Al-Farabi Kazakh National University
Faculty Of Mathematics
Mechanics And Mathematics

Diploma Work Entitled

A Weil Conjectures' Exposition With Application To Elliptic Curves

6B05402 - Mathematics

COMPLETED Mohammad Mahdi Jafari
SUPERVISOR Simon Serovajsky

ADMITTED TO DEFENSE:
PROTOCOL No.
Head of department Imanberdiyev K. B.
Norm Controller Auzerkhan G.

Almaty, 2025

Abstract

The presented thesis is an structured exposition of the Weil conjectures and their application to the theory of elliptic curves over $\mathbb{Q}$. The first part of the work is a foundational component focused on the cohomological apparatus necessary for the proofs of the Weil conjectures, and the second part is a novel approach to a problem concerning the Selmer groups, an equivalence class in the first cohomology of the curve, as the arithmetic application of the tools.

The first part is a very brief exposition of the homological machinary used in modern algebraic geometry following the school of Grothendieck, from the framework of categories and topos into abstract theory of schemes and /l/-adic cohomology. These tools are then used for developing a cohomological interpretation of the zeta functions and L-series, through a derivation of the Lefschetz fixed point formula and an outlined proof of the Weil conjectures, besides the Riemann Hypothesis.

The second part is the application of these tools for arithmetic of elliptic curves over rational numbers, specifically for those with an integral 2-torsion point. We compute the exact selmer groups with tools borrowed from /l/-adic cohomology and local reductions to compute the Selmer ranks. This result contributes to open problems regarding the growth of Mordell-Weil ranks and further open problems regarding the Tate-Shafarevich groups.

An outline of the differences and novelties of this work are provided in the fourth chapter, by avoiding use of quadratic twists in the computation of the Selmer ranks, and contributes insights to the structure of Selmer groups in exceptional families.

Keywords: Algebraic geometry, Elliptic curves, Selmer groups, Galois cohomology, finite field arithmetic

Реферат

Бұл дипломдық жұмыс Вейль болжамдарын және олардың $\mathbb{Q}$ санының өрістеріндегі эллиптикалық қисықтар теориясына қолданылуын құрылымдық түрде баяндайды. Жұмыстың бірінші бөлігінде Вейль болжамдарының дәлелдеулеріне қажетті когомологиялық аппараттың іргелі негіздері қарастырылады, ал екінші бөлігінде бірінші когомологиядағы эквиваленттік кластар – Сельмер топтары бойынша арифметикалық есеп жүргізіледі.

Бірінші бөлім – Гротендик мектебінің бағытын ұстана отырып, заманауи алгебралық геометрияда қолданылатын гомологиялық әдістердің қысқаша экспозициясы. Категориялар мен топостар теориясынан бастап схемалар мен l-аддик когомологиясына дейінгі ұғымдар қарастырылады. Бұл аппарат зета-функциялар мен L-қатарларын когомологиялық интерпретациялау үшін қолданылады. Сонымен қатар, Лефшецтің тұрақты нүкте формуласы туындалып, Вейль болжамдарының (Риман гипотезасынан басқа) дәлелдеулері келтіріледі.

Жұмыстың екінші бөлігінде рационал сандар өрісіндегі бүтін 2-торсионды нүктесі бар эллиптикалық қисықтарға арналған арифметикалық есептер жүргізіледі. l-аддик когомология мен жергілікті редукциялар әдістері арқылы Сельмер топтарының нақты өлшемдері есептеледі. Бұл нәтиже Мордэлл–Вейль рангтерінің өсуі және Тейт–Шафаревич топтарының шектеусіздігі мәселелері бойынша ашық сұрақтарға үлес қосады.

Жұмыстың жаңашылдығы төртінші бөлімде көрсетілген, мұнда Сельмер рангтерін есептеуде квадратикалық бұраулар қолданылмайды. Бұл тәсіл ерекше эллиптикалық қисықтар отбасындағы Сельмер топтарының құрылымы жөнінде жаңа түсініктер береді.

Түйін сөздер: алгебралық геометрия, эллиптикалық қисықтар, Сельмер топтары, Галуа когомологиясы, шектеулі өрістер арифметикасы

Реферат

Данная выпускная работа представляет собой структурированное изложение гипотез Вейля и их приложения к теории эллиптических кривых над полем рациональных чисел $\mathbb{Q}$. Первая часть посвящена построению когомологического аппарата, необходимого для доказательства гипотез Вейля, в то время как вторая часть содержит оригинальный подход к проблеме, связанной с группами Сельмера, которые являются классами эквивалентности в первой когомологии кривой.

Первая часть представляет собой краткое изложение гомологических методов современной алгебраической геометрии, развивавшейся в рамках школы Гротендика — от категорий и топосов к абстрактной теории схем и l-адической когомологии. Этот аппарат используется для когомологической интерпретации дзета-функций и L-рядов, включая вывод формулы Лефшеца о неподвижной точке и схематичное доказательство гипотез Вейля (за исключением гипотезы Римана).

Вторая часть применяет эти методы к арифметике эллиптических кривых над Q, в частности для семейства с целой точкой порядка 2. Посредством инструментов l-адической когомологии и локальных редукций вычисляются размеры групп Сельмера. Полученные результаты вносят вклад в открытые вопросы о возможном росте рангов группы Морделла–Вейля и в проблему структуры группы Тейта–Шафаревича.

Отличия и новизна данной работы изложены в четвёртой главе, где вычисления Сельмер-рангов проводятся без применения квадратичных твистов. Это позволяет получить новые представления о структуре групп Сельмера в исключительных семействах эллиптических кривых.

Ключевые слова: алгебраическая геометрия, эллиптические кривые, группы Сельмера, когомология Галуа, арифметика конечных полей

Contents

Introduction

The presented work is an aim to lay the foundations of modern algebraic geometry, and show an application of this given in the fourth chapter. The first part of this work, the first three chapters, are aimed for a reader unfamiliar with modern algebraic geometry. Basics of ideal theory are assumed, and from this we build up the foundation of modern reading of algebraic geometry, that of categorical interpretations of Alexander Grothendieck and his school, to prove the Weil conjectures besides the Riemann Hypothesis. We go through the basics of category theory, homological algebra, scheme theory and cohomology theory to approach this goal, and familiarize the reader with the state of the art algebraic geometry, as is needed for the latter part of this work.

The second part is a manuscript partially sent for publication showcasing what can be done with the explained tools. We work with the arithmetical and geometrical techniques developed within the first three chapters to investigate the arithmetical properties of certain families of elliptic curves, which an open field of many investigations, beginning from the works of Artin on zeta functions and made quite famous by the works of Wiles on the Fermat's Last Theorem. Our work builds upon the existing literature on this topic to shed light on certain objects made to study elliptic curves over rational numbers, and includes a short survey of open problems to be addressed in the future of this work.

The connection of the two parts grows deeper than an application of the techniques through open conjectures such as that of Birch Swinnerton-Dyer and Beilinson-Bloch-Kato. The center of this algebraic and analytic connections are the L-functions and zeta functions associated to varieties, with which the Weil conjectures are concerned; it would be a disservice to the reader thus not to include the ideas of these objects beforehand to get a sense of urgency these problems hold in the field of arithmetic geometry.

The idea of zeta functions stems from the solutions of a set of algebraic equations in a finite field and the problem of counting such solutions. This problem is due Artin. He began the study of extensions in function fields and their arithmetical properties, i.e, the number of rational solutions to intersection of curves. This lead to the study of zeta function associated to the curve defining the extension under consideration. But to see why zeta functions went under consideration, one must go further back.

Dedekind studied number fields which were rationals with finite number of algebraic extensions. The reason for this is that the divisibility of solutions to a polynomial by primes is governed by the behavior of prime numbers under rationals extended with the solution of the polynomial. It was observed that the number vastly differs for various extensions, and many extensions lose basic properties of natural numbers such as unique factorization. What was observed was that the residue of zeta function associated to the field, the function mimicking the Euler product formula over prime numbers used in Riemann zeta function, was directly related to the behavior of the number field associated to the extension. This was the first sign that there had to be a much deeper connection between algebraic properties of a field and the analytic properties of the zeta function. The work of Artin was thus the extension of class field theory to the case of function fields, since for the case of function fields the classical geometric and algebraic topological tools were available.

A factor that necessitates this text over other pieces of literature on this topic is the emphasis on the arithmetic aspects of algebraic geometry; many existing pieces of literature do not take so much time as to even introduce etale or l-adic cohomology theories only to focus on purely geometrical problems such as that of classification of surfaces. Such problems despite their priority for a geometer are of little interest for a text addressing arithmetic as its main issue, and thus this text set its goal of the exposition as the Weil conjectures; this is more inline with much of the developments of algebraic geometry, and so we return to it for this text.

We introduce the Weil conjectures and zeta functions in the first chapter. We set the goal, which is to construct a Weil cohomology theory suitable for study of finite field arithmetic. The chapter is aimed at demonstrating the nature of a cohomology theory and what makes it important for us, and for a geometrical investigation.

In the second chapter all the needed tools are briefly introduced; many topics are crammed into one chapter, as a fast track course to familiarize the reader with the topic and then immediately introduce the l-adic cohomology theory; for brevity, many of the auxiliary topics and long justifications, or highly abstract category theoretic explanations have been omitted, to avoid making the chapter overly long and making this primarily a textbook of algebraic geometry. Each section of the second chapter therefore capsulated as much as a book of [EGA] or [SGA] series, and thus many omissions were necessary. At the end of the chapter we are finished with the introduction of the l-adic cohomology, and are ready to give a proof of the conjectures.

The third chapter is straightforward. We give a proof of the Lefschetz fixed point formula for the Frobenius endomorphism, from which the Weil conjectures all follow. We do not have much to do in the chapter, so it is quite a brief end for the first part of this text.

The fourth chapter constitutes the original contributions of this thesis. Making use of the cohomological and categorical framework developed in the first part, we shift focus to the arithmetic of elliptic curves defined over the rational numbers. We recall basics of elliptic curves, such as the group structrue, the L-function and auxiliary groups, the Selmer groups and Tate-Shafarevich groups, as the central invariants in the study of rational points.

The goal of this chapter is the computation of the Selmer groups within a narrow family of elliptic curves, namely those with a point of order 2 on the origin. We pursue descent techniques informed by l-adic methods and localization of cohomology classes, and implement a reduction strategy for this family of curves. The algorithm is adopted from Goto [7], and is used to explicitly track growth of Selmer ranks for this family.

This analysis not only shows the application of the cohomological methods explained prior, but also lays the groundwork for future investigations into related open problems, such as that of Birch Swinnerton-Dyer and Beilinson-Bloch-Kato. In the body of the chapter, the divergence of methods from those of Klagsbrun and Lemke-Oliver, who derived the same results from different methods, is discussed.

Chapter 1

The Weil Conjectures

In this section, we introduce the Weil conjectures and the strategy taken to resolve them. Firstly, we will need to introduce the zeta function of a variety. This section follows works of [17] and [12]; the latter includes a through review of this topic.

1.1 Zeta Functions

In his 1846 paper, Riemann prove the the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

extends holomorphically to the entire complex plane, and formulated a hypothesis regarding the distribution of zeros of this function. Since the zeta function admits the prime decomposition

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}$$

, its analytical properties encode arithmetical information regarding $\mathbb{Z}$, including the distribution of prime elements.

Following Riemann, Dedekind defines the zeta function of an arbitrary number field K as

$$\zeta_K(s) = \prod_{\mathcal{P}} \frac{1}{1 - N(\mathcal{P})^{-s}}$$

where $N(\mathcal{P})$ denotes the norm of the prime ideal $\mathcal{P}$. This function, again, encodes the arithmetical information regarding the ring of integers in K, and decomposes

into a product of the Riemann zeta function and a similar series.

Example: (Dedekind zeta function) Consider the number field $\mathbb{Q}(i)$ with ring of integers $\mathbb{Z}[i]$. As primes $p \equiv 1 \pmod 4$ are split into two prime ideals, and 2 is is split as $(1+i)(1-i)$, the zeta function for this field becomes

$$\zeta_K(s) = \frac{1}{1-2^{-s}} \cdot \prod_{p\equiv 1} \frac{1}{(1-p^{-s})^2} \prod_{p\equiv 3} \frac{1}{(1-p^{-s})(1+p^{-s})}$$

we can rewrite this using the Dirichlet character χ_4 as

$$\zeta_K(s) = \zeta(s) \cdot \prod_{p} \frac{1}{1-\chi(p)p^{-s}} = \zeta(s)L(\chi_4, s)$$

where $\chi(1) = -1$, $\chi(-1) = 4$, $\chi(n+4) = \chi(n)$

In 1921, Emil Artin develops the theory of zeta functions of quadratic function fields with finite elements $\mathbb{F}_p(t)$ analog to dedekind zeta functions, and proves that it again decomposes as a rational function of p^{-s}. He also formulates the analog of Riemann hypothesis for this context.

Hasse later proves the Riemann hypothesis for the functional field of an elliptic curve, using endomorphism ring of the curve and lifting from finite fields into infinite fields. Following this, Weil proves the Riemann hypothesis for an arbitrary curve over a finite field.

Weil introduces the geometric language in theory of zeta functions, re-founding algebraic geometry in the way; he then develops the Weil conjectures regarding properties of the zeta function. We now define and develop the basics of zeta functions in context of finite type schemes.

Zeta function of a finite type scheme

Let X be an scheme of finite type over $\mathbb{Z}$. We define

$$\zeta(X, s) = \prod_{\mathcal{P}\in X} \frac{1}{1-N(\mathcal{P})^{-s}}$$

where $\mathcal{P}$ refers to closed points in X, and $N(\mathcal{P})$ is the cardinality of its residue field.

For an scheme defined as a disjoint union of subschemes $\{X_i\}$,

$$\zeta(X,s) = \prod \zeta(X_i,s)$$

For a X a $\mathbb{F}_q$ scheme, we have

$$\zeta(X,s) = \exp(\sum_{n=1}^{\infty} |X(\mathbb{F}_q^n)| \frac{q^{-ns}}{n})$$

Example: for the affine line $\mathbb{A}^1_X$ and projective line $\mathbb{P}^1_X$ on X, we have

$$\zeta(\mathbb{A}^1_{\mathbb{F}_q},s) = \frac{1}{1-q^{1-s}}, \quad \zeta(\mathbb{A}^1_{\mathbb{F}_q},s) = \frac{1}{(1-q^{1-s})(1-q^{-s})}.$$

We prove this by the observation

$$\zeta(\mathbb{A}^1_{\mathbb{F}_q},s) = \exp(\sum_{n=1}^{\infty} |\mathbb{A}^1_{\mathbb{F}_q^n}| \frac{q^{-ns}}{n}) = \exp(\sum_{n=1}^{\infty} \frac{q^{n-ns}}{n}) = \exp(-\log(1-q^{1-s}))$$

and

$$\zeta(\mathbb{P}^1_{\mathbb{F}_q},s) = \zeta(\mathbb{F}_q,s)\zeta(\mathbb{A}^1_{\mathbb{F}_q},s) = \frac{1}{(1-q^{1-s})(1-q^{-s})}.$$

By rewriting the defined zeta function as a function of q^{-s} rather than s, we get the *Hasse-Weil zeta function*

$$Z(X,q^{-s}) = \zeta(X,s).$$

Example: We can rewrite the previous examples as

$$Z(\mathbb{A}^1_{\mathbb{F}_q},t) = \frac{1}{1-t}$$

and

$$Z(\mathbb{P}^1_{\mathbb{F}_q},t) = \frac{1}{(1-t)(1-qt)}.$$

We can now state the first Weil conjecture:

1.2 Statement of the Conjectures

We can now state the Weil Conjectures. Here, we let X denote an n-dimensional, non-singular and projective variety of genus g.

Rationality: Rewriting $\zeta(X,s)$ as $Z(X,T)$ for $T = q^{-s}$, the zeta function is a rational function in T. Further, it can be factorized as

$$Z(X,T) = \prod_{i=0}^{2n} P_i(T)^{(-1)^{i+1}}$$

where each $P_i(T)$ is a polynomial with integer coefficients.

Functional equation: The zeta function has the following functional equation

$$Z(X, q^{-n}T^{-1}) = q^{n\chi/2}T^{\chi}Z(X,T)$$

where $\chi = 2-2g$ is the Euler characteristic of the X.

Betti Numbers: The degree of each polynomial $P_i(n)$ is the i-th Betti number, which is the dimensions of the i-th homology group.

Riemann Hypothesis: The zeros of $P_i(T)$ for all i have the absolute value $q^{i/2}$.

We note that all these properties are inferred from the Riemann zeta function; its rationality follows the Euler product formulation, the functional equation follows Riemann's work, the Betti numbers follows the Affine line having the same topological structure as a point and the Riemann Hypothesis is trivial over finite fields, though it remains open in the global case.

1.3 Weil Cohomology

The approach taken in this work for the proof of these conjectures is the use of Weil cohomology meta-conjecture, titled such by Alexander Grothendieck. This approach uses rather technical machinery from category theory, to which a chapter is thus dedicated.

We now describe the concept of a Weil cohomology; note that since it is not a definition and simply a description, more than one such object may exist. This is indeed the case and we list the existing Weil cohomology theories at the end of this section, along with reasoning for their usage or refusal here.

The Weil cohomology is a functor $H^{\cdot} : V(k)^o \to Vec^*_K$ of smooth projective varieties over the field k to graded vector spaces over field K of characteristic zero. Given X of dimension n, it satisfies the following axioms:

1. For all $X \in V(k)$, $H^i(X)$ is a finite dimensional vector space over K, and if $i \notin [0, 2n]$, $H^i(X) = 0$

2. $H^0(Spec(k)) = K$. The spectrum of a ring is defined in the chapter Schemes.

3. $dim(H^2(\mathbb{P}^1)) = 1$; this space is denoted as $K(-1)$.

4. For varieties X, Y, we have the additive formula

$$H^*(X \sqcup Y) = H^*(X) \oplus H^*(Y)$$

5. For varieties X, Y, we have the following map

$$\mathscr{k}_{X,Y} : H^*(X) \otimes H^*(Y) \to H^*(X \times Y)$$

   which is a natural isomorphism; further, it has graded commutativity such that for $x \in H^i(X), y \in H^j(Y)$, we have $x \otimes y = (-1)^{ij} y \otimes x$. We call this isomorphism the *Künneth map*.

6. There exists a map Tr_X inducing the isomorphism

$$Tr_X : H^{2n}(X) \to K(-n) := K(-1)^{\otimes n}$$

   such that $Tr_{X \times Y} = Tr_X \otimes Tr_Y$ which coupled with the Künneth formula gives the sequence of morphisms

$$H^i(X) \otimes H^{2n-i}(X) \to H^{2n}(X \times X) \to H^{2n}(X) \to K(-n)$$

   We call this the Poincarè duality.

7. For subvarieties of dimension $n - i$ modulo rational equivalence denoted as $CH^i(X)$, we have a homomorphism

$$cl^i_X : CH^i(X) \to H^{2i}(X)(i) := Hom(K(-i), H^{2i}(X))$$

which is compatible with the Künneth map as

$$\kappa_{X\times Y}(cl^i_X(\alpha)\otimes cl^j_Y(\beta)) = cl^{i+j}_{X\times Y}(\alpha\times\beta)$$

.

We can define the cup product as follows:

$$\smile: H^i(X)\times H^j(X)\to H^{i+j}(X)$$

$$a\cup b\in H^{i+j}(X)$$

to turn the Weil cohomology groups into a ring.

1.4 Existing Weil Cohomology theories

In principle, there exist four different Weil cohomology theories by the axioms given above. In this section we briefly discuss why only one is adopted for this work.

Singular cohomology, also known as Betti cohomology from which Betti numbers take name, is the earliest such theory. It is defined over complex manifolds and topological spaces, and provides a cohomology theory via the complex analytic space. This is the weakness of this theory as it fundamentally relies on the complex analytic properties of the underlying space and has no extension for an space defined over an arbitrary field, like the fields of positive characteristic needed for the Weil conjectures; it is thus inapplicable here.

De Rham cohomology is next such theory; a generalization of singular cohomology, it uses Kähler differentials instead of complex ones, and thus for all fields of charactaristic zero. Over the complex numbers it agrees with the singular cohomology, a celebrated theorem of de Rham, but it still fails to work with positive characteristics, at least to be compatible with the Weil's conjectures. We need to make use of certain finite field endomorphisms for the zeta functions, which we cannot use in fields of characteristic zero.

Two Weil cohomologies remain, both valid for the Weil conjectures; crystalline cohomology, and l-adic etale cohomology. In this work we focus on the latter, developed mainly by Grothendieck, and used in the first complete proof of the

Weil conjectures. This method uses sophisticated methods of category theory now crucial for studying algebraic geometry, to successfully unify existing ideas of field theory – Galois theory and the older ideal theory – within a geometric framework. This arithmetic structure allows up to work within finite fields, and this is the main difference with the prior theories, with respect to the Weil conjectures. The Galois theoretic nature of this method also allows future interpretations and works within the field of algebraic geometry.

Crystalline cohomology, which is a p-adic geometrical method developed alongside etale cohomology, though took its final form much later, is a p-adic counterpart to the de Rham cohomology. The earliest proof of the first Weil conjecture, the rationality of zeta function by Dwork, makes use of this method in its infancy. A complete form of this theory and a full proof of the Weil conjectures by this approach did not take form until much later works of Kedlaya however. This approach is a more analytical approach to the problems, and is less aligned with our algebraic disposition in this work. For this reason we have not pursued this method here.

Chapter 2

Categories and Homological Algebra

In this chapter we shall introduce the basics of category theory. We will begin with the definition of categories and basic operation within categories, then move on to an important class of categories generalizing the notion of Abelian groups, namely the Abelian categories. Finally, we will put forward basic tools from homological algebra, namely the idea of sequences.

This chapter loosely follows the ideas of [8] books 1 and 3, [10], and [9] book 4.

2.1 Categories and Functors

Definition: A *category* C consists of two parts; Objects, denoted $Ob(C)$, and morphisms between them, $Hom_C(\cdot,\cdot)$.

Take the category of sets for example. The objects are the sets, and for $A, B \in \mathscr{Sets}$, $Hom(A,B)$ consists of any mapping of one set to the other. Note here that $Ob(\mathscr{Sets})$ is not a set, but a larger object, namely a class.

Other examples include $\mathscr{Rings}$, the category of rings, where $Hom(A,B)$ consists of ring homomorphisms. Similarly, we have category of $\mathscr{Ab}$ of Abelian groups, and $\mathscr{Mod}(A)$ of modules over a ring. The $Hom(\cdot,\cdot)$ operator in each category is again morphisms retaining the category property.

For a category C, one can construct an *opposite category* C^o by taking as $Ob(C^o)$ the objects in C and as morphisms of two objects A, B, $Hom_{C^o}(B,A) =$

$Hom_C(A,B)$. Similarly, a *product category* of C, D can be constructed with objects and Hom operator as Cartesian product of those of C, D.

Definition: A morphism $f : B \to C$ is called a *monomorphism* if for any pair $e_1, e_2 \in Hom(A,B)$, $fe_1 = fe_2$ implies $e_1 = e_2$. Similarly, an *epimorphism* is a morphism $f : B \to C$ such that for any pair $e_1, e_2 \in Hom(A,B)$, $e_1 f = e_2 f$ implies $e_1 = e_2$.

In a category C, one might find an *initial object* $C_{initial}$ such that $Hom(C_{initial}, \cdot)$ consists of a unique morphism. Conversely, a *final object* is an object such that $Hom(\cdot, C_{final})$ consists of a unique morphism. An object which is both initial and final is called a *zero object*.

For two objects of a category A, B, one can construct a *product* $A \times B$ such that there exist unique maps $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$, and for any object X with morphisms $f_1 \in Hom(X,A)$ and $f_2 \in Hom(X,B)$, there exists a unique morphism in $f \in Hom(X, A \times B)$ where $\pi_A \circ f = f_1$ and $\pi_B \circ f = f_2$.

The previous definitions use only Hom operator and therefore identify objects only in relation to other objects in the category. This is an important tool in category theory, as for example, since any two objects that satisfy the axioms as initial, final or product, would by definition have unique morphisms into one another, and hence are isomorphic. Such properties are called *universal properties*.

Example: For $f \in Hom(A,B)$, take the universal object K such that for any $i \in Hom(K,A)$, the composition $f \circ i$ has the image zero, the zero morphism. This object is called the *Kernel* of the morphism f, denoted $Ker(f)$. The opposite object *cokernel* $coKer(f)$ is the universal object C such that for $f : A \to B$ and $j : B \to C$, $j \circ f$ is the zero morphism.

Definition: (Functors) A *Functor* F between two categories C and C' is a map between the objects $Ob(C)$ and $Ob(C')$, and for a morphism $f \in H_C(A,B)$ a functor has the map $F(m) : F(A') \to F(B')$ in $Hom_{C'}(A', B')$. Functors respect the identity and compositions; a *covariant* functor maps compositions as $F(f_1 \circ f_2) = F(f_1) \circ F(f_2)$, while a *contravariant* functor maps them as $F(f_1 \circ f_2) = F(f_2) \circ F(f_1)$.

Here, we remark that a contravariant functor is a covariant functor from the opposite category.

Definition: (Representable Functor) A covariant functor $F : C \to \mathcal{Ens}$ is called *representable* is it is isomorphic to $Hom(A, \cdot)$ for some $A \in C$. A con-

travariant functor $h : C^O \to \mathscr{E}ns$ (a presheaf) is called representable if it is naturally isomorphic to $Hom(\cdot, A)$ for some $A \in C$. For each object in a category we can the representation $h(x)$ such that $h(x)(y) = Hom(y, x)$.

2.2 Limits and Colimits

Definition: (Limits and Colimits) For a category C and a functor $F : J \to C$, where category J consists of objects j_i, the *limit* is the universal object L that can be mapped to all objects $F(j_i)$. Reversing the arrows $F : J \to C^o$ gives us the *colimit*.

While this definition does not seem intuitive, we try to motivate it by a set of examples:

Example: (Product) Consider a category of two object and no morphisms between the two. Mapping $F(j_1) = A$ and $F(j_2) = B$, the limit is the product $A \times B$. Note that for larger J, we get larger products which are still universal.

Example: (inverse limit) Take for category J the category of infinite objects $j_i, i \in \mathbb{N}_0$, such that $Hom(j_m, j_n)$ is empty unless $m = n+1$. The limit L here is called the inverse limit. For example, in category of rings, taking $F(j_i) = \mathbb{Z}/(p^i)$ we get the limit $\mathbb{Z}_p$, the p-adic integers.

2.3 Additive and Abelian Categories

In what follows, we will introduce the axioms of additive and Abelian categories. We will keep in mind as examples the category Ab and $\mathscr{M}od_A$, Abelian groups and modules over the ring A.

Definition: An *additive category* is a category satisfying the following:

- **(Ad.1)**: The set $Hom(A, B)$ has the structure of an Abelian group, such that it distributes over addition, e.g, for $f, g, h \in Hom(A, B)$, $f(a) + g(a) = (f + g)(a)$ and $h \circ (f + g) = h \circ f + h \circ g$.
- **(Ad.2)**: The category has a zero object.
- **(Ad.3)**: The product of any finite number of object exists within the same category.

We define *Abelian categories* using two additional axioms:

- **(Ab.1)**: The kernel and cokernel of any morphism exist.
- **(Ab.2)**: For any morphism f, $im(f) = ker(coker(f))$. [1]

From this, follows that every bijection is an isomorphism. We now define sequences and exactness of pairs of morphisms:

We can similarly define additive functors by the structure of morphism $Hom(A, B) \to Hom(F(A), F(B))$, and preservation of kernels, cokernels and zero objects.

Infinite sums and products

We now introduce some additional Axioms in order of strength, for existence of infinite sums and products:

- (Ab.3) Direct sum of any family (A_i) (indexed by the set I) exists within the category. (Existence of sup)
- (Ab.4) Axiom (Ab.3) is satisfied, and monomorphisms are preserved as such under finite sums.
- (Ab.5) Axiom (Ab.3) is satisfied, and for the indexed family above we have $(\sum_{i\in I} A_i) \cap B = \sum_{i\in I}(A_i \cap B)$.
- (Ab.6) Axiom (Ab.3) holds for any $A \in C$, and any family $(B^j)_{j\in J}$ of increasing directed families of $B^i = (B^j_i)_{i\in I}$ of subobjects $B^j \in A$, we have:

$$\bigcap_{j\in J}\left(\sum_{i\in I_j} B^i_j\right) = \sum_{(i_j)\in\prod I_j}\left(\bigcap_{j\in J} B^i_{i_j}\right)$$

We do not use (Ab.6), but it suffices to note that the category $\mathscr{Ab}$ satisfies all six axioms, and so does the category of modules over a unital ring. We call Abelian categories those which satisfy (Ab.1) and (Ab.2), AB3 those who satisfy (Ab.3) as well, and AB5 those satisfying 4th and 5th axioms.

[1] Toh § 1.4] states this as every morphism of $Coim(u) \to Im(u)$ being an Isomorphism. Vakil [21] states this as every epimorphism being the cokernel of a kernel, and every monomorphism being the kernel of a cokernel. The conditions are equivalent.

We now define an important subobject class of categories.

Definition: A *generator family* in a category C is a family of objects $(U_i)_{i\in I}$ such that for two distinct objects $A, B \in C$ and two morphisms $f, g : A \to B$ and $h : U_i \to A$, we have $f \circ h \neq g \circ h$. Equivalently, we can say that if U is the direct sum of $(U_i)_{i\in I}$, called *a generator*, any object $A \in C$ is isomorphic to a quotient of the a direct sum of objects all identical to U.

We see that in a AB3 category, existence of a family of generators ensures the existence of a generator, as direct sums always exist. An AB5 category which has a generator has the special name, *Grothendieck category*. Later we will see that every such category is a quotient of a $Mod(A)$ category.

Example: Consider in $\mathscr{Ab}$ the group $\mathbb{Z}$. Since for $f, g \in Hom(A, B)$ there exists $f(x) \neq g(x)$ for some $x \in A$, the map $n \to n \cdot x$ in $Hom(\mathbb{Z}, A)$ suffices to show that $\mathbb{Z}$ is a generator.

2.4 Homological algebra in Abelian categories

We now consider exact sequences and certain functorial properties which are crucial in the next steps of our work.

Definition: (Exactness) We define an *exact* pair for a pair of consecutive morphisms u and v if for the sequence

$$A \xrightarrow{u} B \xrightarrow{v} C$$

if $Ker(v) = Im(u)$. In a category with a zero object, a map

$$0 \longrightarrow A' \xrightarrow{f} A \xrightarrow{g} A'' \longrightarrow 0$$

is called a *short exact sequence* if the map f is a monomorphism, and the map g is an epimorphism. Further, a functor $\mathscr{F}$ is called *left (resp. right) exact* if it $\mathscr{F}(f)$ (resp. $\mathscr{F}(g)$) is a monomorphism (resp. epimorphism).

We now present two important examples of such functors:

Example: (Hom(A, ·)) In an Abelian category $\mathbf{C}$, the $Hom(A, \cdot) : \mathbf{C} \times \mathbf{C} \to \mathscr{Ab}$ is *left-exact*; in other words, short exact sequences $0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$ in $\mathbf{C}$ are mapped to $0 \longrightarrow Hom(A, B') \longrightarrow Hom(A, B) \longrightarrow Hom(A, B'')$ in $\mathscr{Ab}$. The same property holds for $Hom(\cdot, B)$, but the groups $Hom(A, B)$ and $Hom(B, A)$

may differ.

Example: (Tensor Product) In the category $\mathscr{M}\text{-}\mathscr{o}\text{-}\mathscr{d}_R$, the tensor product functor $M \otimes \cdot$ is a *right-exact* functor; in other words, the short exact sequence of R modules $0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$ in $\mathscr{M}\text{-}\mathscr{o}\text{-}\mathscr{d}_R$ is mapped to $M \otimes B' \longrightarrow M \otimes B \longrightarrow M \otimes B'' \longrightarrow 0$ in the same category. Note that since $M \otimes A \cong A \otimes M$ for all R modules A, M, this relationship is true for $\cdot \otimes M$ as well.

We now present two important class of objects, namely, injective and projectives. These objects and the associated resolutions become crucial in our setup for understanding cohomological invariants, which can be thought of as the goal of homological algebra.

Definition: (Injective and Projective objects) For objects I, M, N, P in a category $\mathbf{C}$ with a zero object, we call:

- I an *injective object* if for $\varphi \in Hom(M,N), \psi \in Hom(M,I)$ where φ is an epimorphism, there exists $\theta \in Hom(N,I)$ such that $\theta \circ \varphi = \psi$ for all M, N.

- P a *projective object* if for $\varphi^o \in Hom(N,M), \psi^o \in Hom(P,M)$ where ψ^o is a monomorphism, there exists $\theta^0 \in Hom(P,N)$ such that $\theta^o \circ \varphi^o = \psi^o$ for all M, N

We now define projective and injective *resolutions*. Given an object A, an injective resolution is the exact sequence

$$0 \longrightarrow A \longrightarrow I^0 d \longrightarrow I^1 \xrightarrow{d} \dots$$

where I_n is a sequence of injective objects. Similarly, we define a projective resolution as

$$\cdots \xrightarrow{d} P_1 \xrightarrow{d} P_0 \longrightarrow A \longrightarrow 0$$

With P_n a sequence of Projective objects and d surjective.

Remark: For a projective object P, the functor $Hom(P, \cdot)$ is exact; similarly, for an injective object I the functor $Hom(\cdot, I)$ is exact.

If the sequence of projective modules terminates after P_n, i.e, $P_{n+1} = 0$, A has *projective dimension n*. Injective dimension is defined similarly.

Definition: An additive functor $F : C \to C'$ is *effaceable* if for each $A \in C$, there exists a monomorphism $u : A \to M$ for some M such that $F(u) = 0$. Similarly, an additive functor is *coeffaceable* if for some epimorphism $u : P \to A$, $F(u) = 0$.

In an Abelian category C and additive category C', consider two (not necessarily finite) integers a, b with a gap over one. We denote by a *δ-functor* a covariant functor from C to C' in degree $a < i < b$, a system $T = (T^i)$ of additive covariant functors from C to C'; in addition, we take the following morphism

$$\partial : T^i(A'') \longrightarrow T^{i+1}(A')$$

for any exact sequence $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$. This gives us an associated sequence

$$\cdots \longrightarrow T^i(A') \longrightarrow T^i(A) \longrightarrow T^i(A'') \xrightarrow{\partial} T^{i+1}(A') \longrightarrow \ldots$$

which is a *complex*, that is, product of two consecutive morphisms is zero.

For a homomorphism $A \to B$ preserving the exact sequence,the functors T^i and ∂ naturally extend to B.

For the opposite categories of C^o and C'^o, the ∂-functor becomes the ∂^*-functor.

Now assume C' an Abelian category; then image of exact sequence above is exact. A *cohomological* (resp. *homological*) functor is an exact ∂-functor (resp. ∂^*-functor), defined for all degrees.

We will now present an example for each a cohomology and a homology functor, associated to the left-exact functor $Hom(A, \cdot)$ and right-exact $M \otimes \cdot$ defined above. These examples turn out to be general enough to support our work in definition of any (co)homological theory used in the body of this text.

Definition: (Derived functors) We associate to a left (resp. right) exact functor $\mathcal{F}(A)$ a right (resp. left) derivation $R^i\mathcal{F}(A)$ (resp. $L_i\mathcal{F}(A)$) to continue the exact sequences such that the map $\mathcal{F}(A'') \to R^1\mathcal{F}(A')$ is a monomorphism (resp. the map $L_1\mathcal{F}(A'') \to \mathcal{F}(A')$ is an epimorphism).

Example: (Hom and Ext) As seen above, the functor $Hom(\cdot, B)$ is left-exact. We associate to it a right derived functor $Ext^i(\cdot, B)$ such that the sequence $0 \longrightarrow Hom(A', B) \longrightarrow Hom(A, B) \longrightarrow Hom(A'', B) \longrightarrow Ext_1(A', B) \longrightarrow \ldots$ is exact. Now for the object A in this sequence we take the projective resolution $\cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$ and associate to it the sequence $0 \longrightarrow Hom(P_0, B) \longrightarrow Hom(P_1, B) \longrightarrow Hom(P_2, B) \longrightarrow \ldots$ Ext^i is defined as

the ith cohomology of this sequence

$$Ext^i(A,B) = H^i(A,B) = \frac{Ker(Hom(P_i,B) \to Hom(P_{i+1},B))}{Im(Hom(P_{i-1},B) \to Hom(P_i,B))}.$$

Alternatively, we can associate to B the injective resolution

$$0 \longrightarrow B \longrightarrow I_0 \longrightarrow I_1 \longrightarrow \dots$$

And the associated sequence

$$0 \longrightarrow Hom(A,I_0) \longrightarrow Hom(A,I_1) \longrightarrow Hom(A,I_2) \longrightarrow \dots$$

And take the ith cohomology

$$Ext^i(A,B) = H^i(A,B) = \frac{Ker(Hom(A,I_i) \to Hom(A,I_{i+1}))}{Im(Hom(A,I_{i-1}) \to Hom(A,I_i))}.$$

Example: (tensor products and Tor***)*** We define the operator $Tor_i(M,A)$ as the left derived functor of the tensor product $M \otimes \cdot$ such that the sequence

$$\cdots \longrightarrow Tor_1(M,A'') \longrightarrow M \otimes A' \longrightarrow M \otimes A \longrightarrow M \otimes A'' \longrightarrow 0$$

is exact, that is, the arrows are epimorphisms. Similar to the construction above, we can take a projective resolution of $A \cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$ and the associated chain complex $\cdots \longrightarrow M \otimes P_n \longrightarrow \cdots \longrightarrow M \otimes P_1 \longrightarrow M \otimes P_0 \longrightarrow 0$ to get the ith homology classes

$$Tor_i(M,A) = H_i(M,A) = \frac{Ker(M \otimes P_{i-1} \to M \otimes P_i)}{Im(M \otimes P_i \to M \otimes P_{i+1})}.$$

Note that for A, M modules over a commutative ring R, we have $Tor_i(A,M) \cong Tor_i(M,A)$.

2.5 Sheaves and Schemes

We now define sheaves and schemes. The motivation for this unfolds in two steps; Firstly, we would like a topological approach to ring theory; Second, we would

like a categorical approach to topology. This two-fold aims will be necessary for the introduction of etale cohomology, which is the main aim of this chapter.

Sheaves

Here, we first define presheaves as a way of assigning data to each open cover of a topological space. We then restrict our attention to a certain class which preserves local data, and agrees on the overlapping covers, as sheaves.

Definition: (Presheaf) For a topological space X, a *presheaf* of sets contravariant functor $\mathscr{F} : X \to \mathscr{E}ns$ such that:

- For any open cover U of X, there exists a set $\mathscr{F}(U)$ called the section of $\mathscr{F}$ over U.
- There exists a map $res_V^U : \mathscr{F}(U) \to \mathscr{F}(V)$ called the *restriction map*, restricting sheaf from an open cover to an open subcover. In particular, res_U^U amounts to the identity map.

Presheaves of groups or modules can be defined similarly. We now define sheaves by restriction:

Definition: (Sheaf) A *sheaf* is a presheaf with the additional conditions:

- For a covering $\{U_i\}$ of the open cover U and two sections $s, t \in \mathscr{F}(U)$, if $s|_{U_i} = t|_{U_i}$ for all i, then $s = t$.
- For a covering $\{U_i\}$, if two sections agree on all overlaps of the domain, then there exists a section *gluing* the two together, such that its restriction to each cover agrees with the local sections. Following the previous axiom, the gluing is unique.

We now present examples of presheaves and sheaves:

Example: (Constant sheaf) For a topological space X consider the presheaf assigning a set C to all open covers; this is the constant presheaf. Now, to satisfy the sheaf axioms, we modify this presheaf to assign empty set to the empty cover, and multiple copies of C to non-intersecting covers, such that $\mathscr{F}(U) = C^{\pi_0(U)}$.

Example: The operators $L^p(\cdot)$ or $C^n(\cdot)$ assigning measurable or n-continuus function to each open cover of $\mathbb{R}$ are examples of sheaves, this time of modules, as addition and multiplication by real numbers are valid actions in both spaces.

Affine and Projective Schemes

To a ring A with prime ideals p_k, we assign a topology in which open sets are complement of prime ideals. By $V(f)$ we shall mean a set of prime ideals, and by $D(f)$ its complement. We denote this topological space $Spec(A)$

1. $\emptyset, A \in V$ since $V(0) = Spec(A), V(1) = \emptyset$
2. $E \subset E'$ means $V(E') \subset V(E)$, hence $V(\cup E_i) = \cap V(E_i)$
3. $V(EE') = V(E) \cup V(E')$

And therefore, this space is in fact a valid topology. We shall refer to this topology as the *Zariski topology*.

For a ring A, and the topological space $X = Spec(A)$, consider the sheaf O_X which to an open set assigns rational functions of the ring, e.g $f/g,\ f, g \in A$, such that for an open set $U \in X$, the set $\mathscr{F}(U)$ does not vanish. We call this the structure sheaf.

Example: Consider the topological space $X = \mathbb{C}[x]$; the structure ring O_X is the sheaf assigning to each open cover, non-singular functions on the same cover.

2.6 Sites and Topos

We now provide the definitions for Grothendieck topologies and topoi. We begin this section by introduction of universes, which we do not make use of elsewhere. The only problem requiring us to do this is the theoretical incompatibility of usual set theoretical conception of cardinalities with the notion of topos, as the topos grows larger than any cardinality within the ZFC.

Definitions: (Universe) a *universe* is a set such that

- **(U.1)** For $x \in \mathscr{U}$ and $y \in x$, $y \in \mathscr{U}$
- **(U.2)** For $x, y \in \mathscr{U}$, $\{x, y\} \in \mathscr{U}$
- **(U.3)** For $x \in \mathscr{U}$, $P(x) \in \mathscr{U}$
- **(U.4)** Union of elements x_i indexed by $I \in \mathscr{U}$ is an element of $\mathscr{U}$

Note that since the power set of each element is an element of $\mathcal{U}$, the cardinality of $\mathcal{U}$ is higher than all its members; in particular, the relation $\mathcal{U} \in \mathcal{U}$ cannot be verified.

We can define categories for usual categories, such as sets, topological spaces and Abelian groups inside a universe $\mathcal{U}$ denoted as $\mathcal{U}_{Ens}, \mathcal{U}_{Ab}$, etc.

We call an object $\mathcal{U}$ small if it is isomorphic to an element of $\mathcal{U}$. We thus use words like small groups, small categories, etc.

Definition: (Small category) A category C is a $\mathcal{U}_{CAT}$ if for all $x, y \in Ob(C)$, The set $Hom(x, y)$ is $\mathcal{U}$ small. It is small if $Ob(C)$ is fully inside $\mathcal{U}$.

The (Pre)sheaf of sets on a category C within a universe $\mathcal{U}$ is the category of contravariant functors for C with values in $\mathcal{U}_{Ens}$. The category of preshaeves of sets for a category C, $\hat{C}_{\mathcal{U}}$, is a $\mathcal{U}_{CAT}$ is C is small. this does not necessarily hold if C is itself a $\mathcal{U}_{CAT}$.

We now define Sieves.

Definition: (Sieve) For an object $A \in C$, a *Sieve on A* S is a set such that for any $f : B \to A \in S$ and all morphisms $g : B' \to B$, the composition $f \circ g$ is in S.

Example: The minimal sieve on A $\{i_A\}$ of only the identity, and the maximal sieve on A of all morphisms $Hom(\cdot, A)$ are both valid Sieves. Clearly, any sieve on A lies somewhere between the two. The sieves on an object form a set.

Definition: (Base change) A base change of a sieve from S on A to $S \times_A B$ to $B \in Ob(C)$ is the sieve on B defined by the composition of each element in S with a morphism $f : B \to A$.

Definition: (Topology) A topology on a category C assigns to each $A, A' \in C$ a set of sieves $J(A), J(A')$ such that:

1. The maximal sieve h_A of each objects belongs to $J(A)$

2. **Stability under base change** For any morphism $f : A \to A'$ and elements $S \in J(A')$, the base change $S' \times_{A'} A$ is an element of $J(A)$.

3. **Local Character** If for every map $f : A \to A'$ the base change by f of S is an element of $J(A)$, then S is an element of $J(A')$.

We note the two conditions here:

1. For $S, S' \in J(A)$, $S \cap S' \in J(A)$

2. If $S \in J(A)$, $S \subset S'$, $S' \in J(A)$.

Definition: (Topos) In a universe U, a U-topos (or a Topos) E is a site (e.g, category with grothendieck topology) which is isomorphic to $\hat{C}$ category of sheaf of sets for $C \in U$.

A topos E is a U_{CAT} satisfying:

1. Finite projective limits are representable
2. Direct sums indexed by an element of U are representable
3. Equivalence relations in E are universally effective
4. E admits a generator family indexed by an element of U.

Theorem: (Giraud) The following are equivalent for a U_{CAT} E:

1. It is a U topos (from the definition above)
2. E satisfies 1-4 above
3. The U sheaf on E with canonical topology is representable, and E has an small family of generators
4. There exists a category $C \in U$ and a fully faithful functor $i : E \to \hat{C}$ of U presheaves on C admitting a left exact left adjoint.
5. There exists a site $C \in U$ such that projective limits are representable in C and the topology on C is less fine than the canonical topology, such that E is equivalent to the category $\hat{C}$ of \$U\$-sheaves of sets on C

Two topoi E, E' are equivalent if there exists a functor f such that it commutes with inductive limits, admits a right adjoint and is continuous (e.g, preserves limits)

Example: (Topos associated to a topological space) Take X an small topological space and τ_X the category of coverings on X with the canonical topology. Consider $Top(X)$ the topos associated to this space; it is the category of sheaves of sets on the space X, and is equivalent to the etale space (the space of all continuous morphisms into) X.

2.7 Etale and *l*-adic Cohomology

Consider two rings A, B and a ring homomorphism $f : A \to B$. We call this homomorphism *flat* if For an A module M, the functor $M \to M \otimes_A B$ is exact. This condition is equivalent to B being a free A algebra. In such case, the morphism of Schemes $Spec(B) \to Spec(A)$ is also said to be flat. Similarly, the morphism is unramified if it is a finite and separable ring extension. A finitely presented flat and unramified morphism is called an etale morphism.

for two schemes X, Y and two affine schemes $Spec(A), Spec(A[\epsilon]/(\epsilon^2))$ and maps $f : X \to Y$, $h : Spec(A[\epsilon]/(\epsilon^2)) \to Spec(A)$, $\varphi : Spec(A[\epsilon]/(\epsilon^2)) \to X$, $\varphi' : Spec(B) \to Y$, the induced map $g : Spec(A) \to X$:

1. exists: f is smooth
2. is unique: f is unique
3. exists and is unique: f is etale.

For an scheme X, we define the etale site X_{et} as the category of Schemes U with etale morphisms to X, and we define a covering a family of etale morphisms $\{U_i \to U\}$ such that each $\{U_i \to U\}$ are jointly surjective and etale. We refer to the set of covers of U as $Cov(U)$. A sheaf on the etale site is a functor $F : X_{et}^o \to Set$ such that for $Cov(U)$ the diagram

$$F(U) \longrightarrow \prod F(U_i) \rightrightarrows F(U_i \times_U U_j)$$

is an equalizer. We note that the etale site X_{et} is naturally the topos associated to the scheme X.

We recall the definition of fundamental groups $\pi_1(X)$. A fundamental group is the group classifying the covering spaces of X. The finite covering spaces are thus classified with the profinite completion of the fundamental group.

Theorem: (Riemann's Existence) Any etale morphism is a finite-to-one covering space, and conversely every finite-to-one covering space arises this way, from a unique etale cover.

The construction of the etale fundamental group of an scheme X thus follows the definition

$$\pi_1^{et}(X) = \lim_{etale\ Y \to X} Aut_X(Y).$$

Consider a normal scheme $X = \cap SpecR_i$. By $K(X)$ we denote the field of fractions of X, which given R_i are normal, is independent of i. Let L be a finite extension of $K(X)$ and $\tilde{R}_i$ the integral closure of R_i in L. The maximal unramified extension is defined as

$$K(X)_{unr} = \bigcup L | X_L \to X \text{ is etale.}$$

The fundamental etale group is thus defined as $\pi_1^{et}(X) = Gal(K(X)_{unr}/K(X))$.

Hurewic's theorem states that the first homology is isomorphic to the abelianization of the fundamental group. From this, we can construct the first cohomology group as

$$H^1(X, A) \cong Hom(H_1(X, \mathbb{Z}), A) \cong Hom(\pi_1(X), A)$$

We similarly define the first etale cohomology group

$$H^1(X_{et}, A) = Hom(\pi_1^{et}(X), A)$$

Note that we work with finite finite A. Note that for this case, the usual cohomology and etale cohomology of a simply connected manifold coincide. The higher etale cohomology classes are similarly defined for the constant sheaves on the etale sites. We now introduce an important type of etale cohomology, which is the Weil cohomology intended for introduction in this chapter.

Defining the usual sheaf cohomology on this site, we denote by $H^i_{et}(X, A)$ the i-th etale cohomology with coefficients in a finite ring A. For a variety X over a field of characteristic $p \neq l$, we define the l-adic cohomology as $H^i_{et}(X, \mathbb{Z}_l) := \lim_n H^i_{et}(X, \mathbb{Z}/l^n\mathbb{Z})$ and $H^i_{et}(X, \mathbb{Q}_l) := (\lim_n H^i_{et}(X, \mathbb{Z}/l^n\mathbb{Z})) \otimes \mathbb{Q}_l$

Again, consider X over a field k. We can always find an scheme $\bar{X}$ such that X has an open immersion into it and the morphism $\bar{X} \to Spec(k)$ is separated, finite type, and universally closed. We can now define

$$H^i_c(X, \mathbb{Q}_l) := H^i_{et}(\bar{X}, j_!\mathbb{Q}_l)$$

. Where $j_!\mathbb{Q}_l$ is the pushforward sheaf that is Q_l on X and zero elsewhere.

Note for the latter, that the compact support – the definition of scheme on the algebraic closure and completion of the underlying field – means that the cohomological dimension of the compact support agree with those of the usual de

Rham cohomology, thus the finiteness of the cohomology classes is guaranteed. Using properties of sheaves on sites, one can verify the other properties of l-adic cohomology with compact support as a Weil cohomology theory.

Chapter 3

Proofs of The Weil Conjectures

In this chapter, we provide the proofs of the Weil Conjectures 1-3, and a brief discussion of the Deligne's proof of the Riemann Hypothesis. The last conjecture is not proven here since the recreation of the proof requires machinery far beyond what has been discussed so far. The proofs are done following the first work of Deligne on the topic, [3], but the formulations more closely follow thosoe in Milne's formulation in [18].

3.1 Lefschetz fixed point formula

Here, we provide a proof for the main part of this chapter, the Lefschetz fixed point formula. In the next section, we deduce Weil 1-3 from this.

First, consider an endomorphism $f : X \to X$. The number of points fixed by this morphism can be computed as

$$|Fix(f)| = |\Gamma_f \cap \Delta|.$$

For a Variety X over the algebraic closure of the finite field $\bar{F}_q$, denote by f the frobenius endomorphism $Frob : x \mapsto x^q$. It follows from Fermat's little theorem that the fixed points of this endomoprhism are the $\mathbb{F}_q$ rational points of the variety, thus $|Fix(Frob)|\vdash$

$\mathrm{F}_q = |Fix(Frob)|_{\mathbb{F}_q}$. We therefore have the following lemma

For a variety X over the finite field $\mathbb{F}_q$, we have

$$|X(\mathbb{F}_q)| = |\Gamma_{Frob} \cap \Delta|$$

denoting the number of rational points on X.

Consider a map $\varphi : X \to Y$; this map induces a homomorphism of rings $\varphi^* : H^*(Y) \to H^*(X)$. Given that this map is a homomorphism of finite dimensional vector spaces, it has a matrix representation; We denote by $Tr(\varphi|H^*(X))$ the trace of this matrix.

Here we prove that this map is equal to the graph Γ_φ.

Lemma: For any regular map φ and $y \in H^*(Y)$, and $p, q : X \times X \to X$ projection maps, we have

$$p_*(cl_{X\times Y}(\Gamma_\varphi) \cup q^* y)) = \varphi^*(y)$$

Proof: We compute

$$\begin{aligned} p_*(cl_{X\times Y}(\Gamma_\varphi) \cup q^* y) &= p_*((1,\varphi)_* \cup q^* y) \\ &= p_*(1,\varphi)_*(1 \cup (1,\varphi)^* q^* y) \\ &= (p \circ (1,\varphi))_*(1 \cup (q \circ (1,\varphi)^* y)) \\ &= id_*(1_X \cup \varphi^* y) = \varphi^*(y) \end{aligned} \quad (3.1)$$

Lemma: Let (e_i) and (f_i) be the bases of $H^*(X)$ dual relative to the cup product, so that

$$e_i \cup f_j = \delta_{ij} e^{2d}$$

. We have the following:

$$cl_{X\times X}(\Gamma_\varphi) = \sum \varphi^*(e_i) \otimes f_i$$

. This follows the isomorphism induced by the Künneth form and the previous lemma.

We can now prove the Lefschetz fixed point formula for cohomology:

Theorem: (Lefschetz fixed point) Let $\varphi : X \to X$ be a regular endomorphism

of X, a complete non-singular variety over an algebraically closed field K. Then

$$(\Delta \cdot \Gamma_\varphi) = \sum_{r=0}^{2dim(X)} (-1)^r Tr(\varphi | H^r(X, \mathbb{Q}_l)).$$

Proof: Let e_i^r be a basis for H^r, and f_i^{2n-r} the dual for H^{2n-r} induced by Poincare duality. We then have

$$cl(\Gamma_\varphi) = \sum \varphi^*(e_i^r) \otimes f_i^{2d-r}, \text{ and}$$

$$cl(\Delta) = \sum e_i^r \otimes f_i^{2d-r} = \sum (-1)^{r(2d-r)} f_i^{2d-r} \otimes e_i = \sum (-1)^r f_i^{2d-r} \otimes e_i^r$$

taking the product of the sides we get

$$cl_{X\times X}(\Gamma_\varphi \cdot \Delta) = \sum (-1)\varphi^*(e_i^r) f_i^{2d-r} \otimes e_2 d = \sum_r Tr(\varphi^* | H^r)(e^{2d} \otimes e^{2d}).$$

Sending each element of the basis to 1, we get the desired formula.

We can now have our desired version of this as a corollary.

Corollary: We have the following formula for the rational points on a variety over a finite field:

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{2dim(X)} (-1)^i Tr(Frob | H^i(X)).$$

Remark: Consider the case $f = id_X$, the case of the identity morphism for a smooth projective variety. In this case, the Lefschetz trace formula yields an alternating sum of the dimensions of the cohomology classes of the variety, which is the generalized Euler characteristic. In particular for curves, we see that

$$\chi(C) = \sum_r (-1) dim(H^r(C)) = 2 - 2g$$

3.2 Proof of the Weil Conjectures 1-3

We now provide a proof of the Weil conjectures besides the Riemann Hypothesis. First, recall the definition of the zeta function as

$$Z(X,T) = \exp\big(\sum_{n=0}^{\infty} |X(\mathbb{F}_{q^n})| \frac{T^n}{n}\big)$$

which we after logarithmic differentiation and multiplication by T becomes

$$T\frac{d}{dT}\log(Z(X,T)) = \sum_{n=0}^{\infty} |X(\mathbb{F}_{q^n})| T^n.$$

We have the following identity from linear algebra for an endomorphism F of space V

$$T\frac{d}{dT}\log(det(1-FT|V))^{-1}) = \sum_{n=0}^{\infty} Tr(F^n|V)T^n$$

Which, coupled with the Lefschetz fixed point formula, yields the identity

$$Z(X,T) = \prod_{i=0}^{2dim(X)} det(1 - Frob_q^* T|H^i(X))^{(-1)^{i+1}}$$

Where 1 denotes the identity matrix.

Rationality and Betti numbers are clear; the determinant yields a polynomial in degree of $H^i(X)$, and since no Weil cohomology class is infinite, the polynomial remains rational. For the functional equation, notice that the Poincare duality gives a non-degenerate pairing between $H^{2n-i} and H^i. Given that the image of $Frob_q$ in H^{2n-i} is a multiplication by q^n, we have

$$det(1 - Frob_q^* T|H^i) = q^{nb_i} T^{b_i} det(1 - \frac{1}{q^n T} Frob_q^{-1}|H^{2d-i})$$

where b_i are the Betti numbers. Taking the product over all cohomology classes with regards to the alternating grading of the Künneth map, we get

$$Z(X, q^{-n}T^{-1}) = \pm q^{n\chi(X)} T^{\chi(X)} Z(X,T)$$

as desired; the sign here relates to the instances of $q^{n/2}$ as an eigenvalue of the Frobenius action.

This concludes the proofs of the Weil conjectures 1-3. For the Riemann Hypothesis, we need further discussion of the eigenvalues of the Frobenius.

Chapter 4

Application: Elliptic Curve Arithmetic

In this chapter, we will show an application of the cohomological work done thus far. Much of this material has been sent to appear in Kazakh Mathematical Journal, and an abstract of it has been presented in the IMMM conference, April 2025.

4.1 Elliptic Curves

We now briefly introduce the idea of elliptic curves and explain the application of the thus far given context. Our main aim here is to apply the methods and techniques given so far to compute the first etale cohomology class of a family of elliptic curves.

We begin by defining elliptic functions, from which we can define elliptic curves and show the genus 1 property.

Definition: an *elliptic function* f is a doubly periodic function with the periods $w_1, w_2 \in \mathbb{C}$ such that

$$f(z) = f(z + mw_1 + nw_2) \text{ for } m, n \in \mathbb{Z}.$$

We define the period lattice Λ as such linear combinations of w_1, w_2.

We now recall a theorem from complex analysis, introducing constraints on the types of elliptic function:

Theorem: (Liouville)

1. A holomorphic, entire function on the complex plane is constant.
2. The sum of residues of f in the domain $\mathbb{C}/\Lambda$ is zero.
3. Every value of f has the same frequency in $\mathbb{C}/\Lambda$

Proof:

1. take the domain $\mathbb{C}/\Lambda$. If the function f is holomorphic then it is bounded in this domain. Since this implies the function being bounded on the entire complex plane, the function is constant.
2. take the parallelogram $[0, w_1, w_1 + w_2, w_2]$ which defines the domain $\mathbb{C}/\Lambda$. Due to the periodic nature of f, the integral over opposing sides of this parallelogram is zero, hence the sum of residues is zero.
3. take the function $g(z) = \frac{1}{f(z)+f(z_0)}$; given that this function must also be elliptic, the number of occurrences of any $f(z_0)$ must be equal, otherwise $g(z)$ violates the second theorem.

We now move on to one of the main classes of elliptic functions, the Weierstrass elliptic functions.

Definition: The *Weierstrass elliptic function* $\wp(z)$ is defined as

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - 0} \frac{1}{z^2 - \lambda^2} - \frac{1}{\lambda^2}.$$

The derivative of this function is

$$\wp'(z) = -\sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}$$

thus it satisfies the following differential equation:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

with coefficients $g_2 = 60G_4(w_1, w_2)$ and $g_3 = 140G_6(w_1, w_2)$, where G_4, G_6 are the Eisenstein series defined in the accompanying text.

This differential equation gives us our main object of study in this text, *elliptic curves*. Rewriting this relation as

$$y^2 = 4x^3 - ax - b$$

we get the *Weierstrass normal form* of an elliptic curve[1], which by this mapping is isomorphic to the torus $\mathbb{C}/\Lambda$. In general, elliptic curves are smooth and projective algebraic curves of genus one.

Now, using the parameter $\tau = \frac{w_1}{w_2}$ and modularity of Eisenstein series', we get the mapping $\mathbb{H}/SL_2(\mathbb{Z}) \to \Lambda$. From the Weierstrass function, we got the map $\mathbb{C}/\Lambda \to E$. We can complete this route by constructing a map $E \to \mathbb{H}/SL_2(\mathbb{Z})$.

4.2 The Group Structure on $E(\mathbb{Q})$

Given any cubic curve, a key feature is that a line through two distinct rational points on the curve intersects it at a third rational point. This property is the foundation of the group law on elliptic curves. Specifically, if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two rational points on the curve $E(\mathbb{Q})$, their sum, denoted $P + Q = R$, is a third rational point $R = (x_3, y_3)$ that lies on the curve as well. This operation is both geometric (based on the intersection of a line) and algebraic (as part of the elliptic curve's group structure).

A notable feature of the general Weierstrass equation for elliptic curves is that it is symmetric with respect to the y-axis. That is, for any point (x_0, y_0) on the curve, the point $(x_0, -y_0)$ is also a rational point. This symmetry helps define the concept of the identity element in the group. The point $\mathcal{O}$, called the point at infinity, serves as the identity element. Geometrically, $\mathcal{O}$ is the point where the curve intersects the line at infinity. This intersection occurs when the curve is homogenized by introducing a projective coordinate Z, such that the curve equation becomes:

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

When we set $Z = 0$, the intersection at infinity corresponds to the point where $X^3 = 0$, confirming that the curve intersects the line at infinity in exactly three points, one of which is the identity point $\mathcal{O}$.

[1] in characteristics $p \neq 2, 3$ as the curve needs to be smooth

From this construction, the rational points on the elliptic curve, together with the point O, form an Abelian group under the operation of point addition. The addition of two rational points is governed by the geometric construction of intersecting lines (or tangents) on the curve, and this group structure is a central feature of elliptic curves.

A fundamental result in the study of elliptic curves is Mordell's theorem, which states that the group of rational points on an elliptic curve, $E(\mathbb{Q})$, is finitely generated. That is, any rational point Q on the curve can be expressed as a finite sum of independent points $P, P_1, P_2, \ldots, P_r$, where $P_1, P_2, \ldots, P_r$ form a basis for the free part of the group, and P is a point of finite order. In other words, there exists a set of independent rational points $P_1, P_2, \ldots, P_r$, such that every other rational point on the curve can be written as an integer linear combination of these points:

$$Q = bP + a_1P_1 + a_2P_2 + \cdots + a_rP_r,$$

where $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, $b \in \mathbb{Z}/n\mathbb{Z}$. The rank r of the curve is the number of independent points in this basis, giving it the structure of the free group

$$E(\mathbb{Q}) \simeq E_{Tors} \oplus \mathbb{Z}^r$$

Where E_{Tors} is the finite part. In this work, we have set $E_{Tors} \simeq \mathbb{Z}/2\mathbb{Z}$, hense the name 2-torsion.

4.3 L-series Associated to an Elliptic Curve

We now provide the definition for the L-function and the zeta function of an elliptic curve. Firstly, from the isomorphism given above $E \simeq \mathbb{C}/\Lambda$, it follows that the cohomology classes for an elliptic curve are

$$H^{\mathrm{i}}{}_{\mathrm{c}}(E, \mathbb{Q}_{\mathrm{l}}) \begin{cases} i = 0 & \mathbb{Q}_l \\ i = 1 & \mathbb{Q}_l^2 \\ i = 2 & \mathbb{Q}_l \end{cases}$$

from which it follows that the structure of the zeta function attached to an elliptic curve is of the form

$$Z(E,T) = \frac{P_1(T)}{(1-T)(1-qT)}$$

where $deg(P_1(T)) = 2$. To compute this factor exactly, we will use the following auxiliary construction.

For a curve $E : y^2 = x^3 + ax + b$, we have the discriminant $\Delta(E) = -16(4a^3 - 27b^2)$. For odd primes not dividing Δ, we define a reduction of the Elliptic curve as

$$\tilde{E}_p : y^2 = x^3 + \tilde{a}x + \tilde{b}$$

to be the reduction of the curve modulo p. Counting pairs (x, y) modulo p along with the point at infinity we get the result

$$\tilde{E}(\mathbb{F}_p) = p + 1 - \epsilon_p$$

with $\epsilon_p \leq 2\sqrt{p}$. We now construct the *L-function of E* as the product

$$L(E,s) = \prod_{p \text{ prime}} (1 - \frac{\epsilon_p}{p^s} + \frac{1}{p^{2s-1}})^{-1}.$$

Expanding the L-function as an infinite series we get the final result

$$L(E,s) = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}.$$

We note that $\epsilon_n = \prod_{p|n} \epsilon_p$, and that $\epsilon_{p^{k+1}} = \epsilon_p \epsilon_{p^k} - p\epsilon_{p^{k-1}}$.

We can define the zeta function of the elliptic curve from this as

$$Z_p(E,t) = \frac{1 - a_p t + pt^2}{(1-t)(1-pt)}.$$

Putting $t = p^{-s}$, we get

$$Z(E,s) = \frac{1 - a_p p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{s-1})}$$

which we can rewrite as

$$Z(E,t) = \zeta(s)\zeta(s-1)L(E,s)^{-1}$$

As a consequence of the modularity theorem, the L-function of an elliptic curve arises from a modular form, as a result, there exists a holomorphic extension for the function $L(E,s)$ as

$$\xi(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

with the reflection formula

$$\xi(E,s) = \pm\xi(E,2-s).$$

We note that the pole for an elliptic L-function is situated at $s = \frac{3}{2}$. The constant N is an important constant related to the curve called the *conductor*.

The Birch-Swinnerton Dyer conjecture states that the order of vanishing of the L-function at $s = 1$ is equal to the rank of the elliptic curve. Further, it states that the first non-zero Taylor coefficient of the L-function at $s = 1$ is

$$L_1 = \frac{|Ш(E)|\Omega_E R_E c_E}{|E_{Tors}|^2}$$

where Ω_E, R_E, c_E are constants, E_{Tors} is the torsion group of the curve and $Ш(E)$ is the Tate-Shafarevich group of the elliptic curve, the definition of which is given in what follows in the chapter.

4.4 2-Torsion Families and the Rank Problem

Considering an elliptic surface

$$E_{A,B} : y^2 = x^3 + A(t)x + B(t) \text{ for } A, B \in \mathbb{Q}[t], deg(A,B) \leq 2$$

we investigate the rank of its fibers at particular values of t. Generally, it is known that for a rational elliptic surface with generic rank r_E, the subset of fibers with ranks $r_E + \{1,2,3\}$ is not thin. One might ask further questions about the

average ranks of fibers and the method of computing the generators of the weak Mordell-Weil group. This task is carried out by computing the Selmer group.

We begin by marking families of elliptic curves by a 2-torsion point $(\frac{r}{h^2},0)$ and their isogenous family of curves. We consider the families

$$E : y^2 = x^3 + h^2tx - rt - r^3$$

With $h = 1$, e.g, integral torsion points, and translating the torsion to $(0,0)$ we get the family

$$E : Y^2 = X^3 + 2rX^2 + (t^2 + r^2)X$$

and the natural isogeny at the point $(r,0)$.

The main objective of this work is to demonstrate the following:

The upper bound of the Selmer rank for a family of elliptic curves with a rational 2-Torsion up to naive height X is $\log\log X$

In recent years, several authors — most notably Klagsbrun et. al. [14], [13] — have studied the average behavior and distribution of Selmer ranks in families of elliptic curves, often using Tamagawa ratios by the matrix construction described by Monsky in appendix of [11]. In this work, we propose a direct and elementary argument showing that the upper bound of the Selmer ranks in a family of elliptic curves with rational 2-torsion grows like $\log logX$, relying on local Galois cohomology and the probabilistic distribution of twists and local images, as laid out in [7]. Another approach to construction of Selmer groups is the graph theoretical method described in [5], [6] in which methods of graph theory are used to describe the Selmer groups. The same method is used in [16] over $\mathbb{Q}(i)$. A notable similarity in most of these works is the focus on an special case of this problem for curves

$$E : y^2 = x^3 - nx$$

either focusing on the case where n is an square, or general case as in [16]. Our aim is for higher generality in this case, but we note that setting $r = 0$ gives the same curve here.

4.5 Selmer Groups

For a variety A and a number field k with a set of places v, we denote by $A(k_v)$ the set of points on A in the v-completion of k. Let

$$H^i(k, A) := H^i(Gal(\bar{k}/k), A/k)$$

denote the Galois cohomology classes of A, in particular,

$$A(k) = H^0(k, A)$$

is the set of k-rational points on A.

The Tate-Shafavevich group is defined as

$$Ш_{A/k} = ker(H^1(k, A) \to \prod_v H^1(k_v, A))$$

such that the non-trivial elements correspond to homogeneous spaces (also called k-torsors) measuring the failure of Hasse principal. Conjecturally, this value is finite. This is only known to hold for the class of elliptic curves with a zero of order at most one at $L(E/\mathbb{Q}, 1)$, or curves of rank ≤ 1 given that the BSD conjecture is proven for all such curves.

For an isogeny of elliptic curves, we have the following sequence

$$0 \longrightarrow E(k)[\varphi] \longrightarrow E(\bar{k}) \longrightarrow E'(\bar{k}) \longrightarrow 0$$

where $E(k)[\varphi]$ is the kernel of isogeny. Applying Galois cohomology gives us

$$0 \longrightarrow E(k)[\varphi] \longrightarrow E(k) \longrightarrow E'(k) \longrightarrow$$

$$H^1(k, E[\varphi]) \longrightarrow H^1(k, E) \longrightarrow H^1(k, E') \longrightarrow \dots$$

Now, setting $\varphi = m$, the multiplication by m map and rewriting the sequence we get

$$0 \longrightarrow E(k)/mE(k) \xrightarrow{\delta} H^1(k, E[m]) \longrightarrow H^1(k, E)[m] \longrightarrow 0$$

which we can restrict at each place ν to get

$$0 \longrightarrow E(k_\nu)/mE(k_\nu) \xrightarrow{\delta_\nu} H^1(k_\nu, E[m]) \longrightarrow H^1(k_\nu, E)[m] \longrightarrow 0.$$

Notice that given the finitude of $E[\varphi]$, the local Galois cohomology groups $H^i(k_\nu, E[\varphi])$ coinside with the respective etale cohomology groups.

The Selmer group is defined as the kernel

$$Sel^m(E/k) = Ker\big(H^1(k, E[m]) \to H^1(k_\nu, E)[m]/H^1_m(k_\nu, E)\big)$$

for each prime, where

$$H^1_m(k_\nu, E) = \delta_\nu(E'(k_\nu)/m(E(k_\nu))),$$

of the mapping of m-torsion of the first Galois cohomology group to its restriction in all places. In this way, we get the exact sequence

$$0 \longrightarrow E(k)/mE(k) \longrightarrow Sel^m(E/k) \longrightarrow Ш_{E/k}[m] \longrightarrow 0.$$

In [7], an algorithm is given for computing the connecting homomorphisms δ_p and δ_2. These images are used coupled with the definition

$$Sel^\varphi(E/\mathbb{Q}) = \{x \in H^1(\mathbb{Q}, E[\varphi]) \mid res_p(x) \in Im(\delta_p) \text{ for all places } p\} = \bigcap Im(\delta_p)$$

to describe the full Selmer groups for each elliptic curve. A full description of the Selmer group gives an upper bound on the rank of the elliptic curves as we have

$$rank(E) = dim_{F_2} Sel^\varphi(E/\mathbb{Q}) + dim_{F_2} Sel^{\varphi'}(E'/\mathbb{Q}) \\ - dim_{F_2} Ш(E/\mathbb{Q})[\varphi] - dim_{F_2} Ш(E'/\mathbb{Q})[\varphi'] - 2$$

from which it follows that

$$rank(E) \leq dim_{F_2} Sel^2(E/\mathbb{Q}) + dim_{F_2} Sel^2(E'/\mathbb{Q}) - 2$$

relating the rank of elliptic curve to the dimension of the 2-Selmer group spanned as an $\mathbb{F}_2$ vector space. In particular, if the Tate-Shafarevich group is trivial, the

two sides will be equal. We refer to the right side of (1) as the *Selmer rank* of the curve E. In the next section. The algorithm given in [7] is reproduced, which we will use as the basis for our argument.

4.6 Prior Results

The problem of understanding the distribution of Selmer ranks in large families of elliptic curves has attracted significant attention in recent years. Bhargava and Shankar have shown in a series of foundational works that, in large enough families of elliptic curves ordered by height, the average size of 2-Selmer groups is bounded. Specifically, in [2], they establish that the average size of the 2-Selmer group across all elliptic curves over $\mathbb{Q}$ is exactly 3, and in [1], for families with a marked 2-torsion point, the average rises to 6. These results suggest that, for a majority of curves, the Mordell–Weil rank is either 0 or 1, though they do not resolve the Birch and Swinnerton-Dyer conjecture in individual cases.

The behavior in more constrained families—particularly those with prescribed torsion structures—is subtler. In [22], Xiong investigates a specific one-parameter family $E_n : y^2 = x^3 - n^3$, showing that the average size of the 2-Selmer group grows slowly, approximately as $\sqrt{\frac{1}{2}\log\log X}$ as $n \leq X$. A more general result appears in [14], where Klagsbrun and Lemke-Oliver demonstrate that the 2-Selmer rank in families of quadratic twists of curves with a marked 2-torsion point can grow arbitrarily large. Their proof relies on studying the Tamagawa ratio between a curve E and its 2-isogenous partner E',

$$T(E/E') = \frac{|\mathrm{Sel}_{\varphi}(E)|}{|\mathrm{Sel}_{\varphi'}(E')|},$$

and evaluating its 2-adic valuation across quadratic twists E^{χ}. The growth is controlled by local cohomological invariants at primes dividing 2, the discriminants Δ, Δ', and infinity:

$$\mathrm{ord}_2 T(E^{\chi}/E'^{\chi}) = g(\chi) + \sum_{v|2,\Delta,\infty} \left(\dim_{\mathbb{F}_2} H^1_{\varphi}(K_v, E[\varphi]) - 1\right),$$

where $g(\chi)$ involves average Legendre symbols over ramified primes.

In a follow-up work [15], they show that the distribution of Selmer ranks across

such families of twists has mean 0 and variance $\log\log X$, and they deduce that arbitrarily high Selmer ranks occur infinitely often. These results, however, apply specifically to twist families and depend crucially on analyzing the variation of the Tamagawa ratio.

The present work differs in both setting and method. We consider a static family of elliptic curves over $\mathbb{Q}$ with a rational point of order 2 at the origin, not twists. We demonstrate that even without extension to quadratic fields, the Selmer rank can exhibit unbounded growth, and that the average rank exhibits logarithmic fluctuation. While our local analysis uses similar cohomological terms—such as the local image under the Kummer map δ_v—our method is based on direct reduction and descent calculations adapted from Goto [7], rather than Tamagawa ratios or isogeny-based arguments.

Moreover, while [14] suggests a $\sqrt{\log X}$ average size of individual Selmer groups in such families, no published proof of this claim appears in their later work [13], which instead focuses on Cohen–Lenstra-type distributions for Selmer group structures given fixed rank. As such, the present work contributes a distinct perspective on the problem by re-analyzing the growth of 2-Selmer ranks directly over $\mathbb{Q}$, using concrete local-global computations without relying on isogeny decompositions or twist families.

4.7 Algorithm for Computation of the Selmer Group

We now reproduce the algorithm given in [7] to compute the Selmer groups. We note here that the images of the connecting homomorphisms δ_p and δ'_p are orthogonal with the $(,)_p$ Hilbert symbol, such that for all $x \in \delta_p, y \in \delta'_p$ we have $(x,y)_p = 1$.

In the following section, we have the curve

$$E : y^2 = x^3 + Ax^2 + Bx$$

with values

$$a = Ord_p(A), b = Ord_p(B), d = Ord_p(A^2 - 4B)$$

and $(\frac{a}{p})$ denoting the Legendre symbol, and u is a non-square modulo p. We have the following cases

1. $b = 0$:

   (a) $2|d$ and $(\frac{-2A}{p}) = -1 \rightarrow Im(\delta_p) = \mathbb{Z}_p^{\times}\mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$

   (b) otherwise $Im(\delta_p) = \{1\}$

2. $b \neq 0$:

   (a) $a = 0$:

      i. $2|b$ and $(\frac{A}{p}) = -1 \rightarrow Im(\delta_p) = \mathbb{Z}_p^{\times}\mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$.

      ii. otherwise $Im(\delta_p) = \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$.

   (b) $a \neq 0$:

      i. $b = 1 \rightarrow Im(\delta_p) =< B >$.

      ii. $b = 2, a = 1$: let $A = pA', B = p^2B'$, and $\alpha = (\frac{A'^2 - 4B'}{p})$, $\beta = (\frac{A' + 2\sqrt{B'}}{p})$ with $\sqrt{B'}$ denoting the p adic square root:

         A. $\alpha = 0 \rightarrow Im(\delta'_p) =< 2A, A'2 - 4B >$.

         B. $\alpha = -1 \rightarrow Im(\delta_p) =< B >$.

         C. B' is not an square in $\mathbb{Q}_p \rightarrow Im(\delta_p) = \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$.

         D. $\beta = 1 \rightarrow Im(\delta'_p) =< p >$.

         E. $\beta = 1 \rightarrow Im(\delta'_p) =< pu >$.

   (c) $b = 2, a \geq 2$:

      i. $-B$ is not an square in $\mathbb{Q}_p \rightarrow Im(\delta_p) =< B >$.

      ii. $p \equiv 3 \bmod 4 \rightarrow Im(\delta_p) = \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$.

      iii. $p \equiv 1 \bmod 4 \rightarrow Im(\delta_p) =< p >, < pu >$ depending on whether the quartic character of $-B$ in p is 1 or -1.

   (d) $b \geq 3, a = 1 \rightarrow Im(\delta_p) =< B >$.

   (e) $b = 3, a \geq 2 \rightarrow Im(\delta_p) =< -A, B >$.

The algorithm concludes here. For δ_2, the algorithm is similar, but produces, on average, larger groups. The algorithm can be simplified by making use of quartic characters, as done in [16].

4.8 Main Theorem

Let $F(X)$ denote the family of elliptic curves of bounded height:

$$F(X) = \{E_{A,B} : h(E_{A,B}) < X\}$$

where the height function is defined by

$$h(E) = \max(3A^3, 27B^2).$$

We are concerned with the behavior of the 2-Selmer rank $S(E)$ for $E \in F(X)$. Recall that the algorithms described in the previous section define local connecting homomorphisms δ_p and their duals δ'_p, which are orthogonal. These maps capture the image of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ in $H^1(\mathbb{Q}_p, E[2])$, and their interaction across all primes controls the dimension of the 2-Selmer group.

Now consider a curve of the form:

$$E : y^2 = x^3 + pA'x^2 + p^2B'x,$$

which is a quadratic twist of the curve

$$E_p : y^2 = x^3 + A'x^2 + B'x.$$

This twist relation implies that the local images at p can be heuristically related, and in particular, the twisting by p modifies the Selmer rank by introducing or removing local obstructions.

We model the expected size of the image of each local connecting homomorphism δ_p by:

$$\mathbb{E}[|\delta_p|] \approx \sum_{n=1}^{\log X} \frac{n}{p^n} \approx \frac{p}{(p-1)^2} \sim \frac{1}{p},$$

where the last approximation holds in the limit as $X \to \infty$. That is, the expected contribution to the Selmer rank from each prime p behaves like $1/p$.

Summing over all primes $p \leq X$, the total expected Selmer rank satisfies:

$$\mathbb{E}[S(F(X))] \approx \sum_{p \leq X} \frac{1}{p} \sim \log\log X.$$

Possible overlaps (i.e., dependencies between local conditions at different primes) contribute correction terms of order $\sum_{p \neq q} \frac{1}{pq}$, which is convergent and thus does not affect the asymptotic growth. Therefore, we obtain:

$$\mathbb{E}[S(F(X))] \sim \log\log X,$$

which completes the proof of Theorem (1).

This heuristic matches the behavior observed in the works of Klagsbrun–Lemke Oliver [14], [15] and Klagsbrun–Kane [13], who study the distribution of 2-Selmer ranks via Tamagawa ratios and show that the average and variance of Selmer ranks grow like $\log\log X$.

4.9 Conclusion and Prospects

This result shows the growth of Selmer ranks for this family of elliptic curves. From the equation (2) we see that this result, together with an study of the growth of Tate-Shafarevich group could lead to the solution of the following open problem

Problem 1. *Does there exist $B \in \mathbb{Z}$ such that for all elliptic curves E over $\mathbb{Q}$, one has $rank(\mathbb{Q}) \leq B$?*

We note that, in light of results such as [2] and [1], the vast majority of elliptic curve families exhibit bounded average Selmer ranks, making them unlikely sources of counterexamples to bounded rank conjectures. By contrast, families with unbounded Selmer rank—such as the one examined here—become natural candidates for detecting potential violations. In this context, one of two conclusions must hold: either the Mordell–Weil rank becomes unbounded in such families, or the Tate–Shafarevich group (E) absorbs the excess growth. The latter scenario raises a distinct and unresolved problem of its own, as no general algorithm exists for computing (E), and its behavior in large families over $\mathbb{Q}$ remains poorly understood.

The general consensus is in favor of this, for example, as in [19]. We see that in this case the boundedness of the rank would imply that the Tate-Shafarevich group also grows without bounds. There are methods for studying this problem, as in [20], but it remains for future undertakings to apply these to this particular family strictly over $\mathbb{Q}$.

Conclusion

The dissertation thus presented has been structured in two strata. Firstly, a foundation of modern developments in algebraic geometry has been lain out, and second, an application has been presented to show the use of the tools and techniques developed for a problem in arithmetic geometry.

The first part was devoted to the development of the formalism necessary for understanding the modern, categorical interpretation of algebraic geometry. After presenting the problem, that of Weil conjectures, we dedicated a chapter to build up all that was required to address them; categories, sheaves and schemes, cohomological apparata and number theoretical aspects of the finite fields were presented to meet this end. The emphasis on the abstract machinery was quite essential; without a coherent outline of the tools and terminology, not just the Weil conjectures but the application too would remain inaccessible. While not a comprehensive guide, a framework has been drawn and adopted to address the main points of modern geometric language.

The second part was the application of these methodology and machinery to a concrete arithmetical problem, that of Selmer groups and the ranks of elliptic curves. Building on the cohomological framework of the former part, we defined certain auxiliary concepts for the ranks of elliptic curves, applied methods of Galois and etale cohomology, and draw upper bounds for the ranks of Selmer groups and thus demonstrated the use of abstract algebraic concepts to yield concrete results in the theory of arithmetic. While we did not address the analytic theory of the L-functions and the Birch-Swinnerton-Dyer conjecture, as those are far beyond the scope of this dissertation, this application provides a first step into this connection of algebraic and analytic phenomena.

There are many routes that can be addressed from the path outlined in this dissertation; One immediate step is studying the finiteness of Tate-Shafarevich

groups, a problem which remains open even in the narrowest of cases. As the methods of application of the Selmer ranks suggests, however, in our case this could be an attainable goal. The presented homological techniques naturally yielded a method to approach the Selmer groups, and the same methods could be applied again for the Tate-Shafarevich groups, when a more sophisticated approach to the global fields has been established. A more ambitious aim is to connect the algebraic constructions of this work to the analytical theory of the zeta functions. It was briefly mentioned how the L-functions for an elliptic curve contain algebraic data in their central values. It was far beyond the scope of this work, but it remains as a future path to connect these bridges for the solution of the Birch-Swinnerton-Dyer conjecture. This analytic goal would be first of many steps to fully grasp the analytical 'meaning' of what was presented, with the final aim of the Riemann zeta function. Many topics remain to be discussed before that, Galois representations, more cohomological frameworks, and analytic number theory, to name a few; this work however was aimed at being a first step, which now concludes.

This thesis is thus a first step; a point of departure into deeper ends of number theory and geometry. A foundation was presented, the application was shown, and thus further explorations may proceed.

Bibliography

[1] Bhargava, M., Ho, W. *Coregular spaces and genus one curves*, Cambridge J. Math., 4:1, pp. 1-119, 2016.

[2] Bhargava, M., Shankar, A. *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Math., 181:1, pp. 191-242, 2015.

[3] Deligne P. *La conjecture de Weil. I*, Publications Mathématiques de l'IHÉS, 43, 273–307, 1974.

[4] Deligne P. *La conjecture de Weil. II*, Publications Mathématiques de l'IHÉS, **52**, 137–252, 1980.

[5] Feng, K. *on-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. 80, 71–83, 1996.

[6] Feng, K., Xiong, M. *On Selmer groups and Tate-Shafarevich groups for elliptic curves* $y^2 = x^3n^3$, Mathematika 58, no. 2, 236–274, 2012.

[7] Goto, T. *A study on the Selmer groups of elliptic curves with a rational 2-torsion*, Kyushu University Doctoral Thesis, 2002.

[8] Grothendieck A. et. al. *Éléments de géométrie algébrique*, 1960-1974.

[9] Grothendieck A. et. al. *Séminaire de Géométrie Algébrique du Bois Marie*, 1960-1969. [2]

[10] Grothendieck A. *Sur quelques points d'algèbre homologique*, Tohoku Math. J., 9:2, 119-221, 1957.

[2]The EGA and SGA volumes are foundational texts developed under Grothendieck's direction. Though never fully published in traditional form, they are available through the Grothendieck Circle archive: https://webusers.imj-prg.fr/~leila.schneps/grothendieckcircle/.

[11] Heath-Brown, D. R.*The size of Selmer groups for the congruent number problem. II*, Invent. Math., 118, 331–370, 1994.

[12] Kahn, B., *Zeta and L-function of varieties and motives*, Cambridge University Press, 2020.

[13] Kane, D., Klagsbrun, Z. *On the Joint Distribution Of* $Sel_{(E/Q)}$ *and* $Sel_{(E/Q)}$ *in Quadratic Twist Families*, Arxiv (unpublished) 1702.02687, 2017.

[14] Klagsbrun, Z., Lemke-Oliver, R. *The distribution of 2-Selmer ranks of quadratic twists of elliptic curves with partial two-torsion*, Mathematika, 2013.

[15] Klagsbrun, Z., Lemke-Oliver, R. *The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point*, Res. Math. Sci., 1:15.

[16] Kling, A., Savoie, B. *Computing Selmer group for elliptic curves* $y^2 = x^3 + bx$ *over Q(i)*, Arxiv (unpublished) 2410.22714, 2024.

[17] Klingler, B. *ETALE COHOMOLOGY AND THE WEIL CONJECTURES*, online notes at here

[18] Milne, J. *Lectures on Etale Cohomology*, available at his website

[19] Park, J., Poonen, B., Voight, J., Matchett Wood, M. *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. 21:9, pp. 2859–2903, 2019.

[20] Shiga, A. *Behaviors of the Tate-Shafarevich group of elliptic curves under quadratic field extensions*, Arxiv (unpublished) 2411.12316, 2024.

[21] Vakil, R. *Foundations of Algebraic Geometry*, lecture notes, 2017, available at http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf.

[22] Xiong, M. *On Selmer groups of quadratic twists of elliptic curve a two-torsion over Q*, Mathematika, 2013.