Hecke Operators for Non-Congruence Subgroups of Bianchi Groups

I n a u g u r a l - D i s s e r t a t i o n

zur

Erlangung des Doktorgrades der
Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Saeid Hamzeh Zarghani

aus Shiraz, Iran

Düsseldorf, April 2010

Diese Forschung wurde gefördert durch die Deutsche
Forschungsgemeinschaft im Rahmen des Graduiertenkollegs
'Homotopie und Kohomologie' (GRK 1150)

Aus dem Mathematischen Institut
der Heinrich-Heine-Universiät Düsseldorf

Gedruckt mit der Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Heinrich-Heine-Universität Düsseldorf

Referent: Prof. Dr. Wilhelm Singhof
Korreferent: Priv. Doz. Dr. Tobias Finis

Tag der mündlichen Prüfung: 01.07.2010

Contents

Zusammenfassung

Sei $H \leq \Gamma_{-d} = \mathrm{PSL}(2, \mathcal{O}_{-d})$ eine Untergruppe von endlichem Index und d eine quadratfreie natürliche Zahl. Sei H von Level $\mathfrak{a}$, wie in [32] definiert, und sei $\hat{H}$ der Kongruenzabschluß von H. Angenommen $p \in \mathcal{O}_{-d}$ ist eine Primzahl und $\mathfrak{a} + p\mathcal{O}_{-d} = \mathcal{O}_{-d}$. Definiere $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}(2, \mathbb{Q})$. In dieser Arbeit zeigen wir, dass für jeden Γ_{-d}-Modul X und jedes $q \geq 1$, das folgende Diagramm kommutativ ist:

$$\begin{array}{ccc} H^q(H, X) & \xrightarrow{tr_H^{\hat{H}}} & H^q(\hat{H}, X) \\ {\scriptstyle T_g^H}\downarrow & & \downarrow{\scriptstyle T_g^{\hat{H}}} \\ H^q(H, X) & \xleftarrow[res_H^{\hat{H}}]{} & H^q(\hat{H}, X) \end{array}$$

wobei $tr_H^{\hat{H}}$ die Spurabbildung (co-restriction), $res_H^{\hat{H}}$ die Restriktionsabbildung, und T_g^H der der Doppelnebenklasse HgH zugeordnete Hecke-Operator ist. Dies ist eine Verallgemeinerung der Atkin Vermutung, die in einem Spezialfall von Serre (1987) und in Allgemeinen von Berger (1994) bewiesen wurde. Die Vermutung lautet wie folgt: Die Wirkung von Hecke-Operatoren T_p^H auf dem Raum von Spitzeformen $S_k(H)$ von jedem beliebigen Gewicht k, assoziiert zu einer nicht-Kongruenten Untergruppe H von $\mathrm{PSL}(2, \mathbb{Z})$ mit endlichem Index ist dasselbe wie die Wirkung des Hecke-Operators $T_p^{\hat{H}}$ auf $S_k(\hat{H})$, wobei $\hat{H}$ der Kongruenzabschluß von H ist. Dass heißt, dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} S_k(H) & \xrightarrow{Tr_H^{\hat{H}}} & S_k(\hat{H}) \\ {\scriptstyle T_p^H}\downarrow & & \downarrow{\scriptstyle T_p^{\hat{H}}} \\ S_k(H) & \xleftarrow[incl.]{} & S_k(\hat{H}) \end{array}$$

Abstract

Consider a finite index subgroup $H \leq \Gamma_{-d} = \mathrm{PSL}(2, \mathcal{O}_{-d})$, d any square-free natural number. Let H be of level $\mathfrak{a}$, in the sense of [32], and $\hat{H}$ its congruence closure. Suppose that $p \in \mathcal{O}_{-d}$ is prime and $\mathfrak{a} + p\mathcal{O}_{-d} = \mathcal{O}_{-d}$. Define $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}(2, \mathbb{C})$. In this work, we show that for every Γ_{-d}-module X and every $q \geq 1$ the following diagram commutes:

$$\begin{array}{ccc} H^q(H, X) & \xrightarrow{tr_H^{\hat{H}}} & H^q(\hat{H}, X) \\ \Big\downarrow{\scriptstyle T_g^H} & & \Big\downarrow{\scriptstyle T_g^{\hat{H}}} \\ H^q(H, X) & \xleftarrow[res_H^{\hat{H}}]{} & H^q(\hat{H}, X) \end{array}$$

where tr denotes the trace (co-restriction) map, res denotes the restriction map, and T_g^H is the Hecke operator associated to the double coset HgH. This is a generalization of the Atkin's conjecture (now a theorem, first confirmed in a special case by Serre in 1987 and finally proved in general by Berger in 1994): the action of the Hecke operators T_p^H on the space of the cusp forms $S_k(H)$ of any given weight k associated to a non-congruence finite index subgroup $H \leq \mathrm{PSL}(2, \mathbb{Z})$ is essentially the same as the action of the Hecke operators $T_p^{\hat{H}}$ on $S_k(\hat{H})$, where $\hat{H}$ is the congruence closure of H. More precisely, $T_p^H = T_p^{\hat{H}} \circ Tr_H^{\hat{H}}$, where Tr is the trace map between the space of modular forms. That is, the following diagram commutes:

$$\begin{array}{ccc} S_k(H) & \xrightarrow{Tr_H^{\hat{H}}} & S_k(\hat{H}) \\ \Big\downarrow{\scriptstyle T_p^H} & & \Big\downarrow{\scriptstyle T_p^{\hat{H}}} \\ S_k(H) & \xleftarrow[incl.]{} & S_k(\hat{H}) \end{array}$$

Introduction

This thesis provides a first step in the exploration of arithmetic aspects of non-congruence subgroups of Bianchi groups.

Why are non-congruence subgroups important? One simple answer is given by a classical theorem of Belyi: any smooth projective curve defined over a number field is isomorphic to a modular curve for some finite index subgroup of $\mathrm{SL}(2, Z)$. The majority of these groups are non-congruence. While this is a good enough motivation to study non-congruence subgroups, there are other reasons which are more arithmetic in nature.

The first considerations of the arithmetic aspects of non-congruence subgroups came from Atkin who conjectured that Hecke theory on a non-congruence subgroup of $\mathrm{SL}(2, Z)$ was essentially given by the Hecke theory on its congruence closure (see below). This conjecture was proven to be true by Serre, Thompson and later Berger.

While this gives the impression that non-congruence subgroups are arithmetically insignificant, the experimental work of Atkin and Swinnerton-Dyer claims that there is more behind it. They made a series of conjectures about congruences between the Fourier coefficients of modular forms for congruence and non-congruence subgroups of $\mathrm{SL}(2, Z)$. Today there is significant progress towards the establishment of these congruences, especially by Li, Long and Atkin. A major input to this progress came from the fundamental paper of Scholl which attached Galois representations to modular forms for non-congruence subgroups which are simultaneous eigenvectors under the action of the Hecke operators, see [57].

The efforts of Serre, Bass, Lazard, Mennicke and Milnor show that among the groups $\mathrm{SL}(n, R)$, where $n \geq 2$ and R is the ring of integers of a number field K, the only ones that do have non-congruence subgroups are $\mathrm{SL}(2, Z)$ and Bianchi groups, that is, $\mathrm{SL}(2, \mathcal{O})$ with $\mathcal{O}$ the ring of integers of an imaginary quadratic number field. Thus besides $\mathrm{SL}(2, Z)$, it is only natural to investigate the arithmetic of non-congruence subgroups of Bianchi groups (for a good expository reference for these topics, see [46]). In this thesis, we establish the analog of the conjecture of Atkin on the Hecke theory. Let us be more precise now.

For every finite index subgroup H of $\mathrm{PSL}(2, \mathbb{Z})$ ($H \leq_f \mathrm{PSL}(2, \mathbb{Z})$ for short) and every $k, p \in \mathbb{N}$, p prime, let $S_k(H)$ denote the space of the H-cusp forms of weight k and recall that the Hecke operator $T_p^G : S_k(H) \to S_k(H)$ is defined

by

$$T_p^H(f) := \sum_i (f \mid_k \tilde{p}) \mid_k g_i,$$

where $\tilde{p} := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $H = \bigsqcup_i H_p g_i$, and $H_p := H \cap \tilde{p}^{-1} H \tilde{p}$. A conjecture of Atkin (now a theorem, first confirmed in a special case by Serre in 1987 and finally proved in general by Berger in 1994) states that the action of the Hecke operators T_p^H on the space of the cusp forms of any given weight k associated to a non-congruence subgroup $H \leq \mathrm{PSL}(2,\mathbb{Z})$ is closely related to the action of the Hecke operators $T_p^{\hat{H}}$ on $S_k(\tilde{H})$, where $\tilde{H}$ is the congruence closure of H. More precisely,

Theorem. For allmost all prime numbers p, we have $T_p^H = T_p^{\hat{H}} \circ Tr_H^{\hat{H}}$, where Tr is the trace map. That is, the following diagram commutes:

$$\begin{array}{ccc} S_k(H) & \xrightarrow{Tr_H^{\hat{H}}} & S_k(\hat{H}) \\ {\scriptstyle T_p^H}\downarrow & & \downarrow{\scriptstyle T_p^{\hat{H}}} \\ S_k(H) & \xleftarrow[incl.]{} & S_k(\hat{H}) \end{array}$$

Keeping this in mind, and recalling that

1. by the Eichler–Shimura theorem, $S_k(H)$ can be viewed as a subspace of $H^1(H, X_k)$, the first cohomology group of G with coefficients in a certain H-module X_k, and

2. Hecke operators act on the cohomology groups too,

one comes naturally to the question whether the similar digram commutes for cohomology, i.e. whether some diagram like

$$\begin{array}{ccc} H^1(H, X_k) & \xrightarrow{Tr_H^{\hat{H}}} & H^1(\hat{H}, X_k) \\ {\scriptstyle T_g^H}\downarrow & & \downarrow{\scriptstyle T_g^{\hat{H}}} \\ H^1(H, X_k) & \xleftarrow[res]{} & H^1(\hat{H}, X_k) \end{array}$$

happens to commute? (Here g is a suitable element of $\mathrm{PGL}(2,\mathbb{Q})$.) When it comes to asking questions and playing with ideas, why not be much more idealistic, and go even further, asking whether

$$\begin{array}{ccc} H^q(H,X) & \xrightarrow{Tr_H^{\hat{H}}} & H^q(\hat{H},X) \\ {\scriptstyle T_g^H}\downarrow & & \downarrow{\scriptstyle T_g^{\hat{H}}} \\ H^q(H,X) & \xleftarrow[res]{} & H^q(\hat{H},X) \end{array}$$

commutes, for "all" dimensions q and "all" H-modules X? The answer is in fact, yes, and in this work we are going to show this for all finite index subgroups of the so called Bianchi groups, (i.e. $\mathrm{PSL}(2,\mathcal{O}_{-d})$, where $\mathcal{O}_{-d}$ is the ring of integers of $\mathbb{Q}(\sqrt{-d})$, and d is any square-free natural number), for certain elements g (see below). The main idea, which is a generalization of Berger's idea in [9], is as follows: starting with pure group theory, let G be an arbitrary group, $H \leq_f K \leq G$ and $g \in G$ be such that $[H : H_g] < \infty$, $K = (K_g)H$, (where $K_g := K \cap g^{-1}Kg$) and $[K_g : H_g] = [K : H]^2$. We show that for every G-module X and every $q \geq 1$ the following diagram commutes (see 3.5.6):

$$\begin{array}{ccc} H^q(H,X) & \xrightarrow{tr_H^K} & H^q(K,X) \\ {\scriptstyle T_g^H}\downarrow & & \downarrow{\scriptstyle T_g^K} \\ H^q(H,X) & \xleftarrow[res_H^K]{} & H^q(K,X) \end{array}$$

Now let $H \leq_f \Gamma_{-d} = \mathrm{PSL}(2,\mathcal{O}_{-d})$ be of level $\mathfrak{a}$, and $\hat{H}$ be its congruence closure. Suppose that $p \in \mathcal{O}_{-d}$ is prime and $\mathfrak{a} + p\mathcal{O}_{-d} = \mathcal{O}_{-d}$. Define $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}(2,\mathbb{C})$. We show that H and $\hat{H}$ satisfy the above conditions (see 3.6.8). By the term "level" of H here we mean the (unique) ideal $\mathfrak{a}$ of $\mathcal{O}_{-d}$ which is maximal with the property that the normal closure of $\{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PSL}(2,\mathcal{O}_{-d}) \mid a \in \mathfrak{a}\}$ is included in H (see Chapter 2).

Let us here mention that recently there seem to be an increasing interest in the theory of Bianchi automorphic forms, which can be viewed as cohomology classes of subgroups of Bianchi groups with coefficients in certain modules, see [27] and [35]. Our results can be used to deduce that Hecke action on Bianchi automorphic forms for a non-congruence subgroup of $\mathrm{PSL}(2,\mathcal{O}_{-d})$ is essentially the same as the Hecke action on Bianchi automorphic forms for the congruence closure of the subgroup.

This work consists of three chapters:

Chapter 1

It is a brief review of basic definitions and facts about algebraic number fields. We fix some notations and list some easy properties and formulas for later quick

references. Then we come to the number theoretic aspects of algebraic number fields, for example, asking what happens to an integer prime when considered as an element of an algebraic number field. We, however, do not follow the "standard" route of algebraic number theory, defining ramified and inert ideals etc. Instead, we choose a more elementary approach, using ideas of [22]. This chapter continues by recalling some facts about valued fields and places, which will be used in chapter 2.

Chapter 2

This chapter has two goals: first, to create a basic (algebraic) picture of Euclidean Bianchi groups and congruence subgroups, without going through details. We list some presentations of Euclidean Bianchi groups and cite some results about their finite, normal, and abelian subgroups separately to give some ideas of their nature. Then we recall that the congruence subgroups are the most obvious normal subgroups of finite index in Bianchi groups and mention the congruence subgroup property, CSP. We cite an extended notion of level which will be an important notion for our work. We introduce notations for this kind of level and for the notion of congruence hull or closure, and discover some elementary properties of them. We prove, for example, the following (2.3.12)

Proposition. Let H be a subgroup of $G = \mathrm{PSL}(2, R)$, where R is any commutative ring with unit. If H has finite index in G and $char(R) \nmid [G : H_G]$, then $\mathfrak{a}_H$ is non-zero.

The second goal is to prove the CSP for $\mathrm{PSL}(2, \mathcal{O}_{-d}[1/p])$ and showing that for any ideal $I \lhd \mathcal{O}_{-d}$ and for certain elements $g \in \mathrm{PGL}(2, \mathbb{Q}(\sqrt{-d}))$, the amalgamated product $\Gamma(I) *_{\Gamma(I)\cap\Gamma(I)^g} \Gamma(I)^g$ is isomorphic to a finite index subgroup of $PSL(2, \mathcal{O}_{-d}[1/p])$ (2.6.8). This will be used in chapter 3 in order to show that H and its congruence closure $\hat{H}$ satisfy the conditions of the aforementioned pure group theoretic result (see above). At the end of this chapter, we present some computer-aided examples of computing levels of subgroups of $\mathrm{PSL}(2, \mathcal{O}_{-1})$ and $\mathrm{PSL}(2, \mathcal{O}_{-7})$. We see here examples of congruence subgroups which are link complement groups, that is, isomorphic to the fundamental group of the complement in S^3 of some link.

Chapter 3

In this chapter we prove our generalization of Atkin's conjecture. We start by a very short overview of modular forms and Hecke operators in order to discuss Atkin's conjecture. Then we fix our notations for group cohomology and the ac-

tion of double cosets (Hecke algebra) on it. At this point we are able to prove the aforementioned "pure group theoretic soul" of our generalized Atkin's conjecture (3.5.6). This, together with many small results of chapters 1 and 2, leads us to the main result of chapter 3, theorem 3.6.8.

Acknowledgment

First of all, I would like to thank Professor Fritz Grunewald. His support enabled me to start my Ph.D. in Germany. Before the first draft of this work was completed, Professor Grunewald tragically passed away. I dedicate this work to his memory with gratitude and love.

I am also grateful to Professor Wilhelm Singhof for being so kind and helping me complete my Ph.D and to Priv. Doz. Dr. Tobias Finis for serving as the second examiner of this thesis.

During the last three years I was supported by the Graduiertenkolleg 1150 "Homotopie und Kohomologie". I appreciate by the organizers of the GRK 1150.

I would like to express my warmest thanks to Professor Robert Wisbauer, who made it possible for me to come to Germany to continue my studies and I have been grateful to him for his continuous support and helping me in all aspects of my life.Throughout my study, his advice, guidance, and understanding were irreplaceable for my progress. He always listened patiently to me when I had questions or difficulties and alway helped me.

My special thanks to my wife Zahra for her understanding, encouragement and love. Without her help the completion of this work and my studies were not possible at all. Living so far from parents and friends has been always difficult for her, and because of my concentration on Mathematics, she was most of the time alone. Despite of all these, she always provided me with so much love and support.

I am grateful to Professor Oleg Bogopolski for several helpful group theoretic discussions. He listened patiently to me when I was developing the ideas of the main theorem (3.6.8) of this work.

Dr. Saeid Bagheri and his family were always helped me kindly during last years. My warmest thanks to them.

Further, I thank my friend Dr. Haluk Sengun for proof-reading this thesis. His helpful suggestions and comments made my work more complete, readable and understandable. My great thanks to him for all the helpful discussions.

I would like to thank my friends and colleagues Daniel Appel, Dr. Rubén J. Sánchez-García, Dr. Ferit Deniz, Christian Axler and Christian Löffelsend for all the mathematical and non-mathematica discussions and their helpful sugges-tions.

1 Algebraic Number Fields

Any finite extension of the field of rational numbers is called an algebraic number field. In this chapter we study algebraic number fields, as they play a key role in the construction of Bianchi groups, which are fundamental objects for our work in this thesis. In section 1 we fix some basic notations and definitions concerning algebraic number fields and review some facts about the number theory of $\mathbb{Q}[\sqrt{-d}]$. In section 2 we review briefly valued fields and recall some facts about places of a number field.

1.1 Background constructions

Any subfield K of $\mathbb{C}$ which is finite dimensional over $\mathbb{Q}$ is called an **algebraic number field**. We denote the **(sub)ring of integers** of K by $\mathcal{O}_K$, that is, $\mathcal{O}_K$ is the ring of algebraic integers in K. An **order** of an algebraic number field K is a subring of $\mathcal{O}_K$ which is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$.

Theorem and Definition 1.1.1. Let K be an algebraic number field with $n = [K:\mathbb{Q}]$. Then we have the following:

1. $\mathcal{O}_K$ is integrally closed.
2. Every non-zero prime ideal of $\mathcal{O}_K$ is maximal (i.e. $\mathcal{O}_K$ has Krull dimension 1).
3. $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, and hence is Noetherian.
4. For every non-zero ideal I of $\mathcal{O}_K$, $\mathcal{O}_K/I$ is finite.
5. $\mathcal{O}_K$ is a Dedekind domain, (see, for example, the comments after lemma 1.2.4 for a definition) and hence has unique prime ideal decomposition.
6. $\mathcal{O}_K^* = (\mathcal{O} - \{0\}, \cdot)$ is a finitely generated abelian group.
7. If L is another number field with $K \subseteq L$, then $\mathcal{O}_L \cap K = \mathcal{O}_K$.

For a proof see, for example [52].

Notation 1.1.2. Let K be an algebraic number field and $x, y \in K$.

1. $\overline{x}$ denotes the complex conjugate of x. Clearly $\overline{xy} = \overline{x}\,\overline{y}$ and $\overline{x+y} = \overline{x} + \overline{y}$.
2. $N(x) := x\overline{x}$ denotes the so called **norm** of x. Clearly $N(xy) = N(x)N(y)$.
3. $x \mid y$ means there exists $q \in K$ with $qx = y$.

Any algebraic number field K of dimension 2 over $\mathbb{Q}$ is called a **quadratic number field**. Let $K = \mathbb{Q}(\alpha)$, where α satisfies some quadratic equation $ax^2 + bx + c = 0$, with $a, b, c \in \mathbb{Z}$. So $\alpha = (-b \pm \sqrt{A})/2a$ with $A = b^2 - 4ac$. Let $A = A_1^2 d$, with d square-free. Then $K = \mathbb{Q}(\sqrt{d})$. Thus we see that every quadratic number field is of the form $\mathbb{Q}(\sqrt{d})$, where d is any square-free integer.

For any natural number m, define $\boldsymbol{\mathcal{O}_{d,m}} := \mathbb{Z} + m\omega\mathbb{Z}$ where

$$\omega := \omega_d := \begin{cases} \sqrt{d} & \text{if } d \not\equiv 3 \bmod 4 \text{ (iff } -d \not\equiv 1 \bmod 4), \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 3 \bmod 4 \text{ (iff } -d \equiv 1 \bmod 4). \end{cases}$$

For simplicity, denote $\mathcal{O}_{d,1}$ by $\boldsymbol{\mathcal{O}_d}$. We also define $\mathcal{O}_1 := \mathbb{Z}$.

It can be shown ([52]) that $\mathcal{O}_d$ is the ring of integers of $\mathbb{Q}(\sqrt{d})$. The rings $\mathcal{O}_{d,m}$ are orders in $\mathcal{O}_d$. We are particularly interested in number fields $\mathcal{O}_{-d}$, $d \in \mathbb{N}$ in this work. From now on, d will be a square-free *natural* number.

Theorem 1.1.3. Let $0 \neq x = a + b\omega \in \mathcal{O}_{-d}, n \in \mathbb{N}$, and denote by $\mathfrak{U}_{-d}$ the set of unit elements of $\mathcal{O}_{-d}$.

1. $x + \overline{x}$ is always an integer. Moreover, $\mathcal{O}_{-d} = \{u \in \mathbb{Q}(\sqrt{-d}) \mid u + \overline{u}, N(u) \in \mathbb{Z}\}$.
2. If $\omega = \sqrt{-d}$ (i.e. if $d \not\equiv 3 \bmod 4$), then
$$\overline{x} = a - b\omega, \text{ and so } N(x) = a^2 + b^2 d \in \mathbb{N}.$$
3. In case $\omega = \sqrt{-d}$, we have $N(x) = n$ if and only if $|b| \leq \sqrt{n/d}$ and $a = \pm\sqrt{n - db^2}$. Moreover, if $-1 \leq a, b \leq 1$ then $N(x) \in \{0, 1, d, d+1\}$.
4. If $\omega = \frac{1+\sqrt{-d}}{2}$ (i.e. if $d \equiv 3 \bmod 4$), then
$$\overline{x} = a + b - b\omega, \text{ and so } N(x) = a^2 + ab + b^2\frac{d+1}{4} \in \mathbb{N},$$
5. In case $\omega = (1 + \sqrt{-d})/2$, we have $N(x) = n$ if and only if $|b| \leq 2\sqrt{n/d}$ and $a = (-b \pm \sqrt{4n - db^2})/2$. Moreover, if $-1 \leq a, b \leq 1$ then $N(x) \in \{0, 1, (d+1)/4, (d+9)/4\}$.

6. $\mathbb{Q}(\sqrt{-d})$ is the field of fractions of $\mathcal{O}_{-d}$.
7. $x \in \mathcal{O}_{-d}$ is invertible if and only if $N(x) = 1$.
8. $\mathfrak{U}_{-1} = \{\pm 1, \pm i\}$, $\mathfrak{U}_{-3} = \{\pm 1, \pm\omega, \pm\omega^2\}$, and $\mathfrak{U}_{-d} = \{\pm 1\}$ for all other d's.

The proof is straightforward. The following facts are well known:

Theorem and Definition 1.1.4. Let R be any integral domain and $x \in R$ be a non-zero non-unit. x is called **prime** if for every $x, y \in R$ with $p \mid xy$, we have either $p \mid x$ or $p \mid y$. x is called **irreducible** if for every $x, y \in R$ with $p = xy$, we have either x or y is a unit element of R. Clearly, every prime element is irreducible. The converse is true if R is a **GCD domain**, that is, an integral domain in which every two non-zero elements have a greatest common divisor (GCD). Equivalently, any two non-zero elements of R have a least common multiple (LCM). An integral domain is a unique factorization domain (UFD) if and only if it is a noetherian GCD domain.

Theorem 1.1.5. The ring $\mathcal{O}_{-d}$ is Euclidean if and only if $d \in \{1, 2, 3, 7, 11\}$.

See [20] for a proof. Recall that every Euclidean domain is a principal ideal domain (PID) and in every PID the GCD of any two non-zero elements can be written in the form of a linear combination of them. Let us look at the following small results, which could simplify some computations in $\mathcal{O}_{-d}$.

Lemma 1.1.6. Let $a, b, e, f, k \in \mathbb{Z}$, $gcd(a, b) = 1$, and $k \neq 0$. Then $e + f\omega \in k(a + b\omega)\mathcal{O}_{-d}$ if and only if

$$\begin{cases} kN(a+b\omega) \mid (a+b)e + bfd',\ af - be & \text{whenever } d \equiv 3 \bmod 4, \\ kN(a+b\omega) \mid ae + bfd,\ af - be & \text{whenever } d \equiv 1 \bmod 4. \end{cases}'$$

where $d' = (d+1)/4$.

Proof. Straightforward. □

Lemma 1.1.7. Let $m \in \mathbb{Z}$, $d \in \{1, 2, 3, 7, 11\}$, and $x \in \mathcal{O}_{-d}$. If $m \mid N(x)$ then $m \mid N(gcd((m, x))$.

Proof. There exists $y, z \in \mathcal{O}_{-d}$ such that $gcd(m, x) = zm + yx$. So

$$N(gcd((m,x)) = N(zm+yx) = (zm+yx)\overline{(zm+yx)} =$$

$$(zm+yx)(\bar{z}m + \overline{yx}) = N(z)m^2 + mz\overline{yx} + yx\bar{z}m + N(y)N(x).$$

As m divides every summand in the left hand side, we infer that $m \mid N(gcd(m, x))$. □

Proposition 1.1.8. Let $d \in \{1,2,3,7,11\}$ and $x \in \mathcal{O}_{-d}$.

1. For every $m \in \mathbb{Z}$, $gcd(m,x) = 1$ if and only if $gcd(m,N(x)) = 1$.
2. x is prime in $\mathcal{O}_{-d}$ if $N(x)$ is a prime number. (For the converse, see for example corollary 1.1.13 and 1.1.16.)
3. For every $p \in \mathbb{N}$ prime with $p \nmid x$ and $p \mid N(x)$, $\delta := gcd(p,x)$ is a prime element in $\mathcal{O}_{-d}$ of norm p.

Proof. 1. Assume $gcd(m,x) = 1$. So $ym + zx = 1$ for some $y,z \in \mathcal{O}_{-d}$, and hence $zx = 1 - ym$ and $N(z)N(x) = N(1-ym) = (1-ym)(1-\overline{y}m) = 1 - (y+\overline{y})m + N(y)m^2$. As $(y+\overline{y})$ and $N(y)$ are integers, this implies that $gcd(m,N(x)) = 1$. Conversely, assume $gcd(m,N(x)) = 1$. So $am + bx\overline{x} = 1$ for some $a,b \in \mathbb{Z}$, implying $gcd(m,x) = 1$.

2. Clear.

3. Write $p = q\delta$ for some $q \in \mathcal{O}_{-d}$. So $p^2 = N(p) = N(q)N(\delta)$. We claim that neither$N(q)$ nor $N(\delta)$ can be equal 1. For if $N(q) = 1$, then q is invertible and hence $p \mid \delta$ which implies $p \mid x$, contradiction. On the other hand, as $p \mid N(x)$, it follows by the above lemma that $p \mid N(\delta)$, so $N(\delta) \neq 1$. Hence $N(\delta) = N(q) = p$. So δ is a prime element of $\mathcal{O}_{-d}$.

□

We are going to state some simple but helpful number theoretic facts about $\mathbb{Q}[\sqrt{-d}]$. What we do here, is just generalizing some results of Dresden and Dymàček, ([22]), which is about $\mathbb{Z}[i]$, to $\mathcal{O}_{-d}$.

Notation 1.1.9. 1. Let d be an odd square-free natural number and $\mathcal{O} := \mathcal{O}_{-d}$.

2. For every $m \in \mathbb{Z}$, $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$.

3. $\mathbb{F}_q$ denotes the finite field with q elements.

Proposition 1.1.10. (Compare to [22], Theorem 1) Let $m \in \mathbb{N}$. Then $\mathcal{O}/m\mathcal{O} \cong \mathbb{Z}_m[\omega]$.

Proof. Define $\pi_m : \mathcal{O} \to \mathbb{Z}_m[\omega]$ by $\pi_m(a+b\omega) := [a] + [b]\omega$ where $[\,]$ shows the equivalence class of integers modulo m. It can be easily seen that this map is a surjective ring homomorphism and $ke(\pi) = m\mathcal{O}$. □

Lemma 1.1.11. For every $m \in \mathbb{N}$, if $\mathbb{Z}_m[\omega]$ is a field, then m is a prime number. Moreover, if $d \equiv 1 \bmod 4$ then m is odd, if $d \equiv 3 \bmod 8$ then $\mathbb{Z}_2[\omega] \cong \mathbb{F}_4$ and if $d \equiv 7 \bmod 8$ then $\mathbb{Z}_2[\omega] \cong \mathbb{F}_2$.

Proof. Assume that $\mathbb{Z}_m[\omega]$ is a field. It is then clear that m is prime. We have

$$(1+\omega)^2 \overset{2}{\equiv} 1+\omega^2 = \begin{cases} 1-d & \text{if } d \equiv 1 \bmod 4, \\ w + \frac{3-d}{4} & \text{if } d \equiv 3 \bmod 4. \end{cases}.$$

If $d \equiv 1 \bmod 4$ and $m = 2$, then $(1+\omega)^2 \overset{2}{\equiv} 0$, contradiction. So in this case $m \neq 2$. Let $d \equiv 3 \bmod 8$. Then $\frac{3-d}{4} \equiv 0 \bmod 2$ and hence $1+\omega^2 \overset{2}{\equiv} \omega$, that is $\omega^2 \overset{2}{\equiv} \omega - 1$, showing that $\mathbb{Z}_2[\omega]$ is a field with 4 elements. Finally, if $d \equiv 7 \bmod 8$, then $\frac{3-d}{4} \equiv 1 \bmod 2$ and hence $\omega^2 \overset{2}{\equiv} \omega$, that is, $\omega \overset{2}{\equiv} 1$, so $\mathbb{Z}_2[\omega]$ is a field with 2 elements. □

Recall that for two integers a, p, with p prime and $p \nmid a$, a is called a **quadratic residue mod** p if the equation $x^2 = a$ is solvable in $\mathbb{Z}_p$. The symbol $\left(\frac{a}{p}\right)$, called the **Legendre symbol**, is defined to be 1 if a is a quadratic residue mod p, -1 otherwise, and 0 if $p \mid a$.

Proposition 1.1.12. Let $2 < p \in \mathbb{N}$ be prime. Then $\mathcal{O}/p\mathcal{O}$ is a field if and only if $\left(\frac{p}{d}\right) = -1$

Proof. By lemma 1.1.10, $\mathcal{O}/p\mathcal{O} \cong \mathbb{Z}_p[\omega]$. Consider the epimorphism $\phi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[\omega]$ defined via $\phi(x) := \omega$. Clearly we have

$$ke(\phi) = \begin{cases} \langle x^2 - x + \frac{d+1}{4} \rangle & \text{if } d \equiv 3 \bmod 4, \\ \langle x^2 + d \rangle & \text{if } d \equiv 1 \bmod 4. \end{cases}.$$

We know that $\mathcal{O}/p\mathcal{O}$ is a field if and only if $ke(\phi)$ is an irreducible ideal. But $x^2 + d$ is an irreducible polynomial over $\mathbb{Z}_p$ if and only if d is not a quadratic residue mod p, in Legendre symbol $\left(\frac{d}{p}\right) = -1$ which is equivalent to $\left(\frac{p}{d}\right) = -1$ by [39], chapter 5, theorem 1. Similarly, $x^2 - x + \frac{d+1}{4}$ is an irreducible polynomial over $\mathbb{Z}_p$ if and only if $\left(\frac{-d}{p}\right) = -1$, (by [39], chapter 5, exercise 3) which is equivalent to $\left(\frac{p}{d}\right) = -1$ by [39], chapter 5, theorem 1. □

Corollary 1.1.13. Let $2 < p \in \mathbb{N}$ be prime. Then p is prime in $\mathcal{O}_{-d}$ if and only if $\left(\frac{p}{d}\right) = -1$.

Proof. Immediate consequence of the above proposition. □

Proposition 1.1.14. for every square-free natural number $d \neq 1, 3$, we have $\mathcal{O}_{-d}/\omega\mathcal{O}_{-d} \cong \mathbb{Z}/\delta\mathbb{Z}$, where

$$\delta = \begin{cases} d & d \equiv 1 \bmod 4, \\ -(d+1)/4 & d \equiv 3 \bmod 4. \end{cases}$$

Proof. Define $f : \mathcal{O}_{-d} \to \mathbb{Z}/\delta\mathbb{Z}$ by $f(a+b\omega) := a \ mod \ \delta$. Clearly f is a ring epimorphism. On the other hand, since $\omega^2 = \omega - \delta$, we have $\omega \mid \delta$, and hence $ke(f) = \omega\mathcal{O}_{-d}$. □

Proposition 1.1.15. ((Compare to [22], Theorem 2) Let $a, b \in \mathbb{Z} - \{0\}$ with $gcd(a,b) = 1$. Then $\mathcal{O}/(a+b\omega)\mathcal{O} \cong \mathbb{Z}_{N(a+b\omega)}$.

Proof. As $gcd(a,b) = 1$, we have $gcd(b, a^2 + b^2 d) = 1$ (useful when $d \equiv 1 \bmod 4$) and $gcd(b, a^2 + ab + b^2(d+1)/4) = 1$ (useful when $d \equiv 3 \bmod 4$), so b is invertible in $\mathbb{Z}_{N(a+b\omega)}$. Define $\phi : \mathcal{O}/(a+b\omega\mathcal{O}) \to \mathbb{Z}_{N(a+b\omega)}$ with $\phi(x+y\omega) := x - ab^{-1}y$. ϕ is clearly an epimorphisms of the additive underlying groups with $a + b\omega \in ke(\phi)$. We have

$$\phi(x+y\omega)\phi(u+z\omega) = (x - ab^{-1}y)(u - ab^{-1}z) =$$

$$(xu - a^2b^{-2}zy) - ab^{-1}(uy + zx),$$

while

$$\phi((x+y\omega)(u+z\omega)) = \phi((xu + yz\omega^2) + (uy+zx)\omega) =$$

$$\begin{cases} (xu - dzy) - ab^{-1}(uy+zx) & \text{if } d \equiv 1 \bmod 4, \\ (xu - zy(d+1)/4) - ab^{-1}(uy + zx + zy) & \text{if } d \equiv 3 \bmod 4. \end{cases}.$$

Now, since

$$a^2b^{-2} \overset{N(a+b\omega)}{\equiv} \begin{cases} -d & \text{if } d \equiv 1 \bmod 4, \\ -(d+1)/4 - ab^{-1} & \text{if } d \equiv 3 \bmod 4. \end{cases}.$$

we see that ϕ is in fact a ring epimorphism. The aim is now to show that $ke(\phi) = (a+b\omega)\mathcal{O}$. Let $\phi(x+y\omega) = 0$, so $x - ab^{-1}y = 0$ in $\mathbb{Z}_{N(a+b\omega)}$, which implies $bx - ay = 0$ in $\mathbb{Z}_{N(a+b\omega)}$. We have the following two cases:

Case (1) $d \equiv 1 \bmod 4$, so $\omega^2 = -d$: Note that $a^2b^{-2} = -d$ in $\mathbb{Z}_{N(a+b\omega)}$. The equality $bx - ay = 0$ in $\mathbb{Z}_{N(a+b\omega)}$ implies that the coefficient of ω is an integer in the right-hand side of the following expression:

$$\frac{x+y\omega}{a+b\omega} = \frac{ax+bdy}{N(a+b\omega)} + \frac{ay-bx}{N(a+b\omega)}\omega.$$

Now multiplying $bx - ay \equiv 0$ by ab^{-1} we get $ax - a^2b^{-2}by = ax - bdy \equiv 0$, that is, the real part of the $(x+y\omega)/(a+b\omega)$ is also an integer. So $x+y\omega \in a+b\omega\mathcal{O}$, hence $ke(\phi) = a+b\omega\mathcal{O}$.

Case (2) $d \equiv 3 \bmod 4$, so $\omega^2 = \omega - (d+1)/4$: Note that $a^2b^{-2} + ab^{-1} = -(d+1)/4$ in $\mathbb{Z}_{N(a+b\omega)}$. The equality $bx - ay = 0$ in $\mathbb{Z}_{N(a+b\omega)}$ implies that

$$\frac{\overline{x+y\omega}}{\overline{a+b\omega}} = \frac{ax+ay+by(d+1)/4}{N(a+b\omega)} + \frac{bx-ay}{N(a+b\omega)}\omega \in \mathcal{O},$$

that is, $x+y\omega \in a+b\omega\mathcal{O}$, and hence $ke(\phi) = a+b\omega\mathcal{O}$. □

Corollary 1.1.16. Let $a, b \in \mathbb{Z} - \{0\}$ with $(a,b) = 1$. Then $a+b\omega$ is prime in $\mathcal{O}_{-d}$ if and only if $N(a+b\omega)$ is prime in $\mathbb{Z}$.

Proposition 1.1.17. ((Compare to [22], Theorem 4) Let a, b, and k be positive integers with $gcd(a,b) = 1$. Putting $x = a+b\omega$, we have

$$\mathcal{O}/kx\mathcal{O} = \{[e+f\omega] \mid \ 0 \le e < kN(x),\ 0 \le f < k\},$$

where $[\ ]$ denotes the equivalence class modulo $kx\mathcal{O}$. So the ring $\mathcal{O}/kx\mathcal{O}$ is of order $N(kx)$ and has characteristic $kN(x)$.

Proof. We first show that the indicated equivalence classes are distinct. Let $u = [e_1+f_1\omega]$, $v = [e_2+f_2\omega]$ be elements of the right hand side set. If $u = v$ then $(e_1-e_2) + (f_1-f_2)\omega \in kx\mathcal{O}$ and by 1.1.6

$$\begin{cases} kN(x) \mid (a+b)(e_1-e_2) + b(f_1-f_2)d',\ a(f_1-f_2) - b(e_1-e_2) & d \equiv 3 \bmod 4, \\ kN(x) \mid a(e_1-e_2) + b(f_1-f_2)d,\ a(f_1-f_2) - b(e_1-e_2) & d \equiv 1 \bmod 4. \end{cases}$$

In the first case, we get

$$k(a^2+ab+b^2d') \mid b((a+b)(e_1-e_2) + b(f_1-f_2)d') + (a+b)(a(f_1-f_2) -$$

$$b(e_1-e_2)) = (f_1-f_2)(a^2+ab+b^2d'),$$

so that $k \mid f_1 - f_2$. Since both f_1 and f_2 are non-negative and smaller than k, $f_1 = f_2$. Thus $kN(x)$ divides both $(a+b)(e_1-e_2)$ and $b(e_1-e_2)$. Because $gcd(a,b) = 1$, we must have $kN(x) \mid e_1 - e_2$, implying that $e_1 = e_2$.

In the second case, we see that

$$kN(x) = k(a^2+b^2d) \mid b(a(e_1-e_2) + b(f_1-f_2)d) + a(a(f_1-f_2) - b(e_1-e_2))$$

$$= (f_1 - f_2)(a^2 + b^2 d),$$

so that $k \mid f_1 - f_2$. The rest of the argument is similar to the previous case.

We now show that any $u = e + f\omega$ falls into one of these equivalence classes. Since a and b are relatively prime, there exist integers s and t such that $aks + bkt = k$.

Let $d \equiv 1 \bmod 4$ and note that $(ak + bk\omega)(-t + s\omega) = k\omega - m$, for some $m \in \mathbb{Z}$. Now dividing f by k, we get $f = f_1 k + r$, for some $f_1, r \in \mathbb{Z}$ with $0 \leq r < f$. Thus $[u] = [e + f_1 k\omega + r\omega] = [(e + f_1 m) + r\omega]$. As $k(a^2 + b^2 d) \in kx\mathcal{O}$, dividing $e' := e + f_1 m$ by $k(a^2 + b^2 d)$ we get $e' = e'_1 k(a^2 + b^2 d) + r'$ for some $e'_1, r' \in \mathbb{Z}$ with $0 \leq r' < k(a^2 + b^2 d)$, so we have $[e' + r\omega] = [r' + r\omega]$, $0 \leq r' < k(a^2 + b^2 d)$, and $0 \leq r < f$ as desired.

Assume next that $d \equiv 3 \bmod 4$ and note that $(ak + bk\omega)(-t - s + s\omega) = k\omega - m$, for some $m \in \mathbb{Z}$. Arguing similarly, we get $[u] = [r' + r\omega]$, $0 \leq r' < k(a^2 + b^2 d)$, and $0 \leq r < f$.

□

Example 1. Let $n \in \mathbb{N}$ and $\mathcal{O} := \mathcal{O}_{-7}$.

1. For $2 \leq n$, there exist $a, b \in \mathbb{Z}$ with b odd and $gcd(a, b) = 1$ such that $\omega^n = 2a + b\omega$.

2. For $3 \leq n$, there exist $a, b \in \mathbb{Z}$, both odd, with $gcd(a, b) = 1$ such that $\omega^n = a + b\omega$.

3. For $2 \leq n$, we have $\mathcal{O}/\omega^n\mathcal{O} \cong \mathbb{Z}/2^n\mathbb{Z}$, and for $3 \leq n$, we have $\mathcal{O}/(1 - \omega)^n\mathcal{O} \cong \mathbb{Z}/2^n\mathbb{Z}$.

Proof. 1. For $n = 2$, it is clear since $\omega^2 = \omega - 2$. Assume the assertion for n. Write $\omega^{n+1} = \omega(2a + b\omega) = -2b + (2a + b)\omega$. Let $ax + by = 1$ for some $x, y \in \mathbb{Z}$. So $1 = (2a + b)x + (y - x)b$, showing $gcd(2a + b, b) = 1$. As $2a + b$ is odd, it follows that $gcd(2a + b, 2b) = 1$.

2. Similar to (1).

3. Immediate from $(1), (2)$ and proposition 1.1.15.

□

The next theorem (from [40]) is a nice way of classifying ideals generated by (integer) prime numbers in $\mathcal{O}_{-d}$:

Theorem 1.1.18. Let d be a square-free natural number and $p \in \mathbb{N}$ be a prime. Then we have the following cases:

1. If p is odd and $p \nmid d$ then

$$p\mathcal{O}_{-d} = \begin{cases} \langle p, n + \sqrt{-d}\rangle\langle p, n - \sqrt{-d}\rangle & \text{if } \left(\frac{-d}{p}\right) = 1, \\ prime & \text{otherwise.} \end{cases}$$

2. If $p \mid d$ then $p\mathcal{O}_{-d} = \langle p, \sqrt{-d}\rangle^2$.

3. If d is odd then

$$2\mathcal{O}_{-d} = \begin{cases} \langle 2, 1 + \sqrt{-d}\rangle^2 & \text{if } -d \equiv 3 \bmod 4, \\ \langle 2, \frac{1+\sqrt{-d}}{2}\rangle\langle 2, \frac{1-\sqrt{-d}}{2}\rangle & \text{if } -d \equiv 1 \bmod 8, \\ prime & \text{if } -d \equiv 5 \bmod 8. \end{cases}$$

Proof. This follows directly from propositions 13.1.3 and 13.1.4, (p. 190) in [39]. □

The following table which lists some information (including all elements of norm $1, 2$ and 3) about the Euclidean $\mathcal{O}_{-d}$'s will be useful for quick references.

Table 1.1:

d	1	2	3	7	11
ω	i	$\sqrt{-2}$	$(1+\sqrt{-3})/2$	$(1+\sqrt{-7})/2$	$(1+\sqrt{-11})/2$
$N(a+b\omega)$	a^2+b^2	a^2+2b^2	a^2+ab+b^2	$a^2+ab+2b^2$	$a^2+ab+3b^2$
Elements of norm 1	$\pm 1, \pm i$	± 1	$\pm 1, \pm\omega, \pm\omega^2$	± 1	± 1
Elements of norm 2	$\pm(1+i)$, $\pm(1-i)$	$\pm\omega$		$\pm\omega$,$\pm(1-\omega)$	
Elements of norm 3		$\pm(1+\omega)$, $\pm(1-\omega)$	$\pm(1+\omega)$, $\pm(2-\omega)$, $\pm(1-2\omega)$		$\pm\omega$,$\pm(1-\omega)$

1.2 Places of a field

With F we will denote a field and with d any square free natural number. Unless otherwise stated, p denotes a prime number and $\mathcal{O} := \mathcal{O}_{-d}$. We also define

$$\mathcal{O}[\frac{1}{p}] := \{a/p^k \mid \ a \in \mathcal{O},\ k \in \mathbb{N} \cup \{0\}\ \}.$$

This section is devoted to fix some notations and terminology and recall some basic facts about valued fields. We need this constructions in the next chapters. For details and proof of the results, see for example [42], chapter 6. We start with the definition of absolute value:

Definition 1.2.1. Let $|\ |: F \to \mathbb{R}^{\geq 0}$ be a map. Consider the following conditions:

1. $|x| = 0$ if and only if $x = 0$ for every $x \in F$.
2. $|xy| = |x||y|$ for every $x, y \in F$.
3. $|x + y| \leq |x| + |y|$ for every $x, y \in F$.
4. $|x + y| \leq max\{|x|, |y|\}$ for every $x, y \in F$.

Condition (3) is called the **triangle inequality** and condition (4) is called the **ultrametric inequality**. The map $|\ |$ is called an **absolute value** or **norm** on F if it satisfies (1), (2), (3) and $(F, |\ |)$ is then said to be a **valued field**. An absolute value is called **non-Archimedean** if it satisfies (4), otherwise, it is called **Archimedean**.

When the ultrametric inequality holds, then $|x+y| = |x|$ whenever $|y| < |x|$. The trivial absolute value on F is defined by $|0| = 0$ and $|x| = 1$ for all $0 \neq x \in F$, which is non-Archimedean. Any absolute value on a field gives rise to a (metric) topology, compatible with the field operations:

Proposition 1.2.2. Let $|\ |$ be an absolute value on a field F. Then the topology on F induced by the associated metric $d(x, y) := |x - y|$ makes F into a topological field.

We state here the notion of discrete valuation, which is closely related to the notion of absolute value.

Definition 1.2.3. A **discrete valuation** on F is a map $v : F \to \mathbb{Z} \cup \{\infty\}$ such that for all $x, y \in F$,

1. $v(x) = \infty$ if and only if $x = 0$.
2. $v(x + y) \geq min\{v(x), v(y)\}$.

3. $v(xy) = v(x)v(y)$.

The **valuation ring** of F is defined as the subring $F_v := \{x \in F \mid v(x) \geq 0\}$. It is a principal ideal domain and F is its field of fractions. The **valuation ideal** of v in F is $P_v := \{x \in F \mid v(x) > 0\}$. It is the unique maximal ideal of F_v and is generated by any element $x \in F$ with $v(x) = 1$. The **residue class field** of v is the field F_v/P_v.

Any discrete value leads to a non-Archimedean absolute value:

Lemma 1.2.4. Let v be a discrete valuation on F. For every $1 < r \in \mathbb{R}$, define $|x|_{v,r} := r^{-v(x)}$ if $0 \neq x \in F$ and $|0|_{v,r} := 0$. Then $|\ |_{v,r}$ is a non-Archimedean absolute value on F.

Now we briefly study Dedekind domains, as there is a close relationship between discrete valuations defined on the field of fractions of a Dedekind domain and its non-zero prime ideals. We will need these facts later, especially in the proof of 2.6.3. So first we recall the necessary basic definitions. Let R be an integral domain, and let F be its field of fractions. A **fractional** ideal of R is a nonzero finitely generated R-submodule of F. A fractional ideal I is contained in R if and only if it is an (*integral*) ideal of R. Recall that a **Dedekind domain** is an integral domain, which is not a field, and all of its fractional ideals are invertible with respect to the submodule multiplication. Equivalently, a Dedekind domain is an integral domain which is not a field, is integrally closed, Noetherian, and has Krull dimension one (i.e. every non-zero prime ideal is maximal). Another equivalent definition is that a Dedekind domain is an integral domain which is not a field, and in which every non-zero proper ideal factors into a product of prime ideals. It can be shown that such a factorization is then necessarily unique up to the order of the factors. Let D be a Dedekind domain, and let F be its field of fractions. For any fractional ideal M of D, there exists some $a \in D$ with $aM \subseteq D$, and then aM is an ideal of D. If M is any nonzero fractional ideal, then we define $M^{-1} := \{x \in F \mid xM \subseteq D\}$ and $M^0 := D$. It is a non-zero fractional ideal, and $MM^{-1} = D$. In particular, we can consider negative powers of ideals of D and we see easily that for every such ideal $I \trianglelefteq D$ and for every $j \in \mathbb{Z}$, $I^{j+1} \subseteq I^j$:

$$\cdots I^2 \subseteq I \subseteq D = I^0 \subseteq I^{-1} \subseteq I^{-2} \subseteq \cdots,$$

and for every $x \in D$, $(Dx)^j = Dx^j$.

Every non-zero fractional ideal M of F is of the form

$$M = \prod_{i=1}^{l} P_i^{k_i},$$

for a suitable set $\{P_1, \cdots, P_l\}$ of distinct non-zero prime ideals of D and for suitable non-zero *integer* exponents k_i. This expansion is unique up to the order of the factors, and every such expression is a fractional ideal. In particular, if $0 \neq x \in F$, then the principal fractional ideal xD has a factorization as above. If P is a non-zero prime ideal of D, we let $\boldsymbol{v_P(x)}$ be the exponent of P in the prime factorization of xD. We also define $v_P(0) = \infty$. Then:

Proposition 1.2.5. The map v_P is a discrete valuation on F, which, in turn, defines a non-Archimedean absolute value $|\ |_{P,r}$ on F (for every $r > 1$). Moreover, the set $S := D - P$ coincides with $\{x \in D \mid v_P(x) = 0\}$ and if the localization $S^{-1}D$ is regarded as a subring of F, then the valuation ring F_{v_P} coincides with $S^{-1}D$ and its valuation ideal coincides with $S^{-1}P$.

The following simple lemma is often useful:

Lemma 1.2.6. Let $P = pD$ be a principal prime ideal of a Dedekind ring D, for some $p \in D$. Then for every $j \in \mathbb{Z}$, $1 < r \in \mathbb{R}$, and $x \in D$ we have:

1. If $v_P(x) = j$, then there exists $z \in D$ such that $x = p^j z$ and $p \nmid z$.
2. x is in P^j if and only if $v_P(x) \geq j$.
3. If x is in P^j but not in P^{j+1}, then $v_P(x) = j$.
4. $v_P(p^j) = j$, and so $|p^j|_{P,r} = r^{-j}$.

Proof. (1) Decompose $xD = P^j P_1^{c_1} \cdots P_n^{c_n}$ with $c_i > 0$, and $P, P_1, \cdots P_n$ distinct non-zero prime ideals. So there is $z \in P_1^{c_1} \cdots P_n^{c_n}$ such that $x = p^j z$. Let $z = pz_1$, $z_1 \in D$. Since D is a Dedekind domain, every non-zero prime ideal of it is maximal. Since $P, P_1, \cdots P_n$ are distinct, we infer that $p \notin P_i$ for every i. Now by maximality of each P_i, there is $t_i \in D$ as well as $p_i \in P_i$ such that $t_i p + p_i = 1$, so

$$1 = (t_i p + p_i)^{c_i} = t_i^{c_i} p^{c_i} + p p_i u + p_i^{c_i},$$

for some $u \in D$. Multiplying these equations together, we get

$$1 = (t_1 p + p_1)^{c_1} \cdots (t_n p + p_n)^{c_n} = gp + p_1^{c_1} \cdots p_n^{c_n},$$

for some $g \in D$. Multiplying by z_1 and noting that $pz_1 = z \in P_1^{c_1} \cdots P_n^{c_n}$, we see that $z_1 \in P_1^{c_1} \cdots P_n^{c_n}$. Hence, $x = p^{j+1} z_1 \in P^{j+1} P_1^{c_1} \cdots P_n^{c_n}$, that is $xD = P^{j+1} P_1^{c_1} \cdots P_n^{c_n}$, contradicting the uniqueness of ideal decomposition in D.

(2) Let $v_P(x) = n$. By part 1, $x = p^n z$ for some $z \in D$ with $p \nmid z$. If $x \in P^j$ and $n < j$, then $p \mid z$, contradiction. The reverse conclusion is clear.

Finally, (3) is an immediate result of part 2 and (4) is clear by part 1. □

The next proposition lists some of the most important properties of this valuation:

Proposition 1.2.7. Let D be a Dedekind domain regarded as a subring of its field of fractions F. Suppose that v is a discrete valuation on F, and the subring F_v of F contains D. Then:

1. $P := D \cap P_v$ is a non-zero prime ideal of D,
2. The associated discrete valuation v_P coincides with v,
3. $PF_v = P_v$,
4. D is dense in F_v and $D/P \cong F_v/P_v$ as fields,
5. P^n is dense in P_v^n for every $n \geq 1$, and
6. $R + P_v^n = F_v$ for every $n \geq 1$.

Two absolute values $|\ |_1$ and $|\ |_2$ on a field F are said to be **equivalent** if there exists a positive real number c such that $|\ |_1 = (|\ |_2)^c$. For example, if v is a discrete valuation on F, then for all $1 < r \in \mathbb{R}$, the absolute values $|\ |_{v,r}$ are equivalent. Equivalent absolute values yield the same topology on F. Every equivalence class of absolute values on a number field F is called a **place** of F. A place is called **Archimedean** or **non-Archimedean** according as the corresponding absolute values are Archimedean or non-Archimedean. Let F be a number field and $\mathcal{O}$ be its ring of integers. We may identify the set of non-Archimedean places of F with the set of non-zero prime ideals of $\mathcal{O}$ in view of 1.2.5 and the following:

Theorem 1.2.8. Let F be a number field and $\mathcal{O}$ be its ring of integers. Then the only discrete valuations of F are the v_P's, for every non-zero prime ideal P of $\mathcal{O}$. Hence, every nontrivial non-Archimedean absolute value on F is equivalent to $|\ |_{P,r}$ for some non-zero prime ideal P of $\mathcal{O}$ (and any $1 < r \in \mathbb{R}$).

Now we turn our attention to the Archimedean places.

Theorem 1.2.9. Let F be a number field with $[F : \mathbb{Q}] = n$, and let there be r_1 distinct field maps of F into $\mathbb{R}$ and r_2 complex conjugate pairs of distinct field maps of F into $\mathbb{C}$. Then

1. $r_1 + 2r_2 = n$.

2. Each such field map f induces an Archimedean absolute value on F by restriction from $\mathbb{R}$ or $\mathbb{C}$ (that is, $|\ | \circ f$, with $|\ |$ being the ordinary absolute value), and the only equivalences are the ones from pairs of field maps related by complex conjugation.

3. The resulting collection of $r_1 + r_2$ absolute values exhausts the Archimedean absolute values on F, up to equivalence.

We specialize the above theorem in the case of our interest, i.e. $\mathbb{Q}(\sqrt{-d})$, and close this section.

Corollary 1.2.10. The number field $\mathbb{Q}(\sqrt{-d})$ (for any square-free natural number d) has only two Archimedean places, (which are equivalent,) corresponding to an embedding $\mathbb{Q}(\sqrt{-d}) \to \mathbb{C}$ and its conjugate.

2 $\mathrm{PSL}(2,\mathbb{C})$ and its discrete subgroups

Let d be a square-free natural number. Consider the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$ and let $\mathcal{O}_{-d}$ be its ring of integers. The groups $\boldsymbol{\Gamma_{-d} := \mathrm{PSL}(2,\mathcal{O}_{-d})} = \mathrm{SL}(2,\mathcal{O}_{-d})/\{\pm I\}$ are called **Bianchi groups** (cf. [10], [11]). This class of groups is of interest in many different areas. In number theory they naturally come up in the study of L-functions and elliptic curves (see for example [18], [29], [28], [30], [34], [10]). In topology, they are important in the study of 3-manifolds, as every torsion-free subgroup $G \leqslant \Gamma_{-d}$ acts properly, discontinuously and freely on $\mathbb{H}$ and $G/\mathbb{H}$ is a noncompact hyperbolic Riemannian 3-manifold. (cf. [65], [66], [31]) Finally they are also interesting in their own group theoretical right (see for example [24],[25]). Bianchi groups can be considered as the generalization of the classical modular group $\Gamma_1 := \mathrm{PSL}(2,\mathbb{Z})$ ([17]). For $d \in \{1,2,3,7,11\}$ the rings $\mathcal{O}_{-d}$ are Euclidean rings and the corresponding Bianchi groups are called ***Euclidean Bianchi groups*** , which have similar properties to the modular group ([24]).

In this chapter, first we overview some basic constructions related to Bianchi groups in section 2.1, then outline some group theoretical properties of (Euclidean) Bianchi groups in section 2.2. Section 2.3 reviews congruence subgroups and the congruence subgroup problem. In section 2.4, we study the congruence closure of a subgroup of Γ_{-d}. In section 2.5 we prove the perfectness of specific quotients of Euclidean Bianchi groups and discover some properties of their congruence subgroups. In section 2.6 we prove the congruence subgroup property for the groups $\mathrm{SL}(2,\mathcal{O}_{-d}[\frac{1}{p}])$, $p \in \mathcal{O}_{-d}$ prime, which will b needed in the next chapter. finally we close this chapter by section 2.7, in which we use computer algebra system GAP to compute the level of some finite index subgroups of $\mathrm{PSL}(2,\mathcal{O}_{-1})$ and $\mathrm{PSL}(2,\mathcal{O}_{-7})$.

2.1 Basic constructions

Let X be a metric space and G a group acting on X . A family $\{M_i \mid i \in I\}$ of subsets of X is called **locally finite** if any compact subset of X meets only finitely many of the M_i's. We say that G acts **properly discontinuously** on X if the set of all G-orbits of X is locally finite. A closed connected subset F of X , with

$int(F) \neq \emptyset$, is a **fundamental domain** for (the action of) G if $GF = X$ and $int(F) \cap g(int(F)) = \emptyset$ for all $1 \neq g \in G$. Fundamental domains are specially useful for finding finite representations of groups.

Definition 2.1.1. A subgroup Γ of $\mathrm{PSL}(2,\mathbb{C})$ is said to be **discrete** if it contains no sequence of matrices converging element-wise to the identity. Discrete subgroups of $\mathrm{PSL}(2,\mathbb{R})$ are called **Fuchsian groups**. For example, $\mathrm{PSL}(2,\mathbb{Z})$ is a Fuchsian group.

Let $\mathbb{H}^2 := \{z \in \mathbb{C} \mid \ Im(z) > 0\}$ (equipped with the **hyperbolic metric** $ds^2 = \frac{dx^2+dy^2}{y}$) be the **Poincaré (upper) half plane**. A function from $\mathbb{H}^2$ to itself which preserves (hyperbolic) distance is called an **isometry**. The group $\mathrm{PSL}(2,\mathbb{R})$ acts on $\mathbb{H}^2$ by **Möbius transformations**, which are isometries:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}.$$

The group of all isometries of $\mathbb{H}^2$ is denoted by $\boldsymbol{Isom(\mathbb{H}^2)}$. This group is generated by $\mathrm{PSL}(2,\mathbb{R})$ together with the map $z \mapsto -\bar{z}$ and we have $[Isom(\mathbb{H}^2) : \mathrm{PSL}(2,\mathbb{R})] = 2$.

Similarly, let $\mathbb{H}^3 := \mathbb{C} \times \mathbb{R}^+$ be the 3-dimensional hyperbolic space with the hyperbolic metric:

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

The group $\mathrm{PSL}(2,\mathbb{C})$ acts on $\mathbb{H}^3$ in the following way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z,r) := \frac{1}{N}((az+b)\overline{(cz+d)} + a\bar{c}r^2, r), \ where\ N := |cz+d|^2 + |c|^2 r^2.$$

Under this action the hyperbolic metric is invariant. Again the group of all isometries of $\mathbb{H}^3$ is denoted by $\boldsymbol{Isom(\mathbb{H}^3)}$. This group is generated by $\mathrm{PSL}(2,\mathbb{C})$ together with the map $(z,r) \mapsto (-\bar{z},r)$ and we have $[Isom(\mathbb{H}^3) : \mathrm{PSL}(2,\mathbb{C})] = 2$. The following proposition shows one of the reasons why discrete subgroups of $\mathrm{PSL}(2,\mathbb{R})$ and $\mathrm{PSL}(2,\mathbb{C})$ (e.g. Bianchi groups) are so interesting.

Proposition 2.1.2. Let G be a non-discrete subgroup of $PSL(2,\mathbb{R})$ (respectively $PSL(2,\mathbb{C})$). Then there is no fundamental domain for the action of G on $\mathbb{H}^2$ (resp. $\mathbb{H}^3$).

Proof. Let $\{g_n\}$ be a sequence in G which converges element-wise to the identity and let F be a fundamental domain for the action of G. Consider an element x of $int(F)$. So $\{g_n x\}$ converges to x. Hence there is $m \in \mathbb{N}$ such that $int(F) \cap g_m(int(F)) \neq \emptyset$, which is impossible. □

There is a systematic way to produce some discrete subgroups of $\mathrm{PSL}(2,\mathbb{C})$: we just need to find a discrete subring A of $\mathbb{C}$ (with 1), then $\mathrm{PSL}(2,A)$ is a discrete subgroup, and, on the other hand, discrete subrings of $\mathbb{C}$ (with 1) are completely known:

Proposition 2.1.3. 1. For every discrete subring A of $\mathbb{C}$ containing the unit element, $\mathrm{PSL}(2,A)$ is a discrete subgroup of $\mathrm{PSL}(2,\mathbb{C})$.

2. The discrete subrings (with unit) of $\mathbb{C}$ are $\mathbb{Z}$ and $\mathcal{O}_{\pm d,m}$ (see previous chapter), where d is a square-free natural number and m is a natural number.

For a proof, see [19].

Notation 2.1.4.

1. $\Gamma_{-d,m} := \mathrm{PSL}(2,\mathcal{O}_{-d,m})$.
2. $\Gamma_{-d} := \mathrm{PSL}(2,\mathcal{O}_{-d})$.
3. $\Gamma_1 := \mathrm{PSL}(2,\mathcal{O}_1) = \mathrm{PSL}(2,\mathbb{Z})$.

This gives us a class of discrete subgroups of $\mathrm{PSL}(2,\mathbb{C})$. The group Γ_1 is known as the **modular group**. The structure of the modular group is well understood. For example it is isomorphic to the free product of the cyclic groups $\mathbb{Z}/2$ and $\mathbb{Z}/3$, and has a presentation $\Gamma_1 =< x,y \mid x^2 = (xy)^3 = 1 >$. Picard was the first one who studied the group $\Gamma_{-1} = \mathrm{PSL}(2,\mathbb{Z}[i])$ in 1883, and this group is known as the **Picard group** ([51], [53]). For a detailed study of the Picard group, see [24] and [23]. The rings $\mathcal{O}_{-d}$ are the rings of integers of the imaginary quadratic number fields $\mathbb{Q}(\sqrt{-d})$ and, as mentioned before, the groups Γ_{-d} are called the Bianchi groups. The rings $\mathcal{O}_{-d,m}$ for $m \in \mathbb{N}$ are orders in $\mathbb{Q}(\sqrt{-d})$ and the groups $\Gamma_{-d,m}$ are of finite index in the Bianchi groups. (See [59] for a comprehensive study of discrete subgroups of $\mathrm{PSL}(2,\mathbb{C})$.)

2.2 Algebraic structure of Euclidean Bianchi groups

Following the work of Bianchi [11] and Humbert [38], Swan [63] indicated fundamental domains for the action of Bianchi groups on the hyperbolic 3-space and used these fundamental domains to find finite presentations for Bianchi groups Γ_{-d} for some small values of d, while a separate purely algebraic method was given by P.M. Cohn [17] for Euclidean Bianchi groups. A computer implementation of Swan's method was given by R. Riley [56]. For a detailed discussion of the algebraic structure of Bianchi groups, look at [25] and [24]. Let us start our study by fixing some presentations for Euclidean Bianchi groups. Then we mention

some facts about their group structure, their finite and finite index subgroups, and their normal and abelian subgroups.

Recall from section 1.1 that the ring $\mathcal{O}_{-d}$ has a $\mathbb{Z}$-basis consisting of 1 and ω, where

$$\omega := \omega_d := \begin{cases} i\sqrt{d} & \text{if } d \neq 3 \bmod 4 \text{ (iff } -d \neq 1 \bmod 4)\,, \\ \frac{1+i\sqrt{d}}{2} & \text{if } d = 3 \bmod 4 \text{ (iff } -d = 1 \bmod 4). \end{cases}$$

Define the following three matrices of $\mathrm{SL}(2,\mathbb{C})$:

$$A := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, C_d := \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}, J := \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$

and let $a, b, c := c_d$ and j be the respective images of A, B, C and J in $\mathrm{PSL}(2,\mathbb{C})$. Let us list a presentation for each of the Euclidean Bianchi groups in the following theorem. We add a presentation of the modular group Γ_1 for later references.

Theorem 2.2.1. The Euclidean Bianchi groups Γ_{-d}, $d \in \{1,2,3,7,11\}$, and the modular group Γ_1 are finitely presented. Moreover, they have the following presentations:

$$\begin{aligned}
\Gamma_1 &=< a, b \mid b^2 = (ab)^3 = 1 >, \\
\Gamma_{-1} &=< a, b, c, j \mid b^2 = (ab)^3 = [a,c] = j^2 = (aj)^2 = (bj)^2 = (cj)^2 = \\
&\quad = (cbj)^3 = 1 >, \\
\Gamma_{-2} &=< a, b, c \mid b^2 = (ab)^3 = [a,c] = (bc^{-1}bc)^2 = 1 >, \\
\Gamma_{-3} &=< a, b, c \mid b^2 = (ab)^3 = [a,c] = (acbc^{-2}b)^2 = (acbc^{-1}b)^3 = \\
&\quad = a^{-2}c^{-1}bcbc^{-1}bc^{-1}bcb = 1 >, \\
\Gamma_{-7} &=< a, b, c \mid b^2 = (ab)^3 = [a,c] = (bac^{-1}bc)^2 = 1 >, \\
\Gamma_{-11} &=< a, b, c \mid b^2 = (ab)^3 = [a,c] = (bac^{-1}bc)^3 = 1 >,
\end{aligned}$$

where $[x,y]$ denotes the commutator $xyx^{-1}y^{-1}$.

For a proof, see [24] and [31].

It should be noted that the groups Γ_{-2}, Γ_{-7}, and Γ_{-11} decompose as non-trivial amalgamated free products , as well as HNN extensions , see [24]. In contrast, Γ_{-3} dose not decompose neither as a non-trivial amalgamated free product nor as an HNN extension. This was proved by Serre [61] and (independently) by Karrass and Solitar [24] in a pure combinatorial way using the presentation of Γ_{-3}. However, Γ_{-3} is *virtually* a non-trivial amalgamated product, i.e. it has a subgroup of finite index which is a non-trivial amalgamated free product (cf. [23] and [59]). The following theorem is from [59], section 3.4:

Theorem 2.2.2. The group $\Gamma_{-3,2} = \mathrm{PSL}(2, \mathcal{O}_{-3,2})$ decomposes as a non-trivial free product with amalgamation and as an HNN extension and we have: $[\Gamma_{-3} : \Gamma_{-3,2}] = 10$.

Next we consider finite subgroups of Euclidean Bianchi groups. The only possible $finite$ subgroups of Γ_{-d} (all d) are $\mathbb{Z}/2$, $\mathbb{Z}/3$, $D_2 := \mathbb{Z}/2 \times \mathbb{Z}/2$, the symmetric group S_3, and the alternating group A_4 [31]. More precisely, we have:

Theorem 2.2.3.

1. Γ_{-1} contains all possible types of finite subgroups.
2. Γ_{-2} contains $\mathbb{Z}/2$, $\mathbb{Z}/3$, D_2, and A_4, but not S_3.
3. Γ_{-3} contains $\mathbb{Z}/2$, $\mathbb{Z}/3$, A_4, and S_3, but not D_2.
4. Γ_{-7} contains only $\mathbb{Z}/2$, $\mathbb{Z}/3$, and S_3.
5. Γ_{-11} contains only $\mathbb{Z}/2$, $\mathbb{Z}/3$, and A_4.
6. The number of conjugacy classes of finite subgroups of Γ_{-d} is finite.

The above theorem gives also some information about torsion-free subgroups of finite index of Γ_{-d}: Let H be such a subgroup. Any finite subgroup K of Γ_{-d} acts freely on the set of cosets Γ_{-d}/H and so $|K|$ divides $[\Gamma_{-d} : H]$. This is just an special case of the following

Proposition 2.2.4. Let H be a finite index torsion-free subgroup of an arbitrary group G. Then the index $[G : H]$ is divisible by the least common multiple (lcm) of the orders of finite subgroups of G.

Let us now briefly analyze normal subgroups of Euclidean Bianchi groups. First of all recall that ([21]) for any natural number $n > 1$ and any field F, the groups $\mathrm{PSL}(n, F)$ are simple except $\mathrm{PSL}(2, \mathbb{F}_2)$ which is isomorphic to the symmetric group S_3 and $\mathrm{PSL}(2, \mathbb{F}_3)$ which is isomorphic to the alternating group A_4 (to see what happens if we replace F with a local (or arbitrary) ring, look at [59]). Not only are Bianchi groups non-simple, but they have plenty of normal subgroups. For example, as a result of the specific HNN decompositions of Γ_{-2}, Γ_{-7}, and Γ_{-11}, these groups have normal subgroups of any given index n [24]. Of course this is in contrast to both the modular group and Γ_{-1} and Γ_{-3}, for which there are significant gaps in the possible indices of normal subgroups, cf. [25]. The following theorem summarizes these facts in a precise way:

Proposition 2.2.5. 1. Γ_{-1} has no normal subgroup of index $3, 8, 12p^k$ (with p prime and $p \neq 2,3,5,11$), $36p^k$ (with p prime and $p \neq 2,3,11,17$), $12p^kq^j$ (with p and q primes satisfying $1 + pt \nmid 12q^j$ for all t and $p, q \neq 2,3,5,11$), and any $n > 12$ with $12 \nmid n$

2. For each $n \in \mathbb{N}$ there exists a normal subgroup of index n in Γ_{-d} for $d \in \{2,7,11\}$

Let us close this section by the following two results from [24] about abelian subgroups of Bianchi groups:

Theorem 2.2.6. The only abelian subgroups of Γ_{-d} (all d) are cyclic, D_2, or free abelian of rank ≤ 2. In particular,

1. Any abelian subgroup of Γ_{-2} or Γ_{-11} is isomorphic to one of $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, D_2.

2. Any abelian subgroup of Γ_{-7} is isomorphic to one of $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$.

Proposition 2.2.7. Every subgroup of finite index of Γ_{-d} (all d) contains a free abelian subgroup of rank 2. Hence, as every subgroup of a free group is free (Nielsen–Schreier theorem), it follows that a subgroup of finite index of Γ_{-d} cannot be free.

2.3 Congruence subgroups

Let $n \in \mathbb{N}$, $n > 1$, and d be a square-free natural number, or zero. Recall our convention that $\mathcal{O}_1 := \mathbb{Z}$ (2.1.4), and define the following subgroups of $\mathrm{SL}(n, \mathcal{O}_{-d})$: Let $\mathfrak{a}$ be a proper non-zero ideal of $\mathcal{O}_{-d}$. Consider the natural homomorphism $res_{\mathfrak{a}} : \mathrm{SL}(n, \mathcal{O}_{-d}) \to \mathrm{SL}(n, \mathcal{O}_{-d}/\mathfrak{a})$ obtained by restriction mod $\mathfrak{a}$. The kernel of $res_{\mathfrak{a}}$ is called the **principal** or **full congruence subgroup** of **level** $\mathfrak{a}$ and is denoted by $\mathrm{SL}(n, \mathcal{O}_{-d}, \mathfrak{a})$. It is a normal subgroup of $\mathrm{SL}(n, \mathcal{O}_{-d})$ of finite index (see 1.1.1). For example:

$$SL(2, \mathcal{O}_{-d}, \mathfrak{a}) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathcal{O}_{-d}) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \ mod\ \mathfrak{a} \right\}.$$

These subgroups are the most obvious finite-index normal subgroups of $\mathrm{SL}(n, \mathcal{O}_{-d})$. Note that $SL(n, \mathcal{O}_{-d}, \mathfrak{a}) = res_{\mathfrak{a}}^{-1}(\{1\})$, so we can generalize this construction by replacing $\{1\}$ with a more general subgroup: If G is any subgroup of $SL(n, \mathcal{O}_{-d}/\mathfrak{a})$, then $res_{\mathfrak{a}}^{-1}(G)$ is a finite-index subgroup of $\mathrm{SL}(n, \mathcal{O}_{-d})$ (containing $SL(n, \mathcal{O}_{-d}, \mathfrak{a})$). It is called a **congruence subgroup**. Equivalently, G is a

congruence subgroup of $\mathrm{SL}(n, \mathcal{O}_{-d})$ if G contains a full congruence subgroup. There is a similar story for PSL: let $\pi : \mathrm{SL}(n, \mathcal{O}_{-d}) \to \mathrm{PSL}(n, \mathcal{O}_{-d})$ be the canonical surjection and $\mathfrak{a} \trianglelefteq \mathcal{O}_{-d}$. Define $\Gamma(n, \mathcal{O}_{-d}, \mathfrak{a}) := \mathrm{PSL}(n, \mathcal{O}_{-d}, \mathfrak{a}) := \pi(\mathrm{SL}(n, \mathcal{O}_{-d}, \mathfrak{a}))$ and call it the principal congruence subgroup of PSL of level $\mathfrak{a}$. Again, a subgroup G of $\mathrm{PSL}(n, \mathcal{O}_{-d})$ is called congruence if G contains a full congruence subgroup. We summarize these and the closely related notion of level of a congruence subgroup in the following definition, in a slightly more general sense:

Definition 2.3.1. Let R be a commutative ring with unit and $\mathfrak{a}$ a non-zero ideal of R.

1. Consider the map $res_{\mathfrak{a}} : \mathrm{SL}(n, R) \to \mathrm{SL}(n, R/\mathfrak{a})$ obtained by restriction mod $\mathfrak{a}$ (see [6] chapter 5 for a detailed study of this map). The kernel of $res_{\mathfrak{a}}$ is called the **principal** or **full congruence subgroup** of **level** $\mathfrak{a}$ and is denoted by $\mathrm{SL}(n, R, \mathfrak{a})$.

2. Let $\pi : \mathrm{SL}(n, R) \to \mathrm{PSL}(n, R)$ be the canonical surjection and define

$$\Gamma(n, R, \mathfrak{a}) := \mathrm{PSL}(n, R, \mathfrak{a}) := \pi(\mathrm{SL}(n, R, \mathfrak{a}))$$

   and call it the **principal congruence subgroup** of PSL of **level** $\mathfrak{a}$. It is a normal subgroup of $\mathrm{PSL}(n, R)$ since π is surjective. It is easy to see that $\Gamma(n, R, \mathfrak{a})$ is just the kernel of the restriction map $res_{\mathfrak{a}} : \mathrm{PSL}(n, R) \to \mathrm{PSL}(n, R/\mathfrak{a})$.

3. A **congruence subgroup** H of $\mathrm{SL}(n, R)$ or $\mathrm{PSL}(n, R)$ is a subgroup which contains a full congruence subgroup $\mathrm{SL}(n, R, \mathfrak{a})$ or $\mathrm{PSL}(n, R, \mathfrak{a})$ respectively, for some *non-zero* ideal $\mathfrak{a}$ of R. If $\mathfrak{a}$ is maximal among the ideals having this property, we say that H is congruence of **level** $\mathfrak{a}$.

In particular, when $R = \mathcal{O}_{-d}$, every congruence subgroup is of finite index (1.1.3). We must be very careful about the difference of being congruence in SL and PSL. The following lemma (from [59], 6.4) shows that there is a simple relation between congruence subgroups in $\mathrm{SL}(n, R)$ and $\mathrm{PSL}(n, R)$ in seme cases.

Lemma 2.3.2. Let N be a subgroup of $\mathrm{SL}(n, R)$. If N is congruence in $\mathrm{SL}(n, R)$ then $\pi(N)$ is congruence in $\mathrm{PSL}(n, R)$. Conversely, If $\pi(N)$ is congruence in $\mathrm{PSL}(n, R)$ and $-I \in N$ then N is congruence in $\mathrm{SL}(n, R)$. In any of these cases, N and $\pi(N)$ have the same level.

Proof. If N is congruence, say $\mathrm{SL}(n, R, \mathfrak{a}) \subseteq N$ for some ideal $\mathfrak{a}$, then

$$\Gamma(n, R, \mathfrak{a}) = \pi(\mathrm{SL}(n, R, \mathfrak{a})) \subseteq \pi(N).$$

Conversely suppose $\Gamma(n,R,\mathfrak{q}) \subseteq \pi(N)$ for some ideal $\mathfrak{q}$. Let $x \in \mathrm{SL}(n,R,\mathfrak{q})$. So $\pi(x) \in \pi(N)$, hence there is $y \in N$ such that $x = y$ or $x = -y$. In the latter case, since $-I \in N$, $x \in N$. So $\mathrm{SL}(n,R,\mathfrak{q}) \subseteq N$. □

In this work we are particularly interested in the case $R = \mathcal{O}_{-d}, n = 2$ and the groups PSL. The following theorem, from [24], allows us to compute the index of a principal congruence subgroup. (Recall that for $d \in \{1,2,3,7,11\}$ the rings $\mathcal{O}_{-d}$ are Euclidean rings ([24]) and so every ideal of $\mathcal{O}_{-d}$ in these cases is principal.)

Proposition 2.3.3. (Newman Formula) Let $d \in \{1,2,3,7,11\}$ and $z \in \mathcal{O}_{-d}$.

1. We have

$$[\Gamma_{-d} : \Gamma(2,\mathcal{O}_{-d},< z >)] = \rho \cdot |z|^3 \cdot \prod\{1 - 1/|p|^2 \mid \ p \textit{ prime},\ p \mid z\},$$

where

$$\rho := \begin{cases} 1 & \text{if } z \mid 2\,, \\ 1/2 & \text{otherwise.} \end{cases}$$

In particular,

2. If $p \in \mathcal{O}_{-d}$ is prime, then for every $n \in \mathbb{N}$,

$$[\Gamma_{-d} : \Gamma(2,\mathcal{O}_{-d},< p^n >)] = \rho \cdot |p|^{3n-2} \cdot (|p|^2 - 1).$$

3. $|z| \mid [\Gamma_{-d} : \Gamma(2,\mathcal{O}_{-d},< z >)]$. Moreover,

4. If $< z > \neq < \omega >$ for $d = 2$ or $< z > \neq < 2 >$ for $d = 7,11$ then $\Gamma(2,\mathcal{O}_{-d},< z >)$ is torsion-free.

Previously the concept of level was only defined for congruence subgroups as we have seen. Following an idea of Fricke this concept was extended to arbitrary subgroups of $\mathrm{SL}(2,\mathbb{Z})$ of finite index by Wohlfahrt [69], [70]. This has been generalized to $\mathrm{PSL}(n,\mathcal{O}_{-d})$ by Grunewald and Schwermer [32]. Generalizing the concept of level of congruence subgroups, we get an effective criterion for deciding whether or not an arbitrary subgroup of Γ_{-d} of finite index is congruence. We use this method in section 2.6 to compute some subgroup's levels in Γ_{-7} and Γ_{-1} and show that they are congruence. Let us start with some terminology and proving some elementary results:

Definition 2.3.4.

1. For a family $\{X_\alpha \mid \alpha \in A\}$ (for some index set A) of subsets of an arbitrary group we define the **join** of this family, denoted by $\bigvee_{\alpha\in A} X_\alpha$, as the subgroup generated by $\bigcup_{\alpha\in A} X_\alpha$.

2. For a subgroup H of an arbitrary group G, we denote the **normal closure** of H in G by H^G. This is the intersection of all normal subgroups of G containing H. As another description, $H^G =< ghg^{-1} \mid g \in G \text{ and } h \in H >$.

3. Suppose $\mathfrak{a}$ is a non-zero ideal of a commutative ring R with unit. We define the subgroup $\boldsymbol{M(\mathfrak{a})}$ of *unipotent* elements of $\mathrm{PSL}(2,R)$ as follows:

$$M(\mathfrak{a}) := \left\{ \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PSL}(2,R) \mid a \in \mathfrak{a} \right\}.$$

   We denote the normal closure of $M(\mathfrak{a})$ in $\mathrm{PSL}(2,R)$ by $\boldsymbol{Q(\mathfrak{a})}$. Clearly $M(0) = Q(0) = 0$ and if R is a local or Euclidean ring then $Q(R) = \mathrm{PSL}(2,R)$ (see [6], 5.9.2and [33], 2.4). Moreover, by [16] theorem 6.1, $Q(\mathcal{O}_{-d}) = \mathrm{PSL}(2,\mathcal{O}_{-d})$ if and only if $d \in \{1,2,3,7,11\}$.

4. For simplicity put $\Gamma(\mathfrak{a}) := \Gamma(2,R,\mathfrak{a})$, when R is clear from the context.

First of all we recall some facts about the normal closure, which we use later.

Proposition 2.3.5. Let H, K, and H_α ($\alpha \in A$ for some index set A) be subgroups of an arbitrary group G with $H \subseteq K$.

1. We have $H^G = [G,H]H$, where $[G,H] =< [g,h] \mid g \in G \text{ and } h \in H >$ is a normal subgroup of G.
2. $H^{N_G(K)} \leq K$. As a result, if $K \trianglelefteq G$ then $H^G \leq K$.
3. $H^K \leq H^G \leq K^G$.
4. $(\bigvee H_\alpha)^G = \bigvee H_\alpha^G$.
5. $(\bigcap H_\alpha)^G \subseteq \bigcap H_\alpha^G$.

Proof.

1. Putting $X := \{[g,h] \mid g \in G \text{ and } h \in H\}$ and $Y := \{ghg^{-1} \mid g \in G \text{ and } h \in H\}$, we see that $[G,H]H = X \bigvee H$ and $Y \subseteq XH \subseteq X \bigvee H$, so $H^G =< Y >\subseteq [G,H]H$. On the other hand $H \subseteq Y$ and $X \subseteq YY$ so $[G,H]H \subseteq< Y >= H^G$.

2. Immediate from the definitions.

3. Easy verification.

4. Clearly $\bigvee H_\alpha^G \subseteq (\bigvee H_\alpha)^G$ (by (3)). To prove the reverse inclusion, first set $T := (\bigvee H_\alpha^G) = \bigvee([G, H_\alpha]H_\alpha)$ (by (1)) and note that since $\bigvee H_\alpha \subseteq T$, we just need to show that $[G, \bigvee H_\alpha] \subseteq T$. We need the following trivial formula:

   For every $g, x, y \in G$, we have

   $$[g, xy] = y^{-1}[ygx, y]y^2 \cdot x[g, x^{-1}]^{-1}y^{-1}x^{-1}.$$

   Now consider a generator $[g, h_1 \cdots h_n]$ of $[G, \bigvee H_\alpha]$, where $h_i \in H_{\alpha_i}$ for some index α_i. We proceed by induction on n: for $n = 1$ there is nothing to be proved. Assume that for every $\beta_1 \cdots \beta_{n-1} \in A$, $[g, x_1 \cdots x_{n-1}] \in T$ for every $x_j \in H_{\beta_j}$. Let $x := h_1 \cdots h_{n-1}$ and write

   $$[g, h_1 \cdots h_n] = [g, xh_n] = h_n^{-1}[h_n gx, h_n]h_n^2 \cdot x[g, x^{-1}]^{-1}h_n^{-1}x^{-1}.$$

   Now $h_n^{-1}[h_n gx, h_n]h_n^2 \in [G, H_{\alpha_n}]H_{\alpha_n} \subseteq T$, and

   $$x[g, x^{-1}]^{-1}h_n^{-1}x^{-1} = x[g, x^{-1}]^{-1}x^{-1} \cdot xh_n^{-1}x^{-1},$$

   which is an element of T as $x[g, x^{-1}]^{-1}x^{-1} \in T$ by the induction assumption and $xh_n^{-1}x^{-1} \in H_{\alpha_n}^G \subseteq T$.

5. Easy verification.

□

In the following two propositions, we give a list of some basic properties of Q, M, and Γ, which will be used throughout this work.

Theorem 2.3.6. ([6], corollary $5.9.2$) If R is a local ring, then for every $I \trianglelefteq R$, $Q(I) = \Gamma(I)$.

Proposition 2.3.7. Let I and J be two proper non-zero ideals of a commutative ring R with unit such that $I \subseteq J$ and $m,\ n \in \mathbb{Z}$. We have

1. $M(I) \subseteq Q(I) \subseteq \Gamma(I)$.

2. $M(I) \subseteq M(J)$, $Q(I) \subseteq Q(J)$, and $\Gamma(I) \subseteq \Gamma(J)$.

3. If $R = \mathcal{O}_{-d}$ and $\omega = \sqrt{-d}$ (i.e. if $d \neq 3 \bmod 4$), then

$$M(< m + n\omega >) =< a^m c^n,\ a^{-nd} c^m >$$

.

4. If $R = \mathcal{O}_{-d}$ and $\omega = \frac{1+\sqrt{-d}}{2}$ (i.e. if $d = 3 \bmod 4$), then

$$M(< m + n\omega >) =< a^m c^n,\ a^{-n(d+1)/4} c^m >$$

.

Proposition 2.3.8. Let I, J, and J_α $(\alpha \in A)$ be ideals of a commutative ring R with unit. Then:

1. $M(\bigcap\{J_\alpha \mid \alpha \in A\}) = \bigcap\{M(J_\alpha) \mid \alpha \in A\}$.
2. $Q(\bigcap\{J_\alpha \mid \alpha \in A\}) \subseteq \bigcap\{Q(J_\alpha) \mid \alpha \in A\}$.
3. $\Gamma(\bigcap\{J_\alpha \mid \alpha \in A\}) \subseteq \bigcap\{\Gamma(J_\alpha) \mid \alpha \in A\}$.
4. $M(\Sigma I_\alpha) = \bigvee M(I_\alpha)$ and $\bigvee \Gamma(I_\alpha) \subseteq \Gamma(\Sigma I_\alpha)$.
5. $Q(\Sigma I_\alpha) = \bigvee Q(I_\alpha)$

Proof. Parts (1) to (4) are easy to verify. For the last one, use 2.3.5 part (4). □

Now we are ready to define the extended version of level, acording to [32]. Consider an arbitrary subgroup H of $\mathrm{PSL}(2, R)$ of finite index. The set $X = \{I \trianglelefteq R \mid\ Q(I) \subseteq H\}$, partially ordered by inclusion, has the maximum $\Sigma X := \Sigma\{I \mid\ I \in X\}$ by 2.3.8.

Definition 2.3.9. Let R be a commutative ring with unit and H be an arbitrary subgroup of $\mathrm{PSL}(2, R)$ of finite index. Then we say that H is a subgroup of **level** $\mathfrak{a}_H$ if $\mathfrak{a}_H = \Sigma\{I \trianglelefteq R \mid\ Q(I) \subseteq H\}$ (equivalently if $\mathfrak{a}_H$ is a maximal element of $\{I \trianglelefteq R \mid I \neq 0,\ Q(I) \subseteq H\}$). Clearly $\mathfrak{a}_{\Gamma(I)} = I$ for every ideal I of R.

Proposition 2.3.10. Let H, K, and H_α $(\alpha \in A)$ be subgroups of $\mathrm{PSL}(2, R)$ of finite index.

1. If $H \leq K$, then $\mathfrak{a}_H \subseteq \mathfrak{a}_K$.
2. For any family H_α of subgroups of Γ_{-d}, $\mathfrak{a}_{\cap H_\alpha} = \cap \mathfrak{a}_{H_\alpha}$.
3. $\mathfrak{a}_{Hg} = \mathfrak{a}_{gH} = \mathfrak{a}_H$ for every $g \in \Gamma_{-d}$. In particular, $\mathfrak{a}_{H_G} = \mathfrak{a}_H$.

4. For any subgroup $N \leq H$ we have $\mathfrak{a}_{N\cap\Gamma(\mathfrak{a}_H)} = \mathfrak{a}_N$.

Proof.

1. By part (5) of 2.3.8 and the definition of level we have $Q(\mathfrak{a}_H + \mathfrak{a}_K) = Q(\mathfrak{a}_H)Q(\mathfrak{a}_K) \leq K$, so $\mathfrak{a}_H + \mathfrak{a}_K = \mathfrak{a}_K$, that is $\mathfrak{a}_H \subseteq \mathfrak{a}_K$.

2. By part (1) $\mathfrak{a}_{\cap H_\alpha} \subseteq \cap\mathfrak{a}_{H_\alpha}$. On the other hand by 2.3.8 part (2), $Q(\cap\mathfrak{a}_{H_\alpha}) \subseteq \cap Q(\mathfrak{a}_{H_\alpha}) \subseteq \cap H_\alpha$, hence the result follows from the definition of level.

3. Note that for every ideal I, $Q(I)$ is a normal subgroup and use part (2).

4. Immediate result of parts (1) and (2).

□

Corollary 2.3.11. The intersection of any family of congruence subgroups H_α, of level $\mathfrak{a}_\alpha$, is congruence if and only if $\bigcap \mathfrak{a}_\alpha$ is non-zero. In this case, $\mathfrak{a}_{\bigcap H_\alpha} = \bigcap \mathfrak{a}_\alpha$.

Proof. If $\bigcap \mathfrak{a}_\alpha$ is non-zero, then clearly $\bigcap H_\alpha$ is congruence. Conversely, suppose that $\bigcap H_\alpha$ is congruence. So $\mathfrak{a}_{\bigcap H_\alpha} \neq 0$ and by 2.3.10 part (2), $\mathfrak{a}_{\bigcap H_\alpha} \subseteq \bigcap \mathfrak{a}_\alpha$. Therefore $\bigcap \mathfrak{a}_\alpha$ is non-zero. The last equality follows from 2.3.10 part (2). □

There are examples of finite index subgroups of $\mathrm{PSL}(2, k[x])$, k a finite field, of level zero, see [48]. For Γ_{-d}, however, the situation is different, as we see in the next proposition and its corollaries:

Proposition 2.3.12. Let H be a subgroup of $G = \mathrm{PSL}(2, R)$, where R is any commutative ring with unit. If H has finite index in G and $char(R) \nmid [G : H_G]$, then $\mathfrak{a}_H$ is non-zero.

Proof. We know that the normal core of H in G, H_G, has finite index in G, say m. So for every $g \in G$, $g^m \in H_G$. This implies that $M(mR) \subseteq H_G$. Since H_G is normal in G, we have by 2.3.5 part (2), $Q(mR) \subseteq H_G$. Since $char(R) \nmid m$, $mR \neq 0$. Hence the level of H is not zero, too. □

Corollary 2.3.13. Let H be a finite index subgroup of $\mathrm{PSL}(2, R)$, where R is a commutative ring with unit such that $char(R) = 0$. Then $\mathfrak{a}_H$ is non-zero.

Corollary 2.3.14. Let H be a finite index subgroup of Γ_{-d}, for any square-free d. Then $\mathfrak{a}_H$ is non-zero.

As an application of the concept of level, we state the following theorem, which, accompanied with relevant computer programs, gives an effective criterion for checking whether a subgroup of Γ_{-d} of finite index is congruence or not, see section 2.7. For a proof, see for example [32].

Theorem 2.3.15. Let H be a subgroup of Γ_{-d} of level $\mathfrak{a}_H$. Then H is a congruence subgroup if and only if $\Gamma(\mathfrak{a}_H) \subseteq H$.

As we have seen, every congruence subgroup is of finite index. It is not obvious at all whether or not the converse is true. Towards the end of the 19th century, the question was raised if there were examples of (normal) subgroups of finite index in the modular group $\mathrm{PSL}(2,\mathbb{Z})$ other than (full) congruence subgroups. Fricke and Klein (cf. [41] page 63) answered the question affirmatively and exhibited such subgroups (see also [47].) So the converse is not true for $\mathrm{PSL}(2,\mathbb{Z})$. In 1964, Bass, Lazard, and Serre ([7]) and independently Mennicke in 1965 ([50]) discovered that $\mathrm{PSL}(2,\mathbb{Z})$ is exceptional. They proved the following:

Theorem 2.3.16. (Bass–Lazard–Serre (1964), Mennicke (1965)).
If $n > 2$, then $\mathrm{PSL}(n,\mathbb{Z})$ satisfies the **congruence subgroup property (CSP)** , that is, every finite–index subgroup of $\mathrm{PSL}(n,\mathbb{Z})$ is a congruence subgroup.

Later, Mennicke and Newmann proved that $\mathrm{PSL}(n,R)$ satisfies the CSP where R is the ring of integers of every *real* number field and $n > 2$. Finally, in 1967, Bass, Milnor, and Serre proved the following: ([8]).

Theorem 2.3.17. (Bass–Milnor–Serre (1967)). For every square–free natural number d and every $n > 2$, the group $\mathrm{PSL}(n,\mathcal{O}_{-d})$ satisfies the CSP.

On the other hand, Serre in 1970 proved the following

Theorem 2.3.18. The group $\mathrm{PSL}(2,\mathcal{O}_{-d})$, d square–free, contains non–congruence subgroups of finite index.

Note that by 2.3.21, it follows that the group $\mathrm{PSL}(2,\mathcal{O}_{-d})$ contains infinitely many non–congruence subgroups of finite index. Finally, if we consider the following definition:

Definition 2.3.19. Define

$$nsc(d) := min\{[\mathrm{SL}(2,\mathcal{O}_{-d}) : G] \mid G \leq_f \mathrm{SL}(2,\mathcal{O}_{-d}) \text{ is non–congruence}\}$$

$$= min\{[\Gamma_{-d} : G] \mid G \leq_f \Gamma_{-d} \text{ is non–congruenc}\}.$$

Then we have $nsc(1) = 5$, $nsc(2) = 4$, $nsc(3) = 22$, $nsc(7) = 3$, and $nsc(d) = 2$ for all other d's ([32]).

We cite now some interesting results about non-congruence subgroups from [12].

Proposition 2.3.20. Let K be a normal subgroup of $\mathrm{SL}(2,\mathcal{O}_{-d})$ (all d) such that $\mathrm{SL}(2,\mathcal{O}_{-d})/K$ is isomorphic to either the symmetric group S_n or to the alternating group A_n for some $n > 6$. Then K is a non-congruence subgroup.

Proposition 2.3.21. If $\mathrm{PSL}(2,\mathcal{O}_{-d})$ (all d) contains a non-congruence subgroup, then it contains infinitely many such subgroups.

Proof. Let G be a non-congruence subgroup. For every non-zero ideal J of $\mathcal{O}_{-d}$, $G \cap \Gamma(J)$ has finite index in $\mathrm{PSL}(2,\mathcal{O}_{-d})$ and is non-congruence. For every $p \in \mathbb{N}$ prime, we have

$$[\mathrm{PSL}(2,\mathcal{O}_{-d}) : G \cap \Gamma(< p >)] =$$

$$[\mathrm{PSL}(2,\mathcal{O}_{-d}) : \Gamma(< p >)][\Gamma(< p >) : G \cap \Gamma(< p >)],$$

so if for infinitely many prime numbers p, $G \cap \Gamma(< p >)$'s are equal to a common subgroup H, then by 2.3.3 part 3, these prime numbers divide the integer $[\mathrm{PSL}(2,\mathcal{O}_{-d}) : H]$, which is impossible. □

2.4 Congruence closure

Let S be a subgroup of $\mathrm{SL}(2,\mathcal{O}_{-d})$. The intersection of all congruence subgroups of $\mathrm{SL}(2,\mathcal{O}_{-d})$ containing S is not necessarily a congruence subgroup, cf. [48]. When this intersection is congruence, (e.g. when S is of finite index, see below) we denote it by $\hat{S}$ and call it the congruence hull or congruence closure of S. By definition $\hat{S} = S$ if and only if S is a congruence subgroup. When it exists, it is the smallest congruence subgroup containing S and so the index $[\hat{S} : S]$ is a measure of the extent to which S deviates from being a congruence subgroup. Although the congruence closure is not defined for every subgroup of $\mathrm{SL}(2,\mathcal{O}_{-d})$, there are plenty of subgroups for which the closure is defined, as we see in the next theorem. For a proof, see [49].

Theorem 2.4.1. Let G be a finitely generated group and d be any square-free natural number or zero. There exists $S \leq \mathrm{SL}(2,\mathcal{O}_{-d})$ for which $\hat{S}$ is defined, $S \trianglelefteq \hat{S}$, and $\hat{S}/S \cong G$.

Let us cite the definition of the congruence closure precisely and study basic properties of the congruence closure.

Notation 2.4.2.

1. $H^g := g^{-1}Hg$ and ${}^gH := gHg^{-1}$, for an element g and a subgroup H of an arbitrary group G.
2. $H_G := \bigcap\{H^g \mid g \in G\}$ is the normal core of H in G.

Definition 2.4.3. Let R be commutative ring with unit and H be a subgroup of $\mathrm{PSL}(2,R)$. We define the **congruence hull** or **closure** of H in $\mathrm{PSL}(2,R)$ as the smallest congruence subgroup of $\mathrm{PSL}(2,R)$ containing H, when it exists, and denote it by $\hat{H}$. In other words,

$$\hat{H} = \bigcap\{K \leq \mathrm{PSL}(2,R) \mid K \textit{ is congruence and } H \subseteq K\}$$

when this intersection is congruence. Note that there always exists a congruence subgroup containing H, e.g. $H\Gamma(I)$ for every non-zero ideal I of R.

Proposition 2.4.4. Let H be a subgroup of $\mathrm{PSL}(2,R)$, with R a commutative ring with unit. If $\mathfrak{a}_H$ is non-zero, then $\hat{H}$ is defined. In particular, if $R = \mathcal{O}_{-d}$ and H is of finite index in Γ_{-d}, then $\hat{H}$ is defined.

Proof. It can be easily seen that $\Gamma(\mathfrak{a}_H)H$ is the smallest congruence subgroup containing H. So $\hat{H} = \Gamma(\mathfrak{a}_H)H$. □

Proposition 2.4.5. Let H, K be subgroups of $\mathrm{PSL}(2,R)$, with R a commutative ring with unit, such that $\hat{H}$ and $\hat{K}$ are defined.

1. For every congruence subgroup N of $\hat{H}$, $\hat{H} = NH$. In particular, $\hat{H} = \Gamma(\mathfrak{a}_H)H$, if $\mathfrak{a}_H$ is non-zero.
2. If $H \subseteq K$ then $\hat{H} \subseteq \hat{K}$.
3. If $\widehat{H \cap K}$ is defined then $\widehat{H \cap K} \subseteq \hat{H} \cap \hat{K}$.
4. If $\mathfrak{a}_H$ is non-zero then $H_G \widehat{\cap \Gamma}(\mathfrak{a}_H) = \Gamma(\mathfrak{a}_H)$.
5. If $\mathfrak{a}_H$ is non-zero, then for every $N \leq H$ with $\mathfrak{a}_N \neq 0$ and $N \widehat{\cap \Gamma}(\mathfrak{a}_H) = \hat{N}$ we have $N \subseteq \Gamma(\mathfrak{a}_H)$.

Proof.

1. NH is a congruence subgroup containing H and included in $\hat{H}$.
2. Immediate from 2.3.10 part (1) and 2.3.7 part (2).

3. Immediate from 2.3.8 part (3) and 2.3.7 part (2).

4. Immediate from 2.3.10 parts (3) and (4).

5. If $N \cap \widehat{\Gamma(\mathfrak{a}_H)}) = \hat{N}$, then by part (1) and 2.3.10 part (4), $\Gamma(\mathfrak{a}_N)N = \Gamma(\mathfrak{a}_N)(N \cap \Gamma(\mathfrak{a}_H))$. On the other hand $\Gamma(\mathfrak{a}_N) \cap N = \Gamma(\mathfrak{a}_N) \cap (N \cap \Gamma(\mathfrak{a}_H))$, whence the result.

□

2.5 The groups $\mathrm{PSL}(2,R)$

In this section, first, we gather some information about perfectness of the groups $\mathrm{PSL}(2,R)$, for a commutative (local) ring R with unit. Next, we apply this information to the Euclidean Bianchi groups and discover some properties of the level of congruence subgroups.

For every field F and every $2 \leq n \in \mathbb{N}$, the groups $\mathrm{SL}(n,F)$ (and hence $\mathrm{PSL}(n,F)$) are perfect, except in the cases $\mathrm{SL}(2,2)$ and $\mathrm{SL}(2,3)$ ([21]). Recall that a group G is said to be **perfect** if $G' = G$, that is, G has no non-trivial abelian quotient. Clearly every quotient of a perfect group is perfect. We are going to show that the group $\mathrm{SL}(2,R)$ is also perfect, for every commutative local ring R. To prove this, we use the **elementary matrices** $X_{ij}(r)$, $i \neq j, r \in R$, whose entries are the same as the 2×2 identity matrix except for the i,j-th entry, which is r. So $X_{ij}(r) \in \mathrm{SL}(2,R)$ for every $r \in R$. Let $E(2,R)$ denote the subgroup of $\mathrm{SL}(2,R)$ generated by all elementary matrices. We have the following lemmas:

Lemma 2.5.1. Let R be a commutative ring with 1 such that R contains an invertible element a with $a^{-1} \neq a$. Then $E(2,R) \leq [\mathrm{SL}(2,R), \mathrm{SL}(2,R)]$.

Proof. Let $r \in R$ and put $r' := (a^2-1)^{-1}r$. Then

$$[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & r' \\ 0 & 1 \end{pmatrix}] = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}.$$

□

Lemma 2.5.2. Let R be a commutative local ring with 1 and maximal ideal $\mathfrak{m}$. Then $E(2,R) = \mathrm{SL}(2,R)$.

Proof. Consider $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,R)$. If all elements of a row of A are in $\mathfrak{m}$, then for every $X \in \mathrm{SL}(2,R)$, all entries of the same row in AX are in $\mathfrak{m}$, so it cannot be the identity matrix. Similarly, not all entries of a column of A are in $\mathfrak{m}$. Now consider the following cases:

1. $c \notin \mathfrak{m}$ so c is invertible. Putting $c' := (1-a)c^{-1}$ we see that

$$X_{21}(-c) \cdot X_{12}(c') \cdot A \cdot X_{12}(-b-c'd) = I_{2\times 2},$$

hence $A \in E(2,R)$.

2. $b \notin \mathfrak{m}$ so b is invertible. Putting $b' := (1-a)b^{-1}$ we see that

$$X_{12}(-b-c'd) \cdot A \cdot X_{12}(b') \cdot X_{21}(-b) = I_{2\times 2},$$

hence $A \in E(2,R)$.

3. $b, c \in \mathfrak{m}$ so in this case we must have $a, d \notin \mathfrak{m}$. First we note that

$$X_{12}(a^{-1}) \cdot \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a & a^{-2} \\ 0 & a^{-1} \end{pmatrix},$$

hence by case 2, $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in E(2,R)$. Now

$$X_{21}(-ac) \cdot \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \cdot A \cdot X_{21}(-a^{-1}b) = I_{2\times 2},$$

showing that $A \in E(2,R)$.

□

Having this information, it is easy to prove the following

Theorem 2.5.3. Let R be a commutative local ring with 1 and maximal ideal $\mathfrak{m}$ such that $|R/\mathfrak{m}| > 3$. Then $\mathrm{SL}(2,R)$ is perfect.

Proof. As the field $R/\mathfrak{m}$ has more than 3 elements, R must contain an element $a \neq 0$ with $a^{-1} \neq a$ invertible and we are done by the above two lemmas. □

We will use the following special case of this theorem:

Corollary 2.5.4. Let R be an integral domain and I be a maximal ideal of it such that R/I has more than 3 elements. Then for every $j \in \mathbb{N}$, the groups $\mathrm{SL}(2, R/I^j)$ (and hence $\mathrm{PSL}(2, R/I^j)$) are perfect.

Proof. The case $j = 1$ is clear because R/I is a field with more than 3 elements. Note that for every $j > 1$, R/I^j is a local ring with maximal ideal I/I^j. On the other hand, $3 < card(R/I) \leq card(R/I^2) \leq card(R/I^3) \leq \cdots$ so by the above theorem we are done. □

Next, we prove a useful property of the principal congruence subgroups. If $I, J \trianglelefteq R$, where R is a commutative ring with unit such that $J^2 \subseteq I$, then the group $\Gamma(2, R/I, I+J/I)$ is abelian and has a fairly simple structure:

Lemma 2.5.5. Let I, J be ideals of a commutative ring R with unit such that $J^2 \subseteq I$. Then $\Gamma(2, R/I, (I+J)/I) \cong ((I+J)/I, +)^3$. In particular, it is an abelian normal subgroup of $\mathrm{PSL}(2, R/I)$.

Proof. Consider $u = \begin{pmatrix} a+I & b+I \\ c+I & d+I \end{pmatrix}$ and $v = \begin{pmatrix} a'+I & b'+I \\ c'+I & d'+I \end{pmatrix}$ in $\Gamma(2, R/I, I+J/I)$. We have

$$uv = \begin{pmatrix} aa' + bc' + I & ab' + bd' + I \\ ca' + dc' + I & cb' + dd' + I \end{pmatrix}.$$

Now note that, since $b, c, b', c' \in I + J$, and $(I+J)^2 \subseteq I + J^2 \subseteq I$, we have $bc', cb' \in I$. On the other hand, $a-1, a'-1, d-1, d'-1 \in I+J$, so that $ab'-b', bd'-b, ca'-c, dc'-c', aa'-a-a'+1, dd'-d-d'+1 \in (I+J)^2 \subseteq I$. Thus

$$uv = \begin{pmatrix} a+a'-1+I & b'+b+I \\ c+c'+I & d+d'-1+I \end{pmatrix} = vu.$$

On the other hand, since $ad - bc - 1 \in I$, we see that $d + I = 2 - a + I$. Hence the map f defined via $f(u) := (a-1+I, b+I, c+I)$ is clearly an isomorphism of abelian groups from $\Gamma(2, R/I, (I+J)/I)$ to $((I+J)/I, +)^3$. □

Let R be an integral domain and $I \trianglelefteq R$. For every $j \in \mathbb{N}$, define:

$$\begin{cases} \epsilon_{j+1} : \mathrm{PSL}(2, R/I^{j+1}) \to \mathrm{PSL}(2, R/I^j) \\ \epsilon_{j+1} \begin{pmatrix} a+I^{j+1} & b+I^{j+1} \\ c+I^{j+1} & d+I^{j+1} \end{pmatrix} := \begin{pmatrix} a+I^j & b+I^j \\ c+I^j & d+I^j \end{pmatrix}. \end{cases}$$

It is clear that $\epsilon_{j+1} = res_{I^j/I^{j+1}}$, where

$$res_{I^j/I^{j+1}} : \mathrm{PSL}(2, R/I^{j+1}) \to \mathrm{PSL}(2, (R/I^{j+1})/(I^j/I^{j+1}))$$

is the map obtained via restriction mod I^j/I^{j+1}. So by 2.5.5,

$$ke(\epsilon_{j+1}) = \Gamma(2, R/I^{j+1}, I^j/I^{j+1}) \cong (I^j/I^{j+1}, +)^3.$$

Let I be a maximal ideal of R. Then R/I^{j+1} is a local ring with the maximal ideal I^j/I^{j+1}. In this case it is very easy to prove that ϵ_{j+1} is surjective: considering $u = \begin{pmatrix} a+I^j & b+I^j \\ c+I^j & d+I^j \end{pmatrix} \in \mathrm{PSL}(2, R/I^j)$, we see that $ad - bc - 1 \in I^j$, so $ad -$

$bc + I^{j+1}$ is a unit element of R/I^{j+1}. If $e + I^{j+1}$ is its inverse, then $u' = \begin{pmatrix} ea+I^{j+1} & eb+I^{j+1} \\ c+I^{j+1} & d+I^{j+1} \end{pmatrix} \in \mathrm{PSL}(2, R/I^{j+1})$ with $\epsilon(u') = u$.

As a consequense of 2.3.6, we have $\Gamma(2, R/I^{j+1}, I^j/I^{j+1}) = Q(I^j/I^{j+1})$, so we get the following short exact sequence:

$$0 \to (I^j/I^{j+1}, +)^3 \to \mathrm{PSL}(2, R/I^{j+1}) \to \mathrm{PSL}(2, R/I^j) \to 0,$$

As a result, $(I^j/I^{j+1}, +)^3$ is a $\mathrm{PSL}(2, R/I^j)$–module. So we have proved the following

Proposition 2.5.6. Let R be an integral domain and $I \trianglelefteq R$. For every $j \in \mathbb{N}$, $\Gamma(2, R/I^{j+1}, I^j/I^{j+1}) = Q(I^j/I^{j+1}) \cong (I^j/I^{j+1}, +)^3$ and the following sequence is exact:

$$0 \to (I^j/I^{j+1}, +)^3 \to \mathrm{PSL}(2, R/I^{j+1}) \to \mathrm{PSL}(2, R/I^j) \to 0,$$

As a result, $(I^j/I^{j+1}, +)^3$ is a $\mathrm{PSL}(2, R/I^j)$–module.

This result leads immediately to the following facts about orders and solvability of $\mathrm{PSL}(2, \mathbb{Z}/2^j\mathbb{Z})$ and $\mathrm{PSL}(2, \mathbb{Z}/3^j\mathbb{Z})$:

Corollary 2.5.7. For every $j \in \mathbb{N}$, we have $|\mathrm{PSL}(2, \mathbb{Z}/2^j\mathbb{Z})| = 3 \cdot 2^{3j-2}$ and $|\mathrm{PSL}(2, \mathbb{Z}/3^j\mathbb{Z})| = 4 \cdot 3^{3j-2}$.

Proof. The proof is by induction on j. For $j = 1$, there is nothing to prove since $\mathrm{PSL}(2, \mathbb{Z}/2\mathbb{Z}) \cong S_3$ is of order 6 and $\mathrm{PSL}(2, \mathbb{Z}/3\mathbb{Z}) \cong A_4$ is of order 12 (see [21].) Assume that $|\mathrm{PSL}(2, \mathbb{Z}/2^j\mathbb{Z})| = 3 \cdot 2^{3j-2}$ and $|\mathrm{PSL}(2, \mathbb{Z}/3^j\mathbb{Z})| = 4 \cdot 3^{3j-2}$. By 2.5.6, we have the following short exact sequence:

$$0 \to (I^j/I^{j+1}, +)^3 \to \mathrm{PSL}(2, \mathbb{Z}/I^{j+1}) \to \mathrm{PSL}(2, \mathbb{Z}/I^j) \to 0,$$

where I is either $2\mathbb{Z}$ or $3\mathbb{Z}$ respectively. Hence

$$|\mathrm{PSL}(2, \mathbb{Z}/I^{j+1})| = |I^j/I^{j+1}|^3 |\mathrm{PSL}(2, \mathbb{Z}/I^j)|.$$

For $I = 2\mathbb{Z}$, $|I^j/I^{j+1}| = 2$ and for $I = 3\mathbb{Z}$, $|I^j/I^{j+1}| = 3$, and we are done. □

Corollary 2.5.8. Let R be an integral domain and $I \trianglelefteq R$ be such that $\mathrm{PSL}(2, R/I)$ is solvable. Then for every $j \in \mathbb{N}$, the group $\mathrm{PSL}(2, R/I^j)$ is solvable.

Proof. This follows from 2.5.6 by induction. □

Corollary 2.5.9. For every $j \in \mathbb{N}$, the groups $\mathrm{PSL}(2, \mathbb{Z}/2^j\mathbb{Z})$ and $\mathrm{PSL}(2, \mathbb{Z}/3^j\mathbb{Z})$ are solvable.

Proof. Just note that $\mathrm{PSL}(2,\mathbb{Z}/2\mathbb{Z}) \cong S_3$ and $\mathrm{PSL}(2,\mathbb{Z}/3\mathbb{Z}) \cong A_4$ ([21]) are both solvable. □

Let $\mathcal{O} := \mathcal{O}_{-d}$, $d \in \{1,2,3,7,11\}$, $x \in \mathcal{O}$, and $G := \mathrm{PSL}(2,\mathcal{O})$. We shall prove that if x satisfies the condition that each prime appearing in its prime factor decomposition has norm > 3, then the group $G/\Gamma(x\mathcal{O})$ is perfect. We use this fact here to prove some properties of congruence subgroups. Let us start by proving some elementary facts about perfect groups. Let G be a group and $N \trianglelefteq G$ be an abelian normal subgroup of it. Recall that the conjugation action of G on N induces an action of G/N on N, turning N into a G/N-module. The following simple lemma will be useful later:

Lemma 2.5.10. Let N be a normal subgroup of a non-abelian group G with G/N perfect. Then $G = G'N$. Moreover, if N is abelian and a simple G/N-module, then $G = G' \oplus N$.

Proof. Since G/N is perfect, $G/N = (G/N)' = G'N/N$ and hence $G = G'N$. Let N be abelian and a simple G/N-module. Now $G' \cap N$ is a G/N-submodule of N. If $G' \cap N = N$, then $G = G'$, contradiction. So $G' \cap N = 0$. □

Let $x \in \mathcal{O}$. Decompose x as $x = p_1^{e_1} \cdots p_r^{e_r}$ with $e_i > 0$ and p_i's distinct prime elements of $\mathcal{O}$. Let

$$\pi : G \twoheadrightarrow G/\Gamma(I),\ \pi_j : \bigoplus_1^r \mathrm{PSL}(2,\mathcal{O}/\mathcal{O}p_i^{e_i}) \twoheadrightarrow \mathrm{PSL}(2,\mathcal{O}/\mathcal{O}p_j^{e_j})$$

be the canonical projections. We have the following theorem:

Proposition 2.5.11. With the above notation, if $N(p_i) > 3$ for all i, then $G/\Gamma(x\mathcal{O})$ is perfect.

Proof. Put $I := x\mathcal{O}$. Since $p_1^{e_1}, \cdots, p_r^{e_r}$ are co-prime, we have $\mathcal{O} = \mathcal{O}p_1^{e_1} + \cdots + \mathcal{O}p_r^{e_r}$ and hence by the chinese reminder theorem

$$\mathcal{O}/I \cong \mathcal{O}/\mathcal{O}p_1^{e_1} \oplus \cdots \oplus \mathcal{O}/\mathcal{O}p_r^{e_r}$$

which, in turn, gives rise to an isomorphism

$$\psi : G/\Gamma(I) \to \mathrm{PSL}(2,\mathcal{O}/I) \to \mathrm{PSL}(2,\mathcal{O}/\mathcal{O}p_1^{e_1}) \oplus \cdots \oplus \mathrm{PSL}(2,\mathcal{O}/\mathcal{O}p_r^{e_r}).$$

As $N(p_i) > 3$ for all i, by proposition 1.1.17 $|\mathcal{O}/\mathcal{O}p_i| > 3$ hence by corollary 2.5.4 we are done. □

Now we easily see that:

Theorem 2.5.12. Let T be a proper subgroup of $\mathrm{PSL}(2,\mathcal{O}_{-d})$, $d \in \{1,2,3,7,11\}$, of level $x\mathcal{O}_{-d}$ ($0 \neq x \in \mathcal{O}_{-d}$) with $\mathrm{PSL}(2,\mathcal{O}_{-d})' \subseteq T$. If T is congruence, then there exists $p \in \mathcal{O}_{-d}$ prime such that $p \mid x$ and $N(p) \in \{2,3\}$.

Proof. Decompose $x = p_1^{e_1} \cdots p_r^{e_r}$ as above. If $N(p_i) > 3$ for all i, then $G/\Gamma(x\mathcal{O})$ is perfect by the above proposition, so by 2.5.10, $\mathrm{PSL}(2,\mathcal{O}) = T$, contradiction. Hence there exists i with $N(p_i) \in \{2,3\}$. □

Example. Consider the presentation of $\Gamma_{-7} = \mathrm{PSL}(2,\mathcal{O}_{-7})$ given in theorem 2.2.1. Let T be a proper subgroup of Γ_{-7} of level $x\mathcal{O}_{-7}$ ($0 \neq x \in \mathcal{O}_{-7}$) with $\omega \nmid x$ and $1-\omega \nmid x$. If $< ba^3 >^{\Gamma_{-7}} \subseteq T$, then T is non-congruence.

Proof. The only elements of $\mathcal{O}_{-7}$ of norm 2 are $\omega, 1-\omega$ and there is no element of norm 3 (see the table 1.1 at the end of section 1 of chapter 1). It can be easily seen that $\mathrm{PSL}(2,\mathcal{O}_{-d})' = < ba^3 >^{\Gamma_{-7}}$ ($ba^3 = [a^{-1},b][b,a^{-2}]$). Now the above theorem finishes the work. □

2.6 Congruence subgroup property in $\mathrm{SL}(2,\mathcal{O}[\frac{1}{p}])$

Let $p \in \mathcal{O} := \mathcal{O}_{-d}$ be prime, d any square-free natural number. In this section we show that the group $\mathrm{SL}(2,\mathcal{O}[\frac{1}{p}])$ (and hence $\mathrm{PSL}(2,\mathcal{O}[\frac{1}{p}])$) has the congruence subgroup property. Then we prove that the group

$$\Gamma(I) *_{\Gamma(I)\cap\Gamma(I)^g} \Gamma(I)^g$$

is isomorphic to a finite index subgroup of $\mathrm{PSL}(2,\mathcal{O}[\frac{1}{p}])$ which hence satisfies the CSP, where $g := \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}(2,\mathbb{Q}(\sqrt{-d}))$, for every $p \in \mathcal{O}$ prime and every non-zero ideal I of $\mathbb{Q}(\sqrt{-d})$ such that $p \notin I$. This result will be used in the proof of 3.6.7 which, in turn, will be used in the proof of the main theorem of section 3.6, theorem 3.6.4. We will prove the CSP for $\mathrm{SL}(2,\mathcal{O}[\frac{1}{p}])$ in 2.6.3. This is in fact a generalization of Berger's idea [9], based on the Bass-Serre theory of trees.

We start by stating an important theorem of Serre, which is the key for proving the CSP of $\mathrm{SL}(2,\mathcal{O}[\frac{1}{p}])$. For the proof and details of the theorem, see [60], Theorem 2. First recall that:

Definition 2.6.1. Let S_{all} be the set of all places of a number field F and $S \subseteq S_{all}$ be a finite subset of S_{all} containing S_∞, the set of all Archimedean places of F. The ring of **S-integers** of F is by definition:

$$\mathcal{O}_S := \{x \in F \mid v(x) \geq 0, \text{ for every place } v \in S_{all} - S\}$$

$\mathcal{O}_S$ is a Dedekind domain whose maximal ideals are in 1-1 correspondence with the elements of $S_{all} - S$. The aforementioned theorem of Serre says:

Theorem 2.6.2. (Serre) Let S be a finite subset of the places of the field $\mathbb{Q}(\sqrt{-d})$ containing all Archimedean places, and $\mathcal{O}_S$ the subring of S-integers. Then the group $\mathrm{SL}(2,\mathcal{O}_S)$ (and hence $\mathrm{PSL}(2,\mathcal{O}_S)$ by 2.3.2) satisfies the CSP.

We use this for proving the CSP of $\mathrm{PSL}(2,\mathcal{O}[\frac{1}{p}])$:

Proposition 2.6.3. Let $p \in \mathcal{O}$ be prime. Then the group $\mathrm{SL}(2,\mathcal{O}[\frac{1}{p}])$ (and hence $\mathrm{PSL}(2,\mathcal{O}[\frac{1}{p}])$) has the congruence subgroup property.

Proof. Let S_{all} be the set of all places of $F := \mathbb{Q}(\sqrt{-d})$ and S_p be the set of (the two, see 1.2.10) Archimedean places of F together with the non-Archimedean place corresponding to the prime ideal $P := p\mathcal{O}$. We show that $\mathcal{O}_{S_p} = \mathcal{O}[\frac{1}{p}]$, and then theorem 2.6.2 finishes the work. So suppose that $x \in \mathcal{O}_{S_p}$. Decompose $\mathcal{O}x$ as $P_1^{e_1} \cdots P_n^{e_n}$ with P_i's being distinct prime ideals of $\mathcal{O}$. So for all i, we have $e_i < 0$ if and only if $P_i = P$. On the other hand, every negative power of P is contained in $\mathcal{O}[\frac{1}{p}]$, because $P^{-1} = \{\, y \in F \mid\ yp\mathcal{O} \subseteq \mathcal{O}\} = \mathcal{O}[\frac{1}{p}]$, and we are done. □

In order to prove the main result of this section, (i.e. proving that $\Gamma(I) *_{\Gamma(I)\cap\Gamma(I)^g} \Gamma(I)^g \cong \Gamma(I \cdot \mathcal{O}[\frac{1}{p}])$, first we need the following lemmas.

Lemma 2.6.4. Let R be a commutative ring with unit, $p \in R$ with Rp maximal, and $I, J \trianglelefteq R$ coprime to Rp. Then $IJ + Rp^k = R$, for every $k \in \mathbb{N}$.

Proof. Clearly $IJ + Rp = R$. So there exist $r \in R,\ x \in I,\ and\ y \in J$ such that $1 = rp + xy$, and hence $p^{k-1} = xyp^{k-1} + rp^k \in IJ + Rp^k$, so $IJ + Rp^{k-1} = IJ + Rp^k$ for all k, whence the result follows by induction on k. □

Lemma 2.6.5. Let $I \lhd \mathcal{O}$ and $p \in \mathcal{O}$ prime such that $p \notin I$. Set $\tilde{I} := I \cdot \mathcal{O}[\frac{1}{p}]$. Then $\tilde{I}$ is dense in $K := \mathbb{Q}(\sqrt{-d})$ with respect to the topology induced by the absolute value $|\ |_{\mathcal{O}p}$ on K.

Proof. Let $P := \mathcal{O}p$. As $\mathcal{O}$ is a Dedekind domain (1.1.1), every non-zero prime ideal of it is maximal, so $I + P = \mathcal{O}$. Let $x \in K$ and $\epsilon > 0$. Recall from theorem 1.1.3 that $\mathbb{Q}(\sqrt{-d})$ is the field of fractions of $\mathcal{O}$. Write $x = \frac{a_1}{b_1}$ with $a_1, b_1 \in \mathcal{O}$, $b_1 \neq 0$. Suppose that $v_P(a_1) = \alpha,\ v_P(b_1) = \beta$, and use part 1 of lemma 1.2.6 to write $a_1 = p^\alpha a,\ b_1 = p^\beta b$ with $a, b \in \mathcal{O}$ and $p \nmid a, b$, so $x = p^{\alpha-\beta}\frac{a}{b}$. Put $s := \alpha - \beta$. Choose $k \in \mathbb{N}$ such that $p^{-k} < \epsilon$. Let $s < 0$. By the previous lemma, $bI + P^{k-s} = \mathcal{O}$. So there exist $g \in I,\ y \in \mathcal{O}$ such that

$a = bg + yp^{k-s}$, hence $p^{k-s} \mid a - bg$ and by part 2 of 1.2.6, $|a - bg|_P \leq p^{-k+s}$. Thus $|x - p^s g|_P = |p^s \frac{a}{b} - p^s g|_P = |p^s|_P |\frac{a}{b} - g|_P$. Since $|b|_P = 1$, we have $|\frac{a}{b} - g|_P = |a - bg|_P \leq p^{-k+s}$, so $|x - p^s g|_P \leq p^{-s} p^{-k+s} = p^{-k} < \epsilon$ and $p^s g \in \tilde{I}$. The case $s \geq 0$ is handled in a similar way.

□

We now recall some facts about the theory of groups acting on trees which we are going to use to prove that $\Gamma(I) *_{\Gamma(I) \cap \Gamma(I)^g} \Gamma(I)^g \cong \Gamma(I \cdot \mathcal{O}[\frac{1}{p}])$ in 2.6.8. For details, see [13] appendix to chapter 2 and [61].

Recall that if a group G acts on a tree X then an edge $e = (v, v')$ with vertices v to v' is called a **fundamental domain** for the action if every edge of X is G–equivalent to e and every vertex of X is G–equivalent to either v or v' but not both. In this case, the tree consisting of only one edge e with vertices v, v' is isomorphic, as a tree, to X/G and we have $G_g = G_v \cap G_{v'}$, where G_g, G_v, and $G_{v'}$ are the stabilizers of e, v, v' respectively. The following theorem of Serre states that such an action of G gives a decomposition of G as an amalgamated free product:

Theorem 2.6.6. ([13] Theorem $A1$ chapter 2) Let a group G act on a tree X, and let e be an edge with vertices v, v' such that e is a fundamental domain for the action. Then $G = G_v *_{G_e} G_{v'}$.

Let V be a K vector space of dimension 2, where K is a valued field (with discrete value v) with valuation ring R. Recall that a **lattice** of V is any free R–submodule of V of rank 2. If $x \in K^*$, and if L is a lattice of V, then since $xR = Rx$, Lx is also a lattice of V. Thus the group K^* acts on the set of lattices of V and we call the orbit of a lattice L under this action its **class**, and denote it by $[L]$. Two lattices belonging to the same class are called **equivalent**. The set of lattice classes is denoted by $\mathfrak{L}(V)$. Two elements $X, Y \in \mathfrak{L}(V)$ are said to be **adjacent** if lattices L, L' exist such that $X = [L], Y = [L']$, and $L/L' \cong R/xR$, for some $x \in K^*$ with $v(x) = 1$. This relation makes $\mathfrak{L}(V)$ a tree. Moreover, the group $\mathrm{SL}(2, K)$ ($\mathrm{PSL}(2, K)$ resp.) acts on the set of lattices (and on this tree resp.) in the following way: Let $L = l_1 R + l_2 R$ be a lattice and $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, K)$. Then

$$g \cdot L := (al_1 + bl_2)R + (cl_1 + dl_2)R.$$

We have the following theorem

Theorem 2.6.7. ([61], chapter 2,theorem 2) Let $G \leq \mathrm{PSL}(2, K)$ and $L \subseteq L'$ be two adjacent lattices in V. If the closure of G in $\mathrm{PGL}(2, K)$ contains $\mathrm{PSL}(2, K)$, then the edge of $\mathfrak{L}(V)$ with vertices $[L], [L']$ is a fundamental domain for the action of G. Moreover, we have $G_{[L]} = G_L$, and $G_{[L']} = G_{L'}$.

Finally, we are ready to prove the main theorem of this section.

Theorem 2.6.8. Let $0 \neq I \lhd \mathcal{O} = \mathcal{O}_{-d}$ and $p \in \mathcal{O}$ be prime such that $p \notin I$. Define $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}(2, \mathbb{Q}(\sqrt{-d}))$. Then $\Gamma(I) *_{\Gamma(I)\cap\Gamma(I)^g} \Gamma(I)^g \cong \Gamma(I \cdot \mathcal{O}[\frac{1}{p}])$, and the latter satisfies the congruence subgroup property.

Proof. Let $\tilde{I} := I \cdot \mathcal{O}[\frac{1}{p}]$. Consider the p-adic valuation $v : \mathbb{Q}(\sqrt{-d}) \to \mathbb{Z} \cup \{\infty\}$ and let $R := \{x \in \mathbb{Q}(\sqrt{-d}) \mid v(x) \geq 0\}$ be its valuation ring.

We know from the previous lemma that $\tilde{I}$ is dense in $K := \mathbb{Q}(\sqrt{-d})$ with respect to the p-adic norm. We show that the closure of $\Gamma(\tilde{I})$ in $\mathrm{PGL}(2,K)$ contains $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$, and so $\mathrm{PSL}(2,K)$ (see [61], II.1.2 or 2.5.2): Let $\epsilon > 0$ and $x \in K$ be given. Useing density of $\tilde{I}$ in K, choose $b \in \tilde{I}$ such that $|b - x|_p < \epsilon$, then $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma(\tilde{I})$ is in the ϵ-neighborhood of $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$. The argument for $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ is similar.

Now apply the previous two theorems with $G = \Gamma(\tilde{I})$, $L' := R \cdot p^2 \oplus R \cdot p \subseteq L := R \cdot p \oplus R \cdot p$, to see that $\Gamma(\tilde{I}) = G_L *_{G_L \cap G_{L'}} G_{L'}$, where $G_L, G_{L'}$ are the stabilizers of L, L' under the G-action respectively. We show that $G_L = \Gamma(I)$ and $G_{L'} = \Gamma(I)^g$:

Lemma. For every $x \in \tilde{I}$, if $x \notin R$ then $x - 1 \notin I$.

To show that $G_L = \Gamma(I)$, consider $u = \left(\begin{smallmatrix} a+1 & b \\ c & d+1 \end{smallmatrix}\right) \in \Gamma(I)$, with $a, b, c, d \in I$. So

$$\begin{pmatrix} a+1 & b \\ c & d+1 \end{pmatrix} \begin{pmatrix} p \\ 0 \end{pmatrix} = \begin{pmatrix} p(a+1) \\ cp \end{pmatrix},$$

$$\begin{pmatrix} a+1 & b \\ c & d+1 \end{pmatrix} \begin{pmatrix} 0 \\ p \end{pmatrix} = \begin{pmatrix} bp \\ p(d+1) \end{pmatrix}.$$

By the above lemma, $a+1, d+1 \in R$, so $Lu \subseteq L$ for every $u \in \Gamma(I)$, that is $Lu = L$ for every $u \in \Gamma(I)$.

To show that $G_{L'} = \Gamma(I)^g$, consider $u \in \Gamma(I)^g$ and write $u = \left(\begin{smallmatrix} a+1 & b/p \\ cp & d+1 \end{smallmatrix}\right)$ with $a, b, c, d \in I$ and argue as above.

Finally, we note that $\Gamma(\tilde{I})$ is of finite index in $\mathrm{PSL}(2, \mathcal{O}[\frac{1}{p}])$, and then congruence subgroup property follows from 2.6.3. To see this, use 1.2.6 part 1 to show that $\mathcal{O}[\frac{1}{p}]/\tilde{I} \cong \mathcal{O}/I$, and the latter is finite by 1.1.1. □

2.7 Some computational examples

Let $\mathbb{H}^3 := \mathbb{C} \times \mathbb{R}^+$ be the 3-dimensional hyperbolic space. Recall that the group $\mathrm{PSL}(2,\mathbb{C})$ acts on $\mathbb{H}^3$ in the following way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z,r) := \frac{1}{N}((az+b)\overline{(cz+d)} + a\bar{c}r^2, r),$$

where $N := |cz+d|^2 + |c|^2 r^2$. A subgroup G of $\mathrm{PSL}(2,\mathbb{C})$ acts properly discontinuously on $\mathbb{H}^3$ if and only if it is a discrete subgroup. If, in addition, it is torsion-free, then the quotient space $\mathbb{H}^3/G$ gets the structure of a hyperbolic 3-dimensional Riemannian manifold. We call a torsion-free discrete subgroup G of $\mathrm{PSL}(2,\mathbb{C})$ a **link complement (sub)group** if $\mathbb{H}^3/G$ is homeomorphic to $S^3 - L$, where $L \subseteq S^3$ is a **link**, that is, a finite union of m disjoint closed simple curves in the three sphere S^3 ; if $m = 1$, L is a knot. We have for the singular cohomology of the complement $S^3 - L$ the following

Lemma 2.7.1. Let q be a non-negative integer. Then

$$H^q(S^3 - L, \mathbb{Z}) = \begin{cases} \mathbb{Z} & q = 0 \\ \mathbb{Z}^m & q = 1 \\ \mathbb{Z}^{m-1} & q = 2 \\ 0 & q > 2 \end{cases}$$

For a proof, see [58].

Question. For which values of d, the group $\mathrm{PSL}(2,\mathcal{O}_{-d})$ contains a link complement subgroup?

Results on the cohomology of $\mathrm{PSL}(2,\mathcal{O}_{-d})$ (see [67]) limit the values of d for which this is possible to the following list:

$$\{1,2,3,5,6,7,11,15,19,23,31,39,47,71\}.$$

Over the last 20 years, numerous link complement groups have been found in $\mathrm{PSL}(2,\mathcal{O}_{-d})$ for all of these cases. (see [3], [54], [36], [55], [65], [68], and [4]). Furthermore, many of the corresponding links (figure eight knot, Whitehead link, Borromean rings, . . .) have been central to the study of 3-manifolds.

Conversely, a link L in S^3 is called *arithmetic* of type d if $S^3 - L$ is homeomorphic to $\mathbb{H}^3/G$, where G is a torsion-free subgroup of $\mathrm{PSL}(2,\mathcal{O}_{-d})$ of finite index and d is minimal with this property. It can be shown that, every link in S^3 is a sub-link of an arithmetic link of type 1 (see [5]). The figure eight knot is the only arithmetic knot but there exists infinitely many arithmetic links, even with two components, see [54].

In this section we consider some link complement subgroups of small index in the Bianchi groups Γ_{-1} and Γ_{-7} and compute their levels and show that they are congruence. We used the computer algebra system GAP[1] in order to compute indexes and check wether an element is in a subgroup or not.

[1] GAP is a system for computational discrete algebra, with particular emphasis on Computational Group Theory. See http://www.gap-system.org/

The group Γ_{-1}

In this case we have $\omega = i$, $N(m+ni) = m^2+n^2$, and $M(< m+ni >) =< a^m c^n, a^{-n}c^m >$ (2.3.7). We choose the following presentation for Γ_{-1}: (2.2.1)

$$\Gamma_1 =< a,b,c,j \mid b^2 = (ab)^3 = [a,c] = (aj)^2 = (bj)^2 = (cj)^2 = (cbj)^2 = 1 > .$$

The group Γ_{-1} has, up to $Isom(\mathbb{H}^3)$-conjugacy, exactly 2 torsion free subgroups of index 6 with torsion free abelianizations ([31] §4). Their level is determined by the next theorem.

Theorem 2.7.2. Let $e := ba^{-1}cb$.

1. The subgroup $\Gamma_{-1}(12,1) :=< c,e >$ is congruence of level $< -2+2i >$. It is isomorphic to the complement in S^3 of the 2-component link:

2. The subgroup $\Gamma_{-1}(12,5) :=< a,c,bc^2ab >$ is congruence of level $< 1+2i >$. It is isomorphic to the complement in S^3 of the 2-component link:

Proof. It has been proved in [31] that these groups are isomorphic to the complement in S^3 of the given links. So we compute the levels.

1. As $[< a,c,e >:< c : e >] = 2$ by using GAP, we infer that $M(< m+ni >) \subseteq < c,e >$ if and only if $M(< m+ni >) \subseteq < a,e >$ if and only if m,n are even. Now consider $M(< -2+2i >) =< a^{-2}c^2, a^{-2}c^{-2} >$. Use GAP to see that $Q(< -2+2i >) \subseteq < c,e >$, but $Q(< 2 >)$ is not

included in $< c, e >$. Since $-2+2i = (1+i)^3$ is the prime factorization of $-2+2i$, $< -2+2i >$ is the level of $< c, e >$. Again using GAP we compute $[\Gamma_{-1} : Q(< -2+2i >)] = 192$ and using 2.3.3 we see that $[\Gamma_{-1} : \Gamma(-2+2i)] = 192$. So by 2.3.7 part 1, $Q(< -2+2i >) = \Gamma(-2+2i)$.

2. One checks easily that $Q(< 1+2i >) \subseteq \Gamma_{-1}(12,5)$ (similar to part 1). But $1+2i$ is a prime in $\mathcal{O}_{-1}$. Also check that $[\Gamma_{-1} : Q(< 1+2i >)] = [\Gamma_{-1} : \Gamma(1+2i)] = 60$, and deduce that $Q(< 1+2i >) = \Gamma(1+2i)$.

□

The group Γ_{-7}

In this case we have $\omega = (1+\sqrt{(}-7))/2$, $N(m+ni) = m^2+mn+2n^2$, and $M(< m+ni >) =< a^m c^n, a^{-2n} c^{m+n} >$ (2.3.7). Note that since $M(-m+mi) \subseteq < a^{-m}c^m, a^m c^m >$, $Q(-m+mi) \subseteq N_m := (< a^{-m}c^m, a^m c^m >)^{\Gamma_{-7}}$. We choose the following presentation for Γ_{-7}: (2.2.1)

$$\Gamma_{-7} =< a, b, c \mid b^2 = (ab)^3 = [a,c] = (c^{-1}bcba)^2 = 1 >$$

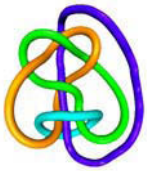
The group Γ_{-7} has, up to $Isom(\mathbb{H}^3)$–conjugacy, exactly 2 torsion free subgroups of index 6 and also 2 of index 12 with torsion free abelianizations ([31] §2). Their level is determined by the next theorem.

Theorem 2.7.3.

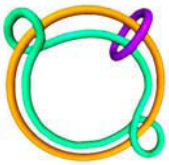
1. The subgroup $\Gamma_{-7}(6,1) :=< a^2, c, bcb >$ is congruence of level $< 2 >$. It is isomorphic to the complement in S^3 of the 3–component link:

2. The subgroup $\Gamma_{-7}(6,5) :=< c, bab >$ is congruence of level $< 2\omega >$. It is isomorphic to the complement in S^3 of the 2–component link:

3. The subgroup $\Gamma_{-7}(12,4) :=< c, bc^2b, bca^2b, abc^2ba^{-1} >$ is congruence of level $< -2+\omega >$. It is isomorphic to the complement in S^3 of the 4–component link:



4. The subgroup $\Gamma_{-7}(12,12) :=< c, bcb, a^{-1}bcba^{-1} >$ is congruence of level $< 2\omega >$. It is isomorphic to the complement in S^3 of the 3–component link:



Proof. Again the fact that these groups are isomorphic to the complement in S^3 of the given links has been proved in [31]. So we compute the levels.

1. Looking at the index $[< a, c, bcb >:< a^2, c, bcb >] = 2$ (use GAP), we infer that $M(< m+n\omega >) \subseteq < a^2, c, bcb >$ if and only if m is even. Now consider $M(< 2 >) =< a^2, c^2 >$. Note that $2 = \omega(1-\omega)$ is the prime factor decomposition of 2. Clearly $M(< \omega >)$ and $M(< 1-\omega >)$ cannot be contained in $< a^2, c, bcb >$. Use GAP to see that $Q(< 2 >) \subseteq < a^2, c, bcb >$, that is, $< 2 >$ is the level of $< a^2, c, bcb >$, and also $[\Gamma_{-7} : Q(< 2 >)] = 36$. Now using 2.3.3 we see that $[\Gamma_{-7} : \Gamma(2)] = 36$ and by 2.3.7 part 1, $Q(< 2 >) = \Gamma(2)$.

2. First observe that a, a^2, and a^3 are not in $\Gamma_{-7}(6,5)$, but a^4 is (by using GAP), which shows that $M(< m + n\omega >) \subseteq \Gamma_{-7}(6,5)$ if and only if $4 \mid m$ and n is even. Using GAP we see that $Q(< 2\omega >) \subseteq \Gamma_{-7}(6,5)$. But $2\omega = \omega^2(1-\omega)$ is the prime factorization of 2ω and non of the subgroups $M(< \omega >)$, $M(< \omega^2 >)$, $M(< 1-\omega >)$, and $M(< \omega(1-\omega) >)$ can be contained in $\Gamma_{-7}(6,5)$, hence $\mathfrak{a}_{\Gamma_{-7}(6,5)} =< 2\omega >$. Again using GAP we compute $[\Gamma_{-7} : Q(< 2\omega >)] = 144$ and using 2.3.3 we see that $[\Gamma_{-7} : \Gamma(2\omega)] = 144$. So by 2.3.7 part 1, $Q(< 2\omega >) = \Gamma(2\omega)$.

3. First look at the index $[\Gamma_{-7}(12,4) \bigvee \{A\} : \Gamma_{-7}(12,4)] = 2$, which shows that $M(< m + n\omega >) \subseteq \Gamma_{-7}(12,4)$ if and only if m is even. Using GAP we see that $Q(< -2+\omega >) \subseteq \Gamma_{-7}(12,4)$. But $-2+\omega = -\omega^2$ is the prime factorization of $-2+\omega$ and $M(< \omega >)$ cannot be contained in $\Gamma_{-7}(12,4)$, hence $\mathfrak{a}_{\Gamma_{-7}(12,4)} =< -2+\omega >$. The rest of the proof is exactly similar to parts 1 and 2: just show that $[\Gamma_{-7} : Q(< -2+\omega >)] = [\Gamma_{-7} : \Gamma(-2+\omega)] = 24$.

4. Again observe that a, a^2, and a^3 are not in $\Gamma_{-7}(12,12)$, but a^4 is, which shows that $M(< m + n\omega >) \subseteq \Gamma_{-7}(12,12)$ if and only if $4 \mid m$ and n is even. Using GAP we see that $Q(< 2\omega >) \subseteq \Gamma_{-7}(12,12)$. But $2\omega = \omega^2(1-\omega)$ is the prime factorization of 2ω and non of the subgroups $M(< \omega >)$, $M(< \omega^2 >)$, $M(< 1-\omega >)$, and $M(< \omega(1-\omega) >)$ can be contained in $\Gamma_{-7}(12,12)$, that is, $\mathfrak{a}_{\Gamma_{-7}(12,12)} =< 2\omega >$. The rest of the proof follows from part 2.

□

3 Hecke Operators

Notation 3.0.4. For an element g and a subgroup H of an arbitrary group G:

1. $H^g := g^{-1}Hg$, ${}^gH := gHg^{-1}$, $H_g := H \cap H^g$, and ${}_gH := H \cap {}^gH$.
2. $\mu_H(g) := [H : H_g] = [H : {}_{g^{-1}}H]$.
3. $H_G := \bigcap\{H^g \mid g \in G\}$ is the normal core of the subgroup H in the group G.
4. We use $\sqcup$ to deonte the disjoint uninion.

3.1 Introduction

The study of modular forms for congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$ has been one of the central topics in number theory for over one century. This theory is now well developed and has broad applications and impact to many branches of mathematics. There is a collection of important linear operators acting on modular forms, called the Hecke operators. The study of Hecke operators associated to congruence subgroups leads to a deep understanding of the structure of the space of modular forms and cusp forms. In contrast, the action of Hecke operators for non-congruence subgroups is rather trivial, as conjectured by Atkin (see below) and proved by Serre (Appndix to[64] and Berger [9]. In this chapter, motivated by the recent interest in the arithmetic of Bianchi modular forms ([14] and [26]), we will prove a generalization of Atkin's conjecture to the cohomology of subgroups of Bianchi groups. Let us first recall standard facts about modular forms and state the Atkin's conjecture. For details, see [62]. Let $\mathrm{GL}(2,\mathbb{R})^+$ be the sub-semigroup of $\mathrm{GL}(2,\mathbb{R})$ consisting of matrices with positive determinant. As in chapter 1, $\mathbb{H}^2 = \{z \in \mathbb{C} \mid Im(z) > 0\}$ is the Poincaré (upper) half plane. The group $\mathrm{GL}(2,\mathbb{R})^+$ acts on $\mathbb{C} \cup \{\infty\}$ by **Möbius transformations**: for every $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{R})^+$ and $z \in \mathbb{C}$,

$$\sigma \cdot z := \frac{az+b}{cz+d},$$

$$\sigma \cdot \infty := \begin{cases} a/c & \text{if } c \neq 0, \\ \infty & \text{otherwise.} \end{cases}$$

An element $\pm I_{2\times 2} \neq \sigma \in \mathrm{SL}(2,\mathbb{R})$ is said to be **parabolic** if $tr(\sigma) = \pm 2$. It is called **elliptic** (**hyperbolic** resp.) if $tr(\sigma) \in \mathbb{R}$ and $|tr(\sigma)| < 2$. (> 2 resp.) Finally, if $tr(\sigma)$ is not real, then σ is called **loxodromic**. The following proposition is well known:

Proposition 3.1.1. ([62], 1.13) Let $\pm I \neq \sigma \in \mathrm{SL}(2,\mathbb{R})$. Then σ has at most two distinct fixed points, and we have

1. σ is parabolic if and only if σ has only one fixed point in $\mathbb{R} \cup \{\infty\}$.
2. σ is elliptic if and only if σ has one fixed point $z \in \mathbb{H}^2$ and the other fixed point is $\bar{z}$.
3. σ is hyperbolic if and only if σ has two fixed points in $\mathbb{R} \cup \{\infty\}$.

Let G be a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. A point $s \in \mathbb{R} \cup \{\infty\}$ is called a **cusp** of G if there exists a parabolic element $\sigma \in G$ such that $\sigma s = s$. Let $Fix_G(s) := \{g \in G \mid gs = s\}$. If s is a cusp of G, then it is well known ([62], 1.17) that $Fix_G(s)/(G \cap \{\pm I\}) \cong \mathbb{Z}$ and any element ($\neq \pm I$) of $Fix_G(s)$ is parabolic.

Let $\mathfrak{F}$ be the complex vector space of all meromorphic functions $f : \mathbb{H}^2 \to \mathbb{C}$. For every $k \in \mathbb{N} \cup \{0\}$, the group $\mathrm{GL}(2,\mathbb{R})^+$ acts on $\mathfrak{F}$ by the so called **weight k** operators $|_k$ as follows:

$$(f \mid_k \sigma)(z) := det(\sigma)^{k/2}(cz+d)^{-k} f(\sigma z),$$

where

$$\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{R})^+,\ f \in \mathfrak{F}.$$

For every subgroup G of $\mathrm{GL}(2,\mathbb{R})^+$, denote the subspace of functions of $\mathfrak{F}$ which are fixed under the action $|_k$ of G and are analytic at every cusp of G by $\mathfrak{F}^G$, and call them the **G–automorphic forms of weight k**. If G is a subgroup of $\mathrm{SL}(2,\mathbb{R})$, the G–automorphic forms are then called G–**modular forms** of weight k. The space $\mathfrak{F}^G$ is often denoted by $M_k(G)$. If a weight k G–automorphic form vanishes at every cusp of G, it is then said to be a G–**cusp form** of weight k and the subspace consisting of G–cusp forms of weight k is denoted by $S_k(G)$. For every $H \leq_f K \leq \mathrm{GL}(2,\mathbb{R})^+$, we denote the **trace map** between the corresponding spaces of automorphic forms by $Tr_H^K : \mathfrak{F}^H \to \mathfrak{F}^K$, that is, $Tr_H^K(f) := \sum_i f \mid_k a_i$, where $K = \sqcup H a_i$.

Although we study abstract Hecke algebras in the next section in more detail, we need to recall their definition in the case of automorphic forms here, in order to mention the Atkin's conjecture. For every $\sigma \in \mathrm{GL}(2,\mathbb{R})^+$, define the operator $T_\sigma^G : \mathfrak{F}_k^G \to \mathfrak{F}_k^G$ by $T_\sigma^G(f) := \sum_j (f \mid_k \sigma) \mid_k g_j$ where $G = \bigsqcup_{j=1}^{\mu(\sigma)} G_\sigma g_j$. In particular, for every $n \in \mathbb{N}$, $T_n^G := T^G_{\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)}$ is called the *Hecke* operator associated to n on the space of the G-automorphic functions.

When the (sub)group G is congruence, the action of Hecke operators is quite successfully used to understand the structure of $M_k(G)$ (and $S_k(G)$, the space of cusp forms), by Hecke [37] and Atkin and Lehner [2]. On the other hand, if G is not congruence, the Hecke operators act in a trivial way. More precisely, let $\hat{G}$ be the congruence closure of G in $\mathrm{PSL}(2,\mathbb{Z})$. Then we have

Conjecture 3.1.2. (Atkin) For every prime number p such that p dosen't divide the level (in the sence of Wohlfart [70]) of G, we have $T_p^G = T_p^{\hat{G}} \circ Tr_G^{\hat{G}}$.

Serre (Appendix to [64] proved this conjecture assuming $G \trianglelefteq \hat{G} = \mathrm{SL}(2,\mathbb{Z})$ and Berger [9] proved it for every finite index subgroup of $\mathrm{SL}(2,\mathbb{Z})$.

We are going to generalize this result in the following way: first by Eichler-Shimura correspondence of cusp forms and cohomology classes [62], instead of $S_k(G)$, we can consider the action of the Hecke operators on the first cohomology group of G with coefficient in a suitable G-module. Next one may want to replace the modular group $\mathrm{SL}(2,\mathbb{Z})$ or $\mathrm{PSL}(2,\mathbb{Z})$ with $\mathrm{PSL}(2,\mathcal{O}_{-d})$ for every square-free natural number d and ask wether a similar result holds for Hecke operators and trace maps between cohomology groups. This is the goal of this chapter, to show that this is true, even for higher cohomology groups. We start by recalling the definitions and basic properties of abstract Hecke algebras and their actions on the cohomology groups in the next section. Then, following the idea of Berger [9], we will prove a general result not only for every group $\mathrm{PSL}(2,\mathcal{O}_{-d})$, but also for all higher cohomology groups of it with coefficients in any G-module . This result is a special case of the theorem 3.5.6 which relates the Hecke operators corresponding to any pair $H \leq_f K \leq G$ of subgroups of an *arbitrary* group G satisfying certain conditions on the indices and the transfer map between respective cohomology groups.

3.2 Abstract Hecke algebras

In this section we recall the definitions and basic properties concerning abstract Hecke algebras, to give an idea of the nature of the Hecke operators. For more

details, see [43]. In this section, G will denote an arbitrary group and R a commutative ring wih unit element except otherwise is explicitly stated.

Definition 3.2.1. Two subgroups H_1, H_2 of G are called **commensurable** if their intersection $H_1 \cap H_2$ has finite index in both H_1, H_2.

Commensurability is an equivalence relation. For a subgroup H of G, we may ask whether all of its conjugates H^g for $g \in G$ are commensurable with H. This is of course not always the case, (see example 1, part 2) but we would like to consider the set of elements g for which this is true (we need it to define Hecke pairs), and give it a name:

Definition 3.2.2. Let $H \leq G$. We define the **commensurator** of H in G as:

$$CM_G(H) := CM(H) := \{g \in G \mid \ H^g \textit{ is commensurable with } H\}$$

It can be easily seen that $CM_G(H)$ is a subgroup of G containing the normalizer of H: $N_G(H) \leq CM_G(H)$.

Examples 1. ([43], chapter $1, 3.5$)

1. $CM_{\mathrm{SL}(2,\mathbb{Q})}(\mathrm{SL}(2,\mathbb{Z})) = \mathrm{SL}(2,\mathbb{Q})$.

2. $CM_{\mathrm{GL}(2,\mathbb{Q})}(\{\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right) \mid n \in \mathbb{Z}\}) = \{\left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right) \mid a, b, d \in \mathbb{Q},\ ad \neq 0\}$.

Let $H \leq G$ and S be a sub-semigroup of $CM(H)$ with $SH = HS = S$. Then (H, S) is called a **Hecke pair** in the group G and we define the R-module $L_R(H, S) = L(H; S)$ as the free R-module with basis $\{Hg \mid \ g \in S\}$. It has in fact a natural H-module structure defined via $(\Sigma r_i Hg_i) \cdot h := \Sigma r_i Hg_i h$, for every $r_i \in R$, $g_i \in S$, and $h \in H$.

Definition 3.2.3. For a Hecke pair (H, S) in G we define its R-**Hecke algebra** $\mathfrak{H}_R(H, S)$ as the (R- and H-) submodule of all H-invariant elements of $L_R(H, S)$:

$$\mathfrak{H}_R(H, S) = \mathfrak{H}(H, S) = \{u \in L(H, S) \mid \ uh = u \ \forall h \in H\}.$$

The multiplication of $\mathfrak{H}(H, S)$ is defined as follows: For $x = \Sigma r_i Hg_i$ and $y = \Sigma t_j Hk_j$ in $\mathfrak{H}(H, S)$, we define $x \cdot y := \Sigma\Sigma r_i t_j Hg_i k_j$.

Clearly for $H = 1$, $\mathfrak{H}_R(1,S)$ is just the semigroup-ring RS. Now suppose that (H,S) is a Hecke pair in G. For $x \in CM(H)$, H_x has finite index in H. So $\mu := \mu_H(x) = [H : H_x]$ is finite. Write H as a union of μ disjoint cosets of H_x, say $H = \bigsqcup_1^\mu H_x h_i$. It is easy then to check that $HxH = \bigsqcup_1^\mu Hxh_i$. Define $\underline{HxH} := \sum_1^\mu Hxh_i$. Then $\underline{HxH} \in \mathfrak{H}(H,S)$. If H is normal in G, then $CM(H) = G$, $H^x = H_x = H$ and $\mu(x) = 1$ for every $x,y,g \in G$. So $HxH = Hx = \underline{HxH} = Hx$. Hence $\mathfrak{H}(H,G)$ is just the group-ring $R\frac{G}{H}$ with the usual multiplication of group-rings.

The elements $\underline{HxH}$ for $x \in S$ make a basis for the R-module $\mathfrak{H}(H,S)$, as we see in the following theorem, in which we also formulate the product rule of $\mathfrak{H}(H,S)$ in terms of these basis elements. Define

$$\nu_x^y(g) :=\mid \{i \mid xh_i y \in HgH\} \mid \text{ and } \xi_x^y(g) = \nu_x^y(g)\mu(y)\mu(g)^{-1},$$

for every $g,x,y \in S$.

Theorem 3.2.4. For a Hecke pair (H,S) in G its R-Hecke algebra $\mathfrak{H}_R(H,S)$ is the free R-module with basis $\{\underline{HgH} \mid g \in S\}$. In terms of this basis, the multiplication of $\mathfrak{H}_R(H,S)$ can be expressed as:

$$\underline{HxH} \cdot \underline{HyH} = \Sigma \xi_x^y(g) \cdot \underline{HgH},$$

where g's come from a decomposition $HxHyH = \sqcup HgH$.

So we may suppress the underlines of the elements $\underline{HxH}$, considering $\mathfrak{H}_R(H,S)$ as the free R-module with basis $\{HgH \mid g \in S\}$ and the above multiplication. We cite one more fact about Hecke algebras here to give a better idea of their nature.

Lemma 3.2.5. Let (H,S) be a Hecke pair in G and $S^{-1} = \{x^{-1} \mid x \in S\}$. Then (H,S^{-1}) is also a Hecke pair and the R-module homomorphism $\mathfrak{H}(H,S) \to \mathfrak{H}(H,S)$ which sends HxH to $Hx^{-1}H$ is an anti-isomorphism of rings. In particular, if S is a group, then the above map is an anti-automorphism of the ring $\mathfrak{H}(H,S)$.

What makes Hecke algebras so interesting is that, as will we see in the following sections, the cohomology groups $H^*(H,A)$, (for every R and G-module A,) are $\mathfrak{H}_R(H,S)$-modules and in addition, the action of this algebra respects the standard constructions of homological algebra, see 3.5.3 and 3.5.4.

3.3 Group cohomology

Let G be a group, and let A be a left G-module. The cohomology of G with coefficients in A can be described using either homogeneous or non-homogeneous co-chains. Let $C^0(G,A) := A$ and, given a positive integer q, let $C^q(G,A)$ denote the group consisting of the A-valued functions $f : G^q \to A$ on the q-fold Cartesian product $G^q = G \times \cdots \times G$. Any such map is called a **non-homogeneous q-co-chain**. We then consider the map

$$\partial_q : C^q(G,A) \to C^{q+1}(G,A),$$

$$(\partial_q f)(g_1 \cdots g_{q+1}) :=$$

$$g_1 f(g_2, \cdots, g_{q+1}) + \sum_1^q (-1)^i f(g_1, \cdots, g_{i-1}, g_i g_{i+1}, \cdots, g_{q+1}) +$$

$$+(-1)^{q+1} f(g_1, \cdots, g_q)$$

and $(\partial_0 a)(g) := ga - g$, for all $g_1, \cdots, g_{q+1} \in G$ and $a \in A$.

Then we have $\partial_q \partial_{q-1} = 0$. The maps ∂ are called the **co-boundary maps** for non-homogeneous co-chains. The associated q-th cohomology group is given by

$$H^q(G,A) := Z^q(G,A)/B^q(G,A)$$

where $Z^q(G,A) := ke(\partial_q)$ and $B^q(G,A) := im(\partial_{q-1})$ and $H^0(G,M) := Z^0(G,A) = A^G$, the submodule of G-invariant elements of A. The elements of ($B^1(G,A)$ resp.) $Z^1(G,A)$ are also called ($inner-$ resp.) $derivations$.

Let $H \leq G$ and $g \in G$. We define the conjugation isomorphism c_g from the q-co-chain group $C^q(H,A)$ to $C^q(g^{-1}Hg,A)$ as follows:

$$c_g(f)(g^{-1}h_1g, \cdots, g^{-1}h_qg) := g^{-1}f(h_1, \cdots, h_q).$$

Clearly it is a chain map, that is, the following diagram commutes for every q:

$$\begin{array}{ccc} C^q(H,A) & \xrightarrow{\partial_q} & C^{q+1}(H,A) \\ \downarrow{\scriptstyle c_g} & & \downarrow{\scriptstyle c_g} \\ C^q(g^{-1}Hg,A) & \xrightarrow{\partial_q} & C^{q+1}(g^{-1}Hg,A) \end{array}$$

The map c_g induces an isomorphism $c_g^* : H^q(H,A) \to H^q(g^{-1}Hg,A)$. For every $u \in H^q(H,A)$, we define

$$u \cdot g := (c_g^*)(u) \in H^q(g^{-1}Hg,A). \tag{3.3.1}$$

We then have the following lemma:

Lemma 3.3.1. Let $H \leq G$ and $g \in G$. For every RG-module A and $q \in \mathbb{N}$, the following digram commutes:

$$\begin{array}{ccc} H^q(H, A) & \xrightarrow{-\cdot g} & H^q(H^g, A) \\ {\scriptstyle res}\downarrow & & \downarrow{\scriptstyle res} \\ H^q({}_gH, A) & \xrightarrow{-\cdot g} & H^q(H_g, A) \end{array}$$

Proof. Easy verification. □

For the sake of completeness, we also define the cohomology using the homogeneous co-chains: for any non-negative integer q, let $\mathfrak{C}^q(G, A) \leq C^{q+1}(G, A)$ be the subgroup consisting of those maps $f : G^{q+1} \to A$ such that

$$f(gg_0, \cdots, gg_q) = gf(g_0, \cdots, g_q)$$

for all $g, g_0, \cdots, g_q \in G$, the so called **homogeneous co-chains**. The co-boundary maps $\delta_q : \mathfrak{C}^q(G, A) \to \mathfrak{C}^{q+1}(G, A)$ are defined as follows:

$$(\delta_q f)(g_0, \cdots, g_{q+1}) := \sum_0^{q+1} (-1)^i f(g_0, \cdots, g_{i-1}, g_{i+1}, \cdots, g_{q+1})$$

and $(\delta_0 f)(g_0, g_1) := f(g_1) - f(g_0)$ for all $g_0, \cdots, g_{q+1} \in G$. Then for $q \geq 1$, the q-th cohomology group is given by

$$H^q(G, A) := ke(\delta_q)/im(\delta_{q-1}).$$

There is a $1-1$ correspondence between $\mathfrak{C}^q(G, A)$ and $C^q(G, A)$, for every $q \geq 1$, which is compatible with the co-boundary maps: Given $f \in C^q(G, A)$ and $\phi \in \mathfrak{C}^q(G, A)$, define

$$f_{\mathtt{H}}(g_0, \cdots, g_q) := g_0 f(g_0^{-1}g_1, g_1^{-1}g_2, \cdots, g_{q-1}^{-1}g_q),$$

$$\phi_{\mathtt{N}}(g_1, \cdots, g_q) := \phi(1, g_1, g_1g_2, \cdots, g_1g_2 \cdots g_q),$$

for all $g_0, \cdots, g_q \in G$. Extending linearly, we get the isomorphisms

$$(-)_{\mathtt{H}} : C^q(G, A) \to \mathfrak{C}^q(G, A), (-)_{\mathtt{N}} : \mathfrak{C}^q(G, A) \to C^q(G, A),$$

which are inverse of each other, and we have $(\partial f)_{\mathtt{H}} = \delta f_{\mathtt{N}}$ and $(\delta\phi)_{\mathtt{N}} = \partial\phi_{\mathtt{H}}$ for all $f \in C^q(G, A)$ and $\phi \in \mathfrak{C}^q(G, A)$, showing that the above two definitions for cohomology coincide.

3.4 Restriction and transfer maps on the cohomology groups

Given a subgroup $H \leq G$ and a G-module A, we know that there is a map $res^G_H : H^n(G,A) \to H^n(H,A)$ induced by the inclusion and called the **restriction** map. Let $H \leq G$ and $[G:H] = n < \infty$. We construct a map going in the other direction, the so called **transfer (or co-restriction) map**. Let $\{s_1, \dots, s_n\}$ be a transversal for the left cosets of H in G and write G as a disjoint union $G = \bigsqcup_1^n Hs_i$. For every left G-module A, there is a homomorphism $tr_{H,G} : A^H \to A^G$, defined via $tr(a) := \sum_1^n s_i a$, called the **transfer map**. This map can be extended uniquely to a map $tr^G_H : H^*(H,A) \to H^*(G,A)$, called also the transfer (or co-restriction) map. We give an explicit description of it: For every $x \in G$, let $\bar{x}$ be the unique element s_i with $x \in Hs_i$. So we have $x\bar{x}^{-1} \in H$. Now for every $k > 0$, $f : H^k \to A \in C^k(H,A)$, and $g_1, \dots g_k \in G$, we have

$$tr^G_H(f)[g_1, \dots, g_k] = \sum_1^n s_i^{-1} f[s_i g_1 \overline{(s_i g_1)}^{-1}, \dots, \overline{(s_i g_1 \dots g_{k-1})} g_k \overline{(s_i g_1 \dots g_k)}^{-1}].$$

This is the transfer (or co-restriction) map on co-chain groups relative to the given transversal. These maps do depend on the choices of the transversal (cf [15]). On the other hand, since a co-restriction map sends cocycles to cocycles and co-boundaries to co-boundaries, there is an induced map on cohomology groups, called transfer (or co-restriction) over cohomology groups, and it can be proved that this map is independent of the choice of the tranversal (see [15]). We denote it also by tr^G_H. The following proposition cites some of the main properties of the restriction and transfer maps. For a proof, see for example [13].

Proposition 3.4.1. Let $H, K \leq G$ with $[G:H] \leq \infty$, A any G-module, and $n \in \mathbb{N}$.

1. If $H \leq K$ then $tr^G_H = tr^G_K \circ tr^K_H$ and $res^G_H = res^K_H \circ res^G_H$.
2. For every $u \in H^n(G,A)$, we have $tr^G_H res^G_H(u) = [G:H]u$.
3. Wirte $G = \bigsqcup_1^m Hg_iK$. Then for every $u \in H^n(G,A)$,

$$res^G_K \circ tr^G_H(u) = \sum_1^m tr^K_{K \cap H^{g_i}} \circ res^{H^{g_i}}_{K \cap H^{g_i}}(ug_i).$$

3.5 The action of Hecke algebras on the cohomology groups

Let R be a commutative ring with unit and G be an arbitrary group. It is well known that for every left RG-module A and every Hecke pair (H,S) in G, there

is a natural right action of the Hecke algebra $\mathfrak{H}(H,S) = \mathfrak{H}_R(H,S)$ on the co-homology groups $H^*(H,A)$ defined in the following way: Let $x \in S$ and write H as a union of $\mu = \mu(x)$ disjoint cosets of H_x in H: $H = \bigsqcup_1^\mu H_x h_i$. It is easy then to check that $HxH = \bigsqcup_1^\mu Hx_i$, where $x_i := xh_i$. Since for every $y \in H$, $HxHy = HxH$, we have $HxH = \bigsqcup_1^\mu Hx_i = \bigsqcup_1^\mu Hx_i y$, so for every $1 \leq i \leq \mu$,

$$x_i y = t_i(y) x_{i(y)} \tag{3.5.1}$$

for a unique element $t_i(y) \in H$ and a unique index $i(y)$. So $(x_{1(y)} \cdots x_{\mu(y)})$ is a permutation of $(x_1 \cdots x_\mu)$. For each $y, y' \in H$, $(x_i y)y' = t_i(y)(x_{i(y)}y') = t_i(y)t_{i(y)}(y')x_{(i(y))(y')}$. On the other hand $x_i(yy') = t_i(yy')x_{i(yy')}$, so

$$i(yy') = (i(y))(y'), t_i(yy') = t_i(y)t_{i(y)}(y'). \tag{3.5.2}$$

Given a non-negative integer q and a left RG-module A, we define the action of HxH on a homogeneous co-chain $\phi \in \mathfrak{C}^q(H,A)$ as follows:

$$(\phi \bullet HxH)[y_0, \ldots, y_q] := \sum_1^\mu x_i^{-1} \phi[t_i(y_0), \ldots, t_i(y_q)],$$

for all $y_0, \cdots, y_q \in H$. It is known that $\phi \bullet HxH \in \mathfrak{C}^q(H,A)$ (see [45], 3.3). The induced map $\mathfrak{T}_x := \mathfrak{T}_x^H : \mathfrak{C}^q(H,A) \to \mathfrak{C}^q(H,A)$ is linear and independent of the choice of the coset decomposition of HxH. Moreover, $\mathfrak{T}_x \circ \delta_q = \delta_q \circ \mathfrak{T}_x$, so it in turn induces a homomorphism $\mathfrak{T}_x : H^q(H,A) \to H^q(H,A)$ which is called the Hecke operator on $H^q(H,A)$ corresponding to the double coset HxH.
The Hecke operators can also be described by non-homogeneous co-chains. For a non-homogeneous co-chain $f \in C^q(H,A)$ define ($q \geq 1$)

$$(f \cdot HxH)(y_1, \ldots, y_q) := \sum_1^\mu x_i^{-1} f[t_i(y_1), t_{i(y_1)}(y_2), t_{i(y_1 y_2)}(h_3) \ldots, t_{i(y_1 \cdots y_{q-1})}(y_q)], \tag{3.5.3}$$

for all $y_1, \cdots, y_q \in H$. Again it is known that $f \cdot HxH \in C^q(H,A)$ and the induced map $T_x := T_x^H : C^q(H,A) \to C^q(H,A)$ is linear, independent of the choice of the coset decomposition of HxH, and compatible with the co-boundary maps, inducing a homomorphism $T_x : H^q(H,A) \to H^q(H,A)$. It can be shown that $T_x(f) = (\mathfrak{T}_x f_{\mathrm{H}})_{\mathrm{N}}$ (see [45] prop. 3.3).

The following compact description of the Hecke operators is in some cases helpful:

Proposition 3.5.1. Consider an RG-module A and a Hecke pair (H,S) in G. Let $x \in S$. For every $u \in H^q(H,A)$, we have $T_x^H(u) = tr_{H_x}^H res_{H_x}^{H^x}(u \cdot x) =$

$tr^H_{H_x}(res^H_{{}_xH}(u)\cdot x)$, where $-\cdot x$ is as in the equation (3.3.1). In other words, the following diagram commutes:

$$\begin{array}{ccc} H^q(H,A) & \xrightarrow{T^H_x} & H^q(H,A) \\ {\scriptstyle res}\downarrow & & \uparrow{\scriptstyle tr} \\ H^q({}_xH,A) & \xrightarrow{-\cdot x} & H^q(H_x,A) \end{array}$$

Proof. We keep the above notations. Let $u=[f]$, where $f\in C^q(H,A)$ and suppose $y_1,\cdots,y_q\in H$ and $1\le i\le \mu$. We have $x_iy_1=t_i(y_1)x_{i(y_1)}$ so $t_i(y_1)=x_iy_1x^{-1}_{i(y_1)}=xh_iy_1h^{-1}_{i(y_1)}x^{-1}$. On the other hand, (using the over-line notation of the previous section) let $\overline{h_iy_1}=h_j$, so $h_iy_1=x^{-1}uxh_j$ for some $h\in H$. Thus $xh_iy_1=hxh_j$, that is, $x_{i(y_1)}=xh_j=x\overline{h_iy_1}$, $j=i(y_1)$, and

$$t_i(y_1)=h=xh_iy_1\overline{h_iy_1}^{-1}x^{-1}.$$

Similarly,

$$t_{i(y_1)}(y_2)=xh_{i(y_1)}y_2\overline{h_{i(y_1)}y_2}^{-1}x^{-1}=x_{i(y_1)}y_2\overline{h_{i(y_1)}y_2}^{-1}x^{-1}=x\overline{h_iy_1}y_2\overline{h_{i(y_1)}y_2}^{-1}x^{-1}.$$

Since $x_{i(y_1)}y_2=t_{i(y_1)}(y_2)x_{i(y_1)(y_2)}$, we have $h_{i(y_1)}y_2=x^{-1}t_{i(y_1)}(y_2)xh_{i(y_1)(y_2)}$, hence $\overline{h_{i(y_1)}y_2}=h_{i(y_1)(y_2)}=h_{i(y_1y_2)}=\overline{h_iy_1y_2}$. So

$$t_{i(y_1)}(y_2)=x\overline{h_iy_1}y_2\overline{h_iy_1y_2}^{-1}x^{-1}.$$

Continuing inductively, we see that

$$(f\cdot HxH)(y_1,\ldots,y_q):=\sum_1^\mu x_i^{-1}f[t_i(y_1),t_{i(y_1)}(y_2),t_{i(y_1y_2)}(h_3)\ldots,t_{i(y_1\cdots y_{q-1})}(y_q)]$$

$$=\sum_1^\mu h_i^{-1}x^{-1}f[xh_iy_1\overline{h_iy_1}^{-1}x^{-1},\cdots,x\overline{h_iy_1\cdots y_{q-1}}y_q\overline{h_iy_1\cdots y_q}^{-1}x^{-1}]$$

$$=(tr^H_{H_x}res^{H^x}_{H_x}(c_x(f)))(y_1,\cdots,y_q),$$

showing that $T^H_x(u)=tr^H_{H_x}res^{H^x}_{H_x}(ux)$. The other equality follows from lemma 3.3.1. □

Lemma 3.5.2. Let H be a normal subgroup of G and A be a G-module. Then for every $q\in\mathbb{N}$, $x\in G$ and every non-homogenous $f\in C^q(H,A)$, we have $\mu(x)=1$ and $(f\cdot HxH)(h_1,\cdots,h_q)=x^{-1}f(t_1(h_1),\cdots,t_1(h_q))$, for all $h_1,\cdots,h_q\in H$.

So far the cohomology groups $H^*(H,A)$ (for every R and G–module A), are $\mathfrak{H}_R(H,S)$–modules. What makes this action homologically interesting is that it respects the standard constructions of homological algebra. For example,

Proposition 3.5.3. ([1] Lemma 1.1.1) Consider a Hecke pair (H,S) in G and let $0 \to A \to B \to C \to 0$ be a short exact sequence of RG–modules. Then the long exact cohomology sequence

$$\cdots \to H^n(H,A) \to H^n(H,B) \to H^n(H,C) \to H^{n+1}(H,A) \to \cdots$$

is then an exact sequence of $\mathfrak{H}(H,S)$–modules, too.

We say that a Hecke pair (H',S') is **dominated** by another Hecke pair (H,S) in G, denoted by $(H',S') \preceq (H,S)$, if $H' \leq H$, $HS' = S$, and $H \cap S'S'^{-1} \subseteq H'$. In this case $\mathfrak{H}(H,S)$ embeds in $\mathfrak{H}(H',S')$ as a subalgebra via the restriction of the map $L(H,S) \to L(H',S')$ which sends $x \in L(H,S)$ to $\Sigma a_i H' g_i$, where $x = \Sigma a_i H g_i$, $g_i \in S'$ and for every (left or right) RG–module A we view the $\mathfrak{H}_R(H',S')$–modules $H^*(H',A)$ as $\mathfrak{H}_R(H,S)$–modules as well. Moreover,

Proposition 3.5.4. ([1] Lemma 1.1.3) With the above notations,

1. if A is a "right" RG–module, then the restriction map

$$res : H^n(H,A) \to H^n(H',A)$$

commutes with the action of $\mathfrak{H}_R(H,S)$.

2. if A is a "left" RG–module and $[H : H'] < \infty$, then the co–restriction map

$$cor : H^n(H',A) \to H^n(H,A)$$

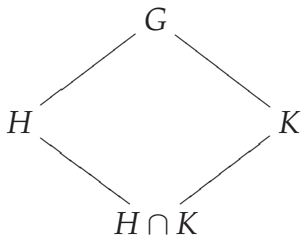
commutes with the action of $\mathfrak{H}_R(H,S)$.

It can be shown also that the Shapiro's lemma is compatible with the Hecke algebra action on the cohomology, see [1] lemma 1.1.4. For more details, see [44].

We now come back to our main task of this section, i.e. to provide the underlying group theoretic tool for our generalization of Atkin's conjecture. We need the following lemma, which will be useful later, specially in the proof of the 3.5.6, the main theorem of this section. It is known as Poincaré lemma:

Lemma 3.5.5. Let $H,K \leq G$. Then $[H : H \cap K] \leq [G : K]$ and if $G = HK$, then equality holds. Conversely, if we have the equality and $[G : K] < \infty$, then

$G = HK$.



The next theorem provides the group theoretic background for our generalization of Atkin's conjecture. If we apply it to a finite index subgroup of $\mathrm{PSL}(2, \mathcal{O}_{-d})$ and its congruence closure, then we get a generalization of Atkin's conjecture for Hecke operators acting on the cohomology groups (see the next section). Our proof is element-wise, as it is more convenient when one wants to make computer-aided calculations.

Theorem 3.5.6. Let $H \leq_f K \leq G$ and $g \in G$ be such that $\mu_H(g) < \infty$ and $K = (K_g)H$. Consider the following conditions:

1. $[K_g : H_g] = [K : H]^2$.
2. $K = H(K \cap {}^gH)$.
3. $[H \cap K^g : H_g] = [K : H]$.
4. For every G-module A and every $q \geq 1$ the following diagram commutes:

$$\begin{array}{ccc} H^q(H, A) & \xrightarrow{tr_H^K} & H^q(K, A) \\ {\scriptstyle T_g^H}\downarrow & & \downarrow{\scriptstyle T_g^K} \\ H^q(H, A) & \xleftarrow[res_H^K]{} & H^q(K, A) \end{array}$$

Then $1 \Leftrightarrow 2 \Leftrightarrow 3$ and $3 \Rightarrow 4$

Proof. The equivalence of $1, 2$ and 3 is easy to prove (see lemma 3.6.3 part 1). We start proving $3 \Rightarrow 4$. Let $\mu := \mu_H(g) = [H : H_g]$ and write $H = \bigsqcup_1^\mu H_g g_i$. Since $K = (K_g)H$, so $K_g g_i \subseteq K$ for every i and $K = \bigcup_1^\mu K_g g_i$. Without lose of generality, assume that $K = \bigsqcup_1^b K_g g_i$ where $b = [K : K_g]$, so

$$KgK = \bigsqcup_1^b Kgg_i. \tag{3.5.4}$$

For every $y \in K$, define $t_i(y)$ as the unique element of K such that $gg_i y = t_i(y)gg_{i(y)}$ for a unique index $i(y)$ (see equation (3.5.1)).

Write

$$H \cap K^g = \bigsqcup_1^m H_g h_j \tag{3.5.5}$$

where $m = [H \cap K^g : H_g]$. By assumption $m = [K : H]$. Since for every j, $gh_j g^{-1} \in K$ and $\{Hgh_j g^{-1} \mid 1 \leq j \leq m\}$ consists of exactly m disjoint co-sets, we see that

$$K = \bigsqcup_1^m Hgh_j g^{-1}. \tag{3.5.6}$$

For every $y \in K$, define $\bar{y}$ as the unique $gh_j g^{-1}$ such that $y \in Hgh_j g^{-1}$.

Since $b = [H : H \cap K^g]$ by 3.5.5, and $\{(H \cap K^g)g_i \mid 1 \leq i \leq b\}$ consists of exactly b disjoint co-sets, we have $H = \bigsqcup_1^b (H \cap K^g)g_i$ so by equation (3.5.5) $H = \bigsqcup_1^b \bigsqcup_1^m H_g h_j g_i$ hence

$$HgH = \bigsqcup_1^b \bigsqcup_1^m Hgh_j g_i = \bigsqcup_1^q \bigsqcup_1^m Hz_{(j,i)}, \tag{3.5.7}$$

where $z_{(j,i)} := gh_j g_i$. For every $x \in H$, define $t_{(j,i)}(x)$ as the unique element of H such that $z_{(j,i)}x = t_{(j,i)}(x)z_{(j,i)(x)}$, for a unique pair of indices $(j,i)(x)$ (see equation (3.5.1)).

We start with $q = 1$. Consider $[f] \in H^1(H, A)$ where $f \in C^1(H, A)$ is a derivation. We show that $(T_g^H f)(x) = T_g^K(tr_H^K(f))(x)$ for every $x \in H$. For every $x \in H$, we compute

$$(T_g^H f)(x) = (f \cdot HgH)(x) = \sum_{i=1}^b \sum_{j=1}^m (gh_j g_i)^{-1} f(t_{(j,i)}(x))$$

and

$$T_g^K(tr_H^K(f))(x) = (tr_H^K(f) \cdot KgK)(x) = \sum_{i=1}^b g_i^{-1} g^{-1} tr_H^K(f)(t_i(x)) =$$

$$\sum_{i=1}^b g_i^{-1} g^{-1} \sum_{j=1}^m (gh_j g^{-1})^{-1} f(gh_j g^{-1} t_i(x)(\overline{gh_j g^{-1} t_i(x)})^{-1}) =$$

$$\sum_{i=1}^b \sum_{j=1}^m g_i^{-1} h_j^{-1} g^{-1} f(w_{(j,i)}(x)),$$

where $w_{(j,i)}(x) := gh_jg^{-1}t_i(x)(\overline{gh_jg^{-1}t_i(x)})^{-1}$. We show that $w_{(j,i)}(x) = t_{(j,i)}(x)$. Clearly $w_{(j,i)}(x) \in H$. Note that $t_i(x)$ satisfies $gg_ix = t_i(x)gg_{i(x)}$, and $\overline{gh_jg^{-1}t_i(x)} = gh_kg^{-1}$ for some k, hence

$$gh_jg_ix = gh_jg^{-1}gg_ix = gh_jg^{-1}t_i(x)gg_{i(x)} =$$

$$gh_jg^{-1}t_i(x)(gh_kg^{-1})^{-1}(gh_kg^{-1})gg_{i(x)} = w_{(j,i)}(x)gh_kg_{i(x)},$$

so by definition of $t_{(j,i)}$,

$$w_{(j,i)}(x) = t_{(j,i)}(x) \text{ for every } x \in H, \tag{3.5.8}$$

and this finishes the case $q = 1$.

Let $q \geq 2$ and consider $[f] \in H^q(H, A)$ where $f \in C^q(H, A)$. We show that

$$(T_g^H f)(x_1, \cdots, x_q) = T_g^K(tr_H^K(f))(x_1, \cdots, x_q)$$

for every $x_1, \cdots, x_q \in H$. We have

$$(T_g^H f)(x_1, \cdots, x_q) = (f \cdot HgH)(x_1, \cdots, x_q)$$

$$= \sum_{i=1}^{b}\sum_{j=1}^{m}(gh_jg_i)^{-1}f(t_{(j,i)}(x_1), \cdots, t_{(j,i)(x_1\cdots x_{q-1})}(x_q)) \tag{3.5.9}$$

and

$$T_g^K(tr_H^K(f))(x_1, \cdots, x_q) = (tr_H^K(f) \cdot KgK)(x_1, \cdots, x_q) =$$

$$\sum_{i=1}^{b} g_i^{-1}g^{-1}tr_H^K(f)(t_i(x_1), \cdots, t_{i(x_1\cdots x_{q-1})}(x_q)) =$$

$$\sum_{i=1}^{b} g_i^{-1}g^{-1}\sum_{j=1}^{m}(gh_jg^{-1})^{-1}f(gh_jg^{-1}t_i(x_1)(\overline{gh_jg^{-1}t_i(x_1)})^{-1}, \cdots,$$

$$\overline{gh_jg^{-1}t_i(x_1)\cdots t_{i(x_1\cdots x_{q-2})}(x_{q-1})}t_{i(x_1\cdots x_{q-1})}(x_q)\overline{gh_jg^{-1}t_i(x_1)\cdots t_{i(x_1\cdots x_{q-1})}(x_q)}^{-1}) \tag{3.5.10}$$

Comparing the corresponding entries of f in equations (3.5.9) and (3.5.10) and recalling the equation (3.5.8), we see that it is enough to show that for every $2 \leq r \leq q$,

$$t_{(j,i)(x_1\cdots x_{r-1})}(x_r) =$$

$$\overline{gh_jg^{-1}t_i(x_1)\cdots t_{i(x_1\cdots x_{r-2})}(x_{r-1})}t_{i(x_1\cdots x_{r-1})}(x_r)\overline{gh_jg^{-1}t_i(x_1)\cdots t_{i(x_1\cdots x_{r-1})}(x_r)}^{-1}. \tag{3.5.11}$$

We prove this as follows. By equation (3.5.8),

$$w_{(j,i)}(x_1 \cdots x_r) = t_{(j,i)}(x_1 \cdots x_r).$$

Using equation (3.5.2), we get

$$t_{(j,i)}(x_1 \cdots x_r) = t_{(j,i)}(x_1) t_{(j,i)(x_1)}(x_2) t_{(j,i)(x_1x_2)}(x_3) \cdots t_{(j,i)(x_1 \cdots x_{r-1})}(x_r),$$

as well as

$$w_{(j,i)}(x_1 \cdots x_r) = gh_jg^{-1}t_i(x_1 \cdots x_r)\overline{(gh_jg^{-1}t_i(x_1 \cdots x_r))}^{-1} =$$

$$gh_jg^{-1}t_i(x_1) \cdots t_{i(x_1 \cdots x_{r-1})}(x_r)\overline{(gh_jg^{-1}t_i(x_1) \cdots t_{i(x_1 \cdots x_{r-1})}(x_r))}^{-1},$$

hence

$$t_{(j,i)}(x_1) t_{(j,i)(x_1)}(x_2) t_{(j,i)(x_1x_2)}(x_3) \cdots t_{(j,i)(x_1 \cdots x_{r-1})}(x_r) =$$

$$gh_jg^{-1}t_i(x_1) \cdots t_{i(x_1 \cdots x_{r-1})}(x_r)\overline{(gh_jg^{-1}t_i(x_1) \cdots t_{i(x_1 \cdots x_{r-1})}(x_r))}^{-1}. \tag{3.5.12}$$

Now we prove equation (3.5.11) by induction on $r \geq 2$. For $r = 2$, equation (3.5.12) reduces to

$$t_{(j,i)}(x_1) t_{(j,i)(x_1)}(x_2) = gh_jg^{-1}t_i(x_1)t_{i(x_1)}(x_2)\overline{(gh_jg^{-1}t_i(x_1)t_{i(x_1)}(x_2))}^{-1}.$$

Since $t_{(j,i)}(x_1)^{-1}gh_jg^{-1}t_i(x_1) = \overline{gh_jg^{-1}t_i(x_1)}$ (by the equation (3.5.8)), we have

$$t_{(j,i)(x_1)}(x_2) = \overline{gh_jg^{-1}t_i(x_1)}t_{i(x_1)}(x_2)\overline{(gh_jg^{-1}t_i(x_1)t_{i(x_1)}(x_2))}^{-1}.$$

Now assuming the equation (3.5.11) for any $s \leq r-1$, we have

$$\overline{gh_jg^{-1}t_i(x_1) \cdots t_{i(x_1 \cdots x_{r-2})}(x_{r-1})} =$$

$$t_{(j,i)(x_1 \cdots x_{r-2})}(x_{r-1})^{-1}\overline{gh_jg^{-1}t_i(x_1) \cdots t_{i(x_1 \cdots x_{r-3})}(x_{r-2})}t_{i(x_1 \cdots x_{r-2})}(x_{r-1}) =$$

$$\cdots =$$

$$t_{(j,i)(x_1 \cdots x_{r-2})}(x_{r-1})^{-1}t_{(j,i)(x_1 \cdots x_{r-3})}(x_{r-2})^{-1} \cdots$$

$$t_{(j,i)}(x_1)^{-1}gh_jg^{-1}t_i(x_1)t_{i(x_1)}(x_2) \cdots t_{i(x_1 \cdots x_{r-2})}(x_{r-1}).$$

Replacing this in the right hand side of the equation (3.5.11) and using the equation (3.5.12) we get

$$\overline{gh_jg^{-1}t_i(x_1)t_{i(x_1)}(x_2)\cdots t_{i(x_1\cdots x_{r-2})}(x_{r-1})}\cdot$$
$$t_{i(x_1\cdots x_{r-1})}(x_r)\overline{gh_jg^{-1}t_i(x_1)\cdots t_{i(x_1\cdots x_{r-1})}(x_r)}^{-1} =$$
$$t_{(j,i)(x_1\cdots x_{r-2})}(x_{r-1})^{-1}t_{(j,i)(x_1\cdots x_{r-3})}(x_{r-2})^{-1}\cdots$$
$$t_{(j,i)}(x_1)^{-1}[gh_jg^{-1}t_i(x_1)t_{i(x_1)}(x_2)\cdots t_{i(x_1\cdots x_{r-2})}(x_{r-1})\cdot$$
$$t_{i(x_1\cdots x_{r-1})}(x_r)\overline{gh_jg^{-1}t_i(x_1)\cdots t_{i(x_1\cdots x_{r-1})}(x_r)}^{-1}] =$$
$$t_{(j,i)(x_1\cdots x_{r-2})}(x_{r-1})^{-1}\cdots t_{(j,i)}(x_1)^{-1}[t_{(j,i)}(x_1)\cdots t_{(j,i)(x_1\cdots x_{r-1})}(x_r)] =$$
$$t_{(j,i)(x_1\cdots x_{r-1})}(x_r),$$

proving equation (3.5.11), which finishes the proof.

□

Corollary 3.5.7. Let $H \leq_f K \trianglelefteq G$ and $g \in G$ be such that $[H : H_g] = [K : H]$. Then for every G-module A and every $q \geq 1$ the following diagram commutes:

$$\begin{array}{ccc} H^q(H,A) & \xrightarrow{tr_H^K} & H^q(K,A) \\ {\scriptstyle T_g^H}\downarrow & & \downarrow{\scriptstyle T_g^K} \\ H^q(H,A) & \xleftarrow[res_H^K]{} & H^q(K,A) \end{array}$$

Corollary 3.5.8. Let $H \leq_f G$ and $g \in G$ be such that $[H : H_g] = [G : H]$. Then for every G-module A and every $q \geq 1$ the following diagram commutes:

$$\begin{array}{ccc} H^q(H,A) & \xrightarrow{tr_H^G} & H^q(G,A) \\ {\scriptstyle T_g^H}\downarrow & \swarrow{\scriptstyle res_H^G} & \\ H^q(H,A) & & \end{array}$$

3.6 Hecke operators for non-congruence subgroups

In this section we use Theorem 3.5.6 to prove a generalization of Atkin's conjecture for Hecke operators on the cohomology groups of $\Gamma_{-d} = \mathrm{PSL}(2, \mathcal{O}_{-d})$, (for all square free natural numbers d) with coefficients in any Γ_{-d}-module. We prove, in a sequence of lemmas, that if $H \leq_f \Gamma_{-d}$ is of level $\mathfrak{a} := \mathfrak{a}_H$, and $p \in \mathcal{O}_{-d}$ is

prime such that $\mathfrak{a} + p\mathcal{O}_{-d} = \mathcal{O}_{-d}$ Then for $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}(2, \mathbb{Q}(\sqrt{-d}))$, $H \leq \hat{H} \leq \Gamma_{-d}$ staisfy the conditions of 3.5.6. In this section, d will be a square free natural number.

We start with some technical elementary lemmas:

Lemma 3.6.1. Let $I \trianglelefteq \mathcal{O}_{-d}$ and $p \in \mathcal{O}_{-d}$ such that $I + p\mathcal{O}_{-d} = \mathcal{O}_{-d}$. Define $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}(2, \mathbb{Q}(\sqrt{-d}))$. Then

$$\Gamma(I) \cap \Gamma(p\mathcal{O}_{-d}) \subseteq \Gamma(I) \cap \Gamma(I)^g \cap {}^g\Gamma(I)$$

.

Proof. Suppose that $1 = v + o \cdot p$ with $v \in I, o \in \mathcal{O}_{-d}$.
Let $u \in \Gamma(I) \cap \Gamma(p\mathcal{O}_{-d})$, so we may write $u = \left(\begin{smallmatrix} a+1 & b \\ c & d+1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a'p+1 & b'p \\ c'p & d'p+1 \end{smallmatrix}\right)$, with $a, b, c, d \in I$ and $a', b', c', d' \in \mathcal{O}_{-d}$. So $u^g = \left(\begin{smallmatrix} a+1 & b/p \\ cp & d+1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a'p+1 & b' \\ c'p^2 & d'p+1 \end{smallmatrix}\right)$. Therefore we have $b/p = b' \in \mathcal{O}_{-d}$, so that $b' = vb' + ob \in I$. This shows that $u^g \in \Gamma(I)$, i.e. $u \in {}^g\Gamma(I)$. The inclusion $\Gamma(I) \cap \Gamma(p\mathcal{O}_{-d}) \subseteq \Gamma(I)^g$ is proved in a similar way.

□

Lemma 3.6.2. Let $f : X \to Y$ be a homomorphism between arbitrary groups X, Y. For every $H \leq K \leq Y$, we have $[f^{-1}(K) : f^{-1}(H)] \leq [K : H]$, and the equality holds if $K = H(K \cap f(X))$. Conversely, if $[K : H] < \infty$ and the equality holds, then $K = H(K \cap f(X))$. As a result, for every $M \leq_f X$, $[f(X) : f(M)] = [X : MKe(f)]$. In particular, $[f(X) : f(M)] \mid [X : M]$.

Proof. f induces an injection from the left cosets of $f^{-1}(H)$ in $f^{-1}(K)$ into the left cosets of H in K by assigning each $xf^{-1}(H)$ to $f(x)H$. It is onto if and only if $K = H(K \cap f(X))$. Now if $[K : H] < \infty$ and the equality holds, then this map is onto and hence $K = H(K \cap f(X))$. Finally for $M \leq_f X$, just put $H = f(M)$, $K = f(X)$. □

Lemma 3.6.3. For any element g of a group G and any subgroups $H \leq_f K \leq G$, we have

1. $[H \cap K^g : H \cap H^g] \leq [K : H]$, equality holds if and only if $K = H(K \cap {}^gH)$.

2. If $K = NH$ for some $N \leq K$, then in (1) equality holds if and only if $N \subseteq H(K \cap {}^gH)$.

3. Let $g \in G$ and $H, N \leq K \leq S \leq G$ with $K = NH$. Set $H_1 := N \cap H_S$, where H_S denotes the normal core of H in S. If $[H_1 \cap N^g : H_1 \cap H_1^g] = [N : H_1]$, then $[H \cap K^g : H \cap H^g] = [K : H]$.

Proof. For (1), consider the map $f = {}^g(-)\,|_H \colon H \to G$. Clearly $f^{-1}(K) = H \cap K^g$ and $f^{-1}(H) = H \cap H^g$, so we are done by 3.6.2. The proofs of $(2), (3)$ are straightforward.

□

Let $g \in G$ and $H \leq K \leq G$. define $\pi, \pi_g : K \cap K^g \to H\backslash\backslash K := \{Hx \mid x \in K\}$ by $\pi(x) := Hx$ and $\pi_g(x) := H({}^g x)$. The function

$$(\pi, \pi_g) : K \cap K^g \to H\backslash\backslash K \times H\backslash\backslash K,$$

is called (π, π_g) for $H \leq K$. If $H \trianglelefteq K$, then π and π_g are homomorphisms with $ke(\pi) = H \cap K^g$ and $ke(\pi_g) = H^g \cap K$ and hence $ke(\pi, \pi_g) = ke(\pi) \cap ke(\pi_g) = H \cap H^g$. In this case (π, π_g) is onto if and only if $[H \cap K^g : H \cap H^g] = [K : H]$.

Lemma 3.6.4. Let $H \leq_f K \leq G$. For any $g \in G$, if the map (π, π_g) is onto then $[H \cap K^g : H \cap H^g] = [K : H]$.

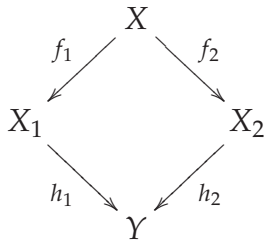
Proof. Let (π, π_g) be onto, and consider an element $x \in K$. So there exists $y \in K \cap K^g$ with $(\pi, \pi_g)(y) = (H, Hx)$, that is, $y \in H$ and $x = h({}^g y)$ for some $h \in H$. So $x \in H(K \cap {}^g H)$. Hence by 3.6.3 part 1, $[H \cap K^g : H \cap H^g] = [K : H]$. □

Lemma 3.6.5. Let $H, N \leq K \leq S \leq G$ with $K = NH$, $[K : H] < \infty$ and $H_1 := N \cap H_S$. For any $g \in G$, if (π, π_g) for (H_1, N) is onto, then $[H \cap K^g : H \cap H^g] = [K : H]$.

Proof. Immediate from previous lemma and part 3 of 3.6.3. □

Finally we need the following lemma:

Proposition 3.6.6. Suppose X, X_1, X_2 are arbitrary groups with epimorphisms $X_1 \overset{f_1}{\twoheadleftarrow} X \overset{f_2}{\twoheadrightarrow} X_2$. If $X \xrightarrow{(f_1, f_2)} X_1 \times X_2$ is not surjective, then there exist a group $Y \neq 1$ and epimorphisms $X_1 \overset{h_1}{\twoheadrightarrow} Y \overset{h_2}{\twoheadleftarrow} X_2$ such that $h_1 f_1 = h_2 f_2$, i.e. the following diagram commutes:



Proof. Let $N_i := Ke(f_i)$ and put $Y := X/(N_1N_2)$. Define $h_i(f_i(x)) := xN_1N_2$ and note that $Y \neq 1$ as (f_1, f_2) is not onto. □

Now we can show that for every finite index subgroup H of Γ_{-d}, its congruence closure, and special elements $g \in PGL(2,\mathbb{C})$, the conditions of 3.5.6 are satisfied:

Proposition 3.6.7. Let $p \in \mathcal{O}_{-d}$ be prime, and define $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G := \mathrm{PGL}(2, \mathbb{Q}(\sqrt{-d}))$. Consider $H \leq_f \Gamma_{-d}$ of level $\mathfrak{a} := \mathfrak{a}_H$, and assume $\mathfrak{a} + p\mathcal{O}_{-d} = \mathcal{O}_{-d}$. Let $\hat{H}$ be the congruence closure of H in Γ_{-d}. then

$$[H \cap \hat{H}^g : H \cap H^g] = [\hat{H} : H].$$

Proof. Set $H_1 := H_{\Gamma_{-d}} \cap \Gamma(\mathfrak{a})$, where $H_{\Gamma_{-d}}$ is the normal core of H in Γ_{-d}. Then $\hat{H} = \Gamma(\mathfrak{a})H$ (2.4.5 part 1) and as $\mathfrak{a}_{H_1} = \mathfrak{a}$, $\hat{H}_1 = \Gamma(\mathfrak{a})$ (2.4.5 part 2). If the map (π, π_g) for $H_1 \leq N := \Gamma(\mathfrak{a})$ is onto, then by 3.6.5 we are done. First we show that both π and π_g are onto:
Consider the canonical surjections $\pi_1 : N \twoheadrightarrow N/H_1$ and $\pi_2 : N \twoheadrightarrow N/(N \cap \Gamma(p\mathcal{O}_{-d}))$ and let $\psi := (\pi_1, \pi_2) : N \to N/H_1 \times N/(N \cap \Gamma(p\mathcal{O}_{-d}))$. If ψ is not onto, then by 3.6.6 there exist a group $T \neq 1$ and $N/H_1 \overset{k_1}{\twoheadrightarrow} T \overset{k_2}{\twoheadleftarrow} N/(N \cap \Gamma(p\mathcal{O}_{-d}))$ such that $k_1\pi_1 = k_2\pi_2$. Suppose $T = N/W$, where $W := ke(k_1\pi_1)$. Since $T \neq 1$, $H_1 \subseteq W \subsetneq N$, and as N is the congruence closure of H_1, therefore W is not congruence. But $N \cap \Gamma(p\mathcal{O}_{-d}) \subseteq W$, contradiction. Hence ψ is onto. Now for $s \in N/H_1$, there exists $t \in N$ such that $\psi(t) = (s,1) = (H_1t,\ (N \cap \Gamma(p\mathcal{O}_{-d}))t\ )$, that is $t \in N \cap \Gamma(p\mathcal{O}_{-d})$ and $s = H_1t$. Now by 3.6.1 $N \cap \Gamma(p\mathcal{O}_{-d}) \subseteq N \cap N^g$, which implies that $\pi(t) = H_1t = s$, i.e. π is onto. On the other hand $N \cap \Gamma(p\mathcal{O}_{-d}) \subseteq N \cap {}^gN$ (again by 3.6.1), implying $t^g \in N \cap {}^gN$, hence $\pi_g(t^g) = H_1({}^g(t^g)) = H_1t = s$, so π_g is also onto.
Now contrarily assume that (π, π_g) for $H_1 \leq N$ is not onto. Then by 3.6.6 there exist a group $Y \neq 1$ and epimorphisms $N/H_1 \overset{h_1}{\twoheadrightarrow} Y \overset{h_2}{\twoheadleftarrow} N/H_1$ such that $h_1\pi = h_2\pi_g$. Now define $F_1 : N \to Y$ and $F_2 : N^g \to Y$ by $F_1(x) := h_1(H_1x)$ and $F_2(x) := h_2(H_1 \cdot {}^gx)$. Clearly $F_1 \mid_{N \cap N^g} = F_2 \mid_{N \cap N^g}$. So we have a map

$$F : N *_{N \cap N^g} N^g \to Y$$

such that $F \mid_N = F_1$ and $F \mid_{N^g} = F_2$. Hence $[N *_{N \cap N^g} N^g : ke(F)] \leq \mid Y \mid \leq [N : H_1] < \infty$ and $[N : N \cap Ke(F)] = \mid Y \mid \geq 1$. So $H_1 \subseteq N \cap ke(F) \subsetneq N$, but N is the congruence closure of H_1, therefore $N \cap ke(F)$ cannot be congruence. Hence by 2.3.11 $ke(F)$ is a non-congruence subgroup of $N *_{N \cap N^g} N^g$ of finite index, contradicting 2.6.8. □

Now we sum up what we have proved so far in this section to prove:

Theorem 3.6.8. Let $H \leq_f \Gamma_{-d} = \mathrm{PSL}(2, \mathcal{O}_{-d})$ (d any square-free natural number) be of level $\mathfrak{a} := \mathfrak{a}_H$, and $\hat{H}$ be its congruence closure. Suppose that $p \in \mathcal{O}_{-d}$ is prime and $\mathfrak{a} + p\mathcal{O}_{-d} = \mathcal{O}_{-d}$ and define $g := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}(2, \mathbb{Q}(\sqrt{-d}))$. Then for every Γ_{-d}-module M and every $q \geq 1$ the following diagram commutes:

$$\begin{array}{ccc} H^q(H, M) & \xrightarrow{tr_H^{\hat{H}}} & H^q(\hat{H}, M) \\ \Big\downarrow{\scriptstyle T_g^H} & & \Big\downarrow{\scriptstyle T_g^{\hat{H}}} \\ H^q(H, M) & \xleftarrow[res_H^{\hat{H}}]{} & H^q(\hat{H}, M) \end{array}$$

Proof. $\hat{H}_g$ is congruence by 3.6.1 and 2.3.8 part 3. Hence by 2.4.5 we have $\hat{H} = (\hat{H}_g)H$. Now using 3.6.7 and 3.5.6 we are done. □

Remark 3.6.9. Note that since the virtual cohomological dimension of a Bianchi group is two, the most interesting cases of these results are for $q = 1, 2$.

Remark 3.6.10. One application of Theorem 3.6.8 is in the theory of Bianchi modular forms for imaginary quadratic fields of class number one.The Eichler-Shimura-Harder correspondence (see [35]) allows us to see these forms as classes in the cohomology of finite index subgroups of Bianchi groups. Theorem 3.6.8 can be used to deduce that Hecke action on Bianchi modular forms for a non-congruence subgroup of a Bianchi group is essentially the same as the Hecke action on Bianchi modular forms for its congruence closure.

Bibliography

[1] A. Ash and G. Stevens, Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues, Journal für die reine und angewandte Mathematik (Crelles Journal) (1986), no. 365, 192--220.

[2] A. O. L. Atkin and J. Lehner, New forms on $\gamma_0(m)$, Math. Ann. **185** (1970), 134--160.

[3] M. Baker, Link complements and integer rings of class number greater than one, Proceedings of the research semester in Low Dimensional Topology at Ohio State University, Walter de Gruyter, Berlin, New York, 1992, pp. 55--59.

[4] _____, Link complements and the Bianchi modular groups, Trans. Amer. Math. Soc. **353** (2001), no. 8, 3229--3246.

[5] _____, All links are sublinks of arithmetic links, Pacific J. Math. **203** (2002), no. 2, 257--263.

[6] H. Bass, Algebraic K-theory, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[7] H. Bass, M. Lazard, and J. P. Serre, Sous-groupes d'indice fini dans $SL(n, Z)$, Bull. Amer. Math. Soc **70** (1964), 385--392.

[8] H. Bass, J. Milnor, and J. P. Serre, Solution of the congruence subgroup problem for $SL_n(n \geq 3)$ and $Sp_{2n}(n \geq 2)$, Publications mathématiques de l'I.H.É.S. **33** (1967), 59--137.

[9] G. Berger, Hecke operators on noncongruence subgroups, C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 9, 915--919.

[10] L. Bianchi, Geometrische Darstellung der Gruppen linearer Substitutstionen mit ganzen complexen Coeffizienten nebst Anwendungen auf die Zahlentheorie, Math. Ann. **38** (1891), 313--333.

[11] _____, Sui gruppi di sostituzioni con coefficienti appartenenti a corpi quadratici imaginari, Math. Ann **40** (1892), 332--412.

[12] J. Britto(Bombay), On the construction of non-congruence subgroups, Acta Arith. **33** (1977), 261--267.

[13] K. S. Brown, Cohomology of groups, 2nd ed. corr. priniting ed., Springer-Verlag New York, 1994.

[14] F. Calegari and B. Mazur, Nearly ordinary galois deformations over arbitrary number fields, Journal of the Inst. of Math. Jussieu **8** (2009), no. 1, 99--177.

[15] E. Choi, Cohomology of groups and transfer theorem, J. Korean Math. Soc. **34** (1997), no. 2, 383--393.

[16] P. M. Cohn, On the structure of the GL_2 of a ring, Publ. I. H. E. S. **30** (1966), 5--53.

[17] _____, A presentation for SL_2 for Euclidean quadratic imaginary number fields, Mathematika **15** (1968), 156--163.

[18] J. E. Cremona, Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields, Compositio Math **51** (1984), 275--323.

[19] R. K. Dennis, The GE_2 property for discrete subrings of $\mathbb{C}$, Proc. AMS, **50** (1975), 77--82.

[20] L. E. Dickson, Algebren und ihre Zahlentheorie, pp. 150--151, Zurich and Leipzig, 1927.

[21] J. Dieudonné, La géométrie des groups classique, Springer, 1963.

[22] G. Dresden and W.M. Dymàček, Finding factors of factor rings over the gaussian integers, American Mathematical Monthly (2005), no. 112, 602 -- 611.

[23] B. Fine, The structure of $PSL_2(R)$, Ann. Math. Study **79** (1974), 145--170.

[24] _____, The Euclidean Bianchi groups, Comm Alg **18** (1990), no. 8, 2461--2484.

[25] B. Fine and M. Newman, The normal subgroup structure of the Picard group, Trans. Amer. Math. Soc **302** (1987), no. 2, 769--786.

[26] T. Finis, F. Grunewald, and P. Tirao, The cohomology of lattices in $\mathrm{SL}(2,\mathbb{C})$, Experiment. Math. **19** (2010), no. 1, 29--63.

[27] E. Ghate, Critical values of the twisted tensor l-function in the imaginary quadratic case, Duke Math. J. **96** (1999), no. 3, 595--638.

[28] F. Grunewald, H. Helling, and J. Mennicke, SL_2 over complex quadratic number fields I, Algebra i Logica **17** (1978), 512--580.

[29] F. Grunewald and J. Mennicke, $SL_2(O)$ and elliptic curves, University of Bielefeld, 1978.

[30] F. Grunewald and J. Schwermer, A non-vanishing theorem for the cuspidal cohomology of SL_2 over imaginary quadratic integers, Math. Ann. **258** (1981), 183--200.

[31] ———, Subgroups of Bianchi groups and arithmetic quotients of hyperbolic 3-space, Trans. Amer. Math. Soc. **335** (1993), no. 1, 47--78.

[32] ———, On the concept of level for subgroups of SL_2 over arithmetic rings, Israel J. Math. **114** (1999), no. 1, 205--220.

[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] G. Harder, Period integrals of Eisenstein cohomology classes and special values of some L-functions, Number theory related to Fermat's last theorem, Progress in Math. vol. 26 Birkhäuser Stuttgart and Basel pp 103-142, 1982.

[35] ———, Eisenstein cohomology of arithmetic groups. The case GL_2, Inventiones Mathematicae **89** (1987), 37--118.

[36] A. Hatcher, Hyperbolic structures of arithmetic type on some link complements, J. London Math. Soc. **27** (1983), no. 2, 345--355.

[37] E. Hecke, Mathematische werke, Vandenhoeck und Ruprecht, Götingen, 1959.

[38] G. Humbert, Sur la reduction des formes d'Hermite dans un corps quadratique imaginaire, C.R. Acad. Sci. Paris **161** (1915), 409--455.

[39] K. Ireland and M. Rosen, A classical introduction to modern number theory, 2nd ed. 1990. corr. 5th printing ed., Springer, 1998.

[40] J. Kim, Classifying quadratic number fields up to Arf equivalence, a dissertation submitted to the graduate faculty of the Louisiana, Jan 2006.

[41] F. Klein, Zur Theorie der elliptischen Modulfunktionen, Math. Ann. **17** (1880), 62--67.

[42] A.W. Knapp, Advanced algebra, Birkhäuser, 2007.

[43] A. Krieg, Hecke algebras, Mem. Amer. Math. Soc **87** (1999), no. 435.

[44] M. Kuga, W. Parry, and C.-H. Sah, Group cohomology and Hecke operators, Manifolds and Lie groups, progress in Mathematics (Y. Matsushima and J. Hano, eds.), vol. 14, Birkhäuser Boston, 1981, pp. 223--266.

[45] M. Lee, Hecke operators on cohomology, Rev. Uni. Math. Argentina **50** (2009), no. 1, 99--144.

[46] L. Long, Finite index subgroups of the modular group and their modular forms, arXive (2007).

[47] W. Magnus, Non-euclidean tesselations and their groups, Academic Press, New York and London, 1974.

[48] A. W. Mason, Anomalus normal subgroups of $SL_2(K[x])$, Quart. J. Math. Oxford **36** (1985), no. 2, 345--358.

[49] A.W. Mason, Congruence hulls in SL_n, J. pure and applied algebra **89** (1993), 255--272.

[50] J. Mennicke, Finite factor groups of the unimodular group, Annals of Math. **81** (1965), no. 1, 31--37.

[51] J. Milnor, Hyperbolic geometry: The first 150 years, Bull. Amer. Math. Soc **6** (1982), no. 1, 9--24.

[52] J. Neukirch, Algebraic number theory, Springer-Verlag New York, 1999.

[53] E. Picard, Sur un groupe de transformations des points de l'espace situé de même côté d'un plan, Bull. Soc. Math. France **12** (1884), 43--47.

[54] A.W. Ried, Arithmeticity of knot complements, J. London Math. Soc. **43** (1991), no. 2, 171--184.

[55] R. Riley, A quadratic parabolic group, Math. Proc. Cambridge Philos. Soc. **77** (1975), 281--288.

[56] _____, Applications of a computer implementation of Poincaré 's theorem on fundamental polyhedra, Math. Comp. **40** (1983), 607--632.

[57] A. J. Scholl, Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences, Inventiones Mathematicae (1985), no. 79, 49--77.

[58] J. Schwermer, A note on link complements and arithmetic groups, Math. Ann. **249** (1980), 107--110.

[59] R. M. Scrath, Normal congruence subgroups of Bianci groups, Ph.D. thesis, Faculty of science at the university of Glasgow, 2003.

[60] J. P. Serre, Le problème des groupes de congruence pour SL_2, Annals of Math. **92** (1970), no. 3, 489--527.

[61] _____, Trees, Springer, 1980.

[62] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten, Publishers and Princeton University Press, 1971.

[63] R. G. Swan, Generators and relations for certain special linear groups, Adv. in Math. **6** (1971), 1--77.

[64] J.G. Thompson, Hecke operators and noncongruence subgroups, Group theory (Singapore 1987), pp. 215--224, de Gruyter, Berlin, 1989.

[65] W. P. Thurston, The geometry and toplology of 3-manifolds, Lecture notes, Princeton Univ. Press, N. J., 1978.

[66] _____, Three dimensional manifolds, Kleinian groups and hyperbolic geometry, Bull. Amer. Math. Soc (N. S.) **6** (1982), 357--381.

[67] K. Vogtmann, Rational homology of Bianchi groups, Math. Ann. **272** (1985), 399--419.

[68] N. Wielenberg, The structure of certain subgroups of the picard group, Math. Proc. Cambridge Philos. Soc. **84** (1978), 427--436.

[69] K. Wohlfahrt, Über dedekindsche Summen und Untergruppen der Modulgrupe, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **23** (1959), 5--10.

[70] _____, An extension of F. Klein's level concept, Illinois J. Math. **8** (1964), 529--535.

Index