An explicit correspondence between certain modular curves

by

Parinaz Salari Sharif

B.Sc., University of Calgary, 2013

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Spring 2017

Approval

Name:	**Parinaz Salari Sharif**
Degree:	**Master of Science (Mathematics)**
Title:	***An explicit correspondence between certain modular curves***
Examining Committee:	**Chair:** Razvan Fetecau Associate Professor

Imin Chen
Senior Supervisor
Associate Professor

Nils Bruin
Supervisor
Professor

Stephen Choi
Internal Examiner
Professor

Date Defended: 3 May 2017

Abstract

In this thesis, we recall an alternative proof of Merel's conjecture, which asserts that a certain explicit correspondence gives the isogeny relation between the Jacobians associated to the normalizer of split and non-split Cartan subgroups. This alternative proof does not require extensive representation theory and can be formulated in terms of certain finite geometries modulo ℓ.

Secondly, we generalize these arguments to exhibit an explicit correspondence which gives the isogeny relation between the Jacobians associated to split and non-split Cartan subgroups. An interesting feature is that the required explicit correspondence is considerably more complicated but can expressed as a certain linear combination of double coset operators whose coefficients we are able to make explicit.

Keywords: Modular curves, explicit correspondences, representation theory, split and non-split Cartan subgroups.

Dedication

To my parents for their unconditional love, support, and sacrifices. My dad who thought me the meaning of generosity and diligence through life. My mom who thought me the meaning of humanity, forgiveness and kindness.

To Dr. Richard Mollin, who encouraged me to pursue my dream in Mathematics. May you rest in peace.

Acknowledgements

I would like to express my deepest gratitude to my senior supervisor Dr. Imin Chen for his extensive support, patience and providing precise editing. I would have never experienced working in my favorite area of Mathematics without your support. I am truly thankful to you for giving me this great opportunity to pursue my childhood dream in Mathematics. I would also like to thank Dr. Nils Bruin for his constructive comments and exceptional guidance through my studies. In addition, I would like to thank Dr. Stephen Choi for reading through my thesis and his valuable feedbacks. I also like to thank my fellow friends in Pure Math and PIMS groups for helping me through my studies and creating a fun space to study at. Lastly and mostly I would like to thank my sister Pooneh, my brothers Pooya and Peyman for always being there for me and their unconditional love.

Table of Contents

List of Figures

Chapter 1

Introduction

Modular curves, which are coarse moduli spaces for elliptic curves with prescribed level structure, appear in the study of Galois torsion structures on elliptic curves.

A well-known example is Mazur's Theorem [5] which states that there are no rational ℓ-isogenies between rational elliptic curves if $\ell > 163$. This result is proven by showing the modular curve $X_0(\ell)$ has no non-cuspidal rational point if $\ell > 163$. Mazur's method is based on descent on the Jacobian of $X_0(\ell)$, but because of the rich arithmetic structure of these curves, the method is more powerful and efficient.

Let ℓ be a prime, and $\mathbb{Z}/\ell\mathbb{Z} = \mathbb{F}_\ell$ be a finite field of cardinality ℓ. For a subgroup H of $\mathrm{GL}_2(\mathbb{F}_\ell)$ which contains -1, it is possible to associate a modular curve X_H. In the case when H is a non-split Cartan subgroup C' or its normalizer N', it is relevant from the point of view of Mazur's method to understand the Jacobian of X_H. In [2], it was proven using the trace formula that $X_{N'}$ and $X_{C'}$ are related by an isogeny over $\mathbb{Q}$ to certain quotients of the Jacobian of the modular curves $X_0(\ell^2)$. Subsequently, [3] gave a proof based on the representation theory of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

In [4], it was conjectured that the above isogeny relation between the Jacobian of $X_{N'}$ and the Jacobian of $X_0(\ell^2)$ was given by a certain explicit correspondence. This was proven in [1] using the representation theory of $\mathrm{GL}_2(\mathbb{F}_\ell)$ and identities in finite double coset algebras.

In this thesis, we recall an alternative proof of Merel's conjecture, which does not require extensive representation theory, based on arguments given by B. Birch and D. Zagier [7]. The proof can be formulated in terms of certain finite geometries over $\mathbb{F}_\ell$ and is largely elementary in its statement and proof, though some algebraic number theory is used.

Secondly, we generalize these arguments to exhibit an explicit correspondence which gives the isogeny relation between the Jacobians associated to split and non-split Cartan subgroups. An interesting feature is that the required explicit correspondence is considerably more complicated but can be expressed as a certain linear combination of double coset operators whose coefficients we are able to make explicit.

The precise statements of the theorems we prove are as follows.

- Let ℓ be an odd prime and ϵ a non-square in $\mathbb{F}_\ell^\times$.
- Let $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.
- Let $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ denote the set of ordered pairs (a, b) of distinct points in $\mathbb{P}^1(\mathbb{F}_\ell)$.
- Let $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim$, where $(a, b) \sim (b, a)$, denote the set of unordered pairs $\{a, b\}$ of distinct points in $\mathbb{P}^1(\mathbb{F}_\ell)$.
- Let $\mathfrak{C}_\ell = \left\{x + y\sqrt{\epsilon} : x \in \mathbb{F}_\ell, y \in \mathbb{F}_\ell^\times\right\}$.
- Let $\mathfrak{H}_\ell = \mathfrak{C}_\ell/\sim$, where $x + y\sqrt{\epsilon} \sim x - y\sqrt{\epsilon}$.

Given an unordered pair $\{a, b\}$ in $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim$, we define in (2.1) a 'geodesic' $\gamma_{\{a,b\}}$ in $\mathfrak{H}_\ell$ between a and b.

Theorem 1.1. *The map*

$$\begin{aligned} \psi^+ : \mathbb{Q}[(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim] &\to \mathbb{Q}[\mathfrak{H}_\ell] \\ \{a, b\} &\mapsto \sum_{x \in \gamma_{\{a,b\}}} x \end{aligned} \tag{1.1}$$

is a surjective $\mathbb{Q}[G]$*-module homomorphism.*

Given an ordered pair (a, b) in $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ and a parameter $s \in \mathbb{F}_\ell^\times$, we define in (3.2) a 'path' $\gamma^s_{(a,b)}$ in $\mathfrak{C}_\ell$ from a to b.

Theorem 1.2. *The map*

$$\begin{aligned} \psi : \mathbb{Q}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta] &\to \mathbb{Q}[\mathfrak{C}_\ell] \\ (a, b) &\mapsto \sum_{s=1}^{\ell-1} (\alpha_s + \beta_s) \sum_{x \in \gamma^s_{(a,b)}} x \end{aligned}$$

is a surjective $\mathbb{Q}[G]$*-module homomorphism, where* $0 \leq \alpha_s, \beta_s \leq \ell - 1$ *are integers satisfying* $\alpha_s \equiv 1 \ (\ell)$ *and* $\beta_s \equiv s^{-1} \ (\ell)$ *for* $s \in \{1, \ldots, \ell - 1\}$.

We explain in Chapter 4 how Theorems 1.1 and 1.2 imply relations between the Jacobians of $X_{N'}$ and $X_{C'}$ and quotients of the Jacobians of the more standard modular curve $X_0(\ell^2)$.

1.1 Terminology and Notation

- ℓ is an odd prime number.
- $\mathbb{F}_\ell$ is a finite field of cardinality ℓ.
- $\mathbb{Z}/\ell\mathbb{Z} = \mathbb{F}_\ell$ is a finite field of cardinality and characteristic ℓ.

- We consider vectors as column vectors with multiplication of matrices on the left (with the consequence that we use the transpose of a row vector in paragraphed text).
- For a ring R with unity, $R^\times$ is its group of units.
- When two sets A and B are in bijection, we denote this by $A \leftrightarrow B$.

1.2 Preliminaries

Let $g \in \mathbb{F}_\ell^\times$ be a primitive root modulo ℓ.

Lemma 1.3. *Let $k \in \mathbb{Z}$, and ℓ be a prime. Then:*

$$\sum_{x=1}^{\ell-1} x^k \equiv \begin{cases} 0 \quad (\ell) & \text{if } k \not\equiv 0 \quad (\ell-1) \\ -1 \quad (\ell) & \text{if } k \equiv 0 \quad (\ell-1) \end{cases}$$

Proof. Let $g^j = x$ for $j = 0, \ldots, \ell-2$, and x goes through values from $1, \ldots, \ell-1$. Then

$$\sum_{x=1}^{\ell-1} x^k = \sum_{j=0}^{\ell-2} g^{jk} = \sum_{j=0}^{\ell-2} (g^k)^j = \frac{(g^k)^{\ell-1} - 1}{g^k - 1} \equiv 0(\ell),$$

by Fermat's Little theorem, unless $g^k \equiv 1(\ell)$. Furthermore, $g^k \equiv 1(\ell)$ if and only if $k \equiv 0(\ell-1)$ because $\operatorname{ord}_\ell g = \ell - 1$. In this case, we have that

$$\sum_{x=1}^{\ell-1} x^k \equiv \sum_{j=0}^{\ell-2} g^{jk} \equiv \sum_{j=0}^{\ell-2} (g^k)^j = \frac{(g^k - 1)((g^k)^{\ell-2} + \ldots + 1)}{g^k - 1} \equiv \ell - 1 \equiv -1 \quad (\ell).$$

□

1.3 Finite Geometry

Let ℓ be an odd prime and $G = \mathrm{GL}_2(\mathbb{F}_\ell)$. In this section, we collect some useful facts about finite geometries, in particular $\mathbb{P}^1(\mathbb{F}_\ell)$ and $\mathbb{P}^1(\mathbb{F}_{\ell^2})$, and relate them to Cartan subgroups of G and their normalizers.

Definition 1.4. *A subgroup C of G is called a split Cartan subgroup of G if it is a conjugate to the group of diagonal matrices,*

$$C = \left\{ \begin{pmatrix} \eta & 0 \\ 0 & \beta \end{pmatrix} : \eta, \beta \in \mathbb{F}_\ell^\times \right\}.$$

From now on, we take C to be equal to the group of diagonal matrices in G. Let $\{1, \eta\}$ be a basis of $\mathbb{F}_{\ell^2}$ over $\mathbb{F}_\ell$. The group $\mathbb{F}_{\ell^2}^\times$ acts on $\mathbb{F}_\ell \times \mathbb{F}_\ell$ with respect to this basis and thus

$\mathbb{F}_{\ell^2}^{\times}$ can be viewed as a subgroup of G, which we denote by C'. In the case $\eta = \sqrt{\epsilon}$, C' is given by

$$C' = \left\{ \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} : (x, y) \neq (0, 0), x, y \in \mathbb{F}_\ell \right\}.$$

Definition 1.5. *A subgroup C' of G is called a non-split Cartan subgroup of G If it is conjugate to the group of matrices in the form of*

$$C' = \left\{ \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} : (x, y) \neq (0, 0), x, y \in \mathbb{F}_\ell \right\}. \tag{1.2}$$

From now on, we take $\eta = \sqrt{\epsilon}$, and C' to be equal to the group of matrices in (1.2). We denote by N the normalizer of C in G, and N' the normalizer of C' in G.

Definition 1.6. *Let K be a field and $\bar{K}$ be an algebraic closure of K. Affine n-space over K is defined as*

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \left\{ (a_1, a_2, ..., a_n) : a_i \in \bar{K} \right\}.$$

Furthermore, we define the set of K-rational points of $\mathbb{A}^n$ as

$$\mathbb{A}^n(K) = \{(a_1, a_2, ..., a_n) \in \mathbb{A}^n : a_i \in K\}.$$

Definition 1.7. *Projective n-space over K is defined as*

$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = \left\{ (a_0, a_1, ..., a_n) : (a_0, a_1, ..., a_n) \in \mathbb{A}^{n+1}(\bar{K}) - \{\underline{0}\} \right\} / \sim,$$

where $(a_0, ..., a_n) \sim (b_0, ..., b_n)$ if and only if there is $\lambda \in \bar{K}^\times$ such that $a_i = \lambda b_i$ for all $i = 0, ..., n$. The relation is an equivalence relation, and we denote equivalence classes by $[a_0 : a_1 : ... : a_n]$. Furthermore, the set of K-rational points of $\mathbb{P}^n$ are defined as

$$\mathbb{P}^n(K) = \{[a_0 : ... : a_n] \in \mathbb{P}^n : a_i \in K\}.$$

Example 1. *The projective line $\mathbb{P}^1(\bar{K})$ can be described as $\left\{ [a : 1] : a \in \bar{K} \right\} \cup \{[1 : 0]\}$. Thus, $\mathbb{P}^1(\bar{K})$ can be thought of as an affine line with an extra point at infinity, i.e. $\mathbb{A}^1(\bar{K}) \cup \{\infty\}$, where we denote $\infty = [1 : 0]$.*

Definition 1.8. *The group action of $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$ via Möbius transformation is defined as*

$$z \mapsto \frac{az + b}{cz + d}, \tag{1.3}$$

where $z \in \mathbb{P}^1(\mathbb{F}_\ell)$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.

Definition 1.9. *The group action of* $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ *on* $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell)$ *is defined as*

$$g(a, b) = (g(a), g(b)),$$

for $(a, b) \in \mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell)$, *and* $g \in G$, *where the action on each copy of* $\mathbb{P}^1(\mathbb{F}_\ell)$ *is as in* (1.3).

Definition 1.10. *The group action of* $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ *on* $\mathfrak{C}_\ell$ *via Möbius transformation is defined as*

$$z \mapsto \frac{az+b}{cz+d},$$

where $z = x + y\sqrt{\epsilon} \in \mathfrak{C}_\ell$, *and* $g \in G$.

Given an element $z \in \mathbb{P}^1(\mathbb{F}_{\ell^2}) - \{\infty\}$, we will often write it as $z = x + y\sqrt{\epsilon}$.

Definition 1.11. *A group action is n-transitive if for every two sets* $\{x_1, x_2, \cdots, x_n\}$ *and* $\{y_1, y_2, \cdots, y_n\}$ *of distinct elements of* G, *there is a* $g \in G$ *such that* $gx_i = y_i$ *for* $1 \leq i \leq n$.

Lemma 1.12. *The group* $\mathrm{GL}_2(\mathbb{F}_\ell)$ *acts 3-transitively on the projective line* $\mathbb{P}^1(\mathbb{F}_\ell)$.

Proof. Let $\{x_1, x_2, x_3\}$ and $\{y_1, y_2, y_3\}$ be two sets of distinct elements of $\mathbb{P}^1(\mathbb{F}_\ell)$. It suffices to show that any three distinct elements of $\mathbb{P}^1(\mathbb{F}_\ell)$ can be mapped to $(0,1), (1,0), (1,1) \in \mathbb{P}^1(\mathbb{F}_\ell)$ by an element of G, respectively. Let $f(x) = \frac{(x-x_1)(x_2-x_3)}{(x-x_3)(x_2-x_1)} \in G$, f maps x_1, x_2, x_3 to points $(0,1), (1,1), (1,0)$ respectively, and $g(y) = \frac{(y-y_1)(y_2-y_3)}{(y-y_3)(y_2-y_1)} \in G$ maps y_1, y_2, y_3 to points $(0,1), (1,1), (1,0)$, respectively. Then the composition $g^{-1} \circ f$ maps x_1, x_2, x_3 to y_1, y_2, y_3 respectively, i.e,

$$\begin{aligned} g^{-1} \circ f(x_1) &= y_1, \\ g^{-1} \circ f(x_2) &= y_2, \\ g^{-1} \circ f(x_3) &= y_3, \end{aligned}$$

which proves 3-transitivity of group action $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$. □

Lemma 1.13. *The group* $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ *acts transitively on* $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ *and* $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim$.

Proof. Any point in $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ is of the form $(a, 1), (a, 0), (a, b)$ for $a, b \in \mathbb{F}_\ell$ and $a \neq b$. Then the following elements in G send $(1, 0)$ to each point of these forms,

$$\begin{pmatrix} a & 0 \\ 1 & 1 \end{pmatrix} (1, 0)^\top = (a, 1)^\top,$$

$$\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix} (1, 0)^\top = (a, 0)^\top,$$

$$\begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix} (1, 0)^\top = (a, b)^\top,$$

which proves the transitivity of this group action. The result for unordered pairs in $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim$ follows. □

Lemma 1.14. *The group $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ acts transitively on $\mathfrak{C}_\ell$ and $\mathfrak{H}_\ell$.*

Proof. Any point in $\mathfrak{C}_\ell$ is of the form $z = x + \sqrt{\epsilon}y$ for $x \in \mathbb{F}_\ell, y \in \mathbb{F}_\ell^\times$. Then the following element in G sends $\begin{pmatrix} \sqrt{\epsilon} \\ 1 \end{pmatrix}$ to point of this type:

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{\epsilon} \\ 1 \end{pmatrix} = \begin{pmatrix} x + \sqrt{\epsilon}y \\ 1 \end{pmatrix},$$

which proves the transitivity of this group action. It thus also follows for points in $\mathfrak{H}_\ell$.

□

Lemma 1.15. *The set of stabilizers of an unordered pair $\{0, \infty\}$ in G is given by*

$$N = Stab_G(\{0, \infty\}) = \left\{ \begin{pmatrix} \star & 0 \\ 0 & \star \end{pmatrix}, \begin{pmatrix} 0 & \star \\ \star & 0 \end{pmatrix} \right\}.$$

Proof. Suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ stabilizes $\{0, \infty\}$, i.e. $g\{0, \infty\} = \{0, \infty\}$. Then we have two cases:

- either g sends 0 to 0 and ∞ to ∞ which means $\begin{cases} g(0) = \frac{a0+b}{c0+d} = 0 \Rightarrow b \equiv 0 \ (\ell), d \not\equiv 0 \ (\ell), \\ g(\infty) = \frac{a\infty+b}{c\infty+d} = \infty \Rightarrow c \equiv 0 \ (\ell), a \not\equiv 0 \ (\ell). \end{cases}$

  This implies that g is either the matrix $\begin{pmatrix} \star & 0 \\ 0 & \star \end{pmatrix}$ where a, d are arbitrary non-zero elements of $\mathbb{F}_\ell$ with $ad \not\equiv 0 \ (\ell)$ in this case.

- or g sends 0 to ∞ and ∞ to 0 which means $\begin{cases} g(0) = \frac{a0+b}{c0+d} = \infty \Rightarrow d \equiv 0 \ (\ell), b \not\equiv 0 \ (\ell), \\ g(\infty) = \frac{a\infty+b}{c\infty+d} = 0 \Rightarrow a \equiv 0 \ (\ell), c \not\equiv 0 \ (\ell). \end{cases}$

This implies that g is the matrix $\begin{pmatrix} 0 & \star \\ \star & 0 \end{pmatrix}$ where b, c are arbitrary non-zero elements of $\mathbb{F}_\ell$ with $bc \not\equiv 0 \ (\ell)$.

□

Corollary 1.16. *The group N above is the normalizer of C in G.*

Proof. An element in G normalizes C if and only if the element stabilizes the set $\{0, \infty\}$. □

Lemma 1.17. *The set of stabilizers of an unordered pair $\{\sqrt{\epsilon}, -\sqrt{\epsilon}\}$ in G is given by*

$$N' = Stab_G(\{\sqrt{\epsilon}, -\sqrt{\epsilon}\}) = \left\{ \begin{pmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & -\epsilon\beta \\ \beta & -\alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_\ell, (\alpha, \beta) \neq (0,0) \right\}.$$

Proof. Suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ stabilizes $\{\sqrt{\epsilon}, -\sqrt{\epsilon}\}$, i.e. $g\{\sqrt{\epsilon}, -\sqrt{\epsilon}\} = \{\sqrt{\epsilon}, -\sqrt{\epsilon}\}$. Then we have two cases:

- either g sends $\sqrt{\epsilon}$ to $\sqrt{\epsilon}$ and $-\sqrt{\epsilon}$ to $-\sqrt{\epsilon}$ which means
$$\begin{cases} g(\sqrt{\epsilon}) = \frac{a\sqrt{\epsilon}+b}{c\sqrt{\epsilon}+d} = \sqrt{\epsilon} \Rightarrow a\sqrt{\epsilon}+b = \sqrt{\epsilon}(c\sqrt{\epsilon}+d) \Rightarrow a \equiv d \equiv \alpha \ (\ell), \text{if}\, c \equiv \beta, b \equiv \epsilon\beta \ (\ell), \\ g(-\sqrt{\epsilon}) = \frac{-a\sqrt{\epsilon}+b}{-c\sqrt{\epsilon}+d} = -\sqrt{\epsilon} \Rightarrow -a\sqrt{\epsilon}+b = -\sqrt{\epsilon}(-c\sqrt{\epsilon}+d) \Rightarrow a \equiv d \equiv \alpha \ (\ell), \text{if}\, c \equiv \beta, b \equiv \epsilon\beta \ (\ell). \end{cases}$$
This implies that g is the matrix $\begin{pmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{pmatrix}$ where α, β are not both zero in $\mathbb{F}_\ell$ with $\alpha^2 - \epsilon\beta^2 \not\equiv 0 \ (\ell)$ in this case.
- or g sends $\sqrt{\epsilon}$ to $-\sqrt{\epsilon}$ and $-\sqrt{\epsilon}$ to $\sqrt{\epsilon}$ which means
$$\begin{cases} g(\sqrt{\epsilon}) = \frac{a\sqrt{\epsilon}+b}{c\sqrt{\epsilon}+d} = -\sqrt{\epsilon} \Rightarrow a\sqrt{\epsilon}+b = -\sqrt{\epsilon}(c\sqrt{\epsilon}+d) \Rightarrow a \equiv -d \equiv \alpha \ (\ell), \text{if}\, c \equiv \beta, b \equiv -\epsilon\beta \ (\ell), \\ g(-\sqrt{\epsilon}) = \frac{-a\sqrt{\epsilon}+b}{-c\sqrt{\epsilon}+d} = \sqrt{\epsilon} \Rightarrow -a\sqrt{\epsilon}+b = \sqrt{\epsilon}(-c\sqrt{\epsilon}+d) \Rightarrow a \equiv -d \equiv \alpha \ (\ell), \text{if}\, c \equiv \beta, b \equiv -\epsilon\beta \ (\ell). \end{cases}$$
This implies that g is the matrix $\begin{pmatrix} \alpha & -\epsilon\beta \\ \beta & -\alpha \end{pmatrix}$ where α, β are not both zero in $\mathbb{F}_\ell$ with $-\alpha^2 + \epsilon\beta^2 \not\equiv 0 \ (\ell)$.

□

Corollary 1.18. *The group N' above is the normalizer of C' in G.*

Proof. An element in G normalizes C' if and only if the element stabilizes the set $\{\sqrt{\epsilon}, -\sqrt{\epsilon}\}$.

□

Lemma 1.19. *The set of stabilizers of an ordered pair $(0, \infty)$ in G is given by*

$$C = Stab_G((0, \infty)) = \left\{ \begin{pmatrix} \star & 0 \\ 0 & \star \end{pmatrix} \right\}.$$

Proof. Suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ stabilizes $(0, \infty)$, i.e. $g(0, \infty) = (0, \infty)$. Then g sends 0 to 0 and ∞ to ∞ which means $\begin{cases} g(0) = \frac{a0+b}{c0+d} = 0 \Rightarrow b \equiv 0\ (\ell), d \not\equiv 0\ (\ell), \\ g(\infty) = \frac{a\infty+b}{c\infty+d} = \infty \Rightarrow c \equiv 0\ (\ell), a \not\equiv 0\ (\ell). \end{cases}$

This implies that g is the matrix $\begin{pmatrix} \star & 0 \\ 0 & \star \end{pmatrix}$ where a, d are arbitrary non-zero elements of $\mathbb{F}_\ell$ with $ad \not\equiv 0\ (\ell)$. □

Lemma 1.20. *The set of stabilizers of the ordered pair* $(\sqrt{\epsilon}, -\sqrt{\epsilon})$ *in* G *is given by*

$$C' = Stab_G((\sqrt{\epsilon}, -\sqrt{\epsilon})) = \left\{ \begin{pmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_\ell, (\alpha, \beta) \neq (0, 0) \right\}.$$

Proof. Suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ stabilizes $(\sqrt{\epsilon}, -\sqrt{\epsilon})$, i.e. $g(\sqrt{\epsilon}, -\sqrt{\epsilon}) = (\sqrt{\epsilon}, -\sqrt{\epsilon})$. Then g sends $\sqrt{\epsilon}$ to $\sqrt{\epsilon}$ and $-\sqrt{\epsilon}$ to $-\sqrt{\epsilon}$ which means

$$\begin{cases} g(\sqrt{\epsilon}) = \frac{a\sqrt{\epsilon}+b}{c\sqrt{\epsilon}+d} = \sqrt{\epsilon} \Rightarrow a\sqrt{\epsilon} + b = \sqrt{\epsilon}(c\sqrt{\epsilon} + d) \Rightarrow a \equiv d \equiv \alpha\ (\ell), \text{if}\, c \equiv \beta, b \equiv \epsilon\beta\ (\ell), \\ g(-\sqrt{\epsilon}) = \frac{-a\sqrt{\epsilon}+b}{-c\sqrt{\epsilon}+d} = -\sqrt{\epsilon} \Rightarrow -a\sqrt{\epsilon} + b = -\sqrt{\epsilon}(-c\sqrt{\epsilon} + d) \Rightarrow a \equiv d \equiv \alpha\ (\ell), \text{if}\, c \equiv \beta\ (\ell), b \equiv \epsilon\beta\ (\ell). \end{cases}$$

This implies that g is the matrix $\begin{pmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{pmatrix}$ where α, β are not both zero in $\mathbb{F}_\ell$ with $\alpha^2 - \epsilon\beta^2 \not\equiv 0\ (\ell)$. □

Lemma 1.21. *The coset space* G/C *is in bijection with ordered pairs of distinct points* (a, b) *of* $\mathbb{P}^1(\mathbb{F}_\ell)$*, that is,* $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$.

Proof. From Lemma 1.13, we know that G acts transitively on $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$. Then,

$$G/\text{Stab}(x) \leftrightarrow \text{Orbit}(x).$$

Since the group action above is transitive, $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ has only one orbit which is itself. Furthermore, let $x = (0, \infty)$, then the stabilizer of x is the set of all diagonal matrices over $\mathbb{F}_\ell^\times$ by Lemma 1.19, which coincides with the split Cartan subgroup C in Definition 1.4. Therefore, there is a bijection between G/C and $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$. □

Lemma 1.22. *The coset space* G/N *is in bijection with unordered pairs of distinct points* $\{a, b\}$ *of* $\mathbb{P}^1(\mathbb{F}_\ell)$*, that is,* $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim$*, where* $(a, b) \sim (b, a)$.

Proof. From Lemma 1.13 , we know that G acts transitively on $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim$. Then,

$$G/\text{Stab}(x) \leftrightarrow \text{Orbit}(x).$$

Since the group action above is transitive, $(\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)-\Delta)/\sim$ has only one orbit which is itself. Furthermore, let $x=\{0,\infty\}$, then the stabilizer of x is the set $\operatorname{Stab}\{0,\infty\}=\left\{\begin{pmatrix}\star & 0\\ 0 & \star\end{pmatrix},\begin{pmatrix}0 & \star\\ \star & 0\end{pmatrix}\right\}$ by Lemma 1.15, which is the normalizer of the split Cartan subgroup C that is denoted by N. Therefore, there is a bijection between G/N and $(\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)-\Delta)/\sim$. □

Lemma 1.23. *The coset space G/C' is in bijection with points $z\in\mathfrak{C}_\ell=\mathbb{P}^1(\mathbb{F}_{\ell^2})-\mathbb{P}^1(\mathbb{F}_\ell)$.*

Proof. From Lemma 1.14, we know that G acts transitively on $\mathfrak{C}_\ell$. Then,

$$G/\operatorname{Stab}(x)\leftrightarrow\operatorname{Orbit}(x),$$

by transitivity of the above group action. This implies that $\mathfrak{C}_\ell$ has only one orbit that is itself. Furthermore, let $x=(\sqrt{\epsilon},-\sqrt{\epsilon})$, then the set of stabilizers of x is the set

$$\left\{\begin{pmatrix}\alpha & \epsilon\beta\\ \beta & \alpha\end{pmatrix}:\alpha,\beta\in\mathbb{F}_\ell\right\}$$

by Lemma 1.20, which coincides with the non-split Cartan subgroup C' in Definition 1.5. Therefore, there is a bijection between G/C' and $\mathfrak{C}_\ell=\mathbb{P}^1(\mathbb{F}_{\ell^2})-\mathbb{P}^1(\mathbb{F}_\ell)$. □

Lemma 1.24. *The coset space G/N' is in bijection with unordered pairs of conjugate points $\{z,\bar{z}\}$ of $\mathfrak{C}_\ell$, that is, $\mathfrak{H}_\ell=\mathfrak{C}_\ell/\sim$, where $\bar{z}\sim z$.*

Proof. From Lemma 1.14, we know that G acts transitively on $\mathfrak{H}_\ell$. Then,

$$G/\operatorname{Stab}(x)\leftrightarrow\operatorname{Orbit}(x).$$

Since the group action above is transitive, $\mathfrak{H}_\ell$ has only one orbit which is itself. Furthermore, let $x=\{\sqrt{\epsilon},-\sqrt{\epsilon}\}$, then the stabilizer of x is

$$\operatorname{Stab}\{\sqrt{\epsilon},-\sqrt{\epsilon}\}=\left\{\begin{pmatrix}\alpha & \epsilon\beta\\ \beta & \alpha\end{pmatrix},\begin{pmatrix}\alpha & -\epsilon\beta\\ \beta & -\alpha\end{pmatrix}:\alpha,\beta\in\mathbb{F}_\ell\right\}$$

by Lemma 1.17, which is the normalizer of non-split Cartan subgroup C' denoted by N'. Therefore, there is a bijection between G/N' and $\mathfrak{H}_\ell=\mathfrak{C}_\ell/\sim$. □

1.4 Double coset operators

We begin this section with a definition of a group ring.

Definition 1.25. *Let G be a finite group with identity element $e\neq 0$, and R be a commutative ring with identity element $1\neq 0$. The group ring, $R[G]$, of G with coefficients in R is the set* *of all formal sums*

$$a_1g_1 + a_2g_2 + \cdots + a_ng_n \qquad a_i \in R, 1 \leq i \leq n.$$

If g_1 is the identity of G we shall write a_1g_1 simply as a_1. Similarly, we shall write the element $1g$ for $g \in G$ simply as g.

Addition is defined componentwise as

$$(a_1g_1 + a_2g_2 + \cdots + a_ng_n) + (b_1g_1 + b_2g_2 + \cdots + b_ng_n)$$
$$= (a_1 + b_1)g_1 + (a_2 + b_2)g_2 + \cdots + (a_n + b_n)g_n.$$

Multiplication is performed by first defining $(ag_i)(bg_j) = (ab)g_k$, where the product ab is taken in R and $g_ig_j = g_k$ is the product in the group G. This product is then extended to all formal sums by the distributive laws so that the coefficients of g_k in the product $(a_1g_1 + \cdots + a_ng_n) \times (b_1g_1 + \cdots + b_ng_n)$ is $\sum_{g_ig_j=g_k} a_ib_j$. It is straightforward to check that these operations make $R[G]$ into a ring. The associativity of multiplication follows from the associativity of the group operation in G. The ring $R[G]$ is commutative if and only if G is a commutative group.

Definition 1.26. *Let M be an additively written abelian group and let $R[G]$ be a group ring. Suppose that for each $m \in M$ and $r \in R[G]$, there is defined an element of M denoted by rm. Then M is a $R[G]$-module if the following conditions hold:*

- *$(r)(a + b) = ra + rb$ for all $a, b \in M$ and $r \in R[G]$.*
- *$(r + s)a = ra + sa$ for all $r, s \in R[G]$ and $a \in M$.*
- *$(rs)a = r(sa)$ for all $a \in M$ and $r, s \in R[G]$.*
- *$1a = a$ for all $a \in M$ where 1 is identity element of $R[G]$.*

Lemma 1.27. *Let H be a subgroup of a group G. Then the free R-module generated by G/H, which we denote by $R[G/H]$ is a $R[G]$-module.*

Proof. The $R[G]$-module structure is induced by multiplication on the left by elements of G. □

Lemma 1.28. *$\mathbb{Z}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta]$ is a $\mathbb{Z}[G]$-module.*

Proof. $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ is in bijection with G/C by Lemma 1.14. Furthermore, $\mathbb{Z}[G/C]$ is a $\mathbb{Z}[G]$-module homomorphism by action of G on G/C on the left by multiplication, therefore $\mathbb{Z}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta]$ is also a $\mathbb{Z}[G]$-module. □

Lemma 1.29. *$\mathbb{Z}[(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim]$ is a $\mathbb{Z}[G]$-module.*

Proof. $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim$ is in bijection with G/N by Lemma 1.22. Furthermore, $\mathbb{Z}[G/N]$ is a $\mathbb{Z}[G]$-module homomorphism by action of G on G/N on the left by multiplication, therefore $\mathbb{Z}[(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta)/\sim]$ is also a $\mathbb{Z}[G]$-module. □

Lemma 1.30. $\mathbb{Z}[\mathfrak{H}_\ell]$ *is a* $\mathbb{Z}[G]$*-module.*

Proof. $\mathfrak{H}_\ell$ is in bijection with G/C' by Lemma 1.23. Furthermore, $\mathbb{Z}[G/C']$ is a $\mathbb{Z}[G]$-module homomorphism by action of G on G/C' on the left by multiplication, therefore $\mathbb{Z}[\mathfrak{H}_\ell]$ is also a $\mathbb{Z}[G]$-module. □

Lemma 1.31. $\mathbb{Z}[\mathfrak{C}_\ell]$ *is a* $\mathbb{Z}[G]$*-module.*

Proof. $\mathfrak{C}_\ell$ is in bijection with G/N' by Lemma 1.24. Furthermore, $\mathbb{Z}[G/N']$ is a $\mathbb{Z}[G]$-module homomorphism by action of G on G/N' on the left by multiplication, therefore $\mathbb{Z}[\mathfrak{C}_\ell]$ is also a $\mathbb{Z}[G]$-module. □

Definition 1.32. *Let M and N be $R[G]$-modules, then a map $\theta : M \mapsto N$ is called an $R[G]$-module homomorphism (or intertwining operator) if for any $a, b \in M, r, s \in R[G]$ we have:*

- $\theta(a + b) = \theta(a) + \theta(b),$
- $\theta(ra) = r\theta(a).$

The set of all $R[G]$-module homomorphisms from M to N is denoted by $Hom_{R[G]}(M, N)$. $Hom_{R[G]}(M, N)$ is an abelian group and an $R[G]$-module, since for all $r, s \in R[G], a \in M$ and $\theta, \eta \in \mathrm{Hom}_{R[G]}(M, N)$, we have $(r)(\theta + \eta)(a) = r\theta(a) + r\eta(a)$, and $(rs)(\theta)(a) = (rs)(\theta(a)) = r(s\theta(a)) = r(\theta(sa)) = \theta(rsa)$.

Definition 1.33. *Let G be a group, H and K be subgroups of G. For each $g \in G$, the double coset HgK of $g \in G$ is defined to be the set*

$$HgK = \{hgk | h \in H, k \in K\}.$$

Here we have two lemmas regarding double cosets which are:

Lemma 1.34. *Let G be a group, H and K be subgroups of G, then*

$$HgK = \bigcup_{\alpha \in H/H_g} \alpha g K,$$

where $H_g = H \cap gKg^{-1}$ and the union is disjoint. We call $[H : H_g]$ the degree of HgK. This is independent of the choice of g in the sense that $deg(HgK) = deg(Hg'K)$ if $HgK = Hg'K$.

Proof. H can be partitioned by its left H_g cosets, i.e,

$$H = \bigcup_{\alpha \in H/H_g} \alpha H_g,$$

furthermore, by Definition 1.33 we know $HgK = \{hgk : h \in H, k \in K\}$, which leads to

$$\begin{aligned} HgK = \bigcup_{\alpha \in H/H_g} \alpha H_g gK = \bigcup_{\alpha \in H/H_g} \alpha(H \cap gKg^{-1})gK = \\ \bigcup_{\alpha \in H/H_g} \alpha(HgK \cap gKg^{-1}gK) = \bigcup_{\alpha \in H/H_g} \alpha(HgK \cap gK) = \\ \bigcup_{\alpha \in H/Hg} \alpha gK, \text{ since } gK \subseteq HgK. \end{aligned}$$

If $\alpha gK = \alpha' gK$, then $\alpha g \in \alpha' gK$ which implies $\alpha \in \alpha' H_g$, therefore $\alpha = \alpha'$ since $\alpha \in H/H_g$ are distinct, which proves that the union is disjoint.

To prove the degree is independent of the choice of g, suppose $g' = hgk$ for some $h \in H, k \in K$. Then

$$\begin{aligned} H_{g'} &= H \cap g'Kg'^{-1} \\ &= H \cap hgkKk^{-1}g^{-1}h^{-1} \\ &= H \cap hgKg^{-1}h^{-1}. \end{aligned}$$

Therefore,

$$h^{-1}H_{g'}h = H_g,$$

yielding the desired result that $[H : H_g] = [H : H_{g'}]$. □

Definition 1.35. *Given a double coset HgK and a decomposition into disjoint cosets*

$$HgK = \bigcup_{\alpha \in \Omega} \alpha gK,$$

we obtain a $\mathbb{Z}[G]$-module homomorphism given by

$$\begin{aligned} (HgK)^* : \mathbb{Z}[G/H] &\to \mathbb{Z}[G/K] \\ xH &\mapsto \sum_{\alpha \in \Omega} x\alpha gK. \end{aligned} \tag{1.4}$$

The $\mathbb{Z}[G]$-module homomorphism from $\mathbb{Z}[G/H]$ to $\mathbb{Z}[G/K]$ is called a double coset operator.

In this setting of finite groups, the following lemma shows that the double coset operators exhaust all $\mathbb{Z}[G]$-module homomorphisms from $\mathbb{Z}[G/H]$ to $\mathbb{Z}[G/K]$.

Lemma 1.36. *Let H and K be subgroups of a group G. Then as $\mathbb{Z}$-modules, there is a canonical isomorphism*

$$\Theta : \mathbb{Z}[H\backslash G/K] \cong Hom_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \mathbb{Z}[G/K]).$$

Proof. Let Ω be a complete set of inequivalent representatives for $H\backslash G/K$ and put $\Theta(HgK) = (HgK)^*$ as in (1.4). It is clear that Θ is injective since $\Theta(\Sigma_{g\in\Omega}\alpha_g HgK) = 0$ means that $\Sigma_{g\in\Omega}\alpha_g HgK = 0$ as an element of $\mathbb{Z}[G/K]$. This occurs if and only if $\alpha_g = 0$ for all $g \in \Omega$.

A $\mathbb{Z}[G]$-module homomorphism $\Theta : \mathbb{Z}[G/H] \to \mathbb{Z}[G/K]$ is determined by its value on the coset H. Since $\Theta(H)$ is an element in $\mathbb{Z}[G/K]$ which is invariant under multiplication on the left by elements in H, we can write $\Theta(H) = \Sigma_{g\in\Omega}\alpha_g HgK$. We then see that $\Omega(H) = \Sigma_{g\in\Omega}\alpha_g\Theta(HgK)$. This shows Θ is surjective. □

Lemma 1.37. *The double coset operator $NN' : \mathbb{Z}[G/N] \to \mathbb{Z}[G/N']$ coincides with the map $\psi^+ : \mathbb{Z}[(\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)-\Delta)/\sim] \to \mathbb{Z}[\mathfrak{H}_\ell]$ in* (1.1) *and is hence a $\mathbb{Z}[G]$-module homomorphism.*

Proof. Since

$$N \cap N' = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \pm\alpha \end{pmatrix} : \alpha \in \mathbb{F}_\ell^\times \right\} \cup \left\{ \begin{pmatrix} 0 & \pm\epsilon\alpha \\ \alpha & 0 \end{pmatrix} : \alpha \in \mathbb{F}_\ell^\times \right\},$$

we have from Lemma 1.34 that

$$NN' = \cup_{\alpha\in\mathbb{F}_\ell^\times/\{\pm1\}} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} N'.$$

The $\mathbb{Z}[G]$-module homomorphism from $\mathbb{Z}[G/N] \to \mathbb{Z}[G/N']$ induced by NN' from Lemma 1.36 is then seen to be the map ψ^+. □

Lemma 1.38. *The double coset operator $C\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}C' : \mathbb{Z}[G/C] \to \mathbb{Z}[G/C']$ coincides with the map $H_s : \mathbb{Z}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta] \to \mathbb{Z}[\mathfrak{C}_\ell]$ in* (3.1) *and is hence a $\mathbb{Z}[G]$-module homomorphism.*

Proof. For $g = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$, we have that

$$C \cap gC'g^{-1} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} : \alpha \in \mathbb{F}_\ell^\times \right\}.$$

Thus, from Lemma 1.34, we have that

$$C\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}C' = \cup_{\alpha\in\mathbb{F}_\ell^\times} \begin{pmatrix} \alpha & \alpha s \\ 0 & 1 \end{pmatrix} C'.$$

The $\mathbb{Z}[G]$-module homomorphism from $\mathbb{Z}[G/C] \to \mathbb{Z}[G/C']$ induced by CC' from Lemma 1.36 is then seen to be the map H_s. $\square$

Chapter 2

Normalizer of Cartan subgroup case

In this Chapter, we explain and give a detailed proof of Merel's conjecture for normalizers of Cartan subgroups using methods in [7]. In this situation, the conjectural explicit intertwining operator is given by a single double coset operator.

Define $\gamma_{\{0,\infty\}} := \mathbb{F}_\ell^\times \sqrt{\epsilon} \subseteq \mathfrak{H}_\ell$, which can be thought of as the geodesic in $\mathfrak{H}_\ell$ between 0 and ∞. Given an unordered pair $\{a, b\}$, there is a $g \in G$ such that $\{a, b\} = \{g(0), g(\infty)\}$, which is unique up to multiplication on the left by N. Thus, we may define

$$\gamma_{\{a,b\}} := g(\gamma_{\{0,\infty\}}), \tag{2.1}$$

which can be thought of as the geodesic in $\mathfrak{H}_\ell$ between a and b.

Lemma 2.1. *A choice for the element g above is given by*

$$\begin{pmatrix} b & a \\ 1 & 1 \end{pmatrix}.$$

Proof. The point at infinity ∞ is denoted by $(1, 0)^\top$ and the point 0 by $(0, 1)^\top$. We require a matrix g such that $g \cdot 0 = (a, 1)^\top$ and $g \cdot \infty = (b, 1)^\top$, which is given by the above matrix. □

We can write the coordinate independent description of that geodesic over $\mathbb{F}_\ell$ using norms which would be $N_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell}(\zeta - \frac{(a+b)}{2}) = r^2$. Furthermore, by definition of norm we have:

$$N_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell}(x + y\sqrt{\epsilon}) = (x + y\sqrt{\epsilon})(x - y\sqrt{\epsilon}) = x^2 - \epsilon y^2,$$

therefore, the equation of that geodesic can be rewritten as:

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon y^2 = \left(\frac{b-a}{2}\right)^2,$$

which is a conic section (see Figure 2.1).

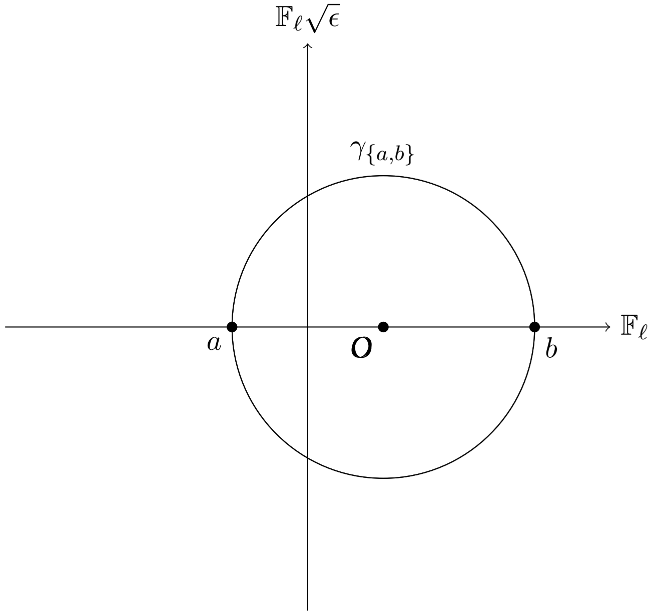

Figure 2.1: Geodesic $\gamma_{\{a,b\}}$ in $\mathfrak{H}_\ell$

The finite field $\mathbb{F}_{\ell^2}$ is a vector space over $\mathbb{F}_\ell$ of dimension 2. The basis $\{1, \sqrt{\epsilon}\}$ gives us an identification $\mathbb{F}_{\ell^2} \cong \mathbb{F}_\ell + \sqrt{\epsilon}\mathbb{F}_\ell$. Thus, for every $z \in \mathbb{F}_{\ell^2}$, we can write $z = x + \sqrt{\epsilon}y$ for some $x, y \in \mathbb{F}_\ell$.

Lemma 2.2. *The quadratic equation*

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon y^2 = \left(\frac{b-a}{2}\right)^2. \tag{2.2}$$

gives the geodesic $\gamma_{\{a,b\}}$ with coordinates(see Figure 2.1)

$$x = \frac{a - \epsilon\lambda^2 b}{1 - \epsilon\lambda^2},$$
$$y = \lambda(\frac{a-b}{1-\epsilon\lambda^2}).$$

.

Proof. Let write $g(\lambda\sqrt{\epsilon},1)^\top$ as a fraction, and rationalize it:

$$\begin{aligned}
&\frac{b\lambda\sqrt{\epsilon}+a}{\lambda\sqrt{\epsilon}+1}\\
=&\frac{b\lambda\sqrt{\epsilon}+a}{\lambda\sqrt{\epsilon}+1}.\frac{\lambda\sqrt{\epsilon}-1}{\lambda\sqrt{\epsilon}-1}\\
=&\frac{b\lambda^2\epsilon+a\lambda\sqrt{\epsilon}-b\lambda\sqrt{\epsilon}-a}{\epsilon\lambda^2-1}\\
=&\frac{b\lambda^2\epsilon-a}{\epsilon\lambda^2-1}+\sqrt{\epsilon}\frac{\lambda(a-b)}{\epsilon\lambda^2-1}\\
=&\frac{a-b\lambda^2\epsilon}{1-\epsilon\lambda^2}+\sqrt{\epsilon}\frac{\lambda(b-a)}{1-\epsilon\lambda^2}.
\end{aligned}$$

Therefore, as $\gamma_{\{a,b\}} \in \mathbb{F}_\ell^\times$ we conclude x, y from the above expression are given by (see Figure 2.1)

$$\begin{aligned}
x &= \frac{a-\epsilon\lambda^2 b}{1-\epsilon\lambda^2},\\
y &= \lambda(\frac{a-b}{1-\epsilon\lambda^2}).
\end{aligned}$$

. Using Maple, we can derive and verify that x, y satisfy 2.2. □

2.1 Coordinates for G/N and G/N'

We need a more convenient coordinate to represent elements in (a certain subset of) $(\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)-\Delta)/\sim$ and $\mathfrak{H}_\ell$, where $(\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)-\Delta)/\sim$ is in bijection with G/N, and $\mathfrak{H}_\ell$ is in bijection with G/N'.

Lemma 2.3. *Let $A = (\mathbb{F}_\ell \times \mathbb{F}_\ell - \Delta)/\sim$ and $B = \big\{(t,n) : t^2 - 4n \neq 0$ is a square in $\mathbb{F}_\ell\big\}$. Then there is a bijection between the sets A and B given by*

$$\{a,b\} \mapsto (a+b, ab).$$

Proof. Let $\kappa : A \to B$ be the map such that κ sends each unordered pair $\{a,b\}$ to (t,n). Here, we need to show that this map is surjective and injective.

Let $\{a,b\}$ and $\{c,d\}$ be two distinct elements of A such that $\kappa(\{a,b\}) = \kappa(\{c,d\})$. Then, $(a+b, ab) = (c+d, cd)$ which implies that $(x-a)(x-b) = (x-c)(x-d)$. Furthermore, unique factorization of polynomial ring $\mathbb{F}_\ell[x]$ implies that either $a = c, b = d$ or $a = d, b = c$. Therefore $\{a,b\} = \{c,d\}$, which is a contradiction. Thus, κ is an injective map.

Let $(t_1, n_1) \in B = \{x^2 - t_1 x + n_1, t_1^2 - 4n_1$ is a square in $\mathbb{F}_\ell\}$. This equation has two solutions $\frac{t_1+m}{2}$ and $\frac{t_1-m}{2}$ in $\mathbb{F}_\ell$, since $\Delta = t_1^2 - 4n_1 = m^2$ is a square in $\mathbb{F}_\ell$. Then, there exist $c, d \in \mathbb{F}_\ell$ such that $\frac{t_1+m}{2} = c$ and $\frac{t_1-m}{2} = d$. Therefore, $n_1 = cd$, and $t_1 = c + d$, hence $(t_1, n_1) = (c + d, cd)$, which proves the surjectivity of κ. Thus, κ is a bijective map.

□

Lemma 2.4. *Let $A' = \mathfrak{H}_\ell$ and $B' = \{(T, N) : T^2 - 4N$ is a non-square in $\mathbb{F}_\ell\}$. Then there is a bijection between the sets A' and B' given by*

$$\{z, \bar{z}\} \mapsto (z + \bar{z}, z\bar{z}).$$

Proof. Let $E = \{\{z, \bar{z}\} : z, \bar{z} \in \mathfrak{H}_\ell\}$ and $K = \{(T, N) : x^2 - Tx + N : \Delta \neq 0\}$. Let $\kappa' : E \to K$ be the map such that κ' sends each unordered pair $\{z, \bar{z}\}$ to (T, N). Here, we need to show that this map is surjective and injective.

Let $\{z_1, \bar{z}_1\}$ and $\{z_2, \bar{z}_2\}$ be two distinct elements of $\mathfrak{H}_\ell$ such that $\kappa'(\{z_1, \bar{z}_1\}) = \kappa'(\{z_2, \bar{z}_2\})$. Then, $(z_1 + \bar{z}_1, z_1\bar{z}_1) = (z_2 + \bar{z}_2, z_2\bar{z}_2)$ implies that $(2x_1, x_1^2 - \epsilon y_1^2) = (2x_2, x_2^2 - \epsilon y_2^2)$ where $z_1 = x_1 + \sqrt{\epsilon} y_1, \bar{z}_1 = x_1 - \sqrt{\epsilon} y_1, z_2 = x_2 + \sqrt{\epsilon} y_2$ and $\bar{z}_2 = x_2 - \sqrt{\epsilon} y_2$, then $x_1 = x_2$ and $y_1 = \pm y_2$. Therefore, we have either $z_1 = z_2, \bar{z}_1 = \bar{z}_2$ or $z_1 = \bar{z}_2, \bar{z}_1 = z_2$. Hence, $\{z_1, \bar{z}_1\} = \{z_2, \bar{z}_2\}$, which is a contradiction. Thus, κ' is an injective map.

Let $(T_1, N_1) \in B' = \{x^2 - T_1 x + N_1, T_1^2 - 4N_1$ is a non-square in $\mathbb{F}_\ell\}$. This equation has two solutions $\frac{T_1+\sqrt{\Delta}}{2}$ and $\frac{T_1-\sqrt{\Delta}}{2}$ in $\mathfrak{H}_\ell$, since $\Delta = T_1^2 - 4N_1$ is a non-square in $\mathbb{F}_\ell$. Then, there exist $z', \bar{z}' \in \mathfrak{H}_\ell = \mathfrak{C}_\ell/\sim$ such that $\frac{T_1+\sqrt{\Delta}}{2} = z'$ and $\frac{T_1-\sqrt{\Delta}}{2} = \bar{z}'$. Therefore, $N_1 = z'\bar{z}'$, and $T_1 = z' + \bar{z}'$, hence $(T_1, N_1) = (z' + \bar{z}', z'\bar{z}')$, which proves the surjectivity of κ'. Thus, κ' is a bijective map.

□

Lemma 2.5. *Let*

$$\begin{aligned} B &= \left\{(t, n) : t^2 - 4n \neq 0 \textit{ is a square in } \mathbb{F}_\ell\right\}, \\ S &= \{(t, m) : m \textit{ is a square in } \mathbb{F}_\ell\}. \end{aligned}$$

Then there is a bijection between the sets B and S given by:

$$(t, n) \mapsto (t, m),$$

where $m = t^2 - 4n$.

Proof. The inverse map is given by $(t, m) \mapsto (t, \frac{t^2-m}{4})$. □

Lemma 2.6. *Let*

$$B' = \left\{(T,N) : T^2 - 4N \text{ is a non-square in } \mathbb{F}_\ell\right\},$$
$$S' = \{(T,M) : M \text{ is a non-square in } \mathbb{F}_\ell\}.$$

Then there is a bijection between the sets B' and S' given by:

$$(T,N) \mapsto (T,M),$$

where $M = T^2 - 4N$.

Proof. The inverse map is given by $(T,M) \mapsto (T, \frac{T^2-M}{4})$. □

2.2 Proof of Theorem 1.1

By Lemma 1.37, ψ^+ is a $\mathbb{Q}[G]$-module homomorphism. To prove Theorem 1.1, it suffices to prove that the restriction

$$\psi^+_{|_{\mathbb{Q}[A]}} : \mathbb{Q}[A] \to \mathbb{Q}[\mathfrak{H}_\ell], \tag{2.3}$$

is an isomorphism of $\mathbb{Q}$-vector spaces.

Using the bijections given by Lemmas 2.3, 2.4, 2.5, and 2.6 to prove (2.3) is equivalent to proving that

$$\psi^+ : \mathbb{Q}[S] \to \mathbb{Q}[S'],$$

is an isomorphism of $\mathbb{Q}$-vector spaces, where ψ^+ is the same map as $\psi^+_{|_{\mathbb{Q}[A]}}$ under the identifications given by two bijections $A \leftrightarrow S$ and $\mathfrak{H}_\ell \leftrightarrow S'$.

Recall the equation giving the geodesic between a and b is

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon y^2 = \left(\frac{b-a}{2}\right)^2,$$

by Lemma 2.2. This equation becomes

$$\begin{aligned}
&\left(x-\frac{a+b}{2}\right)^2-\epsilon y^2=\left(\frac{b-a}{2}\right)^2\\
\iff &\left(x-\frac{t}{2}\right)^2-\epsilon y^2=\left(\frac{l}{2}\right)^2\\
\iff &4\left(x-\frac{t}{2}\right)^2-4\epsilon y^2=l^2\\
\iff &(2x-t)^2-4\epsilon y^2=l^2\\
\iff &(T-t)^2-4\epsilon y^2=l^2\\
\iff &(T-t)^2=l^2+4\epsilon y^2=m+M,
\end{aligned}$$

in the new coordinates from Lemmas 2.5 and 2.6. Here, m and M satisfy $(\frac{m}{\ell})=1$ and $(\frac{M}{\ell})=-1$, where $(\frac{\cdot}{\ell})$ is the Legendre symbol modulo ℓ.

Hence, the matrix of $\psi^+_{|\mathbb{Q}[S]}$ with respect to the basis S is given by

$$a_{(T,M),(t,m)}=\begin{cases}1 & \text{if } (T-t)^2\equiv m+M \quad (\ell),\\ 0 & \text{otherwise.}\end{cases} \tag{2.4}$$

Thus, the above matrix is an $\frac{\ell-1}{2}\times\frac{\ell-1}{2}$ matrix $D_{m,M}$, with entries being the $\ell\times\ell$ matrices given by

$$(D_{m,M})_{t,T}:=\begin{cases}1 & \text{if } (T-t)^2\equiv m+M \quad (\ell),\\ 0 & \text{otherwise.}\end{cases}$$

Let D be the matrix obtained from the $\ell\times\ell$ identity matrix by permuting its columns according to the cycle $(1\,2\,3...\,\ell)$.

Definition 2.7. *A circulant matrix is a matrix of the form*

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{r-1}\\ a_{r-1} & a_0 & a_1 & \dots & a_{r-2}\\ \vdots & & & & \vdots\\ a_1 & a_2 & \dots & a_{r-1} & a_0\end{pmatrix},$$

that is, a matrix whose i-th row is obtained from the $(i-1)$-th row by cyclically shifting the entries one position to the right.

Lemma 2.8. $D_{m,M}=\sum_{x^2\equiv m+M(\ell)}D^x$

Proof. If $m+M$ is not a square in $\mathbb{F}_\ell$, therefore $D_{m,M}$ is a zero matrix due to 0 entries, so $D_{m,M}=\sum_{x^2\equiv m+M(\ell)}D^x=0$.

If $m + M = x^2$ is a square in $\mathbb{F}_\ell$. Then $T - t = \pm x$ and

$$(D_{m,M})_{t,T} = \begin{cases} 1 & T = t \pm x, \\ 0 & \text{otherwise.} \end{cases}$$

In this case, $D_{m,M}$ coincides with $\sum_{x^2 \equiv m+M \ (\ell)} D^x$. □

Let ζ be an ℓ-th root of unity. The matrix $D_{m,M}$ has entries in $\mathbb{Q}[D]$, but we can replace the matrix D by an element in the cyclotomic field $\mathbb{Q}(\zeta)$ in the following manner:

Firstly, D satisfies the polynomial $x^\ell - 1$. Let $m(x)$ be the minimal polynomial of D over $\mathbb{Q}$, then $m(x)$ divides $x^\ell - 1 = (x-1)(x^{\ell-1} + \cdots + x + 1)$. In addition, $x^{\ell-1} + \cdots + x + 1$ is an irreducible polynomial in $\mathbb{Q}[x]$, therefore $m(x) = x^{\ell-1} + \cdots + x + 1$.

Furthermore, the ideal generated by $m(x)$ is the kernel of the surjective homomorphism $\mathbb{Q}[x] \longrightarrow \mathbb{Q}[D]$. By the first isomorphism theorem, we have

$$\mathbb{Q}[D] \cong \frac{\mathbb{Q}[x]}{(m(x))}.$$

By definition of cyclotomic field, $\mathbb{Q}[\zeta] = \frac{\mathbb{Q}[x]}{(m(x))}$, so we get

$$\mathbb{Q}[D] \cong \mathbb{Q}[\zeta].$$

Lemma 2.9. *Let $\mathfrak{L}$ be a prime of $\mathbb{Q}(\zeta)$ above ℓ. Then $\zeta \equiv 1 \ (\mathfrak{L})$.*

Proof. [11, lemma 10.1]. □

From the above discussion, we see that $D_{m,M} = \sum_{x^2 \equiv m+M(\ell)} 1$ (after reduction modulo $\mathfrak{L}$). We label m, M as $m = g^{2i}$ for $0 \leq i \leq r-1$ and $M = \epsilon g^{2j}$ for $0 \leq j \leq r-1$, where $r = \frac{\ell-1}{2}$ and g is a primitive root modulo ℓ. That gives us a new matrix denoted by $D_{i,j}$:

$$D_{i,j} = \sum_{x^2 \equiv g^{2i} + \epsilon g^{2j} \quad (\ell)} 1. \tag{2.5}$$

Proposition 2.10. *The determinant of a circulant matrix (as above) is given by*

$$\prod_{k=0}^{r-1} (a_0 + a_1\omega_k + a_2\omega_k^2 + \ldots + a_{r-1}\omega_k^{r-1}) = \prod_{k=0}^{r-1} \Big(\sum_{j=0}^{r-1} a_j \omega_k^j \Big), \tag{2.6}$$

where $\omega_k = e^{\frac{2\pi i k}{r}} = \omega^k, r \geq 1$ and $\omega = e^{\frac{2\pi i}{r}}$.

Proof. Suppose

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & ... & a_{r-1} \\ a_{r-1} & a_0 & a_1 & ... & a_{r-2} \\ \vdots & & & & \\ a_1 & a_2 & ... & a_{r-1} & a_0 \end{pmatrix},$$

is a circulant matrix. We consider A as linear self map of $\mathbb{C}^r$. Let ω_k be the r-th root of unity for each k, $0 \leq k \leq r-1$. Now, consider the row vector $\frac{1}{\sqrt{r}}(1, \omega_k, \omega_k^2, ..., \omega_k^{r-1})$, whose transpose we denote by $\gamma_k \in \mathbb{C}^r$, and let $\sigma_k = a_0 + a_1\omega_k + a_2\omega_k^2 + ... + a_{r-1}\omega_k^{r-1}$. Then we get that

$$\begin{pmatrix} a_0 & a_1 & ... & a_{r-1} \\ a_{r-1} & a_0 & ... & a_{r-2} \\ \vdots & & & \\ a_1 & a_2 & ... & a_0 \end{pmatrix} \begin{pmatrix} 1 \\ \omega_k \\ \vdots \\ \omega_k^{r-1} \end{pmatrix} = \sigma_k \begin{pmatrix} 1 \\ \omega_k \\ ... \\ \omega_k^{r-1} \end{pmatrix},$$

which implies that σ_k is an eigenvalue of A with normalized eigenvector γ_k. Furthermore, the set $\{\gamma_0, \gamma_1, ..., \gamma_{r-1}\}$ is a linearly independent set in $\mathbb{C}^r$, since the eigenvalues σ_k are distinct, therefore a diagonal matrix with the corresponding eigenvalues is conjugate to A, hence the determinant of A can be obtained by $\det(A) = \prod_{k=0}^{r-1} \sigma_k$. □

For later reference, we call each factor in the above formula *an eigenvalue.* We also assume r is $r = \frac{\ell-1}{2}$.

Lemma 2.11. *The matrix $D_{i,j}$ is an $r \times r$ circulant matrix.*

Proof. This follows because

$$D_{i,j} = \sum_{x^2 \equiv g^{2i} + \epsilon g^{2j}} 1 \equiv \sum_{x^2 \equiv g^2(g^{2(i-1)} + \epsilon g^{2(j-1)})} 1 = D_{i-1,j-1},$$

where the indices are taken modulo ℓ. □

Remark that $D_{0,j} = a_j$ is equal to the number of solutions of $x^2 \equiv 1 + \epsilon g^{2j} \ (\ell)$. To show that $D_{i,j}$ has non-zero determinant, it suffices to show that $D_{i,j}$ has non-zero determinant modulo ℓ in (2.6).

Using the formula for the determinant of a circulant matrix above, it suffices to show in $\mathbb{Z}[\omega]$ that we have

$$a_0 + a_1\omega_k + a_2\omega_k^2 + ... + a_{r-1}\omega_k^{r-1} \not\equiv 0(\vartheta) \tag{2.7}$$

for every $0 \leq k \leq r-1$, where ϑ is a prime above ℓ in $\mathbb{Z}[\omega]$, $\omega_k = \omega^k$ and $\omega = e^{2\pi i/r}$.

Lemma 2.12. *Let ϑ be a prime above ℓ in $\mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/r}$. Then $\omega \equiv g^2(\vartheta)$, where g is a primitive root modulo ℓ.*

Proof. Let $\mathcal{O} = \mathbb{Z}[\omega]$ be the maximal order of $\mathbb{Q}(\omega)$. The residue field of ϑ is $\mathcal{O}/\vartheta \cong \mathbb{F}_\ell$ by [11, Proposition 10.3]. Furthermore, since the polynomial $x^r - 1$ splits in $\mathcal{O}/\vartheta[x] \cong \mathbb{F}_\ell[x]$ with distinct roots $\omega_1 = \omega, \omega_2 = \omega^2, \ldots, \omega_r = \omega^r = 1$, we have that every root of $x^r - 1$ in $\mathbb{F}_\ell$ is a power of $\omega \in \mathcal{O}/\vartheta \cong \mathbb{F}_\ell$. Hence, $\omega \cong g^2 \ (\vartheta)$ for some primitive root g modulo ℓ. □

By the above lemma, to show (2.7), it suffices to show

Lemma 2.13.

$$\sum_{j=0}^{r-1} a_j (g^{2k})^j \not\equiv 0(\ell),$$

for every $0 \leq j, k \leq r-1$.

Proof. The above sum can be calculated as:

$$\begin{aligned}
&\sum_{j=0}^{r-1} D_{0,j} (g^{2k})^j \\
\equiv &\sum_{j=0}^{r-1} a_j (g^{2k})^j \\
\equiv &\sum_{j=0}^{r-1} \left(\sum_{x^2 \equiv 1 + \epsilon g^{2j} \quad (\ell)} 1 \right) (g^{2j})^k \\
\equiv &\sum_{\substack{j=0,\ldots,r-1 \\ x=0,\ldots,\ell-1 \\ x^2 \equiv 1+\epsilon g^{2j} \quad (\ell)}} (g^{2j})^k \\
\equiv 2 &\sum_{\substack{x=0,\ldots,\ell-1 \\ y=1,\ldots,\ell-1 \\ x^2 \equiv 1+\epsilon y^2 \quad (\ell)}} \left(\frac{x^2-1}{\epsilon} \right)^k .
\end{aligned} \tag{2.8}$$

Now, we need to show that (2.8) is non-zero modulo ℓ for every $0 \leq k \leq r-1$.

We can rewrite $(\frac{x^2-1}{\epsilon})$ as y^2 since $y = g^j$ for $0 \leq j \leq r-1$. The conic $x^2 \equiv 1 + \epsilon y^2 \ (\ell)$ is parametrized by $x = \frac{a - \epsilon\lambda^2 b}{1-\epsilon\lambda^2}, y = \frac{\lambda(a-b)}{1-\epsilon\lambda^2}$ from (2.2). Here, we compute $D_{i,j}$ for $i = 0$ which corresponds to $m = 1 = (a-b)^2$. Thus we can rewrite (2.8) as

$$\begin{aligned}
&\sum_{\lambda=1}^{\ell-1} \Big(\frac{\lambda}{1-\epsilon\lambda^2} \Big)^{2k} \\
\equiv &\sum_{\lambda=1}^{\ell-1} (\lambda^{-1} - \epsilon\lambda)^{-2k} \\
\equiv &\sum_{\lambda=1}^{\ell-1} (\lambda^{-1} - \epsilon\lambda)^{2k'},
\end{aligned}$$

where $-2k' \equiv 2k \ (\ell-1)$ and $0 \le 2k' \le \ell - 2$, hence $0 \le k' \le \frac{\ell-3}{2}$. Here, we have to consider two cases.

The first case is $k \ge 1$. By Lemma 1.3, the sum of all terms except the constant terms will be zero modulo ℓ. Therefore, we just have to compute the sum of the constant terms which is

$$\sum_{\lambda=1}^{\ell-1} \frac{(2k')!}{k'!k'!}(-1)^{k'}\epsilon^{k'} \equiv \frac{(2k')!}{k'!k'!}(-1)^{k'+1}\epsilon^{k'} \quad (\ell), \tag{2.9}$$

which is non-zero modulo ℓ, since $2k' < \ell$ for all values of k', hence none of the terms of (2.9) is a multiple of ℓ, therefore it is non-zero modulo ℓ.

The second case is when $k = 0$, then the sum in (2.9) becomes $\sum_{\lambda=1}^{\ell-1} 1 \equiv -1 \not\equiv 0 \ (\ell)$. □

This concludes the proof of Theorem 1.1.

Chapter 3

Cartan subgroup case

In this Chapter, we generalize Merel's conjecture to Cartan subgroups and give a proof by generalizing the methods in [7]. A new feature is that the conjectural explicit intertwining operator is now a linear combination of double coset operators (rather than a single double coset operator), whose coefficients we are able to make explicit.

Define $\gamma_{(0,\infty)} := \mathbb{F}_\ell^\times \sqrt{\epsilon} \subseteq \mathfrak{C}_\ell$, which can be thought of as a path in $\mathfrak{C}_\ell$ from 0 to ∞. Given an ordered pair (a, b), there is a $g \in G$ such that $(a, b) = (g(0), g(\infty))$, which is unique up to multiplication on the left by C. Thus, we may define $\gamma_{(a,b)} := g(\gamma_{(0,\infty)})$, which can be thought as a path in $\mathfrak{C}_\ell$ from a to b (see Figure 3.1).

Here, for each $s = 1, \dots, \ell - 1$, we define the linear operator H_s by:

$$\begin{aligned} H_s : \mathbb{Q}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta] &\longrightarrow \mathbb{Q}[\mathfrak{C}_\ell] \\ (a, b) &\longmapsto \sum_{x \in \gamma^s_{(a,b)}} x. \end{aligned} \tag{3.1}$$

Definition 3.1. *Define $\gamma^s_{(0,\infty)}$ to be $\left\{(\lambda s + \lambda\sqrt{\epsilon}, 1)^\top : \lambda \in \mathbb{F}_\ell^\times, s \in \mathbb{F}_\ell^\times\right\} \subseteq \mathfrak{C}_\ell$. This is a path in $\mathfrak{C}_\ell$ which is a line with slope s.*

By Lemma 2.1, we know that $g = \begin{pmatrix} b & a \\ 1 & 1 \end{pmatrix}$, hence the path in $\mathfrak{C}_\ell$ from a to b can be obtained as

$$\gamma^s_{(a,b)} = g(\gamma^s_{(0,\infty)}) = g(\lambda s + \lambda\sqrt{\epsilon}, 1)^\top = (bs\lambda + b\lambda\sqrt{\epsilon} + a, \lambda s + \lambda\sqrt{\epsilon} + 1)^\top, \tag{3.2}$$

which is represented by an equation defined by the next lemma.

Lemma 3.2. *The quadratic equation*

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon\left(y - \frac{s(b-a)}{2\epsilon}\right)^2 = \frac{(\epsilon - s^2)(a-b)^2}{4\epsilon} \tag{3.3}$$

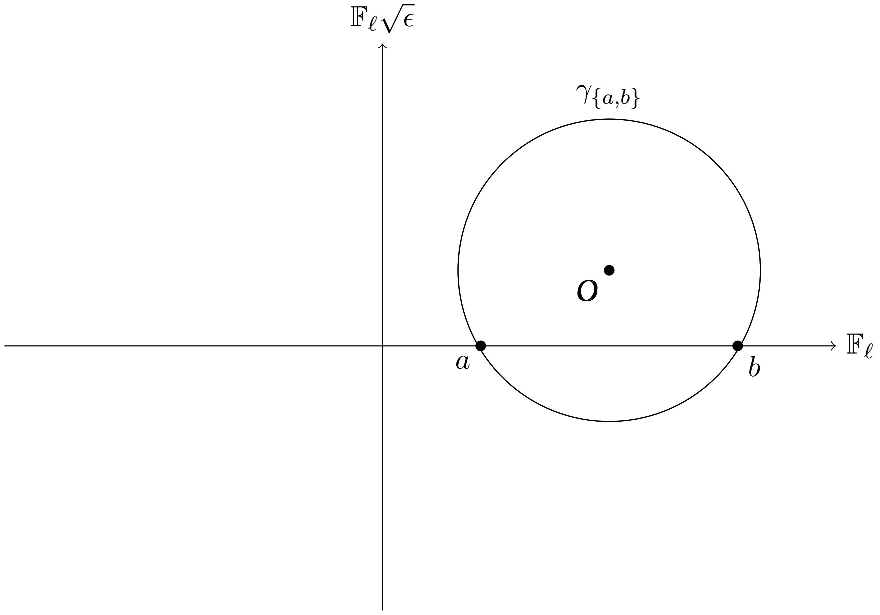

Figure 3.1: Geodesic $\gamma_{\{a,b\}}$ in $\mathfrak{H}_\ell$

gives the path $\gamma^s_{(a,b)}$ *with coordinates (see Figure 3.1)*

$$x = \frac{(b\lambda s + a)(\lambda s + 1) - b\lambda^2\epsilon}{(\lambda s + 1)^2 - \lambda^2\epsilon},$$
$$y = \frac{\lambda(b-a)}{(\lambda s + 1)^2 - \lambda^2\epsilon}.$$

Proof. Let write $g(\lambda s + \lambda\sqrt{\epsilon}, 1)^\top$ as a fraction, and rationalize it:

$$\begin{aligned}
&\frac{b\lambda s + b\lambda\sqrt{\epsilon} + a}{\lambda s + \lambda\sqrt{\epsilon} + 1} = \frac{b\lambda s + b\lambda\sqrt{\epsilon} + a}{(\lambda s + 1) + \lambda\sqrt{\epsilon}}\\
=&\frac{b\lambda s + b\lambda\sqrt{\epsilon} + a}{(\lambda s + 1) - \lambda\sqrt{\epsilon}}.\frac{(\lambda s + 1) + \lambda\sqrt{\epsilon}}{(\lambda s + 1) - \lambda\sqrt{\epsilon}}\\
=&\frac{(b\lambda s + b\lambda\sqrt{\epsilon} + a)(\lambda s + 1 - \lambda\sqrt{\epsilon})}{(\lambda s + 1)^2 - \lambda^2\epsilon}\\
=&\frac{b\lambda^2 s^2 + b\lambda^2 s\sqrt{\epsilon} + a\lambda s + b\lambda s + b\lambda\sqrt{\epsilon} + a - b\lambda^2 s\sqrt{\epsilon} - b\lambda^2\epsilon - a\lambda\sqrt{\epsilon}}{(\lambda s + 1)^2 - \lambda^2\epsilon}\\
=&\frac{b\lambda s(\lambda s + 1) + a(\lambda s + 1) - b\lambda^2\epsilon + \lambda\sqrt{\epsilon}(b-a)}{(\lambda s + 1)^2 - \lambda^2\epsilon}\\
=&\frac{(b\lambda s + a)(\lambda s + 1) - b\lambda^2\epsilon}{(\lambda s + 1)^2 - \lambda^2\epsilon} + \sqrt{\epsilon}\frac{\lambda(b-a)}{(\lambda s + 1)^2 - \lambda^2\epsilon},
\end{aligned}$$

Therefore, as $\gamma^s_{(a,b)} \in \mathbb{F}_\ell^\times$ we conclude x, y from the above expression are given by (see Figure 3.1)

$$x = \frac{(b\lambda s + a)(\lambda s + 1) - b\lambda^2\epsilon}{(\lambda s+1)^2 - \lambda^2\epsilon},$$
$$y = \frac{\lambda(b-a)}{(\lambda s+1)^2 - \lambda^2\epsilon}.$$

Using `Maple`, we can derive and verify that x, y satisfy (3.3). □

3.1 Coordinates for G/C and G/C'

We need more convenient coordinates to represent elements in (a certain subset of) $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ and $\mathfrak{C}_\ell$, where $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ is in bijection with G/C and $\mathfrak{C}_\ell$ is in bijection with G/C'.

Lemma 3.3. *Let $P = \mathbb{F}_\ell \times \mathbb{F}_\ell - \Delta$ and $E = \{(t, t') : t' \neq 0\}$. Then there is a bijection between the sets P and E given by:*

$$(a, b) \mapsto (a + b, a - b).$$

Proof. The inverse map is given by $a = \frac{x+y}{2}$ and $b = \frac{x-y}{2}$. □

Lemma 3.4. *Let $P' = \mathfrak{C}_\ell$ and $E' = \{(T, T') : T' \neq 0\}$. Then there is a bijection between the sets P' and E' given by:*

$$(z, \bar{z}) \mapsto (z + \bar{z}, z - \bar{z}).$$

Proof. The inverse map is given by $z = \frac{z+\bar{z}}{2} + \sqrt{\epsilon}\frac{z-\bar{z}}{2}$ and $\bar{z} = \frac{z+\bar{z}}{2} - \sqrt{\epsilon}\frac{z-\bar{z}}{2}$. □

3.2 Proof of Theorem 1.2

By Lemma 1.38, ψ is a $\mathbb{Q}[G]$-module homomorphism. Using more convenient coordinates to represent elements in (a subset of) $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta$ and $\mathfrak{C}_\ell$, to prove Theorem 1.2, it suffices to prove that the restriction

$$\psi_{|\mathbb{Q}[P]} : \mathbb{Q}[P] \to \mathbb{Q}[\mathfrak{C}_\ell], \tag{3.4}$$

is an isomorphism of $\mathbb{Q}$-vector spaces.

Using the bijections given by Lemma 3.3 and Lemma 3.4, to prove (3.4) is equivalent to proving that

$$\psi : \mathbb{Q}[E] \to \mathbb{Q}[E'],$$

is an isomorphism of $\mathbb{Q}$-vector spaces, where ψ is the same map as $\psi_{|\mathbb{Q}[P]}$ under identifications given by two bijections $P \leftrightarrow E$ and $\mathfrak{C}_\ell \leftrightarrow E'$.

Recall the equation giving the path $\gamma^s_{(a,b)}$ from a to b is

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon\left(y - \frac{s(b-a)}{2\epsilon}\right)^2 = \frac{(\epsilon - s^2)(a-b)^2}{4\epsilon},$$

by Lemma 3.2. By the bijection between G/C and G/C', this equation becomes

$$\begin{aligned}
&\Big(x - \frac{a+b}{2}\Big)^2 - \epsilon\Big(y - \frac{s(b-a)}{2\epsilon}\Big)^2 = \frac{(\epsilon - s^2)(a-b)^2}{4\epsilon} \\
\iff &\frac{1}{4}(2x - (a+b))^2 = \frac{(\epsilon - s^2)(a-b)^2}{4\epsilon} + \frac{\epsilon(2\epsilon y - s(b-a))^2}{4\epsilon^2} \\
\iff &(2x - (a+b))^2 = \frac{(\epsilon - s^2)(a-b)^2 + (2\epsilon y - s(b-a))^2}{\epsilon} \\
\iff &(T-t)^2 = \frac{\epsilon a^2 - 2\epsilon ab + \epsilon b^2 + 4\epsilon^2 y^2 - 4\epsilon ysb + 4\epsilon ysa}{\epsilon} \\
\iff &(T-t)^2 = (a-b)^2 + 4\epsilon y^2 + 4sy(b-a), \qquad (3.5)
\end{aligned}$$

in the new coordinates from Lemma 3.3 and Lemma 3.4. Hence, the matrix of H_s restricted to $\mathbb{Q}[E]$ with respect to the basis E is given by

$$a_{(t,t'),(T,T')}(s) = \begin{cases} 1 & \text{if } (T-t)^2 \equiv t'^2 + 4\epsilon T'^2 + 4sT't' \quad (\ell), \\ 0 & \text{otherwise.} \end{cases} \qquad (3.6)$$

The above matrix is an $(\ell-1) \times (\ell-1)$ matrix $X_{t',T'}(s)$, with entries being the $\ell \times \ell$ matrices $(X_{t',T'})_{t,T}$(s) given by

$$(X_{t',T'})_{t,T}(s) = \begin{cases} 1 & \text{if } (T-t)^2 \equiv t'^2 + 4\epsilon T'^2 + 4sT't' \quad (\ell), \\ 0 & \text{otherwise.} \end{cases}$$

Let X be the matrix which permutes columns of the ℓ by ℓ identity matrix according to the cycle $(1\,2\,3 \cdots \ell)$.

Lemma 3.5. $X_{t',T'}(s) = \sum_{v^2 \equiv t'^2 + 4\epsilon T'^2 + 4sT't' \ (\ell)} X^v$.

Proof. If $t'^2 + 4\epsilon T'^2 + 4sT't'$ is not square in $\mathbb{F}_\ell$, then $X_{t,T}(s)$ is a zero matrix due to 0 entries. Therefore, $X_{t,T}(s) = \sum_{v^2 \equiv t'^2 + 4\epsilon T'^2 + 4sT't' \ (\ell)} X^v = 0$.

If $t'^2 + 4\epsilon T'^2 + 4sT't' = v^2$ is a square in $\mathbb{F}_\ell$. Then $T - t = \pm v$ and

$$(X_{t',T'})_{t,T}(s) = \begin{cases} 1 & T = t \pm v, \\ 0 & \text{otherwise.} \end{cases}$$

In this case, $X_{t',T'}(s)$ coincides with $\sum_{v^2 \equiv t'^2 + 4\epsilon T'^2 + 4sT't' \ (\ell)} X^v$. □

Arguing similarly as in the discussion preceeding Lemma 2.9, we obtain that $X_{t',T'}(s) = \sum_{v^2 \equiv t'^2 + 4\epsilon T'^2 + 4sT't' \ (\ell)} 1$. We label t', T' as $t' = g^i$ and $T' = g^j$ for $0 \leq i, j \leq \ell - 1$, and $(T - t)^2 = v^2$. That gives us a new matrix denoted by $X_{i,j}(s)$ which is given by

$$X_{i,j}(s) = \sum_{v^2 \equiv g^{2i} + 4\epsilon g^{2j} - 4sg^{i+j} \quad (\ell)} 1 \quad (\ell).$$

Lemma 3.6. *The matrix $X_{i,j}(s)$ is a $(\ell - 1) \times (\ell - 1)$ circulant matrix.*

Proof. This follows since

$$X_{i,j}(s) \equiv \sum_{v^2 \equiv g^{2i} + 4\epsilon g^{2j} - 4sg^{i+j} \quad (\ell)} 1 \equiv \sum_{v^2 \equiv g^2(g^{2(i-1)} + 4\epsilon g^{2(j-1)} - 4sg^{i+j-2}) \quad (\ell)} 1 \equiv X_{i-1,j-1}(s) \quad (\ell),$$

where the indices are taken modulo ℓ. Remark, $X_{0,j}(s) = a_j(s)$ is equal to the number of solutions of $v^2 \equiv 1 + 4\epsilon g^{2j} - 4sg^j \ (\ell)$. □

Let $a_j(s) = X_{0,j}(s) = c_j$, and $\omega = e^{\frac{2\pi i}{\ell - 1}}$.

Lemma 3.7. *Let ϑ be a prime above ℓ in $\mathbb{Z}[\omega]$ where $\omega = e^{\frac{2\pi i}{\ell-1}}$. Then $\omega \equiv g \ (\vartheta)$, where g is a primitive root modulo ℓ.*

Proof. Let $\mathcal{O} = \mathbb{Z}[\omega]$ be the maximal order of $\mathbb{Q}(\omega)$. The residue field of ϑ is $\mathcal{O}/\vartheta \cong \mathbb{F}_\ell$ by [11, Proposition 10.3]. Furthermore, since the polynomial $x^{\ell-1} - 1$ splits in $\mathcal{O}/\vartheta[x] \cong \mathbb{F}_\ell[x]$ with distinct roots $\omega_1 = \omega, \omega_2 = \omega^2, \cdots, \omega_{\ell-1} = \omega^{\ell-1} = 1$, we have that every root of $x^{\ell-1} - 1$ in $\mathbb{F}_\ell$ is a power of $\omega \in \mathcal{O}/\vartheta \cong \mathbb{F}_\ell$. Hence, $\omega \cong g \ (\vartheta)$ for some positive root g modulo ℓ. □

The eigenvalue of H_s modulo ℓ can be calculated as

$$\begin{aligned}
&\sum_{j=0}^{\ell-2} a_j(s)\omega^{kj} \\
\equiv &\sum_{j=0}^{\ell-2} a_j(s)(g^k)^j \\
\equiv &\sum_{j=0}^{\ell-2} \left(\sum_{v^2 \equiv 1+4\epsilon g^{2j} - 4sg^j \quad (\ell)} 1 \right) (g^k)^j \\
\equiv &\sum_{j=0}^{\ell-2} \sum_{v^2 \equiv 1+4\epsilon g^{2j} - 4sg^j \quad (\ell)} g^{kj} \\
\equiv &\sum_{\lambda=1}^{\ell-1} y(\lambda)^k \\
\equiv &\sum_{\lambda=1}^{\ell-1} \frac{\lambda^k (a-b)^k}{((\lambda s+1)^2 - \lambda^2\epsilon)^k} \quad (\ell). \qquad (3.7)
\end{aligned}$$

Here, $a_j(s) = X_{0,j}(s)$, which corresponds to $m = 1 = (a-b)^2$, therefore, we can rewrite x, y in λ parametrization as in (3.3) to be:

$$\sum_{\lambda=1}^{\ell-1} \frac{\lambda^k}{((\lambda s+1)^2 - \lambda^2\epsilon)^k}.$$

We now consider a linear combination $\sum_{s=1}^{\ell-1} \alpha_s H_s : \mathbb{Q}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) - \Delta] \to \mathbb{Q}[\mathfrak{C}_\ell]$ of the maps H_s. Note that a linear combination of circulant matrices is circulant. The eigenvalue of $\sum_{s=1}^{\ell-1} \alpha_s H_s$ is thus given by $\sum_{j=0}^{\ell-2} b_j \omega^{kj}$, where $b_j = \sum_{s=1}^{\ell-1} \alpha_s a_j(s)$. Then, we have

$$\begin{aligned}
&\sum_{j=0}^{\ell-2} b_j \omega^{kj} = \sum_{j=0}^{\ell-2} \Big(\sum_{s=1}^{\ell-1} \alpha_s a_j(s) \Big) \omega^{kj} \\
= &\sum_{s=1}^{\ell-1} \alpha_s \sum_{j=0}^{\ell-2} a_j(s)\omega^{kj} \\
= &\sum_{s=1}^{\ell-1} \alpha_s \sum_{\lambda=1}^{\ell-1} y(\lambda, s)^k \\
= &\sum_{\lambda=1}^{\ell-1} \sum_{s=1}^{\ell-1} \alpha_s y(\lambda, s)^k \\
= &\sum_{s=1}^{\ell-1} \alpha_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{\lambda}{(\lambda s+1)^2 - \epsilon\lambda^2} \Big)^k.
\end{aligned}$$

Lemma 3.8. *Let $\alpha_s \equiv 1 \ (\ell)$ for $s \in \mathbb{F}_\ell^\times$, then the sum*

$$\sum_{s=1}^{\ell-1} \alpha_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{\lambda}{(\lambda s+1)^2 - \epsilon\lambda^2}\Big)^k, \tag{3.8}$$

is non-zero modulo ℓ for k even.

Proof. In the case $k = 0$, we cannot use a binomial expansion so we perform a direct computation:

$$\begin{aligned}
&\sum_{s=1}^{\ell-1} \alpha_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{\lambda}{(\lambda s+1)^2 - \epsilon\lambda^2}\Big)^k && (3.9)\\
\equiv &\sum_{s=1}^{\ell-1} \alpha_s(\ell-1) && (3.10)\\
\equiv &(\ell-1)\sum_{s=1}^{\ell-1} \alpha_s && (3.11)\\
\equiv &(\ell-1)\sum_{s=1}^{\ell-1} 1 && (3.12)\\
\equiv &(\ell-1)(\ell-1) && (3.13)\\
\equiv &1 \quad (\ell) && (3.14)
\end{aligned}$$

We choose $k' \in \mathbb{N}$ such that $k \equiv -k' \ (\ell-1)$, and $1 \leq k' \leq \ell-2$. Here, we just need constant terms of $\Big(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\Big)^{k'}$ as the other terms are powers of λ, and the sum of these powers is zero modulo ℓ by Lemma 1.3.

$$\begin{aligned}
&\sum_{s=1}^{\ell-1} \alpha_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{(\lambda s+1)^2 - \epsilon\lambda^2}{\lambda}\Big)^{-k}\\
\equiv &\sum_{s=1}^{\ell-1} \alpha_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{(\lambda s+1)^2 - \epsilon\lambda^2}{\lambda}\Big)^{k'}.
\end{aligned}$$

Hence, we get

$$\begin{aligned}
&\Big(\frac{(\lambda s+1)^2 - \epsilon\lambda^2}{\lambda}\Big)^{k'}\\
=&\Big(\frac{\lambda^2 s^2 + 2\lambda s + 1 - \epsilon\lambda^2}{\lambda}\Big)^{k'}\\
=&(\lambda s^2 + 2s + \lambda^{-1} - \epsilon\lambda)^{k'}\\
=&(\lambda(s^2-\epsilon) + 2s + \lambda^{-1})^{k'}.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}&\text{constant term of } (\lambda(s^2-\epsilon)+2s+\lambda^{-1})^{k'}\\ \equiv&\sum_{i=0}^{\frac{k'}{2}}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \quad \text{for } k' \text{ even.}\end{aligned}$$

Thus,

$$\sum_{s=1}^{\ell-1}\alpha_s\sum_{\lambda=1}^{\ell-1}\Big(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\Big)^{-k} \equiv \qquad \sum_{s=1}^{\ell-1}\alpha_s\sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i.$$

If $\alpha_s \equiv 1 \ (\ell)$ for $s = 1, \dots, \ell-1$, then for $k' > 0$ even, we have that

$$\begin{aligned}&\sum_{s=1}^{\ell-1}\alpha_s\sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i\\ \equiv&\sum_{s=1}^{\ell-1}\sum_{i=0}^{\frac{k'}{2}}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i\\ \equiv&\sum_{i=0}^{\frac{k'}{2}}\sum_{s=1}^{\ell-1}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i\\ \equiv&\epsilon^{\frac{k'}{2}}\frac{k'!}{\frac{k'}{2}!\frac{k'}{2}!}\not\equiv 0 \quad (\ell).\end{aligned}$$

The last equality holds because the only power of s whose exponent is divisible by $\ell-1$ happens when $i = k'/2$. This proves the Lemma. □

Lemma 3.9. *Let $\alpha_s \equiv 1 \ (\ell)$ for $s \in \mathbb{F}_\ell^\times$, then the sum*

$$\sum_{s=1}^{\ell-1}\alpha_s\sum_{\lambda=1}^{\ell-1}\Big(\frac{\lambda}{(\lambda s+1)^2-\epsilon\lambda^2}\Big)^{k}, \tag{3.15}$$

is equal to zero modulo ℓ for k odd.

Proof. We choose $k' \in \mathbb{N}$ such that $k \equiv -k' \ (\ell-1)$, and $1 \leq k' \leq \ell-2$. Hence, we just need constant terms of $\Big(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\Big)^{k'}$ as the other terms are powers of λ, and the sum of these powers is zero modulo ℓ by Lemma 1.3.

$$\begin{aligned}&\sum_{s=1}^{\ell-1}\alpha_s\sum_{\lambda=1}^{\ell-1}\Big(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\Big)^{-k}\\ \equiv&\sum_{s=1}^{\ell-1}\alpha_s\sum_{\lambda=1}^{\ell-1}\Big(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\Big)^{k'}.\end{aligned}$$

Hence, we get

$$\begin{aligned}&\Big(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\Big)^{k'}\\ =&\Big(\frac{\lambda^2s^2+2\lambda s+1-\epsilon\lambda^2}{\lambda}\Big)^{k'}\\ =&(\lambda s^2+2s+\lambda^{-1}-\epsilon\lambda)^{k'}\\ =&(\lambda(s^2-\epsilon)+2s+\lambda^{-1})^{k'}.\end{aligned}$$

Therefore, we have

$$\text{constant term of } (\lambda(s^2-\epsilon)+2s+\lambda^{-1})^{k'}\equiv \sum_{i=0}^{\frac{k'-1}{2}}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \quad (\ell) \quad \text{for } k' \text{ odd}$$

Thus,

$$\sum_{s=1}^{\ell-1}\alpha_s\sum_{\lambda=1}^{\ell-1}\Big(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\Big)^{-k}\equiv \sum_{s=1}^{\ell-1}\alpha_s\sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i.$$

If $\alpha_s\equiv 1\ (\ell)$ for $s=1,\ldots,\ell-1$, then for $k'>0$ odd, we have that

$$\begin{aligned}&\sum_{s=1}^{\ell-1}\alpha_s\sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i\\ \equiv&\sum_{s=1}^{\ell-1}\sum_{i=0}^{\frac{k'-1}{2}}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i\\ \equiv&\sum_{i=0}^{\frac{k'-1}{2}}\sum_{s=1}^{\ell-1}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i\\ \equiv&0 \quad (\ell).\end{aligned}$$

The last equality holds because there are no powers of s whose exponent is divisible by $\ell-1$, which proves the Lemma. □

Lemma 3.10. *Let $\beta_s \equiv s^{-1}$ (ℓ) for $s \in \mathbb{F}_\ell^\times$. Then, the sum*

$$\sum_{s=1}^{\ell-1} \beta_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{\lambda}{(\lambda s+1)^2 - \epsilon\lambda^2}\Big)^k, \tag{3.16}$$

is zero modulo ℓ for k even.

Proof. In the case $k = 0$, we cannot use a binomial expansion so we perform a direct computation:

$$\begin{aligned}
&\sum_{s=1}^{\ell-1} \beta_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{\lambda}{(\lambda s+1)^2 - \epsilon\lambda^2}\Big)^k && (3.17)\\
\equiv&\sum_{s=1}^{\ell-1} \beta_s(\ell-1) && (3.18)\\
\equiv&\sum_{s=1}^{\ell-1} s^{-1}(\ell-1) && (3.19)\\
\equiv&\sum_{s=1}^{\ell-1} s^{\ell-2}(\ell-1) && (3.20)\\
\equiv&(\ell-1)\sum_{s=1}^{\ell-1} s^{\ell-2} && (3.21)\\
\equiv&0 \quad (\ell) && (3.22)
\end{aligned}$$

For $k' > 0$ even, we have that

$$\begin{aligned}
&\sum_{s=1}^{\ell-1} \beta_s \sum_{i=0}^{\lfloor \frac{k'}{2} \rfloor} \frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i\\
\equiv&\sum_{s=1}^{\ell-1} s^{-1} \sum_{i=0}^{\frac{k'}{2}} \frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \quad (\ell)\\
\equiv&\sum_{i=0}^{\frac{k'}{2}} \sum_{s=1}^{\ell-1} s^{-1} \frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \quad (\ell)\\
\equiv&0 \quad (\ell).
\end{aligned}$$

The last equality holds because there are no powers of s whose exponent is divisible by $\ell - 1$, which proves the Lemma. □

Lemma 3.11. *Let $\beta_s \equiv s^{-1}$ (ℓ) for $s \in \mathbb{F}_\ell^\times$. Then the sum*

$$\sum_{s=1}^{\ell-1} \beta_s \sum_{\lambda=1}^{\ell-1} \Big(\frac{\lambda}{(\lambda s+1)^2 - \epsilon\lambda^2}\Big)^k \tag{3.23}$$

is non-zero modulo ℓ for k odd.

Proof. For $k' > 0$ odd, we have that

$$\begin{aligned}
&\sum_{s=1}^{\ell-1} \beta_s \sum_{i=0}^{\left\lfloor \frac{k'}{2} \right\rfloor} \frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \\
\equiv &\sum_{s=1}^{\ell-1} s^{-1} \sum_{i=0}^{\frac{k'-1}{2}} \frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \quad (\ell) \\
\equiv &\sum_{i=0}^{\frac{k'-1}{2}} \sum_{s=1}^{\ell-1} s^{-1} \frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \quad (\ell) \\
\equiv &\epsilon^{\frac{k'-1}{2}} \frac{k'!}{\frac{k'-1}{2}!\frac{k'-1}{2}!} \not\equiv 0 \quad (\ell).
\end{aligned}$$

The last equality holds because the only power of s whose exponent is divisible by $\ell - 1$ happens when $i = \frac{k'-1}{2}$, which proves the Lemma. □

Corollary 3.12. *The operator $\sum_{s=1}^{\ell-1}(\alpha_s + \beta_s)H_s$ has non-zero eigenvalue modulo ℓ for all $k > 0$ in its circulant determinant formula.*

Proof. Using (3.17), the operator $\sum_{s=1}^{\ell-1}(\alpha_s + \beta_s)H_s$ has non-zero eigenvalue for $k = 0$.

Furthermore, by Lemmas 3.8, 3.9, 3.10, and 3.11, the eigenvalue of $\sum_{s=1}^{\ell-1}(\alpha_s + \beta_s)H_s$ is non-zero modulo ℓ for $k > 0$, since the eigenvalue of $\sum_{s=1}^{\ell-1}(\alpha_s + \beta_s)H_s$ for k is the sum of the eigenvalues for k of $\sum_{s=1}^{\ell-1} \alpha_s H_s$ and $\sum_{s=1}^{\ell-1} \beta_s H_s$. □

Thus, the determinant of $\sum_{s=1}^{\ell-1}(\alpha_s + \beta_s)H_s$ is non-zero modulo ℓ and is hence non-zero. This concludes the proof of Theorem 1.2.

Chapter 4

Relations between Jacobians of certain modular curves

In this section, we summarize some applications of the main results of this thesis to Jacobians of modular curves.

Let $X = X(\ell)$ denote the modular curve of full level ℓ structure which has the structure of a projective algebraic curve over $\mathbb{Q}$ for $p \geq 3$ (cf. [10, p.241] or [8]).

The group $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ acts on X and the quotients $X_H := X/H$ by subgroups H of G (which contain -1) exist as projective algebraic curves over $\mathbb{Q}$ [10, p.244] and [8].

Let J denote the Jacobian of X and J_H denote the Jacobian of X_H [9].

Proposition 4.1. *Let $\sigma : \mathbb{Z}[G/H'] \to \mathbb{Z}[G/H]$ be a $\mathbb{Z}[G]$-module homomorphism. Then σ induces a homomorphism of Jacobians $\sigma^* : J_H \to J_{H'}$.*

Proof. This is proved in [1, Lemma 3.3]. □

Definition 4.2. *A sequence of homomorphisms (with increasing index)*

$$\ldots \to C^{i-1} \to_{\sigma^i} C^i \to_{\sigma^{i+1}} C^{i+1} \to \ldots$$

in an abelian category such that the composite of two successive homomorphisms is zero is called a cochain complex. The quotient group $H^i(C^\bullet) = \ker \sigma^{i+1} / \operatorname{im} \sigma^i$ is called the i-th cohomology group of $C^\bullet$. If all the $H^i(C^\bullet) = 0$, then we say that $C^\bullet$ is exact.

Definition 4.3. *A sequence of homomorphisms (with decreasing index)*

$$\ldots \to C_{i+1} \to_{\sigma_{i+1}} C_i \to_{\sigma_i} C_{i-1} \to \ldots$$

in an abelian category such that the composite of two successive homomorphisms is zero is called a chain complex. The quotient group $H_i(C_\bullet) = \ker \sigma_i / \operatorname{im} \sigma_{i+1}$ is called the i-th homology group of $C_\bullet$. If all the $H_i(C_\bullet) = 0$, then we say that $C_\bullet$ is exact.

Proposition 4.4. *Suppose a cochain complex of $\mathbb{Z}[G]$-modules*

$$\ldots \longrightarrow \mathbb{Z}[G/H_{i-1}] \longrightarrow \mathbb{Z}[G/H_i] \longrightarrow \mathbb{Z}[G/H_{i+1}] \longrightarrow \ldots$$

has finite cohomology groups. Then the induced sequence of Jacobians by applying Proposition 4.1 yields a chain complex

$$\ldots \longleftarrow J_{H_{i-1}} \longleftarrow J_{H_i} \longleftarrow J_{H_{i+1}} \longleftarrow \ldots$$

with finite homology groups.

Proof. This is proved in [1, Proposition 3.7]. □

Theorems 1.1 and 1.2 imply that

$$\mathbb{Q}[G/N] \longrightarrow_{\psi^+} \mathbb{Q}[G/N'] \longrightarrow 0 \tag{4.1}$$

$$\mathbb{Q}[G/C] \longrightarrow_{\psi} \mathbb{Q}[G/C'] \longrightarrow 0 \tag{4.2}$$

are exact cochain complexes of $\mathbb{Q}[G]$-modules.

Proposition 4.5. *The following are cochain complexes*

$$\mathbb{Z}[G/N] \longrightarrow_{\psi^+} \mathbb{Z}[G/N'] \longrightarrow 0 \tag{4.3}$$

$$\mathbb{Z}[G/C] \longrightarrow_{\psi} \mathbb{Z}[G/C'] \longrightarrow 0 \tag{4.4}$$

with finite cohomology groups.

Proof. This follows from tensoring the cochain complexes above by $\mathbb{Q}$. If the cohomology groups were not finite, this would contradict the exactness of the cochain complexes in (4.1)-(4.2). □

Applying Proposition 4.4, we obtain:

Corollary 4.6. *The following are chain complexes*

$$0 \longrightarrow J_{N'} \longrightarrow_{\psi^{+*}} J_N \tag{4.5}$$

$$0 \longrightarrow J_{C'} \longrightarrow_{\psi^*} J_C \tag{4.6}$$

with finite homology groups.

The above corollary thus describes the main part of the well-known relations between J_N and $J_{N'}$ (resp. J_C and $J_{C'}$) using explicit correspondences.

It is known that $X_C \cong X_0(\ell^2)$ and $X_N \cong X_0(\ell^2)/\langle w_\ell \rangle$, which are the more standard modular curves studied in the literature.

Bibliography

[1] I. Chen. On Relations between Jacobians of Certain Modular curves, *J. Algebra*, 231 (2000), 414–448.

[2] I. Chen. The Jacobians of non-split Cartan modular curves. Proc. London Math. Soc. (3) 77 (1998), no. 1, 1–38.

[3] B. De Smit and B. Edixhoven Sur un résultat d'Imin Chen. (French) [On a result of Imin Chen] Math. Res. Lett. 7 (2000), no. 2-3, 147–153.

[4] H. Darmon and L. Merel Winding quotients and some variants of Fermat's last theorem. J. Reine Angew. Math. 490 (1997), 81–100.

[5] B. Mazur. Rational isogenies of prime degree, *Invent. Math.* 44 (1978), 129–162.

[6] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones Math.* 15 (1972), 259–331.

[7] B. Birch and D. Zagier. Personal communication with I. Chen, 2000.

[8] N.-M. Katz and B. Mazur. Arithmetic moduli of elliptic curves, *Princeton University Press*, 1985.

[9] P. Swinnerton-Dyer. Analytic theory of abelian varieties, London Mathematical Society Lecture Note Series (Book 14), *Cambridge University Press*, 1974.

[10] B. Mazur and A. Wiles. Class fields of abelian extensions of Q. *Inventiones Mathematicae* 76 (1984), 179-330.

[11] J. Neukirch. Algebraic Number Theory, *Springer-Verlag*, New York, 1999.