An Approach to the Congruence Subgroup Problem via Fractional Weight Modular Forms

by

Daniel Cameron Ellam

A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy

Department of Mathematics

University College London

July 2013

Declaration

I, Daniel Cameron Ellam, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Signed

Abstract

In this thesis we develop a new criterion for the congruence subgroup problem in the case of arithmetic groups of $\mathrm{SU}(2,1)$, which in principle can be checked using a computer. Our main theorem states that if there exists a prime $q > 3$ and a congruence subgroup $\Gamma' \subset \mathrm{SU}(2,1)(\mathbb{Z})$ such that the restriction map $H^2(\mathrm{SU}(2,1)(\mathbb{Z}), \mathbb{F}_q) \to H^2(\Gamma', \mathbb{F}_q)$ is not injective, then the congruence kernel of $\mathrm{SU}(2,1)$ is infinite.

Supervisor: Dr. Richard Hill

Acknowledgements

First and foremost I would like to thank my supervisor Dr Richard Hill for his continued support, attention and patience. Without his guidance and knowledge, this work would not have been possible. I wish to express my gratitude to my family and friends for their support and encouragement, and to my colleagues within the UCL Mathematics department. I would also like to thank EPSRC who have funded me during my research.

I came to UCL as a student hoping to fulfil an academic ambition, and after four years it has allowed me to achieve this and so much more. London has provided me with experiences on which I've built my present and future. Intertwined with those who have come into my life and left it, I will be forever grateful to each for having made this an adventure that will stay with me for the rest of my life.

Contents

Declaration i

Abstract ii

Acknowledgements iii

Introduction 1

1 Definitions and Preliminary Material 6

1.1 SU(2, 1) Defined Over A Field 7

1.2 The Lie Algebra and the Bruhat Decomposition 11

1.3 Arithmetic Subgroups and the Adele Group 17

1.4 The Congruence Subgroup Problem 19

1.4.1 The Classical Formulation 19

1.4.2 Congruence Subgroup Problem for SU(2, 1) 24

1.5 An Approach to the Congruence Subgroup Problem 27

1.5.1 Fractional Weight Forms on SU(2, 1) 27

1.5.2 Metaplectic Covers 31

1.5.3 A Motivational Example 41

2 Generalising Deligne's Theorem **43**

2.1 Some Homological Algebra . . . 44

2.1.1 Technical Results . . . 44

2.1.2 A Result Involving $H^2(V, \mathbb{F}_p)$ . . . 56

2.2 Calculating $H^2(K_f, \mathbb{Z}/q\mathbb{Z})$ . . . 60

2.3 p Split in k . . . 62

2.3.1 $H^1(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$ . . . 62

2.3.2 $H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$, $p \neq q$ . . . 63

2.3.3 $H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_p)$ . . . 71

3 Low Dimensional Cohomology of $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ with p Inert **90**

3.1 $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q)$ . . . 91

3.2 $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q)$ . . . 99

3.2.1 $H^2(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathbb{F}_q)$ . . . 99

3.2.2 $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p)$ . . . 100

4 Low Dimensional Cohomology of $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ with p Ramified **112**

4.1 Initial Results . . . 113

4.2 $H^i(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q)$ for $i = 1, 2$ . . . 117

4.3 $H^i(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p)$ for $i = 1, 2$ . . . 122

Conclusions **135**

Bibliography **139**

Introduction

The *congruence subgroup problem* (CSP) has been studied and is understood for a number of groups. For the group $\mathrm{SL}_2(\mathbb{Z})$, the classical formulation of the CSP is as follows. We define a *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ to be a subgroup containing the kernel of the homomorphism

$$\ker\left(\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right),$$

for N a positive integer. While it is clear that such a subgroup has finite index in $\mathrm{SL}_2(\mathbb{Z})$, the CSP for $\mathrm{SL}_2(\mathbb{Z})$ turns this around and asks if every subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup. It was known to Felix Klein that the congruence subgroup problem has a negative solution for $\mathrm{SL}_2(\mathbb{Z})$ and in fact there are infinitely many non-congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. If we define $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $\Gamma(N) = \ker\left(\Gamma \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right)$, then we can explicitly construct a non-congruence subgroup as in Section 3.4, [30] as follows; let $\Gamma^{'}$ be the subgroup of Γ generated by the matrices $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. Then Γ' is a free group and has index 2 in $\Gamma(2)$. Thus there exists a surjective homomorphism E_A from Γ' to $\mathbb{Z}$ which we construct by taking a word $w \in \Gamma'$ and defining $E_A(w) : \Gamma' \longrightarrow \mathbb{Z}$ to be the sum of the exponents of A in w. Define

$$\Gamma_l = \left\{ g \in \Gamma' : E_A(g) \equiv 0 \mod l \right\},$$

for $l > 0$. Then Γ_l is not a congruence subgroup if l is not a power of 2 (see Section 3.4, [30]).

In contrast to the negative solution for $\mathrm{SL}_2(\mathbb{Z})$, Bass, Lazard and Serre showed in [1] that $\mathrm{SL}_n(\mathbb{Z})$ has a positive solution for $n \geq 3$. However, it was the reformulation of the CSP by Bass, Milnor and Serre in [2] through the introduction of the *congruence kernel* that provided a greater understanding of the CSP. This more precise reformulation gives a means of measuring the deviation of the CSP from a positive solution.

The study of the congruence kernel led to the solution of the CSP for many groups. When G is an absolutely simple, simply connected k-group, Serre conjectured in [28] the following claim regarding the congruence kernel, which became known as the *congruence subgroup conjecture*;

Conjecture. (Congruence Subgroup Conjecture) *Let G be an absolutely simple,* *simply connected k-group. Denoting the congruence kernel by* $\mathrm{Cong}_S(G)$*, then*

(i) if $rk_S(G) \geq 2$ *and* $rk_{k_\mathfrak{p}}(G) > 0$ *for all* $\mathfrak{p} \in S \setminus V_\infty$*, then* $\mathrm{Cong}_S(G)$ *is finite, and*

(ii) if $rk_S(G) = 1$ *then* $\mathrm{Cong}_S(G)$ *is infinite.*

This conjecture is now known for many groups and the current status of the CSP can be summarised by the following theorem (Section 6.7, [30]).

Theorem. *Let k be an algebraic number field and G be a simple, simply-connected k-group of one of the following types: B_n $(n \geq 2)$, C_n $(n \geq 2)$, D_n $(n \geq 5)$, E_7, E_8, F_4, G_2 or a special unitary group* $\mathrm{SU}_m(f)$ $(m \geq 4)$ *of a nondegenerate hermitian form f over either a quadratic extension L/k or a quaternion division algebra D/L with an involution of the second kind. Suppose that $rk_S(G) \geq 2$ and if G is F_4, there is a place $\mathfrak{p} \in S$ such that $rk_{k_\mathfrak{p}}(G) \geq 2$ and if G is of type C_3, then either $S \setminus V_\infty$ is nonempty, or there exists $\mathfrak{p} \in V_\infty$ such that $rk_{k_\mathfrak{p}}(G) \geq 2$. Then* $\mathrm{Cong}_S(G)$ *is central.*

The centrality of the congruence kernel $\mathrm{Cong}_S(G)$ is relevant since when this can be shown, we can relate $\mathrm{Cong}_S(G)$ to the metaplectic kernel and whilst the centrality of $\mathrm{Cong}_S(G)$ is not complete in all cases, the computation of the metaplectic kernel is (see Section 4.9, [30]). We also note however that the CSP is still unknown in a number of cases, including certain special unitary groups of the second kind, which we describe next. The aim of this thesis is to develop a new approach to the congruence subgroup problem and demonstrate its application through the special unitary group $\mathrm{SU}(2,1)$.

To describe the two different kinds of special unitary group, as in [3] we fix a totally real number field F, a quadratic extension E of F with no real embeddings and let $x \mapsto \overline{x}$ denote the non-trivial field automorphism of E/F. We have two ways of constructing the special unitary group. Take D to denote a central simple algebra over E of dimension 9 and $\iota : D \longrightarrow D$ an involution of the second kind, signifying that ι restricts to $x \mapsto \overline{x}$ on E. If in particular $D = M_3(E)$, then there exists a matrix $J \in \mathrm{GL}_3(E)$ such that $\overline{J} = J^t$ and $\iota(g) = J^{-1}\overline{g}^t J$. Given this, we can define a unitary group $\mathrm{U}_\iota(F) = \{g \in M_3(E) : \iota(g)g = Id\}$. The unitary group constructed this way is said to be of *the first kind*. If D is not $M_3(E)$, it must be a division algebra and the corresponding unitary group is said to be of *the second kind*. Whilst we will be primarily interested in the special unitary group $\mathrm{SU}(2,1)$ of the first kind, we explicitly construct a special unitary group of the second kind and describe the relevance of the results in this thesis to such groups in the Conclusions.

The congruence kernel for special unitary groups of the first kind is already known to be infinite, as predicted by the conjecture. This follows from the fact that there exists an arithmetic group Γ such that $H^1(\Gamma, \mathbb{C})$ is non-zero (see Theorem 1 of [3]). In general, when the existence of an arithmetic group Γ is known such that $H^1(\Gamma, \mathbb{C})$ is non-zero, then the congruence kernel is infinite (Section 8, [13]). However for the related groups of the second kind, all arithmetic groups Γ have $H^1(\Gamma, \mathbb{C}) = 0$

and the CSP is still unknown (see Theorem 1 of [3]). As an application of the theory developed in this thesis, we demonstrate its use towards an alternative proof of the non-triviality of the congruence kernel for $\mathrm{SU}(2,1)$. Our main result is the following new criterion for demonstrating that congruence kernels are infinite.

Theorem. *Let* $\mathrm{SU}(2,1)$ *denote a unitary group of the first kind, let* $\Gamma = \mathrm{SU}(2,1)(\mathbb{Z})$ *and* $q > 3$ *be a prime. Suppose there exists a congruence subgroup* $\Gamma' \subset \Gamma$ *such that the restriction map* $H^2(\Gamma, \mathbb{F}_q) \to H^2(\Gamma', \mathbb{F}_q)$ *is not injective. Then the congruence kernel of* $\mathrm{SU}(2,1)$ *is infinite.*

This theorem generalises a result of Deligne [8], which states that if there exists a weight $1/n$ multiplier system on some congruence subgroup for $n > 2$, then the congruence kernel is infinite.

Chapter 1

Definitions and Preliminary Material

In this chapter we introduce the group $\mathrm{SU}(2,1)$ defined over a field and reproduce some of its basic structure that will be of use to us throughout. This will include the Bruhat decomposition of $\mathrm{SU}(2,1)$, its corresponding Lie algebra $\mathfrak{su}(2,1)$ and the group of adele points of $\mathrm{SU}(2,1)$. We describe the congruence subgroup problem and introduce the notion of a fractional weight modular form on $\mathrm{SU}(2,1)$. We then use these concepts to develop some theory that will be used in our approach to the congruence subgroup problem.

1.1 $\mathrm{SU}(2,1)$ Defined Over A Field

Let k denote a field and K a degree 2 extension of k of the form $K = k(\sqrt{-d})$ for $d \in k^\times$. We define $\alpha_0 = \sqrt{-d}$. We have a non-trivial field automorphism of K fixing k given by

$$\overline{a + b\alpha_0} = a - b\alpha_0.$$

Letting A denote a commutative k-algebra, we can construct $\mathrm{SU}(2,1)_{K/k}$ as a functor from commutative k-algebras to groups given by

$$\mathrm{SU}(2,1)_{K/k}(A) = \left\{ g \in \mathrm{SL}_3(A \otimes_k K) : g^t J \overline{g} = J \right\},$$

where J is the Hermitian matrix defined by

$$J = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

and as usual g^t denotes the transpose of the matrix g. Since the extension K/k will always be clear, we write $\mathrm{SU}(2,1)_{K/k}$ as $\mathrm{SU}(2,1)$. When our ground field k is contained in $\mathbb{R}$ and $d > 0$, we can verify that this form has signature $(2,1)$ since a change of coordinates allows us to write

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

and defining $\mathrm{SU}(2,1)$ with respect to this matrix gives us a description of $\mathrm{SU}(2,1)$ isomorphic to our initial definition.

We will often abbreviate the above notation by writing $\mathcal{G} = \mathrm{SU}(2,1)$; we reserve this notation throughout solely for $\mathrm{SU}(2,1)$ and thus

$$\mathcal{G}(k) = \left\{ g \in \mathrm{SL}_3(K) : g^t J \overline{g} = J \right\}.$$

Suppose now that k is a number field. We denote its ring of integers by $\mathcal{O}_k$ and we fix a prime ideal $\mathfrak{p} \subset \mathcal{O}_k$ (we will often say that $\mathfrak{p}$ is prime in k). A choice of $\mathfrak{p}$ allows us to construct a $\mathfrak{p}$-adic norm on k, denoted $|\cdot|_{\mathfrak{p}}$, in the following way; the residue field $\mathcal{O}_k/\mathfrak{p}$ has size q for some $q \in \mathbb{Z}$, and we can factorise $\alpha \in k^\times$ as a product of primes $\mathfrak{p}^e \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ in k. We set $\nu_{\mathfrak{p}}(\alpha) = e$ and the $\mathfrak{p}$-adic norm on k is given by

$$|\alpha|_{\mathfrak{p}} = q^{-\nu_{\mathfrak{p}}(\alpha)},$$

and we set $|0|_{\mathfrak{p}} = 0$. The function $\nu_{\mathfrak{p}}$ is a *discrete valuation* of k. We can complete k with respect to $|\cdot|_{\mathfrak{p}}$ and the resulting field is denoted $k_{\mathfrak{p}}$. The *valuation ring* $\mathcal{O}_{k_{\mathfrak{p}}}$, along with its group of units $\mathcal{O}_{k_\mathfrak{p}}^\times$ and maximal ideal $\mathfrak{m}$, are defined as the sets

$$\begin{aligned} \mathcal{O}_{k_\mathfrak{p}} &= \{x \in k_p : \nu_p(x) \geq 0\}, \\ \mathcal{O}_{k_\mathfrak{p}}^\times &= \{x \in k_p : \nu_p(x) = 0\} \quad \text{and} \\ \mathfrak{m} &= \{x \in k_p : \nu_p(x) > 0\}. \end{aligned}$$

Together with the $\mathfrak{p}$-adic norms on k, we also have the archimedian norms at the infinite places, which are given by embeddings $k \hookrightarrow \mathbb{C}$ and restricting the usual norm $|\cdot|_\infty$ on $\mathbb{C}$ to k. We note that two such embeddings τ and its complex conjugate $\overline{\tau}$ may differ on $\mathbb{C}$, but they still induce the same norm on k. We thus define an equivalence relation on the infinite places, with equivalence classes consisting of embeddings $\{\tau, \overline{\tau}\}$.

Throughout, we will denote the set of equivalence classes of norms on k by V^k. This decomposes as a union of the finite places and infinite places of k, denoted V_f^k and V_∞^k respectively. From the definition of $\mathrm{SU}(2,1)$, we have

$$\mathrm{SU}(2,1)(k_\mathfrak{p}) = \left\{g \in \mathrm{SL}_3\left(k_\mathfrak{p} \otimes_k K\right) : g^t J \overline{g} = J\right\}.$$

The structure of the group $\mathrm{SU}(2,1)(k_\mathfrak{p})$ depends upon the ramification properties of $\mathfrak{p}$ in the field K upstairs. Recall that (see [24]) for a finite extension of number fields L/k, a norm $|\cdot|_\mathfrak{p}$ on k extends to norms $|\cdot|_{\mathfrak{P}_1}, \cdots, |\cdot|_{\mathfrak{P}_n}$ on L where $\mathfrak{P}_1, \cdots, \mathfrak{P}_n$ are primes of L containing $\mathfrak{p}$. We have an isomorphism

$$k_{\mathfrak{p}} \bigotimes_{k} L \cong \bigoplus_{i=1}^{n} L_{\mathfrak{P}_i},$$

and the degree of the extension $[L:k]$ is the sum of the local degrees $[L_{\mathfrak{P}_i} : k_{\mathfrak{p}}]$. Returning to our quadratic extension $K = k(\alpha_0)$, if $\mathfrak{p}$ remains inert in K then $K_{\mathfrak{p}} \cong k_{\mathfrak{p}} \otimes_k K$ is a field and can be written as $k_{\mathfrak{p}}(\alpha_0)$. We then have $\mathrm{SU}(2,1)(k_{\mathfrak{p}}) = \{g \in \mathrm{SL}_3\,(K_{\mathfrak{p}}) : g^t J \overline{g} = J\}$. Similarly, when $\mathfrak{p}$ ramifies as $\mathfrak{p} = \mathfrak{P}^2$ for $\mathfrak{P} \in K$, we have $\mathrm{SU}(2,1)(k_{\mathfrak{p}}) = \{g \in \mathrm{SL}_3\,(K_{\mathfrak{P}}) : g^t J \overline{g} = J\}$. In the case when $\mathfrak{p}$ splits in K, $k_{\mathfrak{p}} \otimes_k K \cong k_{\mathfrak{p}} \oplus k_{\mathfrak{p}}$. There is then an isomorphism $\mathrm{SL}_3(k_{\mathfrak{p}} \oplus k_{\mathfrak{p}}) \cong \mathrm{SL}_3(k_{\mathfrak{p}}) \oplus \mathrm{SL}_3(k_{\mathfrak{p}})$ and we have $\mathcal{G}(k_{\mathfrak{p}}) \cong \mathrm{SL}_3(k_{\mathfrak{p}})$. So to understand $\mathcal{G}(k_p)$, we will need to consider whether $\mathfrak{p}$ is ramified, inert or split in the field K upstairs.

We follow the same notation when given a commutative $\mathcal{O}_k$-algebra A by defining

$$\mathrm{SU}(2,1)(A) = \left\{ g \in \mathrm{SL}_3(A \otimes_{\mathcal{O}_k} \mathcal{O}_K) : g^t J \overline{g} = J \right\}.$$

We will mostly be interested in this construction when $A = \mathcal{O}_{k_{\mathfrak{p}}}$, $A = \mathcal{O}_k/\mathfrak{p}$ or $A = \mathcal{O}_k/\mathfrak{p}^n$.

1.2 The Lie Algebra and the Bruhat Decomposition

We let k denote a general field and K a degree 2 extension of k as before. The Lie algebra corresponding to $\mathcal{G}/k$ is denoted $\mathfrak{g}(k)$ (or simply $\mathfrak{g}$ when the field k is understood) and is given by

$$\mathfrak{g}(k) = \left\{ X \in \mathfrak{sl}_3(K) : X^t J + J\overline{X} = 0 \right\}.$$

There is an automorphism θ of $\mathfrak{g}(k)$ with $\theta^2 = 1$ given by $\theta(X) = -\overline{X}^t$ (see [16]). If we write $\mathfrak{k}$ and $\mathfrak{p}$ to denote the $+1$ and -1 eigenspaces of θ respectively, then we obtain a direct sum decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$. We have a maximal abelian subalgebra of $\mathfrak{p}$ given by

$$\mathfrak{a} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -a \end{pmatrix} : a \in k \right\},$$

and the root system of $\mathfrak{g}$ with respect to $\mathfrak{a}$ is $\Sigma = \{-2\lambda, -\lambda, \lambda, 2\lambda\}$. Thus we have one simple root λ, which as a function of $\mathfrak{a}$ is

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

for all $a \in k$. The root spaces are as usual denoted by $\mathfrak{g}_\phi$ for $\phi \in \Sigma$ and are as follows:

$$
\begin{aligned}
\mathfrak{g}_\lambda &= \{X \in \mathfrak{g} : \mathrm{ad}(a)(X) = \lambda(a)(X)\ \forall a \in \mathfrak{a}\} \\
&= \left\{ \begin{pmatrix} 0 & x & 0 \\ 0 & 0 & -\overline{x} \\ 0 & 0 & 0 \end{pmatrix} : x \in K \right\} \\
\mathfrak{g}_{2\lambda} &= \left\{ \begin{pmatrix} 0 & 0 & y\alpha_0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : y \in k \right\} \\
\mathfrak{g}_0 &= \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & \overline{a} - a & 0 \\ 0 & 0 & -\overline{a} \end{pmatrix} : a \in K \right\} \\
\mathfrak{g}_{-\lambda} &= \left\{ \begin{pmatrix} 0 & 0 & 0 \\ x & 0 & 0 \\ 0 & -\overline{x} & 0 \end{pmatrix} : x \in K \right\} \\
\mathfrak{g}_{-2\lambda} &= \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ y\alpha_0 & 0 & 0 \end{pmatrix} : y \in k \right\}.
\end{aligned}
\tag{1.1}
$$

This gives us the root space decomposition $\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\phi \in \Sigma} \mathfrak{g}_\phi$.

The set Σ is a root system and the Weyl group W of Σ is the group generated by the reflection with respect to the simple root λ. We can identify W with the quotient $N_{\mathcal{G}}(S)/Z_{\mathcal{G}}(S)$, where

$$S = \left\{ \begin{pmatrix} s & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & s^{-1} \end{pmatrix} : s \in k^{\times} \right\},$$

and $N_{\mathcal{G}}(S)$ and $Z_{\mathcal{G}}(S)$ are the normaliser and centraliser of S in $\mathcal{G}(k)$ respectively. Note that W has one non-trivial element which we can represent by the matrix

$$w = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}. \tag{1.2}$$

There are several subgroups of $\mathrm{SU}(2,1)$ that will be important for us. First we note that $\mathrm{SU}(2,1)$ contains algebraic tori S_k and $T_{K/k}$, where S_k is a maximal k-split torus and $T_{K/k}$ is a maximal torus in $\mathrm{SU}(2,1)$. Given a commutative k-algebra A, we realise these as

$$\begin{aligned} S_k &= \left\{ \begin{pmatrix} s & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & s^{-1} \end{pmatrix} : s \in k^\times \right\} \qquad \text{and} \\ T_{K/k}(A) &= \left\{ g \in diag\left(x, y, (xy)^{-1}\right) : x, y \in A \otimes_k K,\ gJ\overline{g} = J \right\}. \end{aligned}$$

We will usually exclude the subscripts k and K/k to ease notation. In particular, $\mathcal{G}(k)$ has a maximal k-split torus and a maximal torus given by

$$\begin{aligned} S &= \left\{ \begin{pmatrix} s & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & s^{-1} \end{pmatrix} : s \in k^\times \right\} \qquad \text{and} \\ T(k) &= \left\{ \begin{pmatrix} x & 0 & 0 \\ 0 & \overline{x}/x & 0 \\ 0 & 0 & \overline{x}^{-1} \end{pmatrix} : x \in K^\times \right\}, \end{aligned}$$

respectively (see [4]). We remark that the Lie algebras of the algebraic tori S_k and $T_{K/k}$ are $\mathfrak{a}$ and $\mathfrak{g}_0$ respectively.

From now on we fix a set of positive roots $\Sigma^+ = \{\lambda, 2\lambda\}$. By Lecture 4 of [16], the *Borel subalgebra* is the Lie subalgebra $\mathfrak{b} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in \Sigma^+} \mathfrak{g}_\alpha$. The subgroup of $\mathcal{G}$ whose Lie algebra is $\mathfrak{b}$ is a Borel subgroup whose k-points have a simple description as the set of upper triangular matrices in $\mathcal{G}(k)$;

$$B(k) = \left\{ \begin{pmatrix} x & r & m \\ 0 & \overline{x}/x & -\overline{r} \\ 0 & 0 & \overline{x}^{-1} \end{pmatrix} : x \in K^{\times},\ r, m \in K \text{ with } \operatorname{Tr}(m) = -\operatorname{N}(r) \right\}.$$

Here we are using the notation $\operatorname{Tr}(m)$ to denote the trace of m and $\operatorname{N}(r)$ to denote the norm of r. We can decompose $B(k)$ as a semidirect product $B(k) = N(k) \rtimes T(k)$, where $N(k)$ is the unipotent subgroup of $\mathcal{G}(k)$ given by

$$N(k) = \left\{ \begin{pmatrix} 1 & r & m \\ 0 & 1 & -\overline{r} \\ 0 & 0 & 1 \end{pmatrix} : r, m \in K \text{ with } \operatorname{Tr}(m) = -\operatorname{N}(r) \right\}.$$

Similarly, we will denote $N(k)^t$ to be the subgroup of $\mathcal{G}(k)$ such that $g \in N(k)^t$ if and only if $g^t \in N(k)$. With the above notation, we arrive at the Bruhat Decomposition (see [4], V.21.29).

Theorem 1.2.1. (The Bruhat Decomposition) *Let k be a field and w represent an element in the Weyl group W. Then $\mathcal{G}(k)$ can be decomposed as a disjoint union of double cosets*

$$\mathcal{G}(k) = \bigcup_{w \in W} B(k) w B(k).$$

1.3 Arithmetic Subgroups and the Adele Group

Recall that we introduced the notation V^k to denote the set of classes of valuations of k when k is an algebraic number field. When we say a prime $\mathfrak{p} \in V^k$, we take this to mean the norm corresponding to $\mathfrak{p}$ as constructed earlier lies in V^k. The *adele ring* $\mathbb{A}_k$ of k is the restricted topological product

$$\mathbb{A}_k = \prod_{\mathfrak{p} \in V^k}{}^{'} k_{\mathfrak{p}},$$

with respect to the subrings $\mathcal{O}_{k_{\mathfrak{p}}}$. This means that an adele $x \in \mathbb{A}_k$ is a collection $(x_{\mathfrak{p}})$ such that each $x_{\mathfrak{p}} \in k_{\mathfrak{p}}$ and $x_{\mathfrak{p}} \in \mathcal{O}_{k_{\mathfrak{p}}}$ for all but finitely many places $\mathfrak{p} \in V_f^k$. We can make $\mathbb{A}_k$ into a ring by using componentwise addition and multiplication. We can topologise $\mathbb{A}_k$ by taking a basis of open sets to consist of sets of the form $\prod_{\mathfrak{p} \in S} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in V^k \setminus S} \mathcal{O}_{k_{\mathfrak{p}}}$, where $S \subset V^k$ is finite and contains V_∞^k, and $U_{\mathfrak{p}} \subset k_{\mathfrak{p}}$ are open subsets for each $\mathfrak{p} \in S$. Note that we can diagonally embed $k \hookrightarrow \mathbb{A}_k$ by the map $x \longmapsto (x, x, \cdots)$, since we may write $x = a/b$ with $a, b \in \mathcal{O}_k$, $b \neq 0$, and b factorises as a finite product of prime ideals. The set of *finite adeles* is denoted $\mathbb{A}_k^f$ and is the restricted product $\mathbb{A}_k^f = \prod'_{\mathfrak{p} \in V_f^k} k_{\mathfrak{p}}$ with respect to the subrings $\mathcal{O}_{k_{\mathfrak{p}}}$. When no confusion will arise, we abbreviate the notation $\mathbb{A}_k$ to $\mathbb{A}$. We introduce two additional pieces of notation. Firstly, $\mathbb{A}(S)$ will denote the set of S-integral adeles which for a finite subset $S \subset V^k$ containing V_∞^k, is $\prod_{\mathfrak{p}\in S} k_\mathfrak{p} \times \prod_{\mathfrak{p}\in V^k\setminus S} \mathcal{O}_{k_\mathfrak{p}}$. Secondly, the S-adeles $\mathbb{A}_S$ is defined as the image of $\mathbb{A}$ under the natural projection of $\prod_\mathfrak{p} k_\mathfrak{p}$ onto $\prod_{\mathfrak{p}\notin S} k_\mathfrak{p}$.

Of particular interest will be the adele points and finite adele points of $\mathcal{G}$, the latter given by

$$\mathcal{G}(\mathbb{A}_k^f) = \left\{ g \in \mathrm{SL}_3(\mathbb{A}_k^f \otimes_k K) : g^t J \overline{g} = J \right\},$$

and the adele points of $\mathcal{G}$ constructed in an analogous way. We note now that $\mathcal{G}(\mathbb{A}_k^f)$ is a topological group with basis of open sets consisting of those of the form

$$\prod_\mathfrak{p} U_\mathfrak{p},$$

where $U_\mathfrak{p} \subset \mathrm{SU}(2,1)(k_\mathfrak{p})$ is open and for all but finitely many $\mathfrak{p}$, $U_\mathfrak{p} = \mathrm{SU}(2,1)(\mathcal{O}_{k_\mathfrak{p}})$.

A crucial property we will need is the strong approximation theorem. Given an algebraic number field k and a finite subset S containing V_∞^k, the strong approximation theorem (with respect to S) for a k-simple, simply connected algebraic group G with $G(S) := \prod_{\mathfrak{p}\in S} G(k_\mathfrak{p})$ noncompact, follows from Theorem 7.12 of [24]. We have the following theorem.

Theorem 1.3.1. (Strong Approximation Theorem) *Let k be an algebraic number field and G a k-simple, simply connected algebraic group over k such that $G(S) = \prod_{\mathfrak{p}\in S} G(k_\mathfrak{p})$ is noncompact. Then the embedding of $G(k)$ into $G(\mathbb{A}_S)$ by the diagonal* *map has dense image in* $G(\mathbb{A}_S)$.

We note that in particular $\mathrm{SU}(2,1)$ defined over k satisfies the strong approximation theorem, thus $\mathrm{SU}(2,1)(k)$ has dense image in $\mathrm{SU}(2,1)(\mathbb{A}_k^f)$.

1.4 The Congruence Subgroup Problem

In most of what comes later we will not have a distinguished set of primes S and we will instead be working with the full adele ring or its subring of finite adeles. However, in the first subsection we will introduce the congruence subgroup problem as it often is in the literature which involves a fixed set of primes S. We will then focus specifically on the congruence subgroup problem for $\mathrm{SU}(2,1)$.

1.4.1 The Classical Formulation

In this section we introduce the congruence subgroup problem as it is stated in [25]. For a subset $S \subset V^k$ containing all the infinite places of k, we define the set of S-integers of k by

$$\mathcal{O}(S) = \left\{ x \in k : |x|_{\mathfrak{p}} \leq 1 \text{ for all } \mathfrak{p} \in V^k \setminus S \right\}.$$

In this section we take an absolutely simple, simply connected linear algebraic group G defined over k, with the added condition that $G(S) = \prod_{\mathfrak{p} \in S} G(k_{\mathfrak{p}})$ is not compact. We note that $\mathrm{SU}(2,1)$ satisfies these conditions, and that such a group G has the strong approximation theorem with respect to S (see Section 7.4 of [24]). We fix an embedding $G \hookrightarrow \mathrm{GL}_n$ over k (the choice of embedding here has no impact on the congruence subgroup problem for G). We construct an arithmetic subgroup by $\Gamma = G(k) \cap \mathrm{GL}_n(\mathcal{O}(S))$ and define $\mathrm{GL}_n(\mathcal{O}(S), \mathfrak{a})$ to be the subgroup of $\mathrm{GL}_n(\mathcal{O}(S))$ consisting of all matrices congruent to the identity matrix modulo a non-zero ideal $\mathfrak{a} \subset \mathcal{O}(S)$. We then define the *principal S-congruence subgroup of level* $\mathfrak{a}$ as $\Gamma(\mathfrak{a}) := \Gamma \cap \mathrm{GL}_n(\mathcal{O}(S), \mathfrak{a})$, and a subgroup $\Gamma' \subset \Gamma$ is called an *S-congruence subgroup* of Γ if it contains $\Gamma(\mathfrak{a})$ for some non-zero ideal $\mathfrak{a}$. It is clear that such subgroups have finite index in Γ, and so we can ask if all subgroups of finite index are of this form;

Congruence Subgroup Problem (CSP): Is every subgroup of finite index in Γ a congruence subgroup?

A natural first example is the group $G = \mathrm{SL}_2$ defined over $\mathbb{Q}$, with $S = V_\infty^{\mathbb{Q}}$ and arithmetic subgroup $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. The congruence subgroups are then the subgroups which contain the kernel of the map

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

for some positive integer N. The CSP for $\mathrm{SL}_2(\mathbb{Z})$ has been solved and it turns out that there are infinitely many subgroups of finite index in Γ that are not congruence subgroups; proofs of this along with constructions of some non-congruence subgroups can be found in [30]. In contrast to this, a positive solution to the CSP was found for $\mathrm{SL}_n(\mathbb{Z})$ with $n \geq 3$ by Bass-Lazard-Serre in [1]. The groups $\mathrm{SL}_n(\mathcal{O}(S))$ for $n \geq 3$ were considered by Bass-Milnor-Serre in [2]; in approaching the congruence subgroup problem for these groups, the *congruence kernel* is constructed as a means of measuring the deviation from a positive solution to the CSP. This comes as a result of a reformulation of the problem in the following way.

Let $\mathfrak{N}_a$ and $\mathfrak{N}_c$ be collections of all normal subgroups of finite index and congruence subgroups of Γ respectively. We then define topologies τ_a and τ_c on Γ which have $\mathfrak{N}_a$ (resp. $\mathfrak{N}_c$) as a base of neighbourhoods of the identity. We call these the *S-arithmetic topology* and the *S-congruence topology* respectively. Taking the completion of Γ with respect to each of these topologies, we obtain two new groups, $\hat{\Gamma}$ and $\bar{\Gamma}$ respectively. Both of these groups can be described in terms of projective limits as $\hat{\Gamma} = \varprojlim_{\Gamma' \in \mathfrak{N}_a} \Gamma/\Gamma'$ and $\bar{\Gamma} = \varprojlim_{\Gamma' \in \mathfrak{N}_c} \Gamma/\Gamma'$. Since τ_a is a stronger topology than τ_c we have a continuous surjective homomorphism

$$\hat{\Gamma} \xrightarrow{\pi_\Gamma} \bar{\Gamma},$$

the kernel of which we define to be the *congruence kernel* and is denoted $\mathrm{Cong}_S(G)$.

The congruence kernel thus fits into a short exact sequence,

$$1 \longrightarrow \mathrm{Cong}_S(G) \longrightarrow \hat{\Gamma} \xrightarrow{\pi_\Gamma} \bar{\Gamma} \longrightarrow 1.$$

We note that $G(k)$ also has the structure of a topological group with respect to the two topologies defined above (see [25]). Furthermore, one can show that the S-congruence topology on $G(k)$ corresponds to the topology we obtain on $G(k)$ through the diagonal embedding $G(k) \hookrightarrow G(\mathbb{A}_S)$ (also in [25]). We can thus complete $G(k)$ in the same way and by the strong approximation theorem (with respect to S), we have

$$G(\mathbb{A}_S^f) = \varprojlim_{\Gamma' \in \mathfrak{N}_c} G(k)/\Gamma',$$

and we define

$$\widetilde{G(\mathbb{A}_S^f)} = \varprojlim_{\Gamma' \in \mathfrak{N}_a} G(k)/\Gamma'.$$

Note that these are indeed both groups; the collections of arithmetic and congruence subgroups each give a filtration on $G(k)$ and these filtrations are both *normal*. Here, normal is taken to mean that for any $g \in G(k)$ and any arithmetic subgroup (resp. congruence subgroup) Γ', $g^{-1}\Gamma' g \supset \Gamma''$ for some arithmetic subgroup (resp. congruence subgroup) Γ''. It follows that $G(\mathbb{A}_S^f)$ and $\widetilde{G(\mathbb{A}_S^f)}$ are both groups, and there is a surjective map $\widetilde{G(\mathbb{A}_S^f)} \to G(\mathbb{A}_S^f)$ whose kernel coincides with $\mathrm{Cong}_S(G)$. The congruence subgroup problem then becomes: Is $\mathrm{Cong}_S(G) = 1$?

We conclude this section by giving some known results to the congruence subgroup problem for a number of groups, along with a conjecture due to Serre. We noted previously that $\mathrm{SL}_2(\mathbb{Z})$ had infinitely many non-congruence subgroups, whereas all subgroups of finite index in $\mathrm{SL}_3(\mathbb{Z})$ are congruence subgroups. It was shown in [2] that there are two possibilities for $\mathrm{Cong}_S(G)$ with $G = \mathrm{SL}_n$ and $n \geq 3$; $\mathrm{Cong}_S(\mathrm{SL}_n)$ is isomorphic to the finite cyclic group μ_k of all roots of unity in k if S is totally complex and is trivial otherwise. In fact, it is shown in [28] that these same conditions on S when $|S| > 1$ gives the same possibilities for $\mathrm{Cong}_S(\mathrm{SL}_2)$. However, if $|S| = 1$, then $\mathrm{Cong}_S(\mathrm{SL}_2)$ is infinite. We conclude with the following conjecture due to Serre [28]. First, we recall that the S-rank of G is defined as $rk_S(G) = \sum_{\mathfrak{p}\in S} rk_{k_\mathfrak{p}}(G)$.

Conjecture 1.4.1. (Congruence Subgroup Conjecture) *Let G be an absolutely simple, simply connected k-group. Then*

(i) if $rk_S(G) \geq 2$ and $rk_{k_\mathfrak{p}} > 0$ for all $\mathfrak{p} \in S \setminus V_\infty$, then $\mathrm{Cong}_S(G)$ is finite, and

(ii) if $rk_S(G) = 1$ then $\mathrm{Cong}_S(G)$ is infinite.

We note that if $rk_S(G) = 0$, then the S-arithmetic groups are finite and therefore $\mathrm{Cong}_S(G)$ is trivial. In the Introduction, we gave two different types of unitary group; those of the *first kind* and the *second kind*. The group $\mathrm{SU}(2, 1)$ as introduced above is of the first kind and has k-rank 1. For this group, the conjecture is already known. However, for the closely related groups of the second kind, the conjecture remains unknown (see for example [3]), although it is known that if the congruence kernel is finite in this case, then it must be trivial (see [26]). Our aim is to develop a new tool for proving this conjecture for $\mathrm{SU}(2,1)$.

1.4.2 Congruence Subgroup Problem for $\mathrm{SU}(2,1)$

Let k be an imaginary quadratic extension of $\mathbb{Q}$ and $S = V_\infty^{\mathbb{Q}}$. Let p denote a prime in $\mathbb{Z}$ and $\mathfrak{p}$ a prime in $\mathcal{O}_k$. From this point onwards, we will always be studying $\mathrm{SU}(2,1)_{k/\mathbb{Q}}$; if there is no mention of the field extension, then it is understood to be $k/\mathbb{Q}$. The aim of this section is to make explicit the results of the previous section for $\mathrm{SU}(2,1)$ and to introduce the notation we will be using in later chapters. We begin with two observations relating congruence subgroups and the compact open subgroups of $\mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f)$.

Proposition 1.4.2. *An arithmetic subgroup* Γ *is a congruence subgroup if and only if it is open in the subspace topology of* $\mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f)$.

Proof. Recall that a set U is open in $\mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f)$ if it contains a set of the form $\prod_p U_p$, where $U_p \subset \mathrm{SU}(2,1)(\mathbb{Q}_p)$ is open and for all but finitely many p, $U_p = \mathrm{SU}(2,1)(\mathbb{Z}_p)$. Equivalently, a set U is open if there exists $N \in \mathbb{Z}$ such that U

contains

$$K_f(N) := \prod_p K_p(N),$$

where we define

$$K_p(N) = \begin{cases} \{g \in \mathrm{SL}_3(\mathbb{Z}_p) : g \equiv I_d \mod N\mathbb{Z}_p\} & p \text{ split in } k, \\ \left\{g \in \mathrm{SU}(2,1)(\mathbb{Z}_p) : g \equiv I_d \mod N\mathcal{O}_{k_p}\right\} & p \text{ inert in } k, \\ \left\{g \in \mathrm{SU}(2,1)(\mathbb{Z}_p) : g \equiv I_d \mod N\mathcal{O}_{k_\mathfrak{p}}\right\} & p = \mathfrak{p}^2 \text{ ramified in } k. \end{cases}$$

The subgroups $K_f(N)$ are compact open subgroups and furthermore

$$(K_f(N) \times \mathrm{SU}(2,1)(\mathbb{R})) \cap \mathrm{SU}(2,1)(\mathbb{Q}) = \Gamma(N).$$

So after unravelling the definitions, we see that if Γ is open in the subspace topology of $\mathrm{SU}(2,1)(\mathbb{A}_\mathbb{Q}^f)$, it must contain some $\Gamma(N)$.

Conversely, suppose that $\Gamma \supset \Gamma(N)$. Choosing a set of representatives $g_i \in \Gamma/\Gamma(N)$, Γ can be written as a disjoint union $\coprod_{g_i} g_i\Gamma(N)$. So Γ is a finite union of open sets, thus is open. □

We introduce some notation. Given a compact open subgroup K_f of $\mathrm{SU}(2,1)(\mathbb{A}_\mathbb{Q}^f)$ as above, we define $\Gamma(K_f) = (K_f \times \mathrm{SU}(2,1)(\mathbb{R})) \cap \mathrm{SU}(2,1)(\mathbb{Q})$. This is a congruence subgroup by the above Proposition. In fact, this map has an inverse and gives us the following Corollary.

Corollary 1.4.3. *The compact open subgroups* $K_f \subset \mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f)$ *are in one-to-one correspondence with congruence subgroups* $\Gamma(K_f)$.

These results tell us that the congruence topology on $\mathrm{SU}(2,1)(\mathbb{Q})$ coincides with the topology induced by embedding $\mathrm{SU}(2,1)(\mathbb{Q})$ into $\mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f)$. Thus by strong approximation we have as we did above,

$$\mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f) = \varprojlim_{\Gamma' \in \mathfrak{R}_c} \mathrm{SU}(2,1)(\mathbb{Q})/\Gamma',$$

and we define

$$\mathrm{SU}\widetilde{(2,1)}(\mathbb{A}_{\mathbb{Q}}^f) = \varprojlim_{\Gamma' \in \mathfrak{R}_a} \mathrm{SU}(2,1)(\mathbb{Q})/\Gamma'.$$

The congruence kernel $\mathrm{Cong}(\mathrm{SU}(2,1))$ for $\mathrm{SU}(2,1)$ then fits into the short exact sequence

$$1 \longrightarrow \mathrm{Cong}(\mathrm{SU}(2,1)) \longrightarrow \mathrm{SU}\widetilde{(2,1)}(\mathbb{A}^f) \longrightarrow \mathrm{SU}(2,1)(\mathbb{A}^f) \longrightarrow 1.$$

1.5 An Approach to the Congruence Subgroup Problem

Having introduced the congruence subgroup problem, we develop the main ideas behind our approach to determining if the congruence kernel is trivial or non-trivial. Recall that we are now defining $\mathrm{SU}(2,1)$ using the imaginary quadratic extension $k/\mathbb{Q}$.

1.5.1 Fractional Weight Forms on $\mathrm{SU}(2,1)$

We begin by introducing the notion of a fractional weight modular form on $\mathrm{SU}(2,1)$. We will show in section 1.5.2 that the existence of certain fractional weight modular forms on $\mathrm{SU}(2,1)$ imply that the congruence kernel is infinite, hence our motivation for introducing the theory.

We let $\Gamma \subset \mathrm{SU}(2,1)(\mathbb{Q})$ denote an arithmetic subgroup, take $V = \mathbb{C}^3$ and $X = \mathbb{P}^2(\mathbb{C})$. Then $\mathrm{SU}(2,1)(\mathbb{Q})$ acts upon V and X in the obvious way and if we take the Hermitian form on V defined by $\langle u, v\rangle = u^t J\overline{v}$, then clearly $\mathrm{SU}(2,1)$ preserves the subsets

$$\begin{aligned} V^+ &= \left\{v \in \mathbb{C}^3 : \langle v, v\rangle > 0\right\}, \\ V^0 &= \left\{v \in \mathbb{C}^3 : \langle v, v\rangle = 0\right\} \quad \text{and} \\ V^- &= \left\{v \in \mathbb{C}^3 : \langle v, v\rangle < 0\right\}. \end{aligned}$$

Let X^- denote the image of V^- in X. Taking k to be a positive integer, we define a weight k modular form (of level Γ) to be a holomorphic function $f : V^- \longrightarrow \mathbb{C}$ such that

$$\begin{aligned} f(\lambda v) &= \lambda^{-k} f(v) \quad \forall \lambda \in \mathbb{C}^\times \quad \text{and} \\ f(\gamma v) &= f(v) \quad \forall \gamma \in \Gamma. \end{aligned}$$

Since any $\begin{bmatrix} x \\ y \\ z \end{bmatrix} \in X^-$ must have $z \neq 0$, we can define a section $X^- \longrightarrow V^-$ by $\begin{bmatrix} x \\ y \\ 1 \end{bmatrix} \longmapsto \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$. Defining

$$\mathcal{H} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2 : \mathrm{Tr}(x) + \mathrm{N}(y) < 0 \right\},$$

we construct a function $g : \mathcal{H} \longrightarrow \mathbb{C}$ by $g\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = f\left(\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}\right)$.

We need to know how Γ acts upon $\mathcal{H}$. To see this, we break $\gamma \in \Gamma$ into blocks by writing $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where A is a matrix of size 2×2, B is 2×1, C is 1×2 and D has size 1×1. Writing $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{H}$, the action is given by

$$\gamma v = \frac{Av + B}{Cv + D} \qquad \gamma \in \Gamma.$$

Noting that $Cv + D$ is a scalar, we now have

$$\begin{aligned}
g(\gamma v) &= g\left(\frac{Av+B}{Cv+D}\right) \\
&= f\left(\begin{pmatrix} \frac{Av+B}{Cv+D} \\ 1 \end{pmatrix}\right) \\
&= (Cv+D)^k f\left(\begin{pmatrix} Av+B \\ Cv+D \end{pmatrix}\right) \\
&= (Cv+D)^k f\left(\gamma \begin{pmatrix} v \\ 1 \end{pmatrix}\right) \\
&= (Cv+D)^k f\left(\begin{pmatrix} v \\ 1 \end{pmatrix}\right) \\
&= (Cv+D)^k g(v).
\end{aligned}$$

We define $j^{'}(\gamma, v) = (Cv + D)^k$ to be the weight k multiplier system on Γ, since given $\gamma_1, \gamma_2 \in \Gamma$ and $v \in \mathcal{H}$ as above, a routine check verifies that

$$j'(\gamma_1\gamma_2, v) = j'(\gamma_1, \gamma_2 v)j'(\gamma_2, v).$$

Similarly, we can then define a weight k/n multiplier system on Γ to be a function

$j : \Gamma \times \mathcal{H} \longrightarrow \mathbb{C}^\times$ such that

$$\begin{aligned} j(\gamma_1\gamma_2, v) &= j(\gamma_1, \gamma_2 v) j(\gamma_2, v) \quad \text{and} \\ j(\gamma, v)^n &= (Cv + D)^k, \end{aligned}$$

where $\gamma \in \Gamma$ is decomposed into blocks A,B,C and D as above. We then define a weight k/n modular form on Γ to be a function $f : \mathcal{H} \longrightarrow \mathbb{C}$ such that for $\gamma \in \Gamma$ and $v \in \mathcal{H}$,

$$f(\gamma(v)) = j(\gamma, v) f(v).$$

We note that once a fractional weight multiplier system has been constructed, we can write down a fractional weight modular form by means of a holomorphic Eisenstein series. In the next section, we will link the existence of certain fractional weight multiplier systems on $\mathrm{SU}(2,1)$ with the size of the congruence kernel for $\mathrm{SU}(2,1)$.

1.5.2 Metaplectic Covers

Throughout this section let G denote an absolutely simple, simply connected linear algebraic group defined over $\mathbb{Q}$ which is also quasi-split over $\mathbb{Q}$. We will also assume that $G(\mathbb{R})$ has a connected n-fold cover for each $n \in \mathbb{N}$. In particular, the results in this section are true for $\mathcal{G}$. Let $\mathbb{A}$ denote the full adele ring of $\mathbb{Q}$ and let μ_2

denote the multiplicative group of order 2. We can construct a canonical topological central extension of $G(\mathbb{A})$ by μ_2, called a *metaplectic extension* of $G(\mathbb{A})$ by μ_2, given by

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{G(\mathbb{A})} & \longrightarrow & G(\mathbb{A}) & \longrightarrow & 1, \\ & & & & & \nwarrow & \uparrow & & \\ & & & & & & G(\mathbb{Q}) & & \end{array}$$

such that the extension splits on the group of rational points $G(\mathbb{Q})$ of G. The reason we call this extension *metaplectic* is due to the fact that it splits over the rational points of G. This is the only non-trivial topological central extension of $G(\mathbb{A})$ by μ_2 which splits on $G(\mathbb{Q})$ (see [9]). If $\mathrm{SU}\widetilde{(2,1)}(\mathbb{R})$ denotes the preimage of $\mathrm{SU}(2,1)(\mathbb{R})$ in the metaplectic extension, we obtain an extension of Lie groups

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{SU}\widetilde{(2,1)}(\mathbb{R}) \longrightarrow \mathrm{SU}(2,1)(\mathbb{R}) \longrightarrow 1.$$

In fact, the fundamental group $\pi_1(\mathrm{SU}(2,1)(\mathbb{R})) \cong \mathbb{Z}$ as can be seen in [21], so $\mathrm{SU}(2,1)(\mathbb{R})$ has a connected n-fold cover for every $n \in \mathbb{N}$ which fits into a central extension

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathrm{SU}\widetilde{(2,1)}(\mathbb{R})^{(n)} \longrightarrow \mathrm{SU}(2,1)(\mathbb{R}) \longrightarrow 1.$$

When $n = 2$, $\widetilde{\mathrm{SU}(2,1)(\mathbb{R})}^{(2)}$ is isomorphic to the preimage of $\mathrm{SU}(2,1)(\mathbb{R})$ in the metaplectic cover and we can show that this extension splits on some congruence subgroup. This is proved by the following Proposition.

Proposition 1.5.1. *Let G be as above. Let $G(\mathbb{R})$ denote the corresponding real Lie group and $\widetilde{G(\mathbb{R})}^{(2)}$ be its preimage in the metaplectic extension. Then there exists a congruence subgroup $\Gamma \subset G(\mathbb{Q})$ such that the extension*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{G(\mathbb{R})}^{(2)} & \longrightarrow & G(\mathbb{R}) & \longrightarrow & 1, \\ & & & & & \nwarrow & \uparrow & & \\ & & & & & & \Gamma & & \end{array}$$

splits on Γ.

Proof. Let $\widetilde{G(\mathbb{R})}$ and $\widetilde{G(\mathbb{A}^f)}$ be the preimages of $G(\mathbb{R})$ and $G(\mathbb{A}^f)$ respectively in the metaplectic cover. Since $\widetilde{G(\mathbb{A}^f)}$ is a topological cover of $G(\mathbb{A}^f)$, there exists a neighbourhood U_1 of the identity $e \in G(\mathbb{A}^f)$ such that the preimage of the restriction map of U_1, $pr^{-1}(U_1)$, is a disjoint union of homeomorphic copies of U_1. We will write $pr^{-1}(U_1) \sim V_1 \dot{\cup} V_2$. We may assume without loss of generality that V_1 is the copy of U_1 containing the identity element of $\widetilde{G(\mathbb{A}^f)}$. The group $\widetilde{G(\mathbb{A}^f)}$ is locally compact and totally disconnected, hence V_1 contains some compact open subgroup. Now, we can assume again without loss of generality that V_1 is a compact open subgroup, hence U_1 is also. We conclude that $V_1 \cong U_1$ as groups and so the extension of $G(\mathbb{A}^f)$ splits on U_1.

Fix a congruence subgroup $\Gamma := G(\mathbb{Q}) \cap (U_1 \times G(\mathbb{R}))$. Recall that (see [20]) for locally compact separable topological groups A and G with A abelian and G acting continuously as a group of automorphisms of A, that the cohomology group with measurable cochains $H^2_m(G, A)$ classifies topological extensions of G by A. So we let $\sigma_{\mathbb{R}} \in H^2_m(G(\mathbb{R}), \mu_2)$ and $\sigma_{\mathbb{A}^f} \in H^2_m(G(\mathbb{A}^f), \mu_2)$ be the 2-cocyles corresponding to their respective extensions above. Now since $G(\mathbb{R})$ is connected, $H^1_m(G(\mathbb{R}), \mu_2) = 0$ and so $H^2_m(G(\mathbb{A}), \mu_2) \cong H^2_m(G(\mathbb{R}), \mu_2) \oplus H^2_m(G(\mathbb{A}^f), \mu_2)$. Thus the 2-cocycle $\sigma_{\mathbb{R}} + \sigma_{\mathbb{A}^f}$ corresponds to the metaplectic extension of $G(\mathbb{A})$ and $\sigma_{\mathbb{R}}\big|_{G(\mathbb{Q})} + \sigma_{\mathbb{A}^f}\big|_{G(\mathbb{Q})} = 0$ since the extension splits on $G(\mathbb{Q})$. Hence

$$
\begin{aligned}
\sigma_{\mathbb{R}}\big|_{G(\mathbb{Q})} &= -\sigma_{\mathbb{A}^f}\big|_{G(\mathbb{Q})} \\
\Longrightarrow \sigma_{\mathbb{R}}\big|_{\Gamma} &= -\sigma_{\mathbb{A}^f}\big|_{G(\mathbb{Q})\cap U_1}.
\end{aligned}
$$

However, we showed that $\sigma_{\mathbb{A}^f}$ splits on U_1 and so $\sigma_{\mathbb{A}^f}\big|_{U_1} = 0$. It follows that the extension

$$
1 \longrightarrow \mu_2 \longrightarrow \widetilde{G(\mathbb{R})} \longrightarrow G(\mathbb{R}) \longrightarrow 1,
$$

splits on Γ. $\square$

We can also prove a partial converse of this result which is due to Deligne [8].

Theorem 1.5.2. *Suppose G is as above, with the added conditions that G has trivial* *congruence kernel. Suppose $G(\mathbb{R})$ has a connected n-fold cover for every $n \in \mathbb{N}$,*

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \widetilde{G(\mathbb{R})} \longrightarrow G(\mathbb{R}) \longrightarrow 1.$$

If there exists a congruence subgroup Γ that lifts to $\widetilde{G(\mathbb{R})}$ for some n, then $n \leq 2$.

Proof. We begin by recalling that G satisfies the strong approximation theorem. Thus $G(\mathbb{Q})$ is dense in $G(\mathbb{A}^f)$ and we have

$$G(\mathbb{A}^f) = \varprojlim G(\mathbb{Q})/\Upsilon,$$

where the projective limit is taken over all congruence subgroups (or equivalently arithmetic subgroups) $\Upsilon \subset \Gamma$. If $i : \Gamma \to \widetilde{G(\mathbb{R})}$ is the lift of Γ to $\widetilde{G(\mathbb{R})}$, we construct

$$\widetilde{G(\mathbb{A}^f)} = \varprojlim \widetilde{G(\mathbb{Q})}/i(\Upsilon),$$

where again the projective limit is taken over all congruence subgroups $\Upsilon \subset \Gamma$. In order to use this to construct an extension of $G(\mathbb{A}^f)$ by $\mathbb{Z}/n\mathbb{Z}$, we first must show that $\widetilde{G(\mathbb{A}^f)}$ is a group.

To do this, we claim that the filtration

$$\mathcal{F} = \{i(\Upsilon) : \Upsilon \text{ is a congruence subgroup of } \Gamma\},$$

is normal, which as we noted above means to say that $\mathcal{F}$ satisfies the property that for any $i(\Upsilon) \in \mathcal{F}$ and any $\tilde{g} \in \widetilde{G(\mathbb{Q})}$, $\tilde{g}^{-1} i(\Upsilon)\tilde{g} \supset i(\Upsilon')$ for some $i(\Upsilon') \in \mathcal{F}$. Once this is shown, it follows that the projective limit is a group. So, take $\tilde{g} \in \widetilde{G(\mathbb{Q})}$ and a congruence subgroup $\Upsilon_0 \subset \Gamma$. Set $g = pr(\tilde{g})$. The subgroup $\Upsilon' = \Upsilon_0 \cap g^{-1}\Upsilon_0 g$ is a congruence subgroup of Γ and $\Upsilon_0 \supset \Upsilon'$. We have two possible lifts of Υ'; i and a lift j given by the composition

$$j : \gamma \longmapsto g\gamma g^{-1} \longmapsto i(g\gamma g^{-1}) \longmapsto \tilde{g}^{-1} i(g\gamma g^{-1})\tilde{g},$$

for $\gamma \in \Upsilon'$. If $i = j$, then Υ' is the subgroup we require since $i(\Upsilon') = j(\Upsilon') \subset \tilde{g}^{-1} i(\Upsilon_0)\tilde{g}$, as required. If not, then we note that i and j differ by elements of $\mathbb{Z}/n\mathbb{Z}$ and since our extensions are central, there exists a group homomorphism

$$\begin{aligned} \Phi : \Upsilon' &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \gamma &\longmapsto i(\gamma)j(\gamma)^{-1}. \end{aligned}$$

Setting $\Upsilon'' := \ker(\Phi)$ gives us a congruence subgroup Υ'' as the kernel of Φ has finite index in Υ_0, and furthermore the lifts i, j coincide on Υ''. Hence $i(\Upsilon'') = j(\Upsilon'') \subset \tilde{g}^{-1} i(\Upsilon_0)\tilde{g}$, as required.

We conclude that $\widetilde{G(\mathbb{A}^f)}$ is a group and we thus have the following extensions giving us a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \widetilde{G(\mathbb{A}^f)} & \longrightarrow & G(\mathbb{A}^f) & \longrightarrow & 1 \\
 & & \| & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \widetilde{G(\mathbb{Q})} & \longrightarrow & G(\mathbb{Q}) & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \widetilde{G(\mathbb{R})} & \longrightarrow & G(\mathbb{R}) & \longrightarrow & 1.
\end{array}$$

Set $\sigma_{\mathbb{A}} = \sigma_{\mathbb{A}^f} - \sigma_{\mathbb{R}}$, where $\sigma_{\mathbb{A}^f}$ and $\sigma_{\mathbb{R}}$ are the 2-cocycles corresponding to the top and bottom extensions of these extensions respectively. It immediately follows that $\sigma_{\mathbb{A}}\big|_{G(\mathbb{Q})} = 0$ and thus the extension splits on $G(\mathbb{Q})$. Hence $\widetilde{G(\mathbb{R})}$ is the preimage in a metaplectic extension of $G(\mathbb{R})$. By the classification of metaplectic extensions, we have $n \leq 2$ as required. □

As a consequence, we have the following Corollary.

Corollary 1.5.3. *If there exists a congruence subgroup* Γ *that lifts to a connected* n*-fold cover of* $\mathrm{SU}(2,1)(\mathbb{R})$ *for some* $n \geq 3$*, then the congruence kernel of* $\mathrm{SU}(2,1)$ *is infinite.*

We stated in the previous section that there is a link between fractional weight multiplier systems on Γ and the congruence kernel. Given the previous Corollary, we can now make this clear by showing how the construction of a weight $1/n$ multiplier system on Γ gives us a lift of Γ to a connected n-fold cover of $\mathcal{G}(\mathbb{R})$.

We know that $\mathcal{G}(\mathbb{R})$ has a connected n-fold cover for each positive integer n, and in fact we can construct the connected n-fold cover of $\mathcal{G}(\mathbb{R})$ in the following way.

First, recall the construction of $\mathcal{H}$ and the blocks of matrices A,B,C and D used to decompose an element $g \in \mathrm{SU}(2,1)$ from section 1.5.1. Define $\widetilde{\mathcal{G}(\mathbb{R})}$ to be the set of pairs $(g, \varphi(v))$ such that $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathcal{G}(\mathbb{R})$ and $\varphi : \mathcal{H} \longrightarrow \mathbb{C}^\times$ is a continuous function satisfying $\varphi(v)^n = Cv + D$ for $v \in \mathcal{H}$. For each choice of $g \in \mathcal{G}(\mathbb{R})$ we have n choices of φ, and we define the group operation on $\widetilde{\mathcal{G}(\mathbb{R})}$ as

$$(g_1, \varphi_1(v))(g_2, \varphi_2(v)) = (g_1 g_2, (\varphi_1(g_2 v))\varphi_2(v)).$$

This makes $\widetilde{\mathcal{G}(\mathbb{R})}$ a group and an n-fold cover of $\mathcal{G}(\mathbb{R})$, and is in fact the connected n-fold cover. To see this, suppose that for each $g \in \mathcal{G}(\mathbb{R})$ we have fixed a function φ_g with $\varphi_g(v)^n = Cv + D$. This defines a section $\mathcal{G}(\mathbb{R}) \longrightarrow \widetilde{\mathcal{G}(\mathbb{R})}$ by $g \mapsto (g, \varphi_g(v))$. We construct a cocycle corresponding to the extension by

$$\Omega(g_1, g_2) = (g_1, \varphi_{g_1}(v))(g_2, \varphi_{g_2}(v))(g_1 g_2, \varphi_{g_1 g_2}(v))^{-1}.$$

Considering the restriction of this cocycle to the maximal torus $T(\mathbb{R}) \subset \mathcal{G}(\mathbb{R})$ and letting z be an element of order n in $T(\mathbb{R}) \cong \mathbb{C}^\times$, we construct the number

$$N = \prod_{i=1}^{n} \Omega(z, z^i). \tag{1.3}$$

Then $N \in \mathbb{Z}/n\mathbb{Z}$ has order n and depends only on the cohomology class of Ω. To see why N has order n, for $z \in T(\mathbb{R})$ of order n we take $z = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \bar{\lambda}/\lambda & 0 \\ 0 & 0 & \bar{\lambda}^{-1} \end{pmatrix} \in T(\mathbb{R})$ and choose $\varphi_z(v) = \bar{\lambda}^{-\frac{1}{n}} = \lambda^{\frac{1}{n}}$. Then noting that $(z, \varphi_{z^i})^{-1} = (z^{-1}, \varphi_{z^{-i}})$, we have

$$\begin{aligned} N &= \prod_{i=1}^{n} (z, \varphi_z)(z^i, \varphi_{z^i})(z^{i+1}, \varphi_{z^{i+1}})^{-1} \\ &= \left[(z, z^{\frac{1}{n}})(z, z^{\frac{1}{n}})(z^{-2}, z^{\frac{-2}{n}})\right] \cdots \left[(z, z^{\frac{1}{n}})(z^{n-1}, z^{\frac{n-1}{n}})\right]\left[(z, z^{\frac{1}{n}})(z^{-1}, z^{\frac{-1}{n}})\right] \\ &= (1,1)\cdots(1,z)(1,1) \\ &= (1,z). \end{aligned}$$

Since z has order n, N must also have order n. In order to show that $\widetilde{\mathcal{G}(\mathbb{R})}$ is the connected n-fold cover of $\mathcal{G}(\mathbb{R})$, we will show that for a disconnected n-fold cover of $\mathcal{G}(\mathbb{R})$, the value of N as constructed in equation 1.3 must have order dividing d where $d|n$ and $d < n$. So take an n-fold cover $\widehat{\mathcal{G}(\mathbb{R})}$ of $\mathcal{G}(\mathbb{R})$ which is not connected. Suppose $\widehat{H}$ denotes the connected component of $\widehat{\mathcal{G}(\mathbb{R})}$. Then $\widehat{H}$ is a d-fold cover for some $d|n$, $d \neq n$. We can then choose a section $s : \mathbb{C}^\times \longrightarrow \widehat{\mathcal{G}(\mathbb{R})}$ such that the image of s lies in $\widehat{H}$. Construct the 2-cocycle corresponding to s. This 2-cocycle must have image lying in $\mathbb{Z}/d\mathbb{Z}$ and so must have order dividing d. In particular, the number N as defined in equation 1.3 must have order dividing d for this 2-cocycle. Thus for the cocycle corresponding to the n-fold cover we constructed above, we must have $d = n$ and so must be connected.

Now, suppose that Γ lifts to $\widetilde{\mathcal{G}(\mathbb{R})}$. This means that for each $\gamma \in \Gamma$, we have an element $(\gamma, \varphi_\gamma) \in \widetilde{\mathcal{G}(\mathbb{R})}$, such that the map $\gamma \mapsto (\gamma, \varphi_\gamma)$ is a group homomorphism. This means we must have $(\gamma_1, \varphi_{\gamma_1}(v))(\gamma_2, \varphi_{\gamma_2}(v)) = (\gamma_1\gamma_2, \varphi_{\gamma_1\gamma_2}(v))$, but also $(\gamma_1, \varphi_{\gamma_1}(v))(\gamma_2, \varphi_{\gamma_2}(v)) = (\gamma_1\gamma_2, (\varphi_{\gamma_1}(\gamma_2 v))\varphi_{\gamma_2}(v))$, so that

$$(\gamma_1\gamma_2, (\varphi_{\gamma_1}(\gamma_2 v))\varphi_{\gamma_2}(v)) = (\gamma_1\gamma_2, \varphi_{\gamma_1\gamma_2}(v)),$$

which tells us that $j : \Gamma \times \mathcal{H} \longrightarrow \mathbb{C}^\times$ defined by $j(\gamma, v) = \varphi_\gamma(v)$ is a multiplier system on Γ. Furthermore, this is a weight $1/n$ multiplier system on Γ since clearly $j(\gamma, v)^n = Cv + D$.

We have shown how a lift of Γ to a connected n-fold cover of $\mathcal{G}(\mathbb{R})$ defines a weight $1/n$ multiplier system on Γ. The same argument follows in reverse to show that a weight $1/n$ multiplier system on Γ can be used to construct a lift of Γ to a connected n-fold cover of $\mathcal{G}(\mathbb{R})$. During the course of this thesis, we will develop and demonstrate the ideas used in this section on the construction of a lift of some congruence subgroup to a connected n-fold cover of $\mathcal{G}(\mathbb{R})$, as a new method to show that the congruence kernel is infinite. In the next chapter we will show how this idea generalises, allowing us to search for certain n-fold lifts of a congruence subgroup Γ' to an arithmetic group Γ, rather than lifts of Γ' to $\widetilde{\mathcal{G}(\mathbb{R})}$. The advantage of looking for lifts of Γ' to Γ has an advantage from a computational perspective, in that the calculations needed to be done to put into practice this method can be done directly through the fundamental domain of Γ. A description of how this may be done can be found in the concluding section of this thesis, when I discuss the application of our main theorem.

1.5.3 A Motivational Example

Take $\mathcal{G} = \mathrm{SU}(2,1)$ as above. Let $\tilde{\sigma} \in H^2(\mathcal{G}(\mathbb{R}), \mathbb{Z})$ correspond to the universal extension of $\mathcal{G}(\mathbb{R})$. Let $\tilde{\sigma}^{(n)}$ denote the image of $\tilde{\sigma}$ in $H^2(\mathcal{G}(\mathbb{R}), \mathbb{Z}/n\mathbb{Z})$ and fix an arithmetic subgroup $\Gamma = \mathrm{SU}(2,1)(\mathbb{Z})$. In [34] it is calculated that $H^2(\Gamma, \mathbb{Z}) \cong \mathbb{Z}$ for $\mathrm{SU}(2,1)$ defined using the field extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ and where Γ is the level 1 arithmetic subgroup. Suppose $\tilde{\sigma}\big|_\Gamma \in H^2(\Gamma, \mathbb{Z})$ generates $H^2(\Gamma, \mathbb{Z})$. Now, we have a short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{f} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

giving (see [5]) a long exact sequence

$$\cdots \longrightarrow H^2(\Gamma, \mathbb{Z}) \xrightarrow{\times n} H^2(\Gamma, \mathbb{Z}) \xrightarrow{f_*} H^2(\Gamma, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^3(\Gamma, \mathbb{Z}) \xrightarrow{\times n} \cdots .$$

Then

$$\tilde{\sigma}^{(n)}\big|_\Gamma = 0 \Longleftrightarrow \tilde{\sigma}\big|_\Gamma \in \ker(f_*) \Longleftrightarrow \tilde{\sigma}\big|_\Gamma = n\tau \quad \text{for some} \quad \tau \in H^2(\Gamma, \mathbb{Z}).$$

Thus the question of the existence of a congruence subgroup $\Gamma' \subset \Gamma$ lifting to a connected n-fold cover for $n \geq 3$ becomes: Given $\tilde{\sigma} \in H^2(\mathcal{G}(\mathbb{R}), \mathbb{Z})$ corresponding to the universal extension of $\mathcal{G}(\mathbb{R})$ such that $\sigma := \tilde{\sigma}\big|_{\Gamma}$ is a generator for $H^2(\Gamma, \mathbb{Z})$, is there a congruence subgroup Γ' such that $\sigma\big|_{\Gamma'}$ becomes a multiple of n for $n \geq 3$?

Chapter 2

Generalising Deligne's Theorem

In the previous chapter we introduced the congruence subgroup problem and outlined a method of approaching it. In this chapter we will develop further these ideas. First we must introduce some specific homological algebra that we will need. We then move onto the central object of study; $H^2_{cts}(K_f, \mathbb{Z}/q\mathbb{Z})$ and how we will calculate it. We will see that this calculation breaks into three cases, depending on whether a given prime p we are considering is split, inert or ramified in k. When p is a rational prime that splits in the imaginary quadratic extension k, $\mathcal{G}(\mathbb{Z}_p) = \mathrm{SL}_3(\mathbb{Z}_p)$. We will then demonstrate the theory we have developed by finding $H^1_{cts}(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$ and $H^2_{cts}(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$ for all split rational primes p and all but finitely many primes q. The corresponding calculations for p inert and ramified are considered in the last two chapters.

2.1 Some Homological Algebra

This section is devoted to developing the specific aspects of homological algebra that will play a role in what we do later. As usual, we will denote the n-dimensional cohomology group of a group G with coefficients in a G-module A by $H^n(G, A)$. The n-th continuous cochain cohomology group of G with coefficients in A will be denoted $H^n_{cts}(G, A)$. We start by introducing the general theory we will need, then taking a compact open subgroup $K_f \subset \mathrm{SU}(2,1)(\mathbb{A}^f_{\mathbb{Q}})$ as we did above and setting $\Gamma = \Gamma(K_f)$, we will develop some of the more specific theory we will use.

2.1.1 Technical Results

To begin, we recall two well-known results from the theory of cohomology of groups, the first of which can be found in Section 2 of [29].

Proposition 2.1.1. *Let G_i be a projective system of profinite groups and let A_i denote an inductive system of discrete G_i-modules. Then*

$$H^n_{cts}(\varprojlim G_i, \varinjlim A_i) = \varinjlim H^n(G_i, A_i) \quad \textit{for all} \quad n \geq 0.$$

We will make frequent use of spectral sequences later on during calculations and a particularly useful tool will be the *Hochschild-Serre Spectral Sequence*; this and detailed introductory accounts of the theory of spectral sequences can be found in [22] and [31].

Theorem 2.1.2. (Hochschild-Serre Spectral Sequence) *Let G denote a profinite group, H a closed normal subgroup and let A be a discrete G-module. There exists a spectral sequence*

$$E_2^{rs} = H^r_{cts}(G/H, H^s_{cts}(H, A)) \Longrightarrow H^{r+s}_{cts}(G, A).$$

We also need to introduce some more technical theory in order to deal with the groups we will be looking at. Almost all of this can be found in Section 1 and the first part of Section 2 of Casselman and Wigner, [7]. We take G to be a locally compact, totally disconnected group and A will be a continuous G-module, meaning that the action $G \times A \to A$ is continuous. For two G-modules U and V, we denote the set of continuous homomorphisms from U to V by $\mathrm{Hom}_{cts}(U, V)$. We take the following definitions from [7].

Definition 2.1.3. *Let A, B, U and V be G-modules. Then*

(i) a strong G-injection *of A into B is a G-morphism which has a continuous left inverse, and*

(ii) A is continuously injective *if given a strong G-injection $f : U \to V$ and a G-morphism $\alpha : U \to A$, there exists a G-extension of α to V.*

Let $C^n(G, A)$ denote the collection of continuous n-cochains on G with values in A, and similarly $Z^n(G, A)$ the set of n-cocycles and $B^n(G, A)$ the set of n-boundaries.

Following Section 1 of [7], we give each $C^n(G, A)$ the compact open topology. From the topology on the cochain spaces, we obtain a topology on the cohomology groups $H^n_{cts}(G, A)$. We will say that $H^n_{cts}(G, A)$ is *strongly Hausdorff* if the injection of $B^n(G, A) \cong C^{n-1}(G, A)/Z^{n-1}(G, A)$ into $Z^n(G, A)$ is a strong injection.

Let H be a closed subgroup of G and let A be a H-module. As usual, we define $\mathrm{ind}_H^G(A)$ to be the set of continuous maps $f : G \to A$ such that $f(gh) = h^{-1}f(g)$ for all $h \in H$, $g \in G$. By Section 1 of [7], if A is continuously injective as a H-module, then $\mathrm{ind}_H^G(A)$ is continuously injective as a G-module. We will also be interested in the instance when H is the trivial group, and we denote this specific case by $C(G, A)$. Since every A is continuously injective with respect to the trivial group, $C(G, A)$ is continuously injective as a G-module. More generally, one can use this to see that the collection of n-cochains are continuously injective G-modules for each n. We will need the following facts.

Theorem 2.1.4. *Suppose G is a locally compact and totally disconnected topological group, let H be a closed subgroup of G and $p \in \mathbb{Z}$ a prime. Then*

(i) $C(G, \mathbb{Z}/p\mathbb{Z})$ is continuously injective as a H-module, thus

$$H^n(H, C(G, \mathbb{Z}/p\mathbb{Z})) = 0,$$

for all $n > 0$.

(ii) Suppose H is also normal in G and A is as above. If the cohomology groups

$H^n(H, A)$ are strongly Hausdorff then there exists a spectral sequence

$$H^r_{cts}(G/H, H^s_{cts}(H, A)) \Longrightarrow H^{r+s}_{cts}(G, A).$$

The first part of this theorem is given by Proposition 4 of [7], and the second is Proposition 5 of [7].

Up until now in this chapter, the meaning of the notation G has varied depending upon the context. From now on, we will be applying these results to $\mathcal{G} = \mathrm{SU}(2,1)$. Before proving the two key Propositions of this section, we first need a couple of additional Lemmas.

Lemma 2.1.5. *Let $K_f \subset \mathcal{G}(\mathbb{A}^f)$ be a compact open subgroup, $p \in \mathbb{Z}$ prime and set $\Gamma = \Gamma(K_f)$. If $C(K_f, \mathbb{Z}/p\mathbb{Z})$ denotes the set of continuous functions from K_f to $\mathbb{Z}/p\mathbb{Z}$, then the cohomology groups*

$$H^n_{cts}(K_f, C(K_f, \mathbb{Z}/p\mathbb{Z})) \qquad \textit{and}$$
$$H^n_{cts}(\Gamma, C(K_f, \mathbb{Z}/p\mathbb{Z})),$$

are strongly Hausdorff.

Proof. We begin by noting that $C(K_f, \mathbb{Z}/p\mathbb{Z})$ is given the compact open topology. Since K_f is compact and $\mathbb{Z}/p\mathbb{Z}$ is discrete, it follows that $C(K_f, \mathbb{Z}/p\mathbb{Z})$ is discrete. By the same argument, $C^n(K_f, C(K_f, \mathbb{Z}/p\mathbb{Z}))$ is discrete, hence $Z^n(K_f, C(K_f, \mathbb{Z}/p\mathbb{Z}))$

is also discrete and it immediately follows that $H^n_{cts}(K_f, C(K_f, \mathbb{Z}/p\mathbb{Z}))$ is strongly Hausdorff.

We now consider $H^n_{cts}(\Gamma, C(K_f, \mathbb{Z}/p\mathbb{Z}))$. We note that Γ is *virtually torsion-free*, in the sense that Γ contains a torsion-free subgroup of finite index (see for instance Chapter VIII, Section 11 of [5]). Furthermore, the virtual cohomological dimension of Γ is finite, thus there exists some finite dimensional, contractible simplicial cell complex $\widetilde{X}$ with a simplicial Γ-action. We let X denote the quotient simplicial complex $X = \Gamma \setminus \widetilde{X}$ and denote by $X(n)$ and $\widetilde{X}(n)$ the set of n-simplices of X and $\widetilde{X}$ respectively. We construct a group

$$A^n = \left\{ f : \widetilde{X}(n) \longrightarrow C(K_f, \mathbb{Z}/p\mathbb{Z}) \right\}.$$

We regard A^n as a Γ-module with Γ-action given by $\gamma \circ f(\Delta) = \gamma f(\gamma^{-1}\Delta)$, where $\gamma \in \Gamma$, $f \in \ A^n$ and $\Delta \in X(n)$. We give A^n the compact open topology and recall (see for instance Chapter VII, Section 7 of [5]) that we have a decomposition $A^n \cong \bigoplus_\sigma \mathrm{ind}_{\Gamma_\sigma}^{\Gamma} C(K_f, \mathbb{Z}/p\mathbb{Z})$, where $\sigma \in \Gamma \setminus \widetilde{X}(n)$ runs through a set of representatives and Γ_σ is the stabiliser subgroup of σ. Each $\mathrm{ind}_{\Gamma_\sigma}^{\Gamma} C(K_f, \mathbb{Z}/p\mathbb{Z})$ has the compact open topology. Now, $C(K_f, \mathbb{Z}/p\mathbb{Z})$ is continuously injective as a Γ_σ-module, so $\mathrm{ind}_{\Gamma_\sigma}^{\Gamma} C(K_f, \mathbb{Z}/p\mathbb{Z})$ is continuously injective as a Γ-module and so each A^n is continuously injective as a Γ-module. We thus obtain an exact sequence of

Γ-modules

$$0 \longrightarrow C(K_f, \mathbb{Z}/p\mathbb{Z}) \longrightarrow A^0 \longrightarrow A^1 \longrightarrow \cdots,$$

which is an injective resolution of $C(K_f, \mathbb{Z}/p\mathbb{Z})$. It is sufficient to show that $(A^n)^\Gamma$ is discrete for each n. This is true since each $\operatorname{ind}_{\Gamma_\sigma}^{\Gamma}(C(K_f, \mathbb{Z}/p\mathbb{Z}))^\Gamma$ is discrete. □

Now, recall the following definitions from Chapter VIII, Section 4 of [5]. A resolution or partial resolution (P_i) of an R-module A is said to be of *finite type* if each P_i is finitely generated. We say that A is of type FP_n for an integer $n \geq 0$ if there exists a partial projective resolution $P_n \to \cdots \to P_0 \to A \to 0$ of finite type.

Definition 2.1.6. *An R-module A is of type FP_∞ if it satisfies one of the following equivalent conditions;*

(i) A has a free resolution of finite type,

(ii) A has a projective resolution of finite type,

(iii) A is of type FP_n for all integers $n \geq 0$.

Applying the above definitions to the specific case $R = \mathbb{Z}\Gamma$ and $A = \mathbb{Z}$, we say that Γ is of type FP_n for $0 \leq n \leq \infty$ if $\mathbb{Z}$ is of type FP_n as a $\mathbb{Z}\Gamma$-module.

Lemma 2.1.7. *Let A_i denote an inductive system of $\mathbb{Z}\Gamma$-modules. Then*

$$\varinjlim H^n(\Gamma, A_i) \cong H^n(\Gamma, \varinjlim A_i),$$

that is, $H^n(\Gamma, -)$ *commutes with direct limits.*

Proof. By Proposition 4.6, Chapter VIII of [5], we are required to show that Γ is of type FP_∞. Since any arithmetic group contains a torsion-free subgroup of finite index, we may choose $\Gamma' \subset \Gamma$ to be such a subgroup. It follows from the work in Chapter VIII, Sections 9 and 11 of [5], that Γ' is of type FP_∞. However, Proposition 5.1 in Chapter VIII of [5] states that if $\Gamma' \subset \Gamma$ has finite index, then Γ is of type FP_n for some $0 \leq n \leq \infty$ if and only if Γ' is of type FP_n. It follows from these results that Γ is of type FP_∞, as required. □

We are now in a position to state and prove the following two Propositions. Before we do, recall that we are denoting the set of continuous functions from K_f to $\mathbb{Z}/p\mathbb{Z}$ by $C(K_f, \mathbb{Z}/p\mathbb{Z})$, and we will often abbreviate this to just $C(K_f)$ when no confusion can arise.

Proposition 2.1.8. *Let* $K_f \subset \mathcal{G}(\mathbb{A}^f)$ *be a compact open subgroup,* $p \in \mathbb{Z}$ *prime and set* $\Gamma = \Gamma(K_f)$*. Let*

$$\overline{H}^s = \varinjlim H^s(\Gamma', \mathbb{Z}/p\mathbb{Z}),$$

where the inductive limit is taken over congruence subgroups $\Gamma' \subset \Gamma$*. We can then construct a spectral sequence*

$$H^r_{cts}\left(K_f, \overline{H}^s\right) \Longrightarrow H^{r+s}\left(\Gamma, \mathbb{Z}/p\mathbb{Z}\right).$$

Proof. By Shapiro's Lemma, we have

$$\begin{aligned} H^s(\Gamma', \mathbb{Z}/p\mathbb{Z}) &= H^s(\Gamma, \mathrm{ind}_{\Gamma'}^{\Gamma}(\mathbb{Z}/p\mathbb{Z})) \\ &= H^s\left(\Gamma, \left\{\text{functions } f : \Gamma/\Gamma' \to \mathbb{Z}/p\mathbb{Z}\right\}\right). \end{aligned}$$

Thus by Lemma 2.1.7 and the strong approximation theorem,

$$\begin{aligned} \overline{H}^s &= \varinjlim H^s(\Gamma', \mathbb{Z}/p\mathbb{Z}) \\ &= H^s(\Gamma, C(K_f, \mathbb{Z}/p\mathbb{Z})). \end{aligned}$$

Now, $C(K_f)$ is a $\Gamma \times K_f$-module, where Γ acts by left translation and K_f by right translation. By Lemma 2.1.5, the cohomology groups $H^s_{cts}(K_f, C(K_f, \mathbb{Z}/p\mathbb{Z}))$ and $H^s_{cts}(\Gamma, C(K_f, \mathbb{Z}/p\mathbb{Z}))$ are strongly Hausdorff and so applying Theorem 2.1.4, we have two spectral sequences converging to the same object;

$$H^r(\Gamma, H^s_{cts}(K_f, C(K_f))) \implies H^{r+s}(\Gamma \times K_f, C(K_f)) \tag{2.1}$$

$$H^r_{cts}(K_f, \overline{H}^s) \implies H^{r+s}(\Gamma \times K_f, C(K_f)). \tag{2.2}$$

Note that

$$
\begin{aligned}
H^s_{cts}(K_f, C(K_f)) &= H^s_{cts}(K_f, \mathrm{ind}_1^{K_f}(\mathbb{Z}/p\mathbb{Z})) \\
&= H^s(1, \mathbb{Z}/p\mathbb{Z}) \qquad \text{(Shapiro's Lemma, [7])} \\
&= \begin{cases} \mathbb{Z}/p\mathbb{Z} & s = 0 \\ 0 & s > 0, \end{cases}
\end{aligned}
$$

hence from equation (2.1), $H^r(\Gamma, \mathbb{Z}/p\mathbb{Z}) \cong H^r(\Gamma \times K_f, C(K_f))$. Equation (2.2) then gives us the desired result,

$$H^r_{cts}(K_f, \overline{H}^s) \Longrightarrow H^{r+s}(\Gamma, \mathbb{Z}/p\mathbb{Z}).$$

□

Proposition 2.1.9. *Letting* Cong$(\mathcal{G})$ *denote the congruence kernel of* $\mathcal{G}$ *and with the notation of Proposition 2.1.8, we have*

$$\overline{H}^1 \cong \mathrm{Hom}_{cts}(\mathrm{Cong}(\mathcal{G}), \mathbb{Z}/p\mathbb{Z}).$$

Proof. Recall that Cong$(\mathcal{G})$ fits into the short exact sequence

$$1 \longrightarrow \mathrm{Cong}(\mathcal{G}) \longrightarrow \overline{K_f} \longrightarrow K_f \longrightarrow 1,$$

where $\overline{K_f} = \varprojlim \Gamma/\Gamma'$ with the projective limit taken over all normal subgroups of Γ of finite index. We consider $C\left(\overline{K_f}, \mathbb{Z}/p\mathbb{Z}\right)$ as a $\Gamma \times \mathrm{Cong}(\mathcal{G})$-module, where Γ acts by left translation and $\mathrm{Cong}(\mathcal{G})$ acts by right translation. Again by Theorem 2.1.4, we have two spectral sequences converging to the same object,

$$H^r_{cts}\left(\mathrm{Cong}(\mathcal{G}), H^s\left(\Gamma, C\left(\overline{K_f}\right)\right)\right) \implies H^{r+s}_{cts}\left(\Gamma \times \mathrm{Cong}(\mathcal{G}), C\left(\overline{K_f}\right)\right) \qquad (2.3)$$

$$H^r\left(\Gamma, H^s_{cts}\left(\mathrm{Cong}(\mathcal{G}), C\left(\overline{K_f}\right)\right)\right) \implies H^{r+s}_{cts}\left(\Gamma \times \mathrm{Cong}(\mathcal{G}), C\left(\overline{K_f}\right)\right). \qquad (2.4)$$

Looking at equation (2.4) and using Theorem (2.1.4), we see that

$$H^s_{cts}\left(\mathrm{Cong}(\mathcal{G}), C\left(\overline{K_f}, \mathbb{Z}/p\mathbb{Z}\right)\right) = \begin{cases} C(K_f, \mathbb{Z}/p\mathbb{Z}) & s = 0 \\ 0 & s > 0. \end{cases}$$

So the spectral sequence (2.4) degenerates and we have $H^r\left(\Gamma, C(K_f, \mathbb{Z}/p\mathbb{Z})\right) = H^r_{cts}\left(\Gamma \times \mathrm{Cong}(\mathcal{G}), C\left(\overline{K_f}, \mathbb{Z}/p\mathbb{Z}\right)\right)$. Using this and spectral sequence (2.3), we have an exact sequence of low degree terms

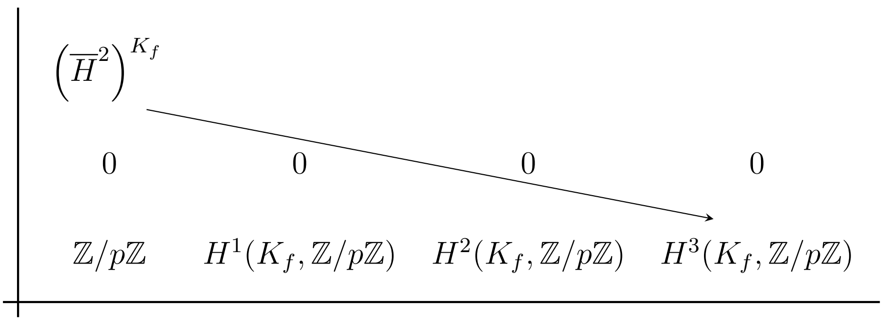
$$1 \longrightarrow H^1_{cts}\left(\mathrm{Cong}(\mathcal{G}), H^0\left(\Gamma, C\left(\overline{K_f}\right)\right)\right) \longrightarrow H^1(\Gamma, C(K_f)) \longrightarrow$$
$$\longrightarrow H^0\left(\mathrm{Cong}(\mathcal{G}), H^1\left(\Gamma, C\left(\overline{K_f}\right)\right)\right).$$

First, $H^0\left(\Gamma, C\left(\overline{K_f}\right)\right) = \mathbb{Z}/p\mathbb{Z}$ since Γ is dense in $\overline{K_f}$, and secondly

$$H^1\left(\Gamma, C\left(\overline{K_f}, \mathbb{Z}/p\mathbb{Z}\right)\right) = \varinjlim H^1(\Gamma', \mathbb{Z}/p\mathbb{Z}),$$

where the direct limit is taken over all normal subgroups $\Gamma' \subset \Gamma$ of finite index. Now, suppose $f \in H^1(\Gamma', \mathbb{Z}/p\mathbb{Z})$ is non-trivial. Let $\Gamma'' = \ker(f)$, so that $f\big|_{\Gamma''} = 0$. Then we see that the image of f in the direct limit $\varinjlim H^1(\Gamma', \mathbb{Z}/p\mathbb{Z})$ is in fact zero, hence $\varinjlim H^1(\Gamma', \mathbb{Z}/p\mathbb{Z}) = 0$. It immediately follows that $H^1(\mathrm{Cong}(\mathcal{G}), \mathbb{Z}/p\mathbb{Z}) \cong \overline{H^1}$. □

This proposition is key to our generalisation of Deligne's Theorem, since it says that if $\mathrm{Cong}(\mathcal{G}) = 1$ then $\overline{H}^1 = 0$. Writing out the individual terms of the spectral sequence in Proposition 2.1.8 with the assumption that $\mathrm{Cong}(\mathcal{G}) = 1$, we arrive at the following E_3-sheet.



This gives us the following 3-term exact sequence,

$$
\begin{array}{ccccccc}
0 \longrightarrow H^2_{cts}(K_f, \mathbb{Z}/p\mathbb{Z}) & \xrightarrow{res} & H^2(\Gamma, \mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\quad\Phi\quad} & \left(\overline{H}^2\right)^{K_f} . \\
 & & & & \| \\
 & & & & \left(\varinjlim H^2(\Gamma', \mathbb{Z}/p\mathbb{Z})\right)^{K_f}
\end{array}
$$

In particular,

$$
\begin{aligned}
\ker(\Phi) &= \ker\left(H^2(\Gamma, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \overline{H}^2\right) \\
&= \left\{\sigma \in H^2(\Gamma, \mathbb{Z}/p\mathbb{Z}) : \exists\, \Gamma' \subset \Gamma \text{ with } \sigma\big|_{\Gamma'} = 0\right\},
\end{aligned}
$$

where Γ' is a congruence subgroup. We arrive at the following theorem.

Theorem 2.1.10. *If* $\mathrm{Cong}(\mathcal{G}) = 1$, *then* $\ker(\Phi) = H^2_{cts}(K_f, \mathbb{Z}/p\mathbb{Z})$.

We can calculate $H^2(K_f, \mathbb{Z}/p\mathbb{Z})$ in many cases and often it will be 0. When it is true that $H^2(K_f, \mathbb{Z}/p\mathbb{Z}) = 0$, our assumption that the congruence kernel is trivial means that $H^2(\Gamma, \mathbb{Z}/p\mathbb{Z})$ must inject into $H^2(\Gamma', \mathbb{Z}/p\mathbb{Z})$ for all congruence subgroups $\Gamma' \subset \Gamma$ by our work above. However, if $H^2(K_f, \mathbb{Z}/p\mathbb{Z}) = 0$ but we can find a congruence subgroup Γ' and a non-trivial cocycle $\sigma \in H^2(\Gamma, \mathbb{Z}/p\mathbb{Z})$ such that $\sigma\big|_{\Gamma'} = 0$, we will have demonstrated that the congruence kernel is infinite.

2.1.2 A Result Involving $H^2(V, \mathbb{F}_p)$

The aim of this section is to prove a useful result needed later on. During this section we let $p \in \mathbb{Z}$ be prime, $\mathbb{F}_p$ the field of p elements and $\widetilde{G}$ be a group such that $V \trianglelefteq \widetilde{G}$ is an n-dimensional $\mathbb{F}_p$-vector space. We thus have a conjugation action of $G := \widetilde{G}/V$ on V and we suppose throughout this section that $\mathbb{F}_p$ is a trivial $\widetilde{G}$-module. Denoting the dual space $\mathrm{Hom}(V, \mathbb{F}_p)$ of V by V^*, we aim to prove that as a G-module, $H^2(V, \mathbb{F}_p)$ fits into a short exact sequence of G-modules in the following way;

$$0 \longrightarrow V^* \longrightarrow H^2(V, \mathbb{F}_p) \longrightarrow \bigwedge^2 V^* \longrightarrow 0.$$

As usual, $\bigwedge^2 V^*$ denotes the second exterior power of V^*. We begin by recalling the following short exact sequence given by the Universal Coefficient Theorem,

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}(H_1(V, \mathbb{Z}), \mathbb{F}_p) \longrightarrow H^2(V, \mathbb{F}_p) \longrightarrow \mathrm{Hom}(H_2(V, \mathbb{Z}), \mathbb{F}_p) \longrightarrow 0. \qquad (2.5)$$

Recall that $H_2(V, \mathbb{Z})$ is the Schur multiplier of V which by [18], can also be realised in the following way,

$$H_2(V, \mathbb{Z}) \cong \ker\left(V \wedge V \xrightarrow{\delta} [V, V]\right)$$
$$\delta(v \wedge w) \longmapsto [v, w]\,,$$

where $[v, w]$ denotes the commutator of $v, w \in V$. Since V is an abelian group, this says that $H_2(V, \mathbb{Z}) \cong V \wedge V$ and furthermore, $H_1(V, \mathbb{Z}) \cong V$ so equation (2.5) becomes

$$0 \longrightarrow \operatorname{Ext}^1_{\mathbb{Z}}(V, \mathbb{F}_p) \longrightarrow H^2(V, \mathbb{F}_p) \longrightarrow \operatorname{Hom}(V \wedge V, \mathbb{F}_p) \longrightarrow 0.$$

We now construct an explicit G-module homomorphism between $H^2(V, \mathbb{F}_p)$ and $\operatorname{Hom}(V \wedge V, \mathbb{F}_p)$. Following Definition 1.1 of [14], if we take $\sigma \in Z^2(V, \mathbb{F}_p)$ and $v, w \in V$, we can construct a map $[-,-]_\sigma : V \times V \longrightarrow \mathbb{F}_p$ given by $[v, w]_\sigma := \sigma(v, w) - \sigma(w, v)$. Note that this map differs from taking commutators of elements of V used above and its difference will be signified in the notation by the explicit use of the 2-cocycle in the subscript. By Theorem 1.2 of [14], this map has properties which we summarise in the following Lemma.

Lemma 2.1.11. *(i) The map $[-,-]_\sigma$ depends only on the cohomology class $[\sigma]$ of σ, and*

(ii) $[-,-]_\sigma$ is bilinear and skew-symmetric.

As a result, we have a well-defined homomorphism

$$\begin{aligned} \mathcal{C} : H^2(V, \mathbb{F}_p) &\longrightarrow \left(\bigwedge^2 V\right)^* \\ [\sigma] &\longmapsto [-,-]_\sigma \quad \text{where} \\ [v, w]_\sigma &:= \sigma(v, w) - \sigma(w, v), \end{aligned}$$

for $\sigma \in H^2(V, \mathbb{F}_p)$ and $v, w \in V$. Furthermore, this homomorphism is easily seen to be G-equivariant, since for $\sigma \in H^2(V, \mathbb{F}_p)$, $v, w \in V$ and $g \in G$ we have

$$[v, w]_{g \circ \sigma} = (g \circ \sigma)(v, w) - (g \circ \sigma)(w, v) = \sigma({}^g v, {}^g w) - \sigma({}^g w, {}^g v) = [{}^g v, {}^g w]_\sigma\,,$$

which shows that $\mathcal{C}(g \circ \sigma) = g \circ \mathcal{C}(\sigma)$. Since $\left(\bigwedge^2 V\right)^* \cong \bigwedge^2 V^*$ as G-modules, we have defined a map from $H^2(V, \mathbb{F}_p)$ to $\bigwedge^2 V^*$. The kernel of the map $\mathcal{C}$ consists of all cocycles $\sigma \in H^2(V, \mathbb{F}_p)$ such that $\sigma(v, w) = \sigma(w, v)$ for all $v, w \in V$. We call these *symmetric cocycles* and we denote the collection of all such cocycles by $H^2_{sym}(V, \mathbb{F}_p)$. The group of symmetric 2-cocycles is precisely $\mathrm{Ext}^1_{\mathbb{Z}}(V, \mathbb{F}_p)$, thus we have a short exact sequence of G-modules

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}(V, \mathbb{F}_p) \longrightarrow H^2(V, \mathbb{F}_p) \longrightarrow \bigwedge^2 V^* \longrightarrow 0. \qquad (2.6)$$

It remains to show that $V^* \cong \mathrm{Ext}^1_{\mathbb{Z}}(V, \mathbb{F}_p)$ as G-modules. We can suppose that without loss of generality, the group G acting on V is $\mathrm{GL}_n(\mathbb{Z})$. Consider the short exact sequence given by

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{\times p} \mathbb{Z}^n \longrightarrow V \longrightarrow 0,$$

which gives is an exact sequence of G-modules

$$0 \longrightarrow \mathrm{Hom}(V, \mathbb{F}_p) \longrightarrow \mathrm{Hom}(\mathbb{Z}^n, \mathbb{F}_p) \xrightarrow{\times p} \mathrm{Hom}(\mathbb{Z}^n, \mathbb{F}_p) \longrightarrow$$
$$\longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}(V, \mathbb{F}_p) \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{F}_p) \longrightarrow \cdots .$$

Since $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{F}_p) = 0$ and the multiplication by p map is just the 0 map in this instance, we have the following isomorphisms of G-modules:

$$\begin{aligned} \mathrm{Hom}(V, \mathbb{F}_p) &\cong \mathrm{Hom}(\mathbb{Z}^n, \mathbb{F}_p) \quad \text{and} \\ \mathrm{Hom}(\mathbb{Z}^n, \mathbb{F}_p) &\cong \mathrm{Ext}^1_{\mathbb{Z}}(V, \mathbb{F}_p). \end{aligned}$$

Thus $V^* = \mathrm{Hom}(V, \mathbb{F}_p) \cong \mathrm{Ext}^1_{\mathbb{Z}}(V, \mathbb{F}_p)$ as G-modules and we have the short exact sequence of G-modules

$$0 \longrightarrow V^* \longrightarrow H^2(V, \mathbb{F}_p) \longrightarrow \bigwedge^2 V^* \longrightarrow 0,$$

as required. We have thus proved the following Lemma.

Lemma 2.1.12. *Let $\widetilde{G}$ be a group and V be an n-dimensional vector space over a finite field $\mathbb{F}_p$ such that $V \trianglelefteq \widetilde{G}$. We have an action of $G := \widetilde{G}/V$ on V, making $H^2(V, \mathbb{F}_p)$ a G-module which fits into a short exact sequence of G-modules*

$$0 \longrightarrow V^* \longrightarrow H^2(V, \mathbb{F}_p) \longrightarrow \bigwedge^2 V^* \longrightarrow 0,$$

where $\bigwedge^2 V^*$ *is the second exterior power of* V^*.

2.2 Calculating $H^2(K_f, \mathbb{Z}/q\mathbb{Z})$

Fix a prime $q \in \mathbb{Z}$. In light of Theorem 2.1.10, our aim from here is to calculate $H^2(K_f, \mathbb{Z}/q\mathbb{Z})$ for $\mathcal{G} = \mathrm{SU}(2,1)$ defined over an imaginary quadratic extension k of $\mathbb{Q}$ and $K_f = \prod_p K_p$. Here, $p \in \mathbb{Z}$ is a rational prime and $K_p = \mathcal{G}(\mathbb{Z}_p)$ is a compact open subgroup of $\mathcal{G}(\mathbb{Q}_p)$. We first observe that

$$\begin{aligned} H^r(K_f, \mathbb{Z}/q\mathbb{Z}) &= H^r\left(\varprojlim_N \prod_{p<N} K_p, \mathbb{Z}/q\mathbb{Z}\right) \\ &= \varinjlim_N H^r\left(\prod_{p<N} K_p, \mathbb{Z}/q\mathbb{Z}\right) \qquad \text{(Proposition 2.1.1).} \end{aligned}$$

We can decompose the right hand side using the Künneth formula. The Künneth formula has a particularly simple description when q is prime, and as usual we will be writing $\mathbb{F}_q$ for the finite field with q elements. We have

$$H^r\left(\prod_{p<N} K_p, \mathbb{F}_q\right) = \bigoplus_{i_2+i_3+i_5+\cdots=r} \left(\bigotimes_{p<N} H^{i_p}(K_p, \mathbb{F}_q)\right).$$

In particular, for $r = 2$ we have

$$H^2\left(\prod_{p<N} K_p, \mathbb{F}_q\right) = \bigoplus_{p<N} H^2(K_p, \mathbb{F}_q) \oplus \bigoplus_{p_1<p_2<N} H^1(K_{p_1}, \mathbb{F}_q) \otimes H^1(K_{p_2}, \mathbb{F}_q).$$

The problem is now to calculate $H^r(K_p, \mathbb{F}_q)$ for $r = 1, 2$ and for each prime $p \in \mathbb{Z}$. If p splits in the field extension k then $\mathcal{G}(\mathbb{Z}_p) = \mathrm{SL}_3(\mathbb{Z}_p)$. If p is inert then we have $\mathcal{G}(\mathbb{Z}_p) = \mathrm{SU}(2,1)(\mathbb{Z}_p)$, so we consider the three cases separately; when p is split, inert and ramified. Certain notation and facts will be common to all three cases however, so we develop them here to avoid repetition.

For a fixed prime $p \in \mathbb{Z}$, let $\mathfrak{p}$ denote the maximal ideal of $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_k$ when p is not split. In the notation that follows, if p is split then we are taking $\mathfrak{p} = p$. With this in mind, we define

$$\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n) = \{g \in \mathcal{G}(\mathbb{Z}_p) : g \equiv I_d \mod \mathfrak{p}^n\}.$$

It is well known (see [24], Section 3.3) that these congruence subgroups form a basis of open neighbourhoods of the identity of $\mathcal{G}(\mathbb{Q}_p)$ and furthermore, $\mathcal{G}(\mathbb{Z}_p) = \varprojlim \mathcal{G}(\mathbb{Z}_p)/\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n)$. These groups give us the following filtration on $\mathcal{G}(\mathbb{Z}_p)$,

$$\mathcal{G}(\mathbb{Z}_p) \supset \mathcal{G}(\mathbb{Z}_p, \mathfrak{p}) \supset \cdots \supset \mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n) \supset \cdots. \tag{2.7}$$

Since we will make frequent use of this filtration, we will often abbreviate the notation by writing $\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n) = \mathcal{G}(n)$. We note that for all $n \geq 1$, $\mathcal{G}(\mathbb{Z}_p, \mathfrak{p})$, $\mathcal{G}(\mathbb{Z}_p, \mathfrak{p})/\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n)$ and $\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n)/\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^{n+1})$ are all pro-p groups (Lemma 3.8 of [24]). Quotients in this filtration act upon other quotients in the filtration; the action of $\mathcal{G}(0)$ on $\mathcal{G}(n)/\mathcal{G}(n+1)$ is by conjugation for all $n \geq 1$ and the action of

$\mathcal{G}(k)$ on $\mathcal{G}(n)/\mathcal{G}(n+1)$ is trivial for all $n, k \geq 1$. Thus we also have a conjugation action of $\mathcal{G}(0)/\mathcal{G}(1)$ upon $\mathcal{G}(n)/\mathcal{G}(n+1)$ for each $n \geq 1$. Here when p is inert, for a commutative ring A we are using

$$\mathrm{SU}(2,1)(A) = \left\{ g \in \mathrm{SL}_3(A \otimes_{\mathbb{Z}} \mathcal{O}_k) : g^t J \overline{g} = J \right\}.$$

In particular, $\mathcal{G}(0)/\mathcal{G}(1) \cong \mathrm{SU}(2,1)(\mathbb{F}_p) = \{g \in \mathrm{SL}_3(\mathbb{F}_{p^2}) : g^t J \overline{g} = J\}$ when p is inert. Since treating the split case turns out to be more straightforward than the ramified and inert cases, we will begin our calculations with p split in k.

2.3 p Split in k

Our aim in this section is to calculate $H^r(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$ for rational primes p, q and $r = 1, 2$. Throughout this section we will be assuming that p splits in the field k upstairs.

2.3.1 $H^1(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$

We will make use of the notion of a perfect group during a number of calculations. Recall that a group G is *perfect* if it equals its own commutator subgroup; that is, G is generated by commutators. We begin with the following Proposition, which completes the calculation of $H^1(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$ for all pairs of primes p, q.

Proposition 2.3.1. *The matrix group* $\mathrm{SL}_3(\mathbb{Z}_p)$ *is perfect for all primes* p.

Proof. Let $E_n(\mathbb{Z}_p)$ denote the subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ generated by all elementary matrices $e_{ij}(z)$ for $1 \leq i, j \leq n$ and $z \in \mathbb{Z}_p$. Recall that $e_{ij}(z)$ has 1's on the diagonal and z in the (i, j) position. Then $\mathrm{SL}_3(\mathbb{Z}_p) = E_3(\mathbb{Z}_p)$ by Proposition 5.4 (*ii*) of [17], and $E_3(\mathbb{Z}_p)$ is perfect by [32], completing the proof. □

Corollary 2.3.2. $H^1(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q) = 0$ *for all primes* p *and* q.

Proof. Since $\mathbb{F}_q$ is a trivial $\mathrm{SL}_3(\mathbb{Z}_p)$-module, $H^1(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q) = \mathrm{Hom}(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$. However, $\mathrm{SL}_3(\mathbb{Z}_p)$ is perfect by Proposition 2.3.1 and thus is generated by commutators. Subsequently, any homomorphism from $\mathrm{SL}_3(\mathbb{Z}_p)$ to the finite field $\mathbb{F}_q$ must be trivial, completing the proof. □

2.3.2 $H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$, $p \neq q$

After finding $H^1(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$ for all pairs of primes p and q, it remains to find $H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q)$; this divides into two cases, $p \neq q$ and $p = q$. In this section we will treat the case $p \neq q$. By the Hochschild-Serre spectral sequence (Theorem 2.1.2) we have

$$H^r(\mathcal{G}(\mathbb{Z}_p)/\mathcal{G}(\mathbb{Z}_p, p), H^s(\mathcal{G}(\mathbb{Z}_p, p), \mathbb{F}_q)) \Longrightarrow H^{r+s}\left(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q\right). \tag{2.8}$$

Since $\mathcal{G}(\mathbb{Z}_p, p)$ is a pro-p group, $H^0(\mathcal{G}(\mathbb{Z}_p, p), \mathbb{F}_q) = \mathbb{F}_q$ and $H^s(\mathcal{G}(\mathbb{Z}_p, p), \mathbb{F}_q) = 0$ for all $s > 0$. However, $\mathcal{G}(\mathbb{Z}_p)/\mathcal{G}(\mathbb{Z}_p, p) \cong \mathcal{G}(\mathbb{F}_p)$ and so from the spectral sequence 2.8

above,

$$H^r(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q) \cong H^r(\mathcal{G}(\mathbb{F}_p), \mathbb{F}_q).$$

Our aim is to calculate the right hand side of this isomorphism, which can be done using K-theory for all but a finite number of p and q. Following Milnor, Introduction to Algebraic K-Theory [19], let R denote a ring with $\lambda, \mu \in R$. For an integer $n \geq 3$ and distinct integers i, j with $1 \leq i, j \leq n$, the *Steinberg group* $\mathrm{St}_n(R)$ is the group defined by generators $x_{ij}(\lambda)$ subject to the relations

$$\begin{aligned} x_{ij}(\lambda)x_{ij}(\mu) &= x_{ij}(\lambda+\mu), \\ [x_{ij}(\lambda), x_{jl}(\mu)] &= x_{il}(\lambda\mu) \;\text{ for }\; i \neq l \;\text{ and} \\ [x_{ij}(\lambda), x_{kl}(\mu)] &= 1 \;\text{ for }\; j \neq k \;\text{ and }\; i \neq l. \end{aligned}$$

There is a canonical homomorphism $\phi : \mathrm{St}_n(R) \longrightarrow \mathrm{GL}_n(R)$ given by $\phi(x_{ij}(\lambda)) = e_{ij}(\lambda)$, where $e_{ij}(\lambda)$ is the elementary matrix with 1's on the diagonal and λ in the (i, j) position. Taking the direct limit of these groups over n, we obtain groups denoted by $\mathrm{St}(R)$ and $\mathrm{GL}(R)$ respectively, along with a canonical homomorphism $\mathrm{St}(R) \to \mathrm{GL}(R)$. The kernel of this homomorphism is denoted $K_2(R)$. In particular, let $\mathbb{F}$ denote any field and C_n the kernel of the map $\mathrm{St}_n(\mathbb{F}) \to \mathrm{SL}_n(\mathbb{F})$, then by Corollary 11.2 of [19], for all $n \geq 3$ the groups C_n are canonically isomorphic to each other and to their direct limit $K_2(\mathbb{F})$. Furthermore, provided we exclude the exceptional cases $\mathrm{SL}_3(\mathbb{F}_2)$, $\mathrm{SL}_3(\mathbb{F}_4)$ and $\mathrm{SL}_4(\mathbb{F}_2)$, we have isomorphisms

$$H^2(\mathrm{SL}_3(\mathbb{F}), \mathbb{F}_q) \cong \mathrm{Hom}(H_2(\mathrm{SL}_3(\mathbb{F})), \mathbb{F}_q) \cong \mathrm{Hom}(K_2(\mathbb{F}), \mathbb{F}_q).$$

However, (see Chapter 4, Section 3, Page 213 of [27]) $K_2(\mathbb{F}_p) = 1$ for every finite field. We conclude that $H^2(\mathrm{SL}_3(\mathbb{F}_p), \mathbb{F}_q) = 0$ for $p > 2$ and all q.

The case $H^2(\mathrm{SL}_3(\mathbb{F}_2), \mathbb{F}_q)$ with $q > 2$ can be dealt with separately. To do this, recall that the order of $\mathrm{SL}_3(\mathbb{F}_p)$ is $p^3(p^2-1)(p^3-1)$, thus $|\mathrm{SL}_3(\mathbb{F}_2)| = 2^3 \times 3 \times 7$. It is well-known that $H^n(G, M) = 0$ for all $n > 0$ when G is any finite group whose order is invertible in some G-module M (see [5]). This leaves us to consider the cases $q = 3, 7$ which can be done by looking at the q-Sylow subgroups of $\mathrm{SL}_3(\mathbb{F}_2)$.

In order to do this we will first indroduce some theory, all of which can be found in either Chapter III of [5] or Chapter XII of [6]. Let G denote a finite group, H a subgroup and M a G-module. We have a homomorphism given by

$$\mathrm{res}_H^G : H^*(G, M) \longrightarrow H^*(H, M),$$

called *restriction*. Taking $g \in G$, we also have isomorphisms

$$c_g : H^*(H, M) \longrightarrow H^*(gHg^{-1}, M).$$

The constructions of these maps can be found in both [5] and [6]. We say that an element $z \in H^*(H, M)$ is *G-invariant* if for all $g \in G$, we have

$$\operatorname{res}^{H}_{H \cap gHg^{-1}} z = \operatorname{res}^{gHg^{-1}}_{H \cap gHg^{-1}} c_g z.$$

Now suppose G_q is a q-Sylow subgroup of G, and M is as above. By Theorem 10.1 of [6], we have a monomorphism

$$H^n(G, M) \hookrightarrow H^n(G_q, M),$$

whose image is the set of G-invariant elements of $H^n(G_q, M)$. A specific instance of this is when for all $g \in G$, either $gG_qg^{-1} = G_q$ or $G_q \cap gG_qg^{-1} = 1$, in which case

$$H^n(G, M) = H^n(G_q, M)^{N_G(G_q)/G_q}.$$

We will often find that our q-Sylow subgroups are either cyclic groups or products of cyclic groups. In order to prove the statements below, we will need a fact concerning the cohomology of cyclic groups that will also be useful to us later on. Firstly, recall that the cohomology ring $H^\bullet(C_p, \mathbb{F}_p)$ of the cyclic group C_p acting trivially on the coefficient module $\mathbb{F}_p$ is given by

$$H^\bullet(C_p, \mathbb{F}_p) \cong \mathbb{F}_p\,[X, Y] \,/\, \left\langle X^2 = 0 \right\rangle, \tag{2.9}$$

where X is in degree 1 and Y is in degree 2 (see Section 6.7 of [31]). In particular, $H^n(C_p, \mathbb{F}_p) \cong \mathbb{F}_p$ for all n. The Sylow subgroups of the groups we will be considering will often be cyclic and when this does happen, we will often have a conjugation action of an element $g \in G$ on this cyclic subgroup. We will be interested in how this action translates into an action on $H^n(C_p, \mathbb{F}_p)$.

Lemma 2.3.3. *Let $\mathbb{Z}/p\mathbb{Z}$ act trivially on $\mathbb{F}_p$, and suppose G is a group with a conjugation action on $\mathbb{Z}/p\mathbb{Z}$ which can be written as ${}^g a = x \times a$ for some $x \in \mathbb{F}_p^\times$, any $a \in \mathbb{Z}/p\mathbb{Z}$ and $g \in G$. If G also acts trivially on $\mathbb{F}_p$, then $g \in G$ acts on $\varphi \in H^1(\mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p)$ by $g \circ \varphi = x^{-1} \times \varphi$ and on $\sigma \in H^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p)$ by $g \circ \sigma = x^{-1} \times \sigma$.*

Proof. Take any $\varphi \in H^1(\mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p) \cong \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p)$. Then for any $g \in G$ and $a \in \mathbb{Z}/p\mathbb{Z}$,

$$\begin{aligned} g \circ \varphi(a) &= \varphi(g^{-1} \circ a) \\ &= \varphi(x^{-1} a) \\ &= x^{-1} \varphi(a) \qquad \text{(since } \varphi \text{ is } \mathbb{F}_p\text{-linear)}, \end{aligned}$$

so G acts by multiplication by x^{-1} on $H^1(\mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p)$.

To find its action on $H^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p)$, we first construct an explicit cocycle $\sigma \in H^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p)$ by considering the short exact sequence

$$1 \longrightarrow \mathbb{F}_p \xrightarrow{i} \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 1,$$

where the map i is multiplication by p. Explicit computation shows that the cocycle corresponding to this extension is

$$\sigma(a,b) = \begin{cases} 1 & a+b \geq p \\ 0 & \text{otherwise} \end{cases} \qquad a,b \in \{0,1,\cdots,p-1\}\,.$$

This gives an isomorphism

$$\begin{aligned} H^2(\mathbb{Z}/p\mathbb{Z},\mathbb{F}_p) &\longrightarrow \mathbb{F}_p \\ \tau &\longmapsto \tau(1,0)+\tau(1,1)+\cdots+\tau(1,p-1), \end{aligned}$$

noting that $\sigma \mapsto 1$. Then $g \circ \sigma(a,b) = \sigma(g^{-1}\circ a, g^{-1}\circ b) = \sigma(x^{-1}a, x^{-1}b)$, so that

$$\begin{aligned} g\circ\sigma &\longmapsto \sigma(x^{-1},0)+\sigma(x^{-1},x^{-1})+\cdots+\sigma(x^{-1},x^{-1}(p-1)) \\ &= \sigma(x^{-1},0)+\sigma(x^{-1},1)+\cdots+\sigma(x^{-1},p-1) \\ &= \sum_{\substack{i\in\mathbb{Z}/p\mathbb{Z} \\ i+x^{-1}\geq p}} 1 \\ &= x^{-1}. \end{aligned}$$

Thus $g \in G$ also acts on $H^2(\mathbb{Z}/p\mathbb{Z},\mathbb{F}_p)$ by multiplication by x^{-1}, completing the proof. □

We can now prove the following Proposition.

Proposition 2.3.4. *$H^2(\mathrm{SL}_3(\mathbb{F}_2), \mathbb{F}_3) = 0$.*

Proof. Clearly the 3-Sylow subgroup is the cyclic group C_3 and since the action of $\mathrm{SL}_3(\mathbb{F}_2)$ on $\mathbb{F}_3$ is trivial, so is the action of C_3. By equation (2.9), we have an injection

$$H^n(\mathrm{SL}_3(\mathbb{F}_2), \mathbb{F}_3) \hookrightarrow \mathbb{F}_3 \qquad \text{for all } n > 0.$$

Consider the following two elements in $\mathrm{SL}_3(\mathbb{F}_2)$:

$$\alpha = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and}$$

$$\beta = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that α has order 3 and so can be taken as a generator of the 3-Sylow subgroup of $\mathrm{SL}_3(\mathbb{F}_2)$. On the other hand, β has order 2 and its conjugation action on α sends α to α^{-1}. Thus β acts upon the generator X of degree 1 in the cohomology ring $H^\bullet(C_3, \mathbb{F}_3)$ by $X \mapsto -X$ (in the additive notation of $H^1(C_3, \mathbb{F}_3)$). Hence by Lemma 2.3.3, β also acts on Y in degree 2 by $Y \mapsto -Y$. Since this means that $Y \mapsto -Y$ under the action of $\beta \in \mathrm{SL}_3(\mathbb{F}_2)$, it follows that there are no $\mathrm{SL}_3(\mathbb{F}_2)$-invariant elements in $H^2(C_3, \mathbb{F}_3)$. □

We can consider the case $q = 7$ in a similar way.

Proposition 2.3.5. $H^2(\mathrm{SL}_3(\mathbb{F}_2), \mathbb{F}_7) = 0$.

Proof. The 7-Sylow subgroup is again the cyclic group C_7. There is a simple way of finding a generator of C_7 in $\mathrm{SL}_3(\mathbb{F}_2)$; we can take a generator of $\mathbb{F}_8^\times$ and consider its multiplication action on a basis for $\mathbb{F}_8$ over $\mathbb{F}_2$. Doing this, we obtain $\alpha = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_2)$ of order 7. Furthermore, we have at least an action of an element of order 3 on this C_7 given by the Frobenius endomorphism. Again this gives us $\beta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_2)$ of order 3. Its conjugation action sends α to α^2 and so recalling the structure of the cohomology ring $H^\bullet(C_7, \mathbb{F}_7)$, β acts on a generator $X \in H^1(C_7, \mathbb{F}_7)$ by $X \mapsto \frac{1}{2}X \equiv 4X \mod 7$. By Lemma 2.3.3, β then also acts on a generator $Y \in H^2(C_7, \mathbb{F}_7)$ by $Y \mapsto 4Y$. It immediately follows that there are no invariant classes in $H^2(C_7, \mathbb{F}_7)$ under the action of $\mathrm{SL}_3(\mathbb{F}_2)$. □

We can put together these computations to form the following Corollary.

Corollary 2.3.6. *Let p and q be rational primes. Then for all $p \neq q$, we have*

$$H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q) = 0.$$

2.3.3 $H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_p)$

We will assume throughout this section that $p > 3$, for reasons that will become apparent later. The case $p = q$ is more involved than the case $p \neq q$; we will use the filtration (2.7) and the Hochschild-Serre spectral sequence from above to inductively calculate $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p)$ for increasing n. The case $n = 1$ we have already done by K-theory and we have $H^2(\mathrm{SL}_3(\mathbb{F}_p), \mathbb{F}_p) = 0$ provided $p > 2$. For $n = 2$, we use the spectral sequence

$$H^r(\mathcal{G}(0)/\mathcal{G}(1), H^s(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p)) \Longrightarrow H^{r+s}(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p),$$

with $r + s = 2$. We have already calculated the term with $(r, s) = (2, 0)$ in section 2.3.2, so we focus on $r = 1$ and $s = 1$.

As we stated earlier, it is well-known that the order of $\mathrm{SL}_3(\mathbb{F}_p)$ is $p^3(p^2-1)(p^3-1)$, thus the p-Sylow subgroup has order p^3 and we may choose it to be the unipotent subgroup N (or $N(\mathbb{F}_p)$ if we wish to specify the field involved) consisting of the upper triangular matrices with 1's down the diagonal. Therefore there exists a monomorphism

$$H^1(\mathrm{SL}_3(\mathbb{F}_p), H^1(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p)) \hookrightarrow H^1(N, H^1(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p)).$$

In fact for each $n > 0$, the quotient $\mathcal{G}(n)/\mathcal{G}(n + 1)$ can be expressed in a simple and convenient manner; each $g \in \mathcal{G}(n)/\mathcal{G}(n+1)$ can be written as $1 + p^n X$ where $X \in M_3(\mathbb{F}_p)$ and $\mathrm{Tr}(X) = 0$. Thus for each $n > 0$, $\mathcal{G}(n)/\mathcal{G}(n+1) \cong \mathfrak{sl}_3(\mathbb{F}_p)$ and the above monomorphism can be rewritten

$$H^1(\mathrm{SL}_3(\mathbb{F}_p), H^1(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)) \hookrightarrow H^1(N, H^1(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)).$$

When $p > 3$, the Killing form on $\mathfrak{sl}_3(\mathbb{F}_p)$ is non-degenerate and gives a $\mathcal{G}(\mathbb{F}_p)$-equivariant isomorphism between $\mathfrak{sl}_3(\mathbb{F}_p)$ and its dual space, $\mathrm{Hom}(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)$. In particular, $H^1(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p) \cong \mathfrak{sl}_3(\mathbb{F}_p)$ as $\mathcal{G}(\mathbb{F}_p)$-modules provided $p > 3$, which is a condition we fixed for p in this section. The image of this monomorphism is then the set of invariant classes in $H^1(N, \mathfrak{sl}_3(\mathbb{F}_p))$ under the action of $\mathrm{SL}_3(\mathbb{F}_p)$ (see [5]). However, rather than finding the invariant classes under the entire group $\mathrm{SL}_3(\mathbb{F}_p)$, we start by finding the invariant classes under the action of the torus in $\mathrm{SL}_3(\mathbb{F}_p)$,

$$T(\mathbb{F}_p) = \left\{ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & (\lambda\mu)^{-1} \end{pmatrix} : \lambda, \mu \in \mathbb{F}_p^\times \right\}.$$

Now, consider the filtration

$$\begin{aligned}\mathfrak{sl}_3(\mathbb{F}_p) \supset \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & * & * \end{pmatrix} \supset \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \supset \begin{pmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix} \supset \\ \supset \begin{pmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \supset \{0\}\,.\end{aligned} \tag{2.10}$$

We abbreviate the subspaces in the above filtration by writing it as

$$\mathfrak{sl}_3(\mathbb{F}_p) = F(0) \supset F(1) \supset \cdots \supset F(4) \supset F(5) = 0.$$

The action of $\mathrm{SL}_3(\mathbb{F}_p)$ (and hence of N and T) on $\mathfrak{sl}_3(\mathbb{F}_p)$ is by conjugation and a direct computation shows that N acts trivially on each quotient $F(i)/F(i+1)$, $0 \leq i \leq 4$. Although we will not use it, we note that we could also construct a similar filtration on $H^1(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)$ with N acting trivially upon successive quotients, only the filtration would go the other way; that is, we would take $F(4)$ to consist of a single non-zero entry in the $(3,1)$ entry instead of the $(1,3)$ as we had above, and $F(1)$ would have a 0 in the $(1,3)$ entry instead of in the $(3,1)$ position. Since the notational advantages are clear, we will use the filtration on $\mathfrak{sl}_3(\mathbb{F}_p)$.

For representations of T, we'll use the notation $\mathbb{F}_p(\phi)$ to signify that T acts upon elements of $\mathbb{F}_p$ by multiplication by some $\phi : T \to \mathbb{F}_p^\times$. When T acts trivially upon $\mathbb{F}_p$, we extend this notation by writing $\mathbb{F}_p(0)$. Following this notation, we can decompose $\mathfrak{sl}_3(\mathbb{F}_p)$ as a representation of T into a direct sum of weight spaces

$$\mathfrak{sl}_3(\mathbb{F}_p) = \mathfrak{g}_0 \oplus \bigoplus_{\phi \in \Phi'} \mathbb{F}_p(\phi), \quad \text{with} \tag{2.11}$$

$$\Phi' = \left\{ (\alpha\beta)^{\pm 1}, \alpha^{\pm 1}, \beta^{\pm 1} \right\}. \tag{2.12}$$

Here we note that $\mathfrak{g}_0$ is 2-dimensional over $\mathbb{F}_p$ and which will often be written as $\mathbb{F}_p(0)^2$, and Φ' is a collection of linear functionals on T with α and β defined by

$$\alpha \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & (\lambda\mu)^{-1} \end{pmatrix} = \lambda/\mu \quad \text{and}$$

$$\beta \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & (\lambda\mu)^{-1} \end{pmatrix} = \mu/(\lambda\mu)^{-1} = \lambda\mu^2.$$

In order to simplify notation, we write the action of T via the linear functionals additively as opposed to multiplicatively and we will often write α in place of $\alpha(t)$ for $t \in T$ when no confusion can arise. So we let

$$\Phi = \{\pm(\alpha + \beta), \pm\alpha, \pm\beta\}. \tag{2.13}$$

With this, the quotients of successive subspaces in the filtration above can be expressed as:

$$\begin{aligned} F(0)/F(1) &= \mathbb{F}_p(-\alpha-\beta), F(1)/F(2) = \mathbb{F}_p(-\alpha)\oplus\mathbb{F}_p(-\beta), F(2)/F(3) = \mathbb{F}_p(0)^2, \\ F(3)/F(4) &= \mathbb{F}_p(\alpha)\oplus\mathbb{F}_p(\beta), F(4)/F(5) = \mathbb{F}_p(\alpha+\beta). \end{aligned}$$

Our strategy to calculate the T-invariants of $H^1(N, \mathfrak{sl}_3(\mathbb{F}_p))$ is to successively calculate the T-invariants of $H^1(N, F(i))$ for decreasing i. We know how T acts upon quotients $F(i)/F(i+1)$ in the filtration, we also need to know how T acts on $H^1(N, \mathbb{F}_p)$ for a trivial N-module $\mathbb{F}_p$. Firstly, $H^1(N, \mathbb{F}_p) \cong \mathrm{Hom}(N, \mathbb{F}_p)$ and if $Z \subset N$ denotes the subgroup

$$Z = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

then Z is precisely the commutator subgroup of N. Hence

$$\mathrm{Hom}(N, \mathbb{F}_p) \cong \mathrm{Hom}(N/Z, \mathbb{F}_p) \cong \mathbb{F}_p \oplus \mathbb{F}_p.$$

We know that T acts on N/Z by multiplication by the linear functional α on the 1-dimensional subspace of N/Z in the $(1,2)$ entry and by multiplication by β on the other subspace in the $(2,1)$ entry. The action on the dual space is then by multiplication by $-\alpha$ on one $\mathbb{F}_p$ factor and by $-\beta$ on the other. Therefore as a T-module, we will write $\mathrm{Hom}(N/Z, \mathbb{F}_p) \cong \mathbb{F}_p(-\alpha) \oplus \mathbb{F}_p(-\beta)$.

With this in mind, we turn our attention to finding $H^1(N, F(i)/F(i+1))$. Since N/Z acts trivially on each of these coefficient modules, as a T-module we have

$$H^1(N, F(i)/F(i+1)) \cong \mathrm{Hom}(N/Z, \mathbb{F}_p) \otimes F(i)/F(i+1),$$

where $\mathbb{F}_p$ here is a trivial N-module. We know how T acts on $\mathrm{Hom}(N/Z, \mathbb{F}_p)$ and $F(i)/F(i+1)$, so we know the action on their tensor product (see Chapter 1 of [11]); we add the linear functionals. Adopting the above notation, we have the following isomorphisms of T-modules:

$$\begin{aligned}
H^1(N, F(4)) &\cong \mathbb{F}_p(\beta) \oplus \mathbb{F}_p(\alpha), \\
H^1(N, F(3)/F(4)) &\cong \mathbb{F}_p(0) \oplus \mathbb{F}_p(-\alpha+\beta) \oplus \mathbb{F}_p(-\beta+\alpha) \oplus \mathbb{F}_p(0), \\
H^1(N, F(2)/F(3)) &\cong \mathbb{F}_p(-\alpha)^2 \oplus \mathbb{F}_p(-\beta)^2, \\
H^1(N, F(1)/F(2)) &\cong \mathbb{F}_p(-2\alpha) \oplus \mathbb{F}_p(-\alpha-\beta) \oplus \mathbb{F}_p(-\beta-\alpha) \oplus \mathbb{F}_p(-2\beta), \\
H^1(N, F(0)/F(1)) &\cong \mathbb{F}_p(-2\alpha-\beta) \oplus \mathbb{F}_p(-2\beta-\alpha).
\end{aligned}$$

We see immediately that there is a subspace $\mathbb{F}_p^2$ of $H^1(N/Z, F(3)/F(4))$ invariant under T. However, simple calculations show that the action of T on the other subspaces are non-trivial provided $p > 3$, hence no subspaces are fixed for any values of i excepting the $\mathbb{F}_p^2$ we have already observed.

Now, take the short exact sequence

$$0 \longrightarrow F(4) \longrightarrow F(3) \longrightarrow F(3)/F(4) \longrightarrow 0,$$

this gives a long exact sequence

$$0 \longrightarrow F(4)^N \longrightarrow F(3)^N \longrightarrow F(3)/F(4)^N \longrightarrow H^1(N, F(4)) \longrightarrow$$
$$\longrightarrow H^1(N, F(3)) \longrightarrow H^1(N, F(3)/F(4)) \longrightarrow \cdots .$$

$\left|T\right| = p^2 - 2p + 1 \equiv 1 \mod p$, so $(-)^T$ is an exact functor on $\mathbb{F}_p\left[T(\mathbb{F}_p)\right]$-modules. Writing $B = N \rtimes T$, we may take T-invariants in this long exact sequence to arrive at the long exact sequence

$$0 \longrightarrow F(4)^B \longrightarrow F(3)^B \longrightarrow F(3)/F(4)^B \longrightarrow H^1(N, F(4))^T \longrightarrow$$
$$\longrightarrow H^1(N, F(3))^T \longrightarrow H^1(N, F(3)/F(4))^T \longrightarrow \cdots .$$

The first 4 terms in the sequence are 0, so this gives

$$0 \longrightarrow H^1(N, F(3))^T \longrightarrow \mathbb{F}_p^2 \longrightarrow H^2(N, F(4))^T \longrightarrow \cdots .$$

It follows that $H^1(N, F(3))^T$ is either $0, \mathbb{F}_p$ or $\mathbb{F}_p^2$. Consider now the short exact sequence

$$0 \longrightarrow F(3) \longrightarrow F(2) \longrightarrow F(2)/F(3) \longrightarrow 0,$$

in the same manner this gives the long exact sequence

$$0 \longrightarrow F(3)^B \longrightarrow F(2)^B \longrightarrow F(2)/F(3)^B \longrightarrow H^1(N, F(3))^T \longrightarrow$$
$$\longrightarrow H^1(N, F(2))^T \longrightarrow H^1(N, F(2)/F(3))^T \longrightarrow \cdots .$$

Note that $F(3)^B = F(2)^B = 0$, $(F(2)/F(3))^B = \mathbb{F}_p^2$ and recall from above that $H^1(N, F(2)/F(3))^T = 0$. With this, the long exact sequence is

$$0 \longrightarrow \mathbb{F}_p^2 \longrightarrow H^1(N, F(3))^T \longrightarrow H^1(N, F(2))^T \longrightarrow 0 \longrightarrow \cdots .$$

From this it becomes clear that the only option for $H^1(N, F(3))^T$ is $\mathbb{F}_p^2$. Hence

$$0 \longrightarrow \mathbb{F}_p^2 \xrightarrow{\sim} \mathbb{F}_p^2 \longrightarrow H^1(N, F(2))^T \longrightarrow 0 \longrightarrow \cdots ,$$

and so $H^1(N, F(2))^T = 0$ and the cohomology we picked up at $F(3)$ disappears at $F(2)$. Following this method up to $F(0)$ and using our calculation that

$$H^1(N, F(i)/F(i+1)) = 0 \quad \text{for} \quad 0 \le i \le 2 \quad \text{and} \quad p > 3,$$

we easily see that $H^1(N, F(0))^T = 0$. Stated in our original notation, we have shown that $H^1(N, \mathfrak{sl}_3(\mathbb{F}_p))^T = 0$. Since $H^1(\mathrm{SL}_3(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F}_p))$ embeds into this, it is immediate that

$$H^1(\mathrm{SL}_3(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F}_p)) = 0 \qquad \text{for } p > 3.$$

In terms of the filtration 2.7, we have $H^1(\mathcal{G}(0)/\mathcal{G}(1), H^1(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p)) = 0$. It remains to find $H^0(\mathcal{G}(0)/\mathcal{G}(1), H^2(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p))$, which corresponds to the $E_2^{0,2}$ entry in the spectral sequence above. That is, we wish to find

$$H^2(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)^{\mathrm{SL}_3(\mathbb{F}_p)}.$$

We begin by recalling the work we did in section 2.1.2 and in particular Lemma 2.1.12. This Lemma is of particular interest to us here where we have $V = \mathfrak{sl}_3(\mathbb{F}_p)$ and $G = \mathrm{SL}_3(\mathbb{F}_p)$ since it tells us that $H^2(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)$ fits into a short exact sequence of $\mathrm{SL}_3(\mathbb{F}_p)$-modules in the following way,

$$0 \longrightarrow H^1(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p) \longrightarrow H^2(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p) \longrightarrow \bigwedge^2 H^1(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p) \longrightarrow 0,$$

or equivalently

$$0 \longrightarrow \mathfrak{sl}_3(\mathbb{F}_p) \longrightarrow H^2(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p) \longrightarrow \bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p) \longrightarrow 0.$$

We will see that $H^2(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)^{\mathrm{SL}_3(\mathbb{F}_p)}$ can be computed by finding $(\mathfrak{sl}_3(\mathbb{F}_p))^{\mathrm{SL}_3(\mathbb{F}_p)}$ and $\left(\bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p)\right)^{\mathrm{SL}_3(\mathbb{F}_p)}$. Since $(\mathfrak{sl}_3(\mathbb{F}_p))^{\mathrm{SL}_3(\mathbb{F}_p)} = 0$, we calculate $\left(\bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p)\right)^{\mathrm{SL}_3(\mathbb{F}_p)}$.

Proposition 2.3.7. *Let $p > 3$ be a prime in $\mathbb{Z}$. Under the conjugation action of $\mathrm{SL}_3(\mathbb{F}_p)$ on $\mathfrak{sl}_3(\mathbb{F}_p)$, we have $\left(\bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p)\right)^{\mathrm{SL}_3(\mathbb{F}_p)} = 0$.*

Proof. Recall the root space decomposition of $\mathfrak{sl}_3(\mathbb{F}_p)$ with respect to the torus $T(\mathbb{F}_p)$. Let Φ denote the set of roots (written additively) as we had in (2.13) and let $\mathfrak{g}_\phi$ denote the eigenspace of the root $\phi \in \Phi$. Then

$$\begin{aligned} \mathfrak{sl}_3(\mathbb{F}_p) &= \mathfrak{g}_0 \oplus \bigoplus_{\phi \in \Phi} \mathfrak{g}_\phi \\ \Longrightarrow \bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p) &= \bigwedge^2 \mathfrak{g}_0 \oplus \bigoplus_{\phi \in \Phi} (\mathfrak{g}_0 \wedge \mathfrak{g}_\phi) \oplus \bigoplus_{\substack{\phi, \varphi \in \Phi \\ \phi > \varphi}} \mathfrak{g}_\phi \wedge \mathfrak{g}_\varphi. \end{aligned}$$

It is clear that

$$\begin{aligned} \left(\bigoplus_{\phi \in \Phi} (\mathfrak{g}_0 \wedge \mathfrak{g}_\phi) \right)^{T(\mathbb{F}_p)} &= 0 \quad \text{and} \\ \left(\bigoplus_{\substack{\phi, \varphi \in \Phi \\ \phi > \varphi}} \mathfrak{g}_\phi \wedge \mathfrak{g}_\varphi \right)^{T(\mathbb{F}_p)} &= \bigoplus_{\substack{\phi \in \Phi \\ \phi > 0}} \mathfrak{g}_\phi \wedge \mathfrak{g}_{-\phi}, \end{aligned}$$

so we have

$$\left(\bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p) \right)^{T(\mathbb{F}_p)} = \bigwedge^2 \mathfrak{g}_0 \oplus \bigoplus_{\substack{\phi \in \Phi \\ \phi > 0}} \mathfrak{g}_\phi \wedge \mathfrak{g}_{-\phi}.$$

The Weyl group W of $\mathrm{SL}_3(\mathbb{F}_p)$ has 6 elements and is isomorphic to the symmetric group of order 6. Consider the action of $w := \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \in W$ on $\bigwedge^2 \mathfrak{g}_0$. Since

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \overset{w}{\longmapsto} \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \wedge \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$
$$= - \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

it follows immediately that $\bigwedge^2 \mathfrak{g}_0$ has no fixed points under the action of W. Furthermore, taking elements $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathfrak{g}_{\alpha+\beta}$ and $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in \mathfrak{g}_{-\alpha-\beta}$, we see that

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overset{w}{\longmapsto} - \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

showing that there are also no fixed points in the subspace $\mathfrak{g}_{\alpha+\beta} \wedge \mathfrak{g}_{-\alpha-\beta}$. We also see that

$$\mathfrak{g}_\alpha \wedge \mathfrak{g}_{-\alpha} \quad \xrightarrow{w} \quad \mathfrak{g}_{-\beta} \wedge \mathfrak{g}_\beta,$$

therefore

$$\left(\bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p)\right)^{T(\mathbb{F}_p)\langle w\rangle} \subseteq \mathfrak{g}_\alpha \wedge \mathfrak{g}_{-\alpha} \oplus \mathfrak{g}_{-\beta} \wedge \mathfrak{g}_\beta.$$

Now take $w' := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in W$. A direct computation gives

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \overset{w'}{\longmapsto} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \text{and}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \overset{w'}{\longmapsto} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

showing that there are no fixed points in the subspace $\mathfrak{g}_\alpha \wedge \mathfrak{g}_{-\alpha} \oplus \mathfrak{g}_{-\beta} \wedge \mathfrak{g}_\beta$ under the action of w' and we conclude that $\left(\bigwedge^2 \mathfrak{sl}_3(\mathbb{F}_p)\right)^{\mathrm{SL}_3(\mathbb{F}_p)} = 0$, as required. □

Given this and $(\mathfrak{sl}_3(\mathbb{F}_p))^{\mathrm{SL}_3(\mathbb{F}_p)} = 0$, it follows that $H^2(\mathfrak{sl}_3(\mathbb{F}_p), \mathbb{F}_p)^{\mathrm{SL}_3(\mathbb{F}_p)} = 0$.

Corollary 2.3.8. *For any prime p in $\mathbb{Z}$ with $p > 3$,*

$$H^0(\mathcal{G}(0)/\mathcal{G}(1), H^2(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p)) = 0.$$

Furthermore, $H^0(\mathcal{G}(0)/\mathcal{G}(n), H^2(\mathcal{G}(n)/\mathcal{G}(n+1), \mathbb{F}_p)) = 0$ for any $n \geq 2$.

Proof. The first of these assertions is what we have just proved. The second follows from the first when we recall that $\mathcal{G}(n)/\mathcal{G}(n+1) \cong \mathfrak{sl}_3(\mathbb{F}_p)$ for all $n \geq 1$, and the action of $\mathcal{G}(0)/\mathcal{G}(n)$ on $\mathcal{G}(n)/\mathcal{G}(n+1)$ is by conjugation. Since $\mathcal{G}(0)/\mathcal{G}(n)$ contains $\mathcal{G}(0)/\mathcal{G}(1)$ as a quotient, the second assertion follows directly from the first. □

Putting the above results together, we have proved that $H^2(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p) = 0$. However, we wish to calculate $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p)$ for each $n \geq 1$. We can do this inductively once we have proved the following Proposition.

Proposition 2.3.9. *Continuing with the above notation, for each $n \geq 1$ and all primes $p > 3$,*

$$H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right)\right) = 0.$$

Proof. The proof is by induction. We've shown the result for $n = 1$ so we suppose the result is true for n. Since the Killing form gives a $\mathcal{G}(0)$-equivariant isomorphism between $H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right)$ and $\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}$ for all $n > 0$, it is sufficient to show that

$H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) = 0$. The short exact sequence

$$1 \longrightarrow \mathcal{G}(n)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n) \longrightarrow 1,$$

gives us the corresponding Hochschild-Serre spectral sequence

$$H^r\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^s\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)\right) \Longrightarrow H^{r+s}\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right).$$

Recall that $\mathcal{G}(n)/\mathcal{G}(n+1)$ acts trivially on $\mathcal{G}(n+1)/\mathcal{G}(n+2)$ when $n \geq 1$ and the spectral sequence gives us an exact sequence of low degree terms,

$$0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) \longrightarrow$$
$$\longrightarrow H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)\right) \longrightarrow H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right).$$

Now, $\mathcal{G}(n)/\mathcal{G}(n+1) \cong \mathcal{G}(n+1)/\mathcal{G}(n+2) \cong \mathfrak{sl}_3(\mathbb{F}_p)$ as $\mathcal{G}(0)$-modules, so by the inductive hypothesis the first term is 0 and the exact sequence becomes

$$0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right) \longrightarrow$$
$$\longrightarrow \operatorname{Hom}\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right)^{\mathcal{G}(0)/\mathcal{G}(n)} \longrightarrow H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right).$$

Recall that $f \in \operatorname{Hom}(\mathcal{G}(n)/\mathcal{G}(n+1), \mathcal{G}(n)/\mathcal{G}(n+1))$ is fixed under the action of $g \in \mathcal{G}(0)/\mathcal{G}(n)$ if and only if $f(X) = g \circ f(g^{-1} \circ X)$. Since only homomorphisms of the form $f(X) = kX$ for $k \in \mathbb{F}_p$ and $X \in \mathfrak{sl}_3(\mathbb{F}_p)$ are fixed under the action of $\mathcal{G}(0)/\mathcal{G}(n)$, it follows that the middle term in this sequence is $\mathbb{F}_p$. Thus the exact sequence is

$$0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right) \longrightarrow \mathbb{F}_p \longrightarrow H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right). \qquad (2.14)$$

The next section of this proof employs similar ideas to those used in parts of the proof of Theorem 2.4.4 in [22], and our strategy is to show that the map between $\mathbb{F}_p$ and $H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right)$ is non-trivial and hence injective. Doing so will show that $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right) = 0$, as required.

Recall that the map from $\mathbb{F}_p$ to $H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right)$ in the exact sequence (2.14) is given by the *transgression map*, which we denote by tg (see Proposition 1.6.6 of [22]). Take the non-trivial 1-cocycle

$$\epsilon \in H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right)\right),$$

given by $\epsilon(X) = X$ for $X \in \mathfrak{sl}_3(\mathbb{F}_p)$, and let $u \in H^2\left(\mathcal{G}(0)/\mathcal{G}(n), \mathcal{G}(n)/\mathcal{G}(n+1)\right)$ be a representative of the cohomology class defining the short exact sequence

$$1 \longrightarrow \mathcal{G}(n)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n) \longrightarrow 1.$$

Choose a section $s : \mathcal{G}(0)/\mathcal{G}(n) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n+1)$ of the projection

$$\begin{array}{rcl} \mathcal{G}(0)/\mathcal{G}(n+1) & \longrightarrow & \mathcal{G}(0)/\mathcal{G}(n) \\ \sigma & \longmapsto & \overline{\sigma}, \end{array}$$

with $s1 = 1$. Such a choice is possible (see Exercise 4, Section 1, Chapter 1 of [22]). We now define a 1-cochain $y : \mathcal{G}(0)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(n)/\mathcal{G}(n+1)$ by

$$y(\sigma) := \sigma(s\overline{\sigma})^{-1}.$$

Note that if $X \in \mathcal{G}(n)/\mathcal{G}(n+1)$, the projection $\overline{X} = 1$. Then $y(X) = X(s\overline{X})^{-1} = X(s1)^{-1} = X$ and so $y\big|_{\mathcal{G}(n)/\mathcal{G}(n+1)} = \epsilon$. Furthermore, for $\sigma_1, \sigma_2 \in \mathcal{G}(0)/\mathcal{G}(n+1)$,

$$\begin{aligned} (\delta y)(\sigma_1, \sigma_2) &= y(\sigma_1\sigma_2)^{-1}(\sigma_1 \circ y(\sigma_2))y(\sigma_1) \\ &= (s\overline{\sigma_1\sigma_2})\sigma_2^{-1}\sigma_1^{-1}\sigma_1\sigma_2(s\overline{\sigma_2})^{-1}\sigma_1^{-1}\sigma_1(s\overline{\sigma_1})^{-1} \\ &= s(\overline{\sigma_1\sigma_2})(s(\overline{\sigma_2}))^{-1}(s(\overline{\sigma_1}))^{-1} \\ &= \left(s(\overline{\sigma_1})s(\overline{\sigma_2})s(\overline{\sigma_1\sigma_2})^{-1}\right)^{-1}. \end{aligned}$$

By definition of tg, $tg(\epsilon) = [\delta y]$. However, the function $s(\overline{\sigma_1})s(\overline{\sigma_2})s(\overline{\sigma_1\sigma_2})^{-1}$ is a 2-cocycle representing the class u we constructed above. Hence if we write 2-cocycles in $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathcal{G}(n)/\mathcal{G}(n+1))$ additively, $tg(\epsilon) = -u$.

It remains to show that u does not represent the trivial class (since then neither will $-u$). That is, we must show that $\mathcal{G}(0)/\mathcal{G}(n+1)$ is not a semidirect product. We can see this by taking an element of order p^n in $\mathcal{G}(0)/\mathcal{G}(n)$ of the form

$$\overline{Z_a} = \begin{pmatrix} 1 & 0 & \overline{a} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $\overline{a} \not\equiv 0 \mod p$. Now, every preimage of this element in $\mathcal{G}(0)/\mathcal{G}(n+1)$ is of the form

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

where $a \equiv \overline{a} \mod p^n$. Since $(Z_a)^k = Z_{ka}$ for all k, we have $(Z_a)^k = I_3$ if and only if $ka \equiv 0 \mod p^{n+1}$. However, as $\overline{a} \not\equiv 0 \mod p$, it follows from the definition of a that $a \not\equiv 0 \mod p$ and so $ka \equiv 0 \mod p^{n+1}$ if and only if $k \equiv 0 \mod p^{n+1}$. So with $\overline{a}$ chosen this way, Z_a always has order p^{n+1} and so every preimage of $\overline{Z_a}$ has order p^{n+1}. It follows that $\mathcal{G}(0)/\mathcal{G}(n+1)$ is not a semidirect product and so u does not represent the trivial class, hence neither does $-u$ and therefore the chosen generator ϵ does not lie in the kernel of the transgression map. The transgression map must then be a monomorphism and from the short exact sequence (2.14), we must then have

$$H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) = 0.$$

It follows from the induction hypothesis that this is 0 for every $n \geq 0$, as required.

□

We can summarise the above work in the following theorem, bringing the split case to a conclusion.

Theorem 2.3.10. *Let p and q be rational primes with p split in k. We have*

(i) $H^1(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q) = 0$ *for all pairs p and q,*

(ii) $H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_p) = 0$ *for all $p > 3$, and*

(iii) $H^2(\mathrm{SL}_3(\mathbb{Z}_p), \mathbb{F}_q) = 0$ *for all $p \neq q$.*

Proof. The first and third statements are Corollary 2.3.2 and Corollary 2.3.6, respectively. For the second, recall that we showed by K-theory that $H^2\left(\mathcal{G}(0)/\mathcal{G}(1), \mathbb{F}_p\right) = 0$. We then also have $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p) = 0$ for all $p > 3$ and all $n \geq 1$ by a simple inductive argument, using Corollary 2.3.8, Proposition 2.3.9 and the Hochschild-Serre spectral sequence

$$H^r\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^s\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right)\right) \Longrightarrow H^{r+s}\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right).$$

Supposing $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p) = 0$ for the inductive hypothesis, then for $p > 3$, all the terms in the E_2^{rs} position with $r + s = 2$ are zero for this spectral sequence, hence $H^2(\mathcal{G}(0)/\mathcal{G}(n+1), \mathbb{F}_p) = 0$. The second statement then follows from

$$\begin{aligned} H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_p) &= H^2(\varprojlim_n \mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p) \\ &= \varinjlim_n H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p) \quad \text{(Proposition 2.1.1)}, \end{aligned}$$

where the limits are taken over $n \geq 1$. □

Thus, excepting the primes $q = 2, 3$, we have completed the calculations for when p is split in k. Our exclusion of the cases $q = 2, 3$ will not be a problem; we can still take any $q \geq 5$ which would then correspond to looking for a congruence subgroup $\Gamma' \subset \mathrm{SU}(2,1)(\mathbb{Z})$ such that the restriction map $H^2(\mathrm{SU}(2,1)(\mathbb{Z}), \mathbb{F}_q) \longrightarrow H^2(\Gamma', \mathbb{F}_q)$ is not injective.

Chapter 3

Low Dimensional Cohomology of $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ with p Inert

In the previous chapter we calculated $H^1(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q)$ and $H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q)$ for when p is split in k. The focus of this chapter will be the calculation of the cohomology groups $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q)$ and $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q)$ for primes p, q with p inert. While our general approach is similar in many areas to the split case, most of the details differ. Recall that for $p \in \mathbb{Z}$ inert, we have

$$\begin{aligned} \mathrm{SU}(2,1)(\mathbb{Q}_p) &= \left\{ g \in \mathrm{SL}_3(\mathbb{Q}_p \otimes_{\mathbb{Q}} k) : g^t J \overline{g} = J \right\} \\ &= \left\{ g \in \mathrm{SL}_3(k_p) : g^t J \overline{g} = J \right\}, \end{aligned}$$

and so we will be interested in the H^1 and H^2 cohomology of $\mathrm{SU}(2,1)(\mathbb{Z}_p) = \left\{g \in \mathrm{SL}_3(\mathcal{O}_{k_p}) : g^t J\overline{g} = J\right\}$ for each p.

3.1 $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q)$

We approach this computation in a similar way to the split case, by looking at when $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ is perfect. We will be able to show that this is true when $p > 2$ and so throughout this section, we will assume $p > 2$; a separate calculation will deal with the case $p = 2$.

Proposition 3.1.1. *Let $p, q \in \mathbb{Z}$ be primes with p inert in the imaginary quadratic extension k of $\mathbb{Q}$. Then $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) = 0$ for all $p > 2$.*

Proof. Recall that we have a filtration on $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ given by equation (2.7) above, which we denote by

$$\mathrm{SU}(2,1)(\mathbb{Z}_p) = \mathcal{G}(0) \supset \mathcal{G}(1) \supset \cdots \supset \mathcal{G}(n) \supset \cdots .$$

Now, $\mathcal{G}(0)/\mathcal{G}(1) \cong \mathrm{SU}(2,1)(\mathbb{F}_p)$ and it will be shown in section 3.2.2 below that $\mathcal{G}(n)/\mathcal{G}(n+1) \cong \mathfrak{su}(2,1)(\mathbb{F}_p)$ for each $n > 0$, where the Lie algebra $\mathfrak{su}(2,1)(\mathbb{F}_p)$ was described in section 1.2. Note that throughout this proof, we will make use of the notation introduced in section 1.2 above.

Using these facts, we have a short exact sequence

$$0 \longrightarrow \mathfrak{su}(2,1)(\mathbb{F}_p) \longrightarrow \mathcal{G}(0)/\mathcal{G}(2) \longrightarrow \mathrm{SU}(2,1)(\mathbb{F}_p) \longrightarrow 0.$$

The group $\mathrm{SU}(2,1)(\mathbb{F}_p)$ is known to be perfect (see Page 389 of [12]) for all $p > 2$. If we can show that $\mathfrak{su}(2,1)(\mathbb{F}_p)$ is contained in the commutator subgroup of $\mathcal{G}(0)/\mathcal{G}(2)$, then $\mathcal{G}(0)/\mathcal{G}(2)$ must also be perfect. To show this, it is sufficient to show that

$$\mathfrak{su}(2,1)(\mathbb{F}_p) \subset \left[\mathrm{SU}(2,1)(\mathbb{F}_p), \mathcal{G}(1)/\mathcal{G}(2)\right].$$

Take $g \in \mathrm{SU}(2,1)(\mathbb{F}_p)$, $X \in \mathfrak{su}(2,1)(\mathbb{F}_p)$ and $1 + pX \in \mathcal{G}(1)/\mathcal{G}(2)$, then

$$g(1+pX)g^{-1}(1-pX) = \left(1 + p(gXg^{-1})\right)(1-pX) = 1 + p\left(gXg^{-1} - X\right).$$

Take any root $Y \notin \mathfrak{g}_0$ of $\mathfrak{su}(2,1)(\mathbb{F}_p)$, then since $p > 2$ we can choose an element in the maximal torus of $\mathrm{SU}(2,1)(\mathbb{F}_p)$, say $t \in T(\mathbb{F}_p)$, such that $tYt^{-1} - Y = cY$ for some $c \neq 0$. Thus all $X \notin \mathfrak{g}_0$ lies in the commutator subgroup of $\mathcal{G}(0)/\mathcal{G}(2)$. Now taking $Y_0 \in \mathfrak{g}_0$ and w the non-trivial element of the Weyl group, the same calculation shows that $\mathfrak{a} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -a \end{pmatrix} : a \in \mathbb{F}_p \right\}$ as defined in section 1.2, satisfies $\mathfrak{a} \subset [\mathcal{G}(0)/\mathcal{G}(2), \mathcal{G}(0)/\mathcal{G}(2)]$. It remains to show that the one-dimensional subspace of elements of the form $\begin{pmatrix} z & 0 & 0 \\ 0 & -2z & 0 \\ 0 & 0 & z \end{pmatrix}$ with $z \in \mathbb{F}_{p^2}$ and $\bar{z} = -z$ lies in the commutator subgroup of $\mathcal{G}(0)/\mathcal{G}(2)$. Rather than continuing with the above method, consider the subgroup $H = \mathfrak{su}(2,1)(\mathbb{F}_p) \cap [\mathcal{G}(0)/\mathcal{G}(2), \mathcal{G}(0)/\mathcal{G}(2)]$. We have shown that H has dimension at least 7 as an $\mathbb{F}_p$-vector space and it is clear that it is a normal subgroup of $\mathcal{G}(0)/\mathcal{G}(2)$. So $SU(2,1)(\mathbb{F}_p)$ acts on H by conjugation and from this, we see that H must be $\mathfrak{su}(2,1)(\mathbb{F}_p)$ since taking for example $\begin{pmatrix} 0 & 0 & 0 \\ x & 0 & 0 \\ 0 & -\overline{x} & 0 \end{pmatrix} \in H$ and $\begin{pmatrix} 1 & r & m \\ 0 & 1 & -\overline{r} \\ 0 & 0 & 1 \end{pmatrix} \in SU(2,1)(\mathbb{F}_p)$,

$$\begin{pmatrix} 1 & r & m \\ 0 & 1 & -\overline{r} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ x & 0 & 0 \\ 0 & -\overline{x} & 0 \end{pmatrix} \begin{pmatrix} 1 & r & m \\ 0 & 1 & -\overline{r} \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} rx & * & * \\ * & \overline{rx} - rx & * \\ * & * & -\overline{rx} \end{pmatrix}.$$

Since $r, x \in \mathbb{F}_{p^2}$, they can be chosen so that $rx \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and so $\overline{rx} - rx \neq 0$. Hence $H = \mathfrak{su}(2,1)(\mathbb{F}_p)$, so $\mathfrak{su}(2,1)(\mathbb{F}_p) \subset [\mathcal{G}(0)/\mathcal{G}(2), \mathcal{G}(0)/\mathcal{G}(2)]$ and since we noted earlier that $SU(2,1)(\mathbb{F}_p)$ is perfect for all $p > 2$, it follows that $\mathcal{G}(0)/\mathcal{G}(2)$ is perfect for all $p > 2$.

Inductively, the short exact sequence

$$0 \longrightarrow \mathfrak{su}(2,1)(\mathbb{F}_p) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n) \longrightarrow 0,$$

shows that $\mathcal{G}(0)/\mathcal{G}(n+1)$ is perfect for all $n > 0$. Thus

$$\mathcal{G}(0)/\mathcal{G}(n) = [\mathcal{G}(0)/\mathcal{G}(n), \mathcal{G}(0)/\mathcal{G}(n)] \subset [\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathrm{SU}(2,1)(\mathbb{Z}_p)],$$

for all $n > 0$, so the commutator subgroup of $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ is dense in $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ and hence $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) = \mathrm{Hom}_{cts}(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) = 0$. □

We now calculate $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_2), \mathbb{F}_q)$ with $q > 2$ separately. First recall that $\mathrm{SU}(2,1)(\mathbb{Z}_p, p)$ is a pro-p group and so for $p \neq q$, we have

$$H^n(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) \cong H^n(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathbb{F}_q).$$

It will be useful for us to know the order of $\mathrm{SU}(2,1)(\mathbb{F}_p)$. To calculate this, recall from section 1.2 the definitions of the groups $B(\mathbb{F}_p)$ and $N(\mathbb{F}_p)$, and the non-trivial element of the Weyl group w. Then the Bruhat decomposition (Theorem 1.2.1) gives us

$$\mathrm{SU}(2,1)(\mathbb{F}_p) = B(\mathbb{F}_p) \sqcup B(\mathbb{F}_p) w B(\mathbb{F}_p).$$

Now, $\left|B(\mathbb{F}_p)\right| = \left|N(\mathbb{F}_p)\right|\left|T(\mathbb{F}_p)\right| = p^3 \times (p^2-1)$ and we can also see that

$$\left|B(\mathbb{F}_p)wB(\mathbb{F}_p)\right| = \left|N(\mathbb{F}_p)\right|w\left|B(\mathbb{F}_p)\right| = p^3 \times p^3(p^2-1),$$

so

$$\left|\,\mathrm{SU}(2,1)(\mathbb{F}_p)\right| = p^3(p^2-1) + p^3p^3(p^2-1) = p^3(p^2-1)(p^3+1).$$

For $p=2$, this is $216 = 2^3 3^3$. So for $q>3$ and $n>0$, $H^n(\mathrm{SU}(2,1)(\mathbb{F}_2), \mathbb{F}_q) = 0$, which leaves only the case $q=3$ to check. As before, we have a monomorphism

$$H^n(\mathcal{G}(\mathbb{F}_2), \mathbb{F}_3) \hookrightarrow H^n(\mathcal{G}(\mathbb{F}_2)_3, \mathbb{F}_3),$$

where $\mathcal{G}(\mathbb{F}_2)_3$ denotes the 3-Sylow subgroup of $\mathcal{G}(\mathbb{F}_2)$. The basic structure of $\mathcal{G}(\mathbb{F}_2)$ and $\mathcal{G}(\mathbb{F}_2)_3$ is given by the following Proposition.

Proposition 3.1.2. *Suppose that* 2 *is inert in* k*. Then* $\mathcal{G}(\mathbb{F}_2) \cong \mathcal{Q}_8 \ltimes \mathcal{G}(\mathbb{F}_2)_3$*, where* $\mathcal{Q}_8$ *is the quaternion group of order* 8 *with generators* $a = \begin{pmatrix} 1 & 1 & z \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ *and* $b = \begin{pmatrix} 1 & z & \overline{z} \\ 0 & 1 & \overline{z} \\ 0 & 0 & 1 \end{pmatrix}$ *with* $z \in \mathbb{F}_4 \setminus \mathbb{F}_2$*, and* $\mathcal{G}(\mathbb{F}_2)_3$ *is the* 3*-Sylow subgroup. Furthermore,*

$\mathcal{G}(\mathbb{F}_2)_3$ is generated by

$$\alpha = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \ \textit{and}\ \gamma = \begin{pmatrix} \bar{z} & z & z \\ 1 & 0 & z \\ 1 & 1 & \bar{z} \end{pmatrix},$$

and is isomorphic to $U(3,3)$, the upper-triangular unipotent matrix group of 3×3 matrices over $\mathbb{F}_3$.

Proof. There is an obvious subgroup of order 8 in $\mathcal{G}(\mathbb{F}_2)$ given by $N(\mathbb{F}_2)$. Explicit computation shows that this is the quaternion group $\mathcal{Q}_8$ and has generators

$$a = \begin{pmatrix} 1 & 1 & z \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & z & \overline{z} \\ 0 & 1 & \overline{z} \\ 0 & 0 & 1 \end{pmatrix},$$

where $z \in \mathbb{F}_4 \setminus \mathbb{F}_2$. We now construct a subgroup of order 27. We can easily spot an element of order 3 given by

$$\alpha = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix},$$

where $\lambda \in \mathbb{F}_4^\times \setminus \mathbb{F}_2^\times$. Another is given by

$$\beta = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

We can generate another element of order 3 by conjugating this element by $a \in \mathcal{Q}_8$;

$$\gamma = a \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} a^{-1} = \begin{pmatrix} \bar{z} & z & z \\ 1 & 0 & z \\ 1 & 1 & \bar{z} \end{pmatrix}.$$

Explicit computation shows that α, β and γ generate a group of order 27 and is the 3-Sylow subgroup $\mathcal{G}(\mathbb{F}_2)_3$. Furthermore, a and b normalize $\mathcal{G}(\mathbb{F}_2)_3$, hence $\mathcal{G}(\mathbb{F}_2)_3$ is normal in $\mathcal{G}(\mathbb{F}_2)$ and is the unique 3-Sylow subgroup of $\mathcal{G}(\mathbb{F}_2)$. We conclude that $\mathcal{G}(\mathbb{F}_2) \cong \mathcal{Q}_8 \ltimes \mathcal{G}(\mathbb{F}_2)_3$. Up to isomorphism $\mathcal{G}(\mathbb{F}_2)_3$ can only be one of five groups:

$$\mathbb{Z}/27\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z} \text{ or } \mathrm{U}(3,3).$$

By elimination, it must be $\mathrm{U}(3,3)$. □

An immediate consequence is the following Corollary.

Corollary 3.1.3. *$H^n(\mathcal{G}(\mathbb{F}_2), \mathbb{F}_3) \cong H^n(\mathcal{G}(\mathbb{F}_2)_3, \mathbb{F}_3)^{\mathcal{Q}_8}$.*

Proposition 3.1.4. *$H^1(\mathcal{G}(\mathbb{F}_2), \mathbb{F}_3) = 0$.*

Proof. By the previous Corollary and the fact that $\mathbb{F}_3$ is acted upon trivially by $\mathcal{G}(\mathbb{F}_2)$, we have

$$\begin{aligned} H^1(\mathcal{G}(\mathbb{F}_2),\mathbb{F}_3) \cong H^1(\mathcal{G}(\mathbb{F}_2)_3,\mathbb{F}_3)^{\mathcal{Q}_8} &\cong \mathrm{Hom}(\mathcal{G}(\mathbb{F}_2)_3,\mathbb{F}_3)^{\mathcal{Q}_8} \\ &\cong \mathrm{Hom}(\mathcal{G}(\mathbb{F}_2)_3/\left[\mathcal{G}(\mathbb{F}_2)_3,\mathcal{G}(\mathbb{F}_2)_3\right],\mathbb{F}_3)^{\mathcal{Q}_8} \\ &\cong \mathrm{Hom}(\langle\beta,\gamma\rangle,\mathbb{F}_3)^{\mathcal{Q}_8}. \end{aligned}$$

Here we have used that $[\mathcal{G}(\mathbb{F}_2)_3,\mathcal{G}(\mathbb{F}_2)_3] \cong \langle\alpha\rangle$. Now, $\mathrm{Hom}(\langle\beta,\gamma\rangle,\mathbb{F}_3) \cong \mathbb{F}_3^2$ but $\mathcal{Q}_8$ acts non-trivially on $\langle\beta,\gamma\rangle$. In particular, ${}^a\beta = \gamma$ and ${}^a\gamma = \beta^{-1}$. Thus the action of a on $\mathcal{G}(\mathbb{F}_2)_3/\left[\mathcal{G}(\mathbb{F}_2)_3,\mathcal{G}(\mathbb{F}_2)_3\right]$ is given by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Taking the inverse and transpose of this matrix gives us the action of a on $H^1(\mathcal{G}(\mathbb{F}_2)_3,\mathbb{F}_3)$. In particular, we have

$$H^1(\mathcal{G}(\mathbb{F}_2)_3,\mathbb{F}_3)^{\mathcal{Q}_8} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{F}_3^2 : \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \right\}.$$

From this, clearly both $x = 0$ and $y = 0$, hence $H^1(\mathcal{G}(\mathbb{F}_2),\mathbb{F}_3) = H^1(\mathcal{G}(\mathbb{F}_2)_3,\mathbb{F}_3)^{\mathcal{Q}_8} = 0$, as required. □

We summarise the above results as follows.

Corollary 3.1.5. *For all pairs of primes* $(p,q) \neq (2,2)$, $H^1\left(\mathcal{G}(\mathbb{Z}_p),\mathbb{F}_q\right) = 0$.

3.2 $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q)$

As with the case when p is split, we will break this calculation into two cases; $p = q$ and $p \neq q$. The method we use for $p = q$ is similar to the split case but is more involved than when $p \neq q$. When $p \neq q$ the computation reduces to finding $H^2(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathbb{F}_q)$. Our method for finding this does not require p and q to be distinct and since it will be useful for us later on to know $H^2(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathbb{F}_p)$, it makes sense to do it all together. So in the following subsection, we will not make the restriction that p and q are distinct.

3.2.1 $H^2(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathbb{F}_q)$

We begin by recalling that $\mathcal{G}(\mathbb{F}_p)$ is perfect (see Page 389 of [12]) for all $p > 2$. The *Schur multiplier* of $\mathcal{G}(\mathbb{F}_p)$ is defined to be the group $H_2(\mathcal{G}(\mathbb{F}_p), \mathbb{Z})$. Since $\mathcal{G}(\mathbb{F}_p)$ is perfect for all $p > 2$, by Section 6.9 of [31] we have

$$H^2(\mathcal{G}(\mathbb{F}_p), \mathbb{F}_q) \cong \mathrm{Hom}(H_2(\mathcal{G}(\mathbb{F}_p), \mathbb{Z}), \mathbb{F}_q).$$

However, Griess showed in [12] that the Schur multiplier of $\mathrm{SU}(2,1)(\mathbb{F}_p)$ is in fact trivial, so it follows that

$$H^2(\mathcal{G}(\mathbb{F}_p), \mathbb{F}_q) = 0 \qquad \text{for } p > 2.$$

We have proved the following Proposition.

Proposition 3.2.1. *For $p > 2$, we have $H^2(\mathcal{G}(\mathbb{F}_p), \mathbb{F}_q) = 0$. In particular, when $p \neq q$ we have*

$$H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q) = 0.$$

The specific case of when $p = 2$ and $q > 3$ has already been done in the previous section; we noted that $|\mathcal{G}(\mathbb{F}_2)| = 2^3 3^3$ and hence $H^n(\mathcal{G}(\mathbb{F}_2), \mathbb{F}_q) = 0$ for all $q > 3$. We summarise the results in this section with the following Corollary.

Corollary 3.2.2. *For all primes p and q with $p > 2$ and $p \neq q$, $H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_p) = 0$. If $p = 2$ and $q > 3$ then we also have $H^2(\mathcal{G}(\mathbb{Z}_2), \mathbb{F}_q) = 0$.*

3.2.2 $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p)$

We will assume that $p > 3$ throughout this section. Our general approach to finding $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p)$ is similar to the one used for the corresponding case with p split. We start with filtration 2.7;

$$\mathcal{G}(0) \supset \mathcal{G}(1) \supset \cdots \supset \mathcal{G}(n) \supset \cdots .$$

We inductively calculate $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p)$ for increasing n by using the Hochschild-Serre spectral sequence. For $n = 1$, we already know from the previous section that

$H^2(\mathcal{G}(\mathbb{F}_p),\mathbb{F}_p)=0$. For $n=2$ we have

$$H^r\left(\mathcal{G}(0)/\mathcal{G}(1), H^s\left(H(1)/\mathcal{G}(2),\mathbb{F}_p\right)\right) \Longrightarrow H^{r+s}(\mathcal{G}(0)/\mathcal{G}(2),\mathbb{F}_p),$$

and we are interested in when $r+s=2$. When $r=2$ and $s=0$, we already know the cohomology group to be trivial. We are left with two possibilities; $r=1$, $s=1$ and $r=0$, $s=2$. We start with the former.

As with the split case, for all $n>0$ there is a simple description of $\mathcal{G}(n)/\mathcal{G}(n+1)$. Each $g\in\mathcal{G}(n)/\mathcal{G}(n+1)$ can be written as $g=1+p^nX$, where $X\in M_3(\mathbb{F}_{p^2})$, $\mathrm{Tr}(X)=0$ and $g^tJ\bar{g}=J$. This last matrix condition tells us that

$$\begin{aligned} g^tJ\bar{g} &= J \\ \Longleftrightarrow (1+p^nX)^tJ\overline{(1+p^nX)} &= J \\ \Longleftrightarrow (1+p^nX^t)(J+p^nJ\overline{X}) &= J \\ \Longleftrightarrow J+p^n(J\overline{X}+X^tJ) &= J \\ \Longleftrightarrow J\overline{X}+X^tJ &\equiv 0 \mod p. \end{aligned}$$

That is, X must lie in the Lie algebra $\mathfrak{su}(2,1)(\mathbb{F}_p)$; we described $\mathfrak{su}(2,1)$ in section 1.2 above. So we in fact have $\mathcal{G}(n)/\mathcal{G}(n+1)\cong\mathfrak{su}(2,1)(\mathbb{F}_p)$ for all $n>0$.

For $p>3$, we have a $\mathcal{G}(\mathbb{F}_p)$-equivariant isomorphism $H^1(\mathfrak{su}(2,1)(\mathbb{F}_p),\mathbb{F}_p)\cong\mathfrak{su}(2,1)(\mathbb{F}_p)$ given by the Killing form. Furthermore, it is clear from the orders of

$\mathcal{G}(\mathbb{F}_p)$ and $N(\mathbb{F}_p)$ that $N(\mathbb{F}_p)$ can be taken as a choice of p-Sylow subgroup for $\mathcal{G}(\mathbb{F}_p)$. Our aim is to calculate the image of the monomorphism

$$H^1(\mathcal{G}(\mathbb{F}_p), \mathfrak{su}(2,1)(\mathbb{F}_p)) \hookrightarrow H^1(N(\mathbb{F}_p), \mathfrak{su}(2,1)(\mathbb{F}_p)).$$

Since $\mathfrak{su}(2,1)(\mathbb{F}_p)$ is a finite dimensional $\mathbb{F}_p$-vector space, we can tensor with the quadratic extension $\mathbb{F}_{p^2}$ of $\mathbb{F}_p$ to obtain for all n,

$$\begin{aligned} H^n(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathfrak{su}(2,1)(\mathbb{F}_p)) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2} &\cong H^n(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathfrak{su}(2,1)(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}) \\ &\cong H^n(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F}_{p^2})). \end{aligned}$$

To ease notation, we will write $\mathbb{F}$ for $\mathbb{F}_{p^2}$. With this formulation, we need to find the image of the monomorphism $H^r(\mathcal{G}(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F})) \hookrightarrow H^r(N(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F}))$.

Proposition 3.2.3. *Let $N(\mathbb{F}_p)$ be as above and $g \in \mathcal{G}(\mathbb{F}_p)$. Then*

$$N \cap g^{-1}Ng = \begin{cases} N & g \in B \\ 1 & \textit{otherwise}, \end{cases}$$

where $B \subset \mathcal{G}(\mathbb{F}_p)$ is the Borel subgroup consisting of all upper triangular matrices. In particular,

$$H^n(\mathcal{G}(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F})) \cong H^n(N(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F}))^{T(\mathbb{F}_p)} \qquad \textit{for all} \quad n > 0,$$

where $T(\mathbb{F}_p)$ *is the maximal torus of* $\mathcal{G}(\mathbb{F}_p)$*.*

Proof. Recall the Bruhat decomposition of $\mathcal{G}(\mathbb{F}_p)$ from Theorem 1.2.1;

$$\mathcal{G}(\mathbb{F}_p) = N(\mathbb{F}_p)T(\mathbb{F}_p) \sqcup N(\mathbb{F}_p)T(\mathbb{F}_p)wN(\mathbb{F}_p),$$

where w is the non-trivial element of the Weyl group of $\mathcal{G}(\mathbb{F}_p)$. It is clear that B normalises N. It remains to show what happens when g has a non-zero $(3,1)$ entry. In this case, we can write $g = nwtn'$ with $n, n' \in N(\mathbb{F}_p)$ and $t \in T(\mathbb{F}_p)$. Now,

$$\begin{aligned} N \cap N^g &= N \cap N^{nwtn'} \\ &= N \cap N^{wtn'} \\ &= (N \cap N^w)^{tn'} \\ &= 1. \end{aligned}$$

Since $B/N(\mathbb{F}_p) \cong T(\mathbb{F}_p)$, we have

$$H^1(\mathcal{G}(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F})) \cong H^1(N(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F}))^{T(\mathbb{F}_p)}.$$

□

We are now in a very similar situation to the split case; we use the same filtration on $\mathfrak{sl}_3(\mathbb{F})$ as we had on $\mathfrak{sl}_3(\mathbb{F}_p)$ in equation (2.10), only now with entries in $\mathbb{F}$ rather than $\mathbb{F}_p$. Similarly, we denote the subspaces in it by $F(i)$ and $N(\mathbb{F}_p)$ can be shown to act trivially on each quotient $F(i)/F(i+1)$ for $0 \le i \le 4$ as before.

As a representation of $T(\mathbb{F}_p)$, we can decompose $\mathfrak{sl}_3(\mathbb{F})$ into a direct sum of weight spaces

$$\mathfrak{sl}_3(\mathbb{F}) = \mathfrak{g}_0 \oplus \bigoplus_{\phi\in\Phi'} \mathbb{F}(\phi),$$

where $\Phi' = \{(\alpha\beta)^{\pm 1}, \alpha^{\pm 1}, \beta^{\pm 1}\}$ is a collection of linear functionals on $T(\mathbb{F}_p)$, this time defined by

$$\begin{aligned} \alpha\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \bar{\lambda}/\lambda & 0 \\ 0 & 0 & \bar{\lambda}^{-1} \end{pmatrix} &= (\lambda)/(\bar{\lambda}/\lambda) = \lambda^{2-p} \quad \text{and} \\ \beta\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \bar{\lambda}/\lambda & 0 \\ 0 & 0 & \bar{\lambda}^{-1} \end{pmatrix} &= (\bar{\lambda}/\lambda)/(\bar{\lambda}^{-1}) = \lambda^{2p-1}, \end{aligned}$$

and $\mathfrak{g}_0$ is 2-dimensional over $\mathbb{F}$ which will often be denoted by $\mathbb{F}(0)^2$. We will write the linear functionals in Φ' additively, and $\Phi = \{\pm(\alpha+\beta), \pm\alpha, \pm\beta\}$ will denote this collection of additive linear functionals. Again, the quotients of successive subspaces in the filtration can be expressed as

$$\begin{aligned} F(0)/F(1) &= \mathbb{F}(-\alpha-\beta),\ F(1)/F(2)=\mathbb{F}(-\alpha)\oplus\mathbb{F}(-\beta),\ F(2)/F(3)=\mathbb{F}(0)^2,\\ F(3)/F(4) &= \mathbb{F}(\alpha)\oplus\mathbb{F}(\beta),\ F(4)/F(5)=\mathbb{F}(\alpha+\beta), \end{aligned}$$

and our strategy will be to successively calculate $H^1(N(\mathbb{F}_p),F(i))^{T(\mathbb{F}_p)}$.

Let Z denote the center of $N(\mathbb{F}_p)$. As a group, $N/Z\cong\mathbb{F}_{p^2}$ and T acts upon it by multiplication by α. We denote this T-module by $\mathbb{F}_{p^2}(\alpha)$. Suppose $\mathbb{F}$ is a trivial T-module. Note that $\mathrm{Hom}(N/Z,\mathbb{F})$ is generated by two homomorphisms; the identity map $x\mapsto x$ and the map $x\mapsto\bar{x}=x^p$. Call these two maps f_1 and f_2. Then $t_\lambda\in T$ acts upon f_1 and f_2 by

$$\begin{aligned} t_\lambda\circ f_1(x) &= f_1(t_\lambda^{-1}x)=f_1(\alpha(t_\lambda^{-1})x)=\alpha(t_\lambda^{-1})x, \quad \text{and}\\ t_\lambda\circ f_2(x) &= f_2(t_\lambda^{-1}x)=f_2(\alpha(t_\lambda^{-1})x)=\overline{\alpha(t_\lambda^{-1})x}=\beta(t_\lambda^{-1})\overline{x}. \end{aligned}$$

Written additively, this is multiplication by $-\alpha$ and $-\beta$ respectively. Hence as a $T(\mathbb{F}_p)$-module, $\mathrm{Hom}(N/Z,\mathbb{F})\cong\mathbb{F}\oplus\mathbb{F}$ and T acts upon one of the copies of $\mathbb{F}$ by multiplication by $-\alpha$ and on the other by $-\beta$. We express this action of T by writing $\mathrm{Hom}(N/Z,\mathbb{F})\cong\mathbb{F}(-\alpha)\oplus\mathbb{F}(-\beta)$.

Now since N/Z acts trivially on each quotient $F(i)/F(i+1)$, as a T-module we have

$$\operatorname{Hom}(N/Z, F(i)/F(i+1)) \cong \operatorname{Hom}(N/Z, \mathbb{F}) \otimes F(i)/F(i+1),$$

where $\mathbb{F}$ denotes a trivial $\mathcal{G}(\mathbb{F}_p)$-module. Adopting the above notation, we have as before the following isomorphisms of T-modules:

$$\begin{aligned}
H^1(N/Z, F(4)) &= \mathbb{F}(\beta) \oplus \mathbb{F}(\alpha), \\
H^1(N/Z, F(3)/F(4)) &= \mathbb{F}(0) \oplus \mathbb{F}(-\alpha+\beta) \oplus \mathbb{F}(-\beta+\alpha) \oplus \mathbb{F}(0), \\
H^1(N/Z, F(2)/F(3)) &= \mathbb{F}(-\alpha)^2 \oplus \mathbb{F}(-\beta)^2, \\
H^1(N/Z, F(1)/F(2)) &= \mathbb{F}(-2\alpha) \oplus \mathbb{F}(-\alpha-\beta) \oplus \mathbb{F}(-\beta-\alpha) \oplus \mathbb{F}(-2\beta), \\
H^1(N/Z, F(0)/F(1)) &= \mathbb{F}(-2\alpha-\beta) \oplus \mathbb{F}(-2\beta-\alpha).
\end{aligned}$$

We see immediately that there is a subspace $\mathbb{F}^2$ of $H^1(N/Z, F(3)/F(4))$ invariant under T. Simple calculations show that the other linear functionals are non-zero for $p > 2$ (and hence also for our assumption $p > 3$), so no other subspaces are fixed for any values of i other than the subspace $\mathbb{F}^2$ we already observed. Finally, noting that $\left|T\right| = p^2 - 1 \equiv -1 \mod p$, it follows that $(-)^T$ is an exact functor on $\mathbb{F}\left[T(\mathbb{F}_p)\right]$-modules. We are now in the same situation as the split case, only with $\mathbb{F}$-modules rather than $\mathbb{F}_p$-modules. Performing the same analysis as when p is split, we see that the cohomology we pick up at $H^1(N/Z, F(3)/F(4))$ disappears further up the filtration. We arrive at the conclusion that $H^1(N, \mathfrak{sl}_3(\mathbb{F}))^T = 0$, and so

$$H^1(\mathrm{SU}(2,1)(\mathbb{F}_p), \mathfrak{sl}_3(\mathbb{F})) = 0 \qquad \text{for } p > 3.$$

In the spectral sequence converging to $H^{r+s}(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p)$, we have shown that $E_2^{2,0} = 0$ and $E_2^{1,1} = 0$. We now consider the $E_2^{0,2}$ term, which involves finding $H^2(\mathfrak{su}(2,1)(\mathbb{F}_p), \mathbb{F}_p)^{\mathrm{SU}(2,1)(\mathbb{F}_p)}$. Viewing $\mathfrak{su}(2,1)(\mathbb{F}_p)$ as an 8-dimensional vector space over $\mathbb{F}_p$, by Lemma 2.1.12 we have a short exact sequence of $\mathrm{SU}(2,1)(\mathbb{F}_p)$-modules,

$$0 \to H^1(\mathfrak{su}(2,1)(\mathbb{F}_p), \mathbb{F}_p) \to H^2(\mathfrak{su}(2,1)(\mathbb{F}_p), \mathbb{F}_p) \to \bigwedge^2 H^1(\mathfrak{su}(2,1)(\mathbb{F}_p), \mathbb{F}_p) \to 0.$$

We will in fact prove a slightly more general Lemma than the result we need in this section, but this will have the advantage that it will also be applicable in the next chapter.

Lemma 3.2.4. *Let $p > 3$ be a rational prime and $\mathrm{SO}(2,1)(\mathbb{F}_p) \subset \mathrm{SU}(2,1)(\mathbb{F}_p)$ the subgroup of all matrices $g \in \mathrm{SL}_3(\mathbb{F}_p)$ such that $g^t J g = J$. Then*

$$H^0(\mathrm{SO}(2,1)(\mathbb{F}_p), H^2(\mathfrak{su}(2,1)(\mathbb{F}_p), \mathbb{F}_p)) = 0.$$

Proof. It will be sufficient to show that both $\left(\bigwedge^2 \mathfrak{su}(2,1)(\mathbb{F}_p)\right)^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$ and $(\mathfrak{su}(2,1)(\mathbb{F}_p))^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$. We note that the maximal $\mathbb{F}_p$-split torus $S(\mathbb{F}_p) \subset \mathrm{SU}(2,1)(\mathbb{F}_p)$ also lies in $\mathrm{SO}(2,1)(\mathbb{F}_p)$, and that $\mathrm{SO}(2,1)(\mathbb{F}_p)$ acts with no fixed points on $\mathfrak{su}(2,1)(\mathbb{F}_p)$. Thus we are left with showing that $\left(\bigwedge^2 \mathfrak{su}(2,1)(\mathbb{F}_p)\right)^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$. Now, as a representation of $S(\mathbb{F}_p)$ we can write $\mathfrak{su}(2,1)(\mathbb{F}_p)$ as

$$\mathfrak{su}(2,1)(\mathbb{F}_p) = \mathfrak{g}_0 \oplus \bigoplus_{\phi \in \Sigma} \mathfrak{g}_\phi,$$

where $\mathfrak{g}_0$ and each $\mathfrak{g}_\phi$ are as in equation (1.1) of section 1.2 (with $k = \mathbb{F}_p$ and $K = \mathbb{F}_{p^2}$) and when written additively instead of multiplicatively, Σ is also as in section 1.2. Then

$$\bigwedge^2 \mathfrak{su}(2,1)(\mathbb{F}_p) = \bigwedge^2 \mathfrak{g}_0 \oplus \bigoplus_{\phi \in \Sigma} (\mathfrak{g}_0 \wedge \mathfrak{g}_\phi) \oplus \bigoplus_{\substack{\phi, \varphi \in \Sigma \\ \phi > \varphi}} \mathfrak{g}_\phi \wedge \mathfrak{g}_\varphi.$$

Taking $S(\mathbb{F}_p)$-invariants, we notice that

$$\begin{aligned} \left(\bigoplus_{\phi \in \Sigma} (\mathfrak{g}_0 \wedge \mathfrak{g}_\phi)\right)^{S(\mathbb{F}_p)} &= 0 \quad \text{and} \\ \left(\bigoplus_{\substack{\phi, \varphi \in \Sigma \\ \phi > \varphi}} \mathfrak{g}_\phi \wedge \mathfrak{g}_\varphi\right)^{S(\mathbb{F}_p)} &= \bigoplus_{\substack{\phi \in \Sigma \\ \phi > 0}} \mathfrak{g}_\phi \wedge \mathfrak{g}_{-\phi}, \end{aligned}$$

so we have

$$\left(\bigwedge^2 \mathfrak{su}(2,1)(\mathbb{F}_p)\right)^{S(\mathbb{F}_p)} = \bigwedge^2 \mathfrak{g}_0 \oplus \bigoplus_{\substack{\phi \in \Sigma \\ \phi > 0}} \mathfrak{g}_\phi \wedge \mathfrak{g}_{-\phi}.$$

Recall from section 1.2, the non-trivial element of the Weyl group which we represented by $w = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \in W \subset \mathrm{SO}(2,1)(\mathbb{F}_p)$. We will see that W preserves the subspaces $\bigwedge^2 \mathfrak{g}_0$ and $\mathfrak{g}_\phi \wedge \mathfrak{g}_{-\phi}$ but acts non-trivially, leaving nothing fixed under its action. So let $z \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Then

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \wedge \begin{pmatrix} z & 0 & 0 \\ 0 & \bar{z} - z & 0 \\ 0 & 0 & -\bar{z} \end{pmatrix} \overset{w}{\longmapsto} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \wedge \begin{pmatrix} -\bar{z} & 0 & 0 \\ 0 & \bar{z} - z & 0 \\ 0 & 0 & z \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \wedge \begin{pmatrix} \bar{z} & 0 & 0 \\ 0 & z - \bar{z} & 0 \\ 0 & 0 & -z \end{pmatrix},$$

but $z \neq \bar{z}$, so $\left(\bigwedge^2 \mathfrak{g}_0\right)^{\langle w \rangle} = 0$. Similarly, for α_0 as in equation (1.1),

$$\begin{pmatrix} 0 & 0 & \alpha_0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \alpha_0 & 0 & 0 \end{pmatrix} \overset{w}{\longmapsto} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \alpha_0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & \alpha_0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$
$$= -\begin{pmatrix} 0 & 0 & \alpha_0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \alpha_0 & 0 & 0 \end{pmatrix},$$

showing that $(\mathfrak{g}_{2\lambda} \wedge \mathfrak{g}_{-2\lambda})^{\langle w \rangle} = 0$. Finally,

$$\begin{pmatrix} 0 & x & 0 \\ 0 & 0 & -\bar{x} \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ y & 0 & 0 \\ 0 & -\bar{y} & 0 \end{pmatrix} \overset{w}{\longmapsto} \begin{pmatrix} 0 & \bar{y} & 0 \\ 0 & 0 & -y \\ 0 & 0 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 \\ -\bar{x} & 0 & 0 \\ 0 & x & 0 \end{pmatrix}.$$

So for $\mathfrak{g}_\lambda \wedge \mathfrak{g}_{-\lambda}$ to have elements fixed by w, we would require

$$\begin{pmatrix} 0 & x & 0 \\ 0 & 0 & -\bar{x} \\ 0 & 0 & 0 \end{pmatrix} = \lambda \begin{pmatrix} 0 & \bar{y} & 0 \\ 0 & 0 & -y \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and}$$
$$\begin{pmatrix} 0 & 0 & 0 \\ y & 0 & 0 \\ 0 & -\bar{y} & 0 \end{pmatrix} = \lambda^{-1} \begin{pmatrix} 0 & 0 & 0 \\ -\bar{x} & 0 & 0 \\ 0 & x & 0 \end{pmatrix},$$

for some $\lambda \in \mathbb{F}_{p^2}$. However, our assumption that $p > 3$ leaves $\lambda = 0$ as the only possibility. Hence $\left(\bigwedge^2 \mathfrak{su}(2,1)(\mathbb{F}_p)\right)^{S(\mathbb{F}_p)\langle w \rangle} = 0$ which immediately implies that $\left(\bigwedge^2 \mathfrak{su}(2,1)(\mathbb{F}_p)\right)^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$. □

Since $\mathrm{SO}(2,1)(\mathbb{F}_p) \subset \mathrm{SU}(2,1)(\mathbb{F}_p)$, we have the following Corollary.

Corollary 3.2.5. *For all rational primes $p > 3$ and all $n > 0$,*

$$H^0(\mathcal{G}(0)/\mathcal{G}(n), H^2(\mathcal{G}(n)/\mathcal{G}(n+1), \mathbb{F}_p)) = 0.$$

An immediate consequence is that $H^2(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p) = 0$. The final result we need for the inert case is the following Proposition.

Proposition 3.2.6. *For all $n > 0$ and $p > 3$ inert,*

$$H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right)\right) = 0.$$

Proof. The proof is the same as the proof of Proposition 2.3.9, which made no use of p being split. □

We can summarise the above work into the following theorem.

Theorem 3.2.7. *Let p and q be rational primes with p inert in k. Then*

(i) $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) = 0$ *for all p and q, excluding the case $p = q = 2$,*

(ii) $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p) = 0$ *for all $p > 3$, and*

(iii) $H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) = 0$ *for all $p > 2$ and $p \neq q$, and all $q > 3$ when $p = 2$.*

Proof. The first statement is Corollary 3.1.5. The second statement follows from Propositions 3.2.1 and 3.2.6, Corollary 3.2.5 and the Hochschild-Serre spectral sequence $H^r\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^s\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right)\right) \implies H^{r+s}\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right)$. This, along with Proposition 2.1.1 gives the second assertion. The third statement is Corollary 3.2.2. □

Chapter 4

Low Dimensional Cohomology of $\mathrm{SU}(2,1)(\mathbb{Z}_p)$ with p Ramified

So far we have successfully shown that, excluding a finite number of small primes, $H^1(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q) = 0$ and $H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q) = 0$ when p is unramified. The final possibility for $p \in \mathbb{Z}$ is that it ramifies in k. This means that there exists a prime ideal $\mathfrak{p} \subset \mathcal{O}_k$ such that $p\mathcal{O}_k = \mathfrak{p}^2$. In this chapter we turn our attention to the cohomology groups H^1 and H^2 of $\mathcal{G}(\mathbb{Z}_p)$ for when $p \in \mathbb{Z}$ ramifies in k. When considering the first cohomology group, we will be able to show that $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) = 0$ for all primes p with $q > 2$ and $(p, q) \neq (3, 3)$. We note however, that in the ramified case we will require a different approach in order to achieve this. For all primes p with $q > 2$ and $(p, q) \neq (3, 3)$, we will once again be able to show that $H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q) = 0$.

Throughout this chapter, p will be a rational prime such that $p\mathcal{O}_k = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p} \subset \mathcal{O}_k$.

4.1 Initial Results

Throughout this section p and q will denote rational primes. We have a filtration on $\mathcal{G}(\mathbb{Z}_p)$ given by

$$\mathcal{G}(\mathbb{Z}_p) \supset \mathcal{G}(\mathbb{Z}_p, \mathfrak{p}) \supset \mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^2) \supset \cdots \supset \mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n) \supset \cdots , \tag{4.1}$$

whose terms we will often abbreviate to just $\mathcal{G}(n)$. It will be important for us to understand the quotients $\mathcal{G}(n)/\mathcal{G}(n+1)$ in this filtration. They behave a little differently to the unramified cases and we determine them in the following Lemma.

Lemma 4.1.1. *The quotients in filtration 4.1 are given by*

$$\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^n)/\mathcal{G}(\mathbb{Z}_p, \mathfrak{p}^{n+1}) = \begin{cases} \mathrm{SO}(2,1)(\mathbb{F}_p) & n = 0, \\ \mathfrak{sl}_2(\mathbb{F}_p) & n \text{ even and positive}, \\ \{X \in \mathfrak{sl}_3(\mathbb{F}_p) : X^t J - JX \equiv 0 \mod \mathfrak{p}\} & n \text{ odd}. \end{cases}$$

Proof. When $n = 0$, we have

$$\mathcal{G}(0)/\mathcal{G}(1) = \left\{ g \in \mathrm{SL}_3(\mathcal{O}_k/\mathfrak{p}) : g^t J \bar{g} = J \right\},$$

but $\bar{g} = g$ when $g \in \mathrm{SL}_3(\mathcal{O}_k/\mathfrak{p})$ and so $\mathcal{G}(0)/\mathcal{G}(1) \cong \mathrm{SO}(2,1)(\mathbb{F}_p)$.

Now take $n > 0$ to be even and let $\pi \in k$ be a prime element, chosen so that $\overline{\pi} \equiv -\pi \mod \mathfrak{p}^2$. Then $g \in \mathcal{G}(n)/\mathcal{G}(n+1)$ can be written in the form $1 + \pi^n X$, where $X \in \mathfrak{sl}_3(\mathcal{O}_k/\mathfrak{p})$ and $(1+\pi^n X)^t J\overline{(1+\pi^n X)} = J$. Now,

$$\begin{aligned}(1+\pi^n X)^t J\overline{(1+\pi^n X)} &= J \\ \iff J + \pi^n(X^t J + JX) &= J \\ \iff X^t J + JX &\equiv 0 \mod \mathfrak{p}.\end{aligned}$$

That is, $X \in \mathfrak{so}(2,1)(\mathbb{F}_p) \cong \mathfrak{sl}_2(\mathbb{F}_p)$. Finally, let $n > 0$ have odd parity. Again, $g \in \mathcal{G}(n)/\mathcal{G}(n+1)$ can be written in the form $1 + \pi^n X$, where $X \in \mathfrak{sl}_3(\mathcal{O}_k/\mathfrak{p})$ and $(1+\pi^n X)^t J\overline{(1+\pi^n X)} = J$. This time the matrix condition gives us

$$\begin{aligned}(1+\pi^n X)^t J\overline{(1+\pi^n X)} &= J \\ \iff J + \pi^n(X^t J - JX) &= J \\ \iff X^t J - JX &\equiv 0 \mod \mathfrak{p}.\end{aligned}$$

□

In light of this Lemma, we will need to know some facts about $\mathrm{SO}(2,1)(\mathbb{F}_p)$. In particular, we will need to know what its q-Sylow subgroups are.

Lemma 4.1.2. *Suppose that $q > 2$ is a rational prime such that q divides the order* *of* $\mathrm{SO}(2,1)(\mathbb{F}_p)$. *The* q*-Sylow subgroup of* $\mathrm{SO}(2,1)(\mathbb{F}_p)$ *is cyclic and can be taken to be a subgroup of one of the following three subgroups of* $\mathrm{SO}(2,1)(\mathbb{F}_p)$*:*

(i) The split torus $S(\mathbb{F}_p)$ *consisting of all matrices of the form*

$$\left\{ \begin{pmatrix} s & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & s^{-1} \end{pmatrix} : s \in \mathbb{F}_p^{\times} \right\},$$

(ii) the subgroup $N(\mathbb{F}_p)$ *of upper triangular matrices with* 1*'s on the diagonal, or*

(iii) the non-split torus in $\mathrm{SO}(2,1)(\mathbb{F}_p)$.

Proof. First, $|\mathrm{SO}(2,1)(\mathbb{F}_p)| = p(p-1)(p+1)$, so that for $q \big| |\mathrm{SO}(2,1)(\mathbb{F}_p)|$, q divides only one of $p-1$, p or $p+1$. Suppose first that $p-1 = q^a m_1$, with $a > 0$, $a, m_1 \in \mathbb{Z}$. Clearly the split torus is a cyclic subgroup of size $p-1$ and from it we can realise a cyclic subgroup of order q^a. The q-Sylow subgroup can then be taken to be this cyclic subgroup of order q^a.

Now, suppose $q = p$. A subgroup of order p can be constructed from the set of matrices of the form

$$N(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & -a^2/2 \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix} : a \in \mathbb{F}_p \right\},$$

which by explicit computation can be seen to be all of the upper triangular matrices in $\mathrm{SO}(2,1)(\mathbb{F}_p)$ with 1's down the diagonal. It is easy to see that this subgroup is cyclic and of order p.

Finally, suppose $p+1 = q^b m_2$, with $b > 0$ and $b, m_2 \in \mathbb{Z}$. We can construct a subgroup of order $p+1$ in the following way. We begin by recalling that $|\,\mathrm{SL}_3(\mathbb{F}_p)| = p^3(p-1)^2(p+1)(p^2+p+1)$, so the q-Sylow subgroup of $\mathrm{SO}(2,1)(\mathbb{F}_p)$ must also be a q-Sylow subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$. Take a quadratic extension $\mathbb{F}_{p^2}$ of $\mathbb{F}_p$ and fix a basis. We can associate every $x \in \mathbb{F}_{p^2}$ with an element of $M_2(\mathbb{F}_p)$ by constructing the $\mathbb{F}_p$-linear transformation given by multiplication by x. Taking the subgroup consisting of only those x with $\mathrm{N}(x) = 1$ gives us a subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ of order $p+1$, called the *non-split torus* of $\mathrm{SL}_2(\mathbb{F}_p)$. In particular, this subgroup is cyclic. Choosing an embedding $\mathrm{SL}_2(\mathbb{F}_p) \hookrightarrow \mathrm{SL}_3(\mathbb{F}_p)$ gives us a cyclic subgroup of order $p+1$ in $\mathrm{SL}_3(\mathbb{F}_p)$. So the q-Sylow subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$ is cyclic of order q^b and hence by conjugating by an element of $\mathrm{SL}_3(\mathbb{F}_p)$ if necessary, it is also a cyclic subgroup of order q^b in $\mathrm{SO}(2,1)(\mathbb{F}_p)$. This subgroup of order q^b can be taken to be the q-Sylow subgroup of $\mathrm{SO}(2,1)(\mathbb{F}_p)$ and is a subgroup of the non-split torus of $\mathrm{SO}(2,1)(\mathbb{F}_p)$, which is a cyclic group. $\square$

4.2 $H^i(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q)$ for $i = 1, 2$

In this section we compute $H^1(\mathcal{G}(0)/\mathcal{G}(1), \mathbb{F}_q)$ and $H^2(\mathcal{G}(0)/\mathcal{G}(1), \mathbb{F}_q)$, which by Lemma 4.1.1 amounts to finding $H^1(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q)$ and $H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q)$, respectively. When $p \neq q$, finding this will also give us both $H^1(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q)$ and $H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q)$, and when $p = q$ the calculations in this section will be used later to find $H^1(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_p)$ and $H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_p)$.

Proposition 4.2.1. *Let $q > 2$ be prime. Then*

$$\begin{aligned} H^1(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q) &= 0 \text{ and} \\ H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q) &= 0, \end{aligned}$$

for all primes p.

Proof. If $q \nmid |\mathrm{SO}(2,1)(\mathbb{F}_p)| = p(p-1)(p+1)$ then the result is clearly true. Otherwise, q divides either p, $p-1$ or $p+1$ and we check each case individually.

First, suppose $q = p$ (and so $p > 2$ under our assumption that $q > 2$). Then $H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_p) \hookrightarrow H^2(N, \mathbb{F}_p)$, where N is the p-Sylow subgroup from part (ii) of Lemma 4.1.2. Denote by $S(\mathbb{F}_p)$ (or simply S) the split torus from part (i) of Lemma 4.1.2. Explicit computation shows us that if $g = sn$ for some $s \in S$ and $n \in N$, then $N \cap g^{-1}Ng = N$. Otherwise by the Bruhat decomposition, g must be of the form $nwsn'$, where w is as in equation (1.2) and $n' \in N$. Then

$N \cap N^{nwsn'} = N^{n'^{-1}s^{-1}} \cap N^w = 1$. Thus

$$H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_p) = H^2(N, \mathbb{F}_p)^S.$$

Recall that N is a cyclic group of order p. The conjugation action of a generator $s_x = \begin{pmatrix} x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^{-1} \end{pmatrix} \in S(\mathbb{F}_p)$ on any $n \in N$ is seen to be multiplication by x, since

$$s_x n s_x^{-1} = s_x \begin{pmatrix} 1 & a & -a^2/2 \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix} s_x^{-1} = \begin{pmatrix} 1 & ax & -(ax)^2/2 \\ 0 & 1 & -ax \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus $s_x \in S$ acts on $H^1(N, \mathbb{F}_p)$ by multiplication by x^{-1} and by Lemma 2.3.3, also acts by multiplication by x^{-1} on $H^2(N, \mathbb{F}_p)$. Thus $H^1(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_p) = H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_p) = 0$.

Suppose $q \big| p-1$. Then by Lemma 4.1.2, the q-Sylow subgroup $\mathcal{G}_q$ lies in the split torus. Suppose $g \in \mathrm{SO}(2,1)(\mathbb{F}_p)$ with $g^{-1}\mathcal{G}_q g \cap \mathcal{G}_q \neq 1$. We claim that g normalises $\mathcal{G}_q$ and $S(\mathbb{F}_p)$. Suppose $\zeta = \begin{pmatrix} \xi & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi^{-1} \end{pmatrix}$ is a generator of $g^{-1}\mathcal{G}_q g \cap \mathcal{G}_q$. Since ζ and $g^{-1}\zeta g$ have the same eigenvalues, $g^{-1}\zeta g$ is either ζ or ζ^{-1}. In particular, note that $w^{-1}\zeta w = \zeta^{-1}$, where again w is as in equation (1.2). We are left with two cases:

if $g^{-1}\zeta g = \zeta$, then g commutes with ζ and hence $g \in S$, as can be seen by direct computation. Otherwise, if $g^{-1}\zeta g = \zeta^{-1}$ then $(gw)^{-1}\zeta gw = \zeta$ and so now $gw \in S$ and again g normalises S. Hence

$$\begin{aligned} H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q) &= H^2(\mathcal{G}_q, \mathbb{F}_q)^{N_{\mathrm{SO}(2,1)(\mathbb{F}_p)}(S)/Z_{\mathrm{SO}(2,1)(\mathbb{F}_p)}(S)} \\ &= H^2(\mathcal{G}_q, \mathbb{F}_q)^{\langle w \rangle}. \end{aligned}$$

The action of w on a generator $b \in \mathcal{G}_q$ is by $b \mapsto b^{-1}$. Thus w acts by multiplication by -1 on $H^1(\mathcal{G}_q, \mathbb{F}_q)$ and again by Lemma 2.3.3, also acts by multiplication by -1 on $H^2(\mathcal{G}_q, \mathbb{F}_q)$. Thus $H^1(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q) = H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q) = 0$.

Now suppose $q \big| p+1$ and $p > 2$; we will consider $p = 2$ separately. Then $\mathcal{G}_q$ is contained in the non-split torus of part (iii) of Lemma 4.1.2. Choose some $r \in \mathbb{F}_p$ such that in the notation of the Legendre symbol, $\left(\frac{r}{p}\right) = -1$. Then

$$\mathbb{F}_{p^2} = \left\{ x + y\sqrt{r} : x, y \in \mathbb{F}_p \right\}.$$

Recalling from the proof of Lemma 4.1.2 the construction of the non-split torus in $\mathrm{SL}_2(\mathbb{F}_p)$, we may write it down explicitly as

$$\left\{ \begin{pmatrix} x & ry \\ y & x \end{pmatrix} : x, y \in \mathbb{F}_p,\ x^2 - ry^2 = 1 \right\}.$$

We note that the non-split torus for $\mathrm{SL}_2(\mathbb{F}_p)$ is an orthogonal group in dimension 2 that preserves the quadratic form determined by the matrix $\begin{pmatrix} -1/r & 0 \\ 0 & 1 \end{pmatrix}$. We now embed the non-split torus of $\mathrm{SL}_2(\mathbb{F}_p)$ into $\mathrm{SL}_3(\mathbb{F}_p)$ via the mapping

$$\begin{pmatrix} x & ry \\ y & x \end{pmatrix} \longmapsto \begin{pmatrix} x & ry & 0 \\ y & x & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{4.2}$$

The image of this map lies in the special orthogonal group that preserves the quadratic form determined by the matrix $J' := \begin{pmatrix} -1/r & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Call this group $\mathrm{SO}(J')(\mathbb{F}_p)$ and denote the subgroup of $\mathrm{SO}(J')(\mathbb{F}_p)$ given by the image of the map 4.2 by H. From Section 62 of [23], there are precisely two non-degenerate quadratic forms in any dimension up to equivalence over a finite field of odd characteristic. This gives two possible choices of orthogonal groups, however in odd dimensions these two orthogonal groups are isomorphic. Thus it suffices to work with the group $\mathrm{SO}(J')(\mathbb{F}_p)$ and the subgroup $H \subset \mathrm{SO}(J')(\mathbb{F}_p)$, rather than $\mathrm{SO}(2,1)(\mathbb{F}_p)$ and its non-split torus. Consider the element

$$s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathrm{SO}(J')(\mathbb{F}_p).$$

We see that the action of s on H is

$$s^{-1}\begin{pmatrix} x & ry & 0 \\ y & x & 0 \\ 0 & 0 & 1 \end{pmatrix} s = \begin{pmatrix} x & -ry & 0 \\ -y & x & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} x & ry & 0 \\ y & x & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}.$$

Now, H is a cyclic subgroup containing the q-Sylow subgroup $\mathcal{G}_q \subset \mathrm{SO}(J')(\mathbb{F}_p)$. Lemma 2.3.3 tells us that s acts on $H^1(H, \mathbb{F}_q)$ and $H^2(H, \mathbb{F}_q)$ by multiplication by -1 and in particular, that s acts on $H^1(\mathcal{G}_q, \mathbb{F}_q)$ and $H^2(\mathcal{G}_q, \mathbb{F}_q)$ by multiplication by -1. It follows immediately that $H^1(\mathrm{SO}(J')(\mathbb{F}_p), \mathbb{F}_q) = H^2(\mathrm{SO}(J')(\mathbb{F}_p), \mathbb{F}_q) = 0$ when $q \big| p+1$, and hence $H^1(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q) = H^2(\mathrm{SO}(2,1)(\mathbb{F}_p), \mathbb{F}_q) = 0$ when $q \big| p+1$.

Finally, we take $p = 2$. Then $\big| \mathrm{SO}(2,1)(\mathbb{F}_2) \big| = 6$ and is the dihedral group of order 6, as can be seen by the matrices

$$\alpha = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Explicit calculations show that $\alpha, \beta \in \mathrm{SO}(2,1)(\mathbb{F}_p)$, $\left|\alpha\right| = 2$, $\left|\beta\right| = 3$ and that $\alpha^{-1}\beta\alpha = \beta^{-1}$. Since the only prime $q > 2$ that divides 6 is $q = 3$, we only have this possibility to check. The 3-Sylow subgroup is clearly $\langle\beta\rangle$ and the conjugation action of α on β gives an action of α on $H^1(\langle\beta\rangle, \mathbb{F}_3)$ and $H^2(\langle\beta\rangle, \mathbb{F}_3)$ by multiplication by -1. Thus $H^1(\mathrm{SO}(2,1)(\mathbb{F}_2), \mathbb{F}_q) = H^2(\mathrm{SO}(2,1)(\mathbb{F}_2), \mathbb{F}_q) = 0$ for all $q > 2$. □

Corollary 4.2.2. *For all primes $p \neq q$, $q > 2$ and p ramified, we have*

$$\begin{aligned} H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) &= 0 \quad \textit{and} \\ H^2(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_q) &= 0. \end{aligned}$$

4.3 $H^i(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p)$ for $i = 1, 2$

We will assume throughout this section that p is a rational prime greater than 3. We calculated that $H^2(\mathcal{G}(0)/\mathcal{G}(1), \mathbb{F}_p) = 0$ and $H^1(\mathcal{G}(0)/\mathcal{G}(1), \mathbb{F}_p) = 0$ in the previous section. We first use this result to find $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p)$, which will complete the calculations for H^1.

Proposition 4.3.1. *Let $p > 3$ be a ramified prime in k. Then*

$$H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p) = 0.$$

Proof. First recall from Proposition 4.2.1 that $H^1(\mathcal{G}(0)/\mathcal{G}(1), \mathbb{F}_p) = 0$, and we noted in the proof of Lemma 3.2.4 above that $(\mathfrak{su}(2,1)(\mathbb{F}_p))^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$, provided $p > 3$. It immediately follows from the fact that $\mathcal{G}(n)/\mathcal{G}(n+1) \subset \mathfrak{su}(2,1)(\mathbb{F}_p)$, that $(\mathcal{G}(n)/\mathcal{G}(n+1))^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$ for all $n > 0$. The spectral sequence

$$H^r(\mathcal{G}(0)/\mathcal{G}(1), H^s(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p)) \Longrightarrow H^{r+s}(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p),$$

gives the following exact sequence of low degree terms

$$0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(1)}, \mathbb{F}_p\right) \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(2)}, \mathbb{F}_p\right) \longrightarrow H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(1)}, H^1\left(\frac{\mathcal{G}(1)}{\mathcal{G}(2)}, \mathbb{F}_p\right)\right).$$

This tells us that $H^1(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p) = 0$. Inductively, the spectral sequence

$$H^r(\mathcal{G}(0)/\mathcal{G}(n), H^s(\mathcal{G}(n)/\mathcal{G}(n+1), \mathbb{F}_p)) \Longrightarrow H^{r+s}(\mathcal{G}(0)/\mathcal{G}(n+1), \mathbb{F}_p),$$

gives us $H^1(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p) = 0$ for all $n > 0$. Thus $H^1(\mathrm{SU}(2,1)(\mathbb{Z}_p), \mathbb{F}_p) = 0$, as required. □

We now consider $H^2(\mathcal{G}(0), \mathbb{F}_p)$, which we do by finding $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p)$ for each $n > 1$. To achieve this, we will once again make use of the Hochschild-Serre spectral sequence

$$H^r(\mathcal{G}(0)/\mathcal{G}(n), H^s(\mathcal{G}(n)/\mathcal{G}(n+1), \mathbb{F}_p)) \Longrightarrow H^{r+s}(\mathcal{G}(0)/\mathcal{G}(n+1), \mathbb{F}_p),$$

with $r + s = 2$. We begin with $n = 1$. Since we have already done the calculation for $r = 2$ and $s = 0$, we take $r = 1$ and $s = 1$ and our immediate aim is to find $H^1(\mathrm{SO}(2,1)(\mathbb{F}_p), H^1(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p))$. First, recall from Lemma 4.1.1 that

$$\mathcal{G}(1)/\mathcal{G}(2) = \left\{ X \in \mathfrak{sl}_3(\mathbb{F}_p) : X^t J - JX \cong 0 \mod \mathfrak{p} \right\}.$$

For brevity, we set $M = \mathcal{G}(1)/\mathcal{G}(2)$ and note that as a $\mathcal{G}(0)$-module, M is also isomorphic to $\mathcal{G}(n)/\mathcal{G}(n+1)$ for all odd $n > 0$. Again for $p > 3$, the Killing form gives an $\mathrm{SO}(2,1)(\mathbb{F}_p)$-equivariant isomorphism between M and $H^1(M, \mathbb{F}_p)$. This, together with Lemma 4.1.2 and the fact that $N \cap g^{-1}Ng = N$ if $g \in N \rtimes S$ and 1 otherwise, gives an isomorphism

$$H^1(\mathrm{SO}(2,1)(\mathbb{F}_p), H^1(M, \mathbb{F}_p)) \cong H^1(N(\mathbb{F}_p), M)^{S(\mathbb{F}_p)}.$$

Direct computation shows that M has dimension 5 as an $\mathbb{F}_p$-vector space, and has a basis given by

$$m_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, m_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, m_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{4.3}$$

$$m_{-1} = m_1^t \text{ and } m_{-2} = m_2^t.$$

We now choose a filtration on M, given by

$$M = M(0) \supset M(1) \supset \cdots \supset M(4) \supset M(5) = 0,$$

where $M(i) = \langle m_{i-2}, \cdots, m_2 \rangle$ for each $0 \leq i \leq 4$. A routine check verifies that each quotient $M(i)/M(i+1)$ is fixed under the action of N. Furthermore, if $s_x = \begin{pmatrix} x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^{-1} \end{pmatrix} \in S(\mathbb{F}_p)$, then s_x acts on $M(i)/M(i+1)$ by multiplication by x^{i-2}, and s_x acts on N by multiplication by x. Given that for each i we have an S-module isomorphism

$$H^1(N, M(i)/M(i+1)) \cong H^1(N, \mathbb{F}_p) \otimes M(i)/M(i+1),$$

we see that s_x acts on $H^1(N, M(i)/M(i+1))$ by multiplication by $x^{-1}x^{i-2} = x^{i-3}$. So, given $x \in \mathbb{F}_p^\times$, we need to know for which $0 \leq i \leq 4$ gives $x^{i-3} = 1$ for all x. Clearly this happens when $i = 3$. However, our assumption that $p > 3$ guarantees that a choice of x with $|x| > 3$ can be made, hence $x^{i-3} = 1$ if and only if $i = 3$. Written another way, this says that $H^1(N, M(3)/M(4))^{S(\mathbb{F}_p)} = \mathbb{F}_p$, and that $H^1(N, M(i)/M(i+1))^{S(\mathbb{F}_p)} = 0$ for $i \neq 3$. We can now proceed in a similar manner to the unramified cases. Namely, take the short exact sequence

$$0 \longrightarrow M(4) \longrightarrow M(3) \longrightarrow M(3)/M(4) \longrightarrow 0,$$

this gives a long exact sequence

$$\begin{aligned} 0 \longrightarrow M(4)^N \longrightarrow M(3)^N \longrightarrow M(3)/M(4)^N \longrightarrow H^1(N, M(4)) \longrightarrow \\ \longrightarrow H^1(N, M(3)) \longrightarrow H^1(N, M(3)/M(4)) \longrightarrow \cdots . \end{aligned}$$

$\left|S\right| = p - 1$ which is clearly coprime to p, so $(-)^S$ is an exact functor on $\mathbb{F}_p\left[S(\mathbb{F}_p)\right]$-modules. Writing $B = N \rtimes S$, we may take S-invariants in this long exact sequence to arrive at the long exact sequence

$$\begin{aligned} 0 \longrightarrow M(4)^B \longrightarrow M(3)^B \longrightarrow M(3)/M(4)^B \longrightarrow H^1(N, M(4))^S \longrightarrow \\ \longrightarrow H^1(N, M(3))^S \longrightarrow H^1(N, M(3)/M(4))^S \longrightarrow \cdots . \end{aligned}$$

The first 4 terms in the sequence are 0, so this gives

$$0 \longrightarrow H^1(N, M(3))^S \longrightarrow \mathbb{F}_p \longrightarrow H^2(N, M(4))^S \longrightarrow \cdots .$$

It follows that $H^1(N, M(3))^S$ is either 0 or $\mathbb{F}_p$. The next quotient $M(2)/M(3)$ in the filtration on M fits into the short exact sequence

$$0 \longrightarrow M(3) \longrightarrow M(2) \longrightarrow M(2)/M(3) \longrightarrow 0,$$

which gives the corresponding long exact sequence

$$0 \longrightarrow M(3)^B \longrightarrow M(2)^B \longrightarrow M(2)/M(3)^B \longrightarrow H^1(N, M(3))^S \longrightarrow$$
$$\longrightarrow H^1(N, M(2))^S \longrightarrow H^1(N, M(2)/M(3))^S \longrightarrow \cdots .$$

Note that $M(3)^B = M(2)^B = 0$, $(F(2)/F(3))^B = \mathbb{F}_p$ and recall from above that $H^1(N, F(2)/F(3))^T = 0$. With this, the long exact sequence is

$$0 \longrightarrow \mathbb{F}_p \longrightarrow H^1(N, M(3))^S \longrightarrow H^1(N, M(2))^S \longrightarrow 0 \longrightarrow \cdots .$$

From this it becomes clear that the only option for $H^1(N, F(3))^S$ is $\mathbb{F}_p$ and subsequently that $H^1(N, M(2))^S = 0$. Carrying on in a similar way, we arrive at the conclusion that $H^1(N, M)^S = 0$. That is,

$$H^1(\mathcal{G}(0)/\mathcal{G}(1), H^1(\mathcal{G}(1)/\mathcal{G}(2), \mathbb{F}_p)) = 0. \tag{4.4}$$

Whilst we do not need the calculation immediately, we will later need to know what $H^1(\mathcal{G}(0)/\mathcal{G}(1), H^1(\mathcal{G}(2)/\mathcal{G}(3), \mathbb{F}_p))$ is. Since this is similar to what we have just done, we will look at it now. For brevity, define $L = \mathcal{G}(2)/\mathcal{G}(3)$ which we note is also isomorphic as a $\mathcal{G}(0)$-module to $\mathcal{G}(n)/\mathcal{G}(n+1)$ for all even $n > 0$. Following what we did above, we see that finding $H^1(\mathcal{G}(0)/\mathcal{G}(1), L)$ amounts to finding $H^1(N, L)^{S(\mathbb{F}_p)}$. The following is a basis for L over $\mathbb{F}_p$:

$$l_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}, l_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, l_{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

Again, choose a filtration on L by

$$L = L(0) \supset L(1) \supset L(2) \supset L(3) = 0,$$

where $L(i) = \langle l_{i-1}, \cdots, l_1 \rangle$ for each $0 \leq i \leq 2$. We are now in a very similar situation to what we had above. Following the same method, we again see that

$$H^1(\mathcal{G}(0)/\mathcal{G}(1), H^1(\mathcal{G}(2)/\mathcal{G}(3), \mathbb{F}_p)) = 0. \tag{4.5}$$

To find $H^2(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p)$, we still need to know $H^0(\mathcal{G}(0)/\mathcal{G}(1), H^2(M, \mathbb{F}_p))$, which corresponds to the $E_2^{0,2}$ entry in the spectral sequence converging to it.

Proposition 4.3.2. *Fix a prime $p > 3$. Then*

$$H^0(\mathcal{G}(0)/\mathcal{G}(1), H^2(M, \mathbb{F}_p)) = 0,$$

and furthermore, $H^0(\mathcal{G}(0)/\mathcal{G}(n), H^2(M, \mathbb{F}_p)) = 0$ for all odd $n > 0$.

Proof. We begin by noting that $M \subset \mathfrak{su}(2,1)(\mathbb{F}_p)$ and from Lemma 3.2.4, we already know that

$$(H^2(\mathfrak{su}(2,1)(\mathbb{F}_p), \mathbb{F}_p))^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0.$$

It follows that $(H^2(M, \mathbb{F}_p))^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$ and $(H^2(M, \mathbb{F}_p))^{\mathcal{G}(0)/\mathcal{G}(n)} = 0$ for all odd $n > 0$, completing the proof. □

Keeping in line with the unramified cases, we have been able to show that $H^2(\mathcal{G}(0)/\mathcal{G}(2), \mathbb{F}_p) = 0$. Of course our ultimate aim is to find $H^2(\mathcal{G}(0)/\mathcal{G}(n), \mathbb{F}_p)$ for each n. We can prove the corresponding Proposition in the ramified case to Proposition 2.3.9 from the split case, only this time the proof needs treating slighty differently due to $\mathcal{G}(n)/\mathcal{G}(n+1)$ having dependency on the parity of n.

Proposition 4.3.3. *For each $n \geq 1$ and all primes $p > 3$,*

$$H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \mathbb{F}_p\right)\right) = 0.$$

Proof. The proof will be by induction. We've shown that the result is true for $n = 1$, and we consider the short exact sequence

$$1 \longrightarrow \mathcal{G}(n)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n+1) \longrightarrow \mathcal{G}(0)/\mathcal{G}(n) \longrightarrow 1,$$

giving us the corresponding Hochschild-Serre spectral sequence

$$H^r\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^s\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)\right) \Longrightarrow H^{r+s}\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right).$$

Recall that $\mathcal{G}(n)/\mathcal{G}(n+1)$ acts trivially on $\mathcal{G}(n+1)/\mathcal{G}(n+2)$ when $n \geq 1$ and the spectral sequence gives us an exact sequence of low degree terms,

$$0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) \longrightarrow$$
$$\longrightarrow H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)\right) \longrightarrow H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right).$$

Here is where the difference lies between the ramified and unramified cases; unlike in the unramified cases, we cannot assume at this stage that $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) = 0$ as part of an inductive hypothesis in the same way as we did in Proposition 2.3.9.

However, we do notice now that

$$H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)\right) = \mathrm{Hom}\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)^{\frac{\mathcal{G}(0)}{\mathcal{G}(n)}},$$

which is isomorphic to either $\mathrm{Hom}(M, L)^{\mathcal{G}(0)/\mathcal{G}(n)}$ or $\mathrm{Hom}(L, M)^{\mathcal{G}(0)/\mathcal{G}(n)}$, depending on the parity of n (recall that M and L are isomorphic as $\mathcal{G}(0)$-modules to $\mathcal{G}(n)/\mathcal{G}(n+1)$ for all odd (resp. even) $n > 0$). In either case, they are both 0 and hence $H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)\right) = 0$. So the exact sequence becomes

$$0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) \longrightarrow 0. \tag{4.6}$$

We now consider the spectral sequence

$$H^r\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^s\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right)\right) \Longrightarrow H^{r+s}\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right).$$

This gives us the left exact sequence

$$\begin{aligned} 0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right) \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right) \longrightarrow \\ \longrightarrow H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right)\right) \longrightarrow H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right). \end{aligned} \tag{4.7}$$

The idea is to use both the sequences in 4.6 and 4.7 together to simultaneously calculate both $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)$ and $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right)$ for increasing n, and thus allowing us to find $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right)$ for each n.

Our induction process starts here. We know from equations (4.4) and (4.5) that $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(1)}, \frac{\mathcal{G}(1)}{\mathcal{G}(2)}\right) = 0$ and $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(1)}, \frac{\mathcal{G}(2)}{\mathcal{G}(3)}\right) = 0$. Suppose for our induction hypothesis that

$$\begin{aligned} H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}\right) &= 0 \quad \text{and} \\ H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) &= 0, \end{aligned}$$

is true for n. So by the inductive hypothesis $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) = 0$ and we immediately have

$$H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+1)}{\mathcal{G}(n+2)}\right) = 0,$$

from the sequence in 4.6. We now must show that $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right) = 0$. First, we note that $\mathcal{G}(n+2)/\mathcal{G}(n+3) = \mathcal{G}(n)/\mathcal{G}(n+1)$. So from the inductive hypothesis we have $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right) = 0$, and from the sequence in 4.7 we have

$$\begin{aligned} 0 \longrightarrow H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right) \longrightarrow \\ \longrightarrow H^0\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^1\left(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right)\right) \longrightarrow H^2\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right). \end{aligned}$$

This time the second term is $\mathbb{F}_p$ and we find ourselves in the same situation as in Proposition 2.3.9 from the split case. However, the proof we gave of Proposition 2.3.9 goes through from here to show that the map between the second and third terms is an isomorphism, and hence that $H^1\left(\frac{\mathcal{G}(0)}{\mathcal{G}(n+1)}, \frac{\mathcal{G}(n+2)}{\mathcal{G}(n+3)}\right) = 0$. This completes the inductive hypothesis and the proof. □

One final calculation remains; we know that $H^0(\frac{\mathcal{G}(0)}{\mathcal{G}(n)}, H^2(\frac{\mathcal{G}(n)}{\mathcal{G}(n+1)}, \mathbb{F}_p)) = 0$ for all odd n from Proposition 4.3.2. For n even, it suffices to prove the following.

Proposition 4.3.4. *Let p be a rational prime greater than 3. Then*

$$H^0(\mathcal{G}(0)/\mathcal{G}(1), H^2(\mathcal{G}(2)/\mathcal{G}(3), \mathbb{F}_p)) = 0,$$

and furthermore, $H^0(\mathcal{G}(0)/\mathcal{G}(n), H^2(\mathcal{G}(n)/\mathcal{G}(n+1), \mathbb{F}_p)) = 0$ for all even $n > 0$.

Proof. Again we begin by noting that $L \subset \mathfrak{su}(2,1)(\mathbb{F}_p)$ and from Lemma 3.2.4, we already know that

$$(H^2(\mathfrak{su}(2,1)(\mathbb{F}_p), \mathbb{F}_p))^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0.$$

We must then have $(H^2(L, \mathbb{F}_p))^{\mathrm{SO}(2,1)(\mathbb{F}_p)} = 0$ and $(H^2(\mathcal{G}(n)/\mathcal{G}(n+1), \mathbb{F}_p))^{\mathcal{G}(0)/\mathcal{G}(n)} = 0$ for all even $n > 0$, completing the proof. □

Propositions 4.3.2 and 4.3.4 immediately give us the following Corollary.

Corollary 4.3.5. *Let $p \in \mathbb{Z}$ be a rational prime greater than 3 which ramifies in k. Then for all $n > 0$*

$$H^0(\mathcal{G}(0)/\mathcal{G}(n), H^2(\mathcal{G}(n)/\mathcal{G}(n+1), \mathbb{F}_p)) = 0.$$

With the results of this section, we arrive at the following theorem.

Theorem 4.3.6. *Let p and q be rational primes such that p ramifies in k. Then*

(i) $H^1(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_p) = H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_p) = 0$ *for* $p > 3$*, and*

(ii) $H^1(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q) = H^2(\mathcal{G}(\mathbb{Z}_p), \mathbb{F}_q) = 0$ *for* $q > 2$ *and all* $p \neq q$.

Proof. The statements for H^1 follow from Corollary 4.2.2 and Proposition 4.3.1. The first statement for H^2 follows from Propositions 4.2.1, 4.3.3 and Corollary 4.3.5. The second statement for H^2 is Corollary 4.2.2. □

Conclusions

In section 2.2, we took a compact open subgroup $K_f = \prod_p K_p$ of $\mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f)$ and began calculating $H^2(K_f, \mathbb{F}_q)$, as was necessary in order to use Theorem 2.1.10. We began by decomposing the cohomology group as

$$H^r(K_f, \mathbb{Z}/q\mathbb{Z}) = \varinjlim_N H^r\left(\prod_{p<N} K_p, \mathbb{Z}/q\mathbb{Z}\right),$$

and applying the Künneth formula with $r = 2$ gave us

$$H^2\left(\prod_{p<N} K_p, \mathbb{F}_q\right) = \bigoplus_{p<N} H^2(K_p, \mathbb{F}_q) \oplus \bigoplus_{p_1<p_2<N} H^1(K_{p_1}, \mathbb{F}_q) \otimes H^1(K_{p_2}, \mathbb{F}_q).$$

This reduced the problem of finding $H^2(K_f, \mathbb{F}_q)$ to that of finding $H^n(K_p, \mathbb{F}_q)$ for $n = 1, 2$ and for each prime $p \in \mathbb{Z}$. Having done this for $K_p = \mathrm{SU}(2,1)(\mathbb{Z}_p)$ in Theorems 2.3.10, 3.2.7 and 4.3.6, we can collect the results together into the following theorem.

Theorem 4.3.7. *Let* $K_f = \prod_p \mathrm{SU}(2,1)(\mathbb{Z}_p) \subset \mathrm{SU}(2,1)(\mathbb{A}_{\mathbb{Q}}^f)$ *where the product is* *taken over all primes* $p \in \mathbb{Z}$*. Then for all primes* $q > 3$*, we have* $H^2(K_f, \mathbb{F}_q) = 0$*.*

Corollary 4.3.8. *Let* $\mathrm{SU}(2,1)$ *denote a unitary group of the first kind, let* $\Gamma = \mathrm{SU}(2,1)(\mathbb{Z})$ *and* $q > 3$ *be a prime. Suppose there exists a congruence subgroup* $\Gamma' \subset \Gamma$ *such that the restriction map* $H^2(\Gamma, \mathbb{F}_q) \to H^2(\Gamma', \mathbb{F}_q)$ *is not injective. Then the congruence kernel of* $\mathrm{SU}(2,1)$ *is infinite.*

Whilst this condition isn't necessary for the congruence kernel to be infinite, it gives us an alternative approach to proving that the congruence kernel is infinite for the cases when $H^1(\Gamma, \mathbb{C}) = 0$ for all arithmetic groups Γ. This in particular is the case for special unitary groups of the second kind. To demonstrate the relevance of our main theorem (Corollary 4.3.8) to the special unitary groups of the second kind, we first describe how one can construct such a group. To do so, take an imaginary quadratic extension $k/\mathbb{Q}$, a division algebra D of dimension 9 over k such that the center of D is k, and an involution $\iota : D \longrightarrow D$ such that ι restricts to $x \mapsto \bar{x}$ on k. We note that we may construct D as follows; take a degree 3 Galois extension L/k with $\mathrm{Gal}(L/k) = \langle \sigma \rangle$. Choosing an element $r \in L$ such that $r \neq N_{L/k}(d)$ for any $d \in L^\times$, the subset

$$\begin{pmatrix} a & b & c \\ r\sigma(c) & \sigma(a) & \sigma(b) \\ r\sigma^2(b) & r\sigma^2(c) & \sigma^2(a) \end{pmatrix} \subset M_3(L),$$

is a division algebra over k of degree 9 (see Chapter 2, Problems 17-19 of [15]). For a commutative $\mathbb{Q}$-algebra A, the algebraic group is given by

$$\mathrm{SU}_1(D,\iota)(A) = \{g \in \mathrm{SL}_1(D \otimes_{\mathbb{Q}} A) : \iota(g)g = 1\}.$$

If we wish to perform similar calculations for special unitary groups of the second kind as we did in chapters 2,3 and 4, we need to understand $\mathrm{SU}_1(D,\iota)(\mathbb{Q}_p)$, for p a rational prime. We say that $D_p := D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is *ramified* if D_p is the unique division algebra over $\mathbb{Q}_p$, and is *unramified* otherwise. When D_p is unramified, $D_p \cong M_3(\mathbb{Q}_p) \times M_3(\mathbb{Q}_p)$ if p splits in k and $D_p \cong M_3(k_p)$ when p is inert in k. However, D is ramified at p for only finitely many primes p (see Chapter XI, Theorem 1, Page 202 of [33]). It follows that if $\mathcal{G}$ and $\mathcal{G}'$ are special unitary groups of the first and second kind respectively, then for all but the finitely many primes p for which D ramifies,

$$\mathcal{G}(\mathbb{Z}_p) \cong \mathcal{G}'(\mathbb{Z}_p).$$

Thus for all but finitely many p, the cohomology calculations required to invoke our main theorem (Corollary 4.3.8), reduce to the cohomology calculations for groups of the first kind as performed in chapters 2,3 and 4.

We discuss briefly now how one can try to explicitly use Corollary 4.3.8. When a fundamental domain for Γ is known, the cohomology of Γ can be calculated directly from its fundamental domain. In fact when the fundamental domain is noncompact, we can hope to find a Γ-equivariant deformation retraction of the fundamental domain to a smaller space known as a *spine*, from which we can compute the cohomology of Γ (see Section 11, [34]). The spine has the structure of a cell complex and so its cohomology can be found combinatorially. The map $H^2(\Gamma, \mathbb{F}_p) \longrightarrow H^2(\Gamma', \mathbb{F}_p)$ can be viewed by Shapiro's Lemma as a map $H^2(\Gamma, \mathbb{F}_p) \longrightarrow H^2(\Gamma, \mathrm{ind}_{\Gamma'}^{\Gamma}(\mathbb{F}_p))$, where $\mathbb{F}_p \longrightarrow \mathrm{ind}_{\Gamma'}^{\Gamma}(\mathbb{F}_p)$ is given by $1 \mapsto (\gamma \mapsto 1)$. The map $H^2(\Gamma, \mathbb{F}_p) \longrightarrow H^2(\Gamma, \mathrm{ind}_{\Gamma'}^{\Gamma}(\mathbb{F}_p))$ can then be computed from the spine of Γ and will take the form of a sparse matrix over $\mathbb{F}_p$. The question of whether this map is injective can be completed by calculating the rank of this matrix.

There are already concrete descriptions of fundamental domains for some groups of the first kind. An example of a spine for $SU(2,1)_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}$ is described in [34] and a fundamental domain for $PU(2,1)_{\mathbb{Q}(\omega)/\mathbb{Q}}$ where ω is a cube root of unity was found in [10].

Bibliography

[1] H. Bass, M. Lazard, and J-P. Serre. Sous-groupes d'indices finis dans $\mathrm{SL}(n, \mathbb{Z})$. *Bull. Amer. Math. Soc.*, 70:385–392, 1964.

[2] H. Bass, J. Milnor, and J-P. Serre. Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$. *Pub. Math. IHES*, 33:59–137, 1967.

[3] D. Blasius and J. Rogawski. Cohomology of congruence subgroups of $\mathrm{SU}(2, l)^p$ and Hodge cycles on some special complex hyperbolic surfaces. In *Regulators in analysis, geometry and number theory*, volume 171 of *Progress in Mathematics*, pages 1–15. Birkhäuser Boston, Boston, MA, 2000.

[4] A. Borel. *Linear Algebraic Groups*, volume 126 of *Graduate Texts in Mathematics*. Springer Verlag, 1991.

[5] K. Brown. *Cohomology of Groups*, volume 87 of *Graduate Texts in Mathematics*. Springer, 1982.

[6] H. Cartan and S. Eilenberg. *Homological Algebra*. PMS-19. Princeton University Press, 1999.

[7] W. Casselman and D. Wigner. Continuous cohomology and a conjecture of Serre's. *Inventiones Mathematicae*, 25(3):199–211, 1974.

[8] P. Deligne. Extensions centrales non résiduellement finies de groupes arithmétiques. *C.R. Acad. Sci. Paris. Série A*, 287:203 – 208, 1978.

[9] V.V. Deodhar. On central extensions of rational points of algebraic groups. *Americal Journal of Mathematics*, 100(2):303–386, 1978.

[10] E. Falbel and J. Parker. The geometry of the Eisenstein-Picard modular group. *Duke Mathematical Journal*, 131(2):249–289, 2006.

[11] W. Fulton and J. Harris. *Representation Theory: A First Course*, volume 129 of *Graduate Texts in Mathematics*. Springer, 1991.

[12] R. Griess. Schur multipliers of finite simple groups of Lie type. *Trans. Amer. Math. Soc*, 183:355–421, 1973.

[13] R. Hill. Construction of eigenvarieties in small cohomological dimensions for semi-simple, simply connected groups. *Documenta Mathematica*, 12:363–397, 2007.

[14] J. Klose. Kommutatoren und 2-Cohomologie $\mathfrak{p}$-adischer Quaternionenschiefkörper. *Mathematische Zeitschrift*, 191(2):261–282, 1986.

[15] A. Knapp. *Advanced Algebra*, volume 2. Springer, 2007.

[16] A. Knapp and P. Trapa. Representations of semisimple Lie groups. In *Representation Theory of Lie Groups*, volume 8, pages 5–88. IAS/Park City Mathematics, 2000.

[17] T.Y. Lam. *Serre's problem on projective modules.* Springer, 2006.

[18] C. Miller. The second homology group of a group; relations among commutators. *Proceedings of the American Mathematical Society*, 3(4):588–595, 1952.

[19] J. Milnor. *Introduction to Algebraic K-Theory*, volume 72 of *Ann. of Math. Studies.* Princeton Univerity Press, 1972.

[20] C.C. Moore. Extensions and low dimensional cohomology theory of locally compact groups. I. *Trans. Amer. Math. Soc*, 113:40–63, 1964.

[21] D.W. Morris. Introduction to arithmetic groups. *arXiv:math/0106063*, 2001.

[22] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323. Springer, 2008.

[23] O.T. O'Meara. *Introduction to quadratic forms.* Springer Verlag, 1973.

[24] V. Platonov and A. Rapinchuk. *Algebraic Groups and Number Theory.* Academic Press, 1991.

[25] G. Prasad and A. Rapinchuk. Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre. *arXiv:0809.1622*, 2008.

[26] A. Rapinchuk. Congruence subgroup problem for algebraic groups: old and new. *Astérisque*, 209:73–84, 1992.

[27] J. Rosenberg. *Algebraic K-theory and its applications*, volume 147. Springer, 1994.

[28] J-P. Serre. Le problème des groupes de congruence pour SL_2. *Ann. Math.*, 92:489–527, 1970.

[29] J-P Serre. *Galois Cohomology.* Springer Verlag, 2002.

[30] B. Sury. *The Congruence Subgroup Problem. An elementary approach aimed at applications.* Number 24 in Texts and Readings in Mathematics. Hindustan Book Agency, 2003.

[31] C. A. Weibel. *An introduction to homological algebra*, volume 38. Cambridge university press, 1995.

[32] C. A. Weibel. *The K-book: An introduction to algebraic K-theory.* Book-in-progress, available at the author's webpage:. http://www.math.rutgers.edu/weibel/Kbook.html, 2011.

[33] A. Weil. *Basic Number Theory*, volume 144. Springer-Verlag, 1995.

[34] D. Yasaki. Explicit reduction theory for $\mathrm{SU}(2,1;\mathbb{Z}[i])$. *arXiv:math/0601071*, 2006.