Arithmetic Path Integrals and Linking Numbers

Yan Yau Cheng

Doctor of Philosophy

The University of Edinburgh

2026

Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where stated otherwise by reference or acknowledgement, the work presented is entirely my own.

(*Yan Yau Cheng*)

To my grandmother, Lo Ho, who raised me and taught me arithmetic as a child.

Abstract

Following the analogy between arithmetic and topology, this thesis studies arithmetic analogues of path integrals and triple symbols.

In the first half of the thesis, we show that an arithmetic path integral over the ℓ-torsion of a Jacobian $J[\ell]$ is equal to the trace of the Frobenius action on a representation of the Heisenberg group $H(J[\ell])$, up to an explicitly determined sign. This is an arithmetic analogue of trace–path integral formulae which arise in quantum field theory, where path integrals over a space of sections of a fibration over a circle can be expressed as the trace of the monodromy action on a Hilbert space.

In the second half, we study arithmetic triple symbols, which can be viewed as an analogue of multiple linking phenomena such as the Borromean links. We will prove some partial results towards the computation of the Massey type arithmetic Chern-Simons action, and towards the construction of characteristic zero arithmetic linking numbers, defined over an infinite cyclotomic field.

Lay Summary

Arithmetic Topology is the field of mathematics that is inspired by the analogy that a knot (i.e. a piece of string with its ends tied together) in 3-dimensional space 'behaves similarly' to a prime number p. Roughly speaking, we say that these two objects behave similarly because they exhibit very similar looking *symmetries*.

Suppose you are standing on a circular platform. In how many ways can you move around and return to your starting position? Well, you could go around the circle clockwise n times for any positive integer n, and you could also go anti-clockwise any positive integer number of times too. These loops encode the symmetries of an object known as the *covering space* in topology, and we say that the *fundamental group* of the circle is equal to the integers $\mathbb{Z}$, since you can loop around the circle any integer number of times.

On the other hand, suppose we had a prime number p. Mathematicians often study primes by considering the remainders of numbers when you divide by p (this is called the finite field $\mathbb{F}_p$). The symmetries of the prime p emerge when you solve equations in this world of remainders. For example, when solving quadratic equations, the quadratic formula $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ has the plus or minus symbol $\pm$. This can be thought of as a 'reflective symmetry' of swapping the solutions of quadratic equations.

When you consider all possible equations and their symmetries over the finite field $\mathbb{F}_p$, it turns out that once again there is one possible symmetry for every integer n. By packaging these symmetries together, we say that the *étale fundamental group* of the prime p is equal to the profinite integers $\widehat{\mathbb{Z}}$ (this can be thought of as a sort of refinement of the integers $\mathbb{Z}$).

In this sense, we see that a knot and a prime have similar looking symmetries, with both symmetry groups looking roughly like the integers. This analogy extends in an intricate manner to other objects in topology and number theory. Given a certain theorem or object in topology, it is often an interesting question to ask what its suitable analogue is in number theory, and vice versa.

In the 1980s, Edward Witten showed that it is possible to compute certain properties of knots (called knot invariants) using methods coming from quantum field theory. This was a big breakthrough that bridges physics and pure mathematics together in a beautiful way.

Inspired by these analogies, Minhyong Kim considered the number theoretic analogue of this framework, and initiated the study of arithmetic quantum field theory. This thesis is built upon this framework. In chapter 3, we prove a theorem that certain arithmetic path integrals can be expressed in terms of a trace, paralleling a similar theorem in physics. In chapter 4, we study the linking behaviour of knots and primes, under the perspective of arithmetic quantum field theory.

Acknowledgements

Firstly, I am deeply grateful to my advisor Minhyong Kim, without whom this thesis would not be possible. Thank you for your invaluable insights and guidance, and for introducing me to the rich and profound field of arithmetic topology.

Thank you also to Akshay Venkatesh, whose unpublished work with Minhyong formed the basis of Chapter 3 of this thesis.

Thank you to Dohyeong Kim and Masanori Morishita for their kind hospitality in Seoul and Kyushu respectively, and for the many illuminating conversations we had during my visit.

Thank you also to my examiners, Clark Barwick and David Treumann, for their careful reading and feedback of this thesis.

I am thankful to the many teachers who supported my mathematical journey through my primary and secondary years at Discovery College, especially Rob Street, Jason Yee, and Edeh Nobari. Without you, I might never have discovered and pursued my passion for mathematics.

To the Glasgow Number Theory Group, especially Adam Morgan, Alex Bartel, Alistair Severn, Damián Gvirtz-Chen, James Rawson, Parth Shimpi and Ruth Raistrick. Thank you for allowing me to join the infernal seminar and taking me in as one of your own.

I am grateful to Adrián Doña Mateo, Benjamin Moore, Danil Koževnikov, Eric Ahlqvist, James Timmins, Malthe Sporring, Xiang Li, and Subrabalan (Subri) Murugesan for the many helpful mathematical discussions during my time in Edinburgh.

To my other mathematical friends around the world: Alvaro Gonzalez Hernandez, Corijn Rudrum, Dan Townsend, Diana Mocanu, Isabel (Izzy) Rendell, James Rawson, Jay Swar, Katerina Santicola, Lee Berry, Mandy Kwok, Nadav Gropper, Robin Visser, and Samuel Lee. Thank you for being my 'conference buddies', and for the many interesting conversations throughout the years.

To my friends in Edinburgh: Adrián, Cassia, Csoban, Danil, Hannah, James, Julia, Karim, Malthe, Matthias, Patrick, Shirley, Tia, and Tuan. Thank you for making me feel so incredibly welcome here, and for the wonderful memories that we've shared.

To my friends from Cambridge: Alejandro, Christian, Dan, Emma, Fox, Gabby, Harvey, Jiacheng (JC), John, Nikita, Parth, and Yuji. Thank you for your continued friendship and support throughout the years.

A special shoutout to the Parlejarveyanyauji group chat, consisting of Parth Shimpi, Alejandro Epelde Blanco, Harvey Yau, and Yuji Okitani. Though we are now scattered across the world, you remain one of my closest support systems, both mathematically and personally.

To my high school friends from Hong Kong, especially Aashman, Ashley, Carlos, Cherie, Christopher, Csoban, Dhiraj, Faye, Jennifer, Jocelyn, Judith, Katie, Kazuya, Lorcan, Margaret, Nicola, Rachel, Seo Jin, Shirley, Soovin, and Jessica. Whether you were listening to my work rants, offering emotional support through flatmageddon, hosting me when I pass through London, or just keeping me company when I'm home, I am grateful for you all.

Thank you to the Law family and the Leung family, for being my home away from home.

Thank you to my grandma, Lo Ho, for raising me and teaching me arithmetic as a child.

Thank you to my parents for always believing in me and supporting me. Thank you for trusting me to forge my own path.

To my little sister Rachel, thank you for being a positive force in my life. Always believe in yourself, because you are capable of incredible things.

Thank you.

Contents

Abstract **iv**

Lay Summary **v**

Acknowledgements **vii**

1 Introduction and Motivation **3**

1.1 Arithmetic Topology . . . 3

1.1.1 Boundaries and Restricted Ramification . . . 4

1.1.2 Decomposition Theory of Knots and Primes . . . 5

1.2 Weil's Trichotomy . . . 7

1.3 Arithmetic Quantum Field Theory and Path Integrals . . . 8

1.4 Outline of Thesis . . . 8

2 Arithmetic Chern–Simons Actions for Function Fields **10**

2.1 Introduction to Arithmetic Topological Quantum Field Theories . . . 10

2.2 The Arithmetic Chern–Simons Action without Boundary . . . 11

2.3 The Arithmetic Chern–Simons with Boundary . . . 12

2.4 Facts about Compactly Supported Étale Cohomology . . . 15

2.4.1 Compactly Supported Cocycles . . . 15

2.4.2 Cup Products between Non-Compact and Compact Cohomology . . . 16

2.4.3 Invariant Map of a Compact Cohomology Class . . . 17

2.5 The Decomposition Formula . . . 18

3 A Trace–Path Integral Formula over Function Fields **20**

3.1 Introduction . . . 20

3.2 Physical Background . . . 23

3.2.1 The Path Integral Formalism . . . 23

3.2.2 Twists and Trace of Monodromy . . . 24

3.2.3 Geometric Quantisation . . . 25

3.3 Trace of Frobenius in the Arithmetic Hilbert Space . . . 26

3.3.1 Representations of the Heisenberg Group . . . 27

3.3.2 Symplectic Actions on the Heisenberg Representations 29
3.3.3 Invariant Spaces of a Symplectic Vector Space 32
3.3.4 Evaluating the Trace 34
3.4 An Arithmetic Path Integral 38
3.4.1 Defining an Arithmetic Action 38
3.4.2 Relation to the Abelian Chern-Simons Pairing 40
3.4.3 Computation of the Arithmetic Path Integral 47
3.5 Proving the Main Theorem 48
3.6 Computational Examples and Remarks 49
3.6.1 Examples where $\mu_{\ell^2} \subset \mathbb{F}_q$ 49
3.6.2 Examples where $\mu_{\ell^2} \not\subset \mathbb{F}_q$ 52
3.6.3 Further Related Questions 56

4 Arithmetic Triple Symbols **57**
4.1 Introduction 57
4.1.1 Linking Numbers in Topology 57
4.1.2 Quadratic and Power Residue Symbols 58
4.1.3 The Borromean Rings and Triple Symbols 59
4.2 Topological Milnor Invariants 60
4.2.1 The Magnus Embedding and Magnus Coefficients 60
4.2.2 Definition of the Milnor $\overline{\mu}$-Invariants 61
4.2.3 The Milnor Representation 62
4.3 Arithmetic Milnor Invariants 63
4.3.1 Pro-ℓ and mod $m = \ell^e$ analogues of Magnus Coefficients 63
4.3.2 Koch's presentation for G_S 64
4.3.3 Milnor $\overline{\mu}_m$-invariants 64
4.3.4 Interpretation via Nilpotent Extensions 65
4.4 Rédei Triple Symbol 65
4.5 Triple Symbols of Characters 67
4.5.1 Setup and Definitions 68
4.5.2 Construction of the Triple Symbol 69
4.5.3 The Arithmetic Chern–Simons Action of Massey Type 73
4.6 Towards Arithmetic Path Integrals of Massey Type 74
4.6.1 A Critical Set 74
4.6.2 Some Examples of Small Rank 76
4.6.3 Equivalence Classes of Alternating Trilinear Forms 78
4.6.4 Towards Explicit Evaluation of the Triple Cup Product 78
4.7 Towards Profinite Triple Symbols 80
4.7.1 Compatibility of Triple Symbols 80

Chapter 1

Introduction and Motivation

1.1 Arithmetic Topology

The field of Arithmetic Topology explores a series of interconnected analogies between number theory and topology, often colloquially called the *knots and primes analogy*. The analogy was first noticed by Mazur, Manin, and Mumford in the 1960s, and since then have been expanded upon by many others. Most notably, Morishita provided a systematic account of the various in the book [Mor24].

The heart of the analogy is that the embedding of a knot into a 3-manifold

$$S^1 \hookrightarrow M,$$

should be viewed as being analogous as the embedding of the spectrum of a finite field into the the spectrum of a number ring $\operatorname{Spec} \mathcal{O}_K$

$$\operatorname{Spec} \mathcal{O}_K/\mathfrak{p} = \operatorname{Spec} \mathbb{F}_q \hookrightarrow \operatorname{Spec} \mathcal{O}_K,$$

where $\mathfrak{p} \triangleleft \mathcal{O}_K$ is a prime ideal of the number ring $\mathcal{O}_K$, inducing an embedding of its finite residue field.

This analogy becomes clearer when the relevant arithmetic objects are viewed under the étale topology. The fundamental group of a knot is equal to $\pi_1(S^1) = \mathbb{Z}$, while the étale fundamental group of a field is equal to its absolute Galois group, and so

$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{F}_q) = \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}.$$

Moreover, the ring of integers of a number field $\mathcal{O}_K$ has étale cohomological dimension 3, with its top degree cohomology with $\mathbb{G}_m$ coefficients equal to

$$H^3_{\text{ét}}(\operatorname{Spec} \mathcal{O}_K, \mathbb{G}_m) = \mathbb{Q}/\mathbb{Z}.$$

The scheme $X = \operatorname{Spec} \mathcal{O}_K$ also satisfies a duality theorem known as Artin–Verdier duality, which should be considered as an arithmetic analogue of Poincaré duality for 3-manifolds.

Theorem 1.1 ([Mil06, Cor. 3.3])**.** There is a pairing given by cup product

$$\langle \cdot, \cdot \rangle : H^r(X, \mathbb{Z}/\ell\mathbb{Z}) \times H^{3-r}(X, \mu_\ell) \xrightarrow{\cup} H^3(X, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$$

which induces an isomorphism

$$H^{3-r}(X, \mu_\ell) \xrightarrow{\sim} H^{3-r}(X, \mathbb{Z}/\ell\mathbb{Z})^\vee.$$

1.1.1 Boundaries and Restricted Ramification

Let V_K denote a tubular neighbourhood of a knot K. The boundary ∂V_K is homotopic to $V_K \setminus K$, the removal of K from its tubular neighbourhood.

Moreover, the boundary ∂V_K of the tubular neighbourhood is homeomorphic to a torus, and its fundamental group lies in the exact sequence

$$0 \to \langle \alpha \rangle \to \pi_1(\partial V_K) \to \langle \beta \rangle \to 0,$$

where α and β refer to the meridian and longitude of the torus respectively.

In algebraic geometry, the completion $\operatorname{Spec} \mathcal{O}_{K_\mathfrak{p}}$ of the number ring $\mathcal{O}_K$ at a prime $\mathfrak{p}$ can be viewed as a thickening of the point $\mathfrak{p}$, and thus is analogous to the tubular neighbourhood V_K

Inverting the maximal ideal $\mathfrak{p}$ of the local ring $\mathcal{O}_{K_\mathfrak{p}}$ gives the local field $K_\mathfrak{p}$. Localisation can be thought of as removing the central knot $\operatorname{Spec} \mathbb{F}_q$ from $\operatorname{Spec} \mathcal{O}_{K_\mathfrak{p}}$, leaving us with the boundary of the tubular neighbourhood.

Moreover, the tame fundamental group $\pi_1^t(\operatorname{Spec} K_\mathfrak{p})$ lies in an exact sequence

$$1 \to I_{K_\mathfrak{p}} \to \pi_1(\operatorname{Spec} K_\mathfrak{p}) \to \langle \sigma \rangle \cong \widehat{\mathbb{Z}} \to 1,$$

where $I_{K_\mathfrak{p}}$ is the tame inertia subgroup generated by the monodromy $\tau \in K_\mathfrak{p}^t / K_\mathfrak{p}$ satisfying $\tau(\sqrt[n]{\pi}) = \zeta_n \sqrt[n]{\pi}$, and $\sigma \in \operatorname{Gal}(K_\mathfrak{p}^{\mathrm{ur}} / K_\mathfrak{p})$ is the Frobenius automorphism.

Let $L = K_1 \cup \cdots K_r$ be a link, this should be analogous to a finite set of primes S, and the link group $\pi_1(M \setminus L)$ should be viewed as analogous to the Galois group of the maximal extension of K that is unramified outside of S

$$\pi_1^{\text{ét}}(X \setminus S) = \pi_1^{\text{ét}}(\operatorname{Spec} \mathcal{O}_K[1/S]) = \operatorname{Gal}(K_S / K).$$

We should think of the objects $\mathcal{O}_K[1/S]$ and $\operatorname{Spec} \mathcal{O}_{K_\mathfrak{p}}$ as manifolds with boundary, with the boundary being (possibly unions of) 2-dimensional tori $\operatorname{Spec} K_\mathfrak{p}$.

To summarise, we have the following series of analogies between arithmetic and topology.

Arithmetic	Topology
Number Ring $\operatorname{Spec} \mathcal{O}_K$	3-Manifold M
Prime ideal $\mathfrak{p} \triangleleft \mathcal{O}_K$	Knot $S^1 \hookrightarrow M$
Artin–Verdier Duality	Poincaré Duality
Local Ring $\operatorname{Spec} \mathcal{O}_{K_\mathfrak{p}}$	Tubular Neighbourhood V_K
Local Field $\operatorname{Spec} K_\mathfrak{p}$	Boundary Torus ∂V_K
Monodromy τ	Meridian α
Frobenius σ	Longitude β
Galois Group with Restricted Ramification $\pi_1^{\text{ét}}(\operatorname{Spec} \mathcal{O}_K[1/S])$	Link Group $\pi_1(M \setminus L)$

1.1.2 Decomposition Theory of Knots and Primes

We illustrate the close analogy between topology and arithmetic by describing the decomposition theory of knots and primes in detail. We quickly recall the decomposition theory in arithmetic.

Decomposition Theory of Primes

Let L/K be an extension of number fields, and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then passing to the field extension we have that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_i|\mathfrak{p}$ are prime ideals of $\mathcal{O}_L$ that lie above $\mathfrak{p}$. We call e_i the ramification degree of $\mathfrak{P}_i$, and say that $\mathfrak{P}_i$ is unramified if $e_i = 1$.

On the other hand, quotienting by these prime ideals induces an extension of finite residue fields. Let us write $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ the residue class degree. Then it is known (e.g. see [Ser79, Chap I.4]) that

$$[L : K] = \sum_{i=1}^{r} e_i f_i.$$

In particular, of L/K is a Galois extension, then the Galois group acts transitively on the set of primes $\mathfrak{P}_i$, and so all the e_i's and f_i's are equal to each other, giving

$$[L : K] = efr.$$

Decomposition Theory of Knots

We first define a covering of 3-manifolds ramified over a link L. This definition is analogous to the definition of ramification in Riemann surfaces, but in 1 dimension higher.

Definition 1.2 (Ramified Covering, [Mor24, 2.1.13])**.** Let $L \hookrightarrow M$ be a link. A continuous map $f\colon N \to M$ of 3-manifolds is a *covering ramified over* L if

- The map $f|_{N\setminus f^{-1}(L)}\colon N \setminus f^{-1}(L) \to M \setminus L$ is a covering map.
- For each of $y \in f^{-1}(L)$, there exists and integer $e \in \mathbb{Z}$ and tubular neighbourhoods $D^2 \times I = U \ni y$, and $D^2 \times I = V \ni f(y)$ containing y and $f(y)$ respectively such that $f(U) = V$, and $f|_U = (z \mapsto z^e) \times \mathrm{id}$. (Here, we view D^2 as the complex unit disc.)

If $f|_{N\setminus f^{-1}(L)}\colon N \setminus f^{-1}(L) \to M \setminus L$ is moreover a Galois covering, then we say that f is a *ramified Galois covering*, and we write its Galois group as

$$\mathrm{Gal}(N/M) \coloneqq \mathrm{Gal}(N \setminus f^{-1}(L)/M \setminus L).$$

Suppose N/M is a Galois covering ramified over L, and let $K \in L$ be a component knot of the link L. Then the preimage $f^{-1}(K)$ will be a link in N, say

$$f^{-1}(K) = K_1 \cup \cdots \cup K_r.$$

The integer e from the definition will be fixed for each point $y \in K_i$ in one of these component knots. We will call this integer e_i the *ramification degree* of the knot K_i.

Let V_K denote a tubular neighbourhood of K, and write V_{K_i} for the connected component of $f^{-1}(V_K)$ which contains K_i.

We fix a basepoint $x \in \partial V_K$ on the boundary torus of V_K, in particular, we pick the tubular neighbourhood to be sufficiently thin so that $V_K \setminus K$ lies in $M \setminus L$. Then since f is a covering

map outside of L, the preimage of the basepoint x must have size n, where n is the degree of the covering map $f|_{N\setminus f^{-1}(L)}\colon N\setminus f^{-1}(L)\to M\setminus L$.

Let $G=\mathrm{Aut}(N\setminus f^{-1}(L)/M\setminus L)$ be the group of Deck transformations of the covering. We define the *decomposition group* of K_i to be the subgroup of G that fixes ∂V_{K_i}

$$D_{K_i}\coloneqq\{g\in G|g(\partial VK_i)=\partial VK_i\}.$$

We remark that if there exists $g\in G$ such that $g(\partial K_i)=\partial K_j$, then D_{K_i} is conjugate to D_{K_j}

$$D_{K_j}=gD_{K_i}g^{-1}.$$

Moreover, g induces a homeomorphism between ∂V_{K_i} and ∂V_{K_j}. In particular, an element $g\in D_{K_i}$ induces an automorphism of ∂V_{K_i}, and gives an isomorphism

$$D_{K_i}\cong\mathrm{Gal}(\partial V_{K_i}/\partial V_K).$$

But since $\partial V_{K_i}/\partial V_K$ is just a covering of tori, this group must be generated by the meridian α and the longitude β.

We define the *Inertia group* I_{K_i} to be the subgroup of D_{K_i} generated by the meridian α. We can also write the inertia group as the kernel of the homomorphism

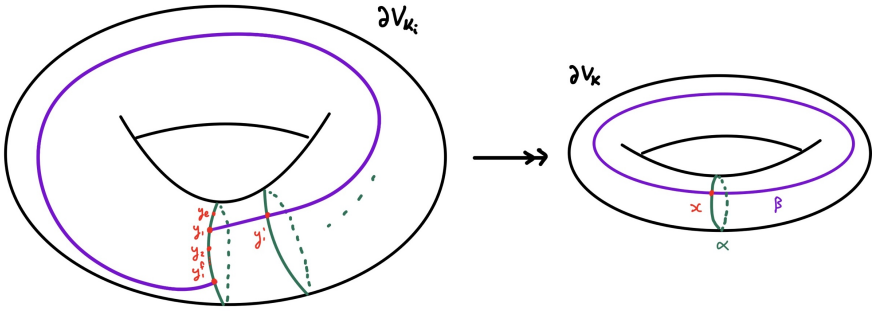
$$D_{K_i}\twoheadrightarrow\mathrm{Gal}(K_i/K).$$

We study the sizes of the decomposition and inertia groups by looking at the preimages of the basepoint $x\in\partial V_K$. Let us fix a preimage $y_1^0\in\partial V_{K_i}\cap f^{-1}(x)$, and write the orbit of y_1^0 under the action of the meridian α as

$$\{y_1,y_2,\dots,y_e\}.$$

This set has exactly size e_i, and thus the size of the inertia group is equal to the ramification degree $\#I_{K_i}=e_i$.

Now we consider the action of the longitude β, let us write $y_i^j\coloneqq\beta^m y_i$. Define the integer f_i to be the minimal m such that $y_1^m\in\{y_1,y_2,\dots,y_e\}$, this is called the *covering degree* of K_i/K.



It is easy to see that the orbit of y_1 under α and β has size e_if_i, and thus we have that

$$n=\sum_{i=1}^{r}e_if_i.$$

If additionally N/M is a ramified *Galois* covering, then the Galois group $\mathrm{Gal}(N/M)$ acts transitively on the set of preimages $f^{-1}(K)$, and thus all the e_i's and f_i's are equal, and thus

$$n=efr,$$

mirroring the arithmetic picture precisely.

1.2 Weil's Trichotomy

In number theory, number fields and function fields are closely related, as their ring of integers are both Dedekind domains. As such, many theorems about number fields have analogues in function fields, and vice versa, although it is often harder to move from function fields to number fields.

Let $X/\mathbb{F}_q$ be a smooth projective curve defined over a finite field. Weil believed [Wei05] that the function field $k(X)$ is an important intermediary bridging the gap between a number field K to the field of meromorphic functions $\mathbb{C}(\Sigma)$ of a Riemann Surface Σ.

Consider the base change of X to the algebraic closure $\overline{X} \coloneqq X \times_{\operatorname{Spec}\mathbb{F}_q} \operatorname{Spec}\overline{\mathbb{F}}_q$ is a curve over an algebraically closed field, we can think of $\overline{X}$ as being analogous to a Riemann surface Σ. Writing down the pushout diagram associated to $\overline{X}$

$$\begin{array}{ccc} \overline{X} & \hookrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec}\overline{\mathbb{F}}_q & \longrightarrow & \operatorname{Spec}\mathbb{F}_q, \end{array}$$

and remarking that the spectrum of an algebraically closed field is analogous to a point, the pushout diagram resembles the following diagram of manifolds

$$\begin{array}{ccc} \Sigma & \hookrightarrow & M \\ \downarrow & & \downarrow \\ 1 & \longrightarrow & S^1. \end{array}$$

In this diagram, M is not just a 3-manifold, but is a fibred 3-manifold over the circle S^1, with fibres being the surface Σ.

Moreover the 3-manifold M can be written as a mapping torus

$$M = \Sigma \times [0,1]/\sim$$

where the equivalence relation $\sim$ identifies $(x,0) \sim (f(x),1)$ via a diffeomorphism $f\colon \Sigma \to \Sigma$. This diffeomorphism f can be viewed as the monodromy action of a generator $\pi_1(S^1)$ on Σ.

In a similar manner, we note that $\pi_1(\operatorname{Spec}\mathbb{F}_q) \simeq \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by the Frobenius Fr_q, which acts on $\overline{X}$. Thus we can view the curve X as a 'mapping torus' with fibers $\overline{X}$

$$X \text{ ' = ' } \overline{X} \times [0,1]/\operatorname{Fr}_q .$$

On the other hand, one could ask if the spectrum of a number ring $\operatorname{Spec}\mathcal{O}_K$ is also analogous to a fibred 3-manifold. The number field case is much more subtle, as $\mathcal{O}_K$ does not possess a Frobenius action in the same way that the curve X does.

One of the motivations of Iwasawa's study of $\mathbb{Z}_p$ extensions of number fields is to define an analogue to the Frobenius action in the case of number fields ([Was97, p. 297], [Och23, p. 52]).

Let K_∞ denote the cyclotomic $\mathbb{Z}_p$ extension of K, and γ be a topological generator of the Galois group $\operatorname{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, then we should view the γ action as being analogous to the Frobenius action Fr_q on $\overline{X}$. In summary

Number Fields	Function Fields	Manifolds
Number Ring $\operatorname{Spec}\mathcal{O}_K$	Smooth Projective Curve $X/\mathbb{F}_q$	3-manifold M
$\mathbb{Z}_p$–extension $\operatorname{Spec}\mathcal{O}_{K[\mu_{p^\infty}]}$	Curve over Algebraic Closure $\overline{X}/\overline{\mathbb{F}}_q$	Riemann Surface Σ
γ action	Frobenius Action	Monodromy Action

1.3 Arithmetic Quantum Field Theory and Path Integrals

Witten proved as part of his Fields medal winning work in the 1980s that it is possible to compute topological invariants via path integrals coming from quantum field theory.

Let M be a d-dimensional manifold, and $\mathcal{F} \to M$ a fiber bundle on M. We define the *space of fields* on M to be

$$\mathcal{F}_M = \Gamma(M, \mathcal{F}).$$

A *classical theory* consists of an action functional

$$\mathcal{A} \colon \mathcal{F}_M \to \mathbb{C}.$$

As an example, if M is a *configuration space* consisting of all possible positions of a physical system, the fiber bundle $\mathcal{F}$ might be the cotangent bundle T^*M of M, which is the *phase space*, representing all possible positions and momenta of our system. In this setting, our classical action $\mathcal{A}$ would be the *Lagrangian* functional.

In a quantum field theory, one often considers integrals of the form

$$\int_{\mathcal{F}_M} e^{-\pi \mathcal{A}(\phi)} d\phi$$

When the theory is *topological*, this integral is a topological invariant of the manifold M, and is often denoted $Z(M)$, called the *partition function*. A path integral can also be defined on manifolds with boundary, in which case additional boundary conditions need to be considered. The partition function in this case would not yield a number, but instead a vector on the Hilbert space.

Axiomatising these properties, one can define a TQFT as a symmetric monoidal functor from the category of cobordisms Cob_n to the category of vector spaces. This axiomatisation is described in section 2.1.

Inspired by the analogies coming from Weil's trichotomy, Minhyong Kim and his collaborators initiated the study of arithmetic topological quantum field theories [Kim18; Chu+20].

Let X be either a smooth projective curve over a finite field, or the spectrum of a number ring. We can think of X as our manifold M.

Let A be a finite group and consider the space of principal A bundles on X

$$\mathcal{M}(A) \coloneqq \mathrm{Hom}_{\mathrm{cts}}(\pi_1(X), A)/A.$$

This can be thought of our arithmetic analogue of the fiber bundle $\mathcal{F}$. Upon defining a suitable action functional $\mathcal{A}$, the associated arithmetic path integral would take the form

$$\sum_{\rho \in \mathcal{M}} e^{2\pi i \mathcal{A}(\rho)}.$$

1.4 Outline of Thesis

In chapter 2, we describe the theory of the arithmetic Chern–Simons action for function fields. The chapter will closely follow the exposition of [Chu+20], where the authors define the arithmetic Chern–Simons action for number fields. The main result of this chapter is the proof of the decomposition formula, which provides a way to compute arithmetic Chern–Simons invariants explicitly via the difference between ramified global trivialisations and unramified local trivialisations.

Chapter 3 is a verbatim inclusion of the preprint [Che25]. In a topological quantum field theory, path integrals over a space $\mathcal{F}$ of sections of a fibration $M \times [0,1]/F \to S^1$ can in fact be computed by instead looking at the action of F on a Hilbert space $\mathcal{H}$ of functions as

$$\mathrm{Tr}(F|\mathcal{H}) = \int_{\mathcal{F}} e^{iA(\gamma)} d\gamma.$$

The main result of the chapter is an arithmetic analogue of the *Trace–Path integral formula*.

Theorem (Theorem 3.32)**.** Let J be the Jacobian of a genus g curve X over a finite field $\mathbb{F}_q$. Let ℓ be an odd prime satisfying $q \equiv 1 \pmod{\ell}$. If Fr_q acts semisimply on the $\mathbb{F}_\ell$-vector space $J[\ell]$, then we have the following equality

$$\mathrm{tr}(\mathrm{Fr}_q\,|\mathcal{H}) = \left(\frac{(-1)^g \det{}'(1-\mathrm{Fr}_q)\det(A)}{\ell}\right) \sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)},$$

where $\det{}'(1-\mathrm{Fr}_q)$ is the *regularised determinant* of the linear map $1-\mathrm{Fr}_q$ on vector space $J[\ell]$. That is, this is the determinant of $1-\mathrm{Fr}_q$ after quotienting the space $J[\ell]$ by its kernel.

The integral on the right hand side can be thought of as the path integral associated to *abelian arithmetic Chern–Simons theory*, while the arithmetic Hilbert space $\mathcal{H}$ is a space of global sections of the Theta bundle.

In chapter 4, we introduce linking numbers and multiple linking numbers in topology and arithmetic. Recent work by Dohyeong Kim and Masanori Morishita in [KM25] interprets the triple linking numbers of primes as a cohomological construction instead, which in the unramified case can be interpreted as an arithmetic Chern–Simons action of *Massey type* [Kim25]. After detailing the theory behind triple symbols of characters and their relation to arithmetic Chern–Simons actions, the chapter concludes with some ongoing work towards computing explicitly the path integral associated to the Massey type Chern–Simons action, and towards defining a characteristic zero profinite arithmetic linking number.

Chapter 2

Arithmetic Chern–Simons Actions for Function Fields

2.1 Introduction to Arithmetic Topological Quantum Field Theories

Define the category of cobordisms Cob_n to have objects being closed oriented $n-1$ manifolds N, and morphisms between N_1, N_2 being an oriented n manifold M with boundary $\partial M = N_1 \sqcup N_2$. Morphisms $M_1 \colon N_1 \to N_2$ and $M_2 \colon N_2 \to N_3$ can be composed by gluing M_1 and M_2 along the boundary component N_2. The category Cob_n is symmetric monoidal by taking the monoidal product to be the disjoint union.

A 3-dimensional topological quantum field theory can be viewed as a symmetric monoidal functor to the category of finite dimensional vector spaces over a field k

$$Z \colon \mathrm{Cob}_3 \to \mathrm{Vect}_k.$$

In general, the target category can be any symmetric monoidal category. This functor Z would send 2-manifolds to vector spaces. In particular, since the empty 2-manifold $\emptyset$ is the unit of the Cob_3, it must be taken to the unit 1-dimensional vector space $k \in \mathrm{Vect}_k$.

Let M be a closed 3-manifold without boundary, then we can write $\partial M = \emptyset \sqcup \emptyset$, and view $M \in \mathrm{End}_{\mathrm{Cob}_3}(\emptyset)$ as an endomorphism of $\emptyset$. Then, we must have $Z(M) \in \mathrm{End}_k(k)$.

Any endomorphisms of the 1-dimensional vector space k is precisely equal to the multiplication of some scalar, thus the TQFT would take the manifold M to a number

$$Z(M) = \lambda \in k.$$

On the other hand, suppose M is instead a 3-manifold with boundary $\partial M = N_1 \sqcup N_2$. Let V, W be $Z(N_1), Z(N_2)$ respectively, then $Z(M)$ should be a linear map

$$Z(M) \colon V \to W.$$

Of course, the splitting $N_1 \sqcup N_2$ is somewhat arbitrary, and we can instead view the boundary of M as

$$\partial M = \emptyset \sqcup (\overline{N}_1 \sqcup N_2),$$

where $\overline{N}_1$ refers to N_1 but with its orientation reversed. Then

$$Z(\overline{N}_1 \sqcup N_2) = V^\vee \otimes W.$$

In which case, we can view the linear map $Z(M)\colon k \to V^\vee \otimes W$ as being uniquely determined by the image of 1, and thus $Z(M)$ can be thought of a vector of $V^\vee \otimes W$.

This makes sense because a vector $\sum f_i \otimes w_i \in V^\vee \otimes W$ induces a linear map $V \to W$ via

$$v \mapsto \sum f_i(v) w_i,$$

and this induces an identification $\mathrm{Hom}_k(V, W) \simeq V^\vee \otimes W$.

In summary, a 3-dimensional TQFT should make the following assignments

3-manifold without boundary	$\rightsquigarrow$	Number $\lambda \in k$
2-manifold without boundary	$\rightsquigarrow$	Vector space V
3-manifold with boundary	$\rightsquigarrow$	Linear map $V \to W$, or Vector in $V^\vee \otimes W$.

The arithmetic Chern–Simons action was defined by Minhyong Kim and his collaborators in [Kim20; Chu+20] in the the number field setting where $X = \operatorname{Spec} \mathcal{O}_K$. While the analogous definitions and results in the function field setting are practically the same, in this chapter we give the definitions and main results analogous to [Chu+19] in the setting of function fields.

Our definition of arithmetic Chern–Simons theory will make the following assignments

$X/\mathbb{F}_q$ smooth projective curve, or $X = \operatorname{Spec} \mathcal{O}_K$ number ring	$\rightsquigarrow$	Number in $\mathbb{Z}/n\mathbb{Z}$
Boundary of Local Fields $\bigsqcup \operatorname{Spec} K_v$	$\rightsquigarrow$	$\mathbb{Z}/n\mathbb{Z}$–Torsor
$U = X \setminus S$ for a finite set of places S	$\rightsquigarrow$	Element of Torsor

There is a small discrepancy since we are assigning to the 2-manifold $\operatorname{Spec} K_v$ a $\mathbb{Z}/n\mathbb{Z}$–torsor rather than a vector space, but one can move between torsors and vector spaces. Suppose that our base field contains the nth roots of unity μ_n, then $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ as Galois modules and sheaves. However, any μ_n torsor naturally induces a $\mathbb{G}_m$ torsor, which is just a line bundle with its zero section removed.

2.2 The Arithmetic Chern–Simons Action without Boundary

Let $X = C/\mathbb{F}_q$ be a smooth projective curve, and $\pi = \pi_1^{\text{ét}}(C, b)$ be the étale fundamental group of C, with basepoint $b\colon \operatorname{Spec} \overline{\mathbb{F}}_q \hookrightarrow C$.

We fix n which is coprime to q and suppose that $\mathbb{F}_q$ contains the nth roots of unity μ_n. (i.e. $q \equiv 1 \mod n$). Then we can fix an isomorphism $\zeta_n\colon \mu_n \to \mathbb{Z}/n\mathbb{Z}$ which in turn induces an isomorphism

$$\zeta_{n,*}\colon H^i(C, \mu_n) \simeq H^i(C, \mathbb{Z}/n\mathbb{Z}).$$

From [Den84, 1.5], there exists a canonical trace isomorphism

$$\mathrm{tr}\colon H^3(C, \mathbb{G}_m) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Lemma 2.1. The following sequence of étale sheaves on C is exact

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{(\cdot)^n} \mathbb{G}_m \longrightarrow 0.$$

Proof. The injectivity of $\mu_n \to \mathbb{G}_m$ is clear, so it suffices to show that the map $(\cdot)^n\colon \mathbb{G}_m \to \mathbb{G}_m$ is surjective as étale sheaves.

Let $U \to C$ be an étale map. Without loss of generality we can assume $U = \operatorname{Spec} R$ is affine since we can always restrict to an affine étale neighbourhood. For $s \in \mathbb{G}_m(U) \cong R^\times$, there is an étale cover $U' = \operatorname{Spec} R' \to \operatorname{Spec} R$ where R' is given by adjoining an nth root of s to R, this is étale since n is coprime to q. Then $s|_{U'}$ is in the image of $(\cdot)^n \colon \mathbb{G}_m(U') \to \mathbb{G}_m(U')$. Thus $(\cdot)^n$ is a surjective map of étale sheaves. □

Using the above exact sequence and the fact that $H^2(C, \mathbb{G}_m) = 0$ from [Den84, 1.1] we can conclude that

$$H^3(C, \mathbb{Z}/n\mathbb{Z}) \simeq H^3(C, \mu_n) \simeq \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Fix a finite group A, called the *gauge group*, and a class $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$. We consider the set of isomorphism classes of principal A-bundles over C, which is given by

$$\mathcal{M}(A) \coloneqq \operatorname{Hom}_{\mathrm{cont}}(\pi, A)/A.$$

Where A acts on the Hom set by conjugation. Given an isomorphism class $[\rho] \in \mathcal{M}(A)$, we can pullback the class c to obtain

$$\rho^*(c) \in H^3(\pi, \mathbb{Z}/n\mathbb{Z}).$$

Note that $\rho^*(c)$ depends only on the isomorphism class of ρ in $\mathcal{M}(A)$, since conjugating c by an element in A gives the same cohomology class in $H^3(A, \mathbb{Z}/n\mathbb{Z})$ (see [Mil20, II.1.27(d)]), and thus pulling back along ρ would give the same cohomology class in $H^3(\pi, \mathbb{Z}/n\mathbb{Z})$.

Finally, from the Hochschild–Serre spectral sequence there is a map

$$j^3 : H^3(\pi, \mathbb{Z}/n\mathbb{Z}) \to H^3(C, \mathbb{Z}/n\mathbb{Z}).$$

Definition 2.2. Given a gauge group A and a cohomology class c, we define the arithmetic Chern–Simons functional without boundary to be the the composition of the maps

$$\mathrm{CS}_c \colon \mathcal{M}(A) \xrightarrow{\rho^*} H^3(\pi, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{j^3} H^3(C, \mathbb{Z}/n\mathbb{Z}) \overset{\zeta_*}{\cong} H^3(C, \mu_n) \xrightarrow{\mathrm{tr}} \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

2.3 The Arithmetic Chern–Simons with Boundary

We keep the notation from above. Let S be a finite set of places (scheme-theoretic points) in C. Let $\pi_S \coloneqq \pi_1^{\text{ét}}(C \setminus S, b)$ and for a point $v \in S$, we denote by C_v the completion of C at the place v and we define $\pi_v \coloneqq \pi_1^{\text{ét}}(C_v) \cong \operatorname{Gal}(\overline{\kappa(C)}_v/\kappa(C)_v)$.

There are maps $i_v \colon \pi_v \to \pi_S$ induced by choices of embeddings $\overline{\kappa(C)} \hookrightarrow \overline{\kappa(C)}_v$. There is also a natural quotient map $\kappa_S \colon \pi_S \to \pi$.

We define

$$Y_S(A) \coloneqq \operatorname{Hom}_{\mathrm{cts}}(\pi_S, A); \quad Y_S^{\mathrm{loc}}(A) \coloneqq \prod_{v \in S} \operatorname{Hom}_{\mathrm{cts}}(\pi_v, A)$$

and denote by $\mathcal{M}_S(A)$ and $\mathcal{M}_S^{\mathrm{loc}}(A)$ be the category with objects being elements of $Y_S(A)$ and $Y_S^{\mathrm{loc}}(A)$ respectively, and morphisms being given by the conjugation action of A. Since all morphisms are invertible, these categories are groupoids, called the *action groupoid*.

There is a restriction functor

$$r_S \colon \mathcal{M}_S(A) \to \mathcal{M}_S^{\mathrm{loc}}(A),$$

where an object $\rho \colon \pi_S \to A$ is restricted at every place in S to obtain the collection:

$$r_S(\rho) = (\rho \circ i_v)_{v \in S}.$$

We are now ready to construct the Chern-Simons Action with boundary. We introduce the following notation for continuous cochains, cocycles, and coboundaries respectively at every

place v

$$C_S^i \coloneqq \prod_{v\in S} C^i(\pi_v, \mathbb{Z}/n\mathbb{Z}); \quad Z_S^i \coloneqq \prod_{v\in S} Z^i(\pi_v, \mathbb{Z}/n\mathbb{Z}); \quad B_S^i \coloneqq \prod_{v\in S} B^i(\pi_v, \mathbb{Z}/n\mathbb{Z}),$$

where we note that $B_S^i \subset Z_S^i \subset C_S^i$.

Let c be a fixed cocycle in $Z^3(A, \mathbb{Z}/n\mathbb{Z})$. Given $\rho_S \coloneqq (\rho_v)_{v\in S}$ we can define

$$c \circ \rho_S = (c \circ \rho_v)_{v\in S} \in Z_S^3.$$

Consider the following exact sequence induced by the coboundary map $d\colon C_S^2 \to Z_S^3$,

$$0 \to H_S^2 \coloneqq Z_S^2/B_S^2 \to C_S^2/B_S^2 \xrightarrow{d} B_S^3 = Z_S^3 \to 0.$$

Then we note that for $c \circ \rho_S \in Z_S^3$, its preimage under d

$$H(\rho_S) \coloneqq d^{-1}(c \circ \rho_S)/B_S^2 \subset C_S^2/B_S^2$$

is a torsor for the group

$$H_S^2 = \prod_{v\in S} H^2(\pi_v, \mathbb{Z}/n\mathbb{Z}) \xrightarrow[\sim]{(\mathrm{inv}_v)_{v\in S}} \prod_{v\in S} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

The group H_S^2 should be thought of as the space of all local boundary trivialisations.

Via the sum map $\Sigma\colon \prod_{v\in S} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, we can push out the torsor $H(\rho_S)$ to obtain an $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ torsor

$$L(\rho_S) \coloneqq \Sigma_*[H(\rho_S)].$$

where L is a map from $Y_S^{\mathrm{loc}}(A) \to \mathrm{TORS}(\frac{1}{n}\mathbb{Z}/\mathbb{Z})$.

Proposition 2.3. The map L extends to a functor

$$L\colon \mathcal{M}_S^{\mathrm{loc}}(A) \to \mathrm{TORS}(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z}),$$

i.e. conjugations of ρ_S by an element in A give rise to a morphism of their corresponding torsors.

Proof. To show this fact we first show that H can be extended to a functor $H\colon \mathcal{M}_S^{loc}(A) \to \mathrm{TORS}(H_S^2)$.

Let $a = (a_v)_{v\in S} \in A^S$, and let Ad_{a_v} be the conjugation action on A by a_v. Then

$$c \circ \mathrm{Ad}_a \coloneqq (c \circ \mathrm{Ad}_{a_v})_{v\in S} \in \prod_{v\in S} Z^3(A, \mathbb{Z}/n\mathbb{Z}).$$

By [Chu+20, Appendix A], for each place v there exists $h_{a_v} \in C^2(A, \mathbb{Z}/n\mathbb{Z})/B^2(A, \mathbb{Z}/n\mathbb{Z})$ such that $c \circ \mathrm{Ad}_{a_v} = c + dh_{a_v}$ and $h_{a_v b_v} = h_{a_v} \circ \mathrm{Ad}_{b_v} + h_{b_v}$.

Given $a\colon \rho_S \to \rho'_S = \mathrm{Ad}_a \circ \rho_S$ a morphism on $\mathcal{M}_S^{loc}(A)$, we let the functor H take it to the morphism $H(a)\colon H(\rho_S) \to H(\rho'_S)$ given by sending $x \in d^{-1}(c \circ \rho_S)/B_S^2$ to

$$x \mapsto x' \coloneqq x + h_a \circ \rho_S = x + (h_{a_v} \circ \rho_v)_{v\in S}.$$

We check that this map is well defined

$$(dx')_v = (dx)_v + d(h_{a_v} \circ \rho_v) = c \circ \rho_v + (dh_{a_v}) \circ \rho_v = (c + dh_{a_v}) \circ \rho_v = c \circ \mathrm{Ad}_{a_v} \circ \rho_v,$$

and thus $dx' = (c \circ \mathrm{Ad}_{a_v} \circ \rho_v)_{v\in S} = c \circ \rho'_S$, and so $x' \in d^{-1}(c \circ \rho'_S)/B^2_S = H(\rho'_S)$, so $H(a)$ is indeed a well defined morphism in the category H^2_S).

Moreover, we check that $H(a)H(b) = H(ab)$. We compute

$$\begin{aligned}(H(a) \circ H(b))(x) &= H(a)(x + h_b \circ \rho_S)\\ &= x + h_b \circ \rho_S + h_a \circ (\mathrm{Ad}_b \circ \rho_S)\\ &= x + (h_b + h_a \circ \mathrm{Ad}_b) \circ \rho_S\\ &= x + h_{ab} \circ \rho_S\\ &= H(ab)(x).\end{aligned}$$

Thus H is a functor. Since the pushout Σ_* is also a functor, their composition $L = \Sigma_* \circ H$ is indeed a functor from $\mathcal{M}^{\mathrm{loc}}_S(A)$ to $\mathrm{TORS}(\frac{1}{n}\mathbb{Z}/\mathbb{Z})$. □

Additionally, by composing with the restriction map $r_S \colon \mathcal{M}_S(A) \to \mathcal{M}^{\mathrm{loc}}_S(A)$ we obtain a functor $L^{\mathrm{glob}} \colon \mathcal{M}_S(A) \to \mathrm{TORS}(\frac{1}{n}\mathbb{Z}/\mathbb{Z})$.

Lemma 2.4. Let $\rho \in \mathcal{M}_S(A)$ and $a \in \mathrm{Aut}(\rho)$. Then

$$L^{\mathrm{glob}}(a) = \mathrm{id}\,.$$

Proof. By definition, $a \in \mathrm{Aut}(\rho)$ means that $\mathrm{Ad}_a \circ \rho = \rho$. And since

$$c \circ \rho = c \circ \mathrm{Ad}_a \circ \rho = (c + dh_a) \circ \rho = c \circ \rho + dh_a \circ \rho,$$

it follows that $dh_a \circ \rho = 0$. This means that $h_a \circ \rho \in H^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$. By the Hasse principle [NSW08, 8.1.17] we know that $\sum_v (h_a \circ \rho)_v = 0$. And thus for any $x \in L^{\mathrm{glob}}(a)(\rho)$

$$\begin{aligned}L^{\mathrm{glob}}(a)(x) &= \Sigma_* \circ H \circ r_S(a)(x)\\ &= \Sigma_*(H(a)((x_v)_{v\in S}))\\ &= \Sigma_*((x_v)_v + (h_a \circ \rho)_v)\\ &= \Sigma_*(x_v)_v + \sum_v (h_a \circ \rho)_v\\ &= x\end{aligned}$$

Thus $L^{\mathrm{glob}}(a)$ is the identity map. □

Finally, we define the CS action with boundary. As with the previous section, we fix a cocycle $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$. By [NSW08, 8.1.18] we have $H^3(\pi_S, \mathbb{Z}/n\mathbb{Z}) = 0$, so given $\rho \in M_S(A)$ the cocycle $c \circ \rho \in B^3(\pi_S, \mathbb{Z}/n\mathbb{Z}) \subset C^3(\pi_S, \mathbb{Z}/n\mathbb{Z})$ is in fact a coboundary, and thus there exists a cocycle $\beta \in C^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$ such that

$$c \circ \rho = d\beta.$$

In particular $i^*_S(\beta) \coloneqq (\beta \circ i_v)_{v\in S}$ is an element of $d^{-1}(c \circ \rho)/B^2_S$, and thus $\Sigma(i^*_S(\beta))$ is an element of the torsor $L^{\mathrm{glob}}(\rho)$. We define this element to be the Chern-Simons action $\mathrm{CS}_c(\rho)$.

Definition 2.5. Keeping the notation as above, define

$$\mathrm{CS}_c(\rho) = \Sigma(i^*_S(\beta)) \in L^{\mathrm{glob}}(\rho).$$

Proposition 2.6. The definition of $\mathrm{CS}_c(\rho)$ is independent of the choice of β.

Proof. Suppose $\beta' = \beta + z$ is a different choice of β, where z is a cocycle in $Z^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$. But the contribution of z vanishes when β' is mapped to $L(\rho \circ i_v)_{v\in S}$ because of the reciprocity law

$$0 \to H^2(\pi_S, \mathbb{Z}/n\mathbb{Z}) \to H^2_S \xrightarrow{\sum_v \mathrm{inv}_v} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0.$$

Thus $CS_c(\rho)$ is independent of the choice of β as desired. □

Additionally, suppose $a\colon \rho_1 \to \rho_2$ is a morphism in $\mathcal{M}_S(A)$, and $\beta_1, \beta_2 \in C^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$ are trivialisations such that $c \circ \rho_i = d\beta_i$. Then $H(a)(\beta_1)$ will also satisfy $c \circ \rho_2 = d(H(a)(\beta_1))$, and thus $H(a)(\beta_1)$ and β_2 differ by an element in $Z^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$. Thus we have the relation

$$L(a)(\mathrm{CS}_c(\rho_1)) = \mathrm{CS}_c(\rho_2).$$

Thus the assignment of $\mathrm{CS}_c(\rho)$ forms an *invariant section* for the functor L^{glob}, and we can define a class

$$\mathrm{CS}_c([\rho]) \in L^{\mathrm{inv}}([\rho]).$$

Where $L^{\mathrm{inv}}([\rho])$ is the $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ torsor of invariant sections for the functor L^{glob}. This means that an element $(s_{\rho'})_{\rho' \in [\rho]} \in L^{\mathrm{inv}}([\rho])$ is a sequence of elements $s_{\rho'} \in L^{\mathrm{glob}}(\rho')$ that are equivariant under morphisms $a\colon \rho_1 \to \rho_2$ in $\mathcal{M}_S(A)$.

We can also think of $L^{\mathrm{inv}}([\rho])$ as the limit of $L^{\mathrm{glob}}(\rho')$ over the indexing category $[\rho]$

$$L^{\mathrm{inv}}([\rho]) \coloneqq \varprojlim_{\rho' \in [\rho]} L^{\mathrm{glob}}(\rho').$$

2.4 Facts about Compactly Supported Étale Cohomology

The decomposition formula in the next section makes use of the theory of compactly supported étale cohomology. For completeness, this section gives a general introduction to the theory of étale cohomology with compact support for both number fields and function fields.

In this section, let F be a global number or function field, with $X = \operatorname{Spec} \mathcal{O}_F$ if F is a number field, and otherwise X is the connected smooth complete projective curve with F as its function field.

Let $\mathcal{G}$ be a locally constant sheaf on X, and T be a set of places of F containing the primes dividing the order of $\mathcal{G}$. If X is a function field then we assert that the characteristic of X does not divide the order of $\mathcal{G}$. We write $U = X \setminus T$.

2.4.1 Compactly Supported Cocycles

For each place $v \in T$ there is a localisation map of cochains

$$\mathrm{loc}_v\colon C^r(U, \mathcal{G}) \to C^r(F_v, \mathcal{G}_v).$$

Consider the map which is the direct sum of local restrictions to the boundary

$$\mathrm{loc}\colon C^\bullet(U, \mathcal{G}) \to \bigoplus_{v \in T} C^\bullet(F_v, \mathcal{G}_v).$$

The mapping cone associated to the map loc is the chain complex

$$\mathrm{cone}^\bullet(\mathrm{loc}) = C^\bullet(U, \mathcal{G})[1] \oplus \bigoplus_{v \in T} C^\bullet(F_v, \mathcal{G}_v)$$

with differential map given by

$$d(g,(z_v)_{v\in T}) = (-dg,(-g_v+dz_v)_v).$$

Here, we write g_v for $\mathrm{loc}_v\, g$, the restriction of g to F_v.

The étale cohomology with compact support is defined to be the cohomology of the mapping cone shifted by -1

$$H^r_c(U,\mathcal{G}) \coloneqq H^r(\mathrm{cone}^\bullet(\mathrm{loc})[-1]).$$

Using this definition, we can give an explicit interpretation of compact cocycles

$$d(g,(z_v)_v) = 0 \iff dg = 0 \text{ and } dz_v = g_v.$$

In other words, specifying a cocycle in $Z^r_c(U,\mathcal{G})$ is equivalent to to specifying a cocycle $c \in Z^r(U,\mathcal{G})$ and cochains $z_v \in C^{r-1}(F_v,\mathcal{G}_v)$ trivialising g_v, so that $dz_v = g_v$.

2.4.2 Cup Products between Non-Compact and Compact Cohomology

Suppose we have already defined cup products on non-compact étale/flat cochains. In this subsection we make sense of the cup product

$$H^r(U,\mathcal{F}) \times H^s_c(U,\mathcal{G}) \xrightarrow{\cup} H^{r+s}_c(U,\mathcal{F}\times\mathcal{G}).$$

Let $f \in Z^r(U,\mathcal{F})$ be a cocycle representing a class in $H^r(U,\mathcal{F})$, and $(g,(z_v)_v)$ be a cocycle represententing a class in $H^s_c(U,\mathcal{G})$. To define the cup product between the cocycles want a cocycle for $H^{r+s}_c(U,\mathcal{F}\times\mathcal{G})$.

Naively we consider simply cupping the elements directly by taking $f\cup g \in Z^{r+s}(U,\mathcal{F}\times\mathcal{G})$ and $f|_v \cup z_v \in C^{r+s-1}(U,\mathcal{F}\times\mathcal{G})$.

Notice that

$$d(f|_v\cup z_v) = df|_v\cup z_v + (-1)^r f|_v \cup dz_v = (-1)^r f|_v \cup dz_v$$

Thus we can define the cup product to be the cocycle:

$$f\cup(g,(z_v)_v) \coloneqq (f\cup g,((-1)^r f|_v\cup z_v)_v)$$

Proposition 2.7. The above map of cocycles induces a well defined map of cohomologies.

Proof. It suffices to show that if one of f or $(g,(z_v)_v)$ is a coboundary and the other is a cocyle, then their cup product is also a coboundary.

Suppose $f = dh$ is a coboundary, then

$$\begin{aligned} f\cup(g,(z_v)_v) &= (dh\cup g,((-1)^r dh|_v\cup z_v)_v)\\ &= (d(h\cup g),((-1)^r d(h|_v\cup z_v) + h|_v\cup g_v)_v)\\ &= d(-h\cup g,((-1)^r h|_v\cup z_v)_v)\end{aligned}$$

is a coboundary.

On the other hand suppose that $(g,(z_v)_v) = d(l,(w_v)_v) = (-dl,(-l_v+dw_v)_v)$, then

$$\begin{aligned} f\cup(g,(z_v)_v) &= (-f\cup dl,(-f_v\cup l_v + f_v\cup dw_v)_v)\\ &= ((-1)^r d(f\cup l),(-f_v\cup l_v + (-1)^{r-1}d(f|_v\cup w_v))_v)\\ &= (-1)^{r-1}d(f\cup l,(f|_v\cup w_v)_v)\end{aligned}$$

is also a coboundary. Thus the cup product defined above factors through the cohomology and defines a pairing between non-compact and compact cohomology. □

2.4.3 Invariant Map of a Compact Cohomology Class

In this subsection we specialise to the case where $\mathcal{G} = \mu_n$. It is known from [Mil06, II.2.6] that there is an isomorphism coming from the invariant map

$$\mathrm{inv}\colon H^3_c(U, \mathbb{G}_m) \to \mathbb{Q}/\mathbb{Z}.$$

From the long exact sequence coming from compact support cohomology,

$$\bigoplus_{v\in T} H^2(F_v, \mu_n) \to H^3_c(U, \mu_n) \to H^3(U, \mu_n),$$

we know that $H^3(U, \mu_n) = 0$ [Mil06, II.2.2], so there is a surjective map

$$\bigoplus_{v\in T} H^2(F_v, \mu_n) \to H^3_c(U, \mu_n) \to 0.$$

This surjective map is given by sending the cocycles $(z_v)_v \in \bigoplus_{v\in T} H^2(F_v, \mu_n)$ to the compact cocycle $(0, (z_v)_v) \in H^3_c(U, \mu_n)$. The invariant map on H^3_c commutes with the sum of local invariant maps inv_v, i.e. this triangle commutes

$$\begin{array}{ccc} \bigoplus_{v\in T} H^2(F_v, \mu_n) & \longrightarrow & H^3_c(U, \mu_n) \\ & \searrow^{\sum_v \mathrm{inv}_v} & \downarrow \mathrm{inv} \\ & & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Thus a cocycle $(0, (z_v)_v)$ would get sent to $\sum_v \mathrm{inv}_v z_v$ under the invariant map.

Now we want to compute the invariant map of a general compact cocycle, say $(g, (z_v)_v) \in Z^3_c(U, \mu_n)$. Since $H^3(U, \mu_n) = 0$, there is a global trivialising cochain, say $w \in C^2(U, \mu_n)$ such that $dw = g$.

Then if we write $w_v = \mathrm{loc}_v w$, we notice that $(g, (w_v)_v) = d(w, (0)_v) \in B^2_c(U, \mu_n)$ is a compact coboundary. This means we can subtract by this coboundary to get another cocycle in the same compact cohomology class

$$(g, (z_v)_v) \sim (g, (z_v)_v) - (g, (w_v)_v) = (0, (z_v - w_v)_v).$$

Thus we can compute the invariant map of a class in $H^3_c(U, \mu_n)$ in the following manner.

Proposition 2.8. Suppose a class in $H^3_c(U, \mu_n)$ is represented by the cocycle $(g, (z_v)_v)$, let $w \in C^2(U, \mu_n)$ be a global trivialisation of g. Then

$$\mathrm{inv}(g, (z_v)_v) = \sum_{v\in T} \mathrm{inv}_v(z_v - w_v).$$

Proof. This follows from

$$\mathrm{inv}(g, (z_v)_v) = \mathrm{inv}(0, (z_v - w_v)_v) = \sum_{v\in T} \mathrm{inv}_v(z_v - w_v).$$

□

2.5 The Decomposition Formula

In practice, the arithmetic Chern-Simons invariant $\mathrm{CS}_c(\rho)$ can be hard to compute, even in the case without boundary. The decompostion formula shows that it is possible to express the Chern–Simons action as the difference between the unramified local trivialisations and a ramified global trivialisation of the cocycle $\rho^*(c)$. We retain the assumptions of previous sections, where $X/\mathbb{F}_q$ is a smooth projective curve, with $\mu_n \subset \mathbb{F}_q$.

The decomposition formula can be viewed as an arithmetic analogue of gluing formulas in topological quantum field theories, where a 3-manifold without boundary M can be decomposed into two 3-manifolds with boundary $M = M_1 \cup_N M_2$, and the value of the partition function on $Z(M)$ can be computed by computing $Z(M_1)$ and $Z(M_2)$ and composing the respective linear maps obtained.

Definition 2.9 (Local Unramified Chern-Simons Action)**.** Given $(\rho\colon \pi \to A) \in \mathcal{M}(A)$, we can precompose this with the map $\pi_v^{ur} \to \pi$ at a place v, to obtain the representation

$$\rho_v^{ur}\colon \pi_v^{\mathrm{ur}} \to \pi \xrightarrow{\rho} A.$$

Noting that by [NSW08, Prop 1.7.7], $H^3(\pi_v^{ur}, \mathbb{Z}/n\mathbb{Z}) = H^3(\widehat{\mathbb{Z}}, \mathbb{Z}/n\mathbb{Z}) = 0$, we see that $c \circ \rho_v^{ur} \in H^3(\pi_v^{ur}, \mathbb{Z}/n\mathbb{Z})$ must have a trivialisation $\beta_v \in C^2(\pi_v^{ur}, \mathbb{Z}/n\mathbb{Z})$, where

$$c \circ \rho_v^{ur} = d\beta_v.$$

Composing with the inflation map $\inf\colon C^i(\pi_v^{ur}, \mathbb{Z}/n\mathbb{Z}) \to C^i(\pi_v, \mathbb{Z}/n\mathbb{Z})$ we get a cochain in $C^2(\pi_v, \mathbb{Z}/n\mathbb{Z})$ that we will also call by abuse of notation β_v, such that $c \circ \rho_v = d\beta_v$. This allows us to associate an element

$$\sum(\beta_v)_{v\in S} \in L([r_S(\rho \circ \kappa_S)]).$$

Where we recall that $\kappa_S\colon \pi_S \to \pi$ is the quotient map.

Theorem 2.10 (Decomposition Formula)**.** Fix a finite gauge group A and $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$. Then for any class $[\rho] \in \mathcal{M}(A)$ and any set of places S of X, we have the formula

$$\mathrm{CS}_c([\rho]) = \sum_{v\in S}(\beta_v) - \mathrm{CS}_c([\rho \circ \kappa_S]).$$

We note that in the statement of this theorem, neither $\sum_{v\in S}(\beta_v)$ nor $\mathrm{CS}_c([\rho\circ\kappa_S])$ are elements of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, but rather they are elements of the $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ torsor $L([r_S(\rho \circ \kappa_S)])$. And as such, the *difference* of these two elements will indeed be an element of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Proof. For each place $v \in S$, let $I_v \subset \pi_v$ be the inertia subgroup of π_v. We once again fix natural homomorphisms

$$\kappa_S\colon \pi_S \to \pi, \quad \kappa_v\colon \pi_v \to \pi,$$

and denote by ρ_S and ρ_v the composition of κ_S and κ_v with $\rho \in \mathrm{Hom}(\pi, M)$ respectively.

Recalling that $j^i\colon H^i(\pi, \mu_n) \to H^i(X, \mu_n)$ is the map from group cohomology to étale cohomology coming from the Hochschild-Serre Spectral sequence, and that $c \in H^3(A, \mathbb{Z}/n\mathbb{Z}) \simeq H^3(A, \mu_n)$. Let us define the class

$$z = j^3 \circ \rho^*(c) \in H^3(X, \mu_n).$$

Since $H^3(X, \mu_n) \simeq H^3_c(U, \mu_n)$, we wish to find a representation of the cocycle z via a compactly supported cocycle in $Z^3_c(U, \mu_n)$.

Let w be a cocycle representing $\rho^*(c) \in H^3(\pi, \mu_n)$. Since $\pi = \pi_1^{\text{ét}}(X, b)$ is unramified, the cochain $\kappa_v^*(w) \in Z^3(\pi_v, \mu_n)$ must in fact come from a cocycle over the quotient π_v/I_v. In other

words it must lie in the image of the map

$$Z^3(\pi_v/I_v, \mu_n) \to Z^3(\pi_v, \mu_n).$$

However, $\pi_v/I_v \simeq \widehat{\mathbb{Z}}$ has cohomological dimension 1 [NSW08, 1.7.7], and thus $H^3(\pi_v/I_v, \mu_n) = 0$. Hence we can choose cocycles

$$b_{-,v} \in Z^2(\pi_v/I_v, \mu_n)$$

such that

$$db_{-,v} = \kappa_v^*(w)|_{\pi_v/I_v}.$$

Furthermore, since $H^2(\pi_v/I_v, \mu_n) = 0$, any two choices for $b_{-,v}$ must differ by an element of $Z^2(\pi_v/I_v) = B^2(\pi_v/I_v)$. Thus $b_{-,v}$ is unique up to a class in $C^2(\pi_v/I_v)/B^2(\pi_v/I_v)$, this precisely defines an element in the torsor $H(\rho \circ \kappa_v)$, corresponding to the local unramified trivialisation β_v defined in definition 2.9.

We can lift each of these cocycles to obtain a cocycle $b_{-,v} \in C^2(\pi_v, \mu_n)$.

Thus z can be represented by the compact cocycle

$$(\kappa_S^*(w), (b_{-,v})_{v \in S}).$$

On the other hand, since $H^3(U, \mu_n) = H^3(\pi_S, \mu_n) = 0$, there must exist a global cochain $b_+ \in C^2(\pi_S, \mu_n)$ such that

$$\kappa_T^*(w) = db_+.$$

We also write

$$b_{+,v} \coloneqq r_v(b_+) \in C^2(\pi_v, \mu_n).$$

By proposition 2.8, we have that

$$\mathrm{CS}_c([\rho]) = \mathrm{inv}(z) = \sum_{v \in T} \mathrm{inv}_v(b_{-,v} - b_{+,v}).$$

Finally, recall the definition of the Chern-Simons action with boundary $\mathrm{CS}_c([\rho \circ \kappa_S])$. It is precisely the element of the pushout torsor $L([r_S(\rho \circ \kappa_S)])$ given by localising a global trivialisation β. This is precisely given by b_+ and the pushout given by $b_{+,v}$.

Thus we conclude with the decomposition formula

$$\mathrm{CS}_c([\rho]) = \sum_{v \in S} (\beta_v) - \mathrm{CS}_c([\rho \circ \kappa_S]).$$

□

Chapter 3

A Trace–Path Integral Formula over Function Fields

3.1 Introduction

In a topological quantum field theory, one often cares about path integrals of an action functional A over a space $\mathcal{F}$ of sections of a fibration $M \times [0,1]/F \to S^1$ (determined by a monodromy $F \circlearrowright M$). The path integral of A over this space can in fact be computed by instead looking at the action of F on a Hilbert space $\mathcal{H}$ of functions as

$$\mathrm{Tr}(F|\mathcal{H}) = \int_{\mathcal{F}} e^{iA(\gamma)} d\gamma.$$

The purpose of this paper is to explain how each of these concepts has an arithmetic analogue, and to prove a version of this trace path integral formula for J the Jacobian of a smooth projective curve X over the finite field $\mathbb{F}_q$.

Fibration $M \times [0,1]/F \to S^1$	::	Jacobian ℓ-torsion $J[\ell] \to \operatorname{Spec} \mathbb{F}_q$
Space of sections $\mathcal{F}$	::	Rational points $J[\ell](\mathbb{F}_q)$
Action functional A	::	Pairing A arising from class field theory
Geometric quantisation of phase space $\mathcal{H}$	::	Global sections of theta line bundle $\mathcal{H}$
Monodromy action F	::	Frobenius action Fr_q

Furthermore, the arithmetic path integral of A can be expressed as the trace of Fr_q on $\mathcal{H}$ just as in the physical setting.

Theorem A (Theorem 3.32)**.** Let J be the Jacobian of a genus g curve X over a finite field $\mathbb{F}_q$. Let ℓ be an odd prime satisfying $q \equiv 1 \pmod{\ell^2}$. If Fr_q acts semisimply on the $\mathbb{F}_\ell$-vector space $J[\ell]$, and $J(\mathbb{F}_q)$ has no points of order ℓ^2, then we have the following equality

$$\mathrm{tr}(\mathrm{Fr}_q\,|\mathcal{H}) = \left(\frac{(-1)^g \det{}'(1-\mathrm{Fr}_q)\det(A)}{\ell}\right) \sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)},$$

where $\det'(1-\mathrm{Fr}_q)$ is the regularised determinant of the linear map $1-\mathrm{Fr}_q$ on vector space $J[\ell]$. That is, this is the determinant of $1-\mathrm{Fr}_q$ after quotienting the space $J[\ell]$ by its kernel.

Regularised determinants are used in mathematical physics to assign finite values on self-adjoint operators of infinite dimensional spaces. Even in finite dimensional vector spaces, the removal of the kernel can be viewed as a kind of regularisation. The occurence of regularised determinants

in our formula strengthens the analogy between arithmetic path integrals and physical path integrals.

Determining signs in arithmetic explicitly can often be an intricate and delicate task, and the main contribution of this paper is the explicit Legendre symbol above. Additionally we also show that this statement is true as long as the Frobenius acts semisimply on $J[\ell]$. A weaker version of theorem 3.32 was initially an unpublished result of Minhyong Kim and Akshay Venkatesh, where they show the formula up to an undetermined sign in the special case where the vector space $J[\ell]$ has an invariant Lagrangian with respect to the Frobenius action.

This result adds to the series of analogies between topology and arithmetic first noticed by Mazur in [Maz] and expanded upon in detail in [Mor24]. For X a smooth projective curve over a finite field $\mathbb{F}_q$, it is natural to compare $\overline{X} := X \times_{\mathbb{F}_q} \operatorname{Spec} \overline{\mathbb{F}}_q$ with a smooth compact Riemann surface Σ. On the other hand, X itself has more in common with a three-manifold N – for instance X has étale cohomological dimension 3 and both sit in Cartesian squares

$$\begin{array}{ccc} \overline{X} & \hookrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} \overline{\mathbb{F}}_q & \longrightarrow & \operatorname{Spec} \mathbb{F}_q \end{array} \qquad \begin{array}{ccc} \Sigma & \hookrightarrow & N \\ \downarrow & & \downarrow \\ 1 & \longrightarrow & S^1 \end{array}$$

where the map $N \to S^1$ is a fibration and $\operatorname{Spec} \overline{\mathbb{F}}_q$ is a point. Under the knots and primes analogy, which views S^1 as being analogous to $\operatorname{Spec} \mathbb{F}_q$, we can view X as analogous to a three-manifold fibred over a circle, with fibres $\overline{X}$.

Moreover, we can write N as a mapping torus

$$N = \Sigma \times [0,1]/F$$

where $\Sigma \times \{0\}$ is identified with $\Sigma \times \{1\}$ via the monodromy action $F : \Sigma \to \Sigma$. In a similar manner we can view X as a mapping torus, where the automorphism $\operatorname{Fr}_q \in \pi_1(\operatorname{Spec} \mathbb{F}_q)$ act on $\overline{X}$ via the Frobenius automorphism

$$X \text{ ‘}=\text{’ } \overline{X} \times [0,1]/\operatorname{Fr}_q .$$

Quantum field theories are often defined as an integral over the ‘space of all paths’ [Hal13]. For example, let the manifold M be the phase space, let $P(x,y)$ denote the space of all paths from y to x in M,

$$P(x,y) := \{\gamma : [0,T] \to M | \gamma(0) = y, \gamma(T) = x\}.$$

An action functional is a function $A : P(x,y) \to \mathbb{C}$, then the kernel function is can be expressed as an integral over all paths in $P(x,y)$

$$K_T(x,y) = \int_{P(x,y)} e^{iA(\gamma)} d\gamma.$$

If we informally consider the kernel function $K_T(x,y)$ as a ‘matrix’ with infinite dimensions, then we can write

$$\operatorname{Tr}(K_T) = \int_x \int_{P(x,x)} e^{iA(\gamma)} d\gamma dx = \int_\Omega e^{iA(\gamma)} d\gamma$$

where Ω is defined to be the space of all loops in M.

In a similar manner which will be explained in detail in the next section, when a field theory is *topological* in nature (i.e. the theory does not depend on the metric of the manifold), then it is possible to express the trace of a monodromy action $F\colon M \to M$ as a path integral over the space of sections $\mathcal{F}$ of the bundle $([0,T] \times M)/F \to S^1$

$$\operatorname{Tr}(F) = \int_{\mathcal{F}} e^{iA(\gamma)} d\gamma.$$

Arithmetic path integrals over number fields have been introduced and computed in [Chu+19], [CK22], and [Car+24], and this paper introduces a function field analogue of arithmetic path integrals. A related construction also motivated by the same analogies can be found in [AV25].

Viewing the curve X as a '3-dimensional spacetime', the Jacobian $\overline{J} = \mathrm{Jac}(\overline{X})$ can be thought of a space of fields on X. For large values of ℓ, the Jacobian torsion $J[\ell]$ can be viewed as an approximation of the space $\overline{J}$. Thus in this paper we take the arithmetic analogue of the phase space of X to be ℓ-torsion $J[\ell]$. (Unfortunately an assumption we make in this paper is that the group of ℓth roots of unity are contained in the base field $\mathbb{F}_q$, so ℓ cannot be arbitrarily large, one interesting direction of further research would be to generalise the results of this paper with the $\mu_\ell \subset \mathbb{F}_q$ condition removed.)

Just as how X can be viewed as a fibred three-manifold, we can in a similar manner view the $J[\ell]$ as being fibred over the circle

$$\begin{array}{ccc} \overline{J}[\ell] & \hookrightarrow & J[\ell] \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\overline{\mathbb{F}}_q) & \longrightarrow & \mathrm{Spec}(\mathbb{F}_q). \end{array}$$

Moreover, we can view a rational point $\gamma \in J[\ell](\mathbb{F}_q)$ as a section over this fibre bundle over S^1

$$\begin{array}{c} J[\ell] \\ \downarrow \uparrow \gamma \\ \mathrm{Spec}\,\mathbb{F}_q. \end{array}$$

This is why in our setting, the integral over the space of all sections is instead replaced with a discrete sum over all $\mathbb{F}_q$-rational points of $J[\ell]$

$$\sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)}.$$

On the other hand, the arithmetic analogue of the Hilbert space $\mathcal{H}$ is given by the space of global sections of a tensor power of the theta line bundle Θ, in analogy to the geometric quantisation construction arising from physics. This will be explained in detail in sections 3.2.3 and 3.3.

Outline of Paper

In section 3.2 we will outline the physical background behind the trace–path integral formula that motivates our main theorem, in particular in section 3.2.3 we will discuss a method to obtain a Hilbert space $\mathcal{H}$ from the phase space M via a process called *geometric quantisation*.

The main theorem itself is proved by evaluating each side of the equality separately and then comparing the two sides. In section 3.3 we evaluate the trace side of the equality. We first define the space $\mathcal{H}$ which is a representation of the Heisenberg group $H(J[\ell])$. In section 3.3.1 and section 3.3.2 we express the Fr_q action on $\mathcal{H}$ explicitly using machinery from [GH09]. In section 3.3.3 we study the g-invariant spaces of symplectic vector space for a symplectomorphism g. We finally compute the trace of the Frobenius action on $\mathcal{H}$ in section 3.3.4 by decomposing $\overline{J}[\ell]$ into a direct sum of Fr_q invariant symplectic subspaces and computing the traces in those spaces separately.

In section 3.4 we will compute the path integral side of the equality. We first properly define the arithmetic action A in terms of a pairing in geometric class field theory. Then in section 3.4.2 we show that the arithmetic action A actually coincides with a function field analogue of the abelian arithmetic Chern-Simons action defined in [Chu+19]. Finally we evaluate the path integral in theorem 3.31.

We prove our main theorem in section 3.5 by combining the results from the two previous sections. In section 3.6 we will provide two explicit examples in the case where $q = 7, \ell = 3$ and $X = E$ is an elliptic curve, and compute the trace and path integral in the examples quite explicitly, and outline some future research directions.

3.2 Physical Background

In this section we go over the physics background that motivates our main result. References for this section include [Hal13], [Zei06], [FS18], [Zin11], [AS12], [Enr+99], and [CLL21].

3.2.1 The Path Integral Formalism

Let the manifold M denote the *phase space* in classical mechanics, which encodes the state of a physical system at a given time. This is typically an even-dimensional symplectic manifold consisting of data about the positions q and momenta p of particles. A *configuration space* is a Lagrangian submanifold L of M, roughly corresponding to the position coordinates. More precisely, L is a half-dimensional Lagrangian submanifold of M with a retraction $q\colon M \to L$.

In a quantum system, the phase space is replaced with a Hilbert space $\mathcal{H}$, which encodes all the possible states of a quantum system. The process in which the Hilbert space $\mathcal{H}$ is obtained from the phase space M is called *quantisation*, and we will discuss this process in more detail in section 3.2.3.

One typical example is when the phase space is a cotangent bundle $M = T^*X$ for some manifold X, in which case we could take the configuration space to be $L = X$ viewed as the zero-section in M, and $\mathcal{H} = L^2(X)$ is the *quantisation* of the symplectic manifold T^*X.

Setting Planck's constant to be 1, Schrödinger's equation can be written as

$$\frac{d\psi}{dt} = -iH\psi,$$

where the ψ is a time-dependent wave function $\psi \in \mathcal{H}$, and H is a self-adjoint operator on $\mathcal{H}$ called the Hamiltonian, representing energy. The path integral formalism arises when representing time evolution according to Schrödinger's equation as

$$[e^{-iHT}\psi](x) = \int_{y\in L} K_T(x,y)\psi(y)dy$$

for some kernel function $K_T(x,y)$. This is an integral over the configuration space L.

The classical Feynmannian path integral formalism interprets the kernel function $K_T(x,y)$ as an integral over a space of paths in the configuration space L. However, the Hamiltonian phase space path integral formalism detailed in [FS18, Section 2.1] and [Zin11, Chap. 10] instead shows that the same kernel function $K_T(x,y)$ can instead be written as an integral over paths in the phase space M. More precisely,

$$K_T(x,y) = \int_{P(x,y)} e^{iA(\gamma)}d\gamma.$$

Here, $A(\gamma)$ is the classical action defined on paths $\gamma\colon [0,T] \to M$, and $P(x,y)$ is a space of paths in the phase space M, where the position co-ordinates of the path start and end at y and x respectively. More precisely,

$$P(x,y) = \{\gamma\colon [0,T] \to M : q(\gamma(0)) = y, q(\gamma(T)) = x\}.$$

We can interpret the kernel function $K_T(x,y)$ as a 'matrix' with infinite dimensions, and under

this viewpoint one has informally

$$\mathrm{Tr}(e^{-iHT}) = \int K_T(x,x)dx.$$

But since we have interpreted $K_T(x,y)$ as an integral over paths in the phase space M, we can substitute the kernel function for the path integral to obtain

$$\mathrm{Tr}(e^{-iHT}) = \int_{x\in L}\int_{P(x,x)} e^{iA(\gamma)}d\gamma dx.$$

Here, the integral is taken over all paths γ in our phase space M where the position co-ordiantes of the end points are equal. In particular the momenta co-ordinates of the paths need not be equal on the end points. We can also write this integral as

$$\mathrm{Tr}(e^{-iHT}) = \int_{\Omega} e^{iA(\gamma)}d\gamma dx,$$

where

$$\Omega = \{\gamma\colon [0,T] \to M : q(\gamma(0)) = q(\gamma(T))\}.$$

3.2.2 Twists and Trace of Monodromy

Note that any map from S^1 to M can be viewed as a section of the trivial bundle

$$S^1 \times M \to S^1.$$

From a geometric point of view, it is natural to 'twist' this situation slightly and integrate over a space of sections of a non-trivial bundle

$$Y = ([0,T]\times M)/F \to S^1,$$

where Y is a mapping torus, and the monodromy map $F\colon M \to M$ is used to glue $T\times M$ to $0\times M$. Sections of this fibre bundle can be identified with $c\colon [0,T]\to M$ such that $Fc(T) = c(0)$. We impose additionally that the monodromy F must also be compatible with the Lagrangian subspace L and retract $q\colon M\to L$ in the sense that $F(L) = L$, and writing F_L for the restriction of the monodromy to L, the following diagram commutes.

$$\begin{array}{ccc} M & \xrightarrow{F} & M \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q} \\ L & \xrightarrow[F_L]{} & L. \end{array}$$

The diffeomorphism F acts on functions in $\mathcal{H}$ via

$$F\psi(x) = \psi(F^{-1}x).$$

Then we can write

$$[Fe^{-iHT}\psi](x) = [e^{-iHT}\psi](F^{-1}x) = \int K_T(F^{-1}x,y)\psi(y)dy.$$

That is, $K_T(F^{-1}x,y)$ is the integral kernel for the operator Fe^{-iHT}. Recalling from earlier that $K_T(x,y) = \int_{P(x,y)} e^{iA(q)}dq$, we have:

$$\mathrm{Tr}(Fe^{-iHT}) = \int K_T(F^{-1}x,x)dx = \iint_{P(F^{-1}x,x)} e^{iA(\gamma)}d\gamma dx.$$

Similarly to the un-twisted case, we can write the kernel function as an integral over just the classical paths, which again can be expressed as an integral over the space of sections of the fibre bundle. In particular, when the theory is *topological* so that the Hamiltonian is zero, we get

$$\mathrm{Tr}(F) = \int_{\mathcal{F}} e^{iA(\gamma)} d\gamma$$

where we use $\mathcal{F}$ to denote the space of paths in the twisted bundle $Y \to S^1$ such that the position co-ordinates form a loop. That is, the integral is taken over the space

$$\mathcal{F} = \{\gamma \colon [0,T] \to M : q(\gamma(0)) = F_L(q(\gamma(T)))\}.$$

3.2.3 Geometric Quantisation

As mentioned above, quantisation refers to the process in which a phase space is replaced with a quantum Hilbert space. More precisely, quantisation is a process

$$(M,\omega) \mapsto \mathcal{H}.$$

Which takes a symplectic manifold (M,ω) to a Hilbert space $\mathcal{H}$. This is also accompanied with a process that sends functions f on M to operators $\widehat{f}$ on the space $\mathcal{H}$. There are various ways in which quantisation can be performed, and usually one needs more data than just the symplectic manifold M. In this section we will briefly sketch the process of *Geometric Quantisation*.

Suppose that (M,ω) is a symplectic manifold. Assume that the symplectic form is in $\omega \in H^2(M,\mathbb{Z})$ and lies in the image of the Chern map $c_1 \colon H^1(M,\mathcal{O}_M^\times) \to H^2(M,\mathbb{Z})$. Then we can construct a line bundle $\mathcal{L}$ such that ω is its Chern class

$$c_1(\mathcal{L}) = \omega.$$

Then the *pre-quantisations* of M can be viewed as the global sections of this line bundle

$$\mathcal{H}_k^{\mathrm{pre}} = H^0(M,\mathcal{L}^{\otimes k}) = \Gamma(M,\mathcal{L}^{\otimes k}).$$

The prequantisation is 'too big' as a space, in order to obtain the quantisation one often takes a polarisation of M and define the quantisation to be the polarised sections of the line bundle instead.

If we additionally suppose M is Kähler with complex structure J, then the Kähler-polarised sections is simply the space of holomorphic sections of $\mathcal{L}^{\otimes k}$

$$\mathcal{H}_k = \Gamma_{\mathrm{hol}}(M,\mathcal{L}^{\otimes k}).$$

This means that the sections of the line bundle $\mathcal{L}^{\otimes k}$ are precisely the algebraic sections of the line bundle.

In particular if $M = X_{hol}$ is a complex projective variety and $\mathcal{L}$ is a line bundle on X with Chern class ω, then we can take the quantisation of M to be the space of sections $\mathcal{H}_k = \Gamma(X,\mathcal{L}^{\otimes k})$.

As an example, when $X = \mathbb{R}^2 = \mathbb{C}$, we can take

$$\mathcal{H} = L^2(\mathbb{R},dx) \quad \text{or} \quad \mathcal{H} = L^2_{\mathrm{hol}}(\mathbb{C}, e^{-|z|^2} i dz d\bar{z}).$$

In fact, by the *Stone-von Neumann Theorem*, since the actions of the center are equal on these two spaces, they are isomorphic as representations of the Heisenberg algebra.

3.3 Trace of Frobenius in the Arithmetic Hilbert Space

Let $W = W(\overline{\mathbb{F}}_q)$ be the Witt vectors over $\overline{\mathbb{F}}_q$ (This is a mixed characteristic ring that is an infinite unramified extension of $\mathbb{Z}_p$ with $\mathrm{Gal}(W/\mathbb{Z}_q) \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$). Throughout this section we fix an embedding $W \hookrightarrow \mathbb{C}$.

Once again let $X/\mathbb{F}_q$ be a curve over a finite field. We fix an algebraic closure $\overline{\mathbb{F}}_q$ denote by $\overline{X}/\overline{\mathbb{F}}_q$ to be the base change of X to the algebraic closure. The goal of this section is to define the arithmetic analogue of the quantisation $\mathcal{H}$ of our phase space $\overline{J}[\ell]$, and then to compute the trace of the Frobenius (which is the arithmetic analogue of the monodromy) on this space.

Define Y to be a lift of $\overline{X}$ to W. That is, Y is a curve over W such that the reduction of Y mod p is $\overline{X}$. Since we have fixed an embedding of $W \hookrightarrow \mathbb{C}$, we can view Y as a complex curve upon base changing to $\mathbb{C}$. Letting J_Y be the Jacobian of $Y \times_W \mathbb{C}$, the Jacobian comes equipped with a canonical principal polarisation coming from the intersection pairing on $Y \times_W \mathbb{C}$, which induces a Riemann form on J_Y. Let $\Theta \to J_Y$ be the theta line bundle associated to this polarisation. We fix an odd prime ℓ such that $q \equiv 1 \mod \ell$ (i.e. so that $\mu_\ell \subset \mathbb{F}_q$), then we define:

Definition 3.1. We define the arithmetic analogue of the quantisation of $J[\ell]$ to be $\mathcal{H}$, the global sections of the theta line bundle

$$\mathcal{H} \coloneqq \Gamma(J_Y, \Theta^{\otimes \ell}).$$

Let $\langle \cdot, \cdot \rangle : J[\ell] \times J[\ell] \to \mu_\ell(\overline{\mathbb{F}}_q)$ be the Weil pairing on $J[\ell]$ induced by the canonical principal polarisation, this is a symplectic form on the $2g$-dimensional $\mathbb{F}_\ell$ vector space $J[\ell]$.

By [OSZ21, Lemma 2.6], it is shown that the Weil pairing when viewed as a class in $H^2(J_Y, \mu_\ell)$ coincides with the Chern class of $c_1(\Theta)$ up to sign. This is why we view the space of sections $\Gamma(J_Y, \Theta^{\otimes \ell})$ as an analogue of the quantisation of our phase space $J[\ell]$.

Since X is defined over $\mathbb{F}_q$ and $\mu_\ell \subset \mathbb{F}_q$, the Frobenius Fr_q acts trivially on $\mu_\ell(\overline{\mathbb{F}}_q)$ and

$$\langle \mathrm{Fr}_q(x), \mathrm{Fr}_q(y) \rangle = \mathrm{Fr}_q \langle x, y \rangle = \langle x, y \rangle .$$

Thus Fr_q is a symplectomorphism in the symplectic group $\mathrm{Sp}(J[\ell])$. We will show in lemma 3.5 that $\mathcal{H}$ is a representation of the symplectic group $\mathrm{Sp}(J[\ell])$. Thus we can consider the action of Fr_q on $\mathcal{H}$ and our goal is the compute the trace of this action

$$\mathrm{Tr}(\mathrm{Fr}_q \,|\mathcal{H}).$$

Under some mild assumptions, we have the following explicit formula for the trace of the Frobenius action on $\mathcal{H}$.

Theorem 3.2. Suppose that the Frobenius Fr_q acts semi-simply on the space $J[\ell]$. Then

$$\mathrm{tr}(\mathrm{Fr}_q \,|\mathcal{H}) = \left(\frac{(-1)^{g - \dim_\ell J[\ell](\mathbb{F}_q)/2} \det'(1 - \mathrm{Fr}_q)}{\mathbb{F}_\ell} \right) \sqrt{|J[\ell](\mathbb{F}_q)|}.$$

Where $\left(\frac{\cdot}{\mathbb{F}_\ell}\right)$ is the Legendre symbol, and $\det'$ is the regularised determinant.

This is a strengthening of an unpublished result by Minhyong Kim and Akshay Venkatesh where the sign in the Legendre symbol was undetermined and there is an added assumption that there must exist a Frobenius–invariant Lagrangian subspace of $J[\ell]$.

An outline of the proof is as follows: We will show in lemma 3.5 that the representation $\mathcal{H}$ is in fact the unique representation of the Heisenberg group $H(J[\ell])$ with identity central character. We then use the machinery from [GH09] outlined in construction 3.4 and construction 3.6 to write down this representation $\mathfrak{H}(V)$ and the action of a symplectomorphism $g \in \mathrm{Sp}(V)$ on this representation explicitly. We derive an expression for the trace of such an action in lemma 3.7

when given a fixed Lagrangian M of V. Finally, in lemmas 3.13 and 3.14 and theorem 3.15 we decompose the symplectic vector space V into a direct sum of g-invariant symplectic subspaces and compute the trace of g action on $\mathfrak{H}(V)$ as a product of the traces of the g action on the smaller spaces to complete the proof.

3.3.1 Representations of the Heisenberg Group

Before we prove theorem 3.2 we first establish some theory about the representations of Heisenberg groups over finite fields. Let $V/\mathbb{F}_\ell$ be a symplectic vector space with symplectic form $\omega : V \times V \to \mathbb{F}_\ell$.

Definition 3.3. Define $H(V)$ to be the *Heisenberg group*, a central extension of V by $\mathbb{F}_\ell$. Explicitly as a set: $H(V) = \mathbb{F}_\ell \times V$ and the group operation is given by

$$(\lambda, a) \circ (\mu, b) = \left(\lambda + \mu + \frac{1}{2}\omega(a, b), a + b\right).$$

This group has center

$$Z := Z(H(V)) = \{(z, 0) : z \in \mathbb{F}_\ell\}.$$

There is also an action by the finite symplectic group $\mathrm{Sp}(V)$ on $H(V)$ via its action on the V part.

A finite analogue of the Stone-von Neumann property, proven in [GH09, 1.2.1], states that for any non-trivial character $\psi : Z \to \mathbb{C}^\times$, there exists a unique (up to isomorphism) irreducible complex unitary representation $\mathfrak{H} = \mathfrak{H}(V, \psi)$ of $H(V)$, $\pi : H(V) \to \mathfrak{H}$ such that

$$\pi|_Z(z) = \psi(z) \cdot \mathrm{Id}_{\mathfrak{H}}.$$

We write $\mathfrak{H} = \mathfrak{H}(V) = \mathfrak{H}(V, \psi)$ if it is clear from context what ψ or V are. Now we construct the representation $\mathfrak{H}(V, \psi)$ explicitly following the construction in section 2.1 of loc. cit.

Construction 3.4. Given a character $\psi : \mathbb{F}_\ell \to \mathbb{C}^\times$, let $\mathbb{C}(H(V), \psi)$ denote the space of (set-valued) functions $f : H(V) \to \mathbb{C}$ such that for $h \in H(V)$ and $z \in \mathbb{F}_\ell$ (where z is viewed as an element of the center of $H(V)$)

$$f(z \cdot h) = \psi(z) f(h).$$

Let an oriented Lagrangian M° be the langrangian M along with a choice of non-zero vector $o_M \in \bigwedge^{top} M$. Then consider the vector subspace C_{M° of $\mathbb{C}(H(V), \psi)$ consisting of functions f such that any $m \in M$ acts trivially

$$f(m \cdot h) = f(h).$$

This vector space has a right $H(V)$ action given by right translation

$$\pi_M(h)[f](h') = f(h' \cdot h).$$

Lemma 3.5. Upon fixing an isomorphism $\mathbb{F}_\ell \to \mu_\ell \subset \mathbb{C}^\times$ which sends 1 to ζ, the Weil pairing is a symplectic form on $J[\ell]$, and the space $\mathcal{H}$ is the unique (up to almost unique isomorphism given by scalar multiplication by $a \in \mathbb{F}_\ell$) irreducible representation of $H(J[\ell])$ with the identity central character $\psi(z) = \zeta^z$.

Proof. Let $\mathcal{G}(\mathcal{L})$ denote the Theta group of $\mathcal{L}$ of all automorphisms of $\mathcal{L}$ lying over translations of J (c.f. [BL04, Section 6.1]). By an analogue of the Stone Von-Neumann Theorem [BL04, Cor 6.4.3, Ex 6.10.3], the global sections of any line bundle $\mathcal{L}$ is a unique irreducible representation $\mathcal{G}(\mathcal{L})$ with identity central character. We will now show that the Heisenberg group $H(J[\ell])$ is a subgroup of the theta group $\mathcal{G}(\Theta^{\otimes \ell})$, and the restricted representation is still irreducible.

By [Mum70, p. 225] the theta group is a central extension of the group $K(\mathcal{L}) = \mathrm{Ker}(\phi_{\mathcal{L}})$ where $\phi_{\mathcal{L}} \colon J_Y \to \mathrm{Pic}^0 J_Y$ is given by $x \mapsto T_x^* \mathcal{L} \otimes \mathcal{L}$

$$0 \to \mathbb{C}^\times \to \mathcal{G}(\mathcal{L}) \to K(\mathcal{L}) \to 0.$$

Since Θ is a principal polarisation, it follows that ϕ_Θ is an isomorphism and $K(\Theta) = 0$. Furthermore, since $\phi_{\Theta^{\otimes \ell}} = \ell \phi_\Theta$ ([Mum70, p. 60]), it follows that $K(\Theta^{\otimes \ell}) = \mathrm{Ker}(\phi_{\Theta^{\otimes \ell}}) = J_Y[\ell]$.

On the other hand, the Heisenberg group $H(J_Y[\ell])$ is an extension of $J_Y[\ell]$ by μ_ℓ. Additionally it is known from [Mum70, p. 228 (5)] that the commutator pairing on $K(\Theta^{\otimes \ell})$ co-incides with the Weil pairing on $J_Y[\ell]$ induced by polarisation $\Theta^{\otimes \ell}$.

Thus there are injections

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_\ell & \longrightarrow & H(J_Y[\ell]) & \longrightarrow & J_Y[\ell] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mathbb{C}^\times & \longrightarrow & \mathcal{G}(\Theta^{\otimes \ell}) & \longrightarrow & K(\Theta^{\otimes \ell}) & \longrightarrow & 0. \end{array}$$

So $\mathcal{H}$ is a representation of $H(J_Y[\ell])$ with the identity central character. To see that the representation is irreducible, suppose that $\mathcal{H} \cong U \oplus V$ is reducible as a $H(J_Y[\ell])$-representation. But any element of $\mathcal{G}(\Theta^{\otimes \ell})$ will differ from an element of $H(J_Y[\ell])$ by an element in $\mathbb{C}$, but since elements in $\mathbb{C}$ acts on $\mathcal{H}$ by scaling, this means that U and V are also invariant subspaces of $\mathcal{G}(\Theta^{\otimes \ell})$, contradicting that $\mathcal{H}$ is an irreducible representation of $\mathcal{G}(\Theta^{\otimes \ell})$.

The uniqueness of this representation follows from another analogue of the Stone Von-Neumann Theorem, see [GH09, Thm 1.2.1].

Finally, since we have picked $q \equiv 1 \mod \ell$, the reduction map from W to $\mathbb{F}_q$ induces an isomorphism of the ℓ-torsion subgroups $J[\ell]$ and $J_Y[\ell]$ as Galois modules, which then induces an isomorphism between $H(J_Y[\ell])$ and $H(J[\ell])$, completing the proof. □

Canonical Intertwining Morphisms

Given any pair of oriented Lagrangians M°, L°, it is shown in [GH09, Thm 2.2.3] that there exists canonical isomorphisms for any pair of oriented Lagrangians

$$T_{M^\circ, L^\circ} \colon C_{L^\circ} \xrightarrow{\sim} C_{M^\circ}.$$

We describe the construction of T_{M°, L° explicitly, following [GH09, 2.4].

Construction 3.6. Let $M^\circ = (M, o_M), L^\circ = (L, o_L)$ be two oriented Lagrangians. Set $I \coloneqq M \cap L$ and $n_I \coloneqq \frac{\dim(I^\perp / I)}{2}$.

The top exterior powers of M and L decompose canonically

$$\begin{aligned} \bigwedge^{top} M &= \bigwedge^{top} I \bigotimes \bigwedge^{top} M/I \\ \bigwedge^{top} L &= \bigwedge^{top} I \bigotimes \bigwedge^{top} L/I. \end{aligned}$$

Since the top exterior powers are 1 dimensional, the orientations o_M, o_L can be decomposed as

$$\begin{aligned} o_M &= \iota_M \otimes o_{M/I} \\ o_L &= \iota_L \otimes o_{L/I} \end{aligned}$$

where $\iota_M, \iota_L \in \bigwedge^{top} I, o_{M/I} \in \bigwedge^{top} M/I$, and $o_{L/I} \in \bigwedge^{top} L/I$.

Define the averaging function $F_{M^\circ,L^\circ}\colon C_{L^\circ} \xrightarrow{\sim} C_{M^\circ}$ to take a function in C_L and sum its values over a transversal of M

$$F_{M^\circ,L^\circ}[f](v) = \sum_{m+I\in M/I} f(m\cdot v).$$

Define the normalisation constant

$$A_{M^\circ,L^\circ} = (G(\tfrac{1}{2},\ell)/\ell)^{n_I}\left(\frac{(-1)^{\binom{n_I}{2}}\frac{\iota_L}{\iota_M}\cdot\omega_\wedge(o_{L/I},o_{M/I})}{\mathbb{F}_\ell}\right).$$

Where:

- $\left(\frac{\cdot}{\mathbb{F}_\ell}\right)$ is the unique quadratic character of the multiplicative group $\mathbb{F}_\ell^\times$. This is the unique non-zero morphism $\mathbb{F}_\ell^\times \to \{\pm 1\}$. (In the case where ℓ is prime, this is the Legendre symbol.)
- $G(\alpha,\ell)$ is the one dimensional Gauss sum

$$G(\alpha,\ell) = \sum_{z\in\mathbb{F}_\ell}\psi(\alpha z^2).$$

- $\omega_\wedge\colon \bigwedge^{top} L/I \times \bigwedge^{top} M/I \to \mathbb{F}_\ell$ is the pairing induced by the symplectic form ω.

Then the canonical intertwining morphism is the averaging morphism times the normalisation constant

$$T_{M^\circ,L^\circ} = A_{M^\circ,L^\circ}\cdot F_{M^\circ,L^\circ}.$$

3.3.2 Symplectic Actions on the Heisenberg Representations

Let $g\in \mathrm{Sp}(V)$, then g acts on $H(V)$, which in turn acts on representations of $H(V)$.

We wish to understand the trace $\mathrm{tr}(g|\mathfrak{H}(V))$, but since $\mathfrak{H}(V)$ is isomorphic to C_{M° for any given lagrangian M°, we make the g action on C_{M° explicit.

Suppose that the image of M under g is gM, then it is easy to check that there is a map from C_{M° to C_{gM° via pre-composing by g^{-1}

$$\begin{aligned} C_{M^\circ} &\to C_{gM^\circ}\\ \phi &\mapsto \phi\circ g^{-1}. \end{aligned}$$

Thus the action of g on C_{M° is the composite of the following maps (c.f. [GH09, Section 2.6])

$$C_{M^\circ} \xrightarrow{g} C_{gM^\circ} \xrightarrow{T_{M^\circ,gM^\circ}} C_{M^\circ}.$$

Lemma 3.7. Let $g\in\mathrm{Sp}(V)$ be any symplectomorphism. Given any Lagrangian M, and any complement M' such that $M\oplus M' = V$, let $\mathcal{S}$ be the set

$$\mathcal{S} \coloneqq \{x\in M' : gx - x \in M + gM\}.$$

and for each $x\in S$, pick $m_x, n_x\in M$ such that

$$gx - x = m_x + gn_x.$$

Then

$$\mathrm{tr}(g|C_{M^\circ}) = A_{M^\circ,gM^\circ}\cdot\sum_{x\in\mathcal{S}}\psi\left(\frac{1}{2}\omega(m_x+n_x,x)\right).$$

Proof. Note that any $f \in \mathbb{C}(H(V), \psi)$ is uniquely determined by its values on $\{0\} \times V \subset H(V)$, since the center must act via the identity. Moreover since the Lagrangian subspace M acts trivially, $f \in C_{M^\circ}$ is uniquely determined by its values on the the group $\{0\} \times M'$.

Thus there is a $\mathbb{C}$-basis $\{i_x\}_{x \in M'}$ on C_{M° indexed by elements in M' such that i_x restricts to the indicator function on $\{0\} \times M'$. Explicitly $i_x \in C_{M^\circ}$ is the function

$$\begin{cases} i_x(z, x) = \psi(z) & \\ i_x(z, m + x) = \psi(z - \frac{1}{2}\omega(m, x)) & \text{for } m \in M, \text{ since } m \cdot (0, x) = (\frac{1}{2}\omega(m, x), m + x) \\ i_x(z, v) = 0 & \text{for } v \notin x + M. \end{cases}$$

Note that via fixing the basis $\{i_x\}$, the trace of g on C_{M° is simply A_{M°, gM° times the the coefficient of i_x appearing in $F_{M^\circ, gM^\circ} \circ g[i_x]$. But this coefficient is equal to evaluation at $(0, x)$, so

$$\operatorname{tr}(g | C_{M^\circ}) = A_{M^\circ, gM^\circ} \cdot \sum_{x \in M'} F_{M^\circ, gM^\circ} \circ g[i_x](0, x).$$

We now evaluate the image of each indicator function i_x under $F_{M^\circ, gM^\circ} \circ g$, at $(0, x)$.

By precomposing with g^{-1} we get the the function $g[i_x](z, h) = i_x(z, g^{-1}(h))$, which explicitly evaluates as

$$\begin{cases} g[i_x](z, gx) = \psi(z) & \\ g[i_x](z, gm + gx) = \psi(z - \frac{1}{2}\omega(m, x)) & \text{for } m \in M \\ g[i_x](z, v) = 0 & \text{for } v \notin gx + gM. \end{cases}$$

Finally we put $g[i_x]$ through the averaging morphism F_{M°, gM° to obtain

$$\begin{aligned} F_{M^\circ, gM^\circ} \circ g[i_x](0, x) &= \sum_{m + I \in M/I} g[i_x](m \cdot (0, x)) \\ &= \sum_{m + I \in M/I} g[i_x](\tfrac{1}{2}\omega(m, x), m + x). \end{aligned}$$

Terms in this sum are non-zero only if $m + x \in gx + gM$, or in other words, the function i_x contributes to the trace of g if and only if $gx - x \in M + gM$. In this case, we write

$$gx - x = m_x + gn_x$$

for some fixed $m_x, n_x \in M$. Note further that since the sum is taken over cosets $m + I \in M/I$, the above sum has precisely one non-zero term. Thus we have

$$\begin{aligned} F_{M^\circ, gM^\circ} \circ g[i_x](0, x) &= g[i_x](\tfrac{1}{2}\omega(m_x, x), m_x + x) \\ &= g[i_x](\tfrac{1}{2}\omega(m_x, x), -gn_x + gx) \\ &= \psi(\tfrac{1}{2}\omega(m_x, x) - \tfrac{1}{2}\omega(-n_x, x)) \\ &= \psi(\tfrac{1}{2}\omega(m_x + n_x, x)) \end{aligned}$$

We quickly check that this sum is independent of the choice of m_x and n_x. If m_x, n_x were replaced with $m'_x = m_x + a, n'_x = n_x + b$, then since $gn_x + m_x = gn'_x + m'_x$ we must have $a = -gb \in M \cap gM = I$. Then

$$\omega(a, x) = \omega(a, m_x + x) = \omega(-gb, -gn_x + gx) = -\omega(b, n_x + x) = -\omega(b, x).$$

Which implies $\omega(m_x + n_x, x) = \omega(m'_x + n'_x, x)$, so this sum is independent of the choices of m_x and n_x.

Finally, our trace is

$$\mathrm{tr}(g|C_{M^\circ}) = A_{M^\circ,gM^\circ} \cdot \sum_{x\in\mathcal{S}} \psi(\tfrac{1}{2}\omega(m_x + n_x, x))$$

as desired. □

An immediate and important consequence of the lemma is the following special case:

Corollary 3.8. Let $g \in \mathrm{Sp}(V)$ be a semi-simple symplectomorphism. Suppose that there exists a Lagrangian M that is also invariant under g, i.e. $g(M) = M$. Then

$$\mathrm{tr}(g|C_M) = \left(\frac{\det(g|M)}{\mathbb{F}_\ell}\right)\sqrt{|V^g|}.$$

Where V^g are the g-fixed points of V.

Proof. Since g is semi-simple, let $M' \subset V$ be a complementary g-invariant subspace such that $V = M \oplus M'$. Then $M = gM$ and $gM' = M'$. For any $x \in \mathcal{S}$, we have that $x - gx \in M \cap M' = 0$. Thus $x \in \mathcal{S}$ if and only if $x = gx$. For each such x we can pick $n_x = m_x = 0$, which turns the trace into the following:

$$\mathrm{tr}(g|C_{M^\circ}) = A_{M^\circ,gM^\circ} \cdot \sum_{x\in\mathcal{S}} \psi(\tfrac{1}{2}\omega(0, x)) = A_{M^\circ,gM^\circ} \cdot \sum_{x\in\mathcal{S}} 1 = A_{M^\circ,gM^\circ} \cdot |\mathcal{S}|$$

where

$$S = \{x \in M' | gx = x\} = (M')^g$$

is the set of g-fixed points of M'.

We first compute $|\mathcal{S}|$. The symplectic pairing ω induces an isomorphism from V to its dual

$$\begin{aligned} D\colon V &\to V^* \\ x &\mapsto \omega(x, -). \end{aligned}$$

Since g is a symplectomorphism, this isomorphism is g-equivariant, i.e. for all $x \in V$

$$g \circ D(x) = \omega(x, g^{-1}(-)) = \omega(gx, -) = D \circ g(x).$$

The inclusion $M \hookrightarrow V$ induces a restriction map $r\colon V^* \to M^*$. Composing with D we note that the kernel of the map $r \circ D\colon V \to M^*$ is precisely M. Thus (as g-modules)

$$M' \simeq V/M \simeq M^*.$$

So the fixed points of M' are the same as the fixed points of M^*. Note that $\phi \in M^*$ is a fixed point if and only if for any $m \in M$, $\phi(m) = \phi(g^{-1}(m))$. In other words, ϕ must factor through the co-invariant module $M/(\mathrm{id} - g^{-1})M = M/(g - \mathrm{id})M =: M_g$, and thus

$$(M^*)^g \simeq (M_g)^*.$$

Moreover, from the exact sequence

$$0 \to M^g \to M \xrightarrow{g-\mathrm{id}} M \to M_g \to 0,$$

we can deduce that (since M is a finite module) M and M' have the same number of invariant elements

$$|(M')^g| = |(M^*)^g| = |(M_g)^*| = |M^g|.$$

Thus we conclude

$$|(M')^g| = \sqrt{|(M')^g||M^g|} = \sqrt{|(M' \times M)^g|} = \sqrt{|V^g|}.$$

Finally we compute A_{gM°,M°. In our setting $I \coloneqq M \cap gM = M$ and $n_I \coloneqq \frac{\dim(I^\perp/I)}{2} = 0$. Moreover the $\omega_\wedge$ term vanishes since M/I is trivial. Thus we have

$$A_{gM^\circ,M^\circ} = \left(\frac{\frac{o_M}{o_{gM}}}{\mathbb{F}_\ell}\right) = \left(\frac{\det(g|M)}{\mathbb{F}_\ell}\right).$$

Thus $\operatorname{tr}(g|C_M) = \left(\frac{\det(g|M)}{\mathbb{F}_\ell}\right)\sqrt{|V^g|}$ as desired. □

3.3.3 Invariant Spaces of a Symplectic Vector Space

We prove some facts about the invariant spaces of a symplectomorphism $g \in \mathrm{Sp}(V)$. Let ω be a symplectic form on a $2g$-dimensional vector space V over a finite field $\mathbb{F}$ of characteristic $\neq 2$. Let $g \in \mathrm{Sp}(V,\omega)$ be a symplectomorphism, and suppose g is represented by the matrix S under the standard symplectic basis.

Proposition 3.9. $\det(S) = 1$

Proof. Viewing ω as an element of $\Lambda^2 V^*$, consider $\Lambda^g\omega \in \Lambda^{2g}V^*$. The top exterior power is 1 dimensional and the determinant of S is equal to its scalar action on the top exterior power $\Lambda^{2g}V^*$. But since $S^*\omega = \omega$, it follows that $S^*(\Lambda^g\omega) = \Lambda^g\omega$ and thus $\det S = 1$. □

Proposition 3.10. Let $\chi_S(t) = \det(tI - S)$ denote the characteristic polynomial of S. If $\lambda \neq \pm 1$ is a root of χ_S with multiplicity d, then λ^{-1} is also a root with multiplicity d.

Moreover, if ± 1 is a root of f_S, then it will occur with even multiplicity.

Proof. Let Ω be the matrix representing ω, then S satisfies $S^T\Omega S = \Omega$. Rearranging we get

$$S^{-1} = \Omega^{-1}S^T\Omega$$

Thus S^{-1} and S have equal characteristic polynomials. On the other hand,

$$\chi_{S^{-1}}(t) = \det(tI - S^{-1}) = \det(tS - I)\det(S^{-1}) = t^{2g}\det(S - \tfrac{1}{t}I) = t^{2g}\chi_S(\tfrac{1}{t}).$$

Thus if λ is a root of χ_S with multiplicity d, then so is λ^{-1}.

The product of all the roots of $\chi_S(t)$ must equal $\det(S) = 1$. Since every non-± 1 eigenvalue must come in reciprocal pairs, it follows that if -1 is a root of χ_S, it must occur with even multiplicity.

Finally, S is even-dimensional and thus 1 must also occur as a root with even multiplicity. □

For an eigenvalue λ of S with algebraic multiplicity d, let $S_\lambda \coloneqq \operatorname{Ker}(\lambda I - S)^d$ denote the *generalised eigenspace* of V corresponding to λ.

Proposition 3.11. Suppose that the characteristic polynomial of S splits completely in $\mathbb{F}$. Given (not neccesarily distinct) eigenvalues λ, μ of S, then

1. If $\lambda\mu \neq 1$, then the spaces S_λ and S_μ are orthogonal. i.e. for $v \in S_\lambda, w \in S_\mu$,

$$\omega(v,w) = 0.$$

In particular this implies that when $\lambda \neq \pm 1$, S_λ is a isotropic subspace of V.

2. If $\lambda = \pm 1$, then S_λ is a symplectic subspace of V.

Proof. 1) Let $v \in S_\lambda, w \in S_\mu$. We say v has rank r if it lies in the kernel of $(\lambda I - S)^r$ but not $(\lambda I - S)^{r-1}$, and similarly for w, we will induct on the sum of the ranks of v and w.

The base case is when v, w are both eigenvectors, in that case

$$\omega(v, w) = \omega(Sv, Sw) = \omega(\lambda v, \mu w) = \lambda\mu\omega(v, w).$$

Since $\lambda\mu \neq 1$, it follows that $\omega(v, w) = 0$.

For the inductive case, suppose v has rank r_1 and w has rank r_2, and assume that $\omega(v', w') = 0$ whenever the ranks of v', w' sum to less than $r_1 + r_2$.

Then by the definition of rank, $Sv = \lambda v + v'$ and $Sw = \mu w + w'$, where v', w' have ranks $r_1 - 1, r_2 - 1$ respectively (If a vector has rank 0 then it is simply the zero vector). Then

$$\begin{aligned}\omega(v, w) = \omega(Sv, Sw) = \omega(\lambda v + v', \mu w + w') &= \omega(v', w') + \omega(\lambda v, w') + \omega(v', \mu w) + \omega(\lambda v, \mu w) \\ &= \omega(\lambda v, \mu w) = \lambda\mu\omega(v, w).\end{aligned}$$

Once again since $\lambda\mu \neq 1$, it follows that $\omega(v, w) = 0$, completing the proof.

2) To show that S_λ is a sympletic subspace of V, it suffices to show that $\omega|_{S_\lambda}$ is a non-degenerate form, since bilinearity and antisymmetry is inherited from ω.

Suppose that $v_0 \in S_\lambda$ satisfies $\omega(v_0, w) = 0$ for any $w \in S_\lambda$. Note that since $\lambda = \pm 1$, for any $\mu \neq \lambda$, $\mu\lambda \neq 1$ and thus by the previous part, $\omega(v_0, w) = 0$ for all $w \in S_\mu$. Since V is a direct sum of all its generalised eigenspaces, this implies that $\omega(v_0, w) = 0$ for all $w \in V$. Since ω is non-degenerate on V, it follows that $v = 0$, proving non-degeneracy of ω in S_λ. □

Lemma 3.12. Suppose $g \in \mathrm{Sp}(V)$ is semisimple, then it is possible to decompose V as a direct sum of g-invariant symplectic subspaces

$$V = S_1 \oplus S_{-1} \oplus V_1 \oplus \cdots \oplus V_r.$$

Where $S_{\pm 1}$ is the ± 1 eigenspace of g respectively, and V_i are subspaces such that the restriction $g|_{V_i}$ of the g-action to V_i has characteristic polynomial f_i, where f_i has no repeated roots.

Proof. For an irreducible monic polynomial $h(t)$, let $h^-(t) \coloneqq t^{\deg h} h(1/t)$ denote the irreducible polynomial with roots being the reciprocals of those of $h(t)$.

Since roots of f come in pairs of λ, λ^{-1} with equal multiplicity, then for each irreducible factor $h(t)$ of $f(t)$, either $h^-(t) = h(t)$, or $h^-(t)$ must also be an irreducible factor of $f(t)$ with the same multiplicity as $h(t)$.

Thus we can write

$$f(t) = (t+1)^a (t-1)^b f_1(t)^{k_1} f_2(t)^{k_2} \dots f_s(t)^{k_s}.$$

Where each f_i is either an irreducible factor satisfying $f_i(t) = f_i^-(t)$, or f_i is a product of two irreducible factors of the form $h(t)h^-(t)$. In both cases $f_i(t)$ has no repeated roots, since finite extensions of $\mathbb{F}$ are separable. Thus we can decompose V into g-invariant subspaces

$$V = S_1 \oplus S_{-1} \oplus W_1 \oplus \cdots \oplus W_s$$

where W_i is the vector subspace of V corresponding to $f_i(t)^{k_i}$. Then over the algebraic closure $W_i \otimes \overline{\mathbb{F}}$ is a symplectic subspace of $V \otimes \overline{\mathbb{F}}$ since it is a direct sum of $S_\lambda \oplus S_{\lambda^{-1}}$ for every pair of roots λ, λ^{-1} of f. Thus W_i is also a symplectic subspace of V.

Thus it suffices to show that each W_i can be further decomposed into $W_{i1} \oplus \cdots \oplus W_{il}$ where each W_{ij} is a g-invariant symplectic subspaces of W_i. We know that the the restricted action $g|_{W_i}$ has characteristic polynomial $f_i^{k_i}$. Let T be a matrix with characteristic polynomial f_i

that is also symplectic with respect to a symplectic form ϖ, then the block diagonal matrix

$$\begin{pmatrix} T & & & \\ & T & & \\ & & \ddots & \\ & & & T \end{pmatrix}$$

with k_i diagonal blocks will have characteristic polynomial $f_i^{k_i}$. This matrix is also symplectic with respect to the symplectic form $\varpi^{\otimes k_i}$.

Applying a suitable change of basis, we can obtain a matrix U that is symplectic with respect to the symplectic form on W_i.

Finally, the summary in [Wal15, p.7] states that any two semisimple elements in $\mathrm{Sp}(V)$ which are conjugate over $\mathrm{GL}(V)$ are also conjugate over $\mathrm{Sp}(V)$. Since both U and $g|_{W_i}$ are semisimple with the same characteristic polynomial, this means that under a suitable basis $g|_{W_i}$ has matrix U. It is clear from construction that the matrix U decomposes into g-invariant symplectic subspaces each with characteristic polynomial f_i, so we are done. □

3.3.4 Evaluating the Trace

Lemma 3.13. Let $g \in \mathrm{Sp}(V)$ be a symplectomorphism. Suppose V decomposes into a direct sum of g-invariant symplectic subspaces

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

Let $\mathfrak{H}_i = \mathfrak{H}(V_i)$ be the the unique representation of V_i with identity central character as described in section 3.3.1. Then

$$\mathrm{tr}(g|\mathfrak{H}(V)) = \prod_{i=1}^{r} \mathrm{tr}(g|\mathfrak{H}_i).$$

Proof. This follows directly from [GH09, Prop 2.14] which asserts that

$$\mathfrak{H}(V) = \bigotimes_{i=0}^{r} \mathfrak{H}_i$$

and the fact that the trace on a tensor product of vector spaces is equal to the product of the traces on each individual component. □

Lemma 3.14. Suppose that $g \in \mathrm{Sp}(V)$ is a semi-simple symplectomorphism which has characteristic polynomial $f(t)$ with no repeated roots, then

$$\mathrm{tr}(g|\mathfrak{H}(V)) = \left(\frac{(-1)^n f(1)}{\mathbb{F}_\ell}\right),$$

where $\dim V = 2n$.

Proof. First we note that since we have assumed that $f(t)$ has no repeated roots, this also means that g does not have any eigenvalues equal to ± 1. This is because by proposition 3.10 any eigenvalue of ± 1 must occur with even multiplicity.

Fix a standard symplectic basis of V and let S denote the matrix representing g in this basis. Since f has no repeated roots, this means that any matrix in $T \in \mathrm{GL}(V)$ with the same characteristic polynomial f will be similar to S (since neither S nor T will have any Jordan blocks as every eigenvalue has multiplicity 1).

Furthermore, by the summary in [Wal15, p. 7], it is shown that the $\mathrm{GL}(V)$ conjugacy class of S intersects $\mathrm{Sp}(V)$ at a unique conjugacy class. This means that any symplectic matrix $T \in \mathrm{Sp}(V)$ with the same characteristic polynomial as g will be similar to S via a symplectomorphism.

Now suppose g has characteristic polynomial

$$f(t) = t^{2n} + a_1 t^{2n-1} + \cdots + a_{n-1} t^{n+1} + a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + 1$$

and construct the block matrix

$$S = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

Where A and B have dimension $n+1 \times n$, C has dimension $n-1 \times n$ and they are

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots \\ 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 0 & \cdots & -1 \\ 0 & 0 & 0 & \cdots & -a_1 \\ 0 & 0 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{n-1} \\ -a_1 & -a_2 & -a_3 & \cdots & -a_n \end{pmatrix}, C = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \end{pmatrix}.$$

It can be checked by a straightforward computation that $\chi_S(t) = f(t)$ and that S preserves the standard symplectic form. Thus under suitable symplectic change of basis, g is represented by the matrix S.

Let $v_1, \ldots, v_n, w_1, \ldots, w_n$ be this standard symplectic basis, then explicitly g is the linear map

$$g\colon \begin{cases} v_i \mapsto v_{i+1} & i \neq n \\ v_n \mapsto w_1 & \\ w_i \mapsto -a_i w_1 + w_{i+1} & i \neq n \\ w_n \mapsto -(v_1 + a_1 v_2 + a_2 v_3 + \cdots + a_{n-1} v_n + a_n w_1). & \end{cases}$$

Now that we have a symplectic basis of g, we fix the Lagrangian M to be the span of $v_1, \ldots, v_n$, the complement M' to be the span of $w_1, \ldots, w_n$ and we apply lemma 3.7 to calculate the trace of g.

We first determine the set $\mathcal{S} = \{x \in M' | gx - x \in M + gM\}$. Noting that $M + gM = M + \mathbb{F}_\ell w_1$, we let $x = \alpha_1 w_1 + \cdots + \alpha_n w_n$ and we require that $gx - x$ have no $w_2 \cdots w_n$ terms. For each $2 \leq i \leq n$, the coefficient of w_i in $x - gx$ being zero implies that $\alpha_i = \alpha_{i-1}$. Thus $\mathcal{S}$ is the 1 dimensional subspace spanned by $w_1 + w_2 + \cdots + w_n$.

Letting $x = w_1 + w_2 + \cdots + w_n$, we compute that

$$\begin{aligned} gx - x &= -(v_1 + a_1 v_2 + a_2 v_3 + \cdots + a_{n-1} v_n) - (a_1 + a_2 + \cdots + a_n + 1) w_1 \\ &= -(v_1 + a_1 v_2 + a_2 v_3 + \cdots + a_{n-1} v_n) - g[(a_1 + a_2 + \cdots + a_n + 1) v_n]. \end{aligned}$$

Thus we can pick $m_x = -(v_1 + a_1 v_2 + a_2 v_3 + \cdots + a_{n-1} v_n)$ and $n_x = -(a_1 + a_2 + \cdots + a_n + 1) v_n$. Then we see that

$$\begin{aligned} \omega(m_x + n_x, x) &= -(a_n + 2a_{n-1} + 2a_{n-2} + \cdots + 2a_1 + 2) \\ &= -f(1) \end{aligned}.$$

Where $f(1)$ is the sum of the coefficients of the characteristic polynomial of g.

Thus we can compute the sum

$$\begin{aligned}\sum_{x\in\mathcal{S}}\psi\left(\frac{1}{2}\omega(m_x+n_x,x)\right) &= \sum_{x\in\mathcal{S}}\psi\left(\frac{1}{2}\omega(m_x+n_x,x)\right)\\ &= \sum_{k\in\mathbb{F}_\ell}\psi\left(\frac{-f(1)}{2}k^2\right)\\ &= \left(\frac{-\frac{1}{2}f(1)}{\mathbb{F}_\ell}\right)G(1,\ell)\end{aligned}.$$

Where the last equality is from [Lan86, p.85]

Finally we compute A_{M°,gM°. We fix the orientation

$$o_M = v_1\wedge v_2\wedge\cdots\wedge v_n$$

and so

$$o_{gM} = g(o_M) = v_2\wedge\cdots\wedge v_n\wedge w_1 = (-1)^{n-1}w_1\wedge v_2\wedge\cdots\wedge v_n.$$

Then we can decompose the orientations via $\iota_M = \iota_{gM} = v_2\wedge\cdots\wedge v_n$, and $o_{M/I} = v_1$, $o_{gM/I} = (-1)^{n-1}w_1$. We note that $n_I = 1$ and so

$$\begin{aligned}A_{M^\circ,gM^\circ} &= (G(\tfrac{1}{2},\ell)/\ell)^{n_I}\left(\frac{(-1)^{\binom{n_I}{2}}\frac{\iota_{gM}}{\iota_M}\cdot\omega_\wedge(o_{gM/I},o_{M/I})}{\mathbb{F}_\ell}\right)\\ &= (G(\tfrac{1}{2},\ell)/\ell)\left(\frac{(-1)^{n-1}\omega(w_1,v_1)}{\mathbb{F}_\ell}\right)\\ &= \frac{1}{\ell}G(\tfrac{1}{2},\ell)\left(\frac{(-1)^n}{\mathbb{F}_\ell}\right)\\ &= \frac{1}{\ell}G(1,\ell)\left(\frac{(-1)^n\frac{1}{2}}{\mathbb{F}_\ell}\right)\end{aligned}.$$

Thus finally by lemma 3.7 we have that

$$\begin{aligned}\operatorname{tr}(g|\mathfrak{H}(V)) = \operatorname{tr}(g|C_{M^\circ}) &= A_{M^\circ,gM^\circ}\cdot\sum_{x\in\mathcal{S}}\psi\left(\frac{1}{2}\omega(m_x+n_x,x)\right)\\ &= \frac{1}{\ell}G(1,\ell)\left(\frac{-\frac{1}{2}}{\mathbb{F}_\ell}\right)\cdot\left(\frac{(-1)^n\frac{1}{2}f(1)}{\mathbb{F}_\ell}\right)G(1,\ell)\\ &= \frac{1}{\ell}G(1,\ell)^2\left(\frac{(-1)^{n-1}f(1)}{\mathbb{F}_\ell}\right)\\ &= \left(\frac{-1}{\mathbb{F}_\ell}\right)\left(\frac{(-1)^{n-1}f(1)}{\mathbb{F}_\ell}\right)\\ &= \left(\frac{(-1)^nf(1)}{\mathbb{F}_\ell}\right).\end{aligned}$$

Where the second last equality is due to [Lan86, p. 87], which asserts that

$$G(1,\ell) = \begin{cases}\sqrt{\ell} & \ell\equiv 1 \pmod 4\\ i\sqrt{\ell} & \ell\equiv 3 \pmod 4.\end{cases}$$

□

Theorem 3.15. Suppose $g\in\mathrm{Sp}(V)$ is semisimple with minimal polynomial f and $\dim V = 2n$.

Then

$$\mathrm{tr}(g|\mathfrak{H}(V)) = \left(\frac{(-1)^{n-(\dim V^g/2)}\det'(1-g)}{\mathbb{F}_\ell}\right)\sqrt{|V^g|},$$

where $\det'$ is the *regularised determinant*.

Proof. By lemma 3.12 decompose V as a direct sum of g-invariant symplectic subspaces

$$V = S_1 \oplus S_{-1} \oplus V_1 \oplus \cdots \oplus V_r.$$

Where $S_{\pm 1}$ is the ± 1 eigenspace of g respectively, and V_i are subspaces such that the restriction $g|_{V_i}$ of the g-action to V_i has characteristic polynomial f_i, where f_i has no repeated roots.

Then by lemma 3.13 we can write

$$\mathrm{tr}(g|\mathfrak{H}(V)) = \mathrm{tr}(g|\mathfrak{H}(S_1))\,\mathrm{tr}(g|\mathfrak{H}(S_{-1}))\prod_{i=1}^{r}\mathrm{tr}(g|\mathfrak{H}(V_i)).$$

Since g acts as Id and $-\mathrm{Id}$ on S_1 and S_{-1} respectively, it is easy to compute the traces using corollary 3.8 by taking any invariant Lagrangian

$$\mathrm{tr}(g|\mathfrak{H}(S_1)) = \sqrt{|S_1|} = \sqrt{|V^g|},$$

and

$$\mathrm{tr}(g|\mathfrak{H}(S_{-1})) = \left(\frac{(-1)^{\dim S_{-1}/2}}{\mathbb{F}_\ell}\right).$$

In particular, note that since S_{-1} is even dimensional, the characteristic polynomial of g restricted to S_{-1} is an even power of $(t+1)$, which in particular means that if we denote f_{-1} as the characteristic polynomial of g on S_{-1}, then we can write instead

$$\mathrm{tr}(g|\mathfrak{H}(S_{-1})) = \left(\frac{(-1)^{\dim S_{-1}/2} f_{-1}(1)}{\mathbb{F}_\ell}\right).$$

Combining this with lemma 3.14 we obtain

$$\begin{aligned}\mathrm{tr}(g|\mathfrak{H}(V)) &= \sqrt{|V^g|}\cdot\left(\frac{(-1)^{\dim S_{-1}/2} f_{-1}(1)}{\mathbb{F}_\ell}\right)\cdot\prod_{i=1}^{r}\left(\frac{(-1)^{(\dim V_i)/2} f_i(1)}{\mathbb{F}_\ell}\right)\\ &= \sqrt{|V^g|}\left(\frac{(-1)^{(\dim S_{-1}+\dim V_1+\cdots\dim V_r)/2} f_{-1}f_1f_2\ldots f_r(1)}{\mathbb{F}_\ell}\right)\end{aligned}.$$

Note that $\dim S_{-1} + \dim V_1 + \cdots \dim V_r = 2n - \dim S_1 = 2n - \dim V^g$, since the 1-eigenspace S_1 is precisely the g fixed points V^g.

Finally, we note that the kernel of $1-g$ is precisely the 1-eigenspace S_1, so the characteristic polynomial of $1-g$ on the quotient V/S_1 is precisely $f_{-1}f_1f_2\ldots f_r(1+t)$. Thus we have the regularised determinant $\det'(1-g)$ is equal to $f_{-1}f_1f_2\ldots f_r(1)$ and so we have

$$\mathrm{tr}(g|\mathfrak{H}(V)) = \left(\frac{(-1)^{n-(\dim V^g/2)}\det'(1-g)}{\mathbb{F}_\ell}\right)\sqrt{|V^g|},$$

as desired. □

Finally we prove the main theorem of this section.

Proof of theorem 3.2. By lemma 3.5 and the Stone-von Neumann property, we know that $\mathcal{H}$ is

isomorphic to $\mathfrak{H}(J[\ell])$. Thus

$$\mathrm{tr}(\mathrm{Fr}_q \,|\mathcal{H}) = \mathrm{tr}(\mathrm{Fr}_q \,|\mathfrak{H}(J[\ell])).$$

Then applying theorem 3.15 and noting that the Fr_q fixed points of $J[\ell]$ is precisely $J[\ell](\mathbb{F}_q)$ we obtain our desired result. □

3.4 An Arithmetic Path Integral

3.4.1 Defining an Arithmetic Action

As mentioned in the introduction, for J the Jacobian of X, there is a diagram

$$\begin{array}{ccc} \overline{J}[\ell] & \hookrightarrow & J[\ell] \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\overline{\mathbb{F}}_q) & \longrightarrow & \mathrm{Spec}(\mathbb{F}_q). \end{array}$$

We can consider the finite group scheme of ℓ-torsion points of the Jacobian, $J[\ell]$, to be a manifold fibered over the circle $\mathrm{Spec}(\mathbb{F}_q)$ with finite fibres.

We can then view a rational ℓ-torsion point $\gamma \in J[\ell](\mathbb{F}_q)$ as a section over this 'fibre bundle over S^1'

$$\begin{array}{c} J[\ell] \\ \downarrow \uparrow \gamma \\ \mathrm{Spec}(\mathbb{F}_q). \end{array}$$

We take $J[\ell]$ to be the arithmetic analogue of the phase space. We will define an arithmetic pairing of the form

$$A\colon J[\ell](\mathbb{F}_q) \times J[\ell](\mathbb{F}_q) \to \frac{1}{\ell}\mathbb{Z}/\mathbb{Z},$$

and the arithmetic action $A(\gamma)$ will be defined as the pairing A of γ with itself $A(\gamma) \coloneqq A(\gamma, \gamma)$.

As a sum over the space $J[\ell](\mathbb{F}_q)$, this can be viewed as being analogous to the space of all loops in the phase space. However, the integral described in section 3.2 is over not just closed loops, but paths where just the position co-ordinates are periodic. It seems our arithmetic result is an analogue of the case where the integral over the phase space loops is equal to the entire integral. We are not entirely sure when this holds, but it seems related to the exactness of the semi-classical approximation.

Let $\mathrm{CH}_0(X) \simeq \mathrm{Pic}(X)$ denote the Chow group, then by geometric class field theory there is a reciprocity map

$$\mathrm{Rec}\colon\ \mathrm{CH}_0(X) \to \pi_1^{\mathrm{ab}}(X).$$

Let $\mathrm{CH}_0(X)^0 \simeq \mathrm{Pic}^0(X) \simeq J(\mathbb{F}_q)$ denote the subgroup of CH_0 consisting of degree 0 algebraic cycles. Then via the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{CH}_0(X)^0 & \longrightarrow & \mathrm{CH}_0 & \xrightarrow{\deg} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Rec}} & & \downarrow & & \\ 0 & \longrightarrow & \pi_1^{\mathrm{ab}}(X)^0 = \pi_1^{\mathrm{ab}}(\overline{X}) & \longrightarrow & \pi_1^{\mathrm{ab}}(X) & \longrightarrow & \widehat{\mathbb{Z}} \simeq \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) & \longrightarrow & 0 \end{array}.$$

The reciprocity map restricts to

$$\mathrm{Rec}\colon J(\mathbb{F}_q) = \mathrm{CH}_0(X)^0 \to \pi_1^{\mathrm{ab}}(X)^0,$$

and also to the ℓ-torsion of both groups

$$\mathrm{Rec}\colon J[\ell](\mathbb{F}_q) = \mathrm{CH}_0(X)^0[\ell] \to \pi_1^{\mathrm{ab}}(X)^0[\ell].$$

On the other hand, an ℓ-torsion point $\gamma \in J[\ell](\mathbb{F}_q)$ defines a line bundle L_γ over X such that $(L_\gamma)^{\otimes \ell} \simeq \mathcal{O}_X$.

Suppose we fix an isomorphism $f\colon (L_\gamma)^{\otimes \ell} \xrightarrow{\sim} \mathcal{O}_X$. Since we assumed that $\mu_\ell \subset \mathbb{F}_q$, fix an isomorphism between μ_ℓ and $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ and identify the two. Then we can define a $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z} = \mu_\ell$ torsor $c_{\gamma,f}$ via the construction

$$c_{\gamma,f}(U) \coloneqq \left\{ y \in \Gamma(L_\gamma, U) : f(y^{\otimes \ell}) = 1 \right\}$$

for any étale map $U \to X$. This torsor defines a class in $c_{\gamma,f} \in H^1\left(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right)$.

Lemma 3.16. Given two torsion points $\beta, \gamma \in J[\ell](\mathbb{F}_q)$ and isomorphisms $g\colon (L_\gamma)^{\otimes \ell} \xrightarrow{\sim} \mathcal{O}_X$, $f\colon (L_\beta)^{\otimes \ell} \xrightarrow{\sim} \mathcal{O}_X$, be chosen isomorphisms of line bundles respectively. Then $L_{\beta+\gamma} = L_\beta \otimes L_\gamma$, and as classes in $H^1\left(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right)$ the addition of torsors is given by

$$c_{\beta,f} + c_{\gamma,g} = c_{\beta+\gamma, g\otimes f}.$$

Proof. $L_{\beta+\gamma} = L_\beta \otimes L_\gamma$ follows from the fact that the group law on the Jacobian is the same as the group law on the Picard group, which is the tensor product of line bundles.

In order to add the two torsors $c_{\beta,g}$ and $c_{\gamma,f}$, we first take the product sheaf $c_{\beta,f} \times c_{\gamma,f}$ which is a $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \times \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ torsor, then we pushout along the summation map $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \times \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \xrightarrow{+} \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ to obtain the torsor $c_{\beta,g} + c_{\gamma,f}$. For any étale $U \to X$, this pushout identifies $(y, z) \in c_{\beta,g} \times c_{\gamma,f}(U)$ with $(\zeta y, \zeta^{-1} z)$, for any root of unity $\zeta \in \mu_\ell$.

This sheaf is clearly the same as the torsor $c_{\beta+\gamma,g\otimes f}$, and thus we conclude that $c_{\beta,g} + c_{\gamma,f} = c_{\beta+\gamma,g\otimes f}$. □

Corollary 3.17. Any two isomorphisms $f, f'\colon (L_\gamma)^{\otimes \ell} \xrightarrow{\sim} \mathcal{O}_X$ will differ only by the scaling of a constant $a \in \mathbb{F}_q^\times$, and thus the torsors $c_{\gamma,f}$ and $c_{\gamma,f'}$ will differ by an element in $H^1\left(\mathrm{Spec}(\mathbb{F}_q), \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right)$, and so an ℓ-torsion point γ defines a class in

$$c_\gamma \in \frac{H^1\left(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right)}{H^1\left(\mathrm{Spec}(\mathbb{F}_q), \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right)}.$$

Proof. This follows directly from the previous lemma by taking $\beta = 0$ and $g = a$ being the scaling map. □

Remark 3.18. Note that by the Kummer exact sequence there is an exact sequence of cohomology

$$0 \to \mathbb{F}_q^\times/\mathbb{F}_q^{\times \ell} \xrightarrow{\kappa} H^1(X, \mu_\ell) \to H^1(X, \mathbb{G}_m)[\ell] \to 0,$$

and $H^1(X, \mathbb{G}_m)[\ell] = \mathrm{Pic}(X)[\ell] = \mathrm{Pic}^0(X)[\ell] = J[\ell](\mathbb{F}_q)$, and thus there is a surjective map given by pushing out a μ_ℓ torsor along the map $\mu_\ell \to \mathbb{G}_m$ to obtain a $\mathbb{G}_m$ torsor

$$s\colon H^1(X, \mu_\ell) \twoheadrightarrow J[\ell](\mathbb{F}_q).$$

Quotienting by the kernel, the inverse of the map

$$\overline{s}\colon \frac{H^1(X, \mu_\ell)}{\mathrm{Im}(\kappa)} \xrightarrow{\sim} J[\ell](\mathbb{F}_q)$$

is precisely the map $\gamma \mapsto c_\gamma$ defined above.

Finally, since there is an isomorphism

$$H^1\left(X, \tfrac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right) = \mathrm{Hom}\left(\pi_1^{\mathrm{ab}}(X), \tfrac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right)$$

we define the pairing

Definition 3.19. Define A to be the pairing of elements in $\mathrm{CH}_0(X)^0[\ell] = J[\ell](\mathbb{F}_q)$ given by

$$A(\gamma, \beta) \coloneqq c_\gamma(\mathrm{Rec}(\beta)),$$

where we view the torsor c_γ as a homomorphism from $\pi_1^{\mathrm{ab}}(X)$ to $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$. Noting that the image of the reciprocity map lies inside the kernel of $\pi_1(X) \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Thus this is a well-defined function

$$A\colon J[\ell](\mathbb{F}_q) \times J[\ell](\mathbb{F}_q) \to \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}.$$

Proposition 3.20. Suppose $J(\mathbb{F}_q)$ has no points of order ℓ^2, then the pairing A is non-degenerate bilinear form on the $\mathbb{F}_\ell$ vector space $J[\ell](\mathbb{F}_q)$.

Proof. The linearity of the first argument follows from lemma 3.16. The linearity of the second argument follows from the linearity of the reciprocity map and Hom.

Fix a non-zero $\beta \in J[\ell](\mathbb{F}_q)$, since $J(\mathbb{F}_q)$ has no points of order ℓ^2, it follows that γ is not ℓ-divisible. Since the reciprocity map $\mathrm{Rec}\colon J(\mathbb{F}_q) \to \pi_1^{\mathrm{ab}}(X)^0$ is an isomorphism, $\mathrm{Rec}(\beta)$ is an ℓ-torsion point of $\pi_1^{\mathrm{ab}}(X)$ that is also not ℓ-divisible. There must exist a homomorphism $\phi\colon \mathrm{Hom}(\pi_1^{\mathrm{ab}}(X)) \to \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ such that $\phi(\mathrm{Rec}(\beta)) \neq 0$, and thus there must exist a γ such that $c_\gamma(\mathrm{Rec}(\beta)) \neq 0$, so A is non-degenerate. □

Letting $A(\gamma) = A(\gamma, \gamma)$, we define the *arithmetic path integral* of A to be

$$\sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)}.$$

Before we compute this path integral, let us first deduce some properties of the action A.

3.4.2 Relation to the Abelian Chern-Simons Pairing

We show that the action A above can be identified wtih a function field analogue of the Abelian Chern-Simons pairing defined in [Chu+19]. Throughout this section we assume that $\mu_{\ell^2} \subset \mathbb{F}_q$, and thus by fixing an isomorphism $\zeta\colon \mu_{\ell^2} \xrightarrow{\sim} \mathbb{Z}/\ell^2\mathbb{Z}$ as Galois modules and sheaves, we can identify all cohomology groups with μ_{ℓ^2} and $\mathbb{Z}/\ell^2\mathbb{Z}$ coefficients, as well as cohomology groups with μ_ℓ and $\mathbb{Z}/\ell\mathbb{Z}$ coefficients.

We recall the statement of Artin–Verdier Duality applied to the sheaf $\mathcal{F} = \mathbb{Z}/\ell\mathbb{Z} \cong \mu_\ell$.

Theorem 3.21 ([Mil06, Cor. 3.3])**.** There is a pairing given by cup product

$$\langle \cdot, \cdot \rangle : H^r(X, \mathbb{Z}/\ell\mathbb{Z}) \times H^{3-r}(X, \mu_\ell) \xrightarrow{\cup} H^3(X, \mathbb{G}_m) \xrightarrow[\mathrm{inv}]{\sim} \mathbb{Q}/\mathbb{Z}$$

which induces an isomorphism

$$H^{3-r}(X, \mu_\ell) \xrightarrow{\sim} H^{3-r}(X, \mathbb{Z}/\ell\mathbb{Z})^\vee$$

Since $H^i(X, \mathbb{Z}/\ell\mathbb{Z})$ is ℓ-torsion, the image of any homomorphism from the group to $\mathbb{Q}/\mathbb{Z}$ must lie in $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$.

We define Bockstein operators δ to be the connecting homomorphism coming from the exact

sequence of sheaves $0 \to \mu_\ell \to \mu_{\ell^2} \to \mu_\ell \to 0$.

$$\delta\colon H^i(X, \mu_\ell) \to H^{i+1}(X, \mu_\ell)$$

Similarly we also define δ' to be the Bockstein operator coming from $0 \to \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}/\ell^2\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z} \to 0$.

$$\delta'\colon H^i(X, \mathbb{Z}/\ell\mathbb{Z}) \to H^{i+1}(X, \mathbb{Z}/\ell\mathbb{Z})$$

These operators are compatible with ζ_* such that there is an equality of maps $\zeta_* \circ \delta' = \delta \circ \zeta_*$. I.e. the following diagram commutes

$$\begin{array}{ccc} H^1(X, \mathbb{Z}/\ell\mathbb{Z}) & \xrightarrow{\delta'} & H^2(X, \mathbb{Z}/\ell\mathbb{Z}) \\ \downarrow{\scriptstyle \zeta_*} & & \downarrow{\scriptstyle \zeta_*} \\ H^1(X, \mu_\ell) & \xrightarrow{\delta} & H^2(X, \mu_\ell). \end{array}$$

Definition 3.22. We define the abelian Chern Simons pairing as follows

$$\mathrm{CS}(\cdot\,,\cdot)\colon H^1(X, \mathbb{Z}/\ell\mathbb{Z}) \times H^1(X, \mu_\ell) \to \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$$

$$(\alpha, \beta) \mapsto \mathrm{inv}(\alpha \cup \delta\beta)$$

Lemma 3.23 ([Chu+19, Lemma 2.1])**.** Given classes $\alpha \in H^1(X, \mathbb{Z}/\ell\mathbb{Z})$ and $\beta \in H^1(X, \mu_\ell)$, the Bockstein operators satisfies the identity

$$\delta(\alpha \cup \beta) = \delta'\alpha \cup \beta - \alpha \cup \delta\beta.$$

Proof. Since X is a projective variety, it suffices by [Mil13, 10.2] to verify the above formula is true in Čech cohomology.

Let $\mathcal{U} = (U_i)_{i\in I}$ be an étale covering of X. We write $U_{ij} \coloneqq U_i \times_C U_j$, $U_{ijk} \coloneqq U_i \times_C U_j \times_C U_k$, etc.

Suppose α is represented by the Čech cocycle $(\alpha_{ij})_{i,j\in I} \in Z^1(\mathcal{U}, \mathbb{Z}/\ell\mathbb{Z})$. In order to compute $\delta'\alpha$ explicitly, we first pick for every pair (i, j), a lift $\widetilde{\alpha}_{ij}$ of α_{ij} to $\mathbb{Z}/\ell^2\mathbb{Z}$. Then the class of $\delta'\alpha$ can be represented by the 2-cocycle whose sections are

$$(\delta'\alpha)_{ijk} \coloneqq d(\widetilde{\alpha})_{ijk} = \widetilde{\alpha}_{ij}|_{U_{ijk}} - \widetilde{\alpha}_{ik}|_{U_{ijk}} + \widetilde{\alpha}_{jk}|_{U_{ijk}}$$

which takes values in $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathbb{Z}/\ell^2\mathbb{Z}$. We can similarly represent $\delta_1\beta$ as a Čech cocyle in the same way.

The cup product $\alpha \cup \beta$ is represented by the cocycle

$$(\alpha \cup \beta)_{ijk} = \alpha_{ij}|_{U_{ijk}} \otimes \beta_{jk}|_{U_{ijk}}$$

which when lifted to $\mathbb{Z}/\ell^2\mathbb{Z} \otimes \mu_{\ell^2}$ is the cocyle $\widetilde{\alpha}_{ij}|_{U_{ijk}} \otimes \widetilde{\beta}_{jk}|_{U_{ijk}}$. Applying the isomorphism

$\mathbb{Z}/\ell^2\mathbb{Z} \otimes \mu_{\ell^2} \simeq \mu_{\ell^2}$ given by $a \otimes b \mapsto a \cdot b$, the cocycle representing $\delta(\alpha \cup \beta)$ will be

$$\begin{aligned}
(\delta(\alpha \cup \beta))_{ijkl} \coloneqq & (\widetilde{\alpha} \cup \widetilde{\beta})_{jkl}|_{U_{ijkl}} - (\widetilde{\alpha} \cup \widetilde{\beta})_{ikl}|_{U_{ijkl}} + (\widetilde{\alpha} \cup \widetilde{\beta})_{ijl}|_{U_{ijkl}} - (\widetilde{\alpha} \cup \widetilde{\beta})_{ijk}|_{U_{ijkl}} \\
&= \left(\widetilde{\alpha}_{jk} \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} - \left(\widetilde{\alpha}_{ik} \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} + \left(\widetilde{\alpha}_{ij} \cdot \widetilde{\beta}_{jl}\right)|_{U_{ijkl}} - \left(\widetilde{\alpha}_{ij} \cdot \widetilde{\beta}_{jk}\right)|_{U_{ijkl}} \\
&= \left((\widetilde{\alpha}_{jk} - \widetilde{\alpha}_{ik}) \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} + \left(\widetilde{\alpha}_{ij} \cdot (\widetilde{\beta}_{jl} - \widetilde{\beta}_{jk})\right)|_{U_{ijkl}} \\
&= \left((\widetilde{\alpha}_{jk} - \widetilde{\alpha}_{ik}) \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} + \left(\widetilde{\alpha}_{ij} \cdot (\widetilde{\beta}_{jl} - \widetilde{\beta}_{jk})\right)|_{U_{ijkl}} + \left(\widetilde{\alpha}_{ij} \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} - \left(\widetilde{\alpha}_{ij} \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} \\
&= \left((\widetilde{\alpha}_{jk} - \widetilde{\alpha}_{ik} + \widetilde{\alpha}_{ij}) \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} + \left(\widetilde{\alpha}_{ij} \cdot (\widetilde{\beta}_{jl} - \widetilde{\beta}_{jk} - \widetilde{\beta}_{kl})\right)|_{U_{ijkl}} \\
&= \left((\delta'\alpha)_{ijk} \cdot \widetilde{\beta}_{kl}\right)|_{U_{ijkl}} + (\widetilde{\alpha}_{ij} \cdot (\delta_1\beta)_{jkl})|_{U_{ijkl}}.
\end{aligned}$$

□

Lemma 3.24. Upon identifying $H^1(X, \mu_\ell)$ with $H^1(X, \mathbb{Z}/\ell\mathbb{Z})$ via ζ^*, the Abelian Chern-Simons pairing is symmetric

$$\mathrm{CS}(\alpha, \beta) = \mathrm{CS}(\beta, \alpha).$$

Proof. Consider the pro-sheaf $\mathbb{Z}_\ell(1) \coloneqq \varprojlim_i \mu_{\ell^i}$, there is an exact sequence

$$0 \to \mathbb{Z}_\ell(1) \xrightarrow{\ell} \mathbb{Z}_\ell(1) \to \mu_\ell \to 0$$

which induces the long exact sequence

$$\cdots \to H^2(X, \mathbb{Z}_\ell(1)) \to H^2(X, \mu_\ell) \to H^3(X, \mathbb{Z}_\ell(1)) \to \cdots.$$

Since $H^3(X, \mathbb{Z}_\ell(1)) = \varprojlim_i H^3(X, \mu_{\ell^i}) = \varprojlim_i H^3(X, \mu_{\ell^i}) = \mathbb{Z}_\ell$ is torsion free, the boundary map $H^2(X, \mu_\ell) \to H^3(X, \mathbb{Z}_\ell(1))$ is a map from an ℓ-torsion group into a torsion-free group, so must be the zero map. This implies that $H^2(X, \mathbb{Z}_\ell(1)) \to H^2(X, \mu_\ell)$ is surjective.

Since the quotient map $\mathbb{Z}_\ell(1) \to \mu_\ell$ factors through μ_{ℓ^2}, the map $H^2(X, \mathbb{Z}_\ell(1)) \to H^2(X, \mu_\ell)$ factors through $H^2(X, \mu_{\ell^2})$, which implies that $H^2(X, \mu_{\ell^2}) \to H^2(X, \mu_\ell)$ is also surjective. Then from the exact sequence

$$\cdots \to H^2(X, \mu_{\ell^2}) \to H^2(X, \mu_\ell) \xrightarrow{\delta_2} H^3(X, \mu_\ell) \to \cdots$$

it is deduced that $\delta_2 \colon H^2(X, \mu_\ell) \to H^3(X, \mu_\ell)$ is the zero map.

Thus, by the previous lemma

$$\delta'\alpha \cup \beta = \alpha \cup \delta\beta.$$

Finally we conclude

$$\mathrm{CS}(\alpha, \beta) = \mathrm{inv}(\alpha \cup \delta\beta) = \mathrm{inv}(\delta'\alpha \cup \beta) = \mathrm{inv}(\beta \cup \delta'\alpha) = \mathrm{inv}(\beta \cup \delta'\alpha) = CS(\beta, \alpha).$$

□

Proposition 3.25. The image of $\mathbb{F}_q^\times$ in $H^1(X, \mu_\ell)$ under the Kummer map lies in the kernel of the Abelian Chern-Simons pairing, and thus the pairing factors into a pairing of the form

$$\mathrm{CS} \colon \frac{H^1(X, \mu_\ell)}{\mathbb{F}_q^\times} \times \frac{H^1(X, \mu_\ell)}{\mathbb{F}_q^\times} \to \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}.$$

Proof. By remark 3.18 it suffices to show that $H^1(\mathrm{Spec}(\mathbb{F}_q), \mathbb{Z}/\ell\mathbb{Z})$ is in the kernel of the pairing.

Consider the commutative diagram

$$\begin{array}{ccc} H^1(\mathrm{Spec}(\mathbb{F}_q), \mathbb{Z}/\ell\mathbb{Z}) & \hookrightarrow & H^1(X, \mathbb{Z}/\ell\mathbb{Z}) \\ \downarrow \delta & & \delta \downarrow \\ H^2(\mathrm{Spec}(\mathbb{F}_q), \mathbb{Z}/\ell\mathbb{Z}) & \longrightarrow & H^2(X, \mathbb{Z}/\ell\mathbb{Z}) \end{array}$$

where both vertical morphisms are the Bockstein connecting homomorphisms coming from the exact sequence $0 \to \mathbb{Z}/\ell\mathbb{Z} \to \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z} \to 0$. But since $\mathrm{Spec}(\mathbb{F}_q)$ has cohomological dimension 1, $H^2(\mathrm{Spec}(\mathbb{F}_q), \mathbb{Z}/\ell\mathbb{Z}) = 0$. Thus the Bockstein of the image of $H^1(\mathrm{Spec}(\mathbb{F}_q), \mathbb{Z}/\ell\mathbb{Z})$ is equal to zero.

Thus if $b \in H^1(\mathrm{Spec}(\mathbb{F}_q), \mathbb{Z}/\ell\mathbb{Z})$, then

$$CS(-, b) = 0.$$

Since we have shown in lemma 3.24 that the pairing is symmetric, the result follows. □

We now wish to show that under the above identifications, the pairings CS and A agree, but first we will show the following proposition, which is the function field analogue of [LST20, Proposition 6.3], the statement and proof of the following theorem follows Section 6.1 of [LST20] quite closely.

Proposition 3.26. The following two pairings $H^1(X, \mathbb{G}_m) \times H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}) \to \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ are equal:

1. Identify $H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ with $\mathrm{Hom}(\pi_1^{\mathrm{ab}}(X), \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ and then with $\mathrm{Hom}(\mathrm{Pic}(X), \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ via the reciprocity map. Identify $H^1(X, \mathbb{G}_m)$ with $\mathrm{Pic}(X)$. Then pair $\mathrm{Pic}(X)$ and $\mathrm{Hom}(\mathrm{Pic}(X), \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ via the evaluation map.

$$\begin{array}{ccccc} H^1(X, \mathbb{G}_m) & \times & H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}) & \longrightarrow & \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \\ \| & & \| & & \\ \mathrm{Pic}(X) & \times & \mathrm{Hom}(\pi_1^{\mathrm{ab}}(X), \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}) & & \downarrow \sim \\ \| & & \| & & \\ \mathrm{Pic}(X) & \times & \mathrm{Hom}(\mathrm{Pic}(X), \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}) & \to & \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \end{array}$$

2. Map $H^1(X, \mathbb{G}_m)$ to $H^2(X, \mu_\ell)$ via κ the Kummer map, then take the cup product with $H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ to obtain an element of $H^3(X, \mu_\ell)$, then take the invariant map to obtain an element of $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$.

$$\begin{array}{ccccccc} H^1(X, \mathbb{G}_m) & \times & H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}) & & & & \\ \downarrow \kappa & & \| & & & \searrow & \\ H^2(X, \mu_\ell) & \times & H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}) & \xrightarrow[\cup]{} & H^3(X, \mu_\ell) & \xrightarrow[\mathrm{inv}]{} & \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \end{array}$$

Proof. Let K be the function field of X. Fix an element $\alpha \in H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$. Since $H^1(X, \mathbb{G}_m) = \mathrm{Pic}(X)$ is generated by divisors of a single point v, it suffices to check that the pairings agree for every $[v]$ and α.

We consider the first pairing. The reciprocity map takes the divisor $[v]$ to $\mathrm{Frob}_v \in \pi_1^{\mathrm{ab}}(X)$. Then pairing of α and $[v]$ is given by the action of Frob_v on the $\overline{\mathbb{F}}_q$-points of α. In particular, since Frob_v acts on K_v, this pairing uniquely determined by the pairing of Frob_v with the pullback $\alpha_v \in H^1(\mathrm{Spec}\, \mathcal{O}_{K_v}, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ of α via the map $\mathrm{Spec}\, \mathcal{O}_{K_v} \to X$.

Now we consider the second pairing. Let π be a uniformiser of K_v, the local field at the point v. We first show that by mapping $\pi \in H^0(K_v, \mathbb{G}_m)$ along the top row of the commutative diagram in lemma 3.27, we get the divisor $[v]$.

We let $U = X \setminus \{v\}$. An element of $H^1_c(U, \mathbb{G}_m)$ can be expressed as a line bundle on U with trivialisation at the punctured neighbourhood $\mathrm{Spec}\, K_v$ of v. Via this identification, the image of the map $H^0(v, \mathbb{G}_m) \to H^1_c(U, \mathbb{G}_m)$ sends the element π to the trivial line bundle with identity trivialisation on U, with trivialisation at v given by multiplication by π.

On the other hand, a line bundle L on U with a trivialisation on the punctured neighbourhood $\mathrm{Spec}\, K_v$ can be uniquely extended to a line bundle on all of X via taking only the sections of $L(U)$ whose image under trivialisation does not have a pole at v. For our line bundle above, the sections of $\mathcal{O}_U$ which do not have poles after multiplying by π are precisely those which have at most a simple pole at v, but this is precisely the sheaf corresponding to the divisor $[v]$.

Thus by the commutative diagram in lemma 3.27, we have that the Artin-Verdier pairing $\mathrm{inv}(\kappa[v] \cup \alpha)$ is equal to the invariant map of the local cup product $\mathrm{inv}_{K_v}(\kappa(\pi) \cup \alpha_v)$. By lemma 3.28 we conclude

$$\mathrm{inv}(\kappa[v] \cup \alpha) = \mathrm{inv}_{K_v}(\kappa(\pi) \cup \alpha_v) = \alpha_v(\mathrm{Frob}_v).$$

□

Lemma 3.27. Let $\alpha \in H^1(X, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$, v be a place of X with punctured neighbourhood $\operatorname{Spec} K_v$, $\alpha_v \in H^1(\mathcal{O}_{K_v}, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ to be the pullback of α via $\operatorname{Spec} \mathcal{O}_{K_v} \to X$, and $U = X - \{v\}$. Then the following diagram commutes:

$$\begin{array}{ccccc}
H^0(K_v, \mathbb{G}_m) & \longrightarrow & H^1_c(U, \mathbb{G}_m) & \longrightarrow & H^1(X, \mathbb{G}_m) \\
\downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\
H^1(K_v, \mu_\ell) & \longrightarrow & H^2_c(U, \mu_\ell) & \longrightarrow & H^2(X, \mu_\ell) \\
\downarrow{\scriptstyle \cup \alpha_v} & & \downarrow{\scriptstyle \cup \alpha} & & \downarrow{\scriptstyle \cup \alpha} \\
H^2(K_v, \mu_\ell) & \longrightarrow & H^3_c(U, \mu_\ell) & \longrightarrow & H^3(X, \mu_\ell) \\
\Vert{\scriptstyle \mathrm{inv}} & & \Vert{\scriptstyle \mathrm{inv}} & & \Vert{\scriptstyle \mathrm{inv}} \\
\frac{1}{\ell}\mathbb{Z}/\mathbb{Z} & = & \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} & = & \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}
\end{array}$$

Where κ is the Kummer map arising from the Kummer exact sequence, the horizontal maps in the left column arise from the exact sequence of compactly supported cohomology in [Mil06, II.2.3(a)], and the horizontal maps in the right column arise from [Mil06, II.2.3(d)] and the fact that $H^r_c(X, \mathcal{F}) = H^r(X, \mathcal{F})$ since X is compact.

Proof. The compactly supported cohomology groups $H^\star_c(U, \mathcal{F})$ are defined as a shifted mapping cone of the localisation morphism of Čech cochains $\mathrm{loc}\colon C^\bullet(U, \mathcal{F}) \to C^\bullet(K_v, \mathcal{F}_v)$, or in other words the compactly supported cohomology groups $H^r_c(U, \mathcal{F})$ are the cohomology groups of the complex

$$\operatorname{cone}^\bullet(\mathrm{loc}[-1]) = C^\bullet(U, \mathcal{F}) \oplus C^\bullet(K_v, \mathcal{F}_v)[-1].$$

So on the level of cochains, the left column horizontal maps $H^r(K_v, \mathcal{F}_v) \to H^{r+1}_c(U, \mathcal{F})$ is given by the inclusion map into the local component of the mapping cone.

On the other hand the right column horizontal arrows are obtained on the level of cochains via the composition

$$C^\bullet(U, \mathcal{F}) \oplus C^\bullet(K_v, \mathcal{F}_v)[-1] \to C^\bullet(U, \mathcal{F}) \to C^\bullet(X, \mathcal{F}).$$

On the level of cochains, the connecting homomorphism κ is obtained via the composition of inverse image and differential maps; and the cup product with α can be interpreted as a tensor product of Čech cocycles. All of these maps commutes with the inclusions, projections and pullbacks, and so the diagram commutes. □

Lemma 3.28. Let $K = K_v$ be a non-archimedean local field. Let $G = \pi_1(\operatorname{Spec} K_v) = \operatorname{Gal}(\overline{K_v}/K_v)$ and $\Gamma = \pi_1(\operatorname{Spec} \mathcal{O}_{K_v}) = \operatorname{Gal}(K_v^{ur}/K_v)$ be the absolute Galois group and maximal unramified Galois group of K_v respectively. Suppose we are given a uniformiser $\pi \in H^0(K_v, \mathbb{G}_m)$ and an element $\alpha \in H^1(\mathcal{O}_{K_v}, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$, then

$$\mathrm{inv}(\kappa(\pi) \cup \alpha) = \alpha(\mathrm{Frob}_v).$$

Here $\alpha \in H^1(\mathcal{O}_{K_v}, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}) = \operatorname{Hom}(\Gamma, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ is viewed as a homomorphism from Γ to $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$.

Proof. Let π_0 be an ℓth root of π so that $\pi_0^\ell = \pi$. Then a cocycle representing $\kappa(\pi) \in H^1(K_v, \mu_\ell)$ is $\sigma \mapsto \frac{\sigma(\pi_0)}{\pi_0}$.

Let ϕ be the cocycle representing $\kappa(\pi) \cup \alpha \in H^2(K_v, \mu_\ell)$. Since the map $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \times \mu_\ell \to \mu_\ell$ is given by $(q, \zeta) \mapsto \zeta^{\ell q}$, it follows that the cocycle ϕ is given by

$$\phi(\sigma, \tau) = \left(\frac{\sigma(\pi_0)}{\pi_0}\right)^{\ell\alpha(\tau)}.$$

Given an element $\sigma \in \Gamma$, let n_σ denote the unique element of $\{0, 1, \ldots, \ell - 1\}$ that is congruent to $\ell\alpha(\sigma)$. This definition can also be naturally be extended to $\sigma \in G$ via quotienting by the inertia subgroup first.

On the other hand, define the cocycle $\psi\colon \Gamma^2 \to K_v^{ur\times}$ giving a class $H^2(\Gamma, K_v^{ur\times})$ via

$$\psi(\sigma,\tau) = \begin{cases} 1 & \text{if } n_\sigma + n_\tau < \ell \\ \pi & \text{if } n_\sigma + n_\tau \geq \ell \end{cases}.$$

We define a cocycle $c\colon G \to \overline{K}_v^\times$ via $c(\sigma) = \pi_0^{n_\sigma}$. Then the coboundary of c is

$$\begin{aligned} dc(\sigma,\tau) &= \frac{\sigma c(\tau) c(\sigma)}{c(\sigma\tau)} \\ &= \frac{\sigma(\pi_0^{n_\tau})\pi_0^{n_\sigma}}{\pi_0^{n_{\sigma\tau}}} \\ &= \begin{cases} \dfrac{\sigma(\pi_0)^{n_\tau}}{\pi_0^{n_\tau}} & \text{if } n_\sigma + n_\tau < \ell \\ \pi\dfrac{\sigma(\pi_0)^{n_\tau}}{\pi_0^{n_\tau}} & \text{if } n_\sigma + n_\tau \geq \ell \end{cases} \\ &= \phi \inf \psi. \end{aligned}$$

Thus $[\phi] = (\inf[\psi])^{-1}$. Thus it suffices to compute $\mathrm{inv}(\inf([\psi]))$.

Now, from [CF67, p. 130] the invariant map $\mathrm{inv}\colon H^2(G, \overline{K}_v^\times) \to \mathbb{Q}/\mathbb{Z}$ is defined as the composition

$$H^2(G, \overline{K}_v^\times) \xleftarrow[\sim]{\inf} H^2(\Gamma, K_v^{ur\times}) \xrightarrow{\nu} H^2(\Gamma, \mathbb{Z}) \xleftarrow[\sim]{\rho} H^1(\Gamma, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\sim]{\gamma} \mathbb{Q}/\mathbb{Z}.$$

Where:

- ν is the map on cohomology induced by the valuation map $K_v^{ur\times} \to \mathbb{Z}$.
- ρ is the connecting homomorphism of the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.
- γ is the homomorphism $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ given by evaluating the homomorphism at the Frobenius element $\mathrm{Frob}_v \in \Gamma$.

Thus we wish to compute $\gamma \circ \rho^{-1} \circ \nu([\psi])$, firstly we see that

$$\nu(\psi)(\sigma,\tau) = \begin{cases} 0 & \text{if } n_\sigma + n_\tau < \ell \\ 1 & \text{if } n_\sigma + n_\tau \geq \ell. \end{cases}$$

On the other hand, by definition $\alpha \in \mathrm{Hom}(\Gamma, \frac{1}{\ell}\mathbb{Z}/\mathbb{Z})$ satisfies $\gamma(\alpha) = \alpha(\mathrm{Frob}_v)$, so it just suffices to prove that $\rho(\alpha) = \nu(\psi)$. Note that the cocycle $a\colon \Gamma \to \mathbb{Q}$ given by $a(\sigma) = \frac{n_\sigma}{\ell}$ is a lift of α, and a has coboundary

$$\begin{aligned} da(\sigma,\tau) &= \sigma a(\tau) + a(\sigma) - a(\sigma\tau) \\ &= \begin{cases} 0 & \text{if } n_\sigma + n_\tau < \ell \\ 1 & \text{if } n_\sigma + n_\tau \geq \ell \end{cases} \\ &= \nu(\psi). \end{aligned}$$

□

Finally, the main result of this subsection is the following theorem, showing that the Abelian Chern-Simons pairing agrees with the Class Field Theory pairing.

Theorem 3.29. Under the isomorphism $\overline{s}\colon \frac{H^1(X,\mu_\ell)}{\mathbb{F}_q^\times} \xrightarrow{\sim} J[\ell](\mathbb{F}_q)$ defined in proposition 3.25, the pairings A and CS agree. In other words the following diagram commutes

$$\begin{array}{ccccc} \frac{H^1(X,\mu_\ell)}{\mathbb{F}_q^\times} & \times & \frac{H^1(X,\mu_\ell)}{\mathbb{F}_q^\times} & \xrightarrow[\text{CS}]{} & \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \\ \downarrow{\scriptstyle \overline{s}} & & \downarrow{\scriptstyle \overline{s}} & & \downarrow \\ J[\ell](\mathbb{F}_q) & \times & J[\ell](\mathbb{F}_q) & \xrightarrow[A]{} & \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}. \end{array}$$

Proof. Let ι denote the map $H^r(X,\mu_\ell) \to H^r(X,\mathbb{G}_m)$ induced by the inclusion $\mu_\ell \hookrightarrow \mathbb{G}_m$.

Given elements $\alpha, \beta \in H^1(X,\mu_\ell)$, we see that the pairing $A(s(\alpha), s(\beta))$ can be identified with pairing (1) of $\iota(\alpha)$ and $\iota(\beta)$ in proposition 3.26.

On the other hand, observe that by functoriality, the map of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_\ell & \longrightarrow & \mu_{\ell^2} & \longrightarrow & \mu_\ell & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mu_\ell & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathbb{G}_m & \longrightarrow & 0 \end{array}$$

induces the following commutative diagram of cohomology:

$$\begin{array}{ccccc} H^r(X,\mu_\ell) & & \xrightarrow{\quad\delta\quad} & & H^r(X,\mu_\ell) \\ & {\scriptstyle\iota}\searrow & & \nearrow{\scriptstyle\kappa} & \\ & & H^r(X,\mathbb{G}_m) & & \end{array}$$

Where the Bockstein map factors through the Kummer map. Then it is easy to see that the pairing $\mathrm{CS}(\alpha,\beta)$ is equal to the pairing (2) of $\iota(\alpha)$ and $\iota(\beta)$ in proposition 3.26.

Finally, by proposition 3.26, these two pairings agree. □

An immediate corollary is the following:

Corollary 3.30. The pairing A is symmetric.

Proof. It follows from theorem 3.29 and lemma 3.24 that A is symmetric. □

3.4.3 Computation of the Arithmetic Path Integral

Theorem 3.31. Suppose $J(\mathbb{F}_q)$ has no points of order ℓ^2 and that $\mu_{\ell^2} \subset \mathbb{F}_q$. Then the arithmetic path integral evaluates to

$$\sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)} = \sqrt{|J[\ell](\mathbb{F}_q)|}\left(\frac{\det A}{\ell}\right)\left(i^{(\ell-1)^2/4}\right)^{\dim_\ell J[\ell](\mathbb{F}_q)}.$$

If additionally the Frobenius Fr_q acts semisimply on $J[\ell]$, then we can express the path integral as

$$\sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)} = \sqrt{|J[\ell](\mathbb{F}_q)|}\left(\frac{(-1)^{(\dim_\ell J[\ell](\mathbb{F}_q))/2}\det(A)}{\ell}\right).$$

Proof. By proposition 3.20 and corollary 3.30 A is a non-degenerate symmetric bilinear form, so we can write the sum as a Gaussian integral over a finite field of the form

$$\sum_{x \in \mathbb{F}_\ell^n} \exp\left[\frac{2\pi i}{l} x Q x^T\right].$$

Here, x is a vector representing γ, Q is the matrix representing A and $n = \dim_\ell J[\ell](\mathbb{F}_q)$. The factor of $\frac{1}{\ell}$ comes from the fact that A has image in $\frac{1}{l}\mathbb{Z}/\mathbb{Z}$ rather than $\mathbb{Z}/\ell\mathbb{Z}$.

Then applying the theorem in [Ner11, Chapter 9, Theorem 3.1], we obtain

$$\begin{aligned}\sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)} &= \ell^{\frac{n}{2}} \left(\frac{\det A}{\ell}\right) \left(i^{(\ell-1)^2/4}\right)^n \\ &= \sqrt{|J[\ell](\mathbb{F}_q)|} \left(\frac{\det A}{\ell}\right) \left(i^{(\ell-1)^2/4}\right)^{\dim_\ell J[\ell](\mathbb{F}_q)}\end{aligned}$$

Noting that

$$i^{(\ell-1)^2/4} = \begin{cases} 1, & \ell \equiv 1 \mod 4 \\ i, & \ell \equiv 3 \mod 4 \end{cases}$$

and thus in particular when $\ell \equiv 1 \mod 4$, this path integral is real and simply evaluates to

$$\sqrt{|J[\ell](\mathbb{F}_q)|} \left(\frac{\det A}{\ell}\right).$$

On the other hand, when $\ell \equiv 3 \pmod 4$, we note that if the Frobenius Fr_q acts semisimply on $J[\ell]$ then by proposition 3.10 that $\dim_\ell J[\ell](\mathbb{F}_q)$ is actually even, so the path integral is also real, and can be written as

$$(-1)^{(\dim_\ell J[\ell](\mathbb{F}_q))/2} \sqrt{|J[\ell](\mathbb{F}_q)|} \left(\frac{\det A}{\ell}\right).$$

Since $\left(\frac{-1}{\ell}\right) = \begin{cases} 1 & \ell \equiv 1 \mod 4 \\ -1 & \ell \equiv 3 \mod 4 \end{cases}$, we can combine these two expressions to obtain

$$\sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)} = \sqrt{|J[\ell](\mathbb{F}_q)|} \left(\frac{(-1)^{(\dim_\ell J[\ell](\mathbb{F}_q))/2} \det(A)}{\ell}\right).$$

□

3.5 Proving the Main Theorem

Finally, we combine the results of theorem 3.31 and theorem 3.2 to obtain our main theorem with all the signs determined.

Theorem 3.32. Let J be the Jacobian of a genus g curve X over a finite field $\mathbb{F}_q$. Let ℓ be an odd prime satisfying $q \equiv 1 \pmod{\ell^2}$. If Fr_q acts semisimply on the $\mathbb{F}_\ell$-vector space $J[\ell]$, and $J(\mathbb{F}_q)$ has no points of order ℓ^2, then we have the following equality

$$\mathrm{tr}(\mathrm{Fr}_q \,|\mathcal{H}) = \left(\frac{(-1)^g \det'(1 - \mathrm{Fr}_q) \det(A)}{\ell}\right) \sum_{\gamma \in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)},$$

where $\det'(1 - \mathrm{Fr}_q)$ is the regularised determinant of the linear map $1 - \mathrm{Fr}_q$ on vector space $J[\ell]$.

Proof. By combining theorems 3.2 and 3.31 we have the following equality where both sides are

equal to $\sqrt{|J[\ell](\mathbb{F}_q)|}$,

$$\left(\frac{(-1)^{g-\dim_\ell J[\ell](\mathbb{F}_q)/2}\det{}'(1-\mathrm{Fr}_q)}{\ell}\right)\mathrm{tr}(\mathrm{Fr}_q\,|\mathcal{H}) = \left(\frac{(-1)^{(\dim_\ell J[\ell](\mathbb{F}_q))/2}\det(A)}{\ell}\right)\sum_{\gamma\in J[\ell](\mathbb{F}_q)} e^{2\pi i A(\gamma)}.$$

Rearranging the Legendre symbols, we obtain the desired result. □

3.6 Computational Examples and Remarks

Although theorem 3.32 requires $\mu_{\ell^2}\subset\mathbb{F}_q$, we expect that the theorem to be true assuming only $\mu_\ell\subset\mathbb{F}_q$. In this section we give 2 sets of examples. One where $\mu_{\ell^2}\subset\mathbb{F}_q$ and one where $\mu_{\ell^2}\not\subset\mathbb{F}_q$.

3.6.1 Examples where $\mu_{\ell^2}\subset\mathbb{F}_q$

In this section we provide two explicit examples of theorem 3.32 for an elliptic curve $X/\mathbb{F}_q$, in the case where $q=19,\ell=3$.

Let us fix an isomorphism $\zeta\colon\{1,7,11\}=\mu_3(\mathbb{F}_{19})\simeq\mathbb{F}_3$ by sending $7\in\mu_3(\mathbb{F}_{19})$ to $1\in\mathbb{F}_3$. We also fix the isomorphism $\psi\colon\mathbb{F}_3\simeq\mu_3(\mathbb{C})$ via $1\mapsto\xi=e^{\frac{2\pi i}{3}}$.

Example 3.33. Let $X=E$ be the curve

$$E: y^2=x^3-5x/\mathbb{F}_{19}.$$

We can check that the only $\mathbb{F}_{19}$-rational 3-torsion point is the origin O_E, and that the 3-torsion group $E[3]$ is defined over the extension $\mathbb{F}_{19^4}/\mathbb{F}_{19}$. Explicitly, let $\mathbb{F}_{19^4}=\mathbb{F}_{19}(\alpha)$, where $\alpha\in\mathbb{F}_{19^4}$ satisfies the minimal polynomial

$$\alpha^4+\alpha^3+2\alpha^2+15\alpha+3=0.$$

Then using the `torsion_basis()` function on SageMath, the 3-torsion $E[3]$ is generated by the elements

$$P_1=(18\alpha^3+\alpha+17,7\alpha^3+15\alpha^2+\alpha+15)$$
$$P_2=(18\alpha^3+\alpha+11,14\alpha^3+4\alpha^2+9\alpha+17).$$

By a straightforward calculation we can see that the Frobenius acts on the basis elements in the following manner

$$\mathrm{Fr}_{19}\,P_1=P_1+2P_2$$
$$\mathrm{Fr}_{19}\,P_2=2P_1+2P_2.$$

Moreover, let $\langle-,-\rangle$ denote the Weil pairing on $E[3]$, via the `weil_pairing()` function on SageMath, we compute that

$$\langle P_1,P_2\rangle=7\in\mu_3(\mathbb{F}_{19}),$$

which we will identify with $\langle P_1,P_2\rangle=1\in\mathbb{F}_3$. From now on the values of the Weil pairing $\langle-,-\rangle$ refer to the values in $\mathbb{F}_3$ after identifying $\zeta\colon\mu_3(\mathbb{F}_{19})\simeq\mathbb{F}_3$.

Since $E[3]$ is a 2-dimensional symplectic space with respect to the Weil pairing, every 1-dimensional subspace is Lagrangian. However, the matrix $\left(\begin{smallmatrix}1&2\\2&2\end{smallmatrix}\right)$ is not diagonalisable over $\mathbb{F}_3$, so there does not exist any Frobenius-invariant Lagrangian. Let us pick the Lagrangian $M=\mathbb{F}_3P_1$, the 1-dimensional subspace generated by P_1. We also pick the complement $M'=\mathbb{F}_3P_2$, so that $E[3]=M\oplus M'$.

We now evaluate $\mathrm{tr}(\mathrm{Fr}_{19}\,|C_{M^\circ})$ via lemma 3.7.

First we compute the constant $A_{M^\circ,\mathrm{Fr}_{19}M^\circ}$. Fix the orientation $o_M = P_1$. Note that M and $\mathrm{Fr}_{19}M$ are transverse, so $I = M \cap \mathrm{Fr}_{19}M = \{O_E\}$ is 0-dimensional, and $n_I = 1$. We also have $o_{\mathrm{Fr}_{19}M} = \mathrm{Fr}_{19}P_1 = P_1 + 2P_2$, and since I is trivial we have that $o_{M/I} = o_M$ and $o_{\mathrm{Fr}_{19}M/I} = o_{\mathrm{Fr}_{19}M}$. We also compute that

$$G(\tfrac{1}{2}, 3) = \sum_{x\in\mathbb{F}_3} \psi(\tfrac{1}{2}x^2) = 1 + \xi^2 + \xi^2 = -i\sqrt{3}.$$

Thus we have

$$\begin{aligned} A_{M^\circ,\mathrm{Fr}_{19}M^\circ} &= (G(\tfrac{1}{2},3)/3)^1 \left(\frac{(-1)^{\binom{1}{2}}\langle P_1 + 2P_2, P_1\rangle}{\mathbb{F}_3}\right). \\ &= \frac{-i\sqrt{3}}{3}\left(\frac{1}{\mathbb{F}_3}\right) \\ &= \frac{-i\sqrt{3}}{3}. \end{aligned}$$

Now we compute the sum portion of the formula in lemma 3.7.

We note that $\mathcal{S} = M'$, since $M + \mathrm{Fr}_{19}M = E[3]$ spans the entire space. For each $x \in M' = \{O_E, P_2, 2P_2\}$, we wish to find elements $m_x, n_x \in M$ such that

$$\mathrm{Fr}_{19}\,x - x = m_x + \mathrm{Fr}_{19}\,n_x,$$

and we wish to evaluate the sum $\sum_{x\in\mathcal{S}} \psi\left(\frac{1}{2}\langle m_x + n_x, x\rangle\right)$.

By inspection, we can make the following choices of m_x, n_x and obtain the following values of $\langle m_x + n_x, x\rangle$

$$\begin{cases} m_{P_2} = O_E, & n_{P_2} = 2P_1, & \langle m_{P_2} + n_{P_2}, P_2\rangle = \langle 2P_1, P_2\rangle = 2 \\ m_{2P_2} = O_E, & n_{2P_2} = P_1, & \langle m_{2P_2} + n_{2P_2}, 2P_2\rangle = \langle P_1, 2P_2\rangle = 2 \\ m_{O_E} = O_E, & n_{O_E} = O_E, & \langle m_{O_E} + n_{O_E}, O_E\rangle = \langle O_E, O_E\rangle = 0 \end{cases}.$$

Thus we evaluate

$$\sum_{x\in\mathcal{S}} \psi\left(\frac{1}{2}\langle m_x + n_x, x\rangle\right) = \xi + \xi + 1 = i\sqrt{3}.$$

Finally, combining the two computations, we have that the trace is equal to

$$\begin{aligned} \mathrm{tr}(\mathrm{Fr}_{19}\,|C_{M^\circ}) &= A_{M^\circ,\mathrm{Fr}_{19}M^\circ} \sum_{x\in\mathcal{S}} \psi\left(\frac{1}{2}\langle m_x + n_x, x\rangle\right) \\ &= \frac{-i\sqrt{3}}{3}(i\sqrt{3}) \\ &= 1. \end{aligned}$$

On the other hand, since $E[3](\mathbb{F}_{19}) = \{O_E\}$ is zero-dimensional, the map A must just be the zero map, and thus the path integral trivially evaluates to 1.

We finally check that our computation indeed satisfies theorem 3.32, we check that the regularised determinant $\det'(1-\mathrm{Fr}_{19})$ is just equal to the determinant $\det(1-\mathrm{Fr}_{19}) = \det(\left(\begin{smallmatrix}0 & 1\\ 1 & 2\end{smallmatrix}\right)) = -1$.

Indeed, the trace and path integral in this example are both equal to 1, and thus differ by the sign

$$\left(\frac{(-1)^g \det'(1-\mathrm{Fr}_{19})}{\mathbb{F}_3}\right) = \left(\frac{1}{\mathbb{F}_3}\right) = 1.$$

Remark 3.34. In the above example, the trace computation was quite involved while the path

integral was trivial since $E[3]$ had no non-trivial $\mathbb{F}_{19}$-rational points. We will now provide a second example where the trace computation is simple due to the existence of an invariant Lagrangian, but the path integral computation is more intricate.

We also remark that in the elliptic curve case it is impossible for both the trace and the path integral to be 'interesting'. Due to our assumptions of the semisimplicity of Frobenius and $\mu_3 \subset \mathbb{F}_{19}$, it follows $E[3](\mathbb{F}_{19})$ must be an even dimensional linear subspace of $E[3]$, which means it must be trivial or the entire space. If it is zero dimensional, then the path integral is trivial; if it is the entire space, then Fr_{19} must act trivially on $E[3]$, and every Lagrangian is Frobenius-invariant.

For higher genus curves there will exist examples where both the trace and path integral are non-trivial computations.

Example 3.35. Let $X = E$ be the curve

$$E : y^2 = x^3 + 12x - 1/\mathbb{F}_{19}.$$

In this case, we notice that the 3-torsion $E[3] \subset E(\mathbb{F}_{19})$ is $\mathbb{F}_{19}$-rational. This means that the Frobenius Fr_{19} acts trivially on the $\mathbb{F}_3$ vector space $E[3]$, and any Lagrangian M would be fixed by the Frobenius action.

By corollary 3.8, it follows that the trace is equal to

$$\mathrm{tr}(\mathrm{Fr}_{19}\,|C_M) = \left(\frac{\det(\mathrm{Fr}_{19}\,|M)}{\mathbb{F}_3}\right)\sqrt{|E[3](\mathbb{F}_{19})|} = 3.$$

Now we move onto the path integral calculation. We use the `torsion_basis()` function on SageMath again, to find the following basis for $E[3]$

$$P_1 = (10, 13)$$
$$P_2 = (15, 18).$$

Let α_i denote the $H^1(E, \mathbb{Z}/3\mathbb{Z}) = \mathrm{Hom}(\pi_1(E), \mathbb{Z}/3\mathbb{Z})$ class associated to P_i. We wish to compute α_i explicitly.

We use the function `basis_function_space()` on SageMath to compute that

$$\mathrm{div}(y + 7x + 12) = 3[P_1] - 3[O_E]$$
$$\mathrm{div}(y + 11x + 7) = 3[P_2] - 3[O_E]$$

Let $f_1 = y + 7x + 12$ and $f_2 = y + 11x + 7$, then the cohomology class α_i corresponds to the extension of global function fields $L_i \coloneqq \mathbb{F}_{19}(E)[\sqrt[3]{f_i}]/\mathbb{F}_{19}(E)$. In particular, α_i corresponds to the homomorphism

$$\alpha_i \colon \sigma \mapsto \zeta\left(\frac{\sigma(\sqrt[3]{f_i})}{\sqrt[3]{f_i}}\right).$$

Explicitly, the field L_i has presentation

$$L_i = \mathrm{Frac}\,\mathbb{F}_{19}[x, y, z]/(y^2 - x^3 - 12x + 1, z^3 - f_i).$$

On the other hand, let $\mathrm{Fr}_{P_i} = \mathrm{Res}\,P_i \in \pi_1^{\mathrm{ab}}(E)$ denote the images of P_i under the reciprocity map. We wish to explicitly write down the action of α_i when restricted to the field extensions L_j, for $i, j \in \{1, 2\}$. We will now compute one of the cases in detail below.

Case $i = 1, j = 2$: Let Q be a place of L_1 lying over P_2. We note that since L_i is an unramified extension of $\mathbb{F}_{19}(E)$, it follows that $t = x - 15$ is a local parameter for Q, so the local field $(L_1)_Q$ can be written as $\mathbb{F}_{19^3}((t))$, where $\mathbb{F}_{19^3}$ is the residue field. Then we can write y as the

power series

$$y = \sqrt{(t+15)^3 + 12(t+15) - 1} = 18 + 8t + 9t^3 + 15t^4 + \cdots .$$

Here, we picked y to be the square root with constant term 18 since it vanishes at the point $P_2 = (15, 18)$.

Then, z is represented by the power series

$$\begin{aligned} z &= \sqrt[3]{y + 7(t+15) + 12} \\ &= \sqrt[3]{2} + 12\sqrt[3]{2}t + 8\sqrt[3]{2}t^2 + \cdots \end{aligned}$$

where $\sqrt[3]{2} \in \mathbb{F}_{19^3}$ generates the residue field extension $\mathbb{F}_{19^3}/\mathbb{F}_{19}$. Applying the Frobenius element to the coefficients of z we obtain

$$\begin{aligned} \mathrm{Fr}_{P_2}(z) &= 7\sqrt[3]{2} + 8\sqrt[3]{2}t + 18\sqrt[3]{2}t^2 + \cdots \\ &= 7z. \end{aligned}$$

Thus we conclude that

$$A(P_1, P_2) = \alpha_1(\mathrm{Fr}_{P_2}) = \zeta\left(\frac{\mathrm{Fr}_{P_2}(z)}{z}\right) = \zeta(7) = 1 \in \mathbb{F}_3.$$

Other Cases: Via the same method, we also compute that $A(P_1, P_1) = 0$, $A(P_2, P_2) = 2$ and $A(P_2, P_1) = 1$.

Thus the pairing A acts via the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$, and the quadratic form associated to it is

$$A(aP_1 + bP_2) = 2ab + 2b^2 = \tfrac{1}{2}(a+2b)^2 - \tfrac{1}{2}a^2 = a^2 - (b-a)^2.$$

Now we can evaluate the path integral

$$\begin{aligned} \sum_{\gamma \in E[\ell](\mathbb{F}_{19})} e^{\frac{2\pi i A(\gamma)}{3}} = \sum_{a,b \in \mathbb{F}_3} \xi^{a^2-(b-a)^2} = \sum_{a \in \mathbb{F}_3} \sum_{c \in \mathbb{F}_3} \xi^{a^2}\xi^{-c^2} &= \left(\sum_{a \in \mathbb{F}_3} \xi^{a^2}\right)\left(\sum_{c \in \mathbb{F}_3} \xi^{-c^2}\right) \\ &= (1 + \xi + \xi)(1 + \xi^2 + \xi^2) \\ &= (i\sqrt{3})(-i\sqrt{3}) \\ &= 3. \end{aligned}$$

Finally, we check that the trace and the path integral computed satisfies theorem 3.32.

We see that $\det A = -1$, and since $1 - \mathrm{Fr}_{19}$ is identically the zero map on $E[3]$, so the regularised determinant is equal to 1. Since both the trace and the path integral evaluate to 3 in this example, they indeed differ by the sign

$$\left(\frac{(-1)^g \det{}'(1 - \mathrm{Fr}_q)\det(A)}{\mathbb{F}_\ell}\right) = \left(\frac{(-1)(1)(-1)}{\mathbb{F}_3}\right) = 1.$$

3.6.2 Examples where $\mu_{\ell^2} \not\subset \mathbb{F}_q$

In this section we provide two explicit examples of theorem 3.32 for an elliptic curve $X = E/\mathbb{F}_q$, in the case where $q = 7, \ell = 3$. In this case we have that $\mu_\ell \subset \mathbb{F}_q$, but $\mu_{\ell^2} \not\subset \mathbb{F}_q$. Similarly to the previous section, one example will be an elliptic curve in which E has no non-trivial 3-torsion, and the other will be where $E(\mathbb{Q})$ contains the full 3-torsion.

Fix the isomorphism $\zeta\colon \{1,2,4\} = \mu_3(\mathbb{F}_7) \simeq \mathbb{F}_3$ by sending $2 \in \mu_3(\mathbb{F}_7)$ to $1 \in \mathbb{F}_3$. We also fix the isomorphism $\psi\colon \mathbb{F}_3 \simeq \mu_3(\mathbb{C})$ via $1 \mapsto \xi = e^{\frac{2\pi i}{3}}$.

Example 3.36. Let $X = E$ be the curve

$$E : y^2 = x^3 + x/\mathbb{F}_7.$$

We can check that the only $\mathbb{F}_7$-rational 3-torsion point is the origin O_E, and that the 3-torsion group $E[3]$ is defined over the extension $\mathbb{F}_{7^4}/\mathbb{F}_7$. Explicitly, let $\mathbb{F}_{7^4} = \mathbb{F}_7(\alpha)$, where α is a primitive 5th root of unity satisfying the minimal polynomial

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0.$$

Then using the `torsion_basis()` function on SageMath, the 3-torsion $E[3]$ is generated by the elements

$$P_1 = (5\alpha^3 + 5\alpha^2 + 5, 2\alpha^3 + 5\alpha^2)$$
$$P_2 = (5\alpha^3 + 5\alpha^2, 3\alpha^3 + 5\alpha^2 + \alpha + 4).$$

By a straightforward calculation we can see that the Frobenius acts on the basis elements in the following manner

$$\mathrm{Fr}_7\, P_1 = 2P_1 + P_2$$
$$\mathrm{Fr}_7\, P_2 = P_1 + P_2.$$

Moreover, let $\langle -, - \rangle$ denote the Weil pairing on $E[3]$, via the `weil_pairing()` function on SageMath, we compute that

$$\langle P_1, P_2 \rangle = 4 \in \mu_3(\mathbb{F}_7),$$

which we will identify with $\langle P_1, P_2 \rangle = 2 \in \mathbb{F}_3$. From now on the values of the Weil pairing $\langle -, - \rangle$ refer to the values in $\mathbb{F}_3$ after identifying $\zeta\colon \mu_3(\mathbb{F}_7) \simeq \mathbb{F}_3$.

Since $E[3]$ is a 2-dimensional symplectic space with respect to the Weil pairing, every 1-dimensional subspace is Lagrangian. However, the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ is not diagonalisable in $\mathbb{F}_3$, so there does not exist any Frobenius-invariant Lagrangian. Let us pick the Lagrangian $M = \mathbb{F}_3 P_1$, the 1-dimensional subspace generated by P_1. We also pick the complement $M' = \mathbb{F}_3 P_2$, so that $E[3] = M \oplus M'$.

We now evaluate $\mathrm{tr}(\mathrm{Fr}_7 \,|C_{M^\circ})$ via lemma 3.7.

First we compute the constant $A_{M^\circ, \mathrm{Fr}_7 M^\circ}$. Fix the orientation $o_M = P_1$. Note that M and $\mathrm{Fr}_7 M$ are transverse, so $I = M \cap \mathrm{Fr}_7 M = \{O_E\}$ is 0-dimensional, and $n_I = 1$. We also have $o_{\mathrm{Fr}_7 M} = \mathrm{Fr}_7 P_1 = 2P_1 + P_2$, and since I is trivial we have that $o_{M/I} = o_M$ and $o_{\mathrm{Fr}_7 M/I} = o_{\mathrm{Fr}_7 M}$. We also compute that

$$G(\tfrac{1}{2}, 3) = \sum_{x \in \mathbb{F}_3} \psi(\tfrac{1}{2}x^2) = 1 + \xi^2 + \xi^2 = -i\sqrt{3}.$$

Thus we have

$$\begin{aligned} A_{M^\circ, \mathrm{Fr}_7 M^\circ} &= (G(\tfrac{1}{2}, 3)/3)^1 \left(\frac{(-1)^{\binom{1}{2}} \langle 2P_1 + P_2, P_1 \rangle}{\mathbb{F}_3} \right). \\ &= \frac{-i\sqrt{3}}{3} \left(\frac{1}{\mathbb{F}_3} \right) \\ &= \frac{-i\sqrt{3}}{3}. \end{aligned}$$

Now we compute the sum portion of the formula in lemma 3.7.

We note that $\mathcal{S} = M'$, since $M + \mathrm{Fr}_7 M = E[3]$ spans the entire space. For each $x \in M' =$

$\{O_E, P_2, 2P_2\}$, we wish to find elements $m_x, n_x \in M$ such that

$$\mathrm{Fr}_7\, x - x = m_x + \mathrm{Fr}_7\, n_x,$$

and we wish to evaluate the sum $\sum_{x\in\mathcal{S}} \psi\left(\frac{1}{2}\langle m_x + n_x, x\rangle\right)$.

By inspection, we can make the following choices of m_x, n_x and obtain the following values of $\langle m_x + n_x, x\rangle$

$$\begin{cases} m_{P_2} = P_1, & n_{P_2} = O_E, & \langle m_{P_2} + n_{P_2}, P_2\rangle = \langle P_1, P_2\rangle = 2 \\ m_{2P_2} = 2P_1, & n_{2P_2} = O_E, & \langle m_{2P_2} + n_{2P_2}, 2P_2\rangle = \langle 2P_1, 2P_2\rangle = 2 \\ m_{O_E} = O_E, & n_{O_E} = O_E, & \langle m_{O_E} + n_{O_E}, O_E\rangle = \langle O_E, O_E\rangle = 0 \end{cases}.$$

Thus we evaluate

$$\sum_{x\in\mathcal{S}} \psi\left(\frac{1}{2}\langle m_x + n_x, x\rangle\right) = \xi + \xi + 1 = i\sqrt{3}.$$

Finally, combining the two computations, we have that the trace is equal to

$$\begin{aligned} \mathrm{tr}(\mathrm{Fr}_7\,|C_{M^\circ}) &= A_{M^\circ,\mathrm{Fr}_7\, M^\circ} \sum_{x\in\mathcal{S}} \psi\left(\frac{1}{2}\langle m_x + n_x, x\rangle\right) \\ &= \frac{-i\sqrt{3}}{3}(i\sqrt{3}) \\ &= 1. \end{aligned}$$

On the other hand, since $E[3](\mathbb{F}_q) = \{O_E\}$ is zero-dimensional, the map A must just be the zero map, and thus the path integral trivially evaluates to 1.

We finally check that our computation indeed satisfies theorem 3.32, we check that the regularised determinant $\det'(1-\mathrm{Fr}_7)$ is just equal to the determinant $\det(1-\mathrm{Fr}_7) = \det(\left(\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right)) = -1$.

Indeed, the trace and path integral in this example are both equal to 1, and thus differ by the sign

$$\left(\frac{(-1)^g \det'(1-\mathrm{Fr}_7)}{\mathbb{F}_3}\right) = \left(\frac{1}{\mathbb{F}_3}\right) = 1.$$

Example 3.37. Let $X = E$ be the curve

$$E : y^2 = x^3 + 2/\mathbb{F}_7.$$

In this case, we notice that the 3-torsion $E[3] \subset E(\mathbb{F}_7)$ is $\mathbb{F}_7$-rational. This means that the Frobenius Fr_7 acts trivially on the $\mathbb{F}_3$ vector space $E[3]$, and any Lagrangian M would be fixed by the Frobenius action.

By corollary 3.8, it follows that the trace is equal to

$$\mathrm{tr}(\mathrm{Fr}_7\,|C_M) = \left(\frac{\det(\mathrm{Fr}_7\,|M)}{3}\right)\sqrt{|E[3](\mathbb{F}_7)|} = 3.$$

Now we move onto the path integral calculation. We use the `torsion_basis()` function on SageMath again, to find the following basis for $E[3]$

$$\begin{aligned} P_1 &= (0, 4) \\ P_2 &= (3, 6). \end{aligned}$$

Let α_i denote the $H^1(E, \mathbb{Z}/3\mathbb{Z}) = \mathrm{Hom}(\pi_1(E), \mathbb{Z}/3\mathbb{Z})$ class associated to P_i. We wish to compute α_i explicitly.

We use the function `basis_function_space()` on SageMath to compute that

$$\begin{aligned}\mathrm{div}(y+3) &= 3[P_1] - 3[O_E] \\ \mathrm{div}(y+3x+6) &= 3[P_2] - 3[O_E]\end{aligned}$$

Let $f_1 = y+3$ and $f_2 = y+3x+6$, then the cohomology class α_i corresponds to the extension of global function fields $L_i \coloneqq \mathbb{F}_7(E)[\sqrt[3]{f_i}]/\mathbb{F}_7(E)$. In particular, α_i corresponds to the homomorphism

$$\alpha_i \colon \sigma \mapsto \zeta \left(\frac{\sigma(\sqrt[3]{f_i})}{\sqrt[3]{f_i}} \right).$$

Explicitly, the field L_i has presentation

$$L_i = \mathrm{Frac}\, \mathbb{F}_7[x,y,z]/(y^2 - x^3 - 2, z^3 - f_i).$$

On the other hand, let $\mathrm{Fr}_{P_i} = \mathrm{Res}\, P_i \in \pi_1^{\mathrm{ab}}(E)$ denote the images of P_i under the reciprocity map. We wish to explicitly write down the action of σ_i when restricted to the field extensions L_j, for $i,j \in \{1,2\}$. We will now compute one of the cases in detail below.

Case $i=1, j=2$: Let Q be a place of L_1 lying over P_2. We note that since L_i is an unramified extension of $\mathbb{F}_7(E)$, it follows that $t = x-3$ is a local parameter for Q, so the local field $(L_1)_Q$ can be written as $\mathbb{F}_{7^3}((t))$, where $\mathbb{F}_{7^3}$ is the residue field. Then we can write y as the power series

$$y = \sqrt{(t+3)^3 + 2} = 6 + 4t + 3t^3 + 5t^4 + \cdots.$$

Here, we picked y to be the square root with constant term 6 since it vanishes at the point $P_2 = (3,6)$.

Then, z is represented by the power series

$$\begin{aligned} z &= \sqrt[3]{y+3} \\ &= \sqrt[3]{2} + 3\sqrt[3]{2}t + 5\sqrt[3]{2}t^2 + \cdots \end{aligned}$$

where $\sqrt[3]{2} \in \mathbb{F}_{7^3}$ generates the residue field extension $\mathbb{F}_{7^3}/\mathbb{F}_7$. Applying the Frobenius element to the coefficients of z we obtain

$$\begin{aligned} \mathrm{Fr}_{P_2}(z) &= 4\sqrt[3]{2} + 6\sqrt[3]{2}t + 3\sqrt[3]{2}t^2 + \cdots \\ &= 4z. \end{aligned}$$

Thus we conclude that

$$A(P_1, P_2) = \alpha_1(\mathrm{Fr}_{P_2}) = \zeta \left(\frac{\mathrm{Fr}_{P_2}(z)}{z} \right) = 2 \in \mathbb{F}_3.$$

Other Cases: Via the same method, we also compute that $A(P_1,P_1) = 0$, $A(P_2,P_2) = 1$ and $A(P_2,P_1) = 2$.

Thus the pairing A acts via the matrix $\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$, and the quadratic form associated to it is

$$A(aP_1 + bP_2) = 4ab + b^2 = (2a+b)^2 - (2a)^2 = (b-a)^2 - a^2.$$

Now we can evaluate the path integral

$$\begin{aligned}\sum_{\gamma\in E[\ell](\mathbb{F}_7)} e^{\frac{2\pi i A(\gamma)}{3}} = \sum_{a,b\in\mathbb{F}_3} \xi^{(b-a)^2-a^2} = \sum_{a\in\mathbb{F}_3}\sum_{c\in\mathbb{F}_3} \xi^{c^2}\xi^{-a^2} &= \left(\sum_{a\in\mathbb{F}_3}\xi^{-a^2}\right)\left(\sum_{c\in\mathbb{F}_3}\xi^{c^2}\right)\\ &= (1+\xi^2+\xi^2)(1+\xi+\xi)\\ &= (-i\sqrt{3})(i\sqrt{3})\\ &= 3.\end{aligned}$$

Finally, we check that the trace and the path integral computed satisfies theorem 3.32.

We see that $\det A = -1$, and since $1 - \mathrm{Fr}_7$ is identially the zero map on $E[3]$ the regularised determinant is equal to 1. Since both the trace and the path integral evaluate to 3 in this example, they indeed differ by the sign

$$\left(\frac{(-1)^g \det{}'(1-\mathrm{Fr}_q)\det(A)}{\ell}\right) = \left(\frac{(-1)(1)(-1)}{3}\right) = 1.$$

3.6.3 Further Related Questions

Remark 3.38. We highlight possible further research directions related to trace–path integral formulae in arithmetic.

1. **An intrinsic proof of the trace–path integral formula.** The current proof evaluates each side of the formula separately and compares them. A more direct proof that shows the trace and the path integral are intrinsically related could be more enlightening.

2. **Trace–path integral formulae for number fields.** By Weil's trichotomy of analogies between number fields, function fields, and manifolds, we should expect a similar formula to exist in the case of number fields. While number fields do not have a Frobenius action, but given a cyclotomic $\mathbb{Z}_p$-extension K_∞/K, the γ action for a topological generator $\gamma \in \mathrm{Gal}(K_\infty/K)$ can be viewed as the analogous action.

Number Fields	Function Fields	Manifolds
Number Ring $\operatorname{Spec}\mathcal{O}_K$	Smooth Projective Curve $X/\mathbb{F}_q$	3-manifold M
$\mathbb{Z}_p$–extension $\operatorname{Spec}\mathcal{O}_{K[\mu_{p^\infty}]}$	Curve over Algebraic Closure $\overline{X}/\overline{\mathbb{F}}_q$	Riemann Surface Σ
γ action	Frobenius Action	Monodromy Action

   A very interesting further research question would be to prove a trace–path integral formula over number fields, where a path integral over $X = \operatorname{Spec}\mathcal{O}_K$ is expressed as the trace an action γ on a space $\mathcal{H}$, analogous to the quantisation of a space of fields on $\operatorname{Spec}\mathcal{O}_{K[\mu_{p^\infty}]}$.

3. **Trace–path integral formulae for other actions.** The trace–path integral formula proved in this paper is for the Abelian Arithmetic Chern–Simons action. In theory one should expect similar formulae to hold for path integrals of other arithmetic actions, such as non-abelian Arithmetic Chern–Simons actions, or the arithmetic BF action defined in [CK22].

4. **Sheaf-Theoretic versions of Trace–Path Integral Formulae.** By studying how the Trace and Path Integrals deform upon varying the curve, one should expect a Trace-Path integral formula which relates to the universal theta divisor on the moduli space $\mathcal{M}_g$ of genus g curves, where the work of this paper can be viewed as the case on a single point in $\mathcal{M}_g$.

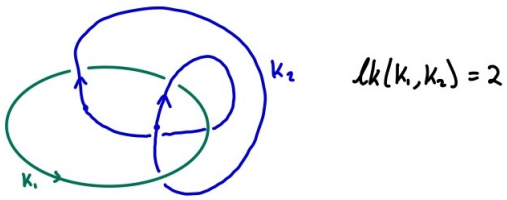
Chapter 4

Arithmetic Triple Symbols

4.1 Introduction

4.1.1 Linking Numbers in Topology

Let $K_1 \cup K_2 \subset S^3$ be a 2 component link. Informally, the linking number $\mathrm{lk}(K_1, K_2)$ measures the number of times K_2 'wraps around' K_1.



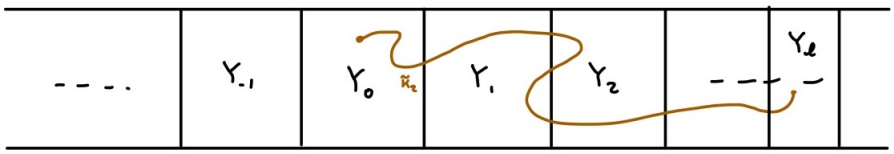
There are many ways to make the linking number precise, but we will now describe the linking number in terms of the monodromy action on cyclic coverings.

Let X_∞ be the $\mathbb{Z}$-cover of $X \coloneqq S^3 \setminus K_1$ which corresponds to the quotient map

$$\psi_\infty \colon \pi_1(S^3 \setminus K_1) \to \mathbb{Z}$$

sending the meridian τ of K_1 to $1 \in \mathbb{Z}$. We can think of X_∞ as the infinite cyclic cover of S_3 that is completely ramified at K_1.

In fact, the construction of X_∞ can be made explicit [Mor24, Example 2.1.12]. Let Σ be a *Seifert Surface* of K_1, this is an oriented surface with boundary, such that $\partial\Sigma = K_1$. For each $i \in \mathbb{Z}$ let Y_i be a manifold with boundary obtained by removing a tubular neighbourhood of K_1 from S^3 and then cutting along the Seifert surface. Let Σ_i^+, Σ_i^- be the two sides obtained from cutting along Σ. Then we can glue together all $\mathbb{Z}$ copies of Y_i by gluing Σ_i^+ with Σ_{i+1}^-. This construction is precisely X_∞.



Under the perspective of this construction, the linking number increases by 1 whenever the $\widetilde{K}_2$ passes from Σ_i^+ to Σ_{i+1}^-, and decreases by 1 when it passes from Σ_{i+1}^- to Σ_i^+.

Let $p\colon X_\infty \to S_3$ denote the (ramified) covering map. Let b be the basepoint of K_2, the preimage $p^{-1}(b) \subset X_\infty$ is a $\mathbb{Z}$-torsor, and lifting K_2 to X_∞ gives us a mondromy action on the torsor $p^{-1}(b)$ corresponding to an element in $\mathbb{Z}$. i.e. Let $K_2\colon [0,1] \to S^3$ have basepoints at b and suppose $\widetilde{K}_2\colon [0,1] \to X_\infty$ is a lift of K_2, then the linking number is given by

$$\mathrm{lk}(K_1, K_2) = \widetilde{K}_2(1) - \widetilde{K}_2(0).$$

By abuse of notation, we let $\tau \in \mathrm{Gal}(X_\infty/X)$ be the generator of the Galois group that corresponds to $1 \in \mathbb{Z}$ under the map $\psi_\infty\colon \pi_1(X) \to \mathrm{Gal}(X_\infty/X) \cong \mathbb{Z}$. By considering $[K_2]$ as an element of $\pi_1(X)$, our discussion above implies that

$$\psi_\infty([K_2]) = \tau^{\mathrm{lk}(K_1,K_2)}.$$

Linking Numbers mod 2

In order to better illustrate the analogy with arithmetic, we specialise to the case of the *Linking Number mod 2* of knots $K_1, K_2 \in S^3$ and describe the linking number explicitly. We keep the same notation as above.

We denote by X_2 the $\mathbb{Z}/2\mathbb{Z}$-cover of X corresponding to the quotient map

$$\psi_2\colon \pi_1(S^3 \setminus K_1) \xrightarrow{\psi_\infty} \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$$

which takes the meridian τ of K_1 to $1 \in \mathbb{Z}/2\mathbb{Z}$.

We once again denote by $p : X_2 \to S^3$ the associated ramified covering map. Let $\widetilde{K}_2$ be a lift of K_2 to X_2. We now consider the preimage $p^{-1}(K_2)$ of the knot K_2. There are two possible cases.

1. If $\mathrm{lk}(K_1, K_2) \equiv 0 \pmod 2$, then $\widetilde{K}_2(1) = \widetilde{K}_2(0)$. This means that the lift of K_2 is itself a knot. Since $|p^{-1}(b)| = 2$, this must mean that
$$p^{-1}(K_2) = \mathfrak{K}_1 \cup \mathfrak{K}_2$$
must be the union of two disjoint knots, each mapping to K_2 under p.

2. If $\mathrm{lk}(K_1, K_2) \equiv 1 \pmod 2$, then $\widetilde{K}_2(1) \neq \widetilde{K}_2(0)$. This means that the lift of K_2 is not a knot but just a path. But the preimage $p^{-1}(K_2)$ must be a closed 1-manifold, this must mean that
$$p^{-1}(K_2) = \mathfrak{K}$$
must be a single knot that forms a degree 2 covering of K_2 under p.

4.1.2 Quadratic and Power Residue Symbols

In a similar manner, we can view the Legendre symbols as an arithmetic analogue of the topological linking number. Let $p, q \in \mathbb{Z}$ be rational primes satisfying $p, q \equiv 1 \pmod 4$.

In this case, the field $\mathbb{Q}(\sqrt{p})$ is the unique $\mathbb{Z}/2\mathbb{Z}$ extension of $\mathbb{Q}$ that is ramified only at p. The Galois group $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ of this extension is generated by the monodromy $\tau\colon \sqrt{p} \mapsto -\sqrt{p}$.

Now consider $\{\mathfrak{q}|q\}$ the set of prime ideals of $\mathbb{Q}(\sqrt{p})$ lying above q. We can also denote this set as the preimage of $p^{-1}(\operatorname{Spec}\mathbb{F}_q)$ of the ramified covering $p : \operatorname{Spec}\mathbb{Z}\left[\frac{\sqrt{p}+1}{2}\right] \to \operatorname{Spec}\mathbb{Z}$. Since $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is unramified at q, there are two possibilities for this preimage.

1. If q splits, then $q\mathcal{O}_{\mathbb{Q}(\sqrt{p})} = \mathfrak{q}_1\mathfrak{q}_2$. In particular, since our field extension is Galois, τ acts transitively on $\{q_1, q_2\}$

   This case occurs when then residue field extension has degree $f = 1$, which is precisely when p is a quadratic residue modulo q.

2. If q is inert, then $q\mathcal{O}_{\mathbb{Q}(\sqrt{p})} = \mathfrak{q}$. In particular, the monodromy τ fixes the ideal $\mathfrak{q}$.

   This case occurs when then residue field extension has degree $f = 2$, which is precisely when p is a quadratic residue modulo q.

We notice that this behaviour is precisely measured by the Legendre symbol

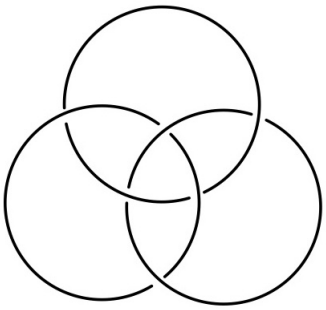
$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if } q = \mathfrak{q}_1\mathfrak{q}_2 \\ -1 & \text{if } q = \mathfrak{q} \end{cases}$$

This is precisely analogous to the study of mod 2 linking numbers in the topological setting, and thus one should view the Legendre symbol as being the arithmetic mod 2 linking number.

In a similar manner, let $K \supset \mu_n$ be a number field containing the nth roots of unity. Then the nth power residue symbol over K of two primes can be thought of as being analogous to the linking number mod n. Details of this analogy can be found in [Mor24, Theorem 9.4.1] and [Mor04, Examples 1.3].

4.1.3 The Borromean Rings and Triple Symbols

The Borromean Rings are is a 3-component link in topology where the component knots are pairwise unlinked, but yet the knots are altogether linked.



In topology, this phenomena is detected via the Milnor invariants. In arithmetic, *triple symbols* such as Redei's triple symbol can be viewed as an analogue of the Milnor invariants, and recent work in [KM25; Kim25] further generalise the triple symbols in a cohomological direction.

Outline of Chapter

Section 4.2 gives an overview of the topological theory of Milnor's invariants. An overview of ts arithmetic analogue, defined by Morishita in [Mor04; Mor24], is in section 4.3. We specialise to the case of the Rédei symbol in section 4.4, which was first defined [Réd39], and interpreted by Morishita as the mod 2 triple linking number of primes. These sections mostly serve as a motivating overview to the theory of arithmetic triple symbols, and proofs in these sections are mostly omitted.

In section 4.5, we go over in detail the recent work of Dohyeong Kim and Masanori Morishita in [KM25; Kim25], where the triple symbol is reinterpreted as a symbol on characters of the

absolute Galois group. It is also possible to view the unramified case as a special case of the arithmetic Chern–Simons action defined in section 2.2.

Finally, sections 4.6 and 4.7 contains some original work and partial lemmas towards some results that I hope to prove in the future.

4.2 Topological Milnor Invariants

This section serves as an exposition to the topological Milnor invariants. Proofs are mostly omitted, but references and comprehensive proofs for the topological theory can be found in [Mil57] and [Mor24, Section 9.1-9.2].

4.2.1 The Magnus Embedding and Magnus Coefficients

Definition 4.1 (Magnus Embedding)**.** Let $F = \langle x_1, \dots x_r \rangle$ denote the free group on r elements, and $\mathbb{Z}\langle\langle X_1, \dots, X_r \rangle\rangle$ denote the free $\mathbb{Z}$ algebra of non-commutative formal power series. Then there is a $\mathbb{Z}$-linear homomorphism defined by

$$\begin{aligned} M\colon \mathbb{Z}[F] &\to \mathbb{Z}\langle\langle X_1, \dots, X_r \rangle\rangle \\ x_i &\mapsto 1 + X_i \\ x_i^{-1} &\mapsto 1 - X_i + X_i^2 - \cdots . \end{aligned}$$

This is an injective map [Mor24, Lem 9.1.1], called the *Magnus embedding*.

Let $I = (i_1 i_2 \dots i_n)$ denote a sequence of not neccesarily distinct indices $1 \le i_s \le r$. Then we define X_I to be the (non-commutative) product

$$X_I \coloneqq X_{i_1} X_{i_2} \cdots X_{i_n}.$$

Additionally, we say that for multi-indices $I = (i_1 i_2 \dots i_n), J = (j_1 j_2 \dots j_m)$, we define their product to simply be their concatentation: $IJ = (i_1 \dots i_n j_1 \dots j_m)$. In particular this implies that $X_I X_J = X_{IJ}$.

Definition 4.2 (Magnus Coefficients)**.** Suppose $\alpha \in \mathbb{Z}[F]$ and consider its image under M. Note that since every element of F gets mapped to a power series with constant term 1, the constant term of α is simply the $\epsilon_{\mathbb{Z}[F]}(\alpha)$, where $\epsilon_{\mathbb{Z}[F]}\colon \mathbb{Z}[F] \to \mathbb{Z}$ is the augmentation map, i.e. the sum of coefficients of the terms in α. For the other terms, let $\mu(I;\alpha)$ denote the coefficient of X_I, so that

$$M(\alpha) = \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_I \mu(I;\alpha) X_I.$$

These $\mu(I;\alpha)$ are called *Magnus Coefficients*.

The Magnus coefficients satisfy the following identity

Proposition 4.3 ([Mor24, Prop 9.1.4])**.** Given elements $\alpha, \beta \in \mathbb{Z}[F]$, we have the relation

$$\mu(I;\alpha\beta) = \sum_{I=JK} \mu(J;\alpha)\mu(K;\beta),$$

where the sum ranges over all pairs of multi-indices (J, K) such that $I = JK$. Here J or K can be the empty multi-index, in which case $\mu((),\alpha) = \epsilon_{\mathbb{Z}[F]}(\alpha)$.

Morishita proves this proposition by relating Magnus coefficients to Fox Derivatives in [Mor24], but I will provide a direct proof of this statement simply by comparing coefficients.

Proof. Since the Magnus embedding is a ring homomorphism, we have that

$$M(\alpha\beta) = M(\alpha)M(\beta).$$

The $\mu(I;\alpha\beta)$ is the coefficient of X_I in $M(\alpha\beta)$, but the X_I terms in the expansion of $M(\alpha)M(\beta) = (\sum_J \mu(J;\alpha)X_J)(\sum_J \mu(K;\beta)X_K)$ are precisely those of the form $\mu(J;\alpha)X_J\mu(K;\beta)X_K$ where $I = JK$, which proves the equality.

□

Fox Derivatives

We can alternatively define the coefficients of the Magnus embedding using Fox derivatives instead. Define the *Fox Derivative* for monomials in $\mathbb{Z}[F]$ to be

$$\begin{cases} \dfrac{\partial x_i}{\partial x_j} \coloneqq \delta_{ij} \\ \dfrac{\partial x_i^{-1}}{\partial x_j} \coloneqq -x_i^{-1}\delta_{ij} \\ \dfrac{\partial}{\partial x_j} x_{i_1}^{e_1} x_{i_2}^{e_2} \cdots x_{i_n}^{e_n} \coloneqq \dfrac{\partial x_{i_1}^{e_1}}{\partial x_j} + x_{i_1}^{e_1}\dfrac{\partial x_{i_2}^{e_2}}{\partial x_j} + \cdots + x_{i_1}^{e_1}\cdots x_{i_{n-1}}^{e_{n-1}}\dfrac{\partial x_{i_n}^{e_n}}{\partial x_j} & (\text{For } e_k = \pm 1) \end{cases}$$

Extending linearly, we obtain a map $\frac{\partial}{\partial x_j}\colon \mathbb{Z}[F] \to \mathbb{Z}[F]$. This derivative satisfies the unique property that for each $\alpha \in \mathbb{Z}[F]$,

$$\alpha = \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j}(x_j - 1).$$

In order to take multiple derivatives, for a multi-index I we define

$$D_I(\alpha) \coloneqq \frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}} = \frac{\partial}{\partial x_{i_1}} \left(\frac{\partial^{n-1}\alpha}{\partial x_{i_2} \cdots \partial x_{i_n}} \right).$$

The coefficients of the Magnus expansion $\mu(I;\alpha)$ and the Fox derivatives is related to Magnus coefficients via [Mor24, Prop 9.1.4]

$$\mu(I;\alpha) = \epsilon_{\mathbb{Z}[F]}(D_I(\alpha)).$$

4.2.2 Definition of the Milnor $\overline{\mu}$-Invariants

Let $L = K_1 \cup \cdots \cup K_r \subset S^3$ be a link. Let F be the free group with r generators $x_1, \ldots, x_r$, where the generator x_i corresponds to a meridian α_i of the knot K_i. Then there is a theorem by Milnor that describes the quotient of $G_L = \pi_1(S^3 \setminus L)$ by its lower central series.

For a group G, define its lower central series via $G^{(1)} \coloneqq [G, G]$ and $G^{(d)} = [G^{(d-1)}, G]$.

Theorem 4.4 ([Mor24, Thm 8.1.1], [Mil57, Thm 4])**.** For each positive integer d, there exists words $y_i^{(d)} \in F$ in the free group such that the quotient of G_L by the dth term of its lower central series has the presentation

$$G_L/G_L^{(d)} = \langle x_1, \cdots, x_r | [x_i, y_i^{(d)}] = 1, F^{(d)} = 1 \rangle.$$

And the words $y_i^{(d)}$ represents the longitude β_i of the knot K_i in $G_L/G_L^{(d)}$.

We make the following definition.

Definition 4.5. Let $I = (i_1 \dots i_n i_{n+1})$ be a multi-index. Given a fixed positive integer d we define

$$\mu^{(d)}(I) = \mu((i_1 \dots i_n); y_{i_{n+1}}^{(d)}).$$

In other words, the Magnus expansion of the words $y_i^{(d)}$ are given by

$$M(y_i^{(d)}) = \epsilon_{\mathbb{Z}[F]}(y_i^{(d)}) + \sum_I \mu(I(i)) X_I.$$

In terms of Fox derivatives, we can also write

$$\mu^{(d)}(I(i)) = \epsilon_{\mathbb{Z}[F]}(D_I(y_i^{(d)})).$$

Proposition 4.6. For $d \geq |I|$, the value of $\mu^{(d)}(I)$ is independent of the choice of d.

Thus we can now define the *Milnor $\overline{\mu}$-invariant*.

Definition 4.7 (Milnor $\overline{\mu}$-invariant)**.** Let $\mu(I)$ be the value of $\mu^{(d)}(I)$ for sufficiently large $d \geq |I|$.

Moreover, define $\Delta(I)$ to be the ideal of $\mathbb{Z}$ generated by $\mu(J)$, where J runs over all cyclic permutations of proper subsequences of the multi-index I.

Then, we can define the *Milnor $\overline{\mu}$ invariant* to be

$$\overline{\mu}(I) \coloneqq \mu(I) \mod \Delta(I).$$

Theorem 4.8 ([Mil57])**.** $\overline{\mu}$ has the following properties

1. For $i \neq j$, $\overline{\mu}(ij) = \mathrm{lk}(K_i, K_j)$.
2. For any multi-index I where $2 \leq |I| \leq d$, $\overline{\mu}(I)$ is indeed a link invariant.
3. $\overline{\mu}$ is invariant under cyclic symmetry, i.e.

$$\overline{\mu}(i_1 \dots i_n) = \overline{\mu}(i_2 \dots i_n i_1).$$

4.2.3 The Milnor Representation

In the introduction, the linking number $\mathrm{lk}(K_1, K_2)$ can be viewed as an invariant measuring the behaviour of the longitude along K_2 on a cyclic covering that is ramified only at K_1. The Milnor invariants can be interpreted similarly, but instead measuring the behaviour of the longitude along K_r, on a nilpotent covering of S^3 that is ramified only at $K_1, \dots, K_{r-1}$. We will now make this precise.

Throughout this section, let $U_n(R) \leq M_n(R)$ be the group of $n \times n$ upper-triangular unipotent matrices in the ring R.

Definition 4.9 (Milnor Representation)**.** Given a multi-index $I = (i_1 \dots i_n)$ we can define the group homomorphism $\rho_I \colon F \to U_n(\mathbb{Z}/\Delta(I))$ given by

$$\alpha \mapsto \begin{pmatrix} 1 & \mu((i_1);\alpha) & \mu((i_1 i_2);\alpha) & \cdots & \mu((i_1 \dots i_{n-1});\alpha) \\ & 1 & \mu((i_2);\alpha) & \cdots & \mu((i_2 \dots i_{n-1});\alpha) \\ & & \ddots & \ddots & \vdots \\ & & & 1 & \mu((i_{n-1});\alpha) \\ & & & & 1 \end{pmatrix} \mod \Delta(I).$$

The convolution identity given in proposition 4.3 implies that the above homomorphism is well defined.

Theorem 4.10. The homomorphism ρ_I factors through the link group $G_L = \pi_1(S^3 \setminus L)$ to obtain a map $\rho_I \colon G_L \to U_n(\mathbb{Z}/\Delta(I))$. Suppose additionally that the multi-indices $i_1, \cdots, i_{n-1}$ are all distinct. Then

1. The homomorphism ρ_I is surjective.
2. Let $M_I \to S^3$ be the Galois covering ramified over $K_{i_1} \cup \cdots \cup K_{i_{n-1}}$ corresponding to $\mathrm{Ker}(\rho_I)$. For a longitude β_{i_n} of K_{i_n} we have
$$\rho_I(\beta_{i_n}) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \overline{\mu}(I) \\ & 1 & \cdots & 0 & 0 \\ & & \ddots & & \vdots \\ & & & 1 & 0 \\ & & & & 1 \end{pmatrix}.$$
3. The $\overline{\mu}(I)$ invariant is equal to zero if and only if the knot K_{i_n} is completely decomposed in the covering $M_I \to S^3$.

4.3 Arithmetic Milnor Invariants

We now describe the arithmetic analogue of Milnor's invariants. Proofs for this section are also omitted, but a comprehensive account can be found in [Mor04] and [Mor24, Section 9.3-9.4].

4.3.1 Pro-ℓ and mod $m = \ell^e$ analogues of Magnus Coefficients

Fix a prime ℓ. Let $\widehat{F}(\ell) = \langle x_1, \ldots, x_r \rangle$ denote the free pro-ℓ group with r generators. By taking pro-ℓ completions of the Magnus embedding $M \colon F \to \mathbb{Z}\langle\langle X_1, \ldots, X_r \rangle\rangle$, we obtain an isomorphism of continuous $\mathbb{Z}_l$-algebras called the pro-ℓ Magnus isomorphism

$$\widehat{M} \colon \mathbb{Z}_\ell[[\widehat{F}(l)]] \xrightarrow{\sim} \mathbb{Z}_\ell \langle\langle X_1, \ldots, X_r \rangle\rangle .$$

Given an element $\alpha \in \mathbb{Z}_\ell[[\widehat{F}(\ell)]]$, we can similarly define the pro-ℓ Magnus coefficients $\widehat{\mu}(I;\alpha) \in \mathbb{Z}_\ell$ to be such the coefficients of the pro-ℓ Magnus expansion

$$\widehat{M}(\alpha) = \epsilon_{\mathbb{Z}_\ell[[\widehat{F}(\ell)]]}(\alpha) + \sum_I \widehat{\mu}(I;\alpha) X_I.$$

A pro-ℓ analogue to the identity in proposition 4.3 can be similarly proved.

Proposition 4.11 ([Mor24, Prop 9.3.4])**.** Given elements $\alpha, \beta \in \mathbb{Z}_\ell[[\widehat{F}(\ell)]]$ and a multi-index I, we have the relation

$$\mu(I;\alpha\beta) = \sum_{I=JK} \mu(J;\alpha)\mu(K;\beta),$$

where the sum ranges over all pairs of multi-indices (J, K) such that $I = JK$. Here J or K can be the empty multi-index, in which case $\mu((),\alpha) = \epsilon_{\mathbb{Z}[F]}(\alpha)$.

Now suppose $m = \ell^e$ for some integer e. If we reduce the pro-ℓ Magnus isomorphism mod m, then we obtain the mod m Magnus isomorphism

$$M_m \colon \mathbb{Z}/m\mathbb{Z}[[\widehat{F}(\ell)]] \simeq \mathbb{Z}/m\mathbb{Z} \langle\langle X_1, \ldots, X_r \rangle\rangle ,$$

and mod m Magnus coefficients $\mu_m(I;\alpha)$ satisfying

$$M_m(\alpha) = \epsilon_{\mathbb{Z}/m\mathbb{Z}[[\widehat{F}(\ell)]]}(\alpha) + \sum_I \mu_m(I;\alpha)X_I.$$

4.3.2 Koch's presentation for G_S

In the topological case, the definition of Milnor's invariants depended on a presentation of a quotient of the link group (theorem 4.4). In this subsection we discuss the arithmetic analogue of that presentation.

Fix a rational prime ℓ and suppose $S = \{p_1, \dots, p_r\}$ be a set of primes of $\mathbb{Q}$ not containing ℓ, we would like to understand the maximal pro-ℓ quotient of $G_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$.

Let τ_i be a monodromy over p_i and σ_i be a lift of the p_i Frobenius. These are elements of G_S which satisfy

$$\begin{aligned} \tau_i(\zeta_{\ell^n}) &= \zeta_{\ell^n}; \quad & \tau_i(\sqrt[\ell^n]{p_i}) &= \zeta_n \sqrt[\ell^n]{p_i} \\ \sigma_i(\zeta_{\ell^n}) &= \zeta_{\ell^n}^{p_i}; \quad & \sigma_i(\sqrt[\ell^n]{p_i}) &= \sqrt[\ell^n]{p_i}. \end{aligned}$$

Consider the free pro-ℓ group $\widehat{F}(\ell) = \langle x_1, \dots, x_r \rangle$, where x_i represents the monodromy τ_i. Then by a theorem of H. Koch[1],

Theorem 4.12 (Presentation of $G_S(\ell)$ [Mor24, Thm 8.2.1])**.** There exist words $y_1, \dots, y_r \in \widehat{F}(\ell)$ that represent the Frobenius σ_i, such that the maximal pro-ℓ quotient of G_S has presentation

$$G_S(\ell) \cong \left\langle x_1, \dots x_r | x_1^{p_1-1}[x_1, y_1] = \cdots = x_r^{p_r-1}[x_r, y_r] = 1 \right\rangle.$$

4.3.3 Milnor $\overline{\mu}_m$-invariants

Following the previous section, we can now define the $\overline{\mu}_m(I)$ invariants.

Definition 4.13. Let y_i be words of $\widehat{F}(\ell)$ that represent the Frobenius σ_i. For a multiindex $I = (i_1 \dots, i_n)$, we define $\widehat{\mu}(I)$ and $\mu_m(I)$ to be

$$\begin{aligned} \widehat{\mu}(I) &\coloneqq \widehat{\mu}((i_1 \dots i_{n-1}); y_i) \\ \mu_m(I) &\equiv \widehat{\mu}(I) \pmod{m}. \end{aligned}$$

Moreover, suppose $m = \ell^e$ is chosen so that $p_i \equiv 1 \pmod{m}$. Let $\Delta_m(I)$ denote the ideal of $\mathbb{Z}/m\mathbb{Z}$ generated by the binomial coefficients $\binom{m}{t}, 1 \le t \le |I|$ and $\mu_m(J)$. Then we define the $\overline{\mu}_m$ invariant to be

$$\overline{\mu}_m(I) \coloneqq \mu_m(I) \mod \Delta_m(I)$$

Theorem 4.14 ([Mor04])**.** The Milnor $\overline{\mu}_m$ invariant has the following properties

1. Let ζ_m be a primitive mth root of unity given in section 4.3.2, then

$$\zeta_m^{\mu_m(ij)} = \left(\frac{p_j}{p_i}\right)_m,$$

   where $\left(\frac{\cdot}{\cdot}\right)_m$ denotes the mth power residue symbol.

2. If $2 \le |I| \le m$, then $\overline{\mu}_m(I) \coloneqq \mu_m(I) \mod \Delta_m(I)$ is an invariant that only depends on S and l.

[1] Supposedly the original proof is in [HKZ78], but I was unable to find any copy of this text online. There seems to be a weaker version of this result in [Koc70, Ch. 11], and [Mor24] also provides a proof.

It should be noted that unlike the topological analogue in theorem 4.8, the arithmetic $\overline{\mu}_m(I)$ invariant does not neccesarily satisfy cyclic symmetry. This is because the base field $\mathbb{Q}$ does not contain a primitive ℓth root of unity for $\ell \neq 2$.

4.3.4 Interpretation via Nilpotent Extensions

The $\overline{\mu}_m$ invariants can be interpreted as a measure of the decomposition of primes in a nilpotent extension.

Definition 4.15 (Pro-ℓ Milnor Representation)**.** Given a multi-index $I = (i_1 \dots i_n)$ we can define the group homomorphism $\rho_{(m,I)} \colon \widehat{F}(\ell) \to U_n((\mathbb{Z}/m\mathbb{Z})/\Delta_m(I))$ given by

$$\alpha \mapsto \begin{pmatrix} 1 & \mu((i_1);\alpha) & \mu((i_1 i_2);\alpha) & \cdots & \mu((i_1 \dots i_{n-1});\alpha) \\ & 1 & \mu((i_2);\alpha) & \cdots & \mu((i_2 \dots i_{n-1});\alpha) \\ & & \ddots & \ddots & \vdots \\ & & & 1 & \mu((i_{n-1});\alpha) \\ & & & & 1 \end{pmatrix} \mod \Delta(I).$$

Once again, it can be checked that this is a well defined group homomorphism.

Theorem 4.16 ([Mor04, 1.2.7])**.** The homomorphism $\rho_{(m,I)}$ factors through $G_S(l)$, and if the indices $i_1, \dots i_{n-1}$ are distinct, then

1. The homomorphism $\rho_{(m,I)}$ is surjective.
2. Let $K_{m,I}/\mathbb{Q}$ be the Galois extension corresponding to $\operatorname{Ker} \rho_{(m,I)}$. Then
$$\operatorname{Gal}(K_{m,I}/\mathbb{Q}) \cong U_n((\mathbb{Z}/m\mathbb{Z})/\Delta_m(I)).$$
This extension is ramified at exactly $p_{i_1}, \dots, p_{i_{n-1}}$ with ramification degree for each prime equal $|(\mathbb{Z}/m\mathbb{Z})/\Delta_m(I)|$.
Additionally, the Frobenius σ_{i_n} is mapped to
$$\sigma_{i_n} \mapsto \begin{pmatrix} 1 & 0 & \cdots & 0 & \overline{\mu}(I) \\ & 1 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & 1 & 0 \\ & & & & 1 \end{pmatrix}$$
3. p_{i_n} is completely decomposed in the extension $K_{m,I}/\mathbb{Q}$ if and only if $\overline{\mu}_m(I) = 0$.

4.4 Rédei Triple Symbol

The previous section gave a very abstract definition of the field extension $K_{m,I}/\mathbb{Q}$ by defining it as the field extension corresponding to the kernel of a Galois representation $G_S(\ell) \to U_n((\mathbb{Z}/m\mathbb{Z})/\Delta_m)$. In this section we outline an explicit construction of $K/\mathbb{Q}$ given by Rédei in [Réd39], for the special case where $\ell = m = 2$, $S = \{p_1, p_2, p_3\}$, and $I = (123)$. Suppose for simplicity that $p_i \equiv 1 \pmod 4$ and $\left(\frac{p_i}{p_j}\right) = 1$ for $1 \leq i \neq j \leq 3$. The details of this construction can also be found in [Mor24, Section 9.4].

Lemma 4.17. Suppose $p_1, p_2, p_3 \equiv 1 \pmod 4$ are primes satisfying $\left(\frac{p_i}{p_j}\right) = 1$ for $i \neq j$. Then there exists pairwise coprime integers x, y, z such that $x^2 = p_1 y^2 + p_2 z^2$, y is even, and $x - y \equiv 1 \mod 4$.

Construction 4.18 ([Mor24, Lem 9.4.6])**.** We write $K_i \coloneqq \mathbb{Q}(\sqrt{p_i})$. Suppose we have a primitive solution (x, y, z) to the above diophantine equation. We set $\alpha_2 = x - y\sqrt{p_1} \in \mathbb{Q}(\sqrt{p_1})$, then we define

$$K = K_1K_2(\sqrt{\alpha_2}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha_2}) = \mathbb{Q}(\sqrt{p_2}, \sqrt{\alpha_2}).$$

This turns out precisely to be the extension that we want. Note that the upper triangular unipotent group mod 2 can be identified with the dihedral group of order 8

$$U_3(\mathbb{F}_2) \cong D_8 = \left\langle s, t | s^2 = t^4 = stst = 1 \right\rangle,$$

via

$$\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \leftrightarrow s$$
$$\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \leftrightarrow t.$$

Theorem 4.19 ([Mor24, 9.4.8])**.** The $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$ via the field automorphisms

$$\begin{aligned} s(\sqrt{p_1}) &= \sqrt{p_1}, \quad s(\sqrt{p_2}) = 2\sqrt{p_2}, \quad s(\sqrt{\alpha_2}) = \sqrt{\alpha_2} \\ t(\sqrt{p_1}) &= -\sqrt{p_1}, \quad t(\sqrt{p_2}) = 2\sqrt{p_2}, \quad t(\sqrt{\alpha_2}) = -\sqrt{\alpha_2} \end{aligned}$$

One can check that these automorphisms indeed satisfy the relations of D_8.

Moreover, we can define the Rédei triple symbol $[p_1, p_2, p_3]$

Definition 4.20. Let σ_{p_3} be the Frobenius of p_3 in $K/\mathbb{Q}$, we define

$$[p_1, p_2, p_3] = \begin{cases} 1 & \sigma_{p_3} = \mathrm{id}_K \\ -1 & \text{otherwise.} \end{cases}$$

Just as how the Legendre symbol $\left(\frac{p}{q}\right)$ can be interpreted as a condition on a lift of q-Frobenius over the extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, we can view the Redei symbol as a generalisation of the Legendre symbol, studying the behavioro of the lift of p_3-Frobenius over a D_8 extension of $\mathbb{Q}$ ramified only at p_1 and p_2.

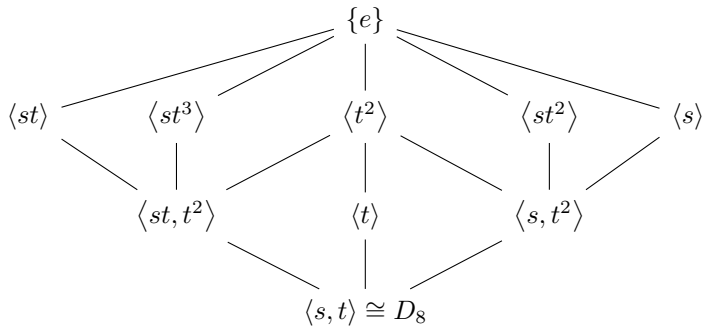
This symbol is related to the Milnor invariants via

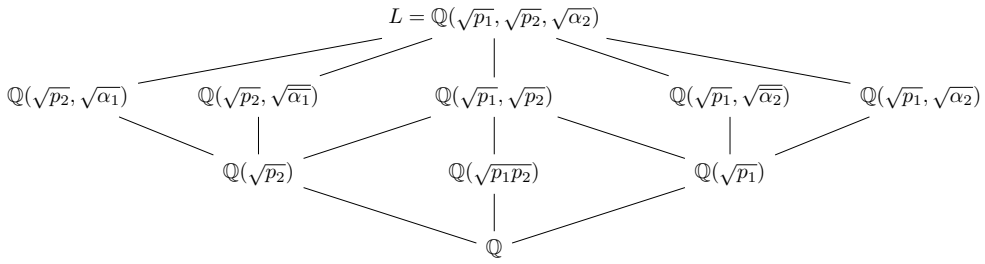
Theorem 4.21 ([Mor24, Thm 9.4.9])**.** The following equality holds

$$(-1)^{\mu_2(123)} = [p_1, p_2, p_3].$$

Subfield structure

Using the identification $\mathrm{Gal}(L/\mathbb{Q}) \cong \left\langle s, t : s^2 = t^4 = stst = 1 \right\rangle$, and defining $\alpha_1 = (\sqrt{\alpha_2} + \sqrt{\overline{\alpha_2}})^2 = \alpha_2 + \overline{\alpha_2} + 2\sqrt{N(\alpha_2)} = 2x + 2z\sqrt{p_2} \in \mathbb{Q}(\sqrt{p_2})$, then the field $L/\mathbb{Q}$ has the following subfield structure, corresponding to the following subgroups.





Remark 4.22. There are other cases in which arithmetic Milnor invariants are explicitly interpreted via an explicit construction of the field extension $K_{(m,I)}$.

1. There also is a similar but more complicated construction by Amano-Mizusawa-Morishita in [AMM18], which can be viewed as the triple linking number mod 3 over the number field $K = \mathbb{Q}(\sqrt{-3})$. In their paper, given 3 prime elements $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ of $\mathcal{O}_K$, they given an explicit construction of a degree 27 extension $\mathfrak{K}_{\mathfrak{p}_1,\mathfrak{p}_2}/K$ which is ramified only at $\mathfrak{p}_1, \mathfrak{p}_2$ with Galois group isomorphic to the upper triangular unipotent group $U_3(\mathbb{F}_3)$. They then define a triple cubic residue symbol $[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]$ which recovers the arithmetic Milnor invariant, and can be interpreted via studying the behaviour of a lift of the $\mathfrak{p}_3$ Frobenius.
2. By extending Koch's theorem to the case of real quadratic number fields, Kuramoto gives explicit interpretations of the mod 2 triple linking number over real quadratic fields in [Kur26].
3. In [Ama14], Amano constructs a degree 64 extension over $\mathbb{Q}$, with Galois group isomorphic to $U_4(\mathbb{F}_2)$, which gives an explicit interpretation to quadruple linking numbers.

Remark 4.23. The density of triplets (p_1, p_2, p_3) of primes which are Borromean was proved (assuming the generalised Riemann Hypothesis) to be $\frac{1}{128}$ by Ishida-Kuramoto-Zheng in [IKZ24]. More precisely they show

$$\lim_{x\to\infty} \frac{\#\{(p_1,p_2,p_3)|p_i < x, (p_1,p_2,p_3) \text{ is Borromean}\}}{\#\{(p_1,p_2,p_3)|p_i < x, p_i \neq p_j (i \neq j)\}} = \frac{1}{128}.$$

In particular, this result implies that there are infinitely many Borromean triplets of prime numbers. Explicit densities of other Milnor invariants described in remark 4.22 are not known currently.

4.5 Triple Symbols of Characters

This section will be a summary of the main results and constructions from [KM25], which defines a triple symbol of Galois characters, and recovers the mod 2 symbols defined by Rédei

and the mod 3 symbols defined by Amano-Mizusawa-Morishita. Proofs from the paper have been expanded with some additional details.

4.5.1 Setup and Definitions

Suppose F is a number field containing the nth roots of unity. Then we can fix a primitive nth root of unity $\zeta\colon \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n$ and corresponding isomorphisms of Galois cohomologies. Let $G \coloneqq \mathrm{Gal}(\overline{F}/F)$.

Let S be a set of places of F, then we denote by F_S the maximal extension of F that is unramified outside of S, and we define $G_S \coloneqq \mathrm{Gal}(F_S/F)$. Since G_S is naturally a quotient of G, there is an inflation map induced by the quotient map $G \twoheadrightarrow G_S$

$$\inf\colon C^i(G_S, \mathbb{Z}/n\mathbb{Z}) \to C^i(G, \mathbb{Z}/n\mathbb{Z}).$$

Definition 4.24 (Global Trivialisation)**.** Let $\phi \in C^i(G, \mathbb{Z}/n\mathbb{Z})$ be a cochain. We say that $\eta \in C^{i-1}(G, \mathbb{Z}/n\mathbb{Z})$ is a *global trivialisation* of ϕ if

$$d\eta = \phi.$$

Moreover, we say that η is a *global trivialisation unramified outside of* S if η lies in the image of the inflation map $\inf\colon C^{i-1}(G_S, \mathbb{Z}/n\mathbb{Z}) \to C^{i-1}(G, \mathbb{Z}/n\mathbb{Z})$.

For a place v of F we let F_v be the completion of F at v. Let F_v^{ur} be the maximal unramified extension of F_v, and we define $G_v \coloneqq \mathrm{Gal}(\overline{F_v}/F_v)$, and $G_v^{ur} \coloneqq \mathrm{Gal}(F_v^{ur}/F_v)$. We also fix an embedding $\overline{F} \hookrightarrow \overline{F_v}$ which identifies G_v as a subgroup of G. The inclusion of G_v into G induces a localisation map of cochains:

$$\mathrm{loc}_v\colon C^i(G, \mathbb{Z}/n\mathbb{Z}) \to C^i(G_v, \mathbb{Z}/n\mathbb{Z})$$

And since G_v^{ur} is a quotient of G_v, there is an inflation map induced by $G_v \twoheadrightarrow G_v^{ur}$:

$$\inf\colon C^i(G_v^{ur}, \mathbb{Z}/n\mathbb{Z}) \to C^i(G_v, \mathbb{Z}/n\mathbb{Z})$$

Definition 4.25 (Local Trivialisation)**.** Let $\phi \in C^i(G, \mathbb{Z}/n\mathbb{Z})$ be a cochain. We say that $\eta_v \in C^{i-1}(G_v, \mathbb{Z}/n\mathbb{Z})$ is a *local trivialisation* of ϕ if

$$d\eta_v = \mathrm{loc}_v\, \phi$$

Moreover, we say that η_v is *unramified* if η lies in the image of the inflation map

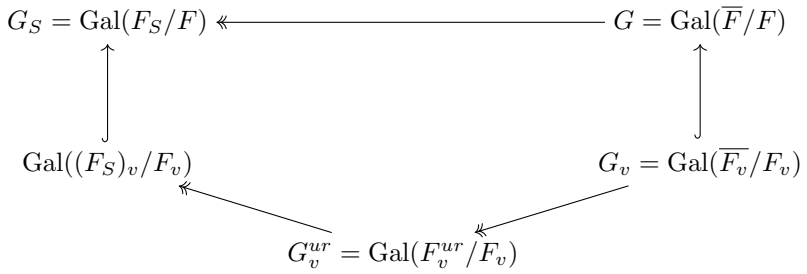
$$\inf\colon C^{i-1}(G_v^{ur}, \mathbb{Z}/n\mathbb{Z}) \to C^{i-1}(G_v, \mathbb{Z}/n\mathbb{Z}).$$

Lemma 4.26. If η is a global trivialisation unramified outside of S for some set S and $v \notin S$, then $\mathrm{loc}_v\, \eta$ is an unramified local trivialisation.

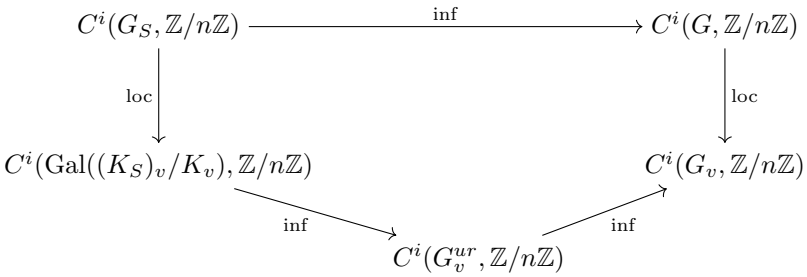
Proof. Since η is unramified outside of S, it must lie in the image of $\inf\colon C^i(G_S, \mathbb{Z}/n\mathbb{Z}) \to C^i(G, \mathbb{Z}/n\mathbb{Z})$.

Given a homomorphism of groups $f\colon G \to G'$, the corresponding map of cochains $C^k(G', A) \to C^k(G, A)$ is given by pre-composing by f. Thus the functor sending a group G to the cochains $C^k(G, \mathbb{Z}/n\mathbb{Z})$ is a contravariant functor.

Denote by $(F_S)_v$ the completion of F_S in $\overline{F_v}$, there is a commutative diagram of Galois groups:



Which induces a commutative diagram of cochains:



Thus if η lies in the image of the inflation map from $C^i(G_S, \mathbb{Z}/n\mathbb{Z})$ it follows from the diagram that $\mathrm{loc}_v\, \eta$ must lie in the image of the inflation map from $C^i(G_v^{ur}, \mathbb{Z}/n\mathbb{Z})$, i.e. it must be an unramified cochain. □

4.5.2 Construction of the Triple Symbol

Let $\chi_i \colon G \to \mathbb{Z}/n\mathbb{Z}$ be characters of G. We wish to define a triple symbol of the form $[\chi_1, \chi_2, \chi_3]_n \in \mathbb{Z}/n\mathbb{Z}$.

By the long exact sequence from Kummer Theory and Hilbert 90, we have

$$F^\times/(F^\times)^n \cong H^1(G, \mu_n) \cong H^1(G, \mathbb{Z}/n\mathbb{Z}).$$

Thus every character $\chi_i \in H^1(G, \mathbb{Z}/n\mathbb{Z})$ comes from a Kummer cocycle, i.e there exists some $\alpha_i \in F^\times$ such that

$$\zeta^{\chi_i(\sigma)} = \frac{\sigma(\sqrt[n]{\alpha_i})}{\sqrt[n]{\alpha_i}}.$$

Let S_i be the set of primes in which χ_i ramifies. We assume that S_1, S_2, S_3 are pairwise disjoint, and that χ_i is tamely ramified at each prime $p \in S_i$. By identifying $\chi_i \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z}) = H^1(G, \mathbb{Z}/n\mathbb{Z}) = H^1(G, \mu_n)$, we can take cup products of these characters.. For each finite place v of F, we further assume that

$$[\mathrm{loc}_v(\chi_i \cup \chi_j)] = 0.$$

For $i \neq j$. Which we will consider as "local linking conditions". Since each χ_i can be viewed as a Kummer cocycle for α_i, one can alternatively ([Mil20, III.4]) view the above condition as the vanishing of the Hilbert symbols $(\alpha_i, \alpha_j)_v = 1$.

In order to construct the triple symbol of characters, we wish to first show that global and local trivialisations of $\chi_1 \cup \chi_2 \cup \chi_3$ exists.

Proposition 4.27 (Existence of global trivialisation [KM25, Prop 1])**.** Let S be a set of primes containing $S_1 \cup S_2 \cup S_3$ and all the primes dividing n and all archimedean places.

There exists a cochain $\eta \in C^2(G, \mathbb{Z}/n\mathbb{Z})$ that globally trivialises $\chi_1 \cup \chi_2 \cup \chi_3$ and is unramified outside of S, i.e.

$$d\eta = \chi_1 \cup \chi_2 \cup \chi_3.$$

And η lies in the image of the inflation map $\inf\colon C^2(G_S, \mathbb{Z}/n\mathbb{Z}) \to C^2(G, \mathbb{Z}/n\mathbb{Z})$

Proof. Since χ_i is unramified outside of S, it represents a cocycle in $C^1(G_S, \mathbb{Z}/n\mathbb{Z})$, and thus $\chi_1 \cup \chi_2 \cup \chi_3$ represents a cocycle in $C^3(G_S, \mathbb{Z}/n\mathbb{Z})$. It suffices to show that $H^3(G_S, \mathbb{Z}/n\mathbb{Z}) = 0$, since then that would imply the existence of η.

Since S contains all primes p dividing n, from [NSW08, Prop 8.3.18] we can conclude that $\mathrm{cd}_p\, G_S \leq 2$. This means that $H^3(G_S, \mathbb{Z}/n\mathbb{Z})$ has no p-torsion for $p|n$.

On the other hand, since the multiplication by n map is the zero map on $\mathbb{Z}/n\mathbb{Z}$, the multiplication by n map on $H^3(G_S, \mathbb{Z}/n\mathbb{Z})$ is also the zero map, and thus $H^3(G_S, \mathbb{Z}/n\mathbb{Z})$ does not have any p-torsion for any $p \nmid n$, and thus $H^3(G_S, \mathbb{Z}/n\mathbb{Z}) = 0$. □

Proposition 4.28 (Existence of unramified local trivialisations [KM25, Prop 2])**.** Let v be a non-archimedean place of F. Assume S_1, S_2, S_3 are pairwise disjoint χ_i is tame, if the local linking condition is satisfied for $i \neq j$

$$[\mathrm{loc}_v(\chi_i \cup \chi_j)] = 0,$$

then there exists a cochain $\eta_v \in C^2(G_v, \mathbb{Z}/n\mathbb{Z})$ such that $d\eta_v = \mathrm{loc}_v(\chi_1 \cup \chi_2 \cup \chi_3)$. Moreover, the η_v is *unramified*, i.e. the cochain lies in the image of the inflation map $C^2(G_v^{ur}, \mathbb{Z}/n\mathbb{Z}) \to C^2(G_v, \mathbb{Z}/n\mathbb{Z})$.

Proof. Since $C^i(-, A \oplus B) \cong C^i(-, A) \oplus C^i(-, B)$, we can without loss of generality assume that $n = l^s$ is a prime power.

Let $\psi_i = \mathrm{loc}_v \circ \chi_i \in C^3(G_v, \mathbb{Z}/n\mathbb{Z})$. Suppose ψ_1, ψ_2, ψ_3 are all unramified, then we note that by [NSW08, Prop 1.7.7] $H^3(G_v^{ur}, \mathbb{Z}/n\mathbb{Z}) = H^3(\widehat{\mathbb{Z}}, \mathbb{Z}/n\mathbb{Z}) = 0$. So there must exist $\eta_v \in C^2(G_v^{ur}, \mathbb{Z}/n\mathbb{Z})$ that trivialises $\psi_1 \cup \psi_2 \cup \psi_3$ as desired.

Otherwise, exactly one ψ_i is ramified and the other two are unramified. WLOG let ψ_1 be ramified. We will prove that $\psi_1 \cup \psi_2 = 0$ as a cochain and thus we can simply pick the trivilaisation $\eta_v = 0$.

Suppose the character ψ_i has order d_i, by Kummer Theory ψ_i is given by a map of the form $\sigma \mapsto \sigma(\sqrt[n]{\beta_i})/\sqrt[n]{\beta_i}$ for $\beta_i \in F_v^\times$, and the extention associated to ψ_i is $F_v(\sqrt[n]{\beta_i})/F_v$. Since the character ψ_i has order d_i, this means that $\gamma_i := \sqrt[n]{\beta_i^{d_i}} \in K_v^\times$. We can consider the Kummer cocycle given by γ_i instead and notice that because we have assumed $n = l^s$ is a prime power, if $F_v(\sqrt[n]{\beta_i})/F_v$ is tamely ramified/unramified, $F_v(\sqrt[n]{\gamma_i})/F_v$ is also tamely ramified/unramified.

Thus we can write

$$\psi_1 = \frac{n}{d_1}\psi_{tm}; \quad \psi_2 = \frac{n}{d_2}\psi_{ur},$$

where $\psi_{tm}, \psi_{ur} \in H^1(G_v, \mathbb{Z}/n\mathbb{Z})$ have order n and are tamely ramified and unramified respectively.

On the other hand since

$$H^1(G_v, \mathbb{Z}/n\mathbb{Z}) \cong F_v^\times/(F_v^\times)^n \cong (\mathbb{Z}/n\mathbb{Z})^2$$

it follows that ψ_{tm}, ψ_{ur} actually span $H^1(G_v, \mathbb{Z}/n\mathbb{Z})$.

By Local Tate Duality [NSW08, Thm 7.2.6], $H^1(G_v, \mathbb{Z}/n\mathbb{Z})$ is dual to itself via the cup product. Thus there must exist some cocycle that when cupped with ψ_{ur} has order n. But since $\psi_{ur} \cup \psi_{ur} = 0$ it follows that $\psi_{ur} \cup \psi_{tm}$ must have order n.

By the local linking condition, we know that as a cohomology class:

$$\begin{aligned}[\psi_1 \cup \psi_2] &= 0 \\ \left[\frac{n}{d_1}\psi_{tm} \cup \frac{n}{d_2}\psi_{ur}\right] &= 0 \\ \frac{n^2}{d_1 d_2}\left[\psi_{tm} \cup \psi_{ur}\right] &= 0\end{aligned}$$

Since $[\psi_{ur} \cup \psi_{tm}]$ has order n, the above expression is equal to zero if and only if $d_1 d_2 | n$.

Finally since the cup product is bilinear on the level of cochains, we have a cochain-level equality

$$\begin{aligned}\psi_1 \cup \psi_2 &= \frac{n^2}{d_1 d_2}(\psi_{tm} \cup \psi_{ur}) \\ &= n\left(\frac{n}{d_1 d_2}\psi_{tm} \cup \psi_{ur}\right) \\ &= 0\end{aligned}$$

as desired. □

Proposition 4.29 (Independence from choices of S and trivialisations [KM25, Prop 3])**.** Let S be a set of places of F containing all archimedean places and also containing $S_1 \cup S_2 \cup S_3$. Suppose $\chi_1 \cup \chi_2 \cup \chi_3$ admits a global trivialisation η unramified outside S and that it admits an unramified local trivialisation η_v for each $v \in F$. Then if we define $\mathfrak{d}(\chi_1, \chi_2, \chi_3) \in \mathbb{Z}/n\mathbb{Z}$ as

$$\mathfrak{d}(\chi_1, \chi_2, \chi_3) = \sum_{v \in S} \mathrm{inv}_v(\mathrm{loc}_v\, \eta - \eta_v)$$

Where $\mathrm{inv}\colon H^2(G_v, \mathbb{Z}/n\mathbb{Z}) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is the local invariant map. This sum is independent of the choice of S and independent of the choices of trivilisation η, η_v.

Proof. Suppose η and η' are two choices of global trivialisation. Then $\eta - \eta' \in H^2(G, \mathbb{Z}/n\mathbb{Z})$.

By the Albert-Brauer-Hasse-Noether theorem, the sum of local invariant maps of any class in $H^2(G, \mathbb{Z}/n\mathbb{Z})$ must be zero, i.e.

$$\sum_v \mathrm{inv}_v \,\mathrm{loc}_v(\eta - \eta') = 0$$

Which implies the sum is independent of choice of global trivialisation unramified outside S.

Now suppose that for some place v, there are two unramified trivialisations η_v and η'_v. Then the difference of the cochains $\eta_v - \eta'_v$ must be an unramified cohomology class lying in the image of $H^2(G_v^{ur}, \mathbb{Z}/n\mathbb{Z})$. However, since $G_v^{ur} \cong \widehat{\mathbb{Z}}$, by [NSW08, Prop 1.7.7] we know that $H^2(G_v^{ur}, \mathbb{Z}/n\mathbb{Z}) = 0$, and thus $\mathrm{inv}_v\, \eta_v - \mathrm{inv}_v\, \eta'_v = \mathrm{inv}_v(\eta_v - \eta'_v) = \mathrm{inv}_v(0) = 0$.

Finally, it suffices to show that if S are sets that contain all archimedean places and $S_1 \cup S_2 \cup S_3$, and admits a global trivialisation η, then replacing S with S' for $S \subset S'$ does not alter the sum. First of all note that since the quotient map $G \to G_S$ factors through G'_S. Thus η also lies in the image of $C^2(G_{S'}, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\inf} C^2(G, \mathbb{Z}/n\mathbb{Z})$ and is a cochain unramified outside S'.

Let v be a place in $S' \setminus S$. We wish to show that $\mathrm{inv}_v(\mathrm{loc}_v\, \eta - \eta_v) = 0$. Since η is unramified outside of S, it follows from lemma 4.26 that $\mathrm{loc}_v\, \eta$ is an unramified local trivialisation. Since η_v is also an unramified cochain, it follows that $\mathrm{loc}_v\, \eta - \eta_v$ is an unramified cocycle in $H^2(G_v^{ur}, \mathbb{Z}/n\mathbb{Z}) = 0$, thus it follows that $\mathrm{inv}_v(\mathrm{loc}_v\, \eta - \eta_v) = 0$, as desired. □

Thus finally we can define the triple symbol

Definition 4.30. Suppose χ_1, χ_2, χ_3 are characters satisfying the assumptions of the above proposition, then we define

$$[\chi_1, \chi_2, \chi_3]_n = \zeta(\mathfrak{d}(\chi_1, \chi_2, \chi_3)).$$

Where $\zeta\colon \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to \mu_n$ was our choice of primitive nth root of unity (We identify $\mathbb{Z}/n\mathbb{Z}$ and $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ in the obvious manner).

We now detail some properties of the triple symbol of characters.

Proposition 4.31. The triple symbol of characters

$$[-,-,-]_n\colon H^1(G, \mathbb{Z}/n\mathbb{Z}) \to \mu_n$$

is an alternating trilinear form on the space of characters $H^1(G, \mathbb{Z}/n\mathbb{Z})$.

Proof. We first prove that the triple symbol is alternating. Let $\sigma \in S_3$ be a permutation with sign $|\sigma|$, we wish to show that $[\chi_{\sigma(1)}, \chi_{\sigma(2)}, \chi_{\sigma(3)}]_n = [\chi_1, \chi_2, \chi_3]_n^{|\sigma|}$ (This is also Corollary 1 of [KM25]). This follows from the fact that the cup product is alternating, i.e.

$$\chi_{\sigma(1)} \cup \chi_{\sigma(2)} \cup \chi_{\sigma(3)} = |\sigma|(\chi_1 \cup \chi_2 \cup \chi_3).$$

In particular, the two triple cup products differ by at most a sign. If η and η_v are global and local trivialisations of $\chi_1 \cup \chi_2 \cup \chi_3$, then $|\sigma|\eta$ and $|\sigma|\eta_v$ are global and local trivialisations of $\chi_{\sigma(1)} \cup \chi_{\sigma(2)} \cup \chi_{\sigma(3)}$. Thus $\mathfrak{d}(\chi_{\sigma(1)}, \chi_{\sigma(2)}, \chi_{\sigma(3)}) = |\sigma|\mathfrak{d}(\chi_1, \chi_2, \chi_3)$, and

$$[\chi_{\sigma(1)}, \chi_{\sigma(2)}, \chi_{\sigma(3)}]_n = [\chi_1, \chi_2, \chi_3]_n^{|\sigma|},$$

as desired.

We now check linearity in the first argument. Suppose $[\chi_1, \chi_2, \chi_3]_n$ and $[\chi_1', \chi_2, \chi_3]_n$ are defined via choices of places S and S' respectively. By taking $T = S \cup S'$, we can assume that the triple symbols are defined over the set of places T instead. This is possible because if η is a global trivialisation of $\chi_1 \cup \chi_2 \cup \chi_3$ unramified outside of S, then it must also be unramified outside of T, and for any $v \in T \setminus S$, we can take $\eta_v = \mathrm{loc}_v\, \eta$ which will be an unramified trivilisation at the place v. Similarly, there exists a global trivialisation η' unramified outside of T and unramified local trivialisations η' for $\chi_1' \cup \chi_2 \cup \chi_3$.

Then by the linearity of the cup product, $\eta + \eta'$ is a global trivialisation of $(\chi_1 + \chi_1') \cup \chi_2 \cup \chi_3$ unramified outside of T, and for each $v \in T$, $\eta_v + \eta_v'$ is an umramified local trivalisation of $(\chi_1 + \chi_1') \cup \chi_2 \cup \chi_3$. Thus

$$\begin{aligned}
\mathfrak{d}(\chi_1 + \chi_1', \chi_2, \chi_3) &= \sum_{v \in T} \mathrm{inv}_v(\mathrm{loc}_v(\eta + \eta') - (\eta_v + \eta_v')) \\
&= \sum_{v \in T} \mathrm{inv}_v(\mathrm{loc}_v\, \eta - \eta_v) + \mathrm{inv}_v(\mathrm{loc}_v\, \eta' - \eta_v') \\
&= \mathfrak{d}(\chi_1, \chi_2, \chi_3) + \mathfrak{d}(\chi_1', \chi_2, \chi_3).
\end{aligned}$$

And thus

$$[\chi_1 + \chi_1', \chi_2, \chi_3]_n = [\chi_1, \chi_2, \chi_3]_n [\chi_1', \chi_2, \chi_3]_n,$$

and the triple symbol is trilinear in the first argument. Combining this with the alternating property of the symbol proves that it is also trilinear in the other arguments. □

Remark 4.32. The Redei triple symbol and other explicit arithmetic triple symbols can be recovered by the triple symbol of characters.

1. Let $p_1, p_2, p_3 \equiv 1 \pmod 4$ be rational primes satisfying the assumptions of definition 4.20.

Define $\chi_i\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z}$ to be the Kummer character coming from p_i, i.e.

$$(-1)^{\chi_i}(g) = \frac{g(\sqrt{p_i})}{\sqrt{p_i}}.$$

Then the triple symbol of the characters χ_i recovers the Redei triple symbol

$$[\chi_1, \chi_2, \chi_3]_2 = [p_1, p_2, p_3].$$

This is proved in [KM25, Thm 2].

2. Similarly, the triple symbol of characters also recovers the Amano-Mizusawa-Morishita mod 3 triple symbol and the mod 2 triple symbol over real quadratic fields mentioned in remark 4.22. Thus we can view this triple symbol of characters as a generalisation of known explicit arithmetic triple symbols.

4.5.3 The Arithmetic Chern–Simons Action of Massey Type

The triple symbol of characters was defined as the difference between ramified global trivialisations and unramified local trivialisations of a degree 3 Galois cocycle. This definition seems quite similar to the statement and proof of the decomposition formula for arithmetic Chern-Simons theory given in theorem 2.10. Turns out, the unramified case of the character triple symbol can be identified with a special case of the arithmetic Chern-Simons action. A reference for this can be found in [Chu+20].

Let A be a finite group, $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$ be a cocyle, then recall (definition 2.2) that the *arithmetic Chern-Simons action* is

$$\begin{aligned} \mathrm{CS}_c\colon \mathrm{Hom}(\pi_1(X), A) &\to \mathbb{Z}/n\mathbb{Z} \\ \rho &\mapsto \mathrm{inv}(j(\rho^*(c))) \end{aligned}$$

where $j\colon H^3(\pi_1(X), \mathbb{Z}/n\mathbb{Z}) \to H^3(X, \mathbb{Z}/n\mathbb{Z})$ is the edge homomorphism coming from the Hochschild-Serre spectral sequence.

Definition 4.33. The *arithmetic Chern-Simons action with Massey type*, as defined in [Kim25], is the specification of (A, c) where $A = (\mathbb{Z}/n\mathbb{Z})^3$ and

$$c = \mathrm{pr}_1 \cup \mathrm{pr}_2 \cup \mathrm{pr}_3 \in H^3((\mathbb{Z}/n\mathbb{Z})^3, \mathbb{Z}/n\mathbb{Z}),$$

where $\mathrm{pr}_i \in H^1(A, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(A, \mathbb{Z}/n\mathbb{Z})$ is the projection map from $(\mathbb{Z}/n\mathbb{Z})^3$ to its ith component.

Turns out when the characters χ_i are unramified characters, the character triple symbol recovers the Chern-Simons action of Massey type.

Theorem 4.34 ([Kim25, Thm 3])**.** Suppose $\rho\colon \pi_1(X) \to (\mathbb{Z}/n\mathbb{Z})^3$ is given by $\rho = (\chi_1, \chi_2, \chi_3)$, where $\chi_i\colon \pi_1(X) = \mathrm{Gal}(K^{\mathrm{ur}}/K) \to \mathbb{Z}/n\mathbb{Z}$ is an unramified character. Then letting CS_c denote the Massey type arithmetic Chern simons of Massey type, there is an equality

$$\exp(2\pi i\, \mathrm{CS}_c(\rho)) = [\chi_1, \chi_2, \chi_3]_n^{-1}.$$

Proof. The proof involves simply comparing the proof of the decomposition formula in theorem 2.10 and the definition of the triple symbol term by term. Firstly note that a character $\chi_i\colon \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}/n\mathbb{Z}$ is unramified if and only if the character factors through $\mathrm{Gal}(\overline{K}/K) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K)$.

Note that since we have taken $c = \mathrm{pr}_1 \cup \mathrm{pr}_2 \cup \mathrm{pr}_3$, the pullback of c along ρ is precisely

$$\rho^*(c) = \chi_1 \cup \chi_2 \cup \chi_3.$$

From propositions 4.27 and 4.28, there exists a set of places S and trivialisations η unramified outside of S and η_v unramified for $v \in S$, of $\chi_1 \cup \chi_2 \cup \chi_3$. Moreover by proposition 4.29 we have the formula

$$\mathfrak{d}(\chi_1, \chi_2, \chi_3) = \sum_{v \in S} \mathrm{inv}_v(\mathrm{loc}_v\, \eta - \eta_v).$$

On the other hand, comparing to the proof of the decomposition formula in theorem 2.10, we can set $\beta_+ = \eta$ to be the global trivialisation unramified outside of S, and $\beta_{-,v} = \eta_v$ to be the local unramified trivialisations. Then we can see that

$$\mathfrak{d}(\chi_1, \chi_2, \chi_3) = -\,\mathrm{CS}_c(\rho),$$

from which the theorem follows. □

Remark 4.35. In [HKM23], it seems an alternate convention is used and their decomposition formula differs from theorem 2.10 (which follows [Chu+20]) by a sign. If that version of the decomposition formula was used instead, then via the same proof one would obtain that $\mathfrak{d}(\chi_1, \chi_2, \chi_3) = \mathrm{CS}_c(\rho)$ and thus

$$\exp(2\pi i\, \mathrm{CS}_c(\rho)) = [\chi_1, \chi_2, \chi_3]_n.$$

4.6 Towards Arithmetic Path Integrals of Massey Type

Since physical path integrals give rise to topological invariants, in this section we wish to evaluate the path integral associated to the arithmetic Chern-Simons action of Massey type, which is the sum of the form

$$\sum_{\rho \in \mathrm{Hom}(\pi, A)} e^{2\pi i\, \mathrm{CS}_c(\rho)}.$$

It should be noted that an explicit formula for this path integral was not obtained in this thesis. However, the following section highlights some partial results and lemmas towards computing the path integral, and example computations in the case where the class group of X has a small p-rank.

Since every homomorphism $\rho\colon \pi \to (\mathbb{Z}/n\mathbb{Z})^3$ can be written as $\rho = (\chi_1, \chi_2, \chi_3)$, where $\chi_i \in \mathrm{Hom}(\pi, \mathbb{Z}/n\mathbb{Z}) = H^1(X, \mathbb{Z}/n\mathbb{Z})$, and

$$\mathrm{CS}_c(\rho) = \mathrm{inv}(\rho^*(c)) = \mathrm{inv}(\chi_1 \cup \chi_2 \cup \chi_3),$$

we can rewrite the sum as

$$\sum_{\chi_1, \chi_2, \chi_3 \in H^1(X, \mathbb{Z}/n\mathbb{Z})} \exp(2\pi i\, \mathrm{inv}(\chi_1 \cup \chi_2 \cup \chi_3)).$$

4.6.1 A Critical Set

From now on we specialise to the case where $n = p$ is an odd prime. Since $H^1(X, \mathbb{Z}/p\mathbb{Z})$ is an $\mathbb{F}_p$-vector space, let $r = \dim_{\mathbb{F}_p} H^1(X, \mathbb{Z}/p\mathbb{Z})$. Then we show that the path integral depends only on the size of a set $\mathcal{S}$.

Proposition 4.36. Define the set $\mathcal{S}$ to be the triples of characters that cup to zero

$$\mathcal{S} = \{(\chi_1, \chi_2, \chi_3) |\, \mathrm{inv}(\chi_1 \cup \chi_2 \cup \chi_3) = 0\}.$$

Then the path integral evaluates to

$$\sum_{\chi_1,\chi_2,\chi_3\in H^1(X,\mathbb{Z}/n\mathbb{Z})} \exp(2\pi i \operatorname{inv}(\chi_1\cup\chi_2\cup\chi_3)) = s - \frac{p^{3r}-s}{p-1},$$

where $s = |\mathcal{S}|$.

Proof. Suppose χ_1, χ_2, χ_3 are characters such that $\mathrm{CS}_c(\chi_1,\chi_2,\chi_3) \neq 0$, by the trilinearity of the Massey type Chern Simons action (see proposition 4.31 and [Kim25, Lem. 12, 13]), it follows that $\exp(2\pi i \operatorname{inv}(\chi_1\cup\chi_2\cup(a\chi_3)))$ is a distinct primitive pth root of unity for every $a = 1, 2, \ldots, p-1$. In particular this means that

$$\sum_{a=1}^{p-1} \exp(2\pi i \operatorname{inv}(\chi_1\cup\chi_2\cup(a\chi_3))) = -1.$$

Moreover, the set of triples of characters χ_1, χ_2, χ_3 satisfying $\mathrm{CS}_c(\chi_1,\chi_2,\chi_3) \neq 0$ clearly satisfy $\chi_3 \neq 0$, and thus can be partitioned into sets of size $p-1$ of the form

$$\{(\chi_1, \chi_2, a\chi_3) | \chi_3 \neq 0, a \in (\mathbb{Z}/p\mathbb{Z})^\times\}.$$

On the other hand, if $\mathrm{CS}_c(\chi_1,\chi_2,\chi_3) = 0$, then clearly $\exp(2\pi i\,\mathrm{CS}_c(\chi_1,\chi_2,\chi_3)) = 1$. Let us define the set $\mathcal{S}$ to be the set of triples of characters such that $\mathrm{CS}_c(\chi_1,\chi_2,\chi_3) = 0$ and let $s = |S|$.

Then the remaining $p^{3r} - s$ triples with non-zero cup product can be partitioned into $\frac{p^{3r}-s}{p-1}$ sets each containing every non-zero root of unity exactly once, contributing -1 to the sum. Then the path integral simply evaluates to

$$\sum_{\chi_1,\chi_2,\chi_3\in H^1(X,\mathbb{Z}/n\mathbb{Z})} \exp(2\pi i \operatorname{inv}(\chi_1\cup\chi_2\cup\chi_3)) = s - \frac{p^{3r}-s}{p-1}.$$

Finally, we notice that the invariant map $\operatorname{inv}\colon H^3(X,\mu_n) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is an isomorphism, so $\mathrm{CS}_c(\chi_1,\chi_2,\chi_3) = 0$ if and only if $\chi_1\cup\chi_2\cup\chi_3 = 0$, thus proving the proposition.

□

From the proposition, we find that the path integral is uniquely determined by the size of the set $\mathcal{S}$. The rest of this section is dedicated towards attempts at computing this set.

We make some observations about the set $\mathcal{S}$. Let $e_1, \ldots, e_r$ be a basis of the $\mathbb{F}_p$-vector space $H^1(X, \mathbb{Z}/p\mathbb{Z})$, and denote by c_{ijk} the cup product

$$c_{ijk} \coloneqq \operatorname{inv}(e_i \cup e_j \cup e_k).$$

We note from the alternating trilinearity of the triple cup product that

- If $\sigma \in S_3$ is a permutation, then $c_{\sigma(ijk)} = |\sigma| c_{ijk}$.
- If any two of i, j, k are equal, then $c_{ijk} = 0$.

On the other hand, suppose $\chi_i \in H^1(X,\mathbb{Z}/p\mathbb{Z})$ can be written as $\chi_i = \sum_j a_{ij}e_j$ when decomposed into a linear combination of the basis elements. Let $A = (a_{ij})$ be the $3\times r$ matrix consisting of these coefficients, and denote by A_j the jth column of A. Then we can write $\operatorname{inv}(\chi_1\cup\chi_2\cup\chi_3)$ as

$$\operatorname{inv}(\chi_1\cup\chi_2\cup\chi_3) = \sum_{i=1}^{r}\sum_{j=1}^{r}\sum_{k=1}^{r} \operatorname{inv}(a_{1i}e_i \cup a_{2j}e_j \cup a_{3k}e_k)$$

$$
\begin{aligned}
&= \sum_{i=1}^{r}\sum_{j=1}^{r}\sum_{k=1}^{r} a_{1i}a_{2j}a_{3k}c_{ijk} \\
&= \sum_{\substack{1\le i,j,k\le r \\ i\neq j, j\neq k, i\neq k}} a_{1i}a_{2j}a_{3k}c_{ijk} \\
&= \sum_{1\le i<j<k\le r} \left(\sum_{\sigma\in S_3} a_{\sigma(1)i}a_{\sigma(2)j}a_{\sigma(3)k}c_{\sigma(ijk)} \right) \\
&= \sum_{1\le i<j<k\le r} \left(\sum_{\sigma\in S_3} a_{\sigma(1)i}a_{\sigma(2)j}a_{\sigma(3)k}|\sigma|c_{ijk} \right) \\
&= \sum_{1\le i<j<k\le r} \det(A_i|A_j|A_k)c_{ijk}.
\end{aligned}
$$

Thus we obtain the following proposition

Proposition 4.37. Let $c_{ijk} = \mathrm{inv}(e_i \cup e_j \cup e_k)$. The set S is in bijection with the set of $3 \times r$ matrices A satisfying

$$\sum_{1\le i<j<k\le r} \det(A_i|A_j|A_k)c_{ijk} = 0.$$

4.6.2 Some Examples of Small Rank

Via the observation in the previous section, we classify the possible values of $s = |\mathcal{S}|$ in cases where $r = \dim_{\mathbb{F}_p}(X, \mathbb{Z}/p\mathbb{Z})$ is small.

By abuse of notation, let us identify the groups

$$\mathrm{inv}\colon H^3(X, \mathbb{Z}/p\mathbb{Z}) \simeq \tfrac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z},$$

and write $\chi_1 \cup \chi_2 \cup \chi_3$ for its image in $\mathbb{Z}/p\mathbb{Z}$ under these isomorphisms.

When $r = 1$ or 2, every triple of cocycles cups to zero, so $s = p^{3r}$.

Rank $r = 3$

If $e_1 \cup e_2 \cup e_3 = 0$, then everything cups to zero, and we once again have $s = p^{3r} = p^9$

Otherwise, we can assume without loss of generality that $e_1 \cup e_2 \cup e_3 = 1$. Then by proposition 4.37, $\mathcal{S}$ is in bijection with the matrices $A = (a_{ij})$ such that $\det(A) = 0$. By counting the non-singular matrices instead, we obtain

$$s = p^9 - (p^3 - 1)(p^3 - p)(p^3 - p^2).$$

Rank $r = 4$

Turns out once again there are 2 possible values for s. If everything cups to zero, and we once again have $s = p^{3r} = p^{12}$.

Otherwise, let us assume without loss of generalise that $e_1 \cup e_2 \cup e_3 = 1$. Then

Lemma 4.38. Via a change of basis one can assume that

$$e_1 \cup e_2 \cup e_4 = e_1 \cup e_3 \cup e_4 = e_3 \cup e_3 \cup e_4 = 0.$$

Proof. Writing $e_i \cup e_j \cup e_k = c_{ijk}$, consider

$$e_4 \mapsto e_4' = e_4 - c_{234}e_1 - c_{134}e_2 - c_{124}e_3$$

and this will be a basis satisfying the above, e.g.

$$e_1 \cup e_2 \cup e_4' = e_1 \cup e_2 \cup e_4 - c_{124} = 0$$

as desired. □

Then, letting $A = (a_{ij})$ be the 3×4 matrix of coefficients of the χ_i's as above, then $\mathcal{S}$ is in bijection with with the matrices A such that the determinant of the first 3 columns $\det(A_1|A_2|A_3)$ is equal to zero and no restrictions on the final column. This gives

$$s = p^3[p^9 - (p^3-1)(p^3-p)(p^3-p^2)].$$

Rank $r = 5$

This time there are 3 possible values for s. Once again, if everything cups to zero, then $p^{3r} = p^{15}$. Otherwise, let us assume without loss of generality that $c_{123} = 1$.

We can apply the transformation from the previous lemma and set

$$e_4 \mapsto e_4' = e_4 - c_{234}e_1 - c_{134}e_2 - c_{124}e_3; \quad e_5 \mapsto e_5' = e_5 - c_{235}e_1 - c_{135}e_2 - c_{125}e_3.$$

This transformation ensures that whenever $i, j \in \{1,2,3\}$ and $k \in \{4,5\}$, the cup product $c_{ijk} = 0$ vanishes. .

Now consider the case where c_{i45} are all equal to zero. Then any triple cup product containing e_4 or e_5 Thus $\mathcal{S}$ is in bijection with with the matrices A such that the determinant of the first 3 columns $\det(A_1|A_2|A_3)$ is equal to zero and no restrictions on the final two columns. This gives

$$s = p^6[p^9 - (p^3-1)(p^3-p)(p^3-p^2)].$$

Finally, we consider the case that at least one of c_{i45} is nonzero. Without loss of generality let $c_{345} = 1$. Then consider the change of basis

$$e_1 \mapsto e_1' = e_1 - c_{145}e_3; \quad e_2 \mapsto e_2' = e_2 - c_{245}e_3.$$

This transformation sets $c_{145} = c_{245} = 0$. It can also be checked when $i, j \in \{1,2,3\}$ and $k \in \{4,5\}$ that c_{ijk} is still equal to zero. Thus via a change of basis this case satisfies

$$c_{123} = c_{345} = 1,$$

and all other triple cup products between the basis elements vanish.

In this case, the set $cS$is in bijection to the set of 3×6 matrices A where

$$\det(A_1|A_2|A_3) + \det(A_3|A_4|A_5) = 0.$$

We count these matrices explicitly, For convenience let A_{ijk} denote the matrix $(A_i|A_j|A_k)$.

1. If $\det(A_{123}) \neq 0$:

   In this case, we can simply go through the number of choices for each column. There are p^3-1, p^3-p, p^3-p^2 choices for A_1, A_2, A_3 respectively. Then there are p^3-p choices for A_4.

   Once A_1 to A_4 are fixed, There are $p^3 - p^2$ choices for A_5 that make the determinant nonzero, but $\frac{p^3-p^2}{p-1} = p^2$ choices that make the determinant of A_{345} the required number

such that $\det(A_3|A_4|A_5) = -\det(A_1|A_2|A_3)$. Thus there are

$$p^2(p^3-1)(p^3-p)^2(p^3-p^2)$$

matrices.

2. Otherwise, $\det(A_1|A_2|A_3) = \det(A_3|A_4|A_5) = 0$:

   If the middle column is zero, then there are p^{12} such matrices

   Otherwise, there are (p^3-1) choices for the middle column. And on each side, there are $p^6 - (p^3-p)(p^3-p^2)$ ways to choose the remaining two columns so that the determinant is equal to zero. So there are

$$p^{12} + (p^3-1)[p^6 - (p^3-p)(p^3-p^2)]^2$$

   such matrices.

Combinding the two cases, we have that

$$\begin{aligned}|\mathcal{S}| &= p^{12} + (p^3-1)[p^6 - (p^3-p)(p^3-p^2)]^2 + p^2(p^3-1)(p^3-p)^2(p^3-p^2) \\ &= p^7(p^7+p^5-p^3-p+1)\end{aligned}$$

The computations in this subsection can be summarised in the following table

Rank r	Conditions on c_{ijk}	$s = \lvert\mathcal{S}\rvert$	Value of Path Integral
$r \geq 1$	$c_{ijk} \equiv 0$	p^{3r}	p^{3r}
$r \geq 3$	$c_{123} = 1$, else 0	$p^{3(r-3)}[p^9 - (p^3-1)(p^3-p)(p^3-p^2)]$	$p^{3(r-3)}[p^9 - (p^3-1)(p^3-p)(p^3-2p^2)]$
$r = 5$	$c_{123} = c_{345} = 1$, else 0	$p^7(p^7+p^5-p^3-p+1)$	$p^8(p^4+p^3-1)$

Table 4.1: Possible values of the Path Integral when $r \leq 5$.

4.6.3 Equivalence Classes of Alternating Trilinear Forms

From the example computations above, we see that propositions 4.36 and 4.37 imply that the Massey type path integral is in fact uniquely determined the coefficients c_{ijk} up to a change of basis of $H^1(X, \mathbb{Z}/p\mathbb{Z})$.

Corollary 4.39. The path integral of Massey type is uniquely determined by the equivalance class of the alternating trilinear form on $H^1(X, \mathbb{Z}/p\mathbb{Z})$ given by the cup product

$$- \cup - \cup - \colon H^1(X, \mathbb{Z}/p\mathbb{Z})^3 \to \tfrac{1}{p}\mathbb{Z}/\mathbb{Z}.$$

Unfortunately, as $r = \dim_{\mathbb{F}_p} H^1(X, \mathbb{Z}/p\mathbb{Z})$ grows, the number of equivalence classes grows extremely rapidly. For example, when $p = 2$, there are 348 different classes alternating trilinear forms on $\mathbb{F}_2^9$ [HP21]. In general, the number of n-dimensional trilinear forms over a finite field $\mathbb{F}_q$ is lower bounded by $q^{n(n^2-9n+2)/6}$ [DS14].

Moreover, given a number field $X = \operatorname{Spec} \mathcal{O}_K$, determining which equivalence class of trilinear form the triple cup product lies in is a non-trivial task. Indeed, determining whether or not all possible equivalence classes can even occur, and how often they occur, would be an interesting arithmetic statistics problem.

4.6.4 Towards Explicit Evaluation of the Triple Cup Product

In this section we attempt to compute the triple cup product directly, using machinery from [AC23] to write the cup product in terms of certain norm conditions.

We use angle brackets to denote the Artin-Verdier duality pairing

$$\langle \cdot, \cdot \rangle \colon H^i(X, \mathbb{Z}/n\mathbb{Z}) \times \mathrm{Ext}_X^{3-i}(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m) \to \mathbb{Q}/\mathbb{Z}$$

Via the calculations in [AC23, Cor 2.15], we can write the groups $H^i(X, \mathbb{Z}/n\mathbb{Z})$ and $\mathrm{Ext}_X^i(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m)$ explcitly

$$H^i(X, \mathbb{Z}/n\mathbb{Z}) = \begin{cases} \mathbb{Z}/n\mathbb{Z} & i = 0 \\ (\mathrm{Cl}\, K/n)^\sim & i = 1 \\ (Z_1/B_1)^\sim & i = 2 \\ \mu_n(K)^\sim & i = 3 \\ 0 & i > 3 \end{cases}, \qquad \mathrm{Ext}_X^i(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m) = \begin{cases} \mu_n(K) & i = 0 \\ Z_1/B_1 & i = 1 \\ \mathrm{Cl}\, K/n & i = 2 \\ \mathbb{Z}/n\mathbb{Z} & i = 3 \\ 0 & i > 3, \end{cases}$$

where $^\sim$ detnotes the Pontryagin dual, and Z_1, B_1 are defined as

$$\begin{aligned} Z_1 &= \{(a, \mathfrak{a}) \in K^\times \oplus \mathrm{Div}(X) | \, \mathrm{div}(a) + n\mathfrak{a} = 0\} \\ B_1 &= \{(b^{-n}, \mathrm{div}(b)) \in K^\times \oplus \mathrm{Div}(X) | b \in K^\times\} \end{aligned}$$

Any character $\chi_i \in H^1(X, \mathbb{Z}/p\mathbb{Z})$ corresponds to a $\mathbb{Z}/p\mathbb{Z}$ torsor of X, which is a cyclic unramified p-extension L_i/K together with a choice of generator $\sigma_i \in \mathrm{Gal}(L_i/K)$.

Moreover, we have assumed that K contains all pth roots of unity and fixed an isomorphism $\zeta \colon \mu_p(X) \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$, the extensions L_i/K must neccesarily be Kummer. Let $\xi \in \mu_p(K)$ denote the preimage of 1 under the map ζ, and there must exist $a_i \in K^\times$ such that the Kummer extensions L_i are given by $L_i = K(a_i^{1/p})$ satisfying

$$\xi = \frac{\sigma_i(a_i^{1/p})}{a_i^{1/p}}.$$

Let $\mathfrak{a} \in \mathrm{Div}\, K$ be a fractional ideal of K such that $\mathfrak{a}\mathcal{O}_{L_1} = \mathrm{div}(a_1^{1/p})$. In other words, $\mathfrak{a}$ is the ideal satisfying $\mathfrak{a}^p = (a_1)$.

Then by [AC23, Prop 1.2], there is an equality

$$\begin{aligned} \mathrm{inv}(\chi_1 \cup \chi_2 \cup \chi_3) &= \langle \chi_1 \cup \chi_2 \cup \chi_3, \xi \rangle \\ &= \langle \chi_2 \cup \chi_3, (a_1^{-1}, \mathfrak{a}) \rangle \end{aligned}$$

Furthermore, let $I \in \mathrm{Div}\, L_2$ be a fractional ideal of L_2 such that $\mathfrak{a}\mathcal{O}_{L_2} = I - \sigma_2(I) + \mathrm{div}(t)$ for some $t \in L_2^\times$ satisfying $N_{L_2/K}(t) = a_1$.

Then via applying [AC23, Prop 1.1], we have that:

$$\begin{aligned} \langle \chi_2 \cup \chi_3, (a_1^{-1}, \mathfrak{a}) \rangle &= \left\langle \chi_3, N_{L_2/K}(I) + \frac{p}{2}\mathfrak{a} \right\rangle \\ &= \left\langle \chi_3, N_{L_2/K}(I) \right\rangle \\ &= \chi_3 \left(N_{L_2/K}(I) \right) \end{aligned}$$

Where the final equality is due to the identification $H^1(X, \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{Hom}(\pi_1(X), \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{Hom}(\mathrm{Cl}(X), \mathbb{Z}/p\mathbb{Z})$ via the Class Field Theory isomorphism, and the term $\frac{p}{2}\mathfrak{a}$ can be ignored when p is odd.

In particular, this is equal to zero if and only if $N_{L_2/K}(I)$ lies in the image of $N_{L_3/K}$.

4.7 Towards Profinite Triple Symbols

Linking numbers and multiple linking numbers mod n are well defined if $\mu_n \subset K$, and are compatible in the sense that if $n|m$, the mod m linking number modded by n gives the mod n linking number.

Given a cyclotomic field $K = \mathbb{Q}(\mu_{p^\infty})$ or $K = \mathbb{Q}(\mu_\infty)$, it should in theory be possible to define $\mathbb{Z}_p$ or $\widehat{\mathbb{Z}}$ (respectively) valued linking numbers, bringing the analogy closer to the case of characteristic zero linking numbers in topology.

It would be very interesting problem to define such a linking number, and determine the arithmetic meaning of these profinite $\mathbb{Z}_p$ or $\widehat{\mathbb{Z}}$ linking numbers. This section provides some partial results towards this goal.

4.7.1 Compatibility of Triple Symbols

In this section we prove that triple symbols of characters defined in definition 4.30 satisfies various compatibility conditions when varying between values of n or passing to field extensions.

Let $n|m$ and $\mu_m \subset K$ for a number field K. Then there is an embedding $\iota\colon \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z}$. Fix a primitive mth root $\zeta\colon \mathbb{Z}/m\mathbb{Z} \to \mu_m$ and we fix a primitive nth root by simply precomposing with ι and identifying the image of that map with μ_n.

Proposition 4.40. Given a character $\chi_i\colon G \to \mathbb{Z}/n\mathbb{Z}$, one can compose with ι to obtain $\iota_*\chi_i\colon G \to \mathbb{Z}/m\mathbb{Z}$, then

$$[\iota_*\chi_1, \iota_*\chi_2, \iota_*\chi_3]_m = ([\chi_1, \chi_2, \chi_3]_n)^{(m/n)^2}.$$

Proof. On the level of cochains, we can write the cup product $\chi_1 \cup \chi_2 \cup \chi_3$ as

$$(\chi_1 \cup \chi_2 \cup \chi_3)(g_1, g_2, g_3) = \chi_1(g_1)\chi_2(g_2)\chi_3(g_3).$$

The embedding $\iota\colon \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z}$ is given by multiplying by $\frac{m}{n}$. Thus we can express the cochain $\iota_*(\chi_1 \cup \chi_2 \cup \chi_3)$ as

$$\iota_*(\chi_1 \cup \chi_2 \cup \chi_3)(g_1, g_2, g_3) = \frac{m}{n}\chi_1(g_1)\chi_2(g_2)\chi_3(g_3).$$

On the other hand, we have that

$$(\iota_*\chi_1 \cup \iota_*\chi_2 \cup \iota_*\chi_3)(g_1, g_2, g_3) = \iota_*\chi_1(g_1)\iota_*\chi_2(g_2)\iota_*\chi_3(g_3) = \left(\frac{m}{n}\right)^3 \chi_1(g_1)\chi_2(g_2)\chi_3(g_3).$$

Now suppose η is a trivialisation of $\chi_1 \cup \chi_2 \cup \chi_3 \in H^3(G, \mathbb{Z}/n\mathbb{Z})$, then $\left(\frac{m}{n}\right)^2 \iota_*\eta$ will trivialise $\iota_*\chi_1 \cup \iota_*\chi_2 \cup \iota_*\chi_3 \in H^3(G, \mathbb{Z}/m\mathbb{Z})$, since

$$d\left(\left(\tfrac{m}{n}\right)^2 \iota_*\eta\right) = \left(\tfrac{m}{n}\right)^3 d\eta = \left(\tfrac{m}{n}\right)^3 (\chi_1 \cup \chi_2 \cup \chi_3) = \iota_*\chi_1 \cup \iota_*\chi_2 \cup \iota_*\chi_3.$$

Moreover, since ι_* commutes with the inflation map, if η is unramified outside of S, then $\iota_*\eta$ is unramified outside of S. We can similarly deduce that if η_v is an unramified local trivialisation of $\chi_1 \cup \chi_2 \cup \chi_3$, then $\left(\frac{m}{n}\right)^2 \iota_*\eta_v$ is also an unramified local trivialisation of $\iota_*\chi_1 \cup \iota_*\chi_2 \cup \iota_*\chi_3$.

Since the invariant map on $H^2(G_v, \mathbb{Z}/n\mathbb{Z})$ is defined by embedding $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n \hookrightarrow \overline{F_v}^\times$ and applying the invariant map $H^2(G_v, \overline{F_v}^\times) \to \mathbb{Q}/\mathbb{Z}$. The map $\mathbb{Z}/n\mathbb{Z} \to \overline{F_v}^\times$ factors through ι so it follows that $\mathrm{inv}_v(\iota_*c) = \mathrm{inv}_v(c)$ and we can conconclude from the fact that ι_* commutes with

loc_v

$$\begin{aligned}\mathfrak{d}(\iota_*\chi_1, \iota_*\chi_2, \iota_*\chi_3) &= \sum_{v\in S} \mathrm{inv}_v(\mathrm{loc}_v \left(\tfrac{m}{n}\right)^2 \iota_*\eta - \left(\tfrac{m}{n}\right)^2 \iota_*\eta_v) \\ &= \left(\tfrac{m}{n}\right)^2 \sum_{v\in S} \mathrm{inv}_v(\iota_*(\mathrm{loc}_v\, \eta - \eta_v)) \\ &= \left(\tfrac{m}{n}\right)^2 \sum_{v\in S} \mathrm{inv}_v(\mathrm{loc}_v\, \eta - \eta_v) \\ &= \left(\tfrac{m}{n}\right)^2 \mathfrak{d}(\chi_1, \chi_2, \chi_3)\end{aligned}$$

And thus

$$[\chi_1, \chi_2, \chi_3]_n^{(m/n)^2} = \zeta\left(\left(\tfrac{m}{n}\right)^2 \mathfrak{d}(\chi_1, \chi_2, \chi_3)\right) = \zeta(\mathfrak{d}(\iota_*\chi_1, \iota_*\chi_2, \iota_*\chi_3)) = [\iota_*\chi_1, \iota_*\chi_2, \iota_*\chi_3]_m.$$

□

Proposition 4.41. Let $q\colon \mathbb{Z}/m\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ be the quotient map. By composing characters $\chi_i\colon G \to \mathbb{Z}/m\mathbb{Z}$ with q we obtain characters $q_*\chi_i\colon G \to \mathbb{Z}/n\mathbb{Z}$, and

$$[q_*\chi_1, q_*\chi_2, q_*\chi_3]_n = ([\chi_1, \chi_2, \chi_3]_m)^{m/n}.$$

Proof. Since q is a map of rings, we note that q_* commutes with cup products, differential maps, and inflation maps. Thus if η is a global trivialisation unramified outside S and η_v an unramified local trivialisation, then so is $q_*\eta$ and $q_*\eta_v$, since

$$dq_*\eta = q_*d\eta = q_*(\chi_1 \cup \chi_2 \cup \chi_3) = q_*\chi_1 \cup q_*\chi_2 \cup q_*\chi_3.$$

Suppose $c \in H^2(G_v, \mathbb{Z}/m\mathbb{Z})$, we wish to compare $\mathrm{inv}_v\, c$ with $\mathrm{inv}_v(q_*c)$. Note that the map $q : \mu_m \twoheadrightarrow \mu_n$ is given by raising to the power of $\frac{m}{n}$, and thus the map $\iota_* \circ q_* : H^2(G_v, \mathbb{Z}/m\mathbb{Z}) \to H^2(G_v, \mathbb{Z}/n\mathbb{Z}) \to H^2(G_v, \mathbb{Z}/m\mathbb{Z})$ is given by multiplication by $\frac{m}{n}$. Composing with the invariant map gives $\mathrm{inv}_v(q_*c) = \frac{m}{n}\,\mathrm{inv}_v(c)$. And thus

$$\begin{aligned}\mathfrak{d}(q_*\chi_1, q_*\chi_2, q_*\chi_3) &= \sum_{v\in S} \mathrm{inv}_v(q_*(\mathrm{loc}_v\, \eta - \eta_v)) \\ &= \frac{m}{n} \sum_{v\in S} \mathrm{inv}_v(\mathrm{loc}_v\, \eta - \eta_v) \\ &= \frac{m}{n} \mathfrak{d}(\chi_1, \chi_2, \chi_3)\end{aligned}$$

Which implies

$$[q_*\chi_1, q_*\chi_2, q_*\chi_3]_n = ([\chi_1, \chi_2, \chi_3]_m)^{m/n}.$$

□

Bibliography

[AV25] Amina Abdurrahman and Akshay Venkatesh. "Symplectic L-functions and Symplectic Reidemeister Torsion (Mod Squares)". In: *Inventiones mathematicae* 241.3 (Sept. 2025), pp. 717–839. ISSN: 1432-1297. DOI: 10.1007/s00222-025-01349-6 (cit. on p. 22).

[AC23] Eric Ahlqvist and Magnus Carlson. "The Étale Cohomology Ring of the Ring of Integers of a Number Field". In: *Research in Number Theory* 9.3 (Sept. 2023), p. 58. ISSN: 2522-0160, 2363-9555. DOI: 10.1007/s40993-023-00467-5 (cit. on pp. 78, 79).

[AS12] Alexander Altland and Ben Simons. *Condensed Matter Field Theory*. 2. ed., [repr.] Cambridge: Cambridge Univ. Press, 2012. ISBN: 978-0-521-76975-4 (cit. on p. 23).

[Ama14] Fumiya Amano. "On a Certain Nilpotent Extension over $\boldsymbol{Q}$ of Degree 64 and the 4-Th Multiple Residue Symbol". In: *Tohoku Mathematical Journal* 66.4 (Dec. 2014), pp. 501–522. ISSN: 0040-8735, 2186-585X. DOI: 10.2748/tmj/1432229194 (cit. on p. 67).

[AMM18] Fumiya Amano, Yasushi Mizusawa, and Masanori Morishita. "On Mod 3 Triple Milnor Invariants and Triple Cubic Residue Symbols in the Eisenstein Number Field". In: *Research in Number Theory* 4.1 (Feb. 2018), p. 7. ISSN: 2363-9555. DOI: 10.1007/s40993-018-0100-7 (cit. on p. 67).

[BL04] Christina Birkenhake and Herbert Lange. *Complex Abelian Varieties*. Ed. by A. Chenciner, S. S. Chern, B. Eckmann, P. De La Harpe, F. Hirzebruch, N. Hitchin, L. Hörmander, M.-A. Knus, A. Kupiainen, G. Lebeau, M. Ratner, D. Serre, Ya. G. Sinai, N. J. A. Sloane, B. Totaro, A. Vershik, M. Waldschmidt, M. Berger, J. Coates, and S. R. S. Varadhan. Vol. 302. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. ISBN: 978-3-642-05807-3 978-3-662-06307-1. DOI: 10.1007/978-3-662-06307-1 (cit. on p. 27).

[Car+24] Magnus Carlson, Hee-Joong Chung, Dohyeong Kim, Minhyong Kim, Jeehoon Park, and Hwajong Yoo. "Path Integrals and P-Adic L-functions". In: *Bulletin of the London Mathematical Society* 56.6 (2024), pp. 1951–1966. ISSN: 1469-2120. DOI: 10.1112/blms.13036 (cit. on p. 22).

[CK22] Magnus Carlson and Minhyong Kim. "A Note on Abelian Arithmetic BF-theory". In: *Bulletin of the London Mathematical Society* 54.4 (2022), pp. 1299–1307. ISSN: 1469-2120. DOI: 10.1112/blms.12629 (cit. on pp. 22, 56).

[CF67] John William Scott Cassels and Albrecht Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference*. London New York San Diego [etc.]: Academic press, 1967. ISBN: 978-0-12-163251-9 (cit. on p. 46).

[CLL21] Kwokwai Chan, Naichung Conan Leung, and Qin Li. "Quantization of Kähler Manifolds". In: *Journal of Geometry and Physics* 163 (May 2021), p. 104143. ISSN: 0393-0440. DOI: 10.1016/j.geomphys.2021.104143 (cit. on p. 23).

[Che25] Yan Yau Cheng. *A Trace-Path Integral Formula over Function Fields*. Sept. 2025. DOI: 10.48550/arXiv.2509.04540. arXiv: 2509.04540 [math] (cit. on p. 9).

[Chu+19] Hee-Joong Chung, Dohyeong Kim, Minhyong Kim, Georgios Pappas, Jeehoon Park, and Hwajong Yoo. "Abelian Arithmetic Chern–Simons Theory and Arithmetic Linking Numbers". In: *International Mathematics Research Notices* 2019.18 (Sept. 2019), pp. 5674–5702. ISSN: 1073-7928, 1687-0247. DOI: 10.1093/imrn/rnx271 (cit. on pp. 11, 22, 40, 41).

[Chu+20] Hee-Joong Chung, Dohyeong Kim, Minhyong Kim, Jeehoon Park, and Hwajong Yoo. "Arithmetic Chern–Simons Theory II". In: *P-Adic Hodge Theory*. Ed. by Bhargav Bhatt and Martin Olsson. Simons Symposia. Cham: Springer International Publishing, 2020, pp. 81–128. ISBN: 978-3-030-43844-9. DOI: 10.1007/978-3-030-43844-9_3 (cit. on pp. 8, 11, 13, 73, 74).

[Den84] Christopher Deninger. "On Artin-Verdier Duality for Function Fields". In: *Mathematische Zeitschrift* 188.1 (Mar. 1984), pp. 91–100. ISSN: 0025-5874, 1432-1823. DOI: 10.1007/BF01163876 (cit. on pp. 11, 12).

[DS14] Jan Draisma and Ron Shaw. "Some Noteworthy Alternating Trilinear Forms". In: *Journal of Geometry* 105.1 (Apr. 2014), pp. 167–176. ISSN: 1420-8997. DOI: 10.1007/s00022-013-0202-2. arXiv: 1102.4768 [math] (cit. on p. 78).

[Enr+99] Arturo Enríquez, Miguel-C Muñoz-Lecanda, Narciso Román-Roy, and Carles Victoria-Monge. "Mathematical Foundations of Geometric Quantization". In: *Extracta mathematicae, ISSN 0213-8743, Vol. 13, Nº 2, 1998, pags. 135-238* (May 1999) (cit. on p. 23).

[FS18] L.D. Faddeev and A.A. Slavnov. *Gauge Fields: Introduction to Quantum Theory*. 2nd ed. CRC Press, Mar. 2018. ISBN: 978-0-429-49382-9. DOI: 10.1201/9780429493829 (cit. on p. 23).

[GH09] Shamgar Gurevich and Ronny Hadani. "Quantization of Symplectic Vector Spaces over Finite Fields". In: *Journal of Symplectic Geometry* 7.4 (2009), pp. 475–502. ISSN: 1527-5256, 1540-2347. DOI: 10.4310/jsg.2009.v7.n4.a4 (cit. on pp. 22, 26–29, 34).

[HKZ78] K. Haberland, H. Koch, and T. Zink. *Galois Cohomology of Algebraic Number Fields*. Deutscher Verlag der Wissenschaften, 1978. ISBN: 978-0-685-87204-8 (cit. on p. 64).

[Hal13] Brian C. Hall. *Quantum Theory for Mathematicians*. Vol. 267. Graduate Texts in Mathematics. New York, NY: Springer, 2013. ISBN: 978-1-4614-7115-8. DOI: 10.1007/978-1-4614-7116-5 (cit. on pp. 21, 23).

[HKM23] Hikaru Hirano, Junhyeong Kim, and Masanori Morishita. "On Arithmetic Dijkgraaf–Witten Theory". In: *Communications in Number Theory and Physics* 17.1 (2023), pp. 1–61. ISSN: 19314523, 19314531. DOI: 10.4310/CNTP.2023.v17.n1.a1 (cit. on p. 74).

[HP21] Jan Hora and Petr Pudlák. "Classification of 9-Dimensional Trilinear Alternating Forms Over GF(2)". In: *Finite Fields and Their Applications* 70 (Feb. 2021), p. 101788. ISSN: 10715797. DOI: 10.1016/j.ffa.2020.101788 (cit. on p. 78).

[IKZ24] Yuki Ishida, Atsuki Kuramoto, and Dingchuan Zheng. *The Density of Borromean Primes*. Mar. 2024. arXiv: 2403.17957 [math] (cit. on p. 67).

[Kim25] Dohyeong Kim. *Arithmetic Chern–Simons Actions of Massey Type and Triple Symbols*. July 2025 (cit. on pp. 9, 59, 73, 75).

[KM25] Dohyeong Kim and Masanori Morishita. "Triple Symbols in Arithmetic". In: *Research in Number Theory* 11.4 (Dec. 2025), p. 86. ISSN: 2522-0160, 2363-9555. DOI: 10.1007/s40993-025-00648-4 (cit. on pp. 9, 59, 67, 69–73).

[Kim18] Minhyong Kim. "Arithmetic Gauge Theory: A Brief Introduction". In: *Modern Physics Letters A* 33.29 (Sept. 2018), p. 1830012. ISSN: 0217-7323, 1793-6632. DOI: 10.1142/S0217732318300124. arXiv: 1712.07602 [hep-th, physics:math-ph] (cit. on p. 8).

[Kim20] Minhyong Kim. "Arithmetic Chern–Simons Theory I". In: *Galois Covers, Grothendieck-Teichmüller Theory and Dessins d'Enfants*. Ed. by Frank Neumann and Sibylle Schroll. Cham: Springer International Publishing, 2020, pp. 155–180. ISBN: 978-3-030-51795-3 (cit. on p. 11).

[Koc70] H. Koch. *Galoissche Theorie Der P-Erweiterungen*. Galloissche Theorie Der P-Erweiterungen. Deutscher Verlag der Wissenschaften, 1970 (cit. on p. 64).

[Kur26] Atsuki Kuramoto. "On Triple Quadratic Residue Symbols in Real Quadratic Fields". In: *Research in the Mathematical Sciences* 13.1 (Mar. 2026), p. 14. ISSN: 2522-0144, 2197-9847. DOI: 10.1007/s40687-025-00593-9 (cit. on p. 67).

[Lan86] Serge Lang. *Algebraic Number Theory*. Graduate Texts in Mathematics. New York, NY: Springer New York, 1986. ISBN: 978-1-4684-0298-8 978-1-4684-0296-4. DOI: 10.1007/978-1-4684-0296-4 (cit. on p. 36).

[LST20] Michael Lipnowski, Will Sawin, and Jacob Tsimerman. *Cohen-Lenstra Heuristics and Bilinear Pairings in the Presence of Roots of Unity*. July 2020. DOI: 10.48550/arXiv.2007.12533. arXiv: 2007.12533 [math] (cit. on p. 43).

[Maz] Barry Mazur. *Remarks on the Alexander Polynomial* (cit. on p. 21).

[Mil06] J S Milne. *Arithmetic Duality Theorems*. 2. ed. Charleston, SC: Booksurge, 2006. ISBN: 978-1-4196-4274-6 (cit. on pp. 3, 17, 40, 45).

[Mil13] J S Milne. *Lectures on Étale Cohomology*. v2.21. 2013 (cit. on p. 41).

[Mil20] J S Milne. *Class Field Theory*. v4.03. 2020 (cit. on pp. 12, 69).

[Mil57] John Milnor. "Isotopy of Links". In: *Algebraic Geometry and Topology*. Ed. by R. H. Fox, D. C. Spencer, and A. W. Tucker. A Symposium in Honor of Solomon Lefschetz. Princeton University Press, 1957, pp. 280–306. ISBN: 978-0-691-07907-3. JSTOR: j.ctt183pmq2.24 (cit. on pp. 60–62).

[Mor04] Masanori Morishita. "Milnor Invariants and Massey Products for Prime Numbers". In: *Compositio Mathematica* 140.01 (Jan. 2004), pp. 69–83. ISSN: 0010-437X, 1570-5846. DOI: 10.1112/S0010437X03000137 (cit. on pp. 59, 63–65).

[Mor24] Masanori Morishita. *Knots and Primes: An Introduction to Arithmetic Topology*. Universitext. Singapore: Springer Nature, 2024. ISBN: 978-981-99-9254-6. DOI: 10.1007/978-981-99-9255-3 (cit. on pp. 3, 5, 21, 57, 59–61, 63–66).

[Mum70] David Mumford. *Abelian Varieties*. Tata Institute of Fundamental Research, Bombay, 1970. ISBN: 978-0-19-560528-0 (cit. on p. 28).

[Ner11] Yurii A. Neretin. *Lectures on Gaussian Integral Operators and Classical Groups*. Feb. 2011. ISBN: 978-3-03719-080-7. DOI: 10.4171/080 (cit. on p. 48).

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Vol. 323. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer, 2008. ISBN: 978-3-540-37888-4 978-3-540-37889-1. DOI: 10.1007/978-3-540-37889-1 (cit. on pp. 14, 18, 19, 70, 71).

[Och23] Tadashi Ochiai. *Iwasawa Theory and Its Perspective*. Mathematical Surveys and Monographs v. 272. Providence, Rhode Island: American Mathematical Society, 2023. ISBN: 978-1-4704-5672-6 978-1-4704-7325-9 (cit. on p. 7).

[OSZ21] Martin Orr, Alexei N. Skorobogatov, and Yuri G. Zarhin. "On Uniformity Conjectures for Abelian Varieties and K3 Surfaces". In: *American Journal of Mathematics* 143.6 (2021), pp. 1665–1702. ISSN: 1080-6377. DOI: 10.1353/ajm.2021.0043. arXiv: 1809.01440 [math] (cit. on p. 26).

[Réd39] Ladislaus Rédei. "Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I." In: 1939.180 (Jan. 1939), pp. 1–43. ISSN: 1435-5345. DOI: 10.1515/crll.1939.180.1 (cit. on pp. 59, 65).

[Ser79] Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics 67. New York, NY: Springer, 1979. ISBN: 978-1-4757-5673-9. DOI: 10.1007/978-1-4757-5673-9 (cit. on p. 5).

[Wal15] G. E. Wall. *The Semisimple Conjugacy Classes in the Symplectic Groups*. Dec. 2015. DOI: 10.48550/arXiv.1512.04520. arXiv: 1512.04520 [math] (cit. on pp. 34, 35).

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Second Edition. Graduate Texts in Mathematics 83. New York, NY: Springer, 1997. ISBN: 978-1-4612-1934-7. DOI: 10.1007/978-1-4612-1934-7 (cit. on p. 7).

[Wei05] Andre Weil. "A 1940 Letter of André Weil on Analogy in Mathematics". Trans. by Martin H. Krieger. In: *Notices of the American Mathematical Society* 52.1 (2005) (cit. on p. 7).

[Zei06] Eberhard Zeidler. *Quantum Field Theory I: Basics in Mathematics and Physics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006. ISBN: 978-3-540-34762-0 978-3-540-34764-4. DOI: 10.1007/978-3-540-34764-4 (cit. on p. 23).

[Zin11] Jean Zinn-Justin. *Path Integrals in Quantum Mechanics*. repr. Oxford Graduate Texts. Oxford: Univ. Press, 2011. ISBN: 978-0-19-856675-5 (cit. on p. 23).