4.15. *Let K be a Noetherian domain of Krull dimension one and suppose that char$K \neq 2$, or 3. Let $N \lhd SL_2(K)$ be a congruence subgroup. Suppose that $o(N) = \mathfrak{q} \neq K$, and $l(N) = \mathfrak{q}^*$. Then*

1. *If K has no ideals of index 2 then $6\mathfrak{q} \leqslant \mathfrak{q}^*$. In particular if 6 is a unit then $\mathfrak{q}^* = \mathfrak{q}$.*

2. *If K has no ideals of index 3 then $16\mathfrak{q} \leqslant \mathfrak{q}^*$.*

3. *If K has no ideals of index 2 or 3 then $2\mathfrak{q} \leqslant \mathfrak{q}^*$.*

Example 5.4.1. Let $K = \mathbb{Z}\left[\frac{1}{6}\right]$. So char$K = 0$, and 6 is a unit in K further, K is a Noetherian domain of Krull dimension one, in fact K is a Dedekind domain of arithmetic type. Recall the material in the section on number theory (1.3). Let $p \in \mathbb{Z}$ be prime and define

$$v_p : \mathbb{Q} \to \mathbb{R}$$

as follows. Let $x \in \mathbb{Q}$, so $x = p^{\alpha}\frac{a}{b}$ where $p \nmid a$, and $p \nmid b$. Then let $v_p(x) = p^{-\alpha}$. Let v_∞ denote the usual Archimedean valuation and let $S = \{v_\infty, v_2, v_3\}$ and form $\mathcal{O}_S$ as indicated in section (1.3). We claim that $K = \mathcal{O}_S$ and so is a Dedekind domain of arithmetic type. Let $x \in \mathcal{O}_S$, so $x = a/b$ where $a, b \in \mathbb{Z}$ are coprime. Suppose that a prime $p \neq 2, 3$ divides b, $b = p^{\gamma}b'$, $\gamma \geqslant 0$, $p \nmid b'$ say. Now a and b are coprime so $p \nmid a$, so

$x = p^{-\gamma}\frac{a}{b'}$, so $v_p(x) = p^{\gamma} > 1$, as $\gamma \geqslant 0$, so $x \notin \mathcal{O}_S$. Contradiction. Hence $\mathcal{O}_S \subseteq K$. Now consider $\frac{a}{2^\alpha 3^\beta} \in K$ and let $p \neq 2, 3$ be prime. So $v_p(\frac{a}{2^\alpha 3^\beta}) = v_p(\frac{p^\gamma a'}{2^\alpha 3^\beta}) = p^{-\gamma} \leqslant 1$, as $\gamma \geqslant 0$, so $\frac{a}{2^\alpha 3^\beta} \in \mathcal{O}_S$. So $K \subseteq \mathcal{O}_S$ and so K is a Dedekind domain of arithmetic type.

Theorem 5.4.16. *Let K be a Noetherian domain of Krull dimension one and suppose that char$K = p$, for some prime p. Let $N \lhd SL_2(K)$ be a congruence subgroup. Suppose that $o(N) = \mathfrak{q} \neq K$, and $l(N) = \mathfrak{q}^*$. Then*

1. *If char$K > 3$ then $\mathfrak{q}^* = \mathfrak{q}$.*

2. *If char$K = 3$ then $\mathfrak{q}\mathcal{M}_3 \leqslant \mathfrak{q}^*$.*

3. *If char$K = 2$ then $\mathfrak{q}^{(4)}\mathcal{M}_2^{(4)} \leqslant \mathfrak{q}^*$.*

Proof. Part 1 is obvious. For part 2 we use the same set up as before. As char$K = 3$ then $2 \in K^*$ and so, by examining the above proofs it is obvious that $\mathfrak{p}_i = \mathfrak{p}_i^*$ unless $|L_i : \mathfrak{m}_i| = 3$ and $o(M_0) = L_i$, in which case, by (5.3.15), $\mathfrak{m}_i \leqslant l(M_0)$. In this case $\mathfrak{m}_i \leqslant \mathfrak{p}_i^*$. Hence $\mathfrak{q}^* = \mathfrak{p}_1^* \dots \mathfrak{p}_t^* = \bigcap \mathfrak{p}_i^* \geqslant \mathfrak{q}\mathcal{M}_3$.

Now suppose that char$K = 2$ so that $2 = 0$ and $2 \notin L_i^*$. Again we use the usual setup. First suppose that $|L_i : \mathfrak{m}_i| > 3$ so, by theorem (5.4.7), $o(M_0) = o(\overline{M})$. If $o(M_0) = L_i$ (ie $\mathfrak{p}_i = K$) then, by (5.3.14), $l(M_0) = o(M_0)$ and so $\mathfrak{p}_i^* = \mathfrak{p}_i = K$. If $o(M_0) \neq L_i$ (ie $\mathfrak{p}_i \neq K$) then, by (5.3.13) $o(M_0)^{(2)} \leqslant l(M_0)$ and so $\mathfrak{p}_i^{(2)} \leqslant \mathfrak{p}_i^*$. Now $|L_i : \mathfrak{m}_i| \neq 3$ for if $|L_i : \mathfrak{m}_i| = 3$ then $3 \in \mathfrak{m}_i$ and 3 is a unit. Now suppose that $|L_i : \mathfrak{m}_i| = 2$. If $o(\overline{M}) = L_i$ (ie $\mathfrak{p}_i = K$) then, by (5.4.7), $o(M_0) = o(\overline{M}) = L_i$, so by (5.3.24), $\mathfrak{m}_i^{(2)} \leqslant l(M_0)$, so $\mathfrak{m}_i^{(2)} \leqslant \mathfrak{p}_i^*$. If $o(\overline{M}) \neq L_i$ (so $o(M_0) \neq L_i$) then, by (5.4.7), $\mathfrak{m}_i o(\overline{M}) \leqslant o(M_0)$ and so, as $o(M_0) \neq L_i$, by (5.3.8) $o(M_0)^{(4)} \leqslant l(M_0)$ so, applying (5.4.12), $\mathfrak{m}_i^{(4)}\mathfrak{p}_i^{(4)} = (\mathfrak{m}_i\mathfrak{p}_i)^{(4)} \leqslant \mathfrak{p}_i^*$. It follows that $\mathfrak{q}^* = \bigcap \mathfrak{p}_i^* \leqslant \mathcal{M}_2^{(4)} \bigcap \mathfrak{p}_i^{(4)} = \mathfrak{q}^{(4)}\mathcal{M}_2^{(4)}$ (again using (5.4.12)).

□

In [57] Mason dealt with the case of a normal subgroup of $SL_2(L)$ where L is a commutative local ring with *principal* maximal ideal $\mathfrak{m}$ of index 2. This meant that in [58] he was only able to derive a relationship between the order and level of a normal congruence subgroup of SL_2 over a Dedekind domain. By dropping this condition in section (5.3) we were able to generalize Mason's work to a normal congruence subgroup of SL_2 over any Noetherian domain of Krull dimension one. For comparison we state Mason's results

Theorem. *([58] theroem 3.6) Let A be a Dedekind domain of arithmetic type (see section (1.3)) and suppose that A is contained in a number field and is not totally imaginary. Let $N \lhd SL_2(A)$ be a congruence subgroup. Suppose that $o(N) = \mathfrak{q}$, and $l(N) = \mathfrak{q}^* \neq 0$. Then*

1. *If A has no ideals of index 2 or 3 and 2 is unramified in A then $\mathfrak{q} = \mathfrak{q}^*$.*
2. *If A has no ideals of index 2 and 2 is unramified in A then $3\mathfrak{q} \leqslant \mathfrak{q}^*$.*
3. *If A has no ideals of index 2 or 3 then $2\mathfrak{q} \leqslant \mathfrak{q}^*$.*
4. *If A has no ideals of index 2 then $6\mathfrak{q} \leqslant \mathfrak{q}^*$.*
5. *If A has no ideals of index 3 then $4\mathfrak{q} \leqslant \mathfrak{q}^*$.*
6. *Otherwise, $12\mathfrak{q} \leqslant \mathfrak{q}^*$.*

Theorem. *([58] theorem 3.14) Let A be a Dedekind domain of arithmetic type and suppose that A is contained in a function field in one variable over a finite field k. Let $N \lhd SL_2(A)$ be a congruence subgroup. Suppose that $o(N) = \mathfrak{q}$, and $l(N) = \mathfrak{q}^* \neq 0$. Then*

1. *If $\mathrm{char}K > 3$ or $|k| = 3^\alpha$, where $\alpha > 1$ then $\mathfrak{q} = \mathfrak{q}^*$.*
2. *If $|k| = 3$ then $\mathfrak{q}\mathcal{M}_3 \leqslant \mathfrak{q}^*$.*
3. *If $|k| = 2^\alpha$, where $\alpha > 1$ then $\mathfrak{q}^2 \leqslant \mathfrak{q}^*$.*
4. *If $|k| = 2$ then $\mathfrak{q}^2\mathcal{M}_2^2 \leqslant \mathfrak{q}^*$.*

So when N has order K we get the same results as Mason. However when N has order distinct for K our results are not as good as Mason's. It is clear from comparing the above with our theorems that the problems arise when K has an ideal of index 2 and when the characteristic is 2. It is not known whether our results are best possible or not. Our results are definitely an extension of Mason's for consider the following argument

Lemma 5.4.17. *Let L be a commutative local ring with principal maximal ideal $\mathfrak{m}$. Then if $\mathfrak{q} \lhd L$ such that $\mathfrak{m}^{i+1} \leqslant \mathfrak{q} \leqslant \mathfrak{m}^i$ then $\mathfrak{q} = \mathfrak{m}^{i+1}$, or $\mathfrak{m}^i$.*

Proof. Suppose that $\mathfrak{m} = \alpha L$, so $\mathfrak{m}^i = \alpha^i L$. Let $k = L/\mathfrak{m}$, so $\mathfrak{m}^{i+1}/\mathfrak{m}^i$ is a k-vector space. Let $x + \mathfrak{m}^{i+1} \in \mathfrak{m}^i/\mathfrak{m}^{i+1}$, where $x \in \mathfrak{m}^i$, so $x = \alpha^i y$, where $y \in L$. Let $\overline{y} = y + \mathfrak{m} \in k$. So $\overline{y}(\alpha^i + \mathfrak{m}^{i+1}) = x + \mathfrak{m}^{i+1}$. So $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is generated by $\alpha^i + \mathfrak{m}^{i+1}$ as a k-vector space and so is one dimensional.

Suppose that $\mathfrak{m}^{i+1} \leqslant \mathfrak{q} \leqslant \mathfrak{m}^i$. So $\mathfrak{q}/\mathfrak{m}^{i+1}$ is a subspace of $\mathfrak{m}^i/\mathfrak{m}^{i+1}$. So, as $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is one dimensional $\mathfrak{q} = \mathfrak{m}^i$, or $\mathfrak{m}^{i+1}$. □

Lemma 5.4.18. *Let L be a commutative local ring with principal maximal ideal $\mathfrak{m}$. Suppose that $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0$. Then $\forall\, 0 \neq \mathfrak{q} \lhd L$, $\mathfrak{q} = \mathfrak{m}^\alpha$, some $\alpha \geqslant 1$.*

Proof. $\exists \alpha \in \mathbb{N}$ such that $\mathfrak{q} \leqslant \mathfrak{m}^\alpha$, otherwise $\mathfrak{q} = 0$. Consider $\mathfrak{q} + \mathfrak{m}^{\alpha+1}$. By (5.4.17), $\mathfrak{q}+\mathfrak{m}^{\alpha+1} = \mathfrak{m}^{\alpha+1}$, or $\mathfrak{m}^\alpha$. If $\mathfrak{q}+\mathfrak{m}^{\alpha+1} = \mathfrak{m}^{\alpha+1}$ then $\mathfrak{q} \leqslant \mathfrak{m}^{\alpha+1}$, contradicting the maximality of α. So $\mathfrak{q} + \mathfrak{m}^{\alpha+1} = \mathfrak{m}^\alpha$. Now let $M = \mathfrak{m}^\alpha/\mathfrak{q}$, so M is a finitely generated L-module. Then $\mathfrak{m}M = (\mathfrak{q} + \mathfrak{m}^{\alpha+1})/\mathfrak{q} = \mathfrak{m}^\alpha/\mathfrak{q} = M$. So, by Nakayama's lemma (see [2] page 21), $M = 0$, ie $\mathfrak{q} = \mathfrak{m}^\alpha$. □

Now, again consider $\mathcal{O} = \mathcal{O}_{3,2} = \mathbb{Z} + i\sqrt{3}\mathbb{Z}$. Let $\mathfrak{m} = (2, 1 + i\sqrt{3})$. Then, as in example (5.1.2), $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}$ of index 2 and $\mathfrak{m}^2 < 2\mathcal{O} < \mathfrak{m}$. Let $L = \mathcal{O}/\mathfrak{m}^n$, any $n \geqslant 2$, so in L the ideal $2L$ is not a power of the maximal ideal and so L has a maximal ideal of index 2 which is not principal. In a Dedekind domain ideals are $\frac{3}{2}$-generated. That is let $\mathfrak{q}$ be an ideal in a Dedekind domain and let $x \in \mathfrak{q}$, then $\exists y \in \mathfrak{q}$ such that $\mathfrak{q}$ is generated by x and y. As a consequence of this every local image of a Dedekind domain has a principal maximal ideal.

Example 5.4.2. In this chapter we have derived a relationship between the order and level of a *normal* congruence subgroup. What about *non-normal* congruence subgroups? Here unfortunately there is no relationship. Let $d, p \in \mathbb{Z}$ such that p is a rational prime and $d > 0$ is square free. Consider the groups $SL_2(\mathcal{O}_{d,p})$. By (3.2.1), $SL_2(\mathcal{O}_{d,p}) \ntriangleleft SL_2(\mathcal{O}_d)$, and clearly $SL_2(\mathcal{O}_d, p\mathcal{O}_d) \leqslant SL_2(\mathcal{O}_{d,p})$ so $SL_2(\mathcal{O}_{d,p})$ is a non-normal congruence subgroup of $SL_2(\mathcal{O}_d)$. However $A, T \in SL_2(\mathcal{O}_{d,p})$, so $o(SL_2(\mathcal{O}_{d,p})) = \mathcal{O}_d$ and $\mathcal{O}_{d,p}/p\mathcal{O}_d \cong \mathbb{F}_p$, so $l(SL_2(\mathcal{O}_{d,p})) = p\mathcal{O}_d$.

Chapter 6

Non-congruence subgroups of the Bianchi groups

We now apply the results of the previous chapter to the Bianchi groups $PSL_2(\mathcal{O}_{d,m})$. We take two view points. First we look at the growth of non-congruence subgroups. Then we look at normal subgroups of small index, showing that all but finitely many normal congruence subgroups are of index divisible by 6. Further we classify the normal congruence subgroups with torsion in $PSL_2(\mathcal{O}_d)$, $d = 7, 11, 19$, and $PSL_2(\mathcal{O}_{1,2})$ and the normal congruence subgroups of index not divisible by 6 in $PSL_2(\mathcal{O}_2)$ and $PSL_2(\mathcal{O}_{3,2})$. Normal subgroups of $PSL_2(\mathcal{O}_{d,m})$ of index not divisible by 6 all have torsion. In [25] Fine shows that for $d = 2, 7, 11$ all principal congruence subgroups of $PSL_2(\mathcal{O}_d)$ are torsion free with the exception of $PSL_2(\mathcal{O}_2, \omega\mathcal{O}_2)$. Let $x_i \in G$, we use the notation $N(x_i)$ to denote the normal closure of the elements x_i in G.

6.1 Counting finite index subgroups

In this section we introduce some basic notions about counting subgroups of finite index. The material has been lifted from the survey article of Lubotzky [46]. Let G be any group. Let $a_n(G)$ denote the number of subgroups of G of index exactly n. Ideally we would like to get a formula for $a_n(G)$. The first attempt to do this was by M. Hall in 1949 [35] in which a recursive formula for the number of subgroups of finite index in a free group of finite rank was given. This method was extended and simplified by Dey [20] and Wohlfahrt [92].

Proposition 6.1.1. *[46] Let $t_n(G)$ be the number of transitive permutation representations of G on n objects. Then*

$$a_n(G) = \frac{t_n(G)}{(n-1)!}$$

Proof. Let $H \leqslant G$ be a subgroup of index n. G acts in an obvious way on G/H. Identify G/H with the set $\{1, \dots, n\}$ such that H is identified with 1. There are $(n-1)!$ ways of doing this. Each of these gives rise to a homomorphism $\varphi : G \to S_n$ such that $\varphi(G)$ is transitive and $\mathrm{Stab}(1) = \{\gamma \in G : \varphi(\gamma)(1) = 1\} = H$. Conversely every transitive permutation representation of G on n objects give a subgroup Stab(1) of index n. Thus $(n-1)!a_n(G) = t_n(G)$. □

Let $h_n(G)$ denote the number of homomorphisms from G to S_n.

Lemma 6.1.2. *[46]*

$$h_n(G) = \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(G) h_{n-k}(G)$$

Proof. Suppose that the orbit of 1 is of length k, $1 \leqslant k \leqslant n$. There are $\binom{n-1}{k-1}$ ways of choosing such an orbit, $t_k(G)$ ways of acting on it, and $h_{n-k}(G)$ ways of acting on its complement. □

Theorem 6.1.3. *[46] Let G be any group then*

$$a_n(G) = \frac{1}{(n-1)!} h_n(G) - \sum_{k=1}^{n-1} \frac{1}{(n-k)!} h_{n-k}(G) a_k(G).$$

Proof.

$$\begin{aligned}
h_n(G) &= \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(G) h_{n-k}(G) && \text{by (6.1.2)} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} (k-1)! a_k(G) h_{n-k}(G) && \text{by (6.1.1)} \\
&= \sum_{k=1}^{n} \frac{(n-1)!}{(n-k)!} a_k(G) h_{n-k}(G) \\
&= (n-1)! a_n(G) + \sum_{k=1}^{n-1} \frac{(n-1)!}{(n-k)!} a_k(G) h_{n-k}(G).
\end{aligned}$$

Therefore

$$a_n(G) = \frac{1}{(n-1)!}h_n(G) - \sum_{k=1}^{n-1} \frac{1}{(n-k)!}h_{n-k}(G)a_k(G).$$

□

Now consider the free group on r generators. Since each generator of F_r can be mapped to one of $n!$ elements of S_n we see that $h_n(F_r) = (n!)^r$. Thus

Theorem 6.1.4. *[35] Let F_r be the free group on r generators. Then*

$$a_n(F_r) = n(n!)^{r-1} - \sum_{k=1}^{n-1} [(n-k)!]^{r-1} a_k(F_r).$$

From this it follows [71] that

Theorem 6.1.5.

$$a_n(F_r) \sim n(n!)^{r-1}$$

In [20] Dey extended this work to free products

Theorem 6.1.6. *Let $G = *_{i=1}^{n} A_i$ be a free product of groups. Let $h_n^i = h_n(A_i)$. Then*

$$a_n(G) = \frac{1}{(n-1)!}\left(\prod_{i=1}^{r} h_n^i\right) - \sum_{k=1}^{n-1} \frac{1}{(n-k)!}a_k(G)\left(\prod_{i=1}^{r} h_{n-k}^i\right).$$

Proof. This follows from (6.1.2) and the fact that $h_n(G) = \prod_{i=1}^{n} h_n^i$. □

Recall that the Modular group $PSL_2(\mathbb{Z}) = \mathbb{Z}_2 * \mathbb{Z}_3$. So we can apply the above theorem from which we get

Proposition 6.1.7. *[71]*

$$a_n(PSL_2(\mathbb{Z})) \sim (12\pi e^{1/2})^{-1/2} \exp\left(\frac{n \log n}{6} - \frac{n}{6} + n^{1/2} + n^{1/3} + \frac{\log n}{2}\right).$$

6.2 The growth of non-congruence subgroups in the groups $SL_2(\mathcal{O}_{d,m})$

Recall the following results

Theorem. (2.2.3) *There exists a surjective homomorphism*

$$SL_2(\mathcal{O}_{d,m}) \longrightarrow F_r$$

where $r = r(d,m)$ the rank of the Zimmert Set and a, t lie in the kernel.

Theorem. (5.4.8) *Let $N \lhd SL_2(\mathcal{O}_{d,m})$ be a congruence subgroup of order $\mathcal{O}_{d,m}$. Then $SL_2(\mathcal{O}_{d,m}, 12\mathcal{O}_{d,m}) \leqslant N$.*

Recall that Zimmert's theorem was not best possible; $r(5) = 1$, but $SL_2(\mathcal{O}_5) \twoheadrightarrow F_2$. So, as before, let $\rho(d,m)$ denote the largest rank of a free quotient of $SL_2(\mathcal{O}_{d,m})$. Let FK denote the kernel of the map from $SL_2(\mathcal{O}_{d,m})$ onto $F_{\rho(d,m)}$. Let $N \lhd SL_2(\mathcal{O}_{d,m})$ containing FK. As $t \in FK$ then N has order $\mathcal{O}_{d,m}$. Therefore if N is a congruence subgroup it must contain $SL_2(\mathcal{O}_{d,m}, 12\mathcal{O}_{d,m})$. Observe that $S \leqslant SL_2(\mathcal{O}_{d,m})$ is a congruence subgroup if and only if *coreS* is a congruence subgroup, where by the core of S we mean the largest normal subgroup contained in S. Thus

Proposition 6.2.1. *Let $S \leqslant SL_2(\mathcal{O}_{d,m})$ and suppose that $FK \leqslant S$. Then with finitely many exceptions S is a non-congruence subgroup.*

Using Newmans result (6.1.5) we get

Theorem 6.2.2. *Asymptotically, the number of non-congruence subgroups in the group, $SL_2(\mathcal{O}_{d,m})$, of index precisely n is at least $n(n!)^{\rho-1}$ where $\rho = \rho(d,m) \geqslant r(d,m)$, the rank of the Zimmert Set.*

The vast number of non-congruence subgroups in the above theorem all come from the largest free quotient, all have order $\mathcal{O}_{d,m}$ and all contain elements of finite order. Are most non-congruence subgroups like this? It would be interesting to know about the growth of non-congruence subgroups of order $\mathfrak{q} \neq \mathcal{O}_{d,m}$, or of torsion free non-congruence subgroups.

We now take the opposite view and look at normal subgroups of the Bianchi groups $PSL_2(\mathcal{O}_{d,m})$ of small index with the aim of determining whether they are congruence or non-congruence. First, we have to take a look at $SL_2(L)$ where L is a local image of $\mathcal{O}_{d,m}$.

6.3 $SL_2(L)$ where L is a local image of $\mathcal{O}_{d,m}$

Let L be a finite local homomorphic image of $\mathcal{O}_{d,m}$ with maximal ideal of index 2. Then we can apply (5.3.22) to get

Theorem 6.3.1. *Let L be a finite local homomorphic image of $\mathcal{O}_{d,m}$ with a maximal ideal $\mathfrak{m}$ of index 2. Let $N \lhd SL_2(L)$ be of order L. Then $4L \leqslant l(N)$.*

We now classify all normal subgroups of $SL_2(L)$ with order L by means of the commutator subgroup viz

Theorem 6.3.2. *Let $N \lhd SL_2(L)$. Then $o(N) = L \Leftrightarrow SL_2(L)' \leqslant N$.*

Now $o(SL_2(L)') = L$, as

$$[A,T] = \left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$$

so ($\Leftarrow$) is obvious. First we describe the ideals of $\mathcal{O}_{d,m}$ of index 2.

Theorem 6.3.3. *If $m \equiv 0 \pmod 2$ then $\mathcal{O}_{d,m}$ has exactly one ideal of index 2, namely $(2, m\omega)$. If $m \equiv 1 \pmod 2$ then the ideals of index 2 are:*

$$\begin{cases} (2, 1+m\omega) & \text{if } d \equiv 1 \pmod 4 \\ (2, m\omega) & \text{if } d \equiv 2 \pmod 4 \\ (2, m\omega), (2, 1+m\omega) & \text{if } d \equiv 7 \pmod 8 \\ \textit{none} & \text{if } d \equiv 3 \pmod 8 \end{cases}$$

Proof. The $m \equiv 0 \pmod 2$ case follows from lemma (3.1.4). If $m \equiv 1 \pmod 2$ then we use the isomorphism given in lemma (3.1.5) ie $\mathcal{O}_{d,m}/2\mathcal{O}_{d,m} \cong \mathcal{O}_d/2\mathcal{O}_d$ where $m\omega \leftrightarrow \omega$. So we can assume that $m = 1$. The generators of the maximal ideals can now be found using the theorem on page 107 of [52]. Let

$$f_\omega(X) = \begin{cases} X^2 + d & \text{if } d \equiv 1, 2 \pmod 4 \\ X^2 - X + \frac{d+1}{4} & \text{if } d \equiv 3 \pmod 4 \end{cases}$$

We decompose $f_\omega \pmod 2$ then if g_i is a factor of $f_\omega \pmod 2$, an ideal of index 2 in $\mathcal{O}_d$ is given by $(2, g_i(\omega))$ (see p. 107 of [52]). First, if $d \equiv 3 \pmod 8$ then $D \equiv 5 \pmod 8$, so

$\chi_K(2) = -1$ (see chapter 3 for the definition) so $\mathcal{O}_d/2\mathcal{O}_d$ is a field and $\mathcal{O}_{d,m}$ has no ideals of index 2. Now suppose that $d \equiv 1, 2 \pmod 4$ so

$$f_\omega(X) = X^2 + d \equiv \begin{cases} (X+1)^2 \pmod 2 & \text{if } d \equiv 1 \pmod 4 \\ X^2 \pmod 2 & \text{if } d \equiv 2 \pmod 4 \end{cases}$$

So if $d \equiv 1 \pmod 4$ then $(2, 1 + m\omega)$ is the only ideal of index 2 in $\mathcal{O}_{d,m}$ and if $d \equiv 2 \pmod 4$ then $(2, m\omega)$ is the only ideal of index 2 in $\mathcal{O}_{d,m}$. Now suppose $d \equiv 7 \pmod 8$, so $(d+1)/4 \equiv 0 \pmod 2$, so $f_\omega(X) \equiv X^2 - X \equiv X(X+1) \pmod 2$. So $\mathcal{O}_{d,m}$ has exactly two ideals of index 2, namely $(2, m\omega)$, and $(2, 1 + m\omega)$. □

We compute $SL_2(L)^{ab}$ using a method developed by P. M. Cohn in [15] which we now describe.

Theorem 6.3.4. *Let L be a commutative local ring. Then*

$$SL_2(L)^{ab} \cong (L/M)^+$$

where M is the additive subgroup of L generated by $\{(u^2 - 1)x : x \in L, u \in L^*\}$ and $\{3(u+1)(v+1) : u, v \in L^*\}$, and $(L/M)^+$ is understood to be an additive group. The isomorphism is given by

$$E(x) = \begin{pmatrix} x & 1 \\ -1 & 0 \end{pmatrix} \longmapsto x - 3 \pmod M$$

Proof. This follows from [15] theorem 2, [14] theorem 4.1, and the fact that $SL_2(L) = E_2(L)$ [3]. □

First, ignore the case $d \equiv 7 \pmod 8$ and $m \equiv 1 \pmod 2$ and let L denote the local ring $\mathcal{O}_{d,m}/4\mathcal{O}_{d,m}$.

Lemma 6.3.5. *If $m \equiv 0 \pmod 2$ then $SL_2(L)^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.*

Proof. $L = \{r + m\omega s : r, s = 0, 1, 2, 3\}$, and it is easy to show that $L^* = \{r + m\omega s : r \equiv 1 \pmod 2\}$. Let $u \in L^*$ then $u^2 - 1 = 0$, or $2m\omega$. Now $2m\omega(r + m\omega s) = 0$, or $2m\omega$. So $\{(u^2 - 1)x\} = \{0, 2m\omega\}$. Let $u, v \in L^*$, it is trvial to show that $3(u+1)(v+1) \in \{0, 2m\omega\}$. So $M = \{0, 2m\omega\}$, so $(L/M)^+ \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. Hence result. □

Similarly we can prove:

Lemma 6.3.6. *Suppose that* $d \equiv 1, 2 \pmod 4$ *and* $m \equiv 1 \pmod 2$. *Then* $SL_2(L)^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Consider the following two matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix}$$

Under Cohn's map $SL_2(L) \twoheadrightarrow SL_2(L)^{ab}$ they behave as follows

$$T = E(-1)E(0)^{-1} \mapsto (-1-3) - (0-3) = -1$$

$$U = E(-m\omega)E(0)^{-1} \mapsto (-m\omega - 3) - (0-3) = -m\omega$$

and so, from the proofs of the above lemmata we see that $SL_2(L)^{ab}$ is generated by the images of T and U ie if $m \equiv 0 \pmod 2$ then $SL_2(L)^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 =< U, T; U^2, T^4, TU = UT >$ and if $d \equiv 1, 2 \pmod 4$ and $m \equiv 1 \pmod 2$ then $SL_2(L)^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 =< U, T; U^2, T^2, TU = UT >$. It follows from this that only one of the normal subgroups of $SL_2(L)$ of index 2 contains T. We will use this observation in the next section and we record it as a lemma.

Lemma 6.3.7. *Suppose* $m \equiv 0 \pmod 2$ *or* $d \equiv 1, 2 \pmod 4$ *and* $m \equiv 1 \pmod 2$. *Then* $\exists N \lhd SL_2(L)$ *of index* 2 *which does not contain* T.

We now deal with the case $d \equiv 7 \pmod 8$ and $m \equiv 1 \pmod 2$. In this case $\mathcal{O}_{d,m}$ has two ideals of index 2, so $\mathcal{O}_{d,m}/4\mathcal{O}_{d,m}$ is not local. Instead we let $\mathfrak{m}$ be one of the ideals of index 2 and $L = \mathcal{O}_{d,m}/\mathfrak{m}^3$. We need to describe $\mathfrak{m}^3$.

Lemma 6.3.8. *If* $\mathfrak{m} = (2, m\omega)$ *then* $\mathfrak{m}^3 = (8, m\omega), (8, 4 + m\omega)$, *or* $(8, \pm 2 + m\omega)$.

Proof. First we calculate generators for $\mathfrak{m}^2$. Clearly $\mathfrak{m}^2 = (4, 2m\omega, (m\omega)^2)$. Now $(m\omega)^2 = m(m\omega) - m^2\frac{d+1}{4}$. Now $d \equiv 7 \pmod 8$ so $(d+1)/4 \equiv 0, 2 \pmod 4$ and $m \equiv 1 \pmod 2$ so $m^2 \equiv 1 \pmod 4$ so

$$(m\omega)^2 = \begin{cases} m\omega \pmod{\mathfrak{m}^2} & \text{if } d \equiv 15 \pmod{16} \\ 2 + m\omega \pmod{\mathfrak{m}^2} & \text{if } d \equiv 7 \pmod{16} \end{cases}$$

and $2(2 + m\omega) \equiv 2m\omega \pmod 4$ so $\mathfrak{m}^2 = (4, m\omega)$, or $(4, 2 + m\omega)$.

Now $\mathfrak{m}^3 = \mathfrak{m}\mathfrak{m}^2$. First suppose that $\mathfrak{m}^2 = (4, m\omega)$, so $d \equiv 15 \pmod{16}$. So $\mathfrak{m}^3 = (8, 2m\omega, (m\omega)^2)$. Again $(m\omega)^2 = m(m\omega) - m^2(d+1)/4$. Now $m \equiv 1 \pmod 2$ so $m(m\omega) \equiv m\omega \pmod{\mathfrak{m}^3}$. Since $m^2 \equiv 1 \pmod 8$ and $(d+1)/4 \equiv 0, 4 \pmod 8$, so $m^2(d+1)/4 \equiv 0, 4 \pmod 8$. So $(m\omega)^2 \equiv m\omega$, or $4 + m\omega \pmod{\mathfrak{m}^3}$. So $\mathfrak{m}^3 = (8, m\omega)$, or $(8, 4 + m\omega)$. Now suppose that $\mathfrak{m}^2 = (4, 2 + m\omega)$. So $\mathfrak{m}^3 = (8, 4m\omega, 2(2 + m\omega), m\omega(2 + m\omega))$. Now $2 \times 2(2 + m\omega) \equiv 4m\omega$, and we can show that $(m\omega)^2 \equiv \pm 2 + m\omega$. Also $2(\pm 2 + m\omega) \equiv 4 + 2m\omega$. So $\mathfrak{m}^3 = (8, \pm 2 + m\omega)$. Hence result. □

In a similar way we can prove

Lemma 6.3.9. *If* $\mathfrak{m} = (2, 1 + m\omega)$ *then* $\mathfrak{m}^3 = (8, \pm 1 + m\omega)$.

Lemma 6.3.10. *Suppose that* $d \equiv 7 \pmod 8$ *and* $m \equiv 1 \pmod 2$. *Let* $\mathfrak{m} \lhd \mathcal{O}_{d,m}$ *be an ideal of index* 2, *so* $\mathfrak{m} = (2, m\omega)$, *or* $(2, 1 + m\omega)$. *Let* $L = \mathcal{O}_{d,m}/\mathfrak{m}^3$. *Then* $SL_2(L)^{ab} \cong \mathbb{Z}_4$.

Proof. Suppose first that $\mathfrak{m} = (2, m\omega)$, so $\mathfrak{m}^3 = (8, m\omega), (8, 4 + m\omega)$, or $(8, \pm 2 + m\omega)$. Suppose $r + m\omega s \in L$, we can assume that $0 \leqslant r, s \leqslant 7$. Then $r + m\omega s \equiv r + m\omega s - s(m\omega) = r \pmod{(8, m\omega)}$, or $r + m\omega s \equiv r + m\omega s - s(4 + m\omega) = r - 4s \pmod{(8, 4 + m\omega)}$, or $r + m\omega s \equiv r + m\omega s - s(\pm 2 + m\omega) = r \pm 2s \pmod{(8, \pm 2 + m\omega)}$. So $L = \{0, 1, 2, 3, 4, 5, 6, 7\} \cong \mathbb{Z}_8$. Applying Cohn's method we see that $SL_2(L)^{ab} \cong \mathbb{Z}_4$.

Now suppose that $\mathfrak{m} = (2, 1 + m\omega s)$, so $\mathfrak{m}^3 = (8, \pm 1 + m\omega)$. As above we can show that $L = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and so $SL_2(L)^{ab} \cong \mathbb{Z}_4$. □

We now present the proof of theorem (6.3.2) as a series of lemmas.

Lemma 6.3.11. *Suppose that* $d \equiv 7 \pmod 8$ *and* $m \equiv 1 \pmod 2$. *Let* $N \lhd SL_2(L)$. *Then* $o(N) = L \Leftrightarrow SL_2(L)' \leqslant N$.

Proof. Let Γ denote $SL_2(L)$. Now $o(\Gamma') = L$, so $(\Leftarrow)$ is obvious. Conversely suppose that $o(N) = L$ and $\Gamma' \nleqslant N$. So, by (5.3.17), $|\Gamma : N| = 2^\alpha$ and Γ/N is non-abelian, so $\alpha \geqslant 3$. So Γ/N is a 2-group of order $\geqslant 8$, so $\exists M \lhd \Gamma$ such that $N \leqslant M$ and $|\Gamma : M| = 8$, and $o(M) = L$. Now $\Gamma^{ab} = \mathbb{Z}_4$, so Γ/M is non-abelian, so $\Gamma/M \cong Q_8$, or D_8, the only non-abelian groups of order 8 [68]. Now $Q_8^{ab} \cong D_8^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so $(\Gamma/M)^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. But $\Gamma \twoheadrightarrow \Gamma/M$, so $\Gamma^{ab} \twoheadrightarrow (\Gamma/M)^{ab}$, so $\mathbb{Z}_4 \twoheadrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$. Contradiction. Hence result. □

Unfortunately this technique does not work in the other cases. Instead we use the observation (5.3.18) that if $N \lhd SL_2(L)$ is of order L then N contains every matrix in $SL_2(L)$

of order 3. Let $N(3)$ denote the normal closure of all elements of order 3. We attempt to show that $SL_2(L)' = N(3)$. Note that because we have shown (5.3.22) that if $o(N) = L$ then $SL_2(L, 4L) \leqslant N$ we can work mod 4. Recall that $SL_2(L) = E_2(L)$ and let

$$E_{12}(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, E_{21}(y) = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}.$$

So $SL_2(L)$ is generated by $E_{12}(x)$ and $E_{21}(y)$ where $x, y = 1, m\omega$. It is easy to compute that

$$[E_{12}(x), E_{21}(y)] = \begin{pmatrix} 1 + xy + (xy)^2 & -x^2y \\ xy^2 & 1 - xy \end{pmatrix}$$

we want to show that $[E_{12}(x), E_{21}(y)] \in N(3)$ for $(x, y) = (1, 1), (1, m\omega), (m\omega, 1), (m\omega, m\omega)$. We make frequent use of lemma (5.3.20) without comment.

Lemma 6.3.12. $[E_{12}(1), E_{21}(1)]^3 = I$.

Lemma 6.3.13. *Suppose that* $d \equiv 1, 2 \pmod 4$ *and* $m \equiv 0 \pmod 2$. *Then* $SL_2(L)' = N(3)$.

Proof. In this case $(m\omega)^2 = -dm^2 = 0$ as $m \equiv 0 \pmod 2$ and we are working mod 4. This shows that $[E_{12}(m\omega), E_{21}(m\omega)] = I$. Now

$$[E_{12}(1), E_{21}(m\omega)] = \begin{pmatrix} 1 + m\omega & -m\omega \\ 0 & 1 - m\omega \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -(1 - m\omega) \\ 1 + m\omega & -1 \end{pmatrix}.$$

Similarly for $[E_{12}(m\omega), E_{21}(1)]$. □

Lemma 6.3.14. *Suppose that* $d \equiv 3 \pmod 4$ *and* $m \equiv 0 \pmod 2$. *Then* $SL_2(L)' = N(3)$.

Proof. First note that if $m \equiv 0 \pmod 4$ then $(m\omega)^2 = 0$, and if $m \equiv 2 \pmod 4$ then $(m\omega)^2 = 2m\omega$. This renders the $m \equiv 0 \pmod 4$ case identical to the $d \equiv 1, 2 \pmod 4$ cases above. So suppose $m \equiv 2 \pmod 4$. Then

$$[E_{12}(1), E_{21}(m\omega)] = \begin{pmatrix} 1 - m\omega & -m\omega \\ 2m\omega & 1 - m\omega \end{pmatrix}$$

and this equals

$$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2m\omega & 1 - m\omega \\ -(1 + m\omega) & -1 + 2m\omega \end{pmatrix} \in N(3)$$

Similarly $[E_{12}(m\omega), E_{21}(1)] \in N(3)$. Now

$$[E_{12}(m\omega), E_{21}(m\omega)] = \begin{pmatrix} 1+2m\omega & 0 \\ 0 & 1+2m\omega \end{pmatrix}$$

and this equals

$$\begin{pmatrix} -1+m\omega & -1 \\ 1+m\omega & -m\omega \end{pmatrix} \begin{pmatrix} -1 & -1+m\omega \\ 1-m\omega & 0 \end{pmatrix} \begin{pmatrix} -1 & -1+2m\omega \\ 1+2m\omega & 0 \end{pmatrix} \in N(3)$$

□

Lemma 6.3.15. *Suppose that $d \equiv 1 \pmod 4$ and $m \equiv 1 \pmod 2$. Then $SL_2(L)' = N(3)$.*

Proof. In this case $(m\omega)^2 = -1$, so

$$[E_{12}(m\omega), E_{21}(1)] = \begin{pmatrix} m\omega & 1 \\ m\omega & 1-m\omega \end{pmatrix}$$

and this equals

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}^2 \begin{pmatrix} 0 & -m\omega \\ -m\omega & -1 \end{pmatrix} \in N(3).$$

similarly $[E_{12}(m\omega), E_{21}(1)] \in N(3)$. Also

$$[E_{12}(m\omega), E_{21}(m\omega)] = \begin{pmatrix} 1 & -m\omega \\ m\omega & 2 \end{pmatrix}$$

so $[E_{12}(m\omega), E_{21}(m\omega)]^3 = I$. Hence result. □

Lemma 6.3.16. *Suppose that $d \equiv 2 \pmod 4$ and $m \equiv 1 \pmod 2$. Then $T^2 \in N(3)$, and so $-I \in N(3)$.*

Proof. By lemma (5.3.20)

$$\begin{pmatrix} 0 & 1+m\omega \\ 3+m\omega & -1 \end{pmatrix} \in N(3)$$

and this equals

$$\begin{pmatrix} 1 & 1+m\omega \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & 3+m\omega \\ 0 & 1 \end{pmatrix} A^{-1} \begin{pmatrix} 1 & 2+2m\omega \\ 0 & 1 \end{pmatrix}$$

$$= T \begin{pmatrix} 1 & m\omega \\ 0 & 1 \end{pmatrix} AT \begin{pmatrix} 1 & 2+m\omega \\ 0 & 1 \end{pmatrix} A^{-1}T^{-1} \begin{pmatrix} 1 & 3+2m\omega \\ 0 & 1 \end{pmatrix}$$

so, as $AT, A^{-1}T^{-1} \in N(3)$, and $4 = 0$, we see that $T^2 \in N(3)$. □

Lemma 6.3.17. *Suppose that* $d \equiv 2 \pmod 4$ *and* $m \equiv 1 \pmod 2$. *Then* $SL_2(L)' = N(3)$.

Proof. In this case $(m\omega)^2 = 2$, so

$$[E_{12}(1), E_{21}(m\omega)] = \begin{pmatrix} -1+m\omega & -m\omega \\ 2 & 1-m\omega \end{pmatrix}$$

and this equals

$$\begin{pmatrix} -1 & 1-m\omega \\ 1+m\omega & 0 \end{pmatrix} \begin{pmatrix} 2+2m\omega & 1-2m\omega \\ 1 & 1+2m\omega \end{pmatrix} \in N(3)$$

Similarly $[E_{12}(m\omega), E_{21}(1)] \in N(3)$. However

$$[E_{12}(m\omega), E_{21}(m\omega)] = \begin{pmatrix} -1 & 2m\omega \\ 2m\omega & -1 \end{pmatrix}$$

and this equals

$$-I \begin{pmatrix} 2m\omega & 1 \\ -1+2m\omega & -1+2m\omega \end{pmatrix} \begin{pmatrix} -1 & -1+2m\omega \\ 1+2m\omega & 0 \end{pmatrix} \in N(3)$$

Hence result. □

We have now proved theorem (6.3.2). From the above we can get an improved lower bound for the level in some cases

Theorem 6.3.18. *Suppose that* $d \equiv 1, 2 \pmod 4)$ *and* $m \equiv 1 \pmod 2$. *Let* $L = \mathcal{O}_{d,m}/4\mathcal{O}_{d,m}$. *Let* $N \lhd SL_2(L)$, $o(N) = L$. *Then* $2L \leqslant l(N)$.

6.4 Non-congruence subgroups of small index in the Bianchi groups

Here we need to be very clear about the differences between SL_2 and PSL_2 so we restate the relevant definitions. Let $\mathcal{O} = \mathcal{O}_{d,m}$ be an order in an imaginary quadratic number field. Let $0 \neq \mathfrak{q} \lhd \mathcal{O}$.

$$SL_2(\mathcal{O}, \mathfrak{q}) = \{M \in SL_2(\mathcal{O}) : M \equiv I \pmod{\mathfrak{q}}\}$$

$SL_2(\mathcal{O}, \mathfrak{q})$ is the *principal congruence subgroup of level* $\mathfrak{q}$. Let $S \leqslant SL_2(\mathcal{O})$. We say that S is a *congruence subgroup* if $SL_2(\mathcal{O}, \mathfrak{q}) \leqslant S$ for some $\mathfrak{q} \lhd \mathcal{O}$. If $\mathfrak{q}$ is the largest $\mathcal{O}$-ideal such that $SL_2(\mathcal{O}, \mathfrak{q}) \leqslant S$ we say that S is of *level* $\mathfrak{q}$. Otherwise S is a *non-congruence subgroup*. Let

$$\varphi : SL_2(\mathcal{O}) \longrightarrow PSL_2(\mathcal{O})$$

be the natural homomorphism. Let $\mathfrak{q} \lhd \mathcal{O}$, then

$$PSL_2(\mathcal{O}, \mathfrak{q}) = \varphi(SL_2(\mathcal{O}, \mathfrak{q}))$$

$PSL_2(\mathcal{O}, \mathfrak{q})$ is the *principal congruence subgroup of level* $\mathfrak{q}$. Let $S \leqslant PSL_2(\mathcal{O})$. We say that S is a *congruence subgroup* if $PSL_2(\mathcal{O}, \mathfrak{q}) \leqslant S$, for some $\mathfrak{q} \lhd \mathcal{O}$. If $\mathfrak{q}$ is the largest $\mathcal{O}$-ideal such that $PSL_2(\mathcal{O}, \mathfrak{q}) \leqslant S$ we say that S is of *level* $\mathfrak{q}$. Otherwise S is a *non-congruence subgroup.*

Lemma 6.4.1. *Let $N \lhd SL_2(\mathcal{O})$ such that $-I \in N$. Let $\overline{N} = \varphi(N)$. Then*

$$N \textit{ is a congruence subgroup } \Leftrightarrow \overline{N} \textit{ is a congruence subgroup}$$

Further N and $\overline{N}$ have the same level.

Proof. Suppose that N is a congruence subgroup. So $SL_2(\mathcal{O}, \mathfrak{q}) \leqslant N$, some $0 \neq \mathfrak{q} \lhd \mathcal{O}$. So $PSL_2(\mathcal{O}, \mathfrak{q}) = \varphi(SL_2(\mathcal{O}, \mathfrak{q})) \leqslant \varphi(N) = \overline{N}$ ie $\overline{N}$ is a congruence subgroup.

Conversely suppose that $\overline{N}$ is a congruence subgroup. So $PSL_2(\mathcal{O}, \mathfrak{q}) \leqslant \overline{N}$, some $\mathfrak{q} \lhd \mathcal{O}$. Suppose that $SL_2(\mathcal{O}, \mathfrak{q}) \nleqslant N$, so $\exists M_1 \in SL_2(\mathcal{O}, \mathfrak{q})$ such that $M_1 \notin N$. But $\varphi(M_1) \in \varphi(SL_2(\mathcal{O}, \mathfrak{q})) = PSL_2(\mathcal{O}, \mathfrak{q}) \leqslant \overline{N} = \varphi(N)$. So $\exists M_2 \in N$ such that $\varphi(M_1) = \varphi(M_2)$. So $M_1 M_2^{-1} \in \ker \varphi = \{\pm I\}$, so $M_1 = \pm M_2$. Now $M_1 \neq M_2$, as $M_1 \notin N$, and $M_2 \in N$. So $M_1 = -M_2 = -IM_2$, but $-I \in N$ and $M_2 \in N$, so $M_1 \in N$. Contradiction. So $SL_2(\mathcal{O}, \mathfrak{q}) \leqslant N$ ie N is a congruence subgroup. □

So the normal congruence subgroups of $SL_2(\mathcal{O})$ of level $\mathfrak{q}$ that contain $-I$ are in one to one correspondence with the normal congruence subgroups of $PSL_2(\mathcal{O})$ of level $\mathfrak{q}$ and they clearly have the same index. So we attempt to classify the normal congruence subgroups of $PSL_2(\mathcal{O})$ of index n by classifying the normal congruence subgroups of $SL_2(\mathcal{O})$ of index n which contain $-I$.

Lemma 6.4.2. *Let $\mathcal{O} = \mathcal{O}_{d,m}$ and suppose that $N \lhd SL_2(\mathcal{O})$. Let $n \in \mathbb{N}$. Then if T^n, and $U^n \in N$ then $E_2(\mathcal{O}, n\mathcal{O}) \leqslant N$.*

Proof. Recall that

$$E_2(\mathcal{O}, n\mathcal{O}) =< I + \alpha e_{ij} : \alpha \in n\mathcal{O}, i \neq j >^{E_2(\mathcal{O})} .$$

Let $\alpha \in n\mathcal{O}$, so $\alpha = n(z_1 + m\omega z_2)$, where $z_1, z_2 \in \mathbb{Z}$. Now

$$\begin{aligned} I + \alpha e_{12} &= \begin{pmatrix} 1 & nz_1 + nm\omega z_2 \\ 0 & 1 \end{pmatrix} \\ &= (T^n)^{z_1}(U^n)^{z_2} \in N. \end{aligned}$$

Similarly $I + \alpha e_{21} \in N$. So, as N is normalized by $E_2(\mathcal{O})$ then $E_2(\mathcal{O}, n\mathcal{O}) \leqslant N$. □

Recall the following results

Theorem. (3.2.2) *Let $\mathcal{O} = \mathcal{O}_{d,m}$. Let $N \lhd SL_2(\mathcal{O})$ be of index n and suppose that $6 \nmid n$. Then N is of order $\mathcal{O}$.*

Theorem. (5.4.10) *Let $\mathcal{O} = \mathcal{O}_{d,m}$. Let $N \lhd SL_2(\mathcal{O})$ be a congruence subgroup of order $\mathcal{O}$ that contains $-I$. Then $SL_2(\mathcal{O}, 6\mathcal{O}) \leqslant N$.*

So that any normal congruence subgroup of $SL_2(\mathcal{O}_{d,m})$ of index not divisible by 6 and containing $-I$ must contain $SL_2(\mathcal{O}_{d,m}, 6\mathcal{O}_{d,m})$. This gives us a method to classify the normal congruence subgroups of $SL_2(\mathcal{O}_{d,m})$ of index not divisible by 6. In fact we can be more precise.

Lemma 6.4.3. *Let $\mathcal{O} = \mathcal{O}_{d,m}$. Let $N \lhd SL_2(\mathcal{O})$ be of index n that contains $-I$ and suppose that $6 \nmid n$. Then*

1. *If $2 \mid n$ and $3 \nmid n$ then N is a congruence subgroup $\Leftrightarrow SL_2(\mathcal{O}, 2\mathcal{O}) \leqslant N$.*

2. *If $2 \nmid n$ and $3 \mid n$ then N is a congruence subgroup $\Leftrightarrow SL_2(\mathcal{O}, 3\mathcal{O}) \leqslant N$.*

3. *If $(6, n) = 1$ then N is a non-congruence subgroup.*

Proof. Now, N is a normal congruence subgroup of index n, so using (6.4.2) and (5.2.5), $SL_2(\mathcal{O}, n\mathcal{O}) \leqslant N$. Applying Wohlfahrts theorem (5.2.3) we see that $SL_2(\mathcal{O}, n\mathcal{O})SL_2(\mathcal{O}, 6\mathcal{O}) = SL_2(\mathcal{O}, \gcd(6, n)\mathcal{O}) \leqslant N$ from which the result follows. □

Let $\mathcal{N}_{d,m}(n)$ denote the number of normal congruence subgroups of $PSL_2(\mathcal{O}_{d,m})$ of index precisely n. So by the above lemma if $(6,n)=1$ then $\mathcal{N}_{d,m}(n)=0$. If $SL_2(\mathcal{O}_{d,m})$ has an infinite cyclic quotient then it has a normal subgroup of every index. In contrast the Modular group has only two normal subgroups which are not of index $6k$, some $k \in \mathbb{N}$ ([70] theorems 8.6 and 8.7). However by (6.4.3), with only finitely many exceptions, every normal *congruence* subgroup of $SL_2(\mathcal{O}_{d,m})$ is of index $6k$, some $k \in \mathbb{N}$. We need the following lemma

Lemma 6.4.4. *Let K be a Noetherian domain of Krull dimension one. Let $\mathfrak{q}_1, \mathfrak{q}_2 \lhd K$ such that $\mathfrak{q}_1 + \mathfrak{q}_2 = K$. Then*

$$SL_2(K/\mathfrak{q}_1\mathfrak{q}_2) \cong SL_2(K/\mathfrak{q}_1) \times SL_2(K/\mathfrak{q}_2)$$

Proof. By the Chinese remainder theorem $K/\mathfrak{q}_1\mathfrak{q}_2 \cong K/\mathfrak{q}_1 \times K/\mathfrak{q}_2$ where the isomorphism is given by $x+\mathfrak{q}_1\mathfrak{q}_2 \mapsto (x+\mathfrak{q}_1, x+\mathfrak{q}_2) = (x_1, x_2)$. Define $\varphi : SL_2(K/\mathfrak{q}_1\mathfrak{q}_2) \to SL_2(K/\mathfrak{q}_1) \times SL_2(K/\mathfrak{q}_2)$ by

$$\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \mapsto \left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right)$$

where $\overline{a} = a + \mathfrak{q}_1\mathfrak{q}_2 \mapsto (a_1, a_2)$ etc. It is simple, if tedious to check that φ is an monomorphism (indeed it is true for any commutative ring). To show that φ is onto we need Wohlfahrt's theorem (5.2.5). By Wohlfahrt $SL_2(K,\mathfrak{q}_1)SL_2(K,\mathfrak{q}_2) = SL_2(K, \mathfrak{q}_1+\mathfrak{q}_2) = SL_2(K)$. Also $SL_2(K,\mathfrak{q}_1) \cap SL_2(K,\mathfrak{q}_2) = SL_2(K,\mathfrak{q}_1\mathfrak{q}_2)$. So in the group $SL_2(K/\mathfrak{q}_1\mathfrak{q}_2) = G$ we have two normal subgroups H, K, say such that $HK = G$ and $H \cap K = 1$. So by [79] theorem 4.1 we have $G \cong H \times K$. Hence result. □

Lemma 6.4.5. *Let $\mathcal{O} = \mathcal{O}_{d,m}$. Let $n \in \mathbb{N}$ and suppose that $2 \mid n$ and $3 \nmid n$. Then*

1. *If $\mathcal{O}$ has no ideals of index 2 then $\mathcal{N}_{d,m}(n) = 0$.*
2. *If $\mathcal{O}$ has an ideal of index 2 then* $\mathcal{N}_{d,m}(n) = \begin{cases} 3 & \textit{if } n=2 \\ 1 & \textit{if } n=4 \\ 0 & \textit{else} \end{cases}$

Proof. Let $N \lhd SL_2(\mathcal{O})$ be a congruence subgroup of index n that contains $-I$. Then by (6.4.3) $SL_2(\mathcal{O}, 2\mathcal{O}) \leqslant N$. There are 3 cases, depending on how many ideals of index two $\mathcal{O}$ has. If $\mathcal{O}$ has no ideals of index 2 then $SL_2(\mathcal{O})/SL_2(\mathcal{O}, 2\mathcal{O}) \cong SL_2(\mathbb{F}_4)$ but $-I \in N$

and $PSL_2(\mathbb{F}_4)$ is simple, so $\mathcal{N}_{d,m}(n) = 0$. Now suppose that $\mathcal{O}$ has exactly one ideal of index 2. Let L denote the local ring $\mathcal{O}/2\mathcal{O}$, so $SL_2(\mathcal{O})/SL_2(\mathcal{O}, 2\mathcal{O}) \cong SL_2(L)$. Now corresponding to N is $\overline{N} \lhd SL_2(L)$, $o(\overline{N}) = L$. So, by (6.3.2), $SL_2(L)' \leqslant \overline{N}$. Now $-I \in N$ so, by (5.3.19), (6.3.5) and (6.3.6), $SL_2(\mathcal{O})/N$ is a factor of $\mathbb{Z}_2 \times \mathbb{Z}_2$ which, by (3.4.10), has exactly 3 non-trivial normal subgroups, all of index 2. The result follows in this case. Finally suppose that $\mathcal{O}$ has two ideals of index 2. In this case, by (6.4.4), $SL_2(\mathcal{O})/SL_2(\mathcal{O}, 2\mathcal{O}) \cong S_3 \times S_3$, so $|SL_2(\mathcal{O}) : SL_2(\mathcal{O}, 2\mathcal{O})| = 2^2 3^2$. So N is of index 2 or 4, so $SL_2(\mathcal{O})/N$ is abelian. Now $(SL_2(\mathcal{O})/SL_2(\mathcal{O}, 2\mathcal{O}))^{ab} \cong S_3^{ab} \times S_3^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and so the answer is as the previous case. □

Lemma 6.4.6. *Let $\mathcal{O} = \mathcal{O}_{d,m}$. Let $n \in \mathbb{N}$ and suppose that $2 \nmid n$ and $3 \mid n$. Then*

1. *If $\mathcal{O}$ has no ideals of index 3 then $\mathcal{N}_{d,m}(n) = 0$.*

2. *If $\mathcal{O}$ has exactly one ideal of index 3 then* $\mathcal{N}_{d,m}(n) = \begin{cases} 1 & \textit{if } n = 3 \\ 0 & \textit{else} \end{cases}$

3. *If $\mathcal{O}$ has exactly two ideals of index 3 then* $\mathcal{N}_{d,m}(n) = \begin{cases} 4 & \textit{if } n = 3 \\ 1 & \textit{if } n = 9 \\ 0 & \textit{else} \end{cases}$

Proof. Let $N \lhd SL_2(\mathcal{O})$ be a congruence subgroup of index n that contains $-I$. Then by (6.4.3), $SL_2(\mathcal{O}, 3\mathcal{O}) \leqslant N$. First suppose that $\mathcal{O}$ has no ideals of index 3. Then $SL_2(\mathcal{O})/SL_2(\mathcal{O}, 3\mathcal{O}) \cong SL_2(\mathbb{F}_9)$ but $-I \in N$ and $PSL_2(\mathbb{F}_9)$ is simple, so $\mathcal{N}_{d,m}(n) = 0$. Now suppose that $\mathcal{O}$ has exactly one ideal of index three, $\mathfrak{m}$, say and let L denote the local ring $\mathcal{O}/3\mathcal{O}$. So, by passing to $SL_2(L)$ and applying (5.3.15) we see that $SL_2(\mathcal{O}, \mathfrak{m}) \leqslant N$. Now $SL_2(\mathcal{O})/SL_2(\mathcal{O}, \mathfrak{m}) = SL_2(\mathbb{F}_3)$, $-I \in N$ and, by [79] exercise 8.11, $PSL_2(\mathbb{F}_3) \cong A_4$ which has exactly one normal subgroup, which is of index 3. Hence result in this case. Finally suppose that $\mathcal{O}$ has exactly two ideals of index three, $\mathfrak{m}_i$, $i = 1, 2$, say. Now, by (6.4.4),

$$\frac{SL_2(\mathcal{O})}{SL_2(\mathcal{O}, 3\mathcal{O})} \cong SL_2(\mathbb{F}_3) \times SL_2(\mathbb{F}_3)$$

and $|SL_2(\mathbb{F}_3)| = 24$ (this follows from [79] theorem 8.8), so $|SL_2(\mathcal{O}) : SL_2(\mathcal{O}, 3\mathcal{O})| = 2^6 3^2$. So N is of index 3 or 9 and so $SL_2(\mathcal{O})/N$ is abelian. Now $SL_2(\mathbb{F}_3)^{ab} \cong \mathbb{Z}_3$ so

$$\left(\frac{SL_2(\mathcal{O})}{SL_2(\mathcal{O}, 3\mathcal{O})}\right)^{ab} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$$

and, $-I^2 = I$ so $-I \in SL_2(\mathcal{O}/3\mathcal{O})'$. Now, by (3.4.10), $\mathbb{Z}_3 \times \mathbb{Z}_3$ has exactly 4 non-trivial normal subgroups, all of index 3. Hence result in this case. □

In [31] Grunewald and Schwermer determine the minimum index of a non-congruence subgroup of a Bianchi group. Let $ncs(d)$ denote the minimum index of a non-congruence subgroup of $PSL_2(\mathcal{O}_d)$. Their main result is

Theorem.

$$ncs(d) = \begin{cases} 5 & \textit{if } d = 1 \\ 4 & \textit{if } d = 2 \\ 22 & \textit{if } d = 3 \\ 3 & \textit{if } d = 7 \\ 2 & \textit{else} \end{cases}$$

In the Modular group the least index of a non-congruence subgroup if 7 ([83] theorem 5.4). There is considerable overlap with Grunewald and Schwermer's theorem and what follows but our techniques are completely different. First recall the following

Theorem.

$$\varphi : \frac{SL_2(\mathcal{O}_{d,m})}{U_2(\mathcal{O}_{d,m})} \twoheadrightarrow F_s$$

where $s = r - 1$, and $r = r(d, m)$, the rank of the Zimmert Set and $U \in \ker \varphi$.

Theorem 6.4.7. *If $r = r(d, m) \geqslant 2$ then $SL_2(\mathcal{O}_{d,m})$ has a normal non-congruence subgroup containing $-I$ of every index.*

Proof. Since $r \geqslant 2$ we have

$$\varphi : \frac{SL_2(\mathcal{O}_{d,m})}{U_2(\mathcal{O}_{d,m})} \twoheadrightarrow \mathbb{Z}$$

and clearly $-I \in \ker \varphi$. Suppose that $N \lhd SL_2(\mathcal{O}_{d,m})$ such that $\ker \varphi \leqslant N$, so $T, U \in N$, so $l(N) = \mathcal{O}_{d,m}$. So, if N is a congruence subgroup then $N = SL_2(\mathcal{O}_{d,m})$. Thus $SL_2(\mathcal{O}_{d,m})$ has a normal non-congruence subgroup containing $-I$ of every index. □

Corollary 6.4.8. *If $r = r(d, m) \geqslant 2$ then $PSL_2(\mathcal{O}_{d,m})$ contains a normal non-congruence subgroup of every index.*

Not included in the above theorem are the cases $d = 1, 2, 3, 7, 11, 19$, and $m = 1$ and $(d, m) = (1, 2), (3, 2)$. We are unable to deal with the cases $(d, m) = (1, 1), (3, 1)$ but we take a closer look at the others later. Recall that it is conjectured that these are the only values of (d, m) such that $PSL(\mathcal{O}_{d,m})$ does not have a free non-abelian quotient.

All the non-congruence subgroups produced above contain the Zimmert kernel and so have torsion. We now show that in any Bianchi group the number of normal congruence subgroups with torsion is finite. Recall

Theorem. (1.1.8) *$I \neq M \in SL_2(\mathcal{O}_{d,m})$ is of finite order if and only if $trM = 0$, or ± 1.*

We now show that the order of a subgroup with torsion is severely restricted. Let $M \in SL_2(\mathcal{O}_{d,m})$ and recall that the order, $o(M)$, of the matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the ideal of $\mathcal{O}_{d,m}$ generated by $b, c, a - d$. The order of any subgroup containing M contains $o(M)$.

Lemma 6.4.9. *Let $M \in SL_2(\mathcal{O}_{d,m})$. Then if $trM = 0$ then $2 \in o(M)$.*

Proof. $a + d = 0$, so $a = -d$. Now $a - d = 2a \in o(M)$. Also $1 = ad - bc = -a^2 - bc$, so $1 + a^2 \in o(M)$. Thus $2a^2 + 2 \in o(M)$ and, because $2a \in o(M)$ we have $2a^2 \in o(M)$. Hence $2 \in o(M)$. □

Lemma 6.4.10. *Let $M \in SL_2(\mathcal{O}_{d,m})$. Then if $trM = \pm 1$ then $3 \in o(M)$.*

Proof. First suppose that $\mathrm{tr}M = -1$, so $a + d = -1$ and $a = -1 - d$. Now $a - d = 2a + 1 \in o(M)$. Also $1 = ad - bc = -a - a^2 - bc$, so $a^2 + a + 1 = -bc \in o(M)$. So $2a^2 + 1 = 2(a^2 + a + 1) - (2a + 1) \in o(M)$. Further $1 - a = 2a^2 + 1 - (2a + 1)a \in o(M)$. So $3 = 2(1 - a) + 2a + 1 \in o(M)$. Similarly if $\mathrm{tr}M = 1$. □

Theorem 6.4.11. *There are only finitely many normal congruence subgroups with torsion in $SL_2(\mathcal{O}_{d,m})$.*

Proof. Let $N \lhd SL_2(\mathcal{O}_{d,m})$ and suppose that N has torsion and is a congruence subgroup. So N contains a matrix M, say with $\mathrm{tr}M = 0$, or ± 1. So 2, or $3 \in o(N)$, so $6 \in o(N)$. Now N is a normal congruence subgroup so, by (5.4.14), $SL_2(\mathcal{O}_{d,m}, 288\mathcal{O}_{d,m}) \leqslant N$ and there are only finitely many such subgroups. □

Example 6.4.1. There are infinitely many non-normal congruence subgroups with torsion in $SL_2(\mathcal{O}_{d,m})$. The groups $SL_2(\mathcal{O}_{d,mn})$, for $n \in \mathbb{N}$, are an example.

Recall that it is conjectured that $PSL_2(\mathcal{O}_{d,m})$ has a free non-abelian quotient for all values of (d,m) except for $(1,1)$, $(2,1)$, $(3,1)$, $(7,1)$, $(11,1)$, $(19,1)$, $(1,2)$, and $(3,2)$. The normal subgroups of $PSL_2(\mathcal{O}_1)$ were studied in [26] where, in particular, the normal subgroups of index < 60 were classified and it was shown that for a wide collection of n, $PSL_2(\mathcal{O}_1)$ had no normal subgroups of index n. The normal subgroups $PSL_2(\mathcal{O}_3)$ were studied in [1] where the normal subgroups of index < 960 were classified and shown to all be congruence subgroups. We now take a closer look at the others.

6.5 The groups $PSL_2(\mathcal{O}_d)$, $d = 2, 7, 11$ and $PSL_2(\mathcal{O}_{3,2})$ and $PSL_2(\mathcal{O}_{1,2})$

In this section we deal exclusively with $PSL_2(\mathcal{O}_{d,m})$, which we denote by $PSL_2(\mathcal{O}_{d,m})$, or $PSL_2(\mathcal{O}_d)$, if $m = 1$. We look first at the groups $PSL_2(\mathcal{O}_d)$, for $d = 2, 7, 11$. In [25] section 4.5.3, Fine attempts to classify the normal subgroups of $PSL_2(\mathcal{O}_d)$, $d = 2, 7, 11$ but his classification is incomplete. We first of all correct his errors. Recall the following presentations

Theorem. *([25] theorem 4.3.1)*

$$PSL_2(\mathcal{O}_2) =< a, t, u; a^2, (at)^3, (u^{-1}aua)^2, [t, u] >$$

$$PSL_2(\mathcal{O}_7) =< a, t, u; a^2, (at)^3, (u^{-1}auat)^2, [t, u] >$$

$$PSL_2(\mathcal{O}_{11}) =< a, t, u; a^2, (at)^3, (u^{-1}auat)^3, [t, u] >$$

We now state and prove the correct version of Fine's results

Theorem 6.5.1. *Let $N \lhd PSL_2(\mathcal{O}_2)$ be of index n and suppose that $6 \nmid n$. Then if $(n, 6) = 1$*

$$N = N(a, t, u^n)$$

if $2 \mid n$ and $3 \nmid n$ then N is one of

$$N(a, t, u^n), N(at, u^{n/2}), N(at, au^{n/2})$$

if $2 \nmid n$ and $3 \mid n$ then N is one of

$$N(a, t, u^n), N(a, u^{n/3}), N(a, tu^{n/3}), N(a, t^2u^{n/3})$$

Proof. Suppose that $(n, 6) = 1$ so $a = at = u^{-1}aua = 1$, so $a = t = 1$, so $PSL_2(\mathcal{O}_2)/N$ is a factor of $\mathbb{Z}$. So $N = N(a, t, u^n)$. Suppose that $2 \mid n$ and $3 \nmid n$, so $at = 1$, so $PSL_2(\mathcal{O}_2)/N$ is a factor of $< a, u; a^2, au = ua > \cong \mathbb{Z}_2 \times \mathbb{Z}$. So, by (3.4.10), $N = N(a, t, u^n), N(at, u^{n/2}), N(at, au^{n/2})$. Now suppose that $2 \nmid n$ and $3 \mid n$, so $a = u^{-1}aua = 1$, so $PSL_2(\mathcal{O}_2)/N$ is a factor of $< t, u; t^3, tu = ut > \cong \mathbb{Z}_3 \times \mathbb{Z}$. So, by (3.4.10), $N = N(a, t, u^n), N(a, u^{n/3}), N(a, tu^{n/3}), N(a, t^2u^{n/3})$. □

Fine ([25] section 4.5.3) correctly classified the normal subgroups of $PSL_2(\mathcal{O}_2)$ of index coprime to 6, didn't deal with the cases $2 \mid n$ and $3 \nmid n$ or $2 \nmid n$ and $3 \mid n$, and erroneously claimed to have classified the normal subgroups of $PSL_2(\mathcal{O}_2)$ with torsion of index $6k$. As can be seen above we have dealt with the case of a normal subgroup of index not divisible by 6 but the case of an index divisible by 6 is very complicated and we have been unable to deal with it. The complications arise because if $N \lhd PSL_2(\mathcal{O}_2)$ is of index $6k$ and has torsion then $PSL_2(\mathcal{O}_2)/N$ is a factor of $\mathbb{Z} \times PSL_2(\mathbb{Z})$ ([25] theorem 4.5.3).

Lemma. *([25] theorem 4.5.3) If $N \lhd PSL_2(\mathcal{O}_7)$ has torsion then $PSL_2(\mathcal{O}_7)/N$ is a factor of $\mathbb{Z}_2 \times \mathbb{Z}$.*

Theorem 6.5.2. *Let $N \lhd PSL_2(\mathcal{O}_7)$ be of index n. Then if $2 \nmid n$*

$$N = N(a, t, u^n)$$

if $2 \mid n$ and N has torsion then N is one of

$$N(a, t, u^n), N(at, u^{n/2}), N(at, au^{n/2})$$

Proof. Suppose that $2 \nmid n$ so $a, u^{-1}auat \in N$, so $a, t \in N$, so $PSL_2(\mathcal{O}_7)/N$ is a factor of $< u > \cong \mathbb{Z}$. So $N = N(a, t, u^2)$.

Now suppose that $2 \mid n$ and N has torsion, so $PSL_2(\mathcal{O}_7)/N$ is a factor of $\mathbb{Z}_2 \times \mathbb{Z}$ so, by (3.4.10), N is one of

$$N(a, t, u^n), N(at, u^{n/2}), N(at, au^{n/2})$$

□

Missing from Fine's classification were the groups $N(at, au^{n/2})$.

Lemma. *([25] theorem 4.5.3) If $N \lhd PSL_2(\mathcal{O}_{11})$ has torsion then $PSL_2(\mathcal{O}_{11})/N$ is a factor of $\mathbb{Z}_3 \times \mathbb{Z}$.*

Theorem 6.5.3. *Let $N \lhd PSL_2(\mathcal{O}_{11})$ be of index n. Then if $3 \nmid n$ then*

$$N = N(a, t, u^n)$$

if $2 \nmid n$, and $3 \mid n$, or $6 \mid n$ and N has torsion then N is one of

$$N(a, t, u^n), N(a, u^{n/3}), N(a, tu^{n/3}), N(a, t^2u^{n/3})$$

Proof. Suppose that $3 \nmid n$, so $at = u^{-1}auat = 1$, so $a = t = 1$, so $N = N(a, t, u^n)$. Suppose that $2 \nmid n$, and $3 \mid n$, so $a = 1$, so $t^3 = 1$, so $PSL_2(\mathcal{O}_{11})/N$ is a factor of $< t, u; t^3, [t, u] >\cong \mathbb{Z}_3 \times \mathbb{Z}$. Similarly, if $6 \mid n$, and N has torsion, then $PSL_2(\mathcal{O}_{11})/N$ is a factor of $\mathbb{Z}_3 \times \mathbb{Z}$. So that, by (3.4.10), $N = N(a, t, u^n), N(a, u^{n/3}), N(a, tu^{n/3}), N(a, t^2u^{n/3})$. □

Missing from Fine's classification were the groups $N(a, tu^{n/3})$ and $N(a, t^2u^{n/3})$.

6.5.1 Normal congruence subgroups of $PSL_2(\mathcal{O}_2)$

Now consider $\mathcal{O}_2$ and let $\omega = i\sqrt{2}$. By (6.3.3), $\mathcal{O}_2$ has one ideal of index 2, namely $\omega\mathcal{O}_2$ and two ideals of index 3, namely $(1+\omega)\mathcal{O}_2$, and $(1-\omega)\mathcal{O}_2$. Thus, by (6.4.5) and (6.4.6), if $n \in \mathbb{N}$ such that $6 \nmid n$ then

$$\mathcal{N}_2(n) = \begin{cases} 3 & \text{if } n = 2 \\ 4 & \text{if } n = 3 \\ 1 & \text{if } n = 4, 9 \\ 0 & \text{else} \end{cases}$$

and so from (6.5.1) all the normal subgroups of $PSL_2(\mathcal{O}_2)$ of index 2

$$N(a, t, u^2), N(at, u), N(at, au)$$

are congruence subgroups, and all the normal subgroups

$$N(a, t, u^3), N(a, u), N(a, tu), N(a, t^2u)$$

of index 3 are congruence subgroups. Exactly one of the normal subgroups

$$N(a, t, u^4), N(at, u^2), N(at, au^2)$$

of index 4 is a congruence subgroup and exactly one of the normal subgroups

$$N(a, t, u^9), N(a, u^3), N(a, tu^3), N(a, t^2u^3)$$

of index 9 is a congruence subgroup. All other normal subgroups of $PSL_2(\mathcal{O}_2)$ of index not divisible by 6 are non-congruence subgroups.

Lemma 6.5.4.

$$PSL_2(\mathcal{O}_2, \omega\mathcal{O}_2) \leqslant N(at, u)$$

Proof. $PSL_2(\mathcal{O}_2)/PSL_2(\mathcal{O}_2, \omega\mathcal{O}_2) \cong S_3$, so $PSL_2(\mathcal{O}_2)$ has a normal congruence subgroup of index 2. By (6.5.1), the normal subgroups of $PSL_2(\mathcal{O}_2)$ of index 2 are:

$$N(a, t, u^2), N(at, u), N(at, au)$$

Now $u \in PSL_2(\mathcal{O}_2, \omega\mathcal{O}_2)$, so $u \in N$. So, clearly, $N \neq N(a, t, u^2), N(at, au)$. Hence $N = N(at, u)$. □

Lemma 6.5.5.

$$N(a, t, u^4), N(at, au^2)$$

are non-congruence subgroups, and

$$PSL_2(\mathcal{O}_2, 2\mathcal{O}_2) \leqslant N(at, u^2), N(a, t, u^2), N(at, au)$$

Proof. Suppose N is one of these groups. Then $PSL_2(\mathcal{O}_2)/N$ is abelian. Suppose N is a congruence subgroup, so because N is of index 2, or 4 we have $PSL_2(\mathcal{O}_2, 2\mathcal{O}_2) \leqslant N$. Now $(PSL_2(\mathcal{O}_2)/PSL_2(\mathcal{O}_2, 2\mathcal{O}_2))^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Suppose $N = N(a, t, u^4), N(at, au^2)$. Then $PSL_2(\mathcal{O}_2)/N \cong \mathbb{Z}_4$. So N is a non-congruence subgroup. By (6.5.1), the only other normal subgroup of $PSL_2(\mathcal{O}_2)$ of index 4 is $N(at, u^2)$. Thus $PSL_2(\mathcal{O}_2, 2\mathcal{O}_2) \leqslant N(at, u^2)$.

Now, by (3.4.10), $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 3 normal subgroups of index 2. By (6.5.1), the normal subgroups of $PSL_2(\mathcal{O}_2)$ of index 2 are

$$N(a, t, u^2), N(at, u), N(at, au)$$

and we have already seen that $PSL_2(\mathcal{O}_2, \omega\mathcal{O}_2) \leqslant N(at, u)$. □

Lemma 6.5.6.

$$PSL_2(\mathcal{O}_2, (1 + \omega)\mathcal{O}_2) \leqslant N(a, tu)$$

Proof. $PSL_2(\mathcal{O}_2)/PSL_2(\mathcal{O}_2, (1+\omega)\mathcal{O}_2) \cong A_4$, and A_4 has a normal subgroup of index 3. By (6.5.1), the normal subgroups of $PSL_2(\mathcal{O}_2)$ of index 3 are:

$$N(a, t, u^3), N(a, u), N(a, tu), N(a, t^2u)$$

Now $tu \in PSL_2(\mathcal{O}_2, (1+\omega)\mathcal{O}_2)$, so $tu \in N$. So, clearly $N \neq N(a, t, u^3), N(a, u)$. Suppose that $N = N(a, t^2u)$. Then $t = t^2uu^{-1}t^{-1} \in N$, so $a, t, u \in N$. Contradiction. Hence $N = N(a, tu)$. □

Lemma 6.5.7.

$$PSL_2(\mathcal{O}_2,(1-\omega)\mathcal{O}_2) \leqslant N(a,t^2u)$$

Proof. $PSL_2(\mathcal{O}_2)/PSL_2(\mathcal{O}_2,(1-\omega)\mathcal{O}_2) \cong A_4$, so, as above, $PSL_2(\mathcal{O}_2)$ has a normal congruence subgroup, N, of index 3. So, by (6.5.1), N is one of

$$N(a,t,u^3), N(a,u), N(a,t^2u)$$

Now $tu^{-1} \in PSL_2(\mathcal{O}_2,(1-\omega)\mathcal{O}_2)$, so $tu^{-1} \in N$. So clearly $N \neq N(a,t,u^3), N(a,u)$. Hence $N = N(a,t^2u)$. □

Lemma 6.5.8.

$$N(a,t,u^9), N(a,tu^3), N(a,t^2u^3)$$

are non-congruence subgroups, and

$$PSL_2(\mathcal{O}_2,3\mathcal{O}_2) \leqslant N(a,u^3), N(a,t,u^3), N(a,u)$$

Proof. Let N be one of these groups and suppose that N is a congruence subgroup. Then because N is of index 3, or 9 we have $PSL_2(\mathcal{O}_2,3\mathcal{O}_2) \leqslant N$. Now if $N = N(a,t,u^9), N(a,tu^3), N(a,t^2u^3)$ then $PSL_2(\mathcal{O}_2)/N \cong \mathbb{Z}_9$, so as $(PSL_2(\mathcal{O}_2)/PSL_2(\mathcal{O}_2,3\mathcal{O}_2))^{ab} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, N is a non-congruence subgroup. The only other normal subgroup of index 9 is $N(a,u^3)$. Hence $PSL_2(\mathcal{O}_2,3\mathcal{O}_2) \leqslant N(a,u^3)$.

Now, by (3.4.10), $\mathbb{Z}_3 \times \mathbb{Z}_3$ has 4 normal subgroups of index 3. By (6.5.1), the normal subgroups of $PSL_2(\mathcal{O}_2)$ of index 3 are

$$N(a,t,u^3), N(a,u), N(a,tu), N(a,t^2u)$$

and we have already seen that $PSL_2(\mathcal{O}_2,(1+\omega)\mathcal{O}_2) \leqslant N(a,tu)$, and $PSL_2(\mathcal{O}_2,(1-\omega)\mathcal{O}_2) \leqslant N(a,t^2u)$. Hence result. □

Hence

Theorem 6.5.9. *The normal congruence subgroups of $PSL_2(\mathcal{O}_2)$ of index not divisible by 6 are precisely:*

Group	*Level*	*Index*	*Abelianization*
$N(at, u)$	ω	2	$\mathbb{Z}_3^2 \times \mathbb{Z}$
$N(a, t, u^2)$	2	2	$\mathbb{Z}_2^3 \times \mathbb{Z}_3 \times \mathbb{Z}$
$N(at, au)$	2	2	$\mathbb{Z}_3 \times \mathbb{Z}$
$N(a, tu)$	$1 + \omega$	3	$\mathbb{Z}_2^3 \times \mathbb{Z}$
$N(a, t^2u)$	$1 - \omega$	3	$\mathbb{Z}_2^2 \times \mathbb{Z}$
$N(a, u)$	3	3	$\mathbb{Z}_2^3 \times \mathbb{Z}$
$N(a, t, u^3)$	3	3	$\mathbb{Z}_2^4 \times \mathbb{Z}_3 \times \mathbb{Z}$
$N(at, u^2)$	2	4	$\mathbb{Z}_3^2 \times \mathbb{Z}$
$N(a, u^3)$	3	9	$\mathbb{Z}_2^7 \times \mathbb{Z}$

Proof. Presentations for each of these groups were found using GAP [24]. These presentations were then abelianized by hand. □

Remark. So we have shown that every subgroup of $PSL_2(\mathcal{O}_2)$ of index 2 is a congruence subgroup and we have an example of a (normal) non-congruence subgroup of $PSL_2(\mathcal{O}_2)$ of index 4. Now $PSL_2(\mathcal{O}_2)/PSL_2(\mathcal{O}_2, \omega\mathcal{O}_2) \cong S_3$ and S_3 has a non-normal subgroup of index 3. Thus $PSL_2(\mathcal{O}_2)$ has a non-normal congruence subgroup of index 3. It is a simple matter to use GAP [24] to show that $PSL_2(\mathcal{O}_2)$ has exactly one non-normal subgroup of index 3. Thus all subgroups of $PSL_2(\mathcal{O}_2)$ of index 3 are congruence subgroups. So the least index of a non-congruence subgroup of $PSL_2(\mathcal{O}_2)$ is 4. This replicates part of Grunewald and Schwermer's theorem ([31] proposition 3.1)

6.5.2 Normal congruence subgroups of $PSL_2(\mathcal{O}_7)$, $PSL_2(\mathcal{O}_{11})$, $PSL_2(\mathcal{O}_{3,2})$, and $PSL_2(\mathcal{O}_{1,2})$

In exactly the same way as we did for $PSL_2(\mathcal{O}_2)$ we can classify Normal congruence subgroups of $PSL_2(\mathcal{O}_7)$, $PSL_2(\mathcal{O}_{11})$, $PSL_2(\mathcal{O}_{3,2})$, and $PSL_2(\mathcal{O}_{1,2})$. However we do have

Lemma 6.5.10. *Let $N \lhd PSL_2(\mathcal{O}_7)$ be of index n. Suppose that $6 \mid n$ and N has torsion. Then N is a non-congruence subgroup.*

Proof. Suppose that N is a congruence subgroup. By (6.5.2) a, or $at \in N$, so by (6.4.1) there is a normal congruence subgroup of $SL_2(\mathcal{O}_7)$ corresponding to N, of order $\mathcal{O}_7$. By applying (5.4.9), (5.3.19) and then (6.4.1) again we see that $PSL_2(\mathcal{O}_7, 2) \leqslant N$. From

(6.5.2) we can see that $PSL_2(\mathcal{O}_7)/N$ is abelian. Now $(PSL_2(\mathcal{O}_7)/PSL_2(\mathcal{O}_7, 2))^{ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so $6 \mid 4$. Contradiction. Hence N is a non-congruence subgroup. □

and in a similar way we can prove

Lemma 6.5.11. *Let $N \lhd PSL_2(\mathcal{O}_{11})$ be of index n. Suppose that $6 \mid n$ and N has torsion. Then N is a non-congruence subgroup.*

Lemma 6.5.12. *Let $N \lhd PSL_2(\mathcal{O}_{1,2})$ be of index n. Suppose that N has torsion and $6 \mid n$. Then N is a non-congruence subgroup.*

So that we get:

Theorem 6.5.13. *The normal congruence subgroups of $PSL_2(\mathcal{O}_7)$ with torsion are precisely:*

Group	*Level*	*Index*	*Abelianization*
$N(at, u)$	ω	2	$\mathbb{Z}_3 \times \mathbb{Z}$
$N(at, au)$	$1 - \omega$	2	$\mathbb{Z}_3 \times \mathbb{Z}$
$N(a, t, u^2)$	2	2	$\mathbb{Z}_2 \times \mathbb{Z}$
$N(at, u^2)$	2	4	$\mathbb{Z}_3^2 \times \mathbb{Z}$

Remark. So we have shown that all subgroups of $PSL_2(\mathcal{O}_7)$ of index 2 are congruence subgroups and we have given an example of a (normal) non-congruence subgroup of index 3 in $PSL_2(\mathcal{O}_7)$. So 3 is the least index of a non-congruence subgroup of $PSL_2(\mathcal{O}_7)$. This replicates a part of Grunewald and Schwermer's theorem ([31] proposition 3.1).

Theorem 6.5.14. *The normal congruence subgroups of $PSL_2(\mathcal{O}_{11})$ with torsion are precisely:*

Group	*Level*	*Index*	*Abelianization*
$N(a, u)$	ω	3	$\mathbb{Z}_2^2 \times \mathbb{Z}$
$N(a, t^2u)$	$1 - \omega$	3	$\mathbb{Z}_2^2 \times \mathbb{Z}$
$N(a, t, u^3)$	3	3	$\mathbb{Z}_3 \times \mathbb{Z}$
$N(a, tu)$	3	3	$\mathbb{Z}_2^2 \times \mathbb{Z}$
$N(a, u^3)$	3	9	$\mathbb{Z}_2^6 \times \mathbb{Z}$

Remark. As stated earlier the unique subgroup of $PSL_2(\mathcal{O}_{11})$ of index 2 is a non-congruence subgroup so clearly 2 is the least index of a non-congruence subgroup. Again this replicates a part of Grunewald and Schwermer's theorem ([31] proposition 3.1).

Theorem 6.5.15. *The normal congruence subgroups of $PSL_2(\mathcal{O}_{3,2})$ of index not divisible by* 6 *are precisely:*

Group	*Level*	*Index*	*Abelianization*
$N(at, aw)$	$\mathfrak{m}_2$	2	$\mathbb{Z}_3^2 \times \mathbb{Z}$
$N(a, t, w^2)$	2	2	$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}$
$N(at, w)$	2	2	$\mathbb{Z}_3^2 \times \mathbb{Z}$
$N(a, tw)$	$\mathfrak{m}_3$	3	$\mathbb{Z}_2 \times \mathbb{Z}$
$N(at, w^2)$	2	4	$\mathbb{Z}_3^3 \times \mathbb{Z}$

where $\mathfrak{m}_2 = (2, 1+i\sqrt{3})$ *is the ideal of index* 2 *in* $\mathcal{O}_{3,2}$, *and* $\mathfrak{m}_3 = (3, 2+2i\sqrt{3})$ *is the ideal of index* 3 *in* $\mathcal{O}_{3,2}$.

Remark. So we have shown that every subgroup of $PSL_2(\mathcal{O}_{3,2})$ of index 2 is a congruence subgroup and we have given an example of a (normal) non-congruence subgroup of index 3 in $PSL_2(\mathcal{O}_{3,2})$. So 3 is the least index of a non-congruence subgroup of $PSL_2(\mathcal{O}_{3,2})$. This is an extension of Grunewald and Schwermer's theorem ([31] proposition 3.1).

Theorem 6.5.16. *The normal congruence subgroups of $PSL_2(\mathcal{O}_{1,2})$ with torsion are precisely*

Group	*Level*	*Index*	*Abelianization*
$N(at, tz, w)$	$\mathfrak{m}_2$	2	$\mathbb{Z}_3 \times \mathbb{Z}^2$
$N(a, t, z, w^2)$	2	2	$\mathbb{Z}_2^4 \times \mathbb{Z}$
$N(at, aw, tz)$	2	2	$\mathbb{Z}^2$
$N(at, tz, w^2)$	2	4	$\mathbb{Z}_3^2 \times \mathbb{Z}$

where $\mathfrak{m}_2 = (2, 2i)$ *is the ideal of index* 2 *in* $\mathcal{O}_{1,2}$.

Remark. So there are exactly three congruence subgroups of index 2 in $PSL_2(\mathcal{O}_{1,2})$. It is a simple matter to use GAP [24] to show that there are exactly 8 subgroups of $PSL_2(\mathcal{O}_{1,2})$ of index 2. So there are exactly 5 non-congruence subgroup of index 2 in $PSL_2(\mathcal{O}_{1,2})$ and 2 is the least index of a non-congruence subgroup of $PSL_2(\mathcal{O}_{1,2})$. This is an extension of Grunewald and Schwermer's theorem ([31] proposition 3.1).

Bibliography

[1] R. G. Alperin. Normal subgroups of $PSL_2(\mathbb{Z}\left[\sqrt{-3}\right])$. *Proc. AMS*, 124(10):2935–2941, 1996.

[2] M. F. Atiyah and I. G. MacDonald. Introduction to commutative algebra. Addison-Wesley Publishing, 1969.

[3] H. Bass. Algebraic K-theory. Benjamin, New York, 1968.

[4] H. Bass, M. Lazard, and J-P. Serre. Sous-groupes d'indice fini dans $SL(n, \mathbb{Z})$. *Bull. AMS*, 70:385–392, 1964.

[5] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for SL_n $(n \geqslant 3)$ and Sp_{2n} $(n \geqslant 2)$. *Publ. I.H.E.S.*, 33:59–137, 1967.

[6] A. F. Beardon. The geometry of discrete groups. Springer-Verlag, 1983.

[7] A. F. Beardon. The geometry of Fuchsian groups. Lecture notes, March 1998. LMS course on Fuchsian groups at The University of Lancaster.

[8] L. Bianchi. Geometrische darstellung der gruppen linearer substitutionen mit ganzen complexen coefficienten nebst anwendungen auf die zahlentheorie. *Math. Ann.*, 38:313–333, 1891.

[9] L. Bianchi. Sui gruppi de sostituzioni lineari con coeficienti appartenenti a corpi quadratici imaginari. *Math. Ann.*, 40:332–412, 1892.

[10] J. Britto. On the construction of non-congruence subgroups. *Acta. Arith.*, 33(

[11] B. Chandler and W. Magnus. The history of combinatorial group theory: A case study in the history of ideas. Springer-Verlag, 1982.

[12] D. E. Cohen. Combinatorial Group Theory: a topological approach. London Math. Soc. Student Text Volume 14, 1989.

[13] H. Cohn. A classical invitation to Algebraic Numbers and Class Fields. Springer-Verlag, 1978.

[14] P. M. Cohn. On the structure of the GL_2 of a ring. *Publ. I.H.E.S.*, 30:5–53, 1966.

[15] P. M. Cohn. A presentation of SL_2 for euclidean imaginary quadratic number fields. *Mathematika*, 15:156–163, 1968.

[16] D. L. Costa. Zero-dimensionality and the GE_2 of polynomial rings. *J. Pure and Applied Algebra*, 50(3):223–229, 1988.

[17] D. L. Costa and G. E. Keller. On the normal subgroups of $SL(2, A)$. *J. Pure and Applied Alg*, 53:201–226, 1988.

[18] D. L. Costa and G. E. Keller. On the normal subgroups of $GL(2, A)$. *J. of Alg.*, 135:395–406, 1990.

[19] R. K. Dennis. The GE_2 property for discrete subrings of $\mathbb{C}$. *Proc. AMS*, 50:77–82, 1975.

[20] I. M. S. Dey. Schreier systems in free products. *Proc. Glasgow Math. Soc.*, 7:61–79, 1965.

[21] J. Dieudonné. La géométrie des groupes classiques. Springer, 1963.

[22] A. Drillick. *The Picard Group*. PhD thesis, New York University, 1971.

[23] J. Elstrodt, F. Grunewald, and J. Mennicke. Groups acting on Hyperbolic space. Springer Monographs in Mathematics,

[24] M. Schönert et al. GAP. RWTH Aachen: Lehrstuhl D für Mathematik, http://www.gap.dcs.st-and.ac.uk/gap.

[25] B. Fine. Algebraic Theory of the Bianchi groups. Marcel Dekker, 1989.

[26] B. Fine and M. Newman. The normal subgroup structure of the Picard group. *Trans. AMS*, 302(2):769–786, 1987.

[27] R. Fricke. Über die substitutionsgruppen welche zu den aus dem Legendreschen Intergralmodul gezogenen Wurzeln gehören. *Math. Annalen*, 28:99–118, 1886.

[28] V. N. Gerasimov. The unit group of free products. *Mat Sb*, 134(1):42–65, 1987.

[29] K. R. Goodearl and P. Menal. Stable range one for rings with many units. *J. Pure and Applied Algebra*, 54(

[30] F. Grunewald, J Mennicke, and L. Vaserstein. On the groups $SL_2(\mathbb{Z}[x])$ and $SL_2(k[x,y])$. *Israel J. Maths*, 86:157–193, 1994.

[31] F. Grunewald and J. Schwermer. On the concept of level for the subgroups of SL_2 over arithmetic rings. Preprint, 1998.

[32] F. J. Grunewald and J. Schwermer. Free non-abelian quotients of SL_2 over orders of imaginary quadratic number fields. *J. of Alg.*, 69:298–304, 1981.

[33] S. K. Gupta and M. P. Murthy. *Suslin's work on linear groups over polynomial rings and Serre problem.* Number 8 in ISI Lecture Notes. MacMillan, 1980.

[34] A. J. Hahn and O.T. O'Meara. The Classical Groups and K-Theory. Springer-Verlag, 1989.

[35] M. Hall. Subgroups of finite index in free groups. *Canad. J. Math.*, 1:187–190, 1949.

[36] D. L. Johnson. Presentations of Groups. London Mathematical Society Lecture Notes Series 22, 1976.

[37] G. A. Jones. Congruence and non-congruence subgroups of the modular group: A survey. In *Proceedings of Groups St. Andrews*, volume 121 of *London Mathematical Society Lecture Notes Series*, pages 223–234. Cambridge University Press, 1985.

[38] S. Katok. Fuchsian groups. University of Chicago Press, 1992.

[39] F. Klein. Zur theorie der elliptischen modulfunctionen. *Math. Annalen*, 17:62–70, 1880.

[40] F. Klein and R. Fricke. Vorlesungen über die Theorie der elliptischen Modulfunctionen. 2 vols, Teubner, Leipzig, 1890, 1892. reprinted by Johnson Reprint, New York, 1965.

[41] M. Kline. Mathematics in Western culture. Penguin Books, 1987.

[42] W. Klingenberg. Lineare gruppen über lokalen ringen. *Amer. J. Math.*, 83:137–153, 1961.

[43] N. H. J. Lacroix. Two dimensional linear groups over local rings. *Canad. J. Math.*, 21:106–135, 1969.

[44] N. H. J. Lacroix and C. Levesque. Sur les sous-groupes normaux de SL_2 sur un anneau local. *Canad. Math. Bull.*, 26(2):209–219, 1983.

[45] A. Lubotzky. Free quotients and the congruence kernel of SL_2. *J. of Alg.*, 77:411–418, 1982.

[46] A. Lubotzky. Counting finite index subgroups. In *Groups St Andrews 1993*, volume 212 of *London Mathematical Society Lecture Notes Series*, pages 368–404. Cambridge University Press, 1995.

[47] A. Lubotzky. Subgroup growth and congruence subgroups. *Invent. Maths*, 119:267–295, 1995.

[48] R. Lyndon and P. Schupp. Combinatorial Group Theory. Springer-Verlag, 1977.

[49] A. M. Macbeath. Groups of homeomorphisms of a simple connected space. *Annals of Mathematics*, 79(3):473–488, 1964.

[50] D. MacHale. Comic Sections: The book of Mathematical jokes, humour, wit and wisdom. Boole Press, Dublin, 1993.

[51] W. Magnus. Noneuclidean tesselations and their groups. Academic Press, 1974.

[52] Yu. I. Manin and A. A. Panchishkin. *Number Theory I*, volume 49 of *Encyclopaedia of Mathematical Sciences*. Springer, 1995.

[53] A. W. Mason. Free quotients of congruence subgroups of SL_2 over a Dedekind ring of arithmetic type contained in a function field. *Math. Proc. Camb. Phil. Soc.*, 101:421–429, 1987.

[54] A. W. Mason. On the GL_2 of a local ring in which 2 is not a unit. *Canad. Math. Bull.*, 30(2):165–176, 1987.

[55] A. W. Mason. Standard subgroups of $GL_2(A)$. *Proc. EMS*, 30:341–349, 1987.

[56] A. W. Mason. Non-standard normal subgroups and non-normal standard subgroups of the Modular group. *Canad. Math. Bull.*, 32(1):109–113, 1989.

[57] A. W. Mason. On GL_2 of a local ring in which 2 is not a unit II. *Comm in Alg*, 17:511–551, 1989.

[58] A. W. Mason. The order and level of a subgroup of GL_2 over a Dedekind domain of arithmetic type. *Proc. Royal Soc. Edin.*, 119A:191–212, 1991.

[59] A. W. Mason. Normal subgroups of level zero of the Bianchi groups. *Bull. London Math. Soc.*, 26:263–267, 1994.

[60] A. W. Mason and R. W. K. Odoni. Non-normal standard subgroups of the Bianchi groups. *Proc. AMS*, 124(3):721–726, 1996.

[61] A. W. Mason, R. W. K. Odoni, and W. W. Stothers. Almost all Bianchi groups have free non-cyclic quotients. *Math. Proc. Camb. Phil. Soc.*, 111(1):1–6, 1992.

[62] A. W. Mason and S. J. Pride. Normal subgroups of prescribed order and zero level of the Modular group and related groups. *J. London Math. Soc.*, 42(2):465–474, 1990.

[63] A. W. Mason and W. W. Stothers. On the subgroups of $GL(n, A)$ which are generated by commutators. *Invent. Math.*, 23:327–346, 1974.

[64] H. Matsumura. Commutative algebra. W. A. Benjamin, Inc., New York, 1970.

[65] D. L. McQuillan. Classification of the normal congruence subgroups of the Modular group. *Amer. J. Math.*, 87:285–296, 1965.

[66] J. Mennicke. Finite factor groups of the unimodular group. *Ann. Math.*, 81:31–37, 1965.

[67] J. Milnor. Hyperbolic geometry: The first 150 years. *Bull. AMS*, 6(1):9–24, 1982.

[68] J. Moody. Groups for Undergraduates. World Scientific Publishing Co., 1994.

[69] P. M. Neumann. The SQ-Universality of some finitely presented groups. *J. Austral. Math. Soc.*, 16:1–6, 1973.

[70] M. Newman. Integral matrices. Academic Press, 1972.

[71] M. Newman. Asymptotic formulas related to free products of cyclic groups. *Math. of Comp.*, 30(136):838–846, 1976.

[72] O. T. O'Meara. Lectures on linear groups. In *Regional Conference Series in Mathematics*, volume 22. American Mathematical Society, 1974.

[73] E. Picard. Sur un groupe de transformations des points de l'espace situé du même côté d'un plan. *Bull. Soc. Math. France*, 12:43–47, 1884.

[74] G. Pick. Über gewisse ganzzahlige lineare Substitutionen welche sich nicht durch algebraische Congruenzen erklären lassen. *Math. Annalen*, 28:119–124, 1886.

[75] A. Pilkington. The $E_2(R)$-normalized subgroups of $GL_2(R)$. *J. of Alg.*, 172:584–611, 1995.

[76] S. J. Pride. The concept of largeness in group theory. In *Word Problems II*, volume 95 of *Studies in Logic and the Foundations of Mathematics*, pages 299–335. North-Holland, 1978.

[77] I. Reiner. Normal subgroups of the unimodular group. *Illinois J. Math.*, 2(

[78] R. Riley. Applications of a computer implementation of Poincaré's theorem on fundamental polyhedra. *Math. of Comp.*, 40(162):607–632, 1983.

[79] J. J. Rotman. The Theory of Groups. Allyn and Bacon, Inc., 1973.

[80] J.-P. Serre. Le problème des groupes de congruence pour SL_2. *Ann. of Math.*, 92:489–527, 1970.

[81] J.-P. Serre. Trees. Springer, Berlin, 1980.

[82] S. Stahl. The Poincaré half-plane. Jones and Bartlett Publishers, 1993.

[83] W. W. Stothers. Level and index in the Modular group. *Proc. Royal Soc. Edin.*, 99A:115–126, 1984.

[84] R. G. Swan. Generators and relations for certain special linear groups. *Adv. in Math.*, 6:1–77, 1971.

[85] L. N. Vaserstein. K_1-theory and the congruence subgroup problem. *Mat Zametki*, 5(English Trans: Math Notes 5 (1969) 141-148.

[86] L. N. Vaserstein. On the normal subgroups of GL_n over a ring. In *Algebraic K-theory, Evanston 1980*, volume 854 of *Lecture Notes in Mathematics*, pages 456–465. Springer-Verlag, 1981.

[87] L. N. Vaserstein. An answer to the question of M. Newman on matrix completion. *Proc. AMS*, 97(

[88] L. N. Vaserstein. Normal subgroups of the general linear groups over Banach algebras. *J. Pure and Applied Algebra*, 41:99–112, 1986.

[89] L. N. Vaserstein. Normal subgroups of the general linear groups over von Neumann regular rings. *Proc. AMS*, 96(2):209–214, 1986.

[90] L. N. Vaserstein. On normal subgroups of GL_2 over rings with many units. *Comp. Math.*, 74:157–164, 1990.

[91] K. Wohlfahrt. An extension of F. Klein's level concept. *Illinois J. Math*, 8:529–535, 1964.

[92] K. Wohlfahrt. Uber einen satz von Dey und die modulgruppe. *Arch. Math.*, 29:455–457, 1977.

[93] R. Zimmert. Zur SL_2 der ganzen Zahlen eines imaginär-quadratischen Zahlkörpers. *Invent. Math.*, 19:73–81, 1973.