Some Preliminary Steps Towards a Formally Verified Proof of the Weil Conjectures

by

Alexander Berenbeim

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2015

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. (Pending: This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.)

I understand that my thesis may be made electronically available to the public.

Alexander Berenbeim

Abstract

This paper is intended as a broad survey of topos theory as motivated by one of the historical motivations for the subject: the Weil conjectures. The structure of this survey has been guided by the goal of formally verifying the proof of the Weil conjectures. Towards that end, this paper consists of 3 parts: Preliminaries; the Proof of the Weil Conjectures; and Future Work.

Part I consists of three chapters whose contents touch upon the different mathematical results needed to realize a formally verified proof of the Weil conjectures. Chapter 1 provides a crash course on categorical logic, developing a connection between fibred categories and type theory, and culminating in an exposition of elementary topoi. Chapter 2 examines Grothendieck topoi and their connection to algebraic geometry and topology, culminating in some brief commentary on describing cohomology theories from the perspective of higher category theory. Chapter 3 surveys the many diverse mathematical results required of a Weil cohomology theory.

Part II consists of three chapters exploring the Weil conjectures properly. Chapter 4 provides a statement of the Weil conjectures. Chapter 5 provides a proof for all the Weil conjectures, sans the proof of the Riemann hypothesis. In its stead, Chapter 5 culminates with a fairly detailed description of the structure of the proof of the Riemann hypothesis. Chapter 6 is a verification of the proof of the Weil conjectures for arbitrary projective varieties.

Finally, Part III consists of a single chapter, the index and bibliography. Chapter 7 presents an outline for a future research program for realizing the goal of this paper.

Acknowledgements

I would first like to begin by thanking my advisor David McKinnon. Without his breadth of knowledge, or his seemingly infinite patience and foresight, this paper would not have been possible. Furthermore, I would like to thank Tobias Fritz and Cecilia Flori for encouraging a far subtler understanding of what constitutes a logic. I would also like to thank Michael Shulman for answering some of my seemingly inane questions, as well as asking a few pointed questions that helped me structure this paper. Finally, I would like to thank Jason Bell and Julian Rosen for attending my talks on weak $\omega-$groupoids and model categories, and raising some questions that the first chapter is intended to satisfy.

To Sam, Sarah, and Ray.

Contents

0.1 Foreword

In looking back on this project, and admitting to myself that I had been naïve about the requisite scope, I can immediately conclude the following: mathematics research is driven in part by beautiful accidents.[1]

I first encountered topos theory entirely by accident. Some time over the summer of 2010, in the midst of preparing to take a course in category theory that fall, I happened upon a copy of Goldblatt's book, *Topoi: A Categorial Analysis of Logic* [7] at a book store in Lincoln Centre while I was waiting for a movie to begin seating. While I had some vague goal of acquiring a copy of Awodey's book on the subject [2], as this was the book required for the course, I had no illusions as to the likelihood of this acquisition occurring that day. Curiously enough, although they did not stock Awodey's book, they did carry Goldblatt's book.[2] Intrigued by the title alone, I picked up the book, started reading through. As often is the case with a compelling mathematical treatise, I lost track of the time.[3] Having missed my show, I purchased the book and set off for a nearby café to continue reading.

In many ways, this chance encounter has informed my subsequent mathematical interests. I mention this, because my initial forays into topos theory start with Lawvere and Tierney's work on elementary topos theory and the topos models of intuitionistic first order logic, and not with Grothendieck and the conjectures that informed his invention of topos theory (not to mention scheme theory or motive theory). That Lawvere noticed that Grothendieck topoi, which as *sheaves on a site* not only provided a generalisation of the notion of topological space, but in doing so, generalised the categorical notion of sets and predicates, struck me at the time as an actual historical accident. In my case, with the basic tools of category, I arrived at the elementary notion of a topos blithely unaware of their historical motivation.

However, I mean more than the personally fortuitous event of finding Goldblatt's book, and more than Lawvere's realization that Grothendieck had stumbled upon a profound way of conceiving mathematical spaces when I say accident. I also mean that in a much broader sense, the motivations

[1] I mean more in the sense of historical, rather than logical, contingencies, although certainly those do apply.

[2] I suspect that this is because Goldblatt's book explicitly discusses logic and is classified as a philosophy book, making it more likely to be stocked by this book seller than a book on pure category theory.

[3] For what it's worth, I did eventually see the film I missed, and I did not miss much.

for these abstractions may seem entirely unrelated, that these connections are drawn up almost as if by chance. After all, how does one get categorcial logic from sheaves on sites, and what did sheaves on sites have to do with the Weil conjectures? The particular accident that I'm dancing around are the ζ functions, and how the concerns of number theorists eventually led to the development of contemporary algebraic geometry and categorical logic.

In principle, anyone with a passing familiarity with grade-school arithmetic (sums, products, and multiplicative inverses) could describe them. Indeed, with a standard undergraduate education, one could describe André Weil's conjectures reasonably well. What commands attention is the sheer volume of research that has been motivated by studying functions analogous to the form

$$\zeta(t) = \sum_{n=1}^{\infty} n^{-t} \tag{0.1.1}$$

While mathematicians had certainly been studying $\zeta(n)$ for specific $n \in \mathbb{Z}^+$ in the centuries prior to Euler, he began the explicit study of $\zeta(t)$ as a real valued function. However, mainstream mathematical interest in these functions can rightly be said to begin with Riemann, who extended ζ via analytic continuation to $\mathbb{C}\backslash\{1\}$. Moreover, he demonstrated that there was a functional relationship between $\zeta(z)$ and $\zeta(1-z)$, and postulated his famous hypothesis that all zeroes of $\zeta(z)$ such that $\Re(z) > 0$ occur when $\Re(z) = \frac{1}{2}$. Riemann, Hadamard and others used $\zeta(z)$ for studying the distribution of prime numbers, in one sense culminating in the prime number theorem, while Dedekind began the generalization of Riemann's hypothesis that ultimately led to the Weil conjectures.

The Weil conjectures themselves developed from Artin and Schmidt's work on algebraic curves, in particular Artin's development of the following zeta function for algebraic curves f over finite fields $\mathbb{F}_q$:

$$\zeta(f,t) := \exp\left(\sum_{m=1}^{\infty} N_m(f)\frac{t^m}{m}\right) \tag{0.1.2}$$

where $N_m(f)$ describes the number of points in the curve $f(\mathbb{F}_{q^m})$, which built off of Dedekind's zeta functions for Weil's insight, and Schmidt's work extending this to all algebraic curves over finite fields. The Weil conjectures generalized Artin's zeta function from curves to arbitrary non-singular,

projective varieties. This restriction to non-singular projective varieties is important, not only because it compactifies the space, but also because it becomes sensible to talk about differentials. This matters, because we can legitimately focus our attention on **étale maps**, which abstract the notion of local isomorphism and unramified field extensions,[4] and to the attendant étale sites and their cohomology theories. Indeed, this is where a seeming divergence between my interest in categorical logic and where the proof of the Weil conjectures properly begins.

However, this divergence is superficial, as it was eventually found that a *Weil cohomology theory*, which is contravariant functor satisfying certain axioms, would be sufficient for proving the Weil conjectures. One such Weil cohomology theory is ℓ-adic cohomology, an étale cohomology that Deligne used to prove the Weil conjecture's Riemann hypothesis analogue. The proof of the Weil conjecture is a consequence of the action of the geometric Frobenius mapping on this cohomology theory, as shown in an incredibly beautiful (if not maddeningly elegant) proof by induction on the dimension of non-singular projective varieties X.[5]

Thus, we have here, the structure of this paper writ small. We begin by considering what is meant by logic, before proceeding through some elementary topos to the category of sheaves on an étale site and some corresponding cohomology theories that allow us to prove the Weil conjectures.[7] If it is not yet clear, the personal motivation for this project stems from a desire to connect what I know about topos theory and categorical logic with their historical antecedent, the Weil conjectures, and if possible, sketch out how they can be proven within an appropriate syntactic category. To this end, I must explicitly state that this paper is a failure.

If the paper strikes the reader as schizophrenic in its goals and its exposition, that is because it has become so out of necessity. The single, intended throughline from elementary topoi to the proof of the conjectures was not fully realized. There are many reasons for this decision, the first being the pedagogical goal on my end to understand the Weil conjectures and their proof.

Of course, there were other, more quotidian, concerns about the length of the paper, which

[4]Not to omit a covering of a Riemann surface with no branch point, but introducing complex analysis this early on in the Foreword strikes me as losing focus on the proverbial plot.

[5]Indeed, the single largest section of the earlier drafts of this paper went to towards reproducing Deligne's proof of the Riemann hypothesis from [5] with inspiration[6] from the structure of the proof as presented in [14]. Once this paper grew to an unjustifiable length, it was eventually excised after many supporting details were removed. Ultimately, this author plans on releasing a series of separate (and hopefully shorter) papers to support a complete proof of this Riemann hypothesis analogue.

[7]I promise the reader that the Weil conjectures will be stated.

led to the further excision of a fairly lengthy subsection about which categories one expects to find generalized trace formula (much of this was a summary of [15]), as well as section summarizing [3], and the argument presented therein establishing an isomorphism between étale cohomology and ordinary sheaf cohomology. There were further casualties of the editing process, the most prominent being the omission of the proof of the Riemann hypothesis, leaving instead, a respectable summary of its proof.[8]

While I may regard this paper as a failure, both in its long term goal of providing a formally verified proof of the Weil conjectures, and even its more modest goal of providing a complete, consolidated proof of the Weil conjectures, what remains is a reasonably thorough survey of the material that in principle allows one to realize the proof of the Weil conjectures in some syntactic category. That is, what remains are some of the preliminary steps.

[8] I would actually argue that it is charitable to call what was present a proof, as most of the argument consisted of treating the specific results as black boxes, to be filled in after appropriately sifting through the relevant work in SGAs 4, 4 $\frac{1}{2}$, 5, and 7.

0.2 A Note on Reading This Paper

One of the biggest challenges reading through the literature is that there is no uniform notational standard. In one sense, this is not a bug of mathematics, but a central feature: the semantic content of mathematics is not a consequence of the notation. That said, good, consistent notation really does help immensely. To that end, certain decisions needed to be made so that a uniform presentation of the material can be achieved. Below is a table matching the type setting with a corresponding mathematical object:

Objects	Description	Examples
(Special) Sets	Blackboard bold	$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_\ell$, $\mathbb{F}_q$
$\{0, 1, 2, \ldots, n\}$	$\lceil n \rceil$	
Power-obect (incl. power sets)	$\mathtt{P}(-)$	$\mathtt{P}(\mathbb{R}), \mathtt{P}(X)$
Categories	Described by small caps	$\mathrm{C}, \textsc{Sets}, \textsc{Top}, \ldots$
Topoi (Abstract)[9]	Boldface	$\mathbf{B}, \mathbf{E}$
(Bi)-Functors (esp. sheaves)	Described by mathcal	$\mathcal{F}, \mathcal{G}, \mathcal{H}^q(-;-)$
limits / projective limits	$\varprojlim$	
co-limits / direct limits	$\varinjlim$	
Type theory	mathtt	$\mathtt{app}(s,t), \mathtt{fst}(z)$
Explicit Formula	mathtt	$\mathtt{dom}[X; f]$
Fibrations		$\begin{array}{cc} \mathrm{E} & \textsc{Sets}^{\to} \\ \downarrow & \downarrow \\ \mathrm{B}, & \Gamma : \textsc{Sets} \end{array}$
Unique morphism	!	

Ideally, notation eliminates ambiguity. However, the categories identified by $\textsc{PSh}(-)$ and $\textsc{Sh}(-)$ will need to be identified by the context.

Part I

Preliminaries

Chapter 1

Some Remarks On Categorical Logic

A caveat for the reader: the subject of categorical logic is far to expansive to be covered in any meaningful sense in a few pages. This chapter is intended to comprise a gentle introduction to the notion that fibrations over suitable categories are intimately connected to logic. In particular, the goal is to provide a minimal amount of exposition that would equip the reader to understand [16], and understand how one might approach the proof of the Weil Conjectures from the perspective of topos theory. Sadly, time and page constraints prevented a deep exposition topos theory, and so the connections that are drawn in this chapter aim to establish that at least any bicartesian closed category has a corresponding syntactical category with implication, conjunction and disjunction. These connections are particularly meaningful once we begin examining topoi proper, as topoi provide for us a rich, geometric logic. Much of this material is covered in greater detail in Chapters 1, 2, and 4 of [9]; Chapters 4 and 6 of [12]; the entirety of [13]; and [16].

1.1 Fibrations, Signatures, and Models

1.1.1 Fibrations, Signatures and Models

The main motivation for this section is to highlight the importance of fibrations for capturing information about slice categories, with the eventual goal of looking at sheaves over $\mathrm{E_T} \downarrow X$ where X is either a variety or a scheme. Towards that end, the importance of a fibred point of view of type theory will be developed first, with the aim of emphasizing that *contexts* are objects in the base category of a fibration, before we define the category of signatures.

Definition 1.1. Let E and B be categories and let $\mathcal{P} : \mathrm{E} \to \mathrm{B}$. Now suppose $f \in \mathrm{E}(X, Y)$ and $u \in \mathrm{B}(I, J)$. We say that f is **Cartesian over u** provided that $\mathcal{P}(f) = u$ and for every $g \in \mathrm{E}(Z, Y)$ such that there is some $w \in \mathrm{B}(\mathcal{P}(Z), I)$ satisfying

$$\mathcal{P}(g) = u \circ w$$

there is a uniquely determined $h \in \mathrm{E}(Z, X)$ with $f \circ h = g$.[1] If f is Cartesian over $\mathcal{P}(f)$, then we say f is **Cartesian**. If for every $Y \in \mathrm{Ob\ E}$ and $u \in \mathrm{B}(I, \mathcal{P}(Y))$, there is a Cartesian morphism $f \in \mathrm{E}(X, Y)$ above u, then $\mathcal{P}$ is a **fibration**. If $\mathcal{P}$ is a fibration, we will denote this by $\mathcal{P} : \begin{smallmatrix}\mathrm{E}\\ \downarrow \\ \mathrm{B}\end{smallmatrix}$.

Furthermore, given that $\mathcal{P}$ is a fibration, if $I \in \mathrm{Ob\ B}$, the **fibre category over I** (or **fibre**) is the category defined as follows:

objects $X \in \mathrm{Ob\ E}$ such that $\mathcal{P}(X) = I$;

morphisms $f \in \mathrm{E}(X, Y)$ such that $\mathcal{P}(f) = \mathrm{id}_I \in \mathrm{B}(I, I)$.

We denote this category by E_I, and by convention say that objects in E_I are **above I** and morphisms f are **above u**.

Finally, we can define a **category of fibrations**, Fib, as follows:

objects fibrations $\mathcal{P} : \begin{smallmatrix}\mathrm{E}\\ \downarrow \\ \mathrm{B}\end{smallmatrix}$;

[1] In this regard, $\mathcal{P}^*(w) = h$.

morphisms pairs of functors $(\mathcal{H} : \mathrm{B} \to \mathrm{A}, \mathcal{K} : \mathrm{E} \to \mathrm{D})$ such $\mathcal{Q}(\mathcal{H}) = \mathcal{K}(\mathcal{P})$ with $\mathcal{Q} : \overset{\mathrm{D}}{\downarrow}\mathrm{A}$, and $\mathcal{H}$ sending Cartesian morphisms in E to Cartesian morphisms in D.

Remark. Not surprisingly, we often refer to B as the base category and E as the total category.

Definition 1.2. Let B be a category with cartesian products.

We denote by $\mathrm{S}(\mathrm{B})$ a category whose objects are pairs (I, X) with $I, X \in \mathrm{Ob}\ \mathrm{B}$, and whose morphisms $(u, f) : (I, X) \to (J, Y)$ are pairs with $u \in \mathrm{B}(I, J)$ and $f \in \mathrm{B}(I \times X, Y)$, such that composition is defined as:

$$(v, g) \circ (u, f) := (v \circ u, g \circ \langle u \circ \pi, f \rangle)$$

The **simple fibration on B** is denoted by $\overset{\mathrm{S}(\mathrm{B})}{\downarrow}\mathrm{B}$ and is derived from the projection functor $\mathrm{S}(\mathrm{B}) \to \mathrm{B}$ given by $(I, X) \mapsto I$ and $(u, f) \mapsto u$.[2] Clearly, the fibre $\mathrm{S}(\mathrm{B})_I$ over $I \in \mathrm{Ob}\ \mathrm{B}$ and hence forms a slice category, referred to as the **simple slice**.

Now let B be a base category with cartesian products and pullbacks, and set the total category E to be the arrow category $\mathrm{B}^{\to}$. The **co-domain fibration** is a fibration $\mathtt{cod} : \overset{\mathrm{B}^{\to}}{\downarrow}\mathrm{B}$.[3] Clearly the fibre category of $I \in \mathrm{Ob}\ \mathrm{B}$ is the slice category $\mathrm{B} \downarrow I$, and the cartesian morphisms in $\mathrm{B}^{\to}$ coincide with pullback squares.[4]

Denote by $\textsc{Mono}(\mathrm{B})$ the full subcategory of $\mathrm{B}^{\to}$ whose objects are monic morphisms. The restricted codomain fibration is similarly a fibration, as the pullback of a monic arrow along any map is monic.

Within a fibre $\textsc{Mono}(\mathrm{B})_I$, we define a pre-order $\leq$ on $f : X \rightarrowtail I$ and $g : Y \rightarrowtail I$ by

$$f \leq g \iff \exists! h \in \mathrm{B}(X, Y), ((h \circ f) = g)$$

The resulting equivalence classes are called **subobjects** of I, and we denote this by $\mathrm{Sub}(I)$.[5]Thus, rather remarkably, while $\textsc{Mono}(\mathrm{B})$ is not a preorder, the fibration $\overset{\textsc{Mono}(\mathrm{B})}{\downarrow}\mathrm{B}$ is a pre-order as the

[2]That this functor forms a fibration is clear; given any $u \in \mathrm{B}(I, J)$, there is an obvious unique map from $(I, Y) \to (J, Y)$, namely, (u, π_2).

[3]Recall that `cod` is defined by $f \in \mathrm{B}(X, I) \mapsto I$ and $(u, f) \mapsto u$.

[4]Recall that morphisms in $\mathrm{B}^{\to}$ are pairs (u, v) such that $u \circ f = v \circ g$.

[5]Crucially, $\mathrm{Sub}(I)$ is a poset.

fibres are all pre-ordered categories.

Now, denote the category whose objects consist of $\mathrm{Sub}(I)$ by $\mathrm{Sub}(\mathrm{B})$. T From this, we derive the **fibration of subobjects of B**, $\begin{smallmatrix}\mathrm{Sub}_{(\mathrm{B})}\\ \downarrow \\ \mathrm{B}\end{smallmatrix}$.

Strictly speaking, there is no difference between subobjects and monic arrows from the categorical point of view. This perspective is actually quite fruitful, as the next two examples demonstrate.

Example 1.1.1. Let B be a category with finite limits, and let $I \in \mathrm{Ob}\ \mathrm{B}$. A **binary relation on I** is a subobject $R \rightarrowtail I \times I$. In this way, we can define the **category of binary relations on B**, $\textsc{Rel}(\mathrm{B})$ as the category whose objects are these monic arrows $r \in \mathrm{B}(R, I \times I)$ and whose morphisms $(R \rightarrowtail I \times I) \to (S \rightarrowtail J \times J)$ are derived from maps $u \in \mathrm{B}(I, J)$ such that there is a unique morphism $! : R \to S$

$$(u \times u) \circ r = s \circ !$$

Given that relations are monomorphisms whose target is a cartesian product, we often write $r := \langle r_1, r_2 \rangle$. Furthermore, in categories with cartesian products, we recover some common logical relations as follows:

reflexivity if $\delta_I = \langle \mathrm{id}_I, \mathrm{id}_I \rangle$ factors through $\langle r_1, r_2 \rangle$, then $\langle r_1, r_2 \rangle$ is **reflexive**;

symmetry if there is a unique map such that $\langle r_1, r_2 \rangle = \langle r_2, r_1 \rangle \circ !$, then $\langle r_1, r_2 \rangle$ is **symmetric**;

transitivity if there is a pullback T of triples,

$$\begin{array}{ccc} T & \xrightarrow{r_{23}} & R \\ {\scriptstyle r_{12}}\downarrow & & \downarrow{\scriptstyle r_1} \\ R & \xrightarrow[r_2]{} & I \end{array}$$

such that there is a unique map $! : T \to R$ such that

$$\begin{array}{ccc} T & \dashrightarrow & R \\ & {\scriptstyle t}\searrow \quad \swarrow{\scriptstyle \langle r_1, r_2 \rangle} & \\ & I \times I & \end{array}$$

with $t = \langle r_1 \circ r_{12}, r_2 \circ r_{23} \rangle$.

If a monomorphism $\langle r_1, r_2 \rangle$, satisfies all three of these, then it is an equivalence relation. Notably, if the diagonal fails to factor through, but symmetry and transitivity hold, then R is a partial equivalence relation.

Example 1.1.2. Define the category of predicates, denoted by $\textsc{Pred} = \mathrm{Sub}(\textsc{Sets})$. Then as before $\textsc{Pred}_I$ are fibre categories over I with a poset structure. Here, the partial ordering is the familiar $\subseteq$ ordering. In fact, each $\textsc{Pred}_I$ corresponds to the poset category of $\langle \mathtt{P}(I), \subseteq \rangle$. In particular, the morphisms in $\textsc{Pred}$ are functions $u :\in \mathrm{Hom}_{\textsc{Sets}}(I, J)$, such that $i \in X$ implies $u(i) \in Y$. For each such u, there is a corresponding substitution functor $u^* : \mathtt{P}(J) \to \mathtt{P}(I)$ in the reverse direction defined by

$$(Y \subseteq J) \mapsto (\{i \mid u(i) \in Y\} \subseteq I)$$

In this way, we define **weakening** as the case of substitution along the cartesian product $\pi : I \times J \to I$, and we define **contraction** along the Cartesian diagonal, $\delta : I \to I \times I$, with

$$\pi^* : \mathtt{P}(I) \to \mathtt{P}(I \times J)$$

by

$$X \mapsto \{(i, j) \mid i \in X, j \in J\}$$

and

$$\delta^* : \mathtt{P}(I \times I) \to I$$

by

$$X \mapsto \{i \in I \mid (i, i) \in X\}$$

respectively. Furthermore, we can define the **predicate of equality** on the cartesian product by

$$\mathtt{Eq}(X) = \{(i, j) \in I \times I \mid i = j, i \in X\}$$

or rather, as a functor $\mathtt{Eq} : \textsc{Sets} \to \textsc{Rel}$ by $I \mapsto \mathtt{I} = \{(i, i) \mid i \in I\}$. Further, we can define quotients

functorially as the left adjoint to equality.

Additionally, we can define quantification functorially from $\mathtt{P}(I \times j) \rightrightarrows \mathtt{P}(I)$ by the mappings

$$\exists : Y \mapsto \exists(Y) := \{i \in I \mid \exists j \in J.(i,j) \in Y\}$$

$$\forall : Y \mapsto \forall(Y) := \{i \in I \mid \forall j \in J.(i,j) \in Y\}$$

Finally, we can define **comprehension** as functor $\{-\} : \textsc{Sets} \to \textsc{Pred}$ by $(Y \subseteq J) \mapsto Y$, i.e.

$$\{(Y \subseteq J)\} = \{j \in J \mid j \in Y\} = Y$$

with "truth" as a functor $\top : \textsc{Sets} \to \textsc{Pred}$ as the suitable left-adjoint functor to comprehension, which is defined by sending sets I to the terminal object of the fibre $\textsc{Pred}_I$, namely, $(I \subseteq I)$.

This gives rise to the following adjoints:

$$\exists \dashv \pi^* \dashv \forall$$

$$\mathtt{Eq} \dashv \delta^*$$

$$\top \dashv \{-\}$$

$$\mathtt{Eq} \dashv \{-\}$$

$$\mathcal{Q} \dashv \mathtt{Eq}$$

In this light, we may regard the operations of predicate logic as structures of the fibration $\begin{smallmatrix}\textsc{Pred}\\ \downarrow \\ \textsc{Sets}\end{smallmatrix}$.

Remark. It bears mentioning after the previous example that there are several techniques for constructing new fibrations: pullbacks and composition. In particular, pullbacks of fibrations are occasionally referred to as a *change-of-base situation*, and can be used to define the category of signatures.[6] This is to stress that wherever fibrations arise, one will be able to find a logic. In the next section we will show how simple fibrations give rise to the simply typed λ-calculus. Similarly, one

[6] This is detailed in [9].

can show that the co-domain fibration corresponds to dependent type theory. Much of the rest of this paper is implicitly concerned with how the subobject fibrations describe an internal predicate logic.

Example 1.1.3. While much of this material can be found in Part D of [11], and can be interpolated from elsewhere, such as [1] and [13], I've found that [9] has the most concise presentation of categorical model theory from the perspective of fibrations, and in line with my goal of finding a *formally verified proof* of the Weil conjectures. The following definitions are largely summarized from Jacobs:

A **signature** Σ is a pair $(\mathtt{T}, \mathtt{F})$, where $\mathtt{T}$ is a set of **types** (alternately called **sorts**), and mapping $\mathtt{F} : \mathtt{T}^\star n \times \mathtt{T} \to \textsc{Sets}$ sending every $\langle \sigma_1, \ldots, \sigma_n \rangle \in \mathtt{T}^\star n$ and $\sigma_{n+1} \in \mathtt{T}$ to a set of function symbols $\mathtt{F}(\langle \sigma_1, \ldots, \sigma_n \rangle, \sigma_{n+1})$, which take inputs of type $\sigma_1, \sigma_2, \ldots, \sigma_n$ and output of type σ_{n+1}.[7] For each function symbol F in $\mathtt{F}(\langle \sigma_1, \ldots, \sigma_n \rangle, \sigma_{n+1})$ is said to be assigned **arity** $\sigma_1, \sigma_2, \ldots, \sigma_n \to \sigma_{n+1}$.

One often writes $|\Sigma|$ for the underlying set of types instead of $\mathtt{T}$; we will use this convention from here on out.. If $|\Sigma|$ has only one type, then the signature is **single typed**; otherwise, Σ is **multi-sorted**.

We define Sign to be the following category:

objects signatures Σ;

morphisms $(u, (f_\alpha)) : \Sigma \to \Sigma'$, where $u : |\Sigma| \to |\Sigma'|$ is a set function, and (f_α) is a family of functions between sets of function symbols with α indexed over all finite length pairs of $\langle \langle \sigma_1, \ldots, \sigma_n \rangle, \sigma_{n+1} \rangle$ such that

$$F : \sigma_1, \sigma_2, \ldots, \sigma_n \to \sigma_{n+1} \Rightarrow f_\alpha(F) : u(\sigma_1), \ldots, u(\sigma_n) \to u(\sigma_{n+1})$$

Clearly, we have an obvious forgetful functor Γ sending Σ to $|\Sigma|$ and morphisms to their underlying function u.

Definition 1.3. Given a signature Σ, we define the collection of **terms** recursively as follows:

1. if x is a variable of sort A, then $x : A$, ;

[7] For greater clarity, $\mathtt{T}^\star n$ refers to the free monoid of finite sequences of $\mathtt{T}$, the **Kleene star**.

2. if $f : A_1, \ldots, A_n \to B$ is a function symbol and $t_1 : A_1, \ldots, t_n : A_n$, then$f(t_1, \ldots, t_n) : B$.

Notice that we define the sort of each term A, and denote this by $t : A$.

Now, in order to associate terms with well-typed strings of symbols, when given a signature Σ, we note that a $|\Sigma|-$**indexed** collection of sets $X = (X_\sigma)_{\sigma \in |\Sigma|}$ can be regarded as a set of variables X_σ for each type in $|\Sigma|$, from which we can define a $|\Sigma|$-index collection of **terms**, $(\mathtt{Terms}_\tau(X))_{\tau \in |\Sigma|}$ as follows:[8]

- $X_\tau \subseteq \mathtt{Terms}_\tau(X)$, such that $\mathtt{Terms}_\tau(X)$ is the set of terms of type τ;
- if $F : \tau_1, \ldots, \tau_n \to \tau_{n+1}$ in Σ and $M_1 \in \mathtt{Terms}_{\tau_1}(X), \ldots, M_n \in \mathtt{Terms}_{\tau_n}(X)$, then

$$F(M_1, \ldots, F_m) \in \mathtt{Terms}_{\tau_{n+1}}(X)$$

In this way, a term is a well-typed string of variables $x \in \bigcup_{\sigma \in |\Sigma|} X_\sigma$ and functions F from $\mathtt{F}$. From here, we have a notion of **free variable**, given by $\mathtt{FV}(x) = \{x\}$ and $\mathtt{FV}(F(M_1, \ldots, M_n)) = \bigcup_{i=1}^{n} \mathtt{FV}(M_i)$. We also recover a notion of **substitution** for terms $y \in X_\tau$ and $N \in \mathtt{Terms}_\tau(X)$ with

$$x[N/y] = \begin{cases} N & x = y \\ x & otherwise. \end{cases}$$

$$F(M_1, \ldots, M_n)[N/y] = F(M_1[N/y], \ldots, M_n[N/y])$$

Given a signature Σ, a **model of** Σ is pair $((A_\sigma)_{\sigma \in |\Sigma|}, [\![-]\!])$, where $(A_\sigma)_{\sigma \in |\Sigma|}$ is a family of carrier sets with a collection of well-typed functions $[\![F]\!] : A_{\sigma_1} \times \cdots \times A_{\sigma_n} \to A_{\sigma_{n+1}}$. Crucially, $[\![-]\!]$ interprets function symbols $F : \sigma_1, \ldots, \sigma_n \to \sigma_{n+1}$ as actual functions. Given a collection X of variable sets $(X_\sigma)_{\sigma \in |\Sigma|}$, a **valuation** is a family $(\rho_\sigma : X_\sigma \to A_\sigma)_{\sigma \in |\Sigma|}$ consisting of functions assigning values in the model to variables, whence an **interpretation** consists of the family of functions

$$([\![-]\!]^\tau_\rho : \mathtt{Terms}_\tau(X) \to A_\tau)_{\tau \in |\Sigma|}$$

[8] Contrast this with how terms are inductively defined in classical model theory.

with $[\![x]\!]^\tau_\rho = \rho_\tau(x)$ for $x \in X_\tau$ and

$$[\![F(M_1, \ldots, M_n)]\!]^\tau_\rho = [\![F]\!]\left([\![M_1]\!]^\tau_\rho, \ldots, [\![M_n]\!]^\tau_\rho\right)$$

In this manner, we have a bijective correspondence between valuations and interpretations $\rho_\sigma \iff [\![-]\!]^\tau_\rho$. We are now equipped to define the category of set theoretic models, S-Model,

Objects triples of the $(\Sigma, (A_\sigma), [\![-]\!])$;

Morphisms pairs of the form $(\phi, (H_\sigma)) : (\Sigma, (A_\sigma), [\![-]\!]) \to (\Sigma', (A'_\sigma), [\![-]\!]')$ such that

- a signature morphism $\phi : \Sigma \to \Sigma'$
- a $|\Sigma|$-indexed collection of set functions $H_\sigma \in \mathrm{Hom}_{\textsc{Sets}}(A_\sigma, A'_{\phi\sigma})$ such that for each function symbol F in Σ,

$$\begin{array}{ccc} A_{\sigma_1} \times \cdots \times A_{\sigma_n} & \xrightarrow{H_{\sigma_1} \times \cdots \times H_{\sigma_n}} & A'_{\phi(\sigma_1)} \times \cdots \times A'_{\phi(\sigma_n))} \\ \Big\downarrow [\![F]\!] & & \Big\downarrow [\![\phi(F)]\!]' \\ A_{\sigma_{n+1}} & \xrightarrow[H_{\sigma_{n+1}}]{} & A'_{\phi(\sigma_{n+1})} \end{array}$$

commutes

The key take-away here is that there are two useful fibrations: $\overset{\text{S-Model}}{\downarrow}{}_{\textsc{Sign}}$ defined by the functor which sends a model to it's underlying signature, and whose fibre over $\Sigma \in \mathrm{Ob}\ \textsc{Sign}$ is the category of models with signature Σ; and one $\overset{\text{S-Model}}{\downarrow}{}_{\textsc{Sets}}$ defined by taking a model to its underlying set of types, whose fibre over $|\Sigma|$ is the category of models of signatures with $|\Sigma|$ as a set of types.

Remark. Rather remarkably, for any Σ and a category B with finite products, a **model of Σ in B** is a functor $\mathcal{M} : \textsc{Cl}(\Sigma) \to \mathrm{B}$ that preserves products, from which we can realize the category of Σ models in B as the subcategory of the hom-category $\textsc{Cat}(\textsc{Cl}(\Sigma), \mathrm{B})$, or rather, $\mathrm{FP}\textsc{Cat}(\textsc{Cl}(\Sigma), \mathrm{B})$, where $\mathrm{FP}\textsc{Cat}$ is the category of categories with finite products.

1.1.2 The Syntax of Calculi of Types And Terms

Now, stepping back from the point of view that has various collections $(X_\sigma)_{\sigma\in|\Sigma|}$ as variables which are already typed such that they form a parameter,[9] we can instead fix the set of variables in advance, much in the same way we may consider a fibre in a fibration.

Definition 1.4. Given a signature Σ, we define the **term calculus** with a denumarably infinite set of variables $\{v_1, v_2, \ldots\}$ as follows:

A **context** Γ is a finite sequence of variable declarations, i.e.

$$\Gamma \equiv (v_1 : \sigma_1, \ldots, v_n : \sigma_n)$$

such that two contexts concatenate with commas, i.e.

$$\Gamma, \Delta \equiv (v_1 : \sigma_1, \ldots, v_n : \sigma_n), (v_{n+1} : \tau_{n+1}, \ldots, v_{n+m} : \tau_{n+m}) \equiv (v_1 : \sigma_1, \ldots, v_n : \sigma_n, v_{n+1} : \tau_{n+1}, \ldots, v_{n+m} : \tau_{n+m})$$

Identity $\dfrac{}{v_1 : \sigma \vdash v_1 : \sigma}$

Function symbol For function symbols $F : \sigma_1, \ldots, \sigma_n \to \sigma_{n+1}$ in Σ, $\dfrac{\Gamma \vdash M_1 : \sigma_1 \qquad \cdots \qquad \Gamma \vdash M_n : \sigma_n}{\Gamma \vdash F(M_1, \ldots, M_n) : \sigma_{n+1}}$

Weakening $\dfrac{v_1 : \sigma_1, \ldots, v_n : \sigma_n \vdash M : \tau}{v_1 : \sigma_1, \ldots, v_n : \sigma_n, v_{n+1} : \sigma_{n+1} \vdash M : \tau}$

Contraction $\dfrac{\Gamma, v_n : \sigma_n, v_{n+1} : \sigma_{n+1} \vdash M : \tau}{\Gamma, v_n : \sigma_n \vdash M : \tau}$

Exchange $\dfrac{\Gamma, v_n : \sigma_n, v_{n+1} : \sigma_{n+1}, \Delta \vdash M : \tau}{\Gamma, v_n : \sigma_{n+1}, v_{n+1} : \sigma_n, \Delta \vdash M[v_n/v_{n+1}, v_{n+1}/v_n] : \tau}$

These five rules form the term calculus of a signature Σ; notably, the final three rules are the structural rules.[10] From the term calculus for Σ, we define the **classifying category** (or **term model**) as the following category:

objects contexts Γ, which are variable declarations of the form:

[9] This is the perspective borrowed from universal algebra.

[10] *Notation.* For readers unfamiliar with proof theory and type theory, $v_1 : \sigma_1$ is read as v_1 witness σ_1 and $\Gamma \vdash M : \tau$ expresses that M is a term of type τ in context Γ.

morphisms With $\Delta = (\tau_1, \ldots, \tau_n)$, n-tuples $(M_1, \ldots, M_n) : \Gamma \to \Delta$ for which we can derive $\Gamma \vdash M_i : \tau_i$. Particularly, the identity morphism on Γ is simply the collection of variables in Γ, and the composition of context morphisms

$$(L_1, \ldots, L_k) = (N_1, \ldots, N_k) \circ (M_1, \ldots, M_m)$$

by simultaneous substitution:

$$L_i = N_i[M_1/v_1, \ldots, M_m/v_m]$$

with associativity of composition preserved by

$$M[N/v_n][L/v_m] \equiv M[N[L/v_m]v_n]$$

for v_m not free in M.

We denote the classifying category by $\textsc{Cl}(\Sigma)$. This is our first syntactically defined category.

Crucially, the classifying category $\textsc{Cl}(\Sigma)$ has finite products. This can quickly be checked by noting that $\emptyset$ is a terminal object, as there is only one morphism from $\Gamma \to \emptyset$, namely the empty sequence for any context Γ. Similarly, concatenation of contexts by commas gives rise to the obvious projection morphisms, i.e.

$$\Gamma \xleftarrow{(v_1,\ldots,v_n)} \Gamma, \Delta \xrightarrow{(v_{n+1},\ldots,v_{nm})} \Delta$$

1.1.3 A Few Remarks on Formula

Although now we have a calculus for terms, we do not have a means of denoting predicates. For this, we'll need *formulae*. In the interest of being exhaustive, the following definition will be used to define many different classes of formula.

Definition 1.5. We recursively define a class Fr of **formulae** over Σ as follows:

Truth $\top \in Fr$. Importantly, $\texttt{FV}(\top) = \emptyset$.

Falsity $\bot \in Fr$. Importantly, $\texttt{FV}(\bot) = \emptyset$.

Relations If $t_1 : A_1, \ldots, t_n : A_n$ are terms, and $R \rightarrowtail A_1 \cdots A_n$ is a relation symbol, then $R(t_1, \ldots, t_n) \in Fr$.

Equality If $s : A$ and $t : A$, then $(s =_A t) \in Fr$. Importantly, $\texttt{FV}(s =_A t)$ is the set of variables occurring in both s or t.

Binary Conjunction[11] If $\phi, \psi \in Fr$, then $(\phi \wedge \psi) \in Fr$. Importantly, $\texttt{FV}(\phi \wedge \psi) = \texttt{FV}(\phi) \cup \texttt{FV}(\psi)$. Notably, we will see that binary conjunction corresponds to the notion of products types.

Binary Disjunction[12] If $\phi, \psi \in Fr$, then $(\phi \vee \psi) \in Fr$. Importantly, $\texttt{FV}(\phi \vee \psi) = \texttt{FV}(\phi) \cup \texttt{FV}(\psi)$. Notably, we will see that binary disjunction corresponds to the notion of co-product types.

Implication If $\phi, \psi \in Fr$, then $(\phi \Rightarrow \psi) \in Fr$. Importantly, $\texttt{FV}(\phi \Rightarrow \psi) = \texttt{FV}(\phi) \cup \texttt{FV}(\psi)$. Notably, we will see that implication corresponds to $\rightarrow$ types.

Negation If $\phi \in Fr$, then $\neg\phi \in Fr$. Importantly, $\texttt{FV}(\neg\phi) = \texttt{FV}(\phi)$.

Universal Quantification If $x : A$ and $\phi \in Fr$, then $(\forall x : A)\phi$.[13] Importantly, $\texttt{FV}((\forall x : A)\phi) = \texttt{FV}(\phi)\backslash\{x\}$. We will not have time to go into $\prod-$types (dependent function types) in detail, however, we have the following type former rules for the $\prod$-type:[14]

$\prod$-Formation $$\frac{\Gamma \vdash A : \Sigma \qquad \Gamma, x : A \vdash B : \Sigma}{\Gamma \vdash \prod\limits_{(x:A)} B : \Sigma}$$

$\prod$-Introduction $$\frac{\Gamma, x : A \vdash b : B}{\Gamma \vdash \lambda(x : A).b : \prod\limits_{(x:A)} B}$$

$\prod$-Elimination $$\frac{\Gamma \vdash f : \prod\limits_{x:A} B \qquad \Gamma \vdash a : A}{\Gamma \vdash f(a) : B[a/x]}$$

$\prod$-Computation $$\frac{\Gamma, x : A \vdash b : B \qquad \Gamma \vdash a : A}{\Gamma \vdash (\lambda(x : A).b)(a) \equiv b[a/x] : B[a/x]}$$

$\prod$-Uniqueness Principle $$\frac{\Gamma \vdash f : \prod\limits_{(x:A)} B}{\Gamma \vdash f \equiv (\lambda x.f(x)) : \prod\limits_{(x:A)} B}$$

[13] If we happen to be working with a single sort, then $\forall x$ is appropriate.
[14] Notably, we've condensed β, η rules into a *computation* rule.

Both the expression $\lambda(x : A).b$ and $\prod_{(x:A)} B$ bind free occurences of x in b and B respectively. The reader is advised to keep in mind that if x does not occur freely in B so tha tB does not depend on A, we recover the ordinary function type $A \to B$.

Existential Quantification If x is a variable, and $\phi \in Fr$, then $(\exists x)\phi$. Importantly, $\mathtt{FV}((\exists x)\phi) = \mathtt{FV}(\phi)\backslash\{x\}$. We will not have time to go into $\sum-$types (dependent pair types) in detail, however the type former rules for Σ are:

$\sum$-Formation $$\frac{\Gamma \vdash A : \Sigma \qquad \Gamma, x : A \vdash B : \Sigma}{\Gamma \vdash \sum_{(x:A)} B : \Sigma}$$

$\sum$-Introduction $$\frac{\Gamma, x : A \vdash B : \Sigma \qquad \Gamma \vdash a : A \qquad \Gamma \vdash b : B[a/x]}{\Gamma \vdash (a, b) : \sum_{(x:A)} B}$$

$\sum$-Elimination $$\frac{\Gamma, z : \sum_{(x:A)} B \vdash C : \Sigma \qquad \Gamma, x : A, y : B \vdash g : C[(x, y)/z] \qquad \Gamma \vdash p : \sum_{x:A} B}{\Gamma \vdash \mathtt{ind}_{\sum_{(x:A)} B}(z.c, x.y.g, p) : C[p/z]}$$

$\sum$-Computation [15]

$$\frac{\Gamma, z : \sum_{(x:A)} B \vdash C : \Sigma \qquad \Gamma, x : A, y : B \vdash g : C[(x, y)/z] \qquad \Gamma \vdash a' : A \qquad \Gamma \vdash b' : B[a'/x]}{\Gamma \vdash \mathtt{ind}_{\sum_{(x:A)} B}(z.C, x.y.g, (a', b') \equiv g[a', b'/x, y] : C[(a', b')/z]}$$

Infinitary Disjunction If I is a set, $\phi_i \in Fr$ for each $i \in I$ and $\bigcup_{i \in I} \mathtt{FV}(\phi_i)$ is finite, then $\bigvee_{i \in I} \phi_i \in Fr$.

Infinitary Conjunction If I is a set, $\phi_i \in Fr$ for each $i \in I$ and $\bigcup_{i \in I} \mathtt{FV}(\phi_i)$ is finite, then $\bigwedge_{i \in I} \phi_i \in Fr$.

These define the following classes of formulae:

Atomic Formulae The smallest set of formulae closed under relations and equality.

Horn Formulae The smallest set of atomic formulae closed under truth and binary conjunction.

Regular Formulae The smallest set of Horn formulae closed under existential quantification.

[15] We call $\mathtt{ind}_{\sum_{(x:A)} B}$ the induction function for dependent pair types. Importantly, $\sum_{(x:A)} B$ binds free occurrences of x in B, although $\mathtt{ind}_{\sum_{(x:A} B}$ has some arguments with free variables beyond those in Γ. When B does not contain free occurrences of x, we find a special case of the cartesian product type former $A \times B$.

Coherent Formulae The smallest set of regular formulae closed under falsity and binary disjunction.

First Order Formulae The smallest set of coherent formulae closed under implication, negation, and universal quantification.

Geometric Formulae The smallest class of coherent formulae closed under infinitary disjunction.

Infinitary First Order Formulae The smallest class of first order formulae closed under infinitary conjunction and disjunction.

1.2 Functorial Semantics in Bicartesian Closed Categories

One of the chief goals of this section is to convince readers that putting a reasonably expressive logic on a type theory amounts to putting a pre-order fibration on a structure. In part, the idea to keep in mind is that the base category of a fibration consists of contexts and the fibre above a context is what is derivable from that context. Throughout, it should suffice to consider the simple fibration mentioned in Section 1.1. Due to (page)-spatio-temporal constraints, the full line from the Grothendieck topoi invoked in the Weil conjectures to a type theory captured by a big topos has not been built. Instead, for any signature Σ, we will construct a simply typed lambda calculus corresponding to bicartesian closed categories that possesses some of the features we want, namely: conjunction, disjunction and implication. Afterwards, a brief sketch of what we mean by propositions and theories will be provided.

Definition 1.6. Given a signature Σ, the **simply typed λ-calculus** $\lambda 1_{(\times,+)}(\Sigma)$ is defined by the following rules:

$\sigma \in |\Sigma|$ **Formation** $\dfrac{}{\vdash \sigma : \mathtt{Type}}$

0**-Formation** $\dfrac{}{\vdash 0 : \mathtt{Type}}$

1**-Formation** $\dfrac{}{\vdash 1 : \mathtt{Type}}$

$\to$**-Formation** $\dfrac{\vdash \sigma : \mathtt{Type} \qquad \vdash \tau : \mathtt{Type}}{\vdash \sigma \to \tau : \mathtt{Type}}$

$+$**-Formation** $\dfrac{\vdash \sigma : \mathtt{Type} \qquad \vdash \tau : \mathtt{Type}}{\vdash \sigma + \tau : \mathtt{Type}}$

$\times$**-Formation** $\dfrac{\vdash \sigma : \mathtt{Type} \qquad \vdash \tau : \mathtt{Type}}{\vdash \sigma \times \tau : \mathtt{Type}}$

1**-Introduction** $\dfrac{}{\vdash \mathtt{tt} : 1}$

$\to$**-Introduction** $\dfrac{\Gamma, v : \sigma \vdash M : \tau}{\Gamma \vdash (\lambda(v : \sigma).M) : \sigma \to \tau}$

$+_L$**-Introduction** $\dfrac{\Gamma \vdash M : \sigma}{\Gamma \vdash \mathtt{inl}(M) : \sigma + \tau}$

$+_R$**-Introduction** $\dfrac{\Gamma \vdash N : \tau}{\Gamma \vdash \mathtt{inr}(N) : \sigma + \tau}$

$\times$**-Introduction** $\dfrac{\Gamma \vdash M : \sigma \qquad \Gamma \vdash N : \tau}{\Gamma \vdash \langle M, N \rangle : \sigma \times \tau}$

0**-Elimination** $\dfrac{}{\Gamma, z : 0 \vdash \{\} : \rho}$

$\rightarrow$**-Elimination** $\dfrac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash MN : \tau}$

$+$**-Elimination** $\dfrac{\Gamma \vdash P : \sigma + \tau \qquad \Gamma, x : \sigma \vdash Q : \rho \qquad \Gamma, y : \tau \vdash R : \rho}{\mathtt{match}(P, \mathtt{inl}(x).Q, \mathtt{inr}(y).R) : \rho}$

$\times_L$**-Elimination** $\dfrac{\Gamma \vdash P : \sigma \times \tau}{\Gamma \vdash \mathtt{fst}(P) : \sigma}$

$\times_R$**-Elimination** $\dfrac{\Gamma \vdash P : \sigma \times \tau}{\Gamma \vdash \mathtt{snd}(P) : \tau}$

Term Calculus These are simply the rules given in Definition 1.3.

Importantly, this is a λ-calculus with exponent, finite co-product, and finite product types built from the signature Σ, with 0 referring to the empty co-product type and 1 referring to the empty product type. Tellingly, we call constructor of the exponent type $\sigma \to \tau$ a **λ-expression**. Significantly, the introduction rules introduce co-projections $\mathtt{inl}(-), \mathtt{inr}(-)$ and projections $\mathtt{fst}(-), \mathtt{snd}(-)$. Additionally, $\mathtt{match}(P, \mathtt{inl}(x).Q, \mathtt{inr}(y).R)$ can be read as follows: given P witnesses $\sigma + \tau$, if P witnesses σ, then do Q with P for variable x; else if P witnesses τ, do R with P for y.[16] Before verifying that the corresponding classifying category for this calculus is bicartesian closed, we will need to introduce the following conversion rules so that we have an appropriate notion of computation:

β**-reduction,** $\to$ $\dfrac{\Gamma, v : \sigma \vdash M : \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash (\lambda v : \sigma.M)N =_\beta M[N/v] : \tau}$

η**-conversion,** $\to$ $\dfrac{\Gamma \vdash M : \sigma \to \tau}{\Gamma \vdash \lambda v : \sigma.Mv =_\eta M : \sigma \to \tau}$

β**-reduction,** 0 $\dfrac{\Gamma, z : 0 \vdash M : \rho}{\Gamma, z : 0 \vdash M =_\beta \{\} : \rho}$

β**-reduction,** 1 $\dfrac{\Gamma \vdash M : 1}{\Gamma \vdash M =_\beta \mathtt{tt} : 1}$

β**-reduction,** $+_L$ $\dfrac{\Gamma \vdash P : \sigma + \tau \qquad \Gamma, x : \sigma \vdash Q : \rho \qquad \Gamma, y : \tau \vdash R : \rho}{\Gamma \vdash \mathtt{match}(\mathtt{inl}(M), \mathtt{inl}(x).Q, \mathtt{inr}(y).R) =_\beta Q[M/x] : \rho)}$

β**-reduction,** $+_R$ $\dfrac{\Gamma \vdash P : \sigma + \tau \qquad \Gamma, x : \sigma \vdash Q : \rho \qquad \Gamma, y : \tau \vdash R : \rho}{\Gamma \vdash \mathtt{match}(\mathtt{inr}(M), \mathtt{inl}(x).Q, \mathtt{inr}(y).R) =_\beta Q[N/y] : \rho)}$

[16] [9] actually identifies $\mathtt{match}$ with $\mathtt{unpack} - \mathtt{as}[\iota_l \mathtt{in} Q, \iota_r \mathtt{in} R]$. In any case, perspicacious readers will get that this is disjunctive.

$$\eta\textbf{-conversion, } + \quad \frac{\Gamma \vdash P : \sigma + \tau \qquad \Gamma, z : \sigma + \tau \vdash R : \rho}{\mathtt{match}(P, \mathtt{inl}(x).R[(\mathtt{inl}(x)/z)], \mathtt{inr}(y).R[\mathtt{inr}(y)/z]) =_\eta R[P/z] : \rho}$$

$$\beta\textbf{-reduction, } \times_L \quad \frac{\Gamma \vdash M : \tau \qquad \Gamma \vdash N : \tau}{\Gamma \vdash \mathtt{fst}(\langle M, N\rangle) =_\beta M : \sigma}$$

$$\beta\textbf{-reduction, } \times_R \quad \frac{\Gamma \vdash M : \tau \qquad \Gamma \vdash N : \tau}{\Gamma \vdash \mathtt{snd}(\langle M, N\rangle) =_\beta N : \tau}$$

$$\eta\textbf{-conversion, } \times \quad \frac{\Gamma \vdash P : \sigma \times \tau}{\Gamma \vdash \langle \mathtt{fst}(P), \mathtt{snd}(P)\rangle =_\eta P : \sigma \times \tau}$$

It warrants mentioning that the β-conversion consists of rules specifies applying the elimination rule to the introduction rule,[17] generating an equivalence relation called the β-equivalence. In some dual sense, η-reduction applies an introduction rule to the elimination rule, generating an equivalence relation called the η-equivalence. Here on out, we use $\equiv$ to denote this equivalence, with the caveat that this should which should not be confused with the judgmental equivalence $\equiv$ occurring at the level of syntax.

We now have a **syntactically constructed category** $\textsc{Cl}1_{(+,\times)}(\Sigma)$ called the $\lambda 1_{(+,\times)}$-classifying category of Σ defined as follows:

objects Contexts Γ;

morphisms with $\Delta = (v_1 : \tau_1, \ldots, v_m : \tau_m)$, morphisms are m-tuples $([M_1], \ldots, [M_m]) : \Gamma \to \Delta$ of equivalence classes of terms M_i such that $\Gamma \vdash M_i : \tau_i$ in $\lambda 1_{+,\times}(\Sigma)$.

Crucially, $\lambda 1_{+,\times}$ is a type theory that allows us to describe the application of a *function* $M : \sigma \to \tau$. Particularly, this corresponds to the categorical notion of exponentials, which the reader can recall are right adjoints to the functor $A \times (-)$, whose co-unit is the evaluation function. This is made explicit by the following proposition:

Proposition 1. $\textsc{Cl}1_{+,\times}(\Sigma)$ *is bicartesian closed.*

Proof. This amounts to verifying the following claims:

Claim 2. *The empty type* 0 *is an initial object.*

[17] In the case of $\to$, this amounts to the evaluation of a function on an argument, and belying the λ-calculus. In a dual sense, the η-reduction of $\to$ corresponds to the extensionality of functions.

Proof. Given the elimination rule, for any type σ, we have $z : 0 \vdash \{\} : \sigma$.

To see the uniqueness up to isomorphism, consider the η-reduction applied to $z : 0 \vdash M : \sigma$, whence we find $z : 0 \vdash M =_\eta \{\} : \rho$. Since this rule demonstrates that in a context where the empty type is inhabited, any term M is necessarily convertible to the empty type. In this way, we find that $[M] \cong [\{\}] : 0 \to \sigma$, whence 0 is an initial object. □

Claim 3. *The unit type* 1 *is a terminal object.*

Proof. This is given by the formation and introduction rules; namely, any context will yield $x : \sigma \vdash \mathtt{tt} : 1$. Under the β-conversion, we see that if $x : \sigma \vdash M : 1$, then $x : \sigma \vdash M =_\beta \mathtt{tt} : 1$, whence $[M] \cong [\mathtt{tt}] : \sigma \to 1$. □

Claim 4. *The arrow type (or more properly, exponent type)* $\sigma \to \tau$ *is the exponential object in* $\textsc{Cl}1_{+,\times}(\Sigma)$

Proof. Given a term $z : \sigma \times \tau \vdash M : \tau$, we have an arrow $\sigma \times \tau \to \rho$ from which we can form the λ-abstraction term

$$x : \sigma \vdash \lambda(y : \tau).M[\langle x, y\rangle / z] : \tau \to \rho$$

From this, we have the categorical abstraction

$$\Lambda([M]) \cong [\lambda(y : \tau).M[\langle x, y\rangle / z]] : \sigma \to (\tau \to \rho)$$

Furthermore, we can define the co-unit (the evaluation morphism) from terms

$$w : (\tau \to \rho) \times \tau \vdash (\mathtt{fst}(w))(\mathtt{snd}(w)) : \rho$$

$$ev :\equiv [(\mathtt{fst}(w))(\mathtt{snd}(w))] : (\tau \to \rho) \times \tau \to \rho$$

A verification that the categorical β and η conversions following from the syntactic conversions can be found in [9]. □

Claim 5. *The co-product type* $\sigma + \tau$ *is a co-product object.*

Proof. Given terms $x : \sigma \vdash \mathtt{inl}(x) : \sigma+\tau$ and $y : \tau \vdash \mathtt{inr}(y) : \sigma+\tau$, we have our obvious coprojection maps $\iota_l : \sigma \to \sigma + \tau$ and $\iota_r : \tau \to \sigma + \tau$. Then, for any pair of terms $x : \sigma \vdash Q : \rho$ and $y : \tau \vdash R : \rho$, we have a pair of morphisms $\sigma \to \rho$ and $\tau \to \rho$, such that we have our cotuple morphism $\sigma + \tau \to \rho$ given by matching, i.e.

$$z : \sigma + \tau \vdash \mathtt{match}(z, \mathtt{inl}(x).Q, \mathtt{inr}(y).R) : \rho$$

with the isomorphisms arising through application of our β and η rules. □

Claim 6. *The product type $\sigma \times \tau$ is a product object.*

Proof. Using $\times-$introduction and elimination, we have for $t : \rho \vdash x : \sigma$ and $t : \rho \vdash y : \tau$,

$$t : \rho \vdash \langle x, y \rangle : \sigma \times \tau$$

giving us maps $\rho \to \sigma$, $\rho \to \tau$ and $\rho \to \sigma \times \tau$. Furthermore, our respective projection morphisms are given by $\mathtt{fst}(\langle x, y \rangle)$ and $\mathtt{snd}(\langle x, y \rangle)$, so that we have $t : \rho \vdash x =_\beta \mathtt{fst}(\langle x, y \rangle) : \sigma$ (and similarly for our second projection). □

Thus, we find that $\textsc{Cl}1_{+,\times}(\Sigma)$ is a bicartesian closed category. Importantly, this means that $\lambda 1_{(+,\times)}$-calculi can be interpreted in bicartesian closed categories. □

At this point, some clarification of terminology is in order:

Definition 1.7. A **sequent** over a signature Σ is a formal expression of the form

$$\phi \vdash_\Gamma \psi$$

where ϕ, ψ are formula over Σ and Γ is a context such that any assignment of individual values to variables in Γ which make ϕ true also make ψ *true*. Notably, a sequent is regular if both formula are regular, coherent if both formula are coherent, etc. A **theory** over a signature Σ is a set $\mathbb{T}$ of sequents over Σ whose elements are the **axioms** of $\mathbb{T}$.

An **algebraic theory** is a theory whose signature has a single sort and no relation symbols apart from logical equality, such that the axioms are of the form $(\top \vdash_\Gamma \phi)$, where $\phi \equiv (s = t)$ and

Γ is the canonical context of ϕ.

Example 1.2.1. We can describe the theory of local rings with coherent theories as follows:

- $((0 = 1) \vdash_{[]} \bot)$;
- $((\exists z)(x + y)z = 1) \vdash_{x,y} ((\exists z)(xz = 1) \vee (\exists z)(yz = 1)))$.

Remark. The first thing to remark upon is that unlike the $\lambda 1$ classifying category from the previous section, the classifying category we just described takes equivalence classes of terms instead of the terms themselves as the constituent of context morphisms. In both cases, we are transforming contexts, which seems like a basic pre-requisite for any deductive system. Of course, we have just constructed a syntactic category that allows for conjunction, disjunction and implication, as well as some notion of truth and falsity, but we do not yet have a clear idea of *propositions*.

To rectify this, a brief sketch of the **propositions-as-types** paradigm is in order. We will need to be explicit about the logic we're working with. Due to the aforementioned spatio-temporal constraints, we'll consider the **minimal intuitionistic logic** for our purposes, which arises when working with the term calculus and rules associated with the arrow type $\rightarrow$ (so for the time being, no notion of truth, falsity, conjunction or disjunction). Given a signature Σ, consider T the formal closure of $|\Sigma|$ under the $\rightarrow$.[18] For $\sigma_1, \ldots, \sigma_n, \tau \in T$, we write

$$\triangle\sigma_1, \ldots, \sigma_n \vdash_{\mathtt{MIL}} \tau$$

if τ is derivable from the assumptions $\sigma_1, \ldots, \sigma_n$ using the $\rightarrow$ introduction and elimination rules. Now, we let $\mathtt{A}$ be some collection of sequents $\sigma_1, \ldots, \sigma_n \vdash \tau$ with $\sigma_i, \tau \in |\Sigma|$. For each $S \in \mathtt{A}$, there is a formation rule,

$$\frac{}{\mathrm{S}}$$

Not surprisingly, we regard the sequents of $\mathtt{A}$ as **axioms**, expressing that S is derivable in any context (which is about as good a working definition of axiom as one can hope for). With some work, this paradigm can be extended to an intuitionistic logic with a $\lambda 1_{(+,\times)}$ calculus. For now we see that for

[18] This simply means what you'd expect: $|\Sigma| \subseteq T$ and if $\sigma, \tau \in T \Rightarrow (\sigma \rightarrow \tau) \in T$.

any Σ, $\mathrm{CL1}_{+,\times}(\Sigma)$ is an object in the category of bicartesian closed categories, denoted by BiCCC. Given an earlier remark, we say that a **model for the** $\lambda 1_{+,\times}(\Sigma)$ in a bicartesian closed category A is a functor $\mathcal{M} : \mathrm{CL1}_{+,\times}(\Sigma) \to \mathrm{A}$. This just generalizes the notion we had earlier (to see how, note that Sets is bicartesian closed). In the case of $\lambda 1_{+,\times}$ coupled with $\prod$ and $\sum$ types, we have the following dictionary:

English	Type Theory
True	1
False	0
A and B	$A \times B$
A or B	$A + B$
If A, then B	$A \to B$
A if and only if B	$(A \to B) \times (B \to A)$
Not A	$A \to 0$
For all $x : A$, $P(x)$ holds	$\prod_{(x:A)} P(x)$
There exists $x : A$ such that $P(x)$	$\sum_{(x:A)} P(x)$

Table 1.1: Handy Logical Dictionary

Importantly, this dictionary establishes that the $\lambda 1_{+,\times}$ calculi is strong enough to provide us propositional logic, and when coupled with the $\prod$ and $\sum$ type formers, predicate logic. In the case of predicate logics, a predicate P over a type A is a family $P : A \to \mathcal{U}$, where $\mathcal{U}$ is our type universe, and P assigns all witnesses to A to a type $P(a)$. It is precisely this translation that gives rise to the propositions-as-types paradigm, as one (not so) simply translates propositions and their proofs into types and their elements. Crucially though, this is an intuitionistic logic, and as such, it does not include classical logical principles such as the law of excluded middle or proofs by contradiction, nor does it rule them out. As a computational logic, type theory provides axiomatic freedom, which means that we can incorporate axioms into the definition of types using the $\sum$ type former. For instance, we define `Monoid` as a type A equipped with a binary operation $m : A \to A \to A$ as follows:[19]

$$\sum_{(A:\mathcal{U})} \sum_{(m:A\to A\to A)} \Big(\prod_{(x:A)} \prod_{(y:A)} \prod_{(z:A)} (m(x, m(y, z)) = m(m(x, y), z)) \times \Big(\sum_{(e:A)} \prod_{(x:a)} ((m(x, e) = m(e, x)) \times (m(x, e) = x))\Big)$$

[19]Given an inhabitant of this type, by applying the appropriate projections, we can extract the carrier A, the operation m, and a witness of either axiom.

1.3 Elementary Topoi

We begin our discussion by defining a particular kind of adjoint functor.

Definition 1.8. A **geometric morphism** $f : \mathbf{E} \to \mathbf{F}$ is an adjoint pair of functors $f^* \dashv f_* : \mathbf{E} \to \mathbf{F}$, such that f^* is left-exact. We call f_* the **direct image** of f and f^* the **inverse image** of f.

Geometric morphisms are morphisms over a very special kind of category called a **topos**.

Definition 1.9. An **elementary topos** is a category $\mathbf{E}$ which

1. is a bicartesian closed category;
2. has an object $\Omega \in \mathrm{Ob}\ \mathbf{E}$, with a map $\top : 1 \to \Omega$ called the **subobject classifier**, which is a pointed object classifying monomorphisms, along with a morphism $\mathtt{P}(-)$ which assigns to each object $X \in \mathrm{Ob}\ \mathbf{E}$ an object $\mathtt{P}(X) \in \mathrm{Ob}\ \mathbf{E}$, where $\mathtt{P}(X)$ is called the **power object of X**, which can be thought of as a generalization of the power set construction in set theory;
3. the functors $\mathrm{Sub}_{\mathbf{E}}(-)$ and $\mathrm{Hom}_{\mathbf{E}}(Y \times -, \Omega)$ such that for each object $X \in \mathrm{Ob}\ \mathbf{E}$, we have two natural isomorphisms $\mathrm{Sub}_{\mathbf{E}} X \cong \mathrm{Hom}_{\mathbf{E}}(X, \Omega)$ and $\mathrm{Hom}_{\mathbf{E}}(Y \times X, \Omega) \cong \mathrm{Hom}_{\mathbf{E}}(X, \mathtt{P}(Y))$.

Example 1.3.1. The canonical example of a topos is the category of sets, Sets, where the subobject classifier consists of the characteristic functions and $\Omega = \{0, 1\}$ such that

$$\begin{array}{ccc} a & \overset{f}{\rightarrowtail} & d \\ {\scriptstyle !}\downarrow & & \downarrow{\scriptstyle \chi_f} \\ 1 & \underset{\top}{\longrightarrow} & \Omega \end{array}$$

commutes.

We also recognize that $\bot : 1 \to \Omega$ is defined by $\bot(*) = 0$. Now, since $\bot : 1 \to \Omega$ is a unique arrow, we can recognize this as the characteristic function defining a subobject classifier for some monic arrow. In this case, the characteristic function is of the unique map from $\emptyset \to 1$, giving us the following pullback square:

$$\begin{array}{ccc} \emptyset & \overset{!}{\rightarrowtail} & 1 \\ {\scriptstyle !}\downarrow & & \downarrow{\scriptstyle \bot} \\ 1 & \underset{\top}{\longrightarrow} & \Omega \end{array}$$

which, in turn, can be used to describe the false maps for any topos. Thus we can say $\bot = \chi^1_0$, where 0^1 indicates the unique map from the initial object to the terminal object.

Furthermore, working within the topos of sets, SETS, we can recognize that $f : X \rightarrowtail Y$ are the inclusion maps $X \hookrightarrow Y$, as these are simply abstract sets. Moreover, in SETS the power object $\mathtt{P}(X)$ or rather Ω^X is just the power-set relation 2^X, as we can identify $\mathtt{P}(X) \cong 2^X$ when working with sets.[20]

In type theory, if $a : \mathtt{Set}$ and if for the type family $P : a \to \mathcal{U}$, for each $x : a$, $\mathtt{P}(X)$ is regarded as a proposition, then we can refer to $\mathtt{P}(-)$ as a membership predicate[21] and identify *subsets* of $b \subseteq a$, with the following useful dictionary between set predicates and dependent pair types:

Rather curiously[22] within the type theoretic construction, where $b : \mathtt{Set}$, every $x : b$ is indistinguishable as sets in an intuitionistic type theory. This is because we are not dealing with the sets of ZFC. Rather, these are the abstract sets. From this example we can see one thing about sets: the logic of SETS is an account of set membership. This structure is rather brutal, as it ignores certain subtleties which may be of interest. Luckily, we have other topoi for that!

Remark. Crucially, Ω retains a lattice structure.

In category theory, if a category C has a terminal object 1, we can define the **elements** of other objects $X \in \mathrm{Ob}\ \mathrm{C}$ as the class of arrows $1 \to X$. In the case of a topos E, the class of arrows

[20] If $a, b : \mathtt{Set}$, and $\chi_a = \chi_b$, where χ_a and χ_b are the standard characteristic functions of sets a,b that identify whether a point in a set c is included in a (b, resp), then we have $a = b$, as they agree on all points, namely $\chi_a(a) = \chi_b(a) = \chi_a(b) = \chi_b(b) = \{1\}$.

[21] Indeed, it is worth recalling that type families are fibrations, in so much as given some type universe $\mathcal{U}$, if $A : \mathcal{U}$, then the type family $P : A \to \mathcal{U}$ is a **fibration** with base space A and each $\mathtt{P}(X)$ is a **fibre** over x, with the dependent pair $\sum_{x:A} \mathtt{P}(X)$ characterizing the **total space of the fibration**. In the case of propositional membership, we have the familiar predicate logic of first order logic, but within the internal logic of other decidedly less quotidian topoi, we often have a typed higher order logic with higher order predicates. One could almost say that this motivates the hunt for a means of modeling type theory in any elementary $(\infty, 1)$-topos (although that would very reductive).

[22] Although curious, this is not shocking at all, and can be considered an instance of the Mengen/Kardinalen paradox that motivated Lawvere to study cohesive sets in the first place.

Set Theory	ITT
$\{x \in a \mid \mathtt{P}(X)\}$	$\sum_{x:A} \mathtt{P}(X)$

$1 \to \Omega$ are the **truth-values** of E. In fact, one ought to think of a topos as being a generalization of the category of sets, in so much as one can do mathematics within different topoi.

That said, it is still immensely fruitful to work with SETS-valued (pre)- sheaves.

Example 1.3.2. If C is locally small, the functor category PSH(C) has functors $\mathcal{F} : \mathrm{C}^{\mathrm{op}} \to \mathrm{SETS}$ for objects and natural transformations $\eta : \mathcal{F} \to \mathcal{G}$ for morphisms. For those familiar with the definition of presheaves, we see that $\mathcal{F} \in \mathrm{Ob\ PSH(C)}$ restricts $x \in \mathcal{F}(X)$ along all arrows $f \in \mathrm{Hom_C}(Y, X)$, as expected. In general, for categories C and D, a **D valued pre-sheaf** is the functor, $\mathcal{F} : \mathrm{C}^{op} \to \mathrm{D}$. Thus, a presheaf is a map such that for each object X in C, $F(X)$ is an object in D, and for each morphism $f : X \to Y$, $\mathcal{F}(f) : F(Y) \to F(X)$ is a morphism in D. Moreover, $\mathcal{F}(g \circ f) = \mathcal{F}(f) \circ \mathcal{F}(g)$ and $\mathcal{F}(\mathrm{id}_X) = \mathrm{id}_{\mathcal{F}(X)}$.

Importantly, each $X \in \mathrm{Ob\ C}$ is associated to a representable functor $\mathrm{Hom_C}(-, X)$, which is clearly a presheaf. For $f \in \mathrm{Hom_C}(Y, X)$, there is a natural transformation

$$\eta : \mathrm{Hom_C}(-, Y) \to \mathrm{Hom_C}(-, X)$$

which when paired with the mapping $X \mapsto \mathrm{Hom_C}(-, X)$, we can use to define a full and faithful functor $\mathcal{Y} : \mathrm{C} \to \mathrm{PSH(C)}$ called the *Yoneda embedding*. The existence of $\mathcal{Y}$ is given by the *Yoneda Lemma*, which asserts that for an arbitrary presheaf $\mathcal{F}(X)$

$$\theta : \mathrm{Hom_{PSH(C)}}(\mathrm{Hom_{SETS}}(-, X), \mathcal{F}) \cong \mathcal{F}(X)$$

defined on η by $\theta(\eta) = \eta_X(\mathrm{id}_X)$.

In particular, given the discussion in chapter 2, if there is a subobject classifier Ω for PSH(C) for small C, then by the Yoneda Lemma,

$$\mathrm{Sub_{PSH(C)}}(\mathrm{Hom_C}(-, X)) \cong \mathrm{Hom_{PSH(C)}}(\mathrm{Hom_C}(-, X), \Omega)$$

Thus, if $\Omega \in \mathrm{Ob\ PSH(C)}$ exists, it has the object function $\Omega(X) \cong \mathrm{Sub_{PSH(C)}}(\mathrm{Hom_C}(-, X))$, which is to be expected since the subobject classifier is classifying subobjects! This is little more than an abstract generalization of the following notion:

Definition 1.10. If C is a locally small category, and $X \in \text{Ob C}$, then a **sieve on X** is some subset of $S \subseteq \text{Ob C} \downarrow X$ such that if $f \in S$ and $f \circ h \in \text{Ob C} \downarrow X$, then $f \circ h \in S$, which we can encode as a definable formula:[23]

$$\texttt{Sieve}[X; S] :\equiv (S \in \texttt{P}(\text{Ob C} \downarrow X)) \to (((f \in S) \wedge ((f \circ h) \in \text{Ob C} \downarrow X)) \to ((f \circ h) \in S))$$

In fact, we recognize that

$$\Omega(X) \cong \text{Sub}_{\text{PSh(C)}}(\text{Hom}_{\text{C}}(-, X)) \cong \{S \mid \texttt{Sieve}[X; S]\}$$

i.e., the sieves on X are in bijective correspondence with the subobjects in PSh(C) of the representable functor $\text{Hom}_{\text{C}}(-, X)$, such that sieves S are identified with the functor

$$Y \mapsto \{f \in S \mid \texttt{dom}[Y; f]\}$$

Moreover, if $f \in \text{Hom}_{\text{C}}(Y, X)$, then $\Omega(f) \in \text{Hom}_{\text{Sets}}(\Omega(Y), \Omega(X))$ is defined by

$$S \mapsto \{g \in \text{Hom}_{\text{C}}(X, C) \mid f \circ g \in S\}$$

where S is a sieve on X. So not only do we have a bijective correspondence of sieves on X with subobjects in PSh(C), but we may also regard the truth subobject classifier $\top : 1 \to \Omega$ as being given by the maximal sieve $\top_X(*) = \text{Ob C} \downarrow X$.

Finally,

Definition 1.11. Given $\mathcal{F}$, we can define an index category called the **category of elements of** $\mathcal{F}$,[24] suggestively denoted by $\int_{\text{C}} \mathcal{F}$. The objects of this category are pairs (X, p) such that $X \in \text{Ob C}$ and $p \in \mathcal{F}(X)$, and the morphisms $u \in \text{Hom}_{\int_{\text{C}} \mathcal{F}}((Y, q), (X, p))$ are simply $u \in \text{Hom}_{\text{C}}(Y, X)$ such that $(\mathcal{F}(u))(q) = p$. Moreover, $\int_{\text{C}} \mathcal{F}$ has an obvious canonical projection functor $\pi_{\mathcal{F}} : \int_{\text{C}} \mathcal{F} \to \text{C}$

[23] Clever readers may also recognize sieves as resembling right ideals of a monoid closed under precomposition. Indeed, this is precisely the case if $\text{C} \equiv \text{Mon}$.

[24] Often known as the **Grothendieck completion**.

defined by $(X, p) \mapsto X$.

In particular, u is chosen so that a fixed $p \in \mathcal{X}$ is taken back into $q \in \mathcal{Y}$. So now, we can define *diagrams* $D : \int_{\mathrm{C}} \mathcal{F} \to \mathrm{C}$ of type $\int_{\mathrm{C}} \mathcal{F}$ such that

$$\varinjlim_{\int_{\mathrm{C}} \mathcal{F}} \mathcal{Y} \circ D \cong \mathcal{F}$$

by the Yoneda embedding.

Thus we have proven the following:

Proposition 7. *In* PSh(C)*, any $\mathcal{F}$ is the canonical colimit of a diagram of representable objects.*

It bears mentioning that colimits $\int_{\mathrm{C}} \mathcal{F}$ can be used to construct pairs of adjoint functors.

Example 1.3.3. Let X be a topological space with a given topology τ_X. We denote by $\Theta(X)$ the partially ordered set of open sets of τ_X, which are obviously ordered by inclusion. The category $\mathrm{PSh}(\Theta(X))$ is also a topos. For a pre-sheaf $\mathcal{F}$, and $U \in \mathrm{Ob}\ \Theta(X)$, it is customary to call the elements of $\mathcal{U}$ the **sections of $\mathcal{F}$ over U**, and the maps $\mathcal{F}(U) \to \mathcal{F}(V)$ the **restriction of sections from U to V.**[25]

Some Other Interesting Topoi

Before we can define other, far more interesting topoi for the purposes of this paper, we will need the following definitions.

Definition 1.12. Given a locally small category C, a **covering family** of $X \in \mathrm{Ob}\ \mathrm{C}$ is a collection χ_X of families of functions $(f_i \in \mathrm{Hom}_{\mathrm{C}}(X_i, X))_{i \in I}$ for some index I. A **coverage** is a mapping that assigns each $X \in \mathrm{Ob}\ \mathrm{C}$ to a covering family χ_X such that

$$(((f_i)_{i \in I} \in \chi_X) \wedge (g \in \mathrm{Hom}_{\mathrm{C}}(Y, X))) \to$$

$$\exists \chi_Y (\exists ((h_j)_{j \in J} \in \chi_Y)(\forall (g \circ h_j)(\exists i \in I(\exists (k_{j,i} \in \mathrm{Hom}_{\mathrm{C}}(Y_j, X_i))(g \circ h_j = f_i \circ k_{j,i})))))$$

[25] It bears mentioning that by the contravariance of presheaves, $V \subseteq U$ must be the case for this to be defined.

i.e., $g \circ h_j$ factors through some f_i for each h_j, or more evocatively, for each h_j, there is some f_i and $k_{j,i}$ so that

$$\begin{array}{ccc} Y_j & \xrightarrow{k_{j,i}} & X_i \\ {\scriptstyle h_j}\downarrow & & \downarrow{\scriptstyle f_i} \\ Y & \xrightarrow[g]{} & X \end{array}$$

commutes.

If $\mathcal{F}$ is a pre-sheaf such that given a family of elements $(s_i \in \mathcal{X})_{i \in I}$,

$$((((g \in \mathrm{Hom_C}(Y, X_i)) \wedge (h \in \mathrm{Hom_C}(Y, X_j))) \to (f_i \circ g = f_j \circ h)) \to (\mathcal{F}(g)(s_i) = \mathcal{F}(h)(s_j))) \to$$

$$(\exists! s \in \mathcal{F}(X)(\mathcal{F}(f_i)(s) = s_i))$$

for each $i \in I$, then $\mathcal{F}$ satisfies the *sheaf axiom* for $(f_i) \in \chi_X$.[26] We say $\mathcal{F}$ is a **sheaf** if the sheaf axiom is satisfied for all covering families of χ_X.

Remark. This situation is immensely simplified when C has pullbacks, because then it suffices to check compatibility of s_i and s_j on the pullback of f_i and f_j. Diagrammatically, this mean that $\mathcal{F}$ satisfies the sheaf axiom for $(X_i \to X)_{i \in I}$ if and only if

$$F(X) \to \prod_{i \in I} F(X_i) \rightrightarrows \prod_{(i,j) \in I \times I} F(X_i \times_X X_j)$$

is an equalizer diagram.

In particular, when looking at $\Theta(X)$, one way to identify sheaves is to define them by presheaves and sieves, as in the following proposition:

Proposition 8. *Let X be a topological space. A presheaf $\mathcal{F}$ on X is a sheaf if and only if for every open set U of X, and every covering sieve S on U, $\iota_S : S \to \mathcal{Y}(U)$ induces the following isomorphism:*

$$Hom(\mathcal{Y}(U), \mathcal{F}) \cong Hom(S, \mathcal{F})$$

[26] The hypothesis of this axiom is called the compatibility condition.

Proof. A proof of this proposition can be found in [12] (pp. 70). □

Theorem 9. *If X is a topological space, then* $\textsc{Sh}(X)$ *is a topos.*

Proof. A full proof of this can be found scattered through [12] and [10]. Broadly speaking, it amounts to verifying the following:

- Verifying that $\textsc{Sh}(X)$ is a cartesian category by verifying that $\textsc{Sh}(X)$ is reflective in $\textsc{PSh}(\Theta(X))$;
- Verifying that $\textsc{Sh}(X)$ is an exponential ideal in $\textsc{PSh}(\Theta(X))$, so that for any sheaf $\mathcal{G}$ and any $\mathcal{F}$, the exponential $\mathcal{G}^{\mathcal{F}}$, which is defined on U to be the set of morphisms $\mathrm{Hom}_{\Theta(X)}(-,U)\times\mathcal{F}\to\mathcal{G}$ and on $f:U\to V$ to be the operation $\mathrm{Hom}_{\Theta(X)}(-,f)\times 1:\mathrm{Hom}_{\Theta(X)}(-,V)\times\mathcal{F}\to\mathrm{Hom}_{\Theta(X)}(-,U)\times\mathcal{F}$, is a sheaf, so that $\textsc{Sh}(X)$ is cartesian closed;
- Verifying that the presheaf Ω on X that takes $\Omega(U)$ to $\Theta(U)$ is a sheaf, so that $\top:1\to\Omega$ can be defined by $\top_U = U\in\Omega(U)$, and induces a classifying map for all $\mathcal{F}\rightarrowtail\mathcal{G}$.

□

Example 1.3.4. The slice category $\textsc{Sets}\downarrow X$ is a topos. This fact is fairly important, since specifying a geometric morphism from $\textsc{Sets}\downarrow X\to\mathbf{E}$ amounts to specifying an $X-$indexed family of points in $\mathbf{E}$. In fact,[27] any Grothendieck topos $\mathbf{E}$ will have *enough points* if and only if there is some set X such that $\textsc{Sets}\downarrow X\to\mathbf{E}$ is a surjection.

Example 1.3.5. The **category of representations of a fixed group G**, denoted $\mathbf{B}G$ is an important topos. The notion of representation of G is a tuple (X,μ), where X is a set and $\mu: X\times G\to X$ is a right-action such that for all $x\in X$, and $g,h\in G$

1. $\mu(x,1)=x$;
2. $\mu(\mu(x,g),h)=\mu(x,gh)$.

Morphisms $f:(X,\mu)\to(Y,\nu)$ are simply $f:X\to Y$ such that $f(\mu(X,g))=\nu(f(X),g)$. In this category, a subobject is just a subset $Y\subseteq X$ that is closed under the action of G. Since $Y\backslash X$ will also be closed under the action of G, the subobject classifier and characteristic function χ_Y are inherited $\textsc{Sets}$. Similarly, this holds for topological groups G.

[27] See (C.2.2) [11] for more details.

Some Interesting Topoi For Studying Smooth Spaces

Example 1.3.6. Ringed topoi emerge rather naturally from the fact that a topos is a cartesian monoidal category.[28] In this case, given a topos E, one can define internally[29] the notion of a (commutative) unital ring. Specifically, these are pairs[30] $(\mathrm{E}, \mathcal{O})$ where $\mathcal{O}$ is a distinguished unital ring object internal to the topos E.

Example 1.3.7. Lined topoi $(\mathbf{E}, R)$ are ringed topoi equipped with both the usual internal ring object $\mathcal{O}$ and a choice of an internal commutative algebra object R over $\mathcal{O}$, called the **line object**.

One interesting example of a lined topos are the sheaves[31] of cartesian spaces, denoted $\mathrm{Sh}(\mathrm{CartSp}_{\mathrm{SMOOTH}})$ whose lined object is the interval[32] object $1 \coprod 1 \to \mathbb{R}$.[33] Suffice to say it is an instance of a Grothendieck topos,[34] as $\mathrm{CartSp}_{\mathrm{SMOOTH}}$ can be made into a small site with a little leg work.[35]

Example 1.3.8. A **smooth topos** is a lined topos where each functor $(-)^{\mathrm{Spec}W} : \mathrm{E} \to \mathrm{E}$ defined by an **R-Weil algebra**[36] W has a right adjoint, known as the **amazing right adjoint**, and the canonical $W \to R^{\mathrm{Spec}(W)}$ is an isomorphism. Effectively this means that each $R-$Weil algebra is infinitesimal and satisfies the Kock-Lawvere axiom.[37]

Topoi as τ-theories

Now we can extend the sketch of $\lambda-$theories with cartesian closed categories to $\tau-$theories.

---

[28] In this case, the categorical product gives the monoidal structure, and the terminal object acts as the unit.

[29] There are two important ways to generalize a category: internalization and enrichment. The gist of an internal category is that within a category A with enough pullbacks, one can construct *another category* if there is an object $V : A$ and an object $E : A$, together with source and target morphisms $s, t : E \to V$, an identity assigning morphism $e : V \to E$ and a composition morphism $c : E \times_V E \to E$ satisfying the usual coherence laws.

[30] Looks an awful like a ringed space, no?

[31] Sheaves are merely pre-sheafs with additional topological structure which tracks the local data of an open set. The two additional requirements are the *locality* and *gluing* requirements: (locality) given an open covering (U_i) of an open set U, and $s, t : F(U)$ such that $s|_{U_i} = t|_{U_i}$ for each i, then $s = t$; (gluing) If for each pair U_i, U_j in the open cover, there two respective sections s_i, s_j which agree on overlaps (i.e $s_i|_{U_i \cap U_j} \cap s_j|_{U_i \cap U_j}$, there is a third section $s \in F(U)$ such that $s|U_i = s_i$ for each i).

[32] In categories with finite limits, such as topoi, a lined object is the copairing of maps $f, g : 1 \to I$, where 1 is a terminal object. This is to say, $[f, g] : 1 \coprod 1 \to I$ is an interval object. In general, it is good practice to associate the interval object to the unit interval.

[33] It is a worthwhile exercise to verify that $\mathrm{Sh}(\mathrm{CartSp}_{\mathrm{SMOOTH}})$ is a topos, as it is not immediately relevant for this paper.

[34] which, as we will see momentarily, are topoi that are equivalent to the categories of sheaves on a small site.

[35] This is tantamount to proving that every paracompact smooth manifold admits a good open cover.

[36] An R**-Weil algebra** is an R-algebra of the form $W = R \oplus J$, where J is an R-finite dimensional nilpotent ideal.

[37] Very briefly, this is the requirement that this topos requires every morphism from an infinitesimal interval $D \subset R$ into R is linear and can be extended uniquely to a linear map $R \to R$.

Definition 1.13. A **τ-signature** is one with type constructors for finite products and power types, along with term constructors:

$$* : 1; \mathtt{FV}(*) = \emptyset$$

$$s : A \wedge t : B \Rightarrow \langle s, t\rangle : A \times B; \mathtt{FV}(\langle s, t\rangle) = \mathtt{FV}(s) \cup \mathtt{FV}(t)$$

$$t : A \times B \Rightarrow \mathtt{fst}(t) : A \wedge \mathtt{snd}(t) : B$$

and if φ is a formula, and $x : A$, then

$$\{x : A \mid \varphi\} : \mathtt{P}(A); \mathtt{FV}(\{x : A \mid \varphi\}) = \mathtt{FV}(\varphi)\backslash\{x\}$$

The τ-calculus whose rules of inference are the *standard* first order rules, with the following product type axiom:

for $x : A, y : B, z : A \times B$

- $x.(x =_1 *)\ x$ has type 1;
- $x, y.(\mathtt{fst}(\langle x, y\rangle) =_A x)$;
- $x, y.(\mathtt{snd}(\langle x, y\rangle) =_B y)$;
- $z.(\langle \mathtt{fst}(z), \mathtt{snd}(z), =\rangle_{A\times B} z)$.

and the following two axioms for power types:

for $w : \mathtt{P}(A)$,

$$\top \vdash_w (w = \{x : A \mid x \in_A w\})$$

and for any formula ϕ, with free variables in the string $\vec{x}, y$,

$$(z \in_A \{y : A \mid \phi\}) \dashv\vdash_{\vec{x},y} \phi[z/y]$$

The takeaway from this is that **a τ-theory** $\mathbb{T}$ is simply a set of sequents over Σ, which are regarded as the non-logical axioms of the theory. In this regard, the usual usual notion of a model for a theory in a topos is simply a structure for its signature satisfying the axioms of $\mathbb{T}$. So, just as

Heyting categories correspondeded to first-order theories, we see that elementary topoi correspond to higher order theories (in general).

Example 1.3.9. One such example of the internal language of a topos corresponding to higher order theories is the **Mitchell-Bénabou language**, $\mathcal{L}\mathbf{E}$,which is one way of describing the objects of $\mathbf{E}$ as if they were sets.

In particular, one regards the objects of $\mathbf{E}$ as types for this language, so that for each type X, there are logical variables $x_1, x_2, \ldots$ of type X, which are interpreted as the identity arrow id_X. Each term σ of type X involves the construction of variables, some of which may be free over X, say w, y and z, with respective types W, Y and Z. Then the **domain of definition** of σ is the product space $W \times Y \times Z$, and whose **interpretation** is an arrow

$$\sigma : W \times Y \times Z \to X$$

in $\mathbf{E}$. Summarizing [12], we can inductively define the terms of this language as follows:

1. For each $x : X$, the interpretation of x is the identity map id_X;

2. Terms σ, τ of types X and Y and interpretations $\sigma : U \to X$ and $\tau : V \to X$ yield a term $\langle \sigma, \tau \rangle$ of type $X \times Y$ with interpretation $\langle \sigma\pi_U, \tau\pi_V \rangle : W \to X \times Y$ where W has projection maps π_U, π_V;

3. Terms $\sigma : U \to X$ and $\tau : V \to X$ yield term $\sigma = \tau$ of type Ω with the interpretation

$$(\sigma = \tau) : W \overset{\langle \sigma\pi_U, \tau\pi_V \rangle}{\longrightarrow} X \times X \overset{\delta}{\longrightarrow} \Omega$$

   where δ is the characteristic map of the diagonal $\Delta : X \rightarrowtail X \times X$;[38]

4. An arrow $f : X \to Y$ of $\mathbf{E}$ and a term $\sigma : U \to X$ of type X yield a term $f \circ \sigma$ of type Y, with the interpretation

$$f \circ \sigma : U \overset{\sigma}{\to} X \overset{f}{\to} Y$$

[38] Terms of type Ω are **formula** of the language $\mathcal{L}\mathbf{E}$.

5. Terms of $\theta : V \to Y^X$ and $\sigma : U \to X$, yield a term $\theta(\sigma)$ of type Y with the interpretation

$$\theta(\sigma) : W \xrightarrow{\langle \sigma\pi_U, \tau\pi_V \rangle} Y^X \times X \xrightarrow{eval} Y$$

where *eval* is the evaluation function;

6. Terms $\sigma : U \to X$ and $\tau : V \to \Omega^X$ yield a term $\sigma \in \tau$ of type Ω, with the interpretation

$$\sigma \in \tau : W \xrightarrow{\langle \sigma\pi_U, \tau\pi_V \rangle} X \times \Omega^X \xrightarrow{eval} \Omega$$

7. A variable $x : X$ and term $\sigma : X \times U \to Z$ yields $\lambda x \sigma$, a term of type Z^X, with the interpretation given by the exponential transpose of σ from the λ-calculus,

$$\lambda x \sigma : U \to Z^X$$

Astute readers can recognize familiar logical operations such as substitution, AND, OR, etc. More importantly, for the terms Ω, we can apply the usual logical connectives and quantifies to get composite terms of type Ω

$$\phi \wedge \psi : W \xrightarrow{\langle \phi\pi_U, \psi\pi_V \rangle} \Omega \times \Omega \xrightarrow{\wedge} \Omega$$

$$\phi \vee \psi : W \xrightarrow{\langle \phi\pi_U, \psi\pi_V \rangle} \Omega \times \Omega \xrightarrow{\vee} \Omega$$

$$\phi \Rightarrow \psi : W \xrightarrow{\langle \phi\pi_U, \psi\pi_V \rangle} \Omega \times \Omega \xrightarrow{\Rightarrow} \Omega$$

$$\neg\phi : W \xrightarrow{\phi} \Omega \xrightarrow{\neg} \Omega$$

As before, quantifiers are adjoints, and validity in this language is simply a matter of a formula $\phi(x, y)$ factoring through $\top : 1 \to \Omega$.

Remark. One particularly interesting application of this language is that we can define the notion of a local ring object in a topos $\mathbf{E}$ as follows:

Example 1.3.10. The ring object R in $\mathbf{E}$ is such that

$$\forall a \in R(\exists b \in R(a \cdot b = 1) \vee \exists b \in R(1 - a) \cdot b = 1)$$

is valid in $\mathbf{E}$, i.e. the union of the following subobjects

$$\{a \in R \mid \exists b(a \cdot b = 1)\} \rightarrowtail R$$

and

$$\{a \in R \mid \exists b((1 - a) \cdot b = 1)\} \rightarrowtail R$$

of R is R itself. This notion of a ring object generalizes the notion that a local ring in SETS is an R with a *unique* maximal ideal.

Chapter 2

Some Remarks On Grothendieck Topos Theory

This entire section assumes familiarity with category theory, but not necessarily a familiarity with algebraic geometry. In particular, this chapter will assume that the reader has some comfort with equalizers and understands that (co-)homology can be understood functorially. The former are particularly important in forming the notion of a sheaf. Sections 2.2 and 2.3 explore the notion of classification and present a few sketches towards the long-term goal of verifying the Weil conjectures with the tools of intuitionistic type theory.

2.1 Grothendieck Topoi: Sites, Sheaves, and Schemes

Although historically prior to the notion of an elementary topos and the description of coverage above, the Grothendieck topos and Grothendieck pre-topology drawn from the notion of sieves themselves were meant to abstract the notion of topological spaces so that one could have a rigorous account of sheaves, [4]. In particular, the original abstractions were intended to provide the following definition:

Definition 2.1. A **site** $(\mathrm{C}, \mathcal{J})$ is a locally small category C stable under pullbacks equipped with a **coverage** $\mathcal{J}$. The system of coverings from $\mathcal{J}$ are called a **(Grothendieck) topology**.

Definition 2.2. If C can be identified with a site $(\mathrm{C}, \mathcal{J})$, then a **sheaf on site** $(\mathbf{C}, \mathcal{J})$ is a presheaf $\mathcal{F}$ satisfying the sheaf condition:

$$\mathcal{F}(U) \to \prod_{i \in I} \mathcal{F}(U_i) \rightrightarrows \prod_{(i,j) \in I \times I} \mathcal{F}(U_i \times_U U_j)$$

is exact for every covering $(U_i \to U)$.

In other words, $\mathcal{F}$ is a sheaf if

$$f \mapsto (f|_{U_i}) : \mathcal{F}(U) \to \prod \mathcal{F}(U_i)$$

identifies $F(U)$ with the subset of the product consisting of families (f_i) such that $f_i|_{U_i \times_U U_j} = f_j|_{U_i \times_U U_j}$ for all $i, j \in I$.

Notation. If $\mathcal{F}$ is a presheaf on C, then we refer to $\mathcal{F}(X)$ as the **sections** of the presheaf over object X. The literature freely alternates between this functor notation, and $\Gamma(U, \mathcal{F})$ to denote the object $\mathcal{F}(U)$, and beginning in chapter 4, we will stick with this convention.

Remark. A **Grothendieck topos** is any category that is equivalent to the category of sheaves on a site. In this sense, a site can be thought of as some category C and some full subcategory of $\mathrm{PSh}(\mathrm{C})$ (i.e. $\mathrm{Sh}(\mathrm{C})$) such that $\alpha \dashv \iota : \mathrm{Sh}(\mathrm{C}) \hookrightarrow \mathrm{PSh}(\mathrm{C})$, with α commuting for all finite limits. When working with $\mathrm{Sh}(\mathrm{C})$, this left adjoint α is simply the sheafification functor. For instance, if we're looking at $\mathrm{Sh}(\Theta(X))$, this would just be the full subcategory of $\mathrm{PSh}(\Theta(X))$ such that for any open

covering $\{X_i\}_{i\in\ I}$ of X.

$$\mathcal{F}(U) \to \prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{(i,j)\in I\times I} \mathcal{F}(U_i \times_U U_j)$$

is an equalizer, as we mentioned earlier. In this case, it's clear that $X_i \times_X X_j$ is actually $X_i \cap X_j$, and so this is easy to verify. Also, it's customary to write $\mathrm{Sh}(\Theta(X))$ as $\mathrm{Sh}(X)$. Notably, Sets is also a Grothendieck topos as the category of sheaves on $\{*\}$.[1] That $\mathrm{Sh}(X_{\acute{e}t})$ is a Grothendieck topos is of particular interest, and will motivate our excursion into *locally ringed spaces*.

In addition to being cartesian closed, locally small and well-powered, Grothendieck topoi are also well-copowered and possess both separating and coseparating sets. Throughout the proof of the Weil conjecture, we can make use of the fact that any left adjoint preserves limits (respectively, right adjoints preserve colimits).[2]

Definition 2.3. Let $\mathbf{E}$ be a Grothendieck topos. We define a **point of a Grothendieck topos** is a geometric morphism $p : \mathrm{Sets} \to \mathbf{E}$. We say $\mathbf{E}$ **has a enough points** if for any two $\alpha, \beta : X \rightrightarrows Y$ for $X, Y \in \mathrm{Ob}\ \mathbf{E}$, there is some $p : \mathrm{Sets} \to \mathbf{E}$ such that

$$p^*(\alpha) \neq p^*(\beta)$$

Remark. For any topological space X, if $\alpha, \beta : \mathcal{F} \rightrightarrows \mathcal{G}$ are distinct morphisms in $\mathrm{Sh}(X)$, then for some point $x \in X$, the stalks of α_x and β_x must be distinct. However, since the stalk maps are the inverse images of α, β under the geometric morphism of $\mathrm{Sets} \to \mathrm{Sh}(X)$ given by the point x, we find that $\mathrm{Sh}(X)$ has enough points.

Example 2.1.1. Let X be a topological space. Recall that the topology of X can be given as a category whose objects are the open sets of X, and whose morphisms are the inclusion relations. A presheaf F of abelian groups on X sends every open subset U of X to an abelian group $F(U)$ and every inclusion $V \subset U$ is sent to an abelian group homomorphism $\rho_{UV} : F(U) \to F(V)$ satisfying the following conditions:

1. $F(\emptyset) = 0$ where $\emptyset$ is the empty set.

[1] This is almost exactly what one ought to expect.
[2] This is a consequence of the Special Adjoint Functor theorem.

2. $\rho_{UU} = id_{F(U)}$.

3. For open inclusions $W \subset V \subset U$, $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

   Furthermore, F is a sheaf if the following additional conditions hold:

4. If U is an open set and $\{V_i\}$ is an open covering of U, and if $s \in F(U)$ is an element such that $s|_{V_i} = 0$ for all i, then $s = 0$;

5. if U is an open set, $\{V_i\}$ form an open covering of U, and if there are elements $s_i \in F(V_i)$ for each i such that for each pair i,j, $s_i|_{V_i \cap V_j} = s_j|_{V_i \cap V_j}$, then there is an element $s \in F(U)$ such that $s|_{V_i} = s_i$ for each i.

We can actually easily accommodate other abelian target categories with this definition, which yields an **abelian sheaf**.

Example 2.1.2. Let X be a topological space and k a field. The **sheaf of $k-$algebras** is a sheaf $\mathcal{O}_X : \Theta(X)^{op} \to \text{CRING} \uparrow k$ such that for every open subset U of X, $\mathcal{O}_X(U)$ is a set of functions $U \to k$ satisfying the following conditions:

1. $\mathcal{O}_X(U)$ is a k-subalgebra of all the $k-$valued functions on U;

2. If $U' \subset U$ is an open subset and $f \in \mathcal{O}_X(U)$, then $f|_{U'} \in \mathcal{O}_X(U')$;

3. A function $f : U \to k$ on an open subset U of V is in $\mathcal{O}_X(U)$ if $f|_{U_i} \in \mathcal{O}_X(U_i)$ for all U_i in some open covering of U.

Remark. This is to say that one way to study k-algebras is to consider the co-slice category of commutative rings under k (as k is clearly a commutative ring).

We Loved This Site So Much, We Put A Ring On It!

Definition 2.4. If X is a topological space, and $\mathcal{O}_X$ is a sheaf of k-algebras, then the pair $(X, \mathcal{O}_X)$ is a **ringed space**. For $p \in X$, consider the pair (f, U), where U is a neighbourhood of p and $f \in \mathcal{O}_X(U)$. A **germ of a function at p** is an equivalence relation on two pairs $(f, U), (f', U')$ such that

$$(f, U) \sim (f', U') \iff \exists U'' \in \text{ob}(\Theta(X)), p \in U'' \text{ and } f|_{U''} = f'_{U''}$$

The equivalence classes of these pairs form a $k-$algebra denoted in the literature by $\mathcal{O}_p$ or $\mathcal{O}_{X,p}$. It is important to recognize that for neighbourhoods U of p

$$\mathcal{O}_p = \varinjlim_{\mathcal{U}_p^X} \mathcal{O}_X(U)$$

(that is, as a direct limit of k-algebras). Finally, it should be clear that morphisms between ringed spaces are continuous maps $\varphi : X \to Y$ such that

$$f \in \text{ob } \mathcal{O}_Y(U) \Rightarrow f \circ \varphi \in \text{ob } \mathcal{O}_X(\varphi^{-1}U)$$

for all open sets $U \in \text{ob}(\Theta(Y))$. A morphism between ringed spaces is an isomorphism if it is a homeomorphism, i.e. it is a bijective mapping and its inverse is a morphism between ringed spaces.

$(X, \mathcal{O}_X)$ is a **locally ringed space** if for each point $p \in X$, for all non-units $a, b \in$ ob $\mathcal{O}_{X,p}$, $a+b$ is not a unit, i.e. the stalk $\mathcal{O}_{X,p}$ is a local ring. A morphism from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is a pair of maps $(f, f^\sharp)$ where $f : X \to Y$ is a continuous map and $f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X$ is a map of shaves of rings on Y such that $f_P^\sharp$ is a local homomorphism of local rigns at each point $P \in X$.

Definition 2.5. Let R be a ring. First, define the formula $\texttt{Prime}[R; \mathfrak{p}]$ as follows:

$$\texttt{Prime}[R; \mathfrak{p}] := (\mathfrak{p} \subset R) \wedge \forall x \forall y((x \cdot y \in \mathfrak{p}) \to ((x \in \mathfrak{p}) \vee (y \in \mathfrak{p})))$$

Next, define $\text{Spec}R := \{\mathfrak{p} \mid \texttt{Prime}[R; \mathfrak{p}]\}$. We can give this set the Zariski topology[3], and proceed to turn it into a locally ringed space, with a sheaf of rings $\mathcal{O}$ on Spec$R$ as follows:

For each prime ideal $\mathfrak{p}$, let $R_\mathfrak{p}$ be the localisation of R at $\mathfrak{p}$. For an open set in $U \subseteq \text{Spec}R$, we first define $\texttt{SpSh}[U, R; s, \mathfrak{p}]$ as follows:

$$\texttt{SpSh}[U, R; s, \mathfrak{p}] := \forall \mathfrak{p}((\mathfrak{p} \in U) \to (s(\mathfrak{p} \in R_\mathfrak{p}) \wedge$$

$$\exists V \exists a \exists f((\mathfrak{p} \in V) \wedge (V \subset U) \wedge (a \in R) \wedge (f \in R) \wedge$$

[3] If $\mathfrak{a}$ is an ideal in R, define $V(\mathfrak{a}) \subseteq \text{Spec}R$ to be the set of all prime ideals containing $\mathfrak{a}$. A topology on Spec$R$ treats $V(\mathfrak{a})$ as the closed sets.

$$\forall \mathfrak{q}((\mathfrak{q} \in V) \to (\neg(f \in \mathfrak{q}) \wedge (s(\mathfrak{q} = a/f)))))$$

In particular, notice that this construction means that s satisfying $\mathtt{SpSh}$ are locally quotients of elements of R, extending the idea of regular functions from fields to arbitrary local rings. Next, then define

$$\mathcal{O}(U) := \{s : U \to \coprod_{\mathfrak{p} \in U} R_{\mathfrak{p}} \mid \mathtt{SpSh}[U, R; s, \mathfrak{p}]\}$$

It can be verified that each $\mathcal{O}(U)$ is a commutative ring with identity. The **spectrum** of R is the pair $(\mathrm{Spec}R, \mathcal{O})$.

Example 2.1.3. Recall that a **graded ring** is a ring $R = \bigoplus_{k \geq 0} R_k$, where R_k are abelian groups such that for any $a, b \geq 0$, $R_a R_b \subseteq R_{a+b}$, and let $R_+ = \bigoplus_{k>0} R_k$. Further recall that homogeneous ideals $\mathfrak{a}$ in a graded ring R satisfy $\mathfrak{a} = \bigoplus_{k \geq 0} (\mathfrak{a} \cap R_k)$. Elements of each factor R_k of the decomposition are called **homogeneous elements of degree d**. If $\mathfrak{a}$ is a homogeneous ideal of R, then $\mathtt{Homg}[R; \mathfrak{a}]$ is satisfied.[4] Next, we set

$$\mathrm{Proj}R := \{\mathfrak{p} \mid \mathtt{Prime}[R; \mathfrak{p}] \wedge \mathtt{Homg}[R; \mathfrak{p}] \wedge (R_+ \not\subseteq \mathfrak{p})\}$$

Furthermore, if $\mathfrak{a}$ is a homogeneous ideal of R, define $V(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Proj}R \mid \mathfrak{p} \supseteq \mathfrak{a}\}$. Since our aim is to study $\mathrm{Proj}R$ as a locally ringed space, we define a topology by taking the closed sets of $\mathrm{Proj}R$ to be the subsets of the form $V(\mathfrak{a})$. With this topology, we form a ringed space $(\mathrm{Proj}R, \mathcal{O})$, where $\mathcal{O}$ is a sheaf of rings defined as follows:
For each $\mathfrak{p} \in \mathrm{Proj}R$, denote by $R_{(\mathfrak{p})}$ the ring of elements of degree zero in the localized ring $M^{-1}R$, where M is the monoid of all the homogeneous elements of R which are not in $\mathfrak{p}$. Then, for any $U \subset \mathrm{Proj}R$, we first set

$$\mathtt{PrSh}[U, R; s] := \forall \mathfrak{p}((\mathfrak{p} \in U) \to ((s(\mathfrak{p}) \in R_{(\mathfrak{p})}) \wedge$$

$$\exists V \exists a \exists f((V \subset U) \wedge (\mathfrak{p} \in V) \wedge (\mathtt{Homg}[R; a]) \wedge (\mathtt{Homg}[R; f]) \wedge (\deg a = \deg f) \wedge$$

$$\forall \mathfrak{q}((\mathfrak{q} \in V) \to (\neg(f \in \mathfrak{q}) \wedge (s(\mathfrak{q}) = a/f) \wedge (s(\mathfrak{q}) \in R_{(\mathfrak{q})})))))$$

[4] We also note that if $\mathtt{Homg}[R; f]$ is satisfied, then f is a homogeneous element of R.

from which we define the sheaf $\mathcal{O}$ on $U \subset \mathrm{Proj}R$ as follows:

$$\mathcal{O}(U) := \{s : U \to \coprod R_{(\mathfrak{p})} \mid \mathtt{PrSh}[U, R; s]\}$$

Then we find that such an $\mathcal{O}$ is a sheaf with the natural restrictions. Hence, for any graded ring R, $(\mathrm{Proj}R, \mathcal{O})$ with $\mathcal{O}$ defined above, we have yet another ringed space.

Example 2.1.4. Let R be a graded ring and let M be a graded $R-$module. The **sheaf associated to M on** $\mathrm{Proj}R$ is denoted by $\tilde{M}$. This sheaf is defined[5] as follows:

For each $\mathfrak{p} \in \mathrm{Proj}R$, let $M_{(\mathfrak{p})}$ be the group of elements of degree 0 in the localization of $T^{-1}M$, where T is the monoid of homogeneous elements in R not in $\mathfrak{p}$. We define $\mathtt{PrSh1}[U, R, M; s]$ similarly to $\mathtt{PrSh}[U, R; s]$, only now we expect $a \in M$ to be homogeneous and the same degree as f. Then, for all open sets $U \subseteq \mathrm{Proj}R$, we define

$$\tilde{M}(U) := \{s : U \to \coprod_{\mathfrak{p} \in U} M_{\mathfrak{p}} \mid \mathtt{PrSh1}[U, R, M; s]\}$$

This becomes a sheaf with the obvious restriction maps.

Now, let $X = \mathrm{Proj}R$, and for any $n \in \mathbb{Z}$ consider $R(n)$ as a module of R, where $R(n) = \bigoplus_{k \geq n} R_k$. we define the sheaf $\mathcal{O}_X(n) \equiv \tilde{R(n)}$. In particular, $\mathcal{O}_X(1)$ is called the **twisted sheaf of Serre**. In general, for any sheaf F of $\mathcal{O}_X-$modules, the **twisted sheaf** is defined as $F(n) :\equiv F \otimes_{\mathcal{O}_X} \mathcal{O}_X(n)$

But these notions should be familiar to us; they are indeed, nothing but generalizations of varieties.

A Detour Into The Veritably Varied World of Varieties

Example 2.1.5. An algebraic set has a ringed space structure.

Recall that an **algebraic set** of an affine n-space $\mathbb{A}^n(k)$ over a field k, denoted $V(S)$, is a subset of k^n is the set of common zeros of some set $S \subset k[X_1, \ldots, X_n]$, the **Zariski topology** on $\mathbb{A}^n(k)$ is defined by taking the open sets to be complements of algebraic sets, and a non-empty subset Y of a topological space X is **irreducible** if it cannot be expressed as the union of two

[5] Courtesy of Hartshorne.

proper, closed subsets Y_1, Y_2. Additionally, recall that the **coordinate ring of V** is defined as the quotient $k[X_1, \ldots, X_n]/\mathfrak{a}$, where V is an algebraic subset of k^n and $\mathfrak{a} = I(V)$ is the ideal generated by V. Further recall that $\mathfrak{a}$ is radical, and so the coordinate ring is a finitely generated, reduced k-algebra. Finally, for $h \in k[V]$, set $D(h) = \{a \in V : h(a) \neq 0\}$.

Now suppose that k is an algebraically closed field. We define the following functions:

$$p \mapsto h(p) : V \to k$$

$$p \mapsto 1/h(p) : D(h) \to k$$

A pair of elements $g, h \in k[V]$ with $h \neq 0$ defines a function

$$p \mapsto \frac{g(p)}{h(p)} : D(h) \to k$$

If $f : U \to k$ on open set U of V is **regular** if for all $p \in U$, there exist $g, h \in k[V]$ such that $f = g/h$ on the a neighbourhood of p. Finally, denote the set of regular functions on U by $\mathcal{O}_V(U)$.

It remains to check that the map $U \mapsto \mathcal{O}_V(U)$ defines a sheaf of k-algebras on V.

The definition of regularity is a local definition, and so it suffices to verify this map yields a k-subalgera. Clearly, constant functions are regular. Now suppose that f, f' are regular on a neighbourhood U of p. Then by the definition of regularity, there are $g, g', h, H' \in k[V]$ with $h(p) \neq 0$ and $H' \neq 0$ such that f, f' agree with $\frac{g}{h}, \frac{g'}{H'}$ respectively near p. Thus $f + f' = \dfrac{gH' + g'h}{hH'}$ near p, and so $f + f'$ is also regular near p. It also immediately follows that $\dfrac{gg'}{hH'}$ is regular, and so ff' is regular. Thus $\mathcal{O}_V(U)$ is a k-algebra.

Definition 2.6. If a ringed space $(X, \mathcal{O}_X)$ is isomorphic to a ringed space $(V, \mathcal{O}_V)$, where V is algebraic set in k^n, for some field k, then $(X, \mathcal{O}_X)$ is **an affine algebraic variety**. For affine varieties V and W, a map $f : V \to W$ is **regular** if it is a morphism of ringed spaces. These allow us to consider the category of affine algebraic varieties AffVar.

Definition 2.7. Recall that for fixed algebraically closed fields k, the **projective n-space**, de-

noted $\mathbb{P}^n(k)$ is the set of equivalence classes of $(n+1)-$tuples of elements in k, not all 0, given by $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$, for $\lambda \in k^\times$. Furthermore, recall that $V \subset \mathbb{P}^n(k)$ is an **algebraic set** if there is a set T of homogeneous polynomials such that $V = Z(T) = \{p \in \mathbb{P}^n(k) : f(p) = 0, \forall f \in T\}$. Then a **projective algebraic variety** is an irreducible algebraic set in $\mathbb{P}^n(k)$ with the induced topology.

Definition 2.8. In general, we define an **algebraic prevariety over k** to be a ringed space $(X, \mathcal{O}_X)$ where X is quasicompact[6] and every point in X has an open neighbourhood U for which $(U, \mathcal{O}_X(U))$ is an affine algebraic variety over.

An algebraic pre-variety is said to be **algebraic variety** if it follows the following separation condition: for every pair of regular maps $\varphi_1, \varphi_2 : Z \to X$ with Z an affine algebraic variety, the set $\{z \in Z : \varphi_1(z) = \varphi_2(z)\}$.

Example 2.1.6. A particularly important sheaf is the **sheaf of regular functions on a variety X**, which is a sheaf of rings on X, denoted by $\mathcal{O}$. If X is a variety over a field k, then for each $U \subseteq X$, $\mathcal{O}(U)$ is the ring of regular functions from $U \to k$, and for each $V \subseteq U$, $\rho_{UV} : \mathcal{O}(U) \to \mathcal{O}(V)$ is the restriction map. Clearly this definition satisfies a presheaf. To quickly see that this is a sheaf, recall that a function which is locally 0 is 0, and a function which is locally regular is regular everywhere by the locality of regular functions.

It bears mentioning that this sheaf is a functor to the slice category of commutative rings over some field k, i.e., $\mathcal{O} : \Theta(X)^{op} \to \mathrm{CRing} \downarrow k$.

Example 2.1.7. Consider the section $\Gamma(\mathbb{P}^1, \mathcal{O}(1))$. We claim that this is equal to the set of homogeneous polynomials of degree 1.

Proof. Recall that for a graded ring R and a graded R-module M, there is a natural functor given by $M_0 \mapsto \Gamma(\mathrm{Proj}R, \tilde{M})$ since $M_0 \hookrightarrow M_{(f)}$ for all $f \in R$.

With $\mathbb{P}^1$ the projective line of some ring A, and with $R = A[x_0, x_1]$ and $M = R(1)$, the degree 0 elements of M are the degree 1 elements of R. These are the homogeneous polynomials of degree 1.

[6] i.e. every open covering of X has a finite subcovering

To see that this is an isomorphism, notice that $\mathbb{P}^1$ is covered by $D(x_0) \cup D(x_1)$, and that over the $D(x_i)$, we have global sections which are rational functions with the x_i in the denominator and of homogeneous degree k. Then the intersection $A[x_0, x_1]_{x_0} \cap A[x_0, x_1]_{x_1} = A[x_0, x_1] = R$. Hence there is an isomorphism. □

And Back Into The Seriously Structured World of Schemes

Definition 2.9. An **affine scheme** is a locally ringed space $(X, \mathcal{O}_X)$ which is isomorphic to the spectrum of some ring. A **scheme** is a locally ringed space $(X, \mathcal{O}_X)$ in which every point has an open neighbourhood U such that as a topological space $(U, \mathcal{O}_X|_U)$ is an affine scheme. In this case, X is the **underlying topological space** of the scheme $(X, \mathcal{O}_X)$ and $\mathcal{O}_X$ is the **structure sheaf**.

Example 2.1.8. If R is a graded ring, then Spec$R$ is a scheme.[7]

Definition 2.10. For any ringed space $(X, \mathcal{O}_X)$, and $x \in X$, we define the stalk as the co-limit of neighbourhoods of points x, i.e.

$$\mathcal{O}_{X,x} = \varinjlim_U \Gamma(U, \mathcal{O}X)$$

where $U \in \mathcal{U}_x^X$.

Example 2.1.9. If X is a scheme, then $\mathcal{O}X, x = \Gamma(U, \mathcal{O}_X)_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal of $\Gamma(U, \mathcal{O}_X)$ corresponding to x. In this way, we can say $(X, \mathcal{O}_{X,x})$ is a **locally ringed space** if the stalks $\mathcal{O}_{X,x}$ are local rings for all $x \in X$. Our next immediate goal is to describe local rings for the étale topology.

Remark. The reader is reminded that $f \in \mathrm{Hom}_{\mathrm{RING}}(X, Y)$ is **flat** if $Y \otimes_X - : X - \mathrm{MOD} \to Y - \mathrm{MOD}$ is exact, and if X and Y are local rings such that

1. $f(\mathfrak{m}_X)Y = \mathfrak{m}_Y$;

2. $Y/\mathfrak{m}_Y$ is finite and separable over $\mathfrak{m}_X$,

[7] This follows from the fact that:

1. For any $\mathfrak{p} \in \mathrm{Proj}R$, the stalk $\mathcal{O}_{\mathfrak{p}}$ is isomorphic to the local ring $R_{\mathfrak{p}}$;
2. For any homogeneous $f \in R_+$, let $D_+(f) = \{\mathfrak{p} \in \mathrm{Proj}R \mid f \notin \mathfrak{p}\}$. Then $D_+(f)$ is open in Proj$R$. Furthermore these open sets cover Proj$R$ and for each such open set we have an isomorphism of locally ringed spaces $(D_+(f), \mathcal{O}|_{D_+(f)}) \cong \mathrm{Spec}R_{(f)}$ where $R_{(f)}$is the subring of elements of degree 0 in the localized ring R_f.

then f is **unramified**.

Definition 2.11. Let $\varphi \in \mathrm{Hom}_{\mathrm{SCH}}(Y, X)$. If for all $y \in Y$, the local homomorphisms $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ are flat, then φ is **flat**.

Remark. To aid topologists, if Z is a closed subscheme of X, then $\iota : Z \hookrightarrow X$ is flat if and only if Z is open, and thus a connected component of X.

Definition 2.12. Let $\varphi \in \mathrm{Hom}_{\mathrm{SCH}}(Y, X)$. If Y has an open cover of affine schemes $(\mathrm{Spec}V_i)_{i\in I}$ such that

$$\mathrm{Spec}U_i = \varphi^{-1}(\mathrm{Spec}V_i)$$

is an open affine subscheme of X and $\varphi|_{\mathrm{Spec}U_i}$ induces

$$\varphi' \in \mathrm{Hom}_{\mathrm{RING}}(V_i, U_i)$$

such that U_i is a finitely generated V_i-algebra, then φ is of **finite type**.

Furthermore, φ is **unramified** if, in addition to being of finite type, for all $y \in Y$,

$$\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$$

are unramified.

Example 2.1.10. An **étale morphism** is a morphism that is both flat and unramified. It will be useful to think of étale morphisms as the generalization of a local homeomorphism. Specifically, for a point p of a topological space X, a map $\varphi : X \to Y$ is **étale at point p** if the map of tangent spaces is an isomorphism, i.e. $d\varphi : TM_x(X) \to TM_{\varphi(x)}(Y)$ is an isomorphism, and so φ is **étale** if it is étale at all points of X. Abstracting further into varieties and schemes, with $V = \mathrm{Specm}\ k[X_1, \ldots, X_n]/\mathfrak{I}$ over some algebraically closed field, such that the geometric tangent cone at the origin is the zero set of

$$\mathfrak{I}_* := \{f_* \mid f \in \mathfrak{I}\}$$

If $k[X_1, \ldots, X_n]/\mathfrak{I}_*$ has nilpotents, we use the tangent cone $\mathrm{Spec}k[X_1, \ldots, X_n]/\mathfrak{I}_*$.

Thus, an **étale site** on X is the pair consisting of slice category of $\text{Et} \downarrow X$, whose morphisms are the étale morphisms $U \to X$ and whose morphisms are the standard slice category morphisms; a collection of surjective families of étale morphisms $(U_i \to U)$ drawn from the slice category. Given our earlier treatment of categorial semantics and dependent type theory, we are equipped to regard these étale maps as terms of type X, where X is a projective variety, with free variables of type U, or rather, free variables in the respective étale families. As will be embellished elsewhere, what we wish to count are these unique terms of X.

An **étale cover** of an algebraic scheme X is a set of jointly surjective étale morphisms

$$\{p_i : U_i \to X\}$$

which are **locally of finite type**, i.e there exists a covering of X by open affine subsets $X_j = \text{Spec}B_j$, and each the inverse image of each X_j in U_i can be covered by affine open subsets $U_{i,j,k} = \text{Spec}A_{i,j,k}$, with $A_{i,j,k}$ a finitely generated X_j-algebra.

From this fairly convoluted definition, we can recognize that one **étale site** of a scheme X is the slice category of $\text{Sch} \downarrow X$ equipped with the coverage $\mathcal{J}$ given by the étale covers. This defines the **big étale site on X**.

Remark. Now that we have a notion of sites, we are equipped with a working notion of topology in terms of coverage and sheaves. In particular, now that we have a good notion of étale morphisms, we can define an **étale topology** defined as follows:

For a space X in some appropriate category C, consider $\text{Et} \downarrow X$ as the subcategory of $\text{C} \downarrow X$. In particular, the objects we consider are etale morphisms $U \to X$. Then an étale covering

$$(\varphi_i : U_i \to U)_{i \in I}$$

is a covering of U if $U = \varphi_i(U_i)$, in which case was say that (φ_i) is a surjective family. We define an étale neighborhood of point x is simply an étale morphism $\varphi : U \to X$ such that there is some $u \in U$. For our needs, we consider a covering $\mathcal{J}$ that simply picks some surjective families (φ_i) of varieties or schemes to form a site $(\text{Et} \downarrow X, \mathcal{J})$, which we denote by $X_{\acute{e}t}$. The sheaves on this site

that we're interested in are Ab valued, and those are precisely the pre-sheaves such that

$$\mathcal{F}(U) \to \prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{(i,j)\in I\times I} \mathcal{F}(U_i \times_U U_j)$$

holds for all coverings.

It remains to show towards our goal of proving the Weil conjectures that $\mathrm{Sh}(X_{\acute{e}t})$ is an abelian category with enough injectives, so that $\mathcal{H}^r(X_{\acute{e}t};\mathcal{F})$ can be computed as the derived functor cohomology. When consider abelian group valued sheaves, clearly $\mathrm{Sh}(X_{\acute{e}t})$ form an additive category.To see that this is an abelian category, simply regard the map from the co-image of a morphism in $\mathrm{Sh}(X_{\acute{e}t})$ to its image; such a map is an isomorphism on its stalks, and hence is an isomorphism between morphisms. Thus we see that $\mathrm{Sh}(X_{\acute{e}t})$ is abelian.

Now, since $\mathrm{Sh}(X_{\acute{e}t})$ and $\mathrm{Sh}(Y_{\acute{e}t})$ are topoi for any schemes or varieties X and Y, a morphism $\pi : Y \to X$ induces a geometric morphism between $\mathrm{Sh}(X_{\acute{e}t})$ and $\mathrm{Sh}(Y_{\acute{e}t})$, namely $\pi^* \dashv \pi_* : \mathrm{Sh}(Y_{\acute{e}t}) \to \mathrm{Sh}(X_{\acute{e}t})$.[8][9] While it is clear that π_* is exact on pre-sheaves, it is generally not right exact for sheaves; crucially, π_* will be exact if π is a finite map or a closed immersion.

Finally, let $\mathcal{F} \in \mathrm{Ob}\ \mathrm{Sh}(X_{\acute{e}t})$. For any $x \in X$, we can choose a geometric point $\iota_x : \bar{x} \to X$ with its image x and an embedding $\mathcal{F}_{\bar{x}} \hookrightarrow I(x)$ of the abelian group $\mathcal{F}_{\bar{x}}$ into an injective abelian group via some pre-sheaf $\mathcal{P}$, from which we find that $\iota_{x*}(I(x))$ is injective.[10] Since products of injective objects are injective, $\prod \iota_{x*}(I(x))$ will define an injective sheaf, here denoted by $\mathcal{I}$. In this manner, we can construct an embedding for any sheaf $\mathcal{F}$ on $X_{\acute{e}t}$ as the composition of the natural inclusions $\mathcal{F} \hookrightarrow \mathcal{P}^* \hookrightarrow \mathcal{I}$. Thus, we see that we have enough injectives.

[8] For clarity, consider the direct image of any presheaf $\mathcal{F}$ on $Y_{\acute{e}t}$ and étale $U \to X$ by

$$\pi_*\mathcal{F}(U) = \mathcal{F}(U \times_X Y)$$

Since $U \times_X Y \to Y$ is étale, it follows that $\pi_*\mathcal{F}$ is a pre-sheaf on $X_{\acute{e}t}$. Moreover, if $\mathcal{F}$ is a sheaf, then $\pi_*\mathcal{F}$ is a sheaf as well, as we can restrict π_* from $\mathrm{PSh}(Y_{\acute{e}t})$ to $\mathrm{Sh}(Y_{\acute{e}t})$.

[9] To check adjointness, we can simply define the pushforward π_* of sheaves $\mathcal{F}$ in terms of the sheafification functor applied to to the colimit of $\mathcal{F}$ over the following diagrams of étale maps:

$$\begin{array}{ccc} V & \rightarrowtail & U \\ \downarrow & & \downarrow \\ X & \longrightarrow & Y \end{array}$$

[10] As a reminder, $\mathcal{F}_{\bar{x}} = (\iota^*\mathcal{F})(\bar{x})$ for any geometric point.

Finally, we observe that we have the following change of basis theorems:

Theorem 10. (Proper Base Change Theorem) *Let $\pi : X \to S$ be proper, and let $Y = X \times_S T$ be the pull-back for some morphism $f : T \to S$, i.e.*

$$\begin{array}{ccc} Y & \xrightarrow{f'} & X \\ {\scriptstyle \pi'}\downarrow & & \downarrow{\scriptstyle \pi} \\ T & \xrightarrow[\pi]{} & S \end{array}$$

Then for any torsion sheaf on X, there is a canonical isomorphism:

$$f^*(\mathcal{R}^r\pi_*\mathcal{F}) \to \mathcal{R}^r\pi'_*(f'^*\mathcal{F})$$

2.2 Classifying Topoi

Remark. The idea of classifying structures is not a new one unique to the predilections of topos theorists. Indeed, one of the principle activities of a research mathematician is the classification of certain structures (or theories) up to some notion of equivalence, be it homotopy, or isomorphism, or path equality. However, topos theory provides mathematicians with a framework for describing *new* classifying structures, namely by classiying structures over a topos by maps into another, suitably constructed topos.

In one sense, all topoi classify some structure by virtue of the fact any topos is equipped with geometric morphisms. To that end, once we've defined a classifying topos, I'll give a few examples of a classifying topos.

Definition 2.13. Let $\mathbf{E}$ and $\mathbf{F}$ be two topoi. Then $\textsc{Hom}(\mathbf{E}, \mathbf{F})$ is a category whose objects are geometric morphisms $f : \mathbf{E} \to \mathbf{F}$ and whose morphisms are natural transformations $f^* \to g^*$.

Definition 2.14. Let $\mathbb{T}$ by a collection of axioms that we wish to describe some structure. By convention, we denote the **$\mathbb{T}$-models** in $\mathbf{E}$ by M.[11] The functor $\mathcal{M}(\mathbf{E}, \mathbb{T})$ is a contravariant set-valued functor of $\mathbf{E}$ for any arbitrary $\mathbb{T}$, which takes $\mathbf{E}$ to the set of all $\mathbb{T}-$models in $\mathbf{E}$, and where the inverse image of a geometric morphism $f : \mathbf{F} \to \mathbf{E}$ will carry any $\mathbb{T}-$model M in $\mathbf{E}$ to a $\mathbb{T}-$structure f^*M in $\mathbf{F}$.[12]

Definition 2.15. Suppose that $\mathbb{T}$ is a geometric theory with a given signature σ. The **classifying topos** for $\mathbb{T}$ is some Grothendieck topos $\mathbf{B}(\mathbb{T})$ over $\textsc{Sets}$, such that there is the following natural equivalence of categories $\kappa_{\mathbf{E}} : \textsc{Hom}(\mathbf{E}, \mathbf{B}(\mathbb{T})) \cong \mathcal{M}(\mathbf{E}, \mathbb{T})$, i.e.

$$\begin{array}{ccc} \textsc{Hom}(\mathbf{E}, \mathbf{B}(\mathbb{T})) & \xrightarrow{\kappa_{\mathbf{E}}} & \mathcal{M}(\mathbf{E}, \mathbb{T}) \\ \Big\downarrow{\scriptstyle \textsc{Hom}(f, \mathbf{B}(\mathbb{T}))} & & \Big\downarrow{\scriptstyle - \circ f} \\ \textsc{Hom}(\mathbf{F}, \mathbf{B}(\mathbb{T})) & \xrightarrow[\kappa_{\mathbf{F}}]{} & \mathcal{M}(\mathbf{F}, \mathbb{T}) \end{array}$$

[11] These are alternatively all such $\mathbb{T}-$structures in a topos $\mathbf{E}$.
[12] To convince yourself this works, consider the geometric morphism over $\textsc{Sets}$.

commutes. A rather powerful result of this naturality is that for every geometric morphism f, $\kappa_{\mathbf{F}}(f^*M) \cong \kappa_{\mathbf{E}}(M) \circ f$.

Remark. Much of the initial impulse behind this project has been inspired by the following theorem:

Theorem 11. *Suppose that* $\mathbb{T}$ *is a geometric theory. Then* $\mathbb{T}$ *has a classifying topos.*

Example 2.2.1. (Object Classifiers)A prototypical classifying topos is a Grothendieck topos called the **object classifier**, denoted $\mathbf{S}[U]$ with the property that for any cocomplete topos $\mathbf{E}$, there is an equivalence between Ob $\mathbf{E}$ and $f : \mathbf{E} \to \mathbf{S}[U]$, i.e. there is an natural equivalence $c_{\mathbf{E}} : \mathbf{E} \xrightarrow{\sim} \textsc{Hom}(\mathbf{E}, \mathbf{S}[U])$ sending $X \in$ Ob $\mathbf{E}$ to the characteristic geometric morphism $\mathbf{E} \to \mathbf{S}[U]$.

Example 2.2.2. While the previous example is a relatively nice example of a classifying topos, the prototypical (and for this paper, the most important) example of classifying algebraic and geometric structures by their maps into a given space comes from topology. While the study of cohomology developed in part by research into classifying fibrations using the tools of Galois theory,[13] the classifying space for cohomology, or the *Eilenberg-Mac Lane space* classifies the cohomology classes by assigning them to a map from the underlying space X to the Eilenberg-Mac Lane space. Specifically, this is a classification of every $n-$dimensional cohomology of *any* space X to a unique map up to homotopy.

The traditional, nonsingular cohomology functors are defined defined as bi-functors

$$\mathcal{H}^n(-;-) : \textsc{Top} \times \textsc{Ab} \to \textsc{Ab}$$

that are contravariant with respect to topological spaces X and covariant for spaces G. Rather importantly, for any $f, g \in \mathrm{Hom}_{\textsc{Top}}(X, Y)$, if $f \simeq g$, then they induce the same group cohomology homomorphism, so that the Eilenberg-Mac Lane space, denoted by $K(G, n)$ for each cohomology functor $\mathcal{H}^n(-; G)$, is a space such that $\mathcal{H}^n(K(G, n); G) \cong \mathrm{Hom}_{\textsc{Ab}}(G, G)$. With some work, one shows that every n-dimensional cohomology class for any topological space X arises by pulling back the universal cohomology class $\gamma_n \in \mathcal{H}^n(K(G, n); G)$, along the map $X \to K(G, n)$. From here, we can use $K(G, n)$ to construct *new* cohomology operations. Now, one of the key steps to proving the

[13] I have Postnikov towers in mind.

Weil conjectures (from the point of view of intuitionistic type theory) begins with the recognition that although there are many species of cohomology, many of them can be captured by the following definition:

Definition 2.16. Given an $(\infty,1)-$category $\mathbf{H}$ with objects X and A, an *intelligible A-cohomology of X* is defined in terms of the $(\infty,1)$-categorical hom-space $\mathbf{H}(X,A)$, which is regarded as an $\omega-$groupoid. In particular, **cocycles on X with coefficients in A** are $c \in \mathrm{Ob}\ \mathbf{H}(X,A)$, and the **coboundaries** are arrows $\delta \in \mathrm{Ar}\ \mathbf{H}(X,A)$. The **A-cohomology set of X** is defined to be the set of connected components of $\pi_0\mathbf{H}(X,A)$, i.e. $\mathcal{H}(X;A) := \pi_0\mathbf{H}(X,A)$, and for any A-cocycle c on X and B-cocycles k on A, the class of the composite cocycles, denoted $[k(c)]$ and given by

$$[k(c)] := [k \circ c] \in \mathcal{H}(X;A)$$

is the **characteristic class of c with respect to k.**

If A admits deloopings to objects in an $\omega-$groupoid $\mathbf{B}^n A$, then the **A-cohomology of degree n** is the set of connected components of the ω-groupoid from X to the objects in $\omega-$groupoid $\mathbf{B}^n A$, i.e.

$$\mathcal{H}^n(X;A) := \pi_0\mathbf{H}(X,\mathbf{B}^n(A))$$

Noticeably absent from this definition is the notion of cochains, which arise when working within specific models for $\mathbf{H}(X,A)$ determined by objects A that are components of a *spectrum object* in Stab $\mathbf{H}$.[14]

2.2.1 Étale cohomology

Remark. Building off of our discussion of abelian cohomology in Example 2.2.2, $\Gamma(X_{ét},-) : \mathrm{Sh}(X_{ét}) \to \mathrm{Ab}$ is the **global section functor** defined by the mapping $\mathcal{F} \mapsto \Gamma(X,\mathcal{F})$. Clearly $\Gamma(X_{ét},-)$ is covariant, and moreover, it is left exact. Because this functor is left exact, we can intelligibly discuss the cohomology of étale sheaves. Most importantly, it is known that there is a spectral sequence relating the derived functor of étale cohomology to the familiar Čech cohomology theory,so that the

[14]This is a very wonky way of saying that given $\Sigma^\infty \dashv \Omega^\infty :$ Stab $\mathbf{H} \to \mathbf{H}$, where Ω^∞ is the canonical forgetful functor whose left adjoint Σ^∞ *freely stabilizes* any object of $\mathbf{H}$, so that $A \equiv E_n :\equiv \Omega^\infty \circ \Sigma^n E$.

cohomology theories relevant to the proof of the Weil conjectures can actually be computed.

Definition 2.17. Suppose that $X_{\acute{e}t}$ is an étale site and $\Gamma(X_{\acute{e}t}, -)$ is the global section functor. We then set $\mathcal{H}^r(X_{\acute{e}t}; -) := \mathcal{R}^r\Gamma(X_{\acute{e}t}, -)$, so that the r^{th} **étale cohomology functor** is simply the r^{th} right derived functor of the global section functor. Thus it should be clear how $\mathcal{H}^r(X_{\acute{e}t}; -)$ acts on sheaves $\mathcal{F}$. Given $\mathcal{F}$ and an injective resolution $\mathcal{I}^\bullet$, we first apply $\Gamma(X_{\acute{e}t}, -)$ to $\mathcal{I}^\bullet$ to obtain the following complex:

$$\Gamma(X_{\acute{e}t}, \mathcal{I}^0) \to \Gamma(X_{\acute{e}t}, \mathcal{I}^1) \to \Gamma(X_{\acute{e}t}, \mathcal{I}^2) \to \cdots$$

From here, we can apply $\mathcal{R}^r$ to recover the appropriate r^{th} cohomology group. In particular, these functors are uniquely determined up to isomorphism.

Chapter 3

Weil Cohomology Theories and the Proof of the Weil Conjectures

One rather remarkable fact about Riemann's original zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{3.0.1}$$

is that it has a deep connection with prime numbers, as exhibited by the following identity:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \tag{3.0.2}$$

This fact was proven by Euler for $\Re(s) > 1$, and relies on little more than elementary facts about geometric series and the fundamental theorem of arithmetic. Among the remarkable properties of zeta functions is there is a functional equation, which in some cases captures topological information.[1] In the case of Equation (3.0.2), this functional equation is given by

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s) \tag{3.0.3}$$

[1] This is certainly the case with the Weil conjectures, and non-singular projective varieties over fields of positive characteristic.

With this functional equation, it can be shown that $\zeta(s)$ has zeros for $s \in 2\mathbb{Z}$, called *trivial zeros*.[2] However, in stark contrast to these trivial zeroes, characterizing the set of the non-trivial zeros for $\zeta(s)$ is currently one of the greatest unsolved problems in mathematics, the *Riemann hypothesis*. This problem has attracted much research attention over the last century and a half, and the study of zeta functions has found much application across many different areas of geometry ranging from complex analytic geometry to arithmetic geometry.

One example of this reach is the study of the class of meromorphic zeta functions on the complex plane that behave like analytic continuations of traces of powers for suitable differential operators H, e.g.

$$s \mapsto \zeta(s); \qquad s \mapsto \mathrm{Tr}\left(\frac{1}{H}\right)^s \tag{3.0.4}$$

For sufficiently well behaved H, such as Feynman propagators, these sums are in the form $s \mapsto \sum_{\lambda} \lambda^{-s}$, where the eigenvalues express vacuum amplitudes.

Dedekind zeta functions are among the earliest generalizations of the Riemann zeta function, generalizing ζ from $\mathbb{Q}$ to arbitrary number fields K and their rings of integers $\mathcal{O}_K$. Analogously, just as one considers Dedekind zeta functions to study arbitrary number fields, one can consider *Weil zeta functions* to study certain function fields.

The Weil zeta functions are of particular interest to this project, both as the inspiration for topos theory and the source of inspiration for the tools of modern algebraic geometry (schemes), but also in their own right as the motivation for étale cohomology, as well as for the practical purpose of discerning the number of solutions for polynomial equations over finite fields.

A *Weil zeta function*,

$$\zeta(X;t) = \exp\left(\sum_{m=1} N_m \frac{t^m}{m}\right) \tag{3.0.5}$$

is a zeta function for arithmetic varieties X_0 over finite fields $\mathbb{F}_q$ with algebraic closure $\mathbb{F}$, and where N_m is the number of points in $X = X_0 \times_{\mathbb{F}_q} \mathbb{F}$, the corresponding scheme over $\mathbb{F}$, which are rational over the field $\mathbb{F}_{q^r}$, i.e. they lie in $\mathbb{F}_{q^r}$. Weil conjectured that the Weil zeta function crucially satisfies the following four properties:

[2] This fact follows rather immediately by considering the value of $\sin\left(\frac{\pi s}{2}\right)$ for these values s.

1. (Betti Numbers) Define the i^{th} Betti number $\beta_i = \beta_i(X)$ to be the degree of $P_i(X;t)$. Then $\chi = \sum(-1)^i\beta_i$. If X has a lift to a variety Y of characteristic zero, then β_i is precisely the i^{th} Betti number for Y in the traditional sense.

   Remark. Importantly, for a space Y, the r^{th} Betti number refers to the rank of the r^{th} homology group of Y. Classically, these correspond to a *measure* of higher-dimensional connectivity of Y, and is related to the *Euler characteristic*. That the classical notions hold in the case of non-singular projective varieties is an important geometric fact.

2. (Rationality) $\zeta(X;t)$ is the quotient of polynomials $P_i(X,t)$ with rational coefficients, given by

$$\zeta(X;t) = \frac{P_1(X;t)\cdot P_3(X;t)\cdot \ldots \cdot P_{2n-1}(X;t)}{P_0(X;t)\cdots P_{2n}(X;t)} \tag{3.0.6}$$

3. (Functional Equation) Where χ is the self intersection number of the diagonal Δ of $X \times X$,

$$\zeta(X;\frac{1}{q^n t}) = \pm q^{n\chi/2}t^{\chi}\zeta(X;t) \tag{3.0.7}$$

4. (Analogue of Riemann Hypothesis) $P_i(X;t) = \prod(1-\lambda_{ij}t)$, and λ_{ij} are algebraic integers with $|\lambda_{ij}| = q^{i/2}$.

Although one can use diverse techniques to prove these conjectures in individual cases, a great deal of formal machinery is required to prove these conjectures for the appropriate arbitrary varieties. The pursuit of proof for the conjectures can be characterized as a search for the right cohomology theory for varieties, such that the cohomology yields both the correct Betti numbers as well as having its coefficients in a field of characteristic zero. This latter fact is of immense importance, as it allows one to make use of the facts about the cohomology varieties over the complex numbers, among them the Comparison Theorem:

Theorem 12. (Comparison Theorem) *Let X be a non-singular variety over $\mathbb{C}$. Then, for any finite abelian group Λ, and $r \geq 0$,*

$$\mathcal{H}^r(X_{\acute{e}t};\Lambda) \cong \mathcal{H}^r(X_{cx};\Lambda)$$

Another crucial result from complex geometry is the Lefschetz fixed point formula for a regular map $\varphi : X \to X$, where X is a complete nonsingular variety over an algebraically closed field k:

$$(\Gamma_\varphi \cdot \Delta) = \sum (-1)^r \mathrm{Tr}(\varphi | \mathcal{H}^r(X; \mathbb{Q}_\ell)) \tag{3.0.8}$$

3.1 Weil Cohomology Theories

Grothendieck's most crucial contribution to proving these conjectures was the observation that a *Weil cohomology theory* is a pre-requisite for proving the conjectures, and his development of one such cohomology theory, the *ℓ-adic cohomology*, which is defined as follows:

Definition 3.1. Let X be a scheme of finite type over an algebraically closed field k of characteristic $p \geq 0$ and let $\ell \neq p$ be a prime number. We define the *ℓ-adic integers* as the projective limit

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$$

and let the *ℓ-adic numbers* $\mathbb{Q}_\ell$ be the quotient field of $\mathbb{Z}_\ell$. The *ℓ-adic cohomology* of X is then defined as:.

$$\mathcal{H}^q(X;\mathbb{Q}_\ell) = \varprojlim_n \mathcal{H}^q(X_{\acute{e}t};\mathbb{Z}/\ell^n\mathbb{Z}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

Throughout this chapter we detail material invoked in the proofs throughout Part II. In particular, this chapter sketches the properties of a Weil cohomology theory, illustrating how $\ell-$adic cohomologies are one instance of such a theory. This material is necessarily prior to the proof of the Weil conjecture, and so in order to achieve the long-term goal of a formally verified proof of the Weil conjectures, these results ought to be formulated in some internal language as geometric formula, as described in Chapters 2 and 3.

Definition 3.2. A **Weil cohomology theory** is a contravariant functor $\mathcal{H}^*$ taking nonsingular projective varieties X of dimension n to graded K-algebras, where K is a field of characteristic zero, such that $\mathcal{H}^*(X)$ is a graded K-algebras satisfying the following:

1. For $r \in \lceil 2d \rceil$, $\mathcal{H}^r(X)$ are finite dimensional K-vector spaces;
2. $\mathcal{H}^r(X) = 0$ for $r \notin \lceil 2d \rceil$;
3. $\mathcal{H}^{2d}(X) \cong K$;
4. **(Künneth Formula)** $\mathcal{H}^*(X) \otimes \mathcal{H}^*(Y) \cong \mathcal{H}^*(X \times Y)$;
5. **(Poincaré Duality)** $\mathcal{H}^r(X) \times \mathcal{H}^{2n-r}(X) \to \mathcal{H}^{2n}(X) \cong K$;

6. **(Cycle Maps)** There exists $\gamma_X : \mathcal{C}^r(X) \to \mathcal{H}^{2r}(X)$, where $\mathcal{C}^r(X)$ is the free group generated by prime cycles[3] of codimension r, such that γ_X satisfies certain compatibility conditions with respect to the functorality of $\mathcal{H}$, the Künneth formula, and Poincaré duality, and such that $\gamma_X : \mathbb{Z} \hookrightarrow K$ if X is a point.

   Some authors extend these to the Lefschetz axioms:

7. For any smooth hyperplane section $j : W \subset X$ and $r \leq n-2$, $j^* : \mathcal{H}^r(X) \cong \mathcal{H}^r(W)$, and j^* monic for $r \leq n-1$;

8. Further, for $\omega = \gamma_X(W) \in \mathcal{H}^2(X)$, the *Lefschetz operator* $L : \mathcal{H}^r(X) \to \mathcal{H}^{r+2}(X)$ is defined by $x \mapsto x \cdot \omega$, and $L^r : \mathcal{H}^{n-r}(X) \to \mathcal{H}^{n+r}(X)$ is an isomorphism for $r \in \lceil n \rceil \backslash \{0\}$.

With the proof of the Weil conjectures in mind, ideally this chapter would be devoted to justifying how we get a Lefschetz trace formula for $\ell-$adic cohomology functor $\mathbb{Q}_\ell$. In turn, this means showing that we have a Künneth formula, Poincaré duality, and a *good cycle map*. However, due to time constraints, this chapter is mostly left as exposition with occasional proofs. Many of the results that we admit here should present reasonably attainable goals for future work.

For some commutative ring R with unity, denote the group of singular p-cochains of X with coefficients in R by $S^p(X, R) = \mathrm{Hom}(S_{\mathrm{P}}(X), R)$. Furthermore, let $T : \Delta_{p+q} \to X$ be a singular $p+q$ simplex. Then, we define the map

$$S^p(X, R) \times S^q(X; R) \xrightarrow{\smile} S^{p+q}(X, R)$$

by

$$\langle c^p \smile c^q, T \rangle = \langle c^p, T \circ l(\varepsilon_0, \ldots, \varepsilon_p) \rangle \cdot \langle c^q, T \circ l(\varepsilon_p, \ldots, \varepsilon_{p+q}) \rangle \tag{3.1.1}$$

where the cochain $c^p \smile c^q$ is the *cup product* of the cochains c^p and c^q, and where the mapping $T \circ l$ is just the restriction of T to the faces Δ_p and Δ_q of Δ_{p+q} for $(\varepsilon_0, \ldots, \varepsilon_p)$ and $(\varepsilon_p, \ldots, \varepsilon_{p+q})$ respectively.[4] It can be shown that this definition is bilinear and associative, and moreover, that it

[3] Recall that a prime cycle on X is an irreducible, closed subvariety.

[4] This requires that we define $l(w_0, \ldots, w_p)$ to be the linear singular simplex mapping ε_i into w_i for $0 \leq i \leq p$.

induces such an operation on

$$\mathcal{H}^p(X;R) \times \mathcal{H}^q(X;R) \to \mathcal{H}^{p+q}(X;R)$$

where the cohomology class $\{z^0\}$ is the unity element.

Throughout this paper, we denote the *cohomology ring* of X with coefficients in a commutative ring with identity R by $\mathcal{H}^*(X;-) = \oplus\mathcal{H}^i(X;R)$, where the cup product turns this group into a ring with a unity element.

Definition 3.3. A **perfect pairing** is an R-linear isomorphism of R modules $\phi : M \to \mathrm{Hom}_R(N, L)$ such that $\phi(m)(n) := e(m,n)$, where $e : M \times N \to L$ is an R-bilinear mapping satisfying

1. $e(rm, n) = e(m, rn) = re(m, n)$
2. $e(m_1 + m_2, n) = e(m_1, n) + e(m_2, n)$
3. $e(m, n_1 + n_2) = e(m, n_1) + e(m, n_2)$

for any $r \in R$, $m, m_1, m_2 \in M$ and $n, n_1, n_2 \in N$.

The following lemma, found in [8], Appendix C, Lemma 4.3, will be necessary for proving the functional equation:

Lemma 13. *Let $\phi : V \times W \to K$ be a perfect pairing over a field K. Let $f \in End_K(V)$ and $g \in End_K(W)$ and $\lambda \in K^\times$ such that for all $x \in V$ and $y \in W$,*

$$\phi(f(x), g(y)) = \lambda\phi(x, y)$$

Then

$$\det(id - tg) = \frac{(-1)^d \lambda^d t^d}{\det(f)} \cdot \det(id - \frac{f}{\lambda t})$$

and

$$\det(g) = \frac{\lambda^d}{\det(f)}$$

Remark. This lemma will become useful when paired with the assumption Poincaré duality and the existence of a perfect pairing between cohomology groups regarded as vector spaces over $\mathbb{Q}_\ell$.

3.2 Good Cycle Maps

In order to associate a cohomology class to an algebraic cycle on a variety, we require the existence of a *good* cycle map

$$cl_X^* : C\mathcal{H}^r(X;-) \to \mathcal{H}^r(X;-)$$

The rest of this section explores what this actually entails.

Notation. First, we fix our notation. Let k be an algebraically closed field of characteristic p and X be a non-singular variety over k. Let $\Lambda = \mathbb{Z}/\ell^n\mathbb{Z}$ for $\ell, n \in \mathbb{Z}^+$ such that $\ell \neq p$. Finally, set

$$\mathcal{H}^*(X;\Lambda) := \bigoplus_{r\geq 0} \mathcal{H}^{2r}(X;\Lambda(r))$$

such that $\mathcal{H}^*(X;\Lambda)$ is a ring under the cup product. Eventually, we will want to have $\mathcal{H}^*(X;\mathbb{Q}_\ell) := \bigoplus_{r\geq 0} \mathcal{H}^{2r}(X;\mathbb{Q}_\ell(r))$.

Remark. With $\Lambda = \mathbb{Z}/\ell^n\mathbb{Z}$, $n \in \mathbb{Z}^+$ as above, and any ring R such that n is a unit in R, we define $\mu_n(R)$ to be the group of n^{th} roots of unity in R, and

$$\mu_n(R)^{\otimes r} = \begin{cases} \mu_n(R) \otimes \cdots \otimes \mu_n(R) & \text{r copies, } r > 0 \\ \Lambda & r = 0 \\ \mathrm{Hom}_\Lambda(\mu_n(R)^{\otimes -r}, \Lambda) & r < 0 \end{cases}$$

We note that the r^{th}-twist of Λ, $\Lambda(r)$ is the sheaf on $X_{\acute{e}t}$ such that for any étale and affine $U \to X$,

$$\Gamma(U, \Lambda(r)) = \mu_n(\Gamma(U, \mathcal{O}_U))^{\otimes r}$$

Notably, if the ground field of X, contains the n^{th} roots of unity, then each sheaf is isomorphic to the constant sheaf of Λ and the choice of our primitive root of unity determines isomorphisms

$$\Lambda(r) \cong \Lambda$$

for all r, so that each sheaf $\Lambda(r)$ is locally constant.

In order to introduce the notion of **Gysin sequences** (and maps), we admit the following theorem:

Theorem 14. *Let k be an algebraically closed field, and let Z be a nonsingular subvariety of X, such that every connected component of Z has codimension c in every corresponding component of X. For any locally constant sheaf $\mathcal{F}$ of Λ-modules on X,*

$$\mathcal{R}^r i^! \mathcal{F} \cong (i^* \mathcal{F}) \qquad r = 2c$$

and otherwise

$$\mathcal{R}^r i^! \mathcal{F} = 0$$

Notation. Let (Z, X) be as in the theorem. Then we say (Z, X) is a smooth pair. We set $U = X \backslash Z$, and denote the inclusion of Z in X by i and the inclusion of U in X by j. For a sheaf $\mathcal{F}$ on X, we define $\mathcal{F}^!$ to be the largest subsheaf of $\mathcal{F}$ with support on a closed sub-variety Z of X, so that for any étale map $\varphi : V \to X$, we find for $f : \mathcal{F} \to j_* j^* \mathcal{F}$ that

$$\mathcal{F}^! = \ker(f)$$

by

$$\mathcal{F}^!(V) = \Gamma_{\varphi^{-1}(Z)}(V, \mathcal{F}) = \ker(\mathcal{F}(V) \to \mathcal{F}(\varphi^{-1}(U)))$$

Finally, it is natural to regard $i^! \mathcal{F}$ as the sheaf $\mathcal{F}$ restricted to Z.

Definition 3.4. For X a nonsingular variety over an algebraically closed field k, let

$$C^*(X) := \oplus C^i(X),$$

where $C^i(X)$ are the free abelian groups generated by the prime cycles of codimension i whose elements are the algebraic cycles of codimension I on X. Then the quotient $C\mathcal{H}^r(X; \Lambda)$ of $C^*(X)$ by rational equivalence becomes a ring relative to the *intersection product* called the **Chow ring**. In

particular, there is a canonical homomorphism of graded rings

$$cl_X^* : C\mathcal{H}^r(X;\Lambda) \to \mathcal{H}^r(X;\Lambda)$$

which for our purposes will be given by

$$cl^r : C^r(X) \to \mathcal{H}^{2r}(X;\Lambda(r))$$

which is defined as follows:

Let Z be a prime cycle in X with codimension r and let Y be the singular locus of Z. There is an isomorphism

$$\mathcal{H}^{2r}(X;\Lambda)_Z \cong \mathcal{H}^{2r}(X\backslash Y;\Lambda)_{Z\backslash Y}$$

from which we define $cl_X(Z)$ to be the image of 1 under the following mapping:

$$\Lambda \cong \mathcal{H}^0(Z\backslash Y;\Lambda(r)) \cong \mathcal{H}^{2r}(X\backslash Y;\Lambda(r))_{Z\backslash Y} \cong \mathcal{H}^{2r}(X;\Lambda(r))_Z \to \mathcal{H}^{2r}(X;\Lambda(r))$$

Since we've defined this for the unit, we can extend this linearly to obtain the desired homomorphism.

For the purposes of the proof of the Weil conjectures using ℓ-adic cohomology classes, what this really entails is that we prove there exist s a canonical homomorphism of graded rings such that $cl_X^* : C\mathcal{H}^1(X;\Lambda) \to \mathcal{H}^2(X;\Lambda(1))$, where $\Lambda = \mathbb{Z}/\ell^n\mathbb{Z}$ for $\ell \neq p$, where p is the characteristic of the ground field k. Notably, we will be able to extend these maps to the cohomologies of $\mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$.

Lemma 15. *Suppose (e_i) is a basis for $\mathcal{H}^r(X;\mathbb{Q}_\ell)$, and suppose (f_i) is a basis of $\mathcal{H}^r(X;\mathbb{Q}_\ell)$ that is dual relative to the cup-product with (e_i), such that $e_i \smile f_j = \delta_{ij}e^{2n}$. Then for any regular $\varphi : X \to X$, with induced $\phi^* : \mathcal{H}^r(X;\mathbb{Q}_\ell) \to \mathcal{H}^r(X;\mathbb{Q}_\ell)$,*

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

Proof. First, we notice that (f_i) forms a basis for $\mathcal{H}^r(X;\mathbb{Q}_\ell)$ as a $\mathbb{Q}_\ell$-vector space. Then, since $\mathcal{H}^*(X\times X;\mathbb{Q}_\ell) \cong \mathcal{H}^r(X;\mathbb{Q}_\ell) \otimes \mathcal{H}^r(X;\mathbb{Q}_\ell)$, we can regard the (f_i) as also forming the basis for a

$\mathcal{H}^r(X;\mathbb{Q}_\ell)$-module. Thus

$$cl_{X\times X}(\Gamma_\varphi) = \sum a_i \otimes f_i$$

for unique elements $a_i \in \mathcal{H}^r(X;-)$. Then, since $p_*(cl_{X\times Y}(\Gamma_\varphi) \cup q^*(y)) = \varphi^*(y)$,

$$\varphi^*(e_j) = p_*((\sum_i a_i \otimes f_i) \cup (1 \otimes e_j)) = p_*(a_j \otimes e^{2n}) = a_j$$

□

3.3 Künneth Formulae

Although obscure, it is known that for groups G and H that the extension functor $\texttt{Ext}(H, G)$ not only measures how much $\text{Hom}(H, G)$ fails to be exact, but quite literally does so by giving the set of isomorphism classes of extensions of G by H. We can parse this by considering these classes to be described by short exact sequences

$$0 \to G \to J \to H \to 0$$

with the obvious isomorphisms. This leads us to the following theorem:

Theorem 16. (Universal Coefficient Theorem) *If C is a chain complex of free abelian groups with homology groups $\mathcal{H}_n(C; -)$, then $\mathcal{H}^n(C; G)$ of the cochain complex $Hom(C_n, G)$ is determined by the split exact sequences*

$$0 \to \texttt{Ext}(\mathcal{H}_{n-1}(C; -), G) \to \mathcal{H}^n(C; G) \xrightarrow{h} Hom(H_n(C), G) \to 0$$

One special case of this theorem that is immensely useful concerns computing the cohomology of a product space, which are reached in our relevant cohomology ring by means of the cup product. When considering some notion of a product space, this result is then known as a called *Künneth formula*. For now, we treat the following isomorphism as a black box:

$$\mathcal{H}^r(X \times Y; E) \cong \mathcal{H}^r(X; E) \otimes \mathcal{H}^r(Y; E)$$

from which we find

$$\mathcal{H}^r(X \times X; -) \cong \mathcal{H}^r(X; -) \otimes \mathcal{H}^r(X; -)$$

by the pairing

$$p^*(a) \smile q^*(b) \cong a \otimes b$$

where $p, q : X \times X \to X$ are the canonical projection maps. Since $\mathcal{H}^r(X; \mathbb{Q}_\ell) = \oplus \mathcal{H}^r(X; \mathbb{Q}_\ell)$, we are thus working with a $\mathbb{Q}_\ell$-algebra. Even more remarkable, for any cohomology with similar formal

properties to the ℓ-adic cohomology, similar results to the Weil conjectures follow- these are *Weil cohomology theories*. The full development of $\ell-$*adic cohomology* from [4] is beyond the scope of this paper, although [14] develops the essentials in greater detail, and [8] concisely summarizes (most of) the following key properties of ℓ*-adic cohomology*, assuming that X is a smooth and proper scheme of finite type over an algebraically closed field k of characteristic $p \geq 0$:

- If X is a complete non-singular variety over an algebraically closed field k of characteristic $p \neq 0$, X can be *lifted to characteristic 0* if

  1. there is a discrete valuation ring R with a field of fractions K of characteristic 0 and residue field k;
  2. a scheme $\pi : \chi \to S$, with $S = \text{Spec}R$, which is proper and smooth over S whose special fibre is X.

- For any complete nonsingular variety X_0 over an algebraically closed field k of characteristic > 0 that has been lifted to a complete nonsingular variety X_1 in K, characteristic 0, then

  $$\mathcal{H}^q(X_0; \Lambda) \cong \mathcal{H}^q(X_{cm}; \Lambda)$$

  for all q, where X_{cm} is the associated complex manifold in the classical topology;

- By the comparison theorem, if X is smooth and proper over $\mathbb{C}$, then

  $$\mathcal{H}^q(X; \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \cong \mathcal{H}^q(X_{cm}; \mathbb{Q}_\ell)$$

- We regard the $\mathcal{H}^q(X; \mathbb{Q}_\ell)$ groups as a vector spaces over $\mathbb{Q}_l$. By the cohomology of complex projective space, the $\mathcal{H}^q(X; \mathbb{Q}_\ell)$ are 0, except for $0 \leq q \leq 2n$, where $n = \dim X$. In particular, if M is a module and X is a projective n-space over $\mathbb{C}$, then

  $$\mathcal{H}^q(\mathbb{P}^n(\mathbb{C}); M) = \begin{cases} M & q \in \{0, 2, \ldots, 2n\} \\ 0 & \textit{otherwise.} \end{cases}$$

so it suffices to notice that we can regard $\mathbb{Q}_\ell$ above as a module as $\mathbb{Z}_\ell$ can be given a finitely generated module M by the family $(M_n, f_{n+1} : M_{n+1} \to M_n)_{n\in\mathbb{N}}$ such that

- for all n, M_n is a finite $\mathbb{Z}/\ell^n\mathbb{Z}$ module;
- for all n, the map $f_{n+1} : M_{n+1} \to M_n$ induces an isomorphism $M_{n+1}/\ell^n M_{n+1} \to M_n$

such that we can recognize $M = \varprojlim M_n = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathbb{Q}_\ell$, and so in this case, we immediately are left with

$$\mathcal{H}^q(\mathbb{P}^n(\mathbb{C}); \mathbb{Q}_\ell) = \begin{cases} \mathbb{Q}_\ell & q \in \{0, 2, \ldots, 2n\} \\ 0 & \textit{otherwise.} \end{cases}$$

In general, when given the $\mathbb{Q}_\ell$ sheaf, it is a sheaf of $\mathbb{Q}_\ell$ modules. Since $\mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ as a module over $\mathbb{Z}_\ell$ is simply $\mathbb{Q}_\ell$ as a one dimensional vector space, when working with the cohomology of complex projective n-space, we only need to consider a single basis element. In general, we will not be as lucky.

- $\mathcal{H}^i(X; \mathbb{Q}_l)$ is a contravariant functor in X;
- For all q, r, there is a cup-product structure

$$\mathcal{H}^q(X; \mathbb{Q}_\ell) \times \mathcal{H}^r(X; \mathbb{Q}_\ell) \to \mathcal{H}^{q+r}(X; \mathbb{Q}_\ell)$$

- (*Poincaré duality*) $\mathcal{H}^{2n}(X; \mathbb{Q}_\ell)$ is 1-dimensional and the cup-product pairing

$$\mathcal{H}^q(X; \mathbb{Q}_\ell) \times \mathcal{H}^{2n-q}(X; \mathbb{Q}_\ell) \to \mathcal{H}^{2n}(X; \mathbb{Q}_\ell)$$

  is a perfect pairing for each $q \in \{0, 1, \ldots, 2n\}$;
- (*Lefschetz fixed point theorem*) Let $f : X \to X$ be a morphism with isolated fixed points. For each fixed point $x \in X$ with multiplicity 1, let

$$N(f, X) = \sum (-1)^q \mathrm{Tr}(f^*; \mathcal{H}^q(X; \mathbb{Q}_\ell))$$

where f^* is the induced map on the cohomology of X;

- If Z is a subvariety of codimension q, then associated to Z is a cohomology class $\eta(Z) \in \mathcal{H}^{2q}(X;\mathbb{Q}_\ell)$, which is a homomorphism from the Chow ring $CH(X)$ to the cohomology ring $\mathcal{H}^*(X;\mathbb{Q}_\ell)$. If $\bar{x} \in X$ is a closed point, then $\eta(\bar{x}) \in \mathcal{H}^{2n}(X;\mathbb{Q}_\ell)$ is nonzero.[5]

[5]This is detailed in section 23 in [14]. By linearity, we extend this map to cycles, and notice for future reference that the intersection of cycles becomes the cup-product of cohomology classes.

3.4 Poincaré Duality

As in the classical case, we let U denote an oriented, connected $m-$dimensional complex manifold. Then there is a canonical isomorphism

$$\mathcal{H}^r(U;\mathbb{Z}/n\mathbb{Z})_c \cong \mathcal{H}_{2m-r}(U;\mathbb{Z}/n\mathbb{Z})$$

and so by the duality of $\mathcal{H}^q(-;-)$ and $\mathcal{H}_q(-;-)$, this is rewritten as a *perfect pairing*

$$\mathcal{H}^r(U;\mathbb{Z}/n\mathbb{Z})_c \times \mathcal{H}^{2m-r}(U;\mathbb{Z}/n\mathbb{Z}) \to \mathcal{H}^{2m}(U;\mathbb{Z}/n\mathbb{Z})_c \cong \mathbb{Z}/n\mathbb{Z}$$

after one chooses a primitive 4^{th} root of unity.

Remark. For now, we'll treat this as a black box, but for a nonsingular variety X of dimension d over an algebraically closed field k, and for $\Lambda = \mathbb{Z}/n\mathbb{Z}$, where n is coprime to the characteristic of k, where $\Lambda(m) = \mu_n^{\otimes m}$, there is a unique isomorphism

$$\eta(X) : \mathcal{H}^{2d}(X;\Lambda(d))_c \to \Lambda$$

which sends $cl(P)$ to 1 for any closed point P on X, called the *trace map*.

In particular, Poincaré duality gives us a non-degenerate pairing

$$\mathcal{H}^r(X;\mathbb{Q}_\ell) \times \mathcal{H}^{2d-r}(X;\mathbb{Q}_\ell) \to \mathcal{H}^{2d}(X;\mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$$

In general, we denote the canonical generator of $\mathcal{H}^{2d}(X;-)$ by e^{2d}, and treat the following items as black boxes to be opened in a future module:

1. π_* is uniquely determined by

$$\eta_X(\pi_*(y) \smile x) = \eta_Y(y \smile \pi^*(x))$$

for $x \in \mathcal{H}^{2n-r}(X;\Lambda(n))_c, y \in \mathcal{H}^r(Y;\Lambda)$

2. If $\pi : Y \hookrightarrow Z$ is a closed immersion, then π_* is the Gysin map where

$$\pi_*(1_Y) = cl_X(Y)$$

where 1_Y is the identity element of $\mathcal{H}^0(Y;\Lambda) = \Lambda$.

3. $(\pi_1 \circ \pi_2)_* = \pi_{1*} \circ \pi_{2*}$

4. If X, Y are complete, then for $x \in \mathcal{H}^r(X;-)$ and $y \in \mathcal{H}^s(X;-)$

$$\pi_*(y \smile \pi^*(x)) = \pi_*(y) \smile x$$

Thus, for any regular map $\varphi : X \to Y$ and any $y \in \mathcal{H}^r(Y;)$, we find that

$$\begin{aligned} p_*(cl_{X\times Y}(\Gamma_\varphi) \smile q^*(y)) &\overset{(2)}{=} p_*((1,\varphi)_*(1) \smile q^*(y)) \\ &\overset{(4)}{=} p_*(1,\varphi)_*(1 \smile (1,\varphi)^* q^* y) \\ &\overset{(3)}{=} (p \circ (1,\varphi))_*(1 \smile (q \circ (1,\varphi))^* y) \\ &= \mathbf{1}_*(1_X \smile \varphi^* y) \\ &= \varphi^*(y) \end{aligned}$$

3.5 Trace Formulae

Notation. From here on out, we fix the following notation. For any nonsingular variety X, and regular map $\varphi : X \to X$, Γ_φ denotes the graph of φ and Δ denotes the diagonal of X.

Theorem 17. *(***Lefschetz Fixed Point Formula***) For any complete nonsingular variety X over an algebraically closed field k, with regular map $\varphi : X \to X$, then*

$$(\Gamma_\varphi \cdot \Delta) = \sum (-1)^r \, Tr(\varphi | \mathcal{H}^r(X; \mathbb{Q}_\ell))$$

Proof. Suppose $\{e_i^r\}$ is a basis for $\mathcal{H}^r(X; \mathbb{Q}_\ell)$ and that $\{f_i^{2n-r}\}$ is the dual basis for $\mathcal{H}^{2n-r}(X; \mathbb{Q}_\ell)$. Then with cl as above and Lemma 15, we have

$$cl(\Gamma_\varphi) = \sum_{r,i} \varphi^*(e_i^r) \otimes f_i^{2n-r}$$

and then, for the diagonal Δ,

$$\begin{aligned} cl(\Delta) &= \sum_{r,i} e_i^r \otimes f_i^{2n-r} \\ &= \sum_{r,i} (-1)^{r(2n-r)} f_i^{2n-r} \otimes e_i^r \end{aligned}$$

as a consequence of $\otimes$ inheriting the $\mathbb{Z}_2-$graded algebra structure[6] of the $\smile$ operation,i.e. for homogeneous elements

$$e_i^r \otimes f_i^{2n-r} = (-1)^{r(2n-r)} f_i^{2n-r} \otimes e_i^r$$

and since $(-1)^{r(2n-r)} = (-1)^{2nr-r^2} = (-1)^r$, we find that

$$\sum_{r,i} (-1)^{r(2n-r)} f_i^{2n-r} \otimes e_i^r \quad = \quad \sum_{r,i} (-1)^r f_i^{2n-r} \otimes e_i^r$$

[6]In fact, we ought to recognize the familiar exterior product, $\wedge : \mathcal{H}^*(M; -) \times \mathcal{H}^*(M; -) \to \mathcal{H}^*(M; -)$.

Then, when we take the product of $cl(\Gamma_\varphi)$ and $cl(\Delta)$, by Poincaré duality, we find

$$cl_{X\times X}(\Gamma_\varphi \cdot \Delta) = \sum_{r,i} (-1)^r \varphi^*(e_i^r) f_i^{2n-r} \otimes e^{2n}$$

But $\sum_i \varphi^*(e_i^r) f_i^{2n-r} = \sum_i (\sum_j a_{ji} e_j^r) \cdot f_i^{2n-r} = \sum_i a_{ii} e^{2n} = \mathrm{Tr}(\varphi^* | \mathcal{H}^r(-;-)) e^{2n}$, since $e_i^r \cdot f_j^{2n-r} = \delta_{ij} e^{2n}$, and so

$$cl_{X\times X}(\Gamma_\varphi \cdot \Delta) = \sum_r (-1)^r \mathrm{Tr}(\varphi^* | \mathcal{H}^r(X; \mathbb{Q}_\ell))(e^{2n} \otimes e^{2n})$$

When we apply $\eta_{X\times X}$ from (1), to this expression, we get the trace function. □

Finally, we admit the following useful proposition as a criterion for identifying when $(\Gamma_F \cdot \Delta)_P = 1$ for a fixed point P.

Proposition 18. *Let X be a nonsingular variety, and let Y and Z be closed subvarieties of X. Suppose that P is an irreducible component of $Y \cap Z$. Then $(Y \cdot Z)_P = 1$ if*

1. *Y and Z are non-singular at P;*
2. *$Tgt_P(Y) \cap Tgt_P(Z) = 0$;*
3. *$\dim Y + \dim Z = \dim X$.*

3.6 Some Brief Remarks On Lefschetz Pencils

Deligne's proof of the Riemann hypothesis crucially rests on a geometric reduction argument and the cohomological properties of Lefschetz pencils. This section exists to summarize some of what these results that are required. First, we begin with the following definitions:

Definition 3.5. Let X_0 be an even dimensional projective variety over $\mathbb{F}_q$ and let X be its extension over $\mathbb{F}$. For an embedding $X \hookrightarrow \mathbb{P}^n$, we take a linear subspace $A \subset \mathbb{P}^n$ of codimension 2, and denote by D the space parametrizing the hyperplanes $H \supset A$. Crucially, $D \cong \mathbb{P}^1$. We define an algebraic variety

$$X^* := \{(x, H) \in X \times D \mid x \in H\}$$

equipped with the natural maps. We call one of these maps, $\pi : X^* \to D$, a **Lefschetz pencil**.[7]

In proving the Riemann hypothesis we will be studying the cohomology of X^* using these pencils π. Specifically, we will study the *higher direct images* of the pencils by means of their *Leray spectral sequence*,

$$E_2^{r,d} := \mathcal{H}^r(D; \mathcal{R}^d\pi_*\mathbb{Q}_\ell)$$

Moreover, since $D \cong \mathbb{P}^1$, this amounts to studying

$$E_2^{r,d} = \mathcal{H}^r(\mathbb{P}^1; \mathcal{R}^d\pi_*\mathbb{Q}_\ell)$$

Towards the end of describing the proof of the Riemann hypothesis, we admit the following claims:

Claim 19. *$\mathcal{R}^{n-2}\pi_*\mathbb{Q}_\ell$ is a constant sheaf on $\mathbb{P}^1$.*

Proof. Admitted as a black box. □

Claim 20. *$(\mathcal{R}^{n-2}\pi_*\mathbb{Q}_\ell)_u = \mathcal{H}^{n-2}(X_u; \mathbb{Q}_\ell)$.*

Proof. Admitted as a black box. □

In order to describe the cohomology of a Lefschetz pencil, we will need a means of describing monodromy at a critical point, whence the following formula:

[7] This name is inspired by the correspondence of fibres $\pi^{-1}(t)$ over $t \in \mathbb{P}^1$ with hyperplane sections $H_t \cap X$, for $H_t \subset \mathbb{P}^n$.

Theorem 21. (Picard-Lefschetz formula) *Let $n = 2m + 1$ be the dimension of the fibre of a pencil π. We denote the canonical epimorphism $I_s \to \mathbb{Z}_\ell(1)$ by t. Then, with*

$$t(\sigma)(x \smile \delta_s)\delta_s \in V(1 + (m - n) + m) = V,$$

we find that

$$\sigma_s \in I_s$$

acts on V by

$$\sigma_s(x) = x \pm t(\sigma_s)(x \smile \delta_s)\delta$$

with the signing depending on n mod 4.

V the sheaf $(\mathcal{R}^n\pi_*\mathbb{Q}_\ell)$. We have a filtration,

$$V \supset E \supset E \cap E^\perp \supset 0 \qquad (\dagger)$$

whose existence follows from the comments made in Chapter 3, section 5.

Remark. The existence of this filtration requires a greater discursion into *Lefschetz pencils* and the *cohomology of Lefschetz Pencils* than this paper allows. However, the following dictionary will be vital for understanding this filtration:

- $\pi : X^* \to \mathbb{P}^1$ is the map arising from a Lefschetz pencil;
- Let $S \subset \mathbb{P}^1$ denote the subset of the projective line such that X_s is singular;
- Set $U = S^c = \mathbb{P}^1 \backslash S$;
- Set $\pi_1(U) = \pi_1^{tame}(U, \overline{\eta})$;
- Set I_s to be the tame fundamental group at s;
- For now, we treat the following claim as a black box:

  Claim 22. *Where n is the dimension of the fibres of π, for $r \neq n, n + 1$, the sheaves $\mathcal{R}^r\pi_*\mathbb{Q}_\ell$ are locally constant.*

- Drawing from another black box, by the *proper base change theorem*, $\mathcal{R}^n\pi_*\mathbb{Q}_\ell U$ is a locally constant, and so $V_{\bar{\eta}}$ becomes $\pi_1(U, \bar{\eta})$;

- Let $E \subset V$ denote the *space of vanishing cycles*. In particular, Milne treats as a black box this claim:

  Claim 23. *For each $s \in S$, there exists $\delta_s \in V(m) := V \otimes \mathbb{Q}_\ell(m)$, where $m = \dfrac{\dim \textit{fibre} - 1}{2}$.*

  From this claim, we generate $E(M)$ as the subspace of $V(m)$ generated by δ_s;

- $E^\perp$ is the orthogonal complement of E in $\mathcal{H}^n(X_\eta; \mathbb{Q}_\ell)$ under the **pairing map** $\psi : V \times V \to Q_\ell(-n)$. In particular, $E^\perp := \mathcal{H}^n(X_\eta; \mathbb{Q}_\ell)^{\pi_1}$.[8]

The underlying rationale of the geometric reduction in Deligne's proof stems from the technique of studying the hyperplane sections of a projective variety in order to study the cohomology of the variety. In particular, this m

Theorem 24. (Weak Lefschetz- étale) *Suppose X is a non-singular projective variety, and Y is a smooth hyperplane section of X. Then for all $r \geq 2$, there are maps*

$$\mathcal{H}^{r-2}(Y; \mathbb{Q}_\ell) \to \mathcal{H}^r(X; \mathbb{Q}_\ell)$$

which are compatible with the action of the geometric Frobenius on X extended to $\mathcal{H}(X; \mathbb{Q}_\ell)$ so that

1. *For $r = d + 1$, $\mathcal{H}^{d-1}(Y; \mathbb{Q}_\ell) \to \mathcal{H}^{d+1}(X; \mathbb{Q}_\ell)$ is surjective.*
2. *For $r > d + 1$, $\mathcal{H}^{r-2}(Y; \mathbb{Q}_\ell) \to \mathcal{H}^r(X; \mathbb{Q}_\ell)$ is an isomorphism.*

Finally, we will need the following result from Kazhdan and Margulis:

Theorem 25. *For odd n, $\pi : X^* \to \mathbb{P}^1$ a pencil, η a generic geometric point, and $S \subset \mathbb{P}^1$ such that X_S is singular. Then the image $\pi_1(\mathbb{P}^1 \backslash S, \bar{\eta})$ in $Sp(E/E \cap E^\perp, \psi)$ is open.*[9]

[8] This is proved in [14], Proposition 32.2.

[9] We denote by $Sp(E, \psi)$ is the symplectic group of ψ, i.e. the group of $\lambda \in GL(E)$ such that $\psi(\lambda e, \lambda e') = \psi(e, e')$ for all $e, e' \in E$. We can easily extend this notion to the quotient $E/(E \cap E^\perp)$.

Part II

The Proof of the Weil Conjectures

Chapter 4

The Statement of The Weil Conjectures

The first thing to note about the Weil conjectures is that they're statements made regarding a rational function with some desirable properties that take non-singular projective varieties over the algebraic closure of finite fields as an argument. Under the paradigm established in part I, we can interpret this function as terms of type $\mathbb{Q}$ with free variables of type $\mathbb{F}$ in some category containing fields as objects. However, from a more practical perspective, the first abstraction that needs to be understood is what these functions, of the form

$$\zeta(X_0, t) := \exp\left(\sum_{m=1}^{\infty} N_m(X_0)\frac{t^m}{m}\right) \tag{4.0.1}$$

are describing in the classical sense.

Concretely understood, these functions are tracking the number of homomorphisms $\mathrm{Spec}\mathbb{F}_{p^m} \to X$, where p is a fixed prime and m ranges over $\mathbb{Z}^+$, X is the extension of a variety X_0 over the algebraic closure of $\mathbb{F}_q$, and $N_m(X_0)$ is the number of rational points of X_0 over the extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ of degree m. This is vital when one delves into the topos interpretation of these conjectures, as one begins to track what is meant by a *point* or an *element* (that is, any map from the terminal

object in a category of sheaves on sites). It goes without saying that some of the first insights that can considered are drawn from facts about the formal power series ring, $\mathbb{Q}[[t]]$. The conjectures are as follows:

Conjecture 26. (The Weil Conjectures) *We begin by fixing our notational conventions. First, fix prime $p \in \mathbb{Z}$, and then for any $q = p^a$, with $a \in \mathbb{Z}^+$, for convenience we denote the the algebraic closure of $\mathbb{F}_q$ by $\mathbb{F}$. Next, for a non-singular, absolutely irreducible variety X_0 over $\mathbb{F}_q$, we let X denote X_0 as a variety of dimension d over $\mathbb{F}_q$, such that X is connected. Then, we let ℓ be any prime not equal to p. Notably, all of this information can be captured by the following triple (p, a, X_0). Finally, the specific conjectures are as follows:*

(Generating Function)

Proposition 27. *Given a triple (p, a, X_0), we set $q := p^a$. Then the number of rational points on X_0 over the extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ with degree m is given by*

$$N_m(X_0) = \sum_r (-1)^r \, Tr(F^m | \mathcal{H}^r(X; \mathbb{Q}_\ell)) \tag{4.0.2}$$

where F is the Frobenius map. The sequence $(N_1(X_0), N_2(X_0), N_3(X_0), \ldots)$ has as its corresponding generating function, the zeta function $\zeta(X_0, t)$ from Equation 4.0.1 satisfying:

$$\sum_{n \geq 1} N_m(X_0) t^{m-1} = \frac{d}{dt} \log \zeta(X_0, t) \tag{4.0.3}$$

Remark. Traditionally, there are four Weil conjectures, and this is not one of them. However, in the light of this proposition, the other conjectures are possible.

(Betti Numbers) *First, some additional notation.*

Notation. With the triple (p, a, X_0), we set $d = \dim X_0$ and let $r \in \lceil 2d \rceil$. With $m \in \mathbb{N}$, we denote the characteristic polynomial of the associated Frobenius F^m with respect to $\mathcal{H}^r(X; \mathbb{Q}_\ell)$ by

$$P_{r,m} = \det(\mathrm{id} - F^m t | \mathcal{H}^r(X; \mathbb{Q}_\ell)) \tag{4.0.4}$$

Furthermore, we note that each $P_{r,1}(t)$ is polynomial of the form

$$P_{r,1}(t) = \prod_{i=1}^{\beta_r}(1 - \lambda_{r,i}t) \in \mathbb{Q}_\ell[t] \tag{4.0.5}$$

for $r \in \lceil 2d \rceil$, with $\lambda_{r,i}$ the reciprocal of roots of $P_{r,1}$.

Theorem 28. (Betti Numbers) *Set $\beta_r = \deg P_{r,1}(t)$. Then the Euler-characteristic of X_0 is $\chi = \sum(-1)^r\beta_r$. Furthermore, with X the extension of X_0 to $\mathbb{F}$, if X lifts to a variety Y in characteristic zero, then with Y defined over a number field embedded in $\mathbb{C}$ (i.e., as a variety over the complex numbers), each β_r is the r^{th} Betti number of Y.*

(Rationality)

Theorem 29. *For each triple (p, a, X_0), and with characteristic polynomials and Betti numbers as in Theorem 28, each $P_{r,1}(t)$ can be written as the product of polynomials of the form*

$$P_{r,1}(t) = \prod_{i=1}^{\beta_r}(1 - \lambda_{r,i}t) \in \mathbb{Q}_\ell[t] \tag{4.0.6}$$

for $r \in \lceil 2d \rceil$, so that Equation 4.0.1 can be expressed as the follows:

$$\zeta(X_0, t) = \prod_{i=0}^{2d}(P_i(X_0, t))^{(-1)^{i+1}} \tag{4.0.7}$$

Remark. This was actually the first of the conjectures to be proven. The original proof, from Dwork [6] makes use of p-adic analysis, and is worth studying in its own right. However, it was inadequate for proving the rest of the conjectures (in particular, the Riemann hypothesis). The proof explored in this paper is from Grothendieck, and makes use of $\ell-$adic cohomology theory.

(Functional Equation: Poincaré Duality)

Theorem 30. *For any triple (p, a, X_0), with β_r and χ as in Theorem 28, $\zeta(X_0, t)$ satisfies*

$$\zeta(X_0, 1/q^d t) = \pm q^{d\chi/2} t^\chi \zeta(X_0, t)$$

with $\chi = \sum(-1)^r \beta_r = (\Delta \cdot \Delta)$.

(Riemann Hypothesis)

Theorem 31. *For each* $P_{r,1}(t)$*, the eigenvalues are algebraic integers such* $|\lambda_{r,i}| = q^{r/2}$*. Furthermore, the poles of* $\zeta(X_0, z)$ *are on the lines* $\Re(z) = 0, 1, 2, \ldots \dim X$ *and the zeroes are on the lines* $\Re(z) = \frac{1}{2}, \frac{3}{2}, \ldots, \frac{\dim X - 1}{2}$.

Remark. This was the last of the conjectures to be proven. Deligne first proved this conjecture in 1974 using Lefschetz pencils and an estimate argument. He proved a general form bounding the weights of the pushforward of a sheaf. For spatial considerations, we will only provide a broad overview of his first argument.

Remark. As mentioned in Chapter 3, each of these conjectures follow formally from the existence of a suitable cohomology theory on algebraic variety, called a *Weil cohomology theory*. Moreover, the first three conjectures follow more or less immediately given any such theory.[1] Although throughout this project we will work exclusively with *étale cohomology* theories, and will admit various properties about these cohomology functors so as to focus on the main thrust of the proof, it is worth stressing these are cohomologies which crucially satisfy conditions for the Lefschetz fixed point theorem. The proof of the final conjecture, the *Riemann hypothesis*, can best be understood as an limit argument that goes about bounding the eigenvalues of the Frobenius acting on $\mathcal{H}^r(-; \mathbb{Q}_\ell)$ for $r = 0, 1, 2$, and appropriate, non-singular projective varieties X_0.

[1] Well, I shouldn't say immediately, but relative to the proof of the Riemann hypothesis, they appear with little effort.

Chapter 5

The Proof of the Weil Conjectures

The proof presented can be made to apply to any *Weil cohomology theories*, although the results are stated in terms of any ℓ-adic cohomology such that $\ell \neq p$. Assuming that X is a nonsingular, proper scheme of finite type over an algebraically closed field k of characteristic $p > 0$, the properties we will make use of are as follows:

- If X is a complete non-singular variety over an algebraically closed field k of characteristic $p \neq 0$, X can be *lifted to characteristic 0* if

  1. there is a discrete valuation ring R with a field of fractions K of characteristic 0 and residue field k;

  2. a scheme $\pi : \chi \to S$, with $S = \text{Spec}R$, which is proper and smooth over S whose special fibre is X.

- For any complete nonsingular variety X_0 over an algebraically closed field k of characteristic > 0 that has been lifted to a complete nonsingular variety X_1 in K, characteristic 0, then

$$\mathcal{H}^q(X_0; \Lambda) \cong \mathcal{H}^q(X_{cm}; \Lambda)$$

  for all q, where X_{cm} is the associated complex manifold in the classical topology;

- By the comparison theorem, if X is smooth and proper over $\mathbb{C}$, then

$$\mathcal{H}^q(X;\mathbb{Q}_\ell)\otimes_{\mathbb{Q}_\ell}\mathbb{C}\cong\mathcal{H}^q(X_{cm};\mathbb{Q}_\ell)$$

- For $X=\mathbb{P}^n$, we regard the groups $\mathcal{H}^q(X;\mathbb{Q}_\ell)$ as vector spaces over $\mathbb{Q}_l$. By the cohomology of complex projective space, the $\mathcal{H}^q(X;\mathbb{Q}_\ell)$ are 0, except for $0\leq q\leq 2n$, where $n=\dim X$. In particular, if M is a module and X is a projective n-space over $\mathbb{C}$, then

$$\mathcal{H}^q(\mathbb{P}^n(\mathbb{C});M)=\begin{cases}M & q\in\{0,2,\ldots,2n\}\\ 0 & otherwise.\end{cases}$$

  So in particular,

$$\mathcal{H}^q(\mathbb{P}^n(\mathbb{C});\mathbb{Q}_\ell)=\begin{cases}\mathbb{Q}_\ell & q\in\{0,2,\ldots,2n\}\\ 0 & otherwise.\end{cases}$$

- $\mathcal{H}^i(X;\mathbb{Q}_l)$ is a contravariant functor in X;

- For all q,r, there is a cup-product structure

$$\mathcal{H}^q(X;\mathbb{Q}_\ell)\times\mathcal{H}^r(X;\mathbb{Q}_\ell)\to\mathcal{H}^{q+r}(X;\mathbb{Q}_\ell)$$

- (*Poincaré duality*) $\mathcal{H}^{2n}(X;\mathbb{Q}_\ell)$ is 1-dimensional and the cup-product pairing

$$\mathcal{H}^q(X;\mathbb{Q}_\ell)\times\mathcal{H}^{2n-q}(X;\mathbb{Q}_\ell)\to\mathcal{H}^{2n}(X;\mathbb{Q}_\ell)$$

  is a perfect pairing for each $q\in\{0,1,\ldots,2n\}$;

- (*Lefschetz fixed point theorem*) Let $f:X\to X$ be a morphism with isolated fixed points. For each fixed point $x\in X$ with multiplicity 1, let

$$N(f,X)=\sum(-1)^q\mathrm{Tr}(f^*;\mathcal{H}^q(X;\mathbb{Q}_\ell))$$

  where f^* is the induced map on the cohomology of X;

- If Z is a subvariety of codimension q, then associated to Z is a cohomology class $\eta(Z) \in \mathcal{H}^{2q}(X;\mathbb{Q}_\ell)$. The map η is a homomorphism from the Chow ring $CH(X)$ to the cohomology ring $\mathcal{H}^*(X;\mathbb{Q}_\ell)$. If $\bar{x} \in X$ is a closed point, then $\eta(\bar{x}) \in \mathcal{H}^{2n}(X;\mathbb{Q}_\ell)$ is nonzero.[1]

[1]This is detailed in section 23 in [14]. By linearity, we extend this map to cycles, and notice for future reference that the intersection of cycles becomes the cup-product of cohomology classes.

5.1 Defining $N_m(X_0)$ By Expressing The Number of Rational Points In The Extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ of degree m in X_0.

Proof. **[Prop 27]**This proof proceeds by induction, starting with a proof of the following claim, before applying Theorem 17, to obtain the desired result.

Claim 32. $N_1 = (\Gamma_F \cdot \Delta)$*, i.e. the number of points of* X_0 *with coordinates in* $\mathbb{F}_q$ *is equal to the intersection of the graph of the Frobenius with the diagonal.*

Proof. Letting $\mathbb{F}$ denote the closure of $\mathbb{F}_q$, it is clear that an element $a \in \mathbb{F}$ will lie in $\mathbb{F}_q$ if and only if $a^q = a$. Thus, $X^F = X(\mathbb{F}_q)$ simply by considering the description of the Frobenius in terms of the coordinates of points. Furthermore, for a fixed point P of F, we find $(dF)_P = 0$.[2] As a consequence, we find that 1 is not an eigenvalue of $(dF)_P$.

Now, since Γ_F and Δ are both isomorphic to X_0, we find that conditions (i) and (iii) of Proposition 18 are satisfied, and since $\mathrm{Tgt}_{(P,P)}(\Gamma_F)$ is the graph of $(dF)_P$, and $\mathrm{Tgt}_{(P,P)}(\Delta)$ is the graph of $\mathrm{id}_{\mathrm{Tgt}_P(X)}$, condition (ii) holds (since 1 is not an eigenvalue). Thus by Proposition 18, we have $(\Gamma_F \cdot \Delta)_P = 1$, and as each fixed point occurs with multiplicity 1, we find that $N_1 = (\Gamma_F \cdot \Delta)$. □

Claim 33. $N_1 = \sum_r (-1)^r Tr(F|\mathcal{H}^r(X;\mathbb{Q}_\ell))$

Proof. This follows by application of the *Lefschetz Fixed Point theorem* to the previous claim. □

Claim 34. $X^{F^m} = X(\mathbb{F}_{q^m})$

Proof. The Frobenius map of X relative to $X_{0,\mathbb{F}_{q^m}}$ is simply F^m. □

Thus the general case N_m follows. Hence,

$$N_m(X_0) := \sum_r (-1)^r \mathrm{Tr}(F^m|\mathcal{H}^r(X;\mathbb{Q}_\ell))$$

We now verify the final claim.

[2] To see this, simply consider an affine neighbourhood of P, $U_0 = \mathrm{Specm}\ A_0$, with $A_0 = \mathbb{F}_q[x_1, \ldots, x_n]$, from which $x_i \circ F = x_i^q$. Thus $(dx_i)_P \circ (dF)_P = (dx_i^q)_P = q x_i^{q-1} (dx_i)_P = 0$.

Claim 35. *With* $\zeta(X_0,t) = \exp\left(\sum_{m=1}^{\infty} N_m(X_0)\frac{t^m}{m}\right)$,

$$\sum_{m\geq 1} N_m(X_0)t^{m-1} = \frac{d}{dt}\log\zeta(X_0,t)$$

Proof. Immediately, we find $\log\zeta(X_0,t) = \sum_{m=1}^{\infty} N_m(X_0)\frac{t^m}{m}$ and by linearity,

$$\frac{d}{dt}\left(\sum_{m=1}^{\infty} N_m(X_0)\frac{t^m}{m}\right) = \sum_{m=1}^{\infty} N_m(X_0)t^{m-1}$$

□

□

5.2 The Proof of the First Three Conjectures

5.2.1 Betti Numbers

The proof of Theorem 28 is a consequence of the following theorem:

Theorem 36. *Fix k, an algebraically closed field of positive characteristic p, and K, a field of characteristic zero. Now suppose that there is a lift from X_0, a variety over k, to X_1, a variety over K. Then for any finite abelian group Λ, the following cohomology groups are isomorphic:*

$$\mathcal{H}^r(X_0;\Lambda) \cong \mathcal{H}^r(X_{1,K^{al}};\Lambda)$$

We admit this theorem for now, remarking only that the isomorphism between étale and singular cohomologies extends from finite $\Lambda \cong \mathbb{Z}/\ell^n\mathbb{Z}$ to $\mathbb{Q}_\ell$ by passing to the limit of $\mathbb{Z}/\ell^n\mathbb{Z}$ and then tensoring with $\mathbb{Q}_\ell$.

Proof. **(Theorem 28)**Recall that any complete non-singular variety X over an algebraically closed field k of characteristic $p \neq 0$ can be *lifted to characteristic zero* if:

1. k is the residue field of some discrete valuation ring R with a field of fractions K of characteristic zero;

2. X is a special fibre for a proper and smooth scheme $\pi : \rho \to \mathrm{Spec}R$.

We want to show given a lift from a variety X_0 over an algebraically closed field k of positive characteristic p to a variety Y over a field of characteristic 0, that the Betti numbers of X_0 are precisely the Betti numbers of Y. To that end, first suppose there is a lift with $\Lambda = \mathbb{Z}/\ell^n\mathbb{Z}$, R an appropriate[3] discrete valuation ring, and ρ a non-singular, projective scheme over $\mathrm{Spec}R$. Since we can regard $\mathbb{Q}_\ell$ in terms of locally constant sheaves, by the Theorem 4.

$$\mathcal{H}^r(X;\mathbb{Q}_\ell) \cong \mathcal{H}^r(\rho \times_{\mathrm{Spec}R} \mathrm{Spec}\mathbb{C};\mathbb{Q}_\ell)$$

[3]This means that there is some maximal $\mathfrak{p} \subset R$ such that $R/\mathfrak{p} \cong \mathbb{F}_q$.

Furthermore, in applying Theorem 36, we find:

$$\mathcal{H}^r(\rho \times_{\mathrm{Spec}R} \mathrm{Spec}\mathbb{C}; \mathbb{Z}/\ell^n\mathbb{Z}) \cong \mathcal{H}^r((\rho \times_{\mathrm{Spec}R} \mathrm{Spec}\mathbb{C})^{an}; \mathbb{Z}/\ell^n\mathbb{Z})$$

after which we extend[4] this result to find

$$\mathcal{H}^r(\rho \times_{\mathrm{Spec}R} \mathrm{Spec}\mathbb{C}; \mathbb{Q}_\ell) \cong \mathcal{H}^r((\rho \times_{\mathrm{Spec}R} \mathrm{Spec}\mathbb{C})^{an}; \mathbb{Q}_\ell)$$

thus yielding a comparison result of the ℓ-adic cohomology of X with the singular cohomology of the lifting to $\mathbb{C}$. Hence, with $Y = (\rho \times_{\mathrm{Spec}R} \mathrm{Spec}\mathbb{C})^{an}$, we find that the r^{th} Betti number of Y is precisely $\deg P_{r,1}(t)$, as desired. □

5.2.2 Rationality

Before beginning this proof, we admit the following Lemma from Bourbaki, Algèbre, IV.5.

Lemma 37. *Let $k \subset K$ be fields, and let $f(t) \in k[[t]]$. If $f(t) \in K(t)$, then $f(t) \in k(t)$.*

Proof. **(Theorem 29)** We first prove that $\zeta(X_0, t) = \prod_{i=0}^{2d} P_i(t)^{(-1)^{i+1}}$, before proving rationality.[5]

Claim 38. $\zeta(X_0, t) = \exp(\sum_{m\geq 1}(\sum_{i=0}^{2d}(-1)^i Tr(F^m|\mathcal{H}^i(X_0; \mathbb{Q}_\ell)))\frac{t^m}{m})$.

Proof.

$$\begin{aligned}\zeta(X_0, t) &\overset{def}{=} \exp\left(\sum_{m\geq 1} N_m(X_0)\frac{t^m}{m}\right)\\ &\overset{Prop(27)}{=} \exp\left(\sum_{m\geq 1}(\sum_{i=0}^{2d}(-1)^i \mathrm{Tr}(F^m|\mathcal{H}^r(X_0; \mathbb{Q}_\ell)))\frac{t^m}{m}\right)\end{aligned}$$

□

Claim 39. $\zeta(X_0, t) = \prod_{i=0}^{2d}\left(\exp(\sum_{m=1}^{\infty} Tr(F^m|\mathcal{H}^r(X; \mathbb{Q}_\ell))\frac{t^m}{m})\right)^{(-1)^i}$.

[4] Recall, that $\mathcal{H}^r(X; \mathbb{Z}_\ell) := \varinjlim_n \mathcal{H}^r(X; \mathbb{Z}/\ell^n\mathbb{Z})$, and $\mathcal{H}^r(X; \mathbb{Q}_\ell) := \mathcal{H}^r(X; \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

[5] By construction $P_{r,m} \in \mathbb{Q}_\ell[t]$.

Proof. Since we have just proven that $\zeta(X_0,t) = \exp(\sum_m (\sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(F^m | \mathcal{H}^r(X_0;))) \frac{t^m}{m})$,this follows by moving the inner sum of $\exp(\sum_m (\sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(F^m | \mathcal{H}^r(X_0;))) \frac{t^m}{m})$ outside. □

Finally,

Claim 40. *If $p_\varphi = \prod(1 - c_i t)$ is the characteristic polynomial of an endomorphism φ of a vector space V over k, then $Tr(\varphi^m | V) = \sum c_i^m$*

Proof. This is standard linear algebra. We may assume there exists a basis $\mathcal{B}$ relative to which the representation of φ is an upper triangular matrix with the c_i in the diagonal (possibly by extending k if necessary). Then, relative to this basis $\mathcal{B}$, φ^m has c_i^m along the diagonal, whence the result. □

Now, setting $P_r(t) := P_{r,1}(t) = \prod(1 - \lambda_i t)$, we use the formal series expansion of log, finding:

$$\log((P_r(t))^{-1}) = -\sum_i \log(1 - \lambda_i t) = \sum_i \sum_{m=1}^{\infty} \lambda_i^m \frac{t^m}{m} = \sum_{m=1}^{\infty} \sum_i \lambda_i^m \frac{t^m}{m} = \sum_{m=1}^{\infty} \mathrm{Tr}(F^m | \mathcal{H}^r(X; \mathbb{Q}_\ell))$$

Thus $\exp(\mathrm{Tr}(F^m | \mathcal{H}^r(X; \mathbb{Q}_\ell))) = \exp(\log(P_r(t))^{-1}) = (P_r(t))^{-1}$, whence we can conclude:

$$\zeta(X_0,t) = \prod_{i=0}^{2d} \left(\exp(\log(P_i(t))^{-1})\right)^{(-1)^i} = \prod_{i=0}^{2d} (P_i(X_0,t))^{(-1)^{i+1}}$$

Claim 41. *$\zeta(X_0,t)$ is rational.*

Proof. We have shown that $\zeta(X_0,t)$ is a rational function with coefficients in $\mathbb{Q}_\ell$. By Lemma 37, we find that it is a rational function with coefficients in $\mathbb{Q}$. Hence, it is rational. □

□

5.2.3 Poincaré Duality (The Functional Equation)

Before beginning our proof, we admit the two following propositions:

Proposition 42. *Let $\pi : X \to Y$ be a proper map of smooth separated varieties of the same dimension d over algebraically closed field k, with push-forward $\pi_* : \mathcal{H}^r(X; \mathbb{Q}_\ell) \to \mathcal{H}^r(Y; \mathbb{Q}_\ell)$ and*

pullback $\pi^* : \mathcal{H}^r(Y;\mathbb{Q}_\ell) \to \mathcal{H}^r(X;\mathbb{Q}_\ell)$*, for arbitrary* $r \in \lceil 2d \rceil$*. If* $\pi : X \to Y$ *is a finite map of degree* δ*, then* $\pi_* \circ \pi^* = \delta$*, i.e. multiplication by* δ *in the cohomology group* $\mathcal{H}^r(Y;\mathbb{Q}_\ell)$*.*

Proposition 43. *Let* $\pi : X \to X$ *be a proper map of smooth separated varieties over an algebraically closed field* k*. If* $\pi : X \to X$ *is a finite map of degree* δ*, then:*

1. π^* *acts as the identity on* $\mathcal{H}^0(X;-)$*;*
2. π_* *acts as multiplication by* δ *on* $\mathcal{H}^0(X;-)$*.*

With these two propositions, we are armed to prove Theorem 30.

Proof. **(Theorem 30)** Given X with $\dim X = d$, first, we note that for the Frobenius F, F^* and F_* take $\mathcal{H}^r(X;\mathbb{Q}_\ell)$ to $\mathcal{H}^r(X;\mathbb{Q}_\ell)$. We first make the following mild claim:

Claim 44. F *is finite morphism with degree* q^d*.*

Proof. First, for clarity, in the affine case of $\mathbb{A}^n$, F is defined as the homomorphism of $\mathbb{F}$-algebras given by $T_i \mapsto T_i^q$. Clearly, $\mathbb{F}[T_1,\ldots,T_n]$ is free of rank q^n over the image of F, i.e. $\mathbb{F}[T_1^q,\ldots,T_n^q]$.

In the general case, we choose a transcendence basis $T_1,\ldots,T_d$ for the function field $\mathbb{F}_q(X_0)$ of X_0. We extend F to the homomorphism $f : \mathbb{F}(X) \to \mathbb{F}(X)$. Thus

$$f\mathbb{F}(X) \cap \mathbb{F}(T_1,\ldots,T_d) = f\mathbb{F}(T_1,\cdots,T_d)$$

whence

$$\mathbb{F}(X) = f\mathbb{F}(X) \cdot \mathbb{F}(T_1,\ldots,T_d)$$

Thus

$$[\mathbb{F}(X) : f\mathbb{F}(X)] = [\mathbb{F}(T_1,\ldots,T_d) : f\mathbb{F}(T_1,\ldots,T_d)] = q^d$$

□

Next, we first admit[6] the following pairing:

$$\phi : \mathcal{H}^{2d-r}(X;\mathbb{Q}_\ell) \times \mathcal{H}^r(X;\mathbb{Q}_\ell(d)) \to \mathcal{H}^{2d}(X;\mathbb{Q}_\ell) \xrightarrow{\eta_X} \mathbb{Q}_\ell$$

[6]In particular, this would just be an application of Poincaré duality

which we simplify to

$$\varphi : \mathcal{H}^{2d-r}(X;\mathbb{Q}_\ell) \times \mathcal{H}^r(X;\mathbb{Q}_\ell(d)) \to \mathbb{Q}_\ell$$

where $\mathbb{Q}_\ell(d)$ is the d^{th} Tate twist of $\mathbb{Q}_\ell$.

Claim 45. *For any $x \in \mathcal{H}^{2d-r}(X;\mathbb{Q}_\ell)$ and any $y \in \mathcal{H}^r(X;\mathbb{Q}_\ell)$,*

$$\eta_X(F_*(x) \smile y) = \eta_X(x \smile F^*(y))$$

Proof. This follows from the definition of the pullback of F. □

Claim 46. *The eigenvalues of $F^*|\mathcal{H}^r(X;\mathbb{Q}_\ell)$ and $F_*|\mathcal{H}^{2d-r}(X;\mathbb{Q}_\ell)$ agree.*

Proof. This follows from the previous claim. □

Now we make the following claims that we will use to describe $P_i(1/q^d t)$:

Claim 47. $\det(F^* \mid \mathcal{H}^{2d-r}(X;\mathbb{Q}_\ell)) = \dfrac{q^{d\beta_r}}{\det(F^* \mid \mathcal{H}^r(X;\mathbb{Q}_\ell))}$.

Proof. We apply Lemma 13, noting that β_r describes the dimension of the domain of the perfect pairing. □

More explicitly,

Claim 48. $P_{2d-r}(t) = \dfrac{(-1)^{\beta_r} q^{d\beta_r} t^{\beta_r}}{\det(F^* \mid \mathcal{H}^r(X;\mathbb{Q}_\ell))} P_r(1/q^d t)$.

Proof. We apply Lemma 13. □

Finally, with the relationship between eigenvalues of our F^* established, and our results from

Theorems 28 and 29, we find

$$\begin{aligned}
\zeta(X_0, 1/q^d t) &\overset{Thm29}{=} \prod_{r=0}^{2d} (P_{r,1}(1/q^d t))^{(-1)^{r+1}} \\
&\overset{47,48}{=} \prod_{r=0}^{2d} P_{2d-r,1}(t)^{(-1)^{r+1}} \cdot \frac{(-1)^\chi q^{d\chi} t^\chi}{\prod_{r=0}^{2d} \det(F^* \mid \mathcal{H}^r(X; \mathbb{Q}_\ell))^{(-1)^r}} \\
&= \pm \frac{q^{d\chi} t^\chi}{q^{d\chi/2}} \zeta(X_0, t) \\
&= \pm q^{d\chi/2} t^\chi \zeta(X_0, t)
\end{aligned}$$

as desired. □

5.3 The Structure of the Proof of the Riemann Hypothesis

I suppose it is appropriate at this point to mention that Deligne's first proof of the Riemann hypothesis in [5] was the basis for his Fields medal.[7] Whereas the spark of this thesis is closer to the spirit of Grothendieck's approach to the Weil conjectures, which can be thought of as abstracting the problem to the point where solving it becomes tractable, Deligne's proof strikes one as considerably more tangible, and closer to the spirit of the classical geometers. Very broadly put, his proof consists of a very elegant (and highly nested) limiting argument. As mentioned earlier, the proof of the Weil conjectures is like a matryoshka doll. Nowhere is this observation more apparent than with the proof of the Riemann hypothesis. With the long term goal of realizing these proofs within the framework of Intuitionistic Type Theory, one can be readily interpret this proof as an elegant nesting of inductive results on constant sheaves.

Further, I must mention that while many of the components to the following proof have been raised throughout this paper, there remain too many black boxes for me to suggest I will have provided anything resembling a completely satisfactory exposition of Deligne's actual proof. Instead, I have provided a reasonably comprehensive,[8] albeit high-level, summary of the proof of the Riemann hypothesis, starting with the geometric reductions demonstrating that it suffices to prove an approximate result for an equivalent statement of Theorem 31 with respect to the middle cohomology groups of even dimension, and the mechanics by which one proves these remaining results. The structure of the argument precedes as follows:

First, following Deligne in [5], one shows that it suffices to prove Theorem 31 in an *equivalent* case, namely

Theorem 49. *Let X_0 be a nonsingular projective variety over $\mathbb{F}_q$. Then the eigenvalues of F on $\mathcal{H}^r(X;\mathbb{Q}_\ell)$ are algebraic numbers whose conjugates all have modulus $q^{r/2}$.*

That we can do this should strike the reader as fairly apparent, since what is under investigation in Theorem 31 are the $P_{r,1}$ polynomials. After which we further reduce to the case of $\mathbb{F}_{q^m}$ for $m \in \mathbb{N}$. This follows because the Frobenius $F : X \to X$ is defined relative to the field $\mathbb{F}_q$, the Frobenius

[7] If for no other reason than to emphasize that his proof demonstrates some breathtaking mathematical artistry, even when it points outwards to various results found scattered through SGAs 4, 4.5, 5, and 7.

[8] Modulo the material already present in this paper.

$F_m : X \to X$ relative to $\mathbb{F}_{q^m}$ is simply F^m, from which given an eigenvalue λ of F on $\mathcal{H}^r(X;\mathbb{Q}_\ell)$, we have λ^m as an eigenvalue of F_m on $\mathcal{H}^r(X;\mathbb{Q}_\ell)$. We then further our reduction by proving the following proposition:

Proposition 50. *Assume that for all nonsingular projective varieties X_0 of even dimension n over $\mathbb{F}_q$, every eigenvalue $\lambda$of F on $\mathcal{H}^n(X;\mathbb{Q}_\ell)$ is an algebraic number such that*

$$q^{(n-1)/2} < |\lambda_c| < q^{(n+1)/2)}$$

for all complex conjugates of λ. Then Theorem 49 holds for all nonsingular projective varieties.

Remark. This result follows from the Künneth formula, since for any eigenvalue λ of F on $\mathcal{H}^n(X;\mathbb{Q}_\ell)$, λ^m will be an eigenvalue of F on $\mathcal{H}^{nm}(X^m;\mathbb{Q}_\ell)$. Then, by considering F_m so that the cohomology group is of an even power, we find

$$q^{(mn-1)/} \leq |\lambda|^m \leq q^{(mn+1)/2}$$

After which we can then take the m^{th} root and let m tend to ∞ over $2\mathbb{Z}$, finding that $|\lambda| = q^{n/2}$.

At this point, we then begin an induction argument on the dimension of X_0. In the base case that $\dim X_0 = 0$, the result is obvious. Assuming the result holds up to arbitrary n, we then apply Poincaré duality to eigenvalues λ of F on $\mathcal{H}^r(X;\mathbb{Q}_\ell)$ to find that q^n/λ is an eigenvalue of F on $\mathcal{H}^{2n-r}(X;\mathbb{Q}_\ell)$.

It will then obvious that to finish the proof, it suffices to assume $r > n$. This will require a proof of *Bertini's theorem*, which shows that there is a hyperplane H in $\mathbb{P}^m$ such that $Y := H \cap X$ is a nonsingular variety. One then makes use of the Gysin sequence defined for (X, Y), and because $X \backslash Y$ will be affine, by the weak Lefschetz theorem, $\mathcal{H}^r(X\backslash Y;\mathbb{Q}_\ell) = 0$ for $r > n$. In this way, the Gysin map $i_* : \mathcal{H}^{r-2}(Y;\mathbb{Q}_\ell(-1)) \to \mathcal{H}^r(X;\mathbb{Q}_\ell)$ will be surjective for $r > n$. At this point, one then inducts on the eigenvalues of F on $\mathcal{H}^{r-2}(Y;\mathbb{Q}_\ell)$, finding that they are algebraic numbers whose conjugates have modulus $q^{(r-2)/2}$. Further, since $F \circ i_* = q(i_* \circ F)$, the eigenvalues of F on $\mathcal{H}^r(X;\mathbb{Q}_\ell)$ will be algebraic numbers with conjugates $q^{r/2}$

What will remain then is to show is the following theorem:

Theorem 51. *Let $m \in \mathbb{N}$. For any nonsingular projective variety X_0 of dimension $n = 2(m+1)$ over $\mathbb{F}_q$, the Frobenius acts rationally on $\mathcal{H}^n(X; \mathbb{Q}_\ell)$ such that every eigenvalue λ is an algebraic number satisfying*

$$q^{(n-1)/2} < |\lambda'| < q^{(n+1)/2} \qquad (\star n)$$

for all complex conjugates of λ.

This proof follows from proving the following, crucial lemma:

Lemma 52. *If V satisfies $(\star n)$ and $W \subset V$ is stable under φ, then both W and V/W satisfy $(\star n)$. Furthermore, if there exists a filtration*

$$V \supset V_1 \supset \cdots \supset V_r \supset 0$$

that is stable under φ such that for all i, the associated endomorphism of V_i/V_{i+1} defined by φ satisfies $(\star n)$, then φ satisfies $(\star n)$.

It is prudent to state the following corollary, where φ is the geometric Frobenius, F:

Corollary 53. *Suppose F is the geometric Frobenius, and both $V \subset \mathcal{H}^r(X; \mathbb{Q}_\ell)$ and $W \subset \mathcal{H}^s(Y; \mathbb{Q}_\ell)$ are both stable under F. Further suppose that ϕ is a $\mathbb{Q}_\ell$ linear map such that for any $v \in V$,*

$$\phi(F(v)) = q^{(r-s)/2} F(\phi(v))$$

Then,

1. *If φ is surjective, $(\star)$ holds for V implies $(\star)$ holds for W;*
2. *If φ is injective, $(\star)$ holds for W implies $(\star)$ holds for V.*

After proving this lemma, we are able to assume there is a Lefschetz pencil for X_0 of even dimension, which will be rational over $\mathbb{F}_q$. In order to make this induction proof tractable, one first demonstrates that it is sufficient to prove that $(\star n)$ holds for varieties X^* obtained from X by blowing them up along $A \cap X$, where A is an axis of a Lefschetz pencil π.[9] This makes use of some of

[9]The actual proof is fairly elaborate, with the best, and possibly only source, still being [5]. One can find a high level summary in [14], in the proof of Lemma 33.2, as to what needs to be shown.

the desirable properties of Lefschetz pencils, namely that A crosses X transversally and that $A \cap X$ is a nonsingular subvariety of codimension 2. The actual reason why this reduction is acceptable is that the map $\varphi : X^* \to X$ is a proper map, which allows us to use Theorem 4.

Notably, we establish the existence of a pencil π with only a finite number of singular fibres, each fibre having only one singular point which is an ordinary double point. In analyzing the cohomology of X^*, we account for the variation of these fibres by using the higher direct images of the pencil π, $\mathcal{R}^n\pi_*\mathbb{Q}_\ell$ so that we wind up studying the *Leray spectral sequences of* π,

$$E_2^{r,n} := \mathcal{H}^r(\mathbb{P}^1; \mathcal{R}^n\pi_*\mathbb{Q}_\ell)$$

Thankfully, there is an iterative process[10] showing that if $(\star m)$ holds for the following:

1. $E_2^{0,n} = \mathcal{H}^2(\mathbb{P}^1; \mathcal{R}^{n-2}\pi_*\mathbb{Q}_\ell)$;
2. $E_0^{2,n-2} = \mathcal{H}^0(\mathbb{P}^1; \mathcal{R}^n\pi_*\mathbb{Q}_\ell)$;
3. $E_1^{1,n-1} = \mathcal{H}^1(\mathbb{P}^1; \mathcal{R}^{n-1}\pi_*\mathbb{Q}_\ell)$.

then $(\star n)$ will hold for $\mathcal{H}^n(X^*; \mathbb{Q}_\ell)$ as desired. So we then proceed by proving $(\star n)$ for these three cases as follows:

5.3.1 $\mathcal{H}^2(\mathbb{P}^1; \mathcal{R}^{n-2}\pi_*\mathbb{Q}_\ell)$

The proof proceeds from facts about Lefschetz pencils, namely that $\mathcal{R}^{n-2}\pi_*\mathbb{Q}_\ell$ is constant on $\mathbb{P}^1$ and that $(\mathcal{R}^{n-2}\pi_*\mathbb{Q}_\ell)_u = \mathcal{H}^{n-2}(X_u; \mathbb{Q}_\ell)$. Thus, it suffices to prove $(\star n)$ for $\mathcal{H}^{n-2}(X_u; \mathbb{Q}_\ell)$. We do this by taking these facts, and consider the induced cohomology sequence of

$$0 \to j_!j^*\mathbb{Q}_\ell \to \mathbb{Q}_\ell \to i_*i^*\mathbb{Q}_\ell \to 0$$

where Y_0 is a nonsingular hyperplane section such that $X_0 \backslash Y_0$ is affine. This allows us to apply Poincaré duality and then the weak Lefschetz theorem to identify that

$$\mathcal{H}^{n-2}(X_u \backslash Y; \mathbb{Q}_\ell)_c \cong \mathcal{H}^n(X_u \backslash Y; \mathbb{Q}_\ell)^\vee = 0$$

[10] Also, helpfully summarized in [14], but whose exposition is effectively scattered throughout the SGA.

From this we can conclude that the corresponding map $\mathcal{H}^{n-1}(X_u;\mathbb{Q}_\ell) \to \mathcal{H}^{n-1}(Y;\mathbb{Q}_\ell)$ must be injective.[11] Then induction on even n, with $(\star n)$ holding for Y, $(\star n)$ holds for X by Lemma 13.

5.3.2 $\mathcal{H}^0(\mathbb{P}^1;\mathcal{R}^n\pi_*\mathbb{Q}_\ell)$

The proof here makes use of an earlier assumption that the vanishing cycles are nonzero. In particular, one shows that $\mathcal{R}^n\pi_*\mathbb{Q}_\ell$ is constant, and that $\mathcal{H}^0(\mathbb{P}^1;\mathcal{R}^n\pi_*\mathbb{Q}_\ell) = \mathcal{H}^n(X_u;\mathbb{Q}_\ell)$. Thus it suffices to show $(\star n)$ for $\mathcal{H}^n(X_u;\mathbb{Q}_\ell)$. In order to do this, we make use of the weak Lefschetz theorem to find the **surjective Gysin map** $\mathcal{H}^{n-2}(Y;\mathbb{Q}_\ell(-1)) \to \mathcal{H}^n(X_u;\mathbb{Q}_\ell)$, after which we simply apply the induction hypothesis to hyperplanes $Y \subset X$. One may also prove this result as dual to $\mathcal{H}^2(\mathbb{P}^1;\mathcal{R}^n\pi_*\mathbb{Q}_\ell)$ result.

5.3.3 $\mathcal{H}^1(\mathbb{P}^1;\mathcal{R}^{n-1}\pi_*\mathbb{Q}_\ell)$

The complicated technical machinery invoked in this proof is why a complete exposition of the Weil conjectures has been omitted from this paper. The following is a high level summary of how one begins to prove this result:

Step 1 First, with S denoting the set for which X^* is singular, we choose $u \in \mathbb{P}^1\backslash S$, and then verify the existence of the following filtration

$$(\mathcal{R}^{n-1}\pi_*\mathbb{Q}_\ell)_u \supset E \supset E \cap E^\perp \supset 0$$

where E is a finite dimensional $\mathbb{Q}_\ell$-vector space endowed with a continuous action of $\pi_1(U_0)$ of weight n, such that U_0 is a nonsingular affine curve over $\mathbb{F}_q$.

Step 2 Then, with U denoting the subset of $\mathbb{P}^1$ such that X_u is non-singular, we use the **Picard-Lefschetz formula** to describe the filtration from Step 1 as a filtration of $\pi_1(U)$-modules[12] with the following corresponding filtration on (constant) sheaves

$$j^*\mathcal{R}^{n-1}\pi_*\mathbb{Q}_\ell \supset \mathcal{E} \supset \mathcal{E} \cap \mathcal{E}^\perp \supset 0$$

[11] As the corresponding sequence is essentially $0 \to A \to B \to 0$

[12] So that $\pi_1(U) = \pi_1^{tame}(U,\bar{\eta})$

where $\mathcal{E}$ corresponds to E as a locally constant sheaf of $\mathbb{Q}_\ell$ vector spaces, and $j : U \to \mathbb{P}^1$.

Step 3 We apply j_* to the filtration from Step 2, to find the following filtration of interest:

$$\mathcal{R}^n\pi_*\mathbb{Q}_\ell \supset j_*\mathcal{E} \supset j_*(\mathcal{E} \cap \mathcal{E}^\perp) \supset 0$$

Step 4 Next, we verify that the first and third quotients of the filtration in Step 3 are constant.

Step 5 Next, we prove that for each quotient $(\star n)$ holds. We proceed by induction on $E/E \cap E^\perp$. Because $E/E\cap E^\perp$ is a simple π_1-module (hence, there is either no vanishing cycle in $E\cap E^\perp$, or it is zero and $E \subset E^\perp$), this amounts to even more case analysis. Within these two cases, in the relatively trivial case where the vanishing cycles are in E, this argument consists of demonstrating that there are exact sequences whose cohomology sequences are well behaved such that F acts on $\mathbb{Q}_\ell(m-n-1)$ as $q^{n-m-1} = q^{n/2}$ (recall that we are inducing on m with $n = 2(m+1)$). In the second case, the reduction proceeds by taking advantage of what I'll informally refer to as a *transfer property* of cohomology maps with the monic/epic universal mapping properties. In particular, this entails constructing an epimorphism $\mathcal{H}^1(\mathbb{P}^1; j_*\mathcal{E}) \to \mathcal{H}^1(\mathbb{P}^1; \mathcal{R}^{n-1}\pi_*\mathbb{Q}_\ell)$ and a monomorphism $\mathcal{H}^1(\mathbb{P}^1; \mathcal{R}^{n-1}\pi_*\mathbb{Q}_\ell) \to \mathcal{H}^1(\mathbb{P}^1; j_*(\mathcal{E} \cap \mathcal{E}^\perp))$. The reduction proof consists of demonstrating that it suffices to prove $(\star n)$ for $\mathcal{H}^1(\mathbb{P}^1; j_*(\mathcal{E} \cap \mathcal{E}^\perp))$.This proof of this result is the following lemma:

Lemma 54. *Let $n \in \mathbb{Z}$, and with E as a $\pi_1(U_0)$ module corresponding to a locally constant $\mathcal{E}$ as above, assume that*

1. *For all closed points of $x \in U_0$ (i.e. non-zero prime ideals), one has a Frobenius element that fixes some prime ideal of the, whose inverse, F_x acts rationally on E;*
2. *There is a non-degenerate $\pi_1(U_0)$-invariant skew symmetric form*

$$\psi : E \times E \to \mathbb{Q}_\ell(-n)$$

3. *The image of $\pi_1(U)$ in $Sp(E, \psi)$ is open in the ℓ-adic topology.*

Then

- *The eigenvalues of F_x on $\mathcal{E}_x$ have modulus $(q^{\deg x})^{n/2}$.*
- *The action of F on $\mathcal{H}^1(U;\mathcal{E})_c$ is rational, and its eigenvalues all have modulus $\leq q^{n/2+1}$.*
- *With $j : U \hookrightarrow \mathbb{P}^1$, the action fo F on $\mathcal{H}^1(\mathbb{P}^1; j_*\mathcal{E})$ is rational and the eigenvalues satisfy*

$$q^{n/2} < |\lambda| < q^{n/2+1}$$

Remark. What applying the main Lemma entails in either case is checking that for all closed points, the Frobenius on E is rational, that there is a non-degenerate, π_1 invariant, skew-symmetric form $\psi : E \times E \to \mathbb{Q}_\ell(-n)$, and that the geometric monodromy condition, which requires the image of $\pi_1(U)$ in $Sp(E,\psi)$ is open in the ℓ-adic topology, holds. Each of these requires its own separate, nested proof.

The reduction of the induction argument to this case follows from the proof that $\mathcal{H}^1(\mathbb{P}^1; j_*\mathcal{E}) \to \mathcal{H}^1(\mathbb{P}^1; \mathcal{R}^{n-1}\pi_*\mathbb{Q}_\ell)$ is a epimorphism, such that if $(\star n)$ holds for $\mathcal{H}^1(\mathbb{P}^1; j_*\mathcal{E})$, then it will hold for $\mathcal{H}^1(\mathbb{P}^1; \mathcal{R}^{n-1}, \pi_*\mathbb{Q}_\ell)$. Furthermore, since $\mathcal{H}^1(\mathbb{P}^1; j_*\mathcal{E}) \to \mathcal{H}^1(\mathbb{P}^1; j_*(\mathcal{E} \cap \mathcal{E}^\perp))$ is injective, if $(\star n)$ holds in $\mathcal{H}^1(\mathbb{P}^1; j_*(\mathcal{E} \cap \mathcal{E}^\perp))$, it must hold in $\mathcal{H}^1(\mathbb{P}^1; j_*\mathcal{E})$.

Chapter 6

A Verification of the Weil conjectures for $\mathbb{P}^n$

As one slightly non-trivial example of these conjectures, let's work with a nice non-singular projective variety, $\mathbb{P}^n$.

Remark. Let X be a simply reduced scheme of finite type over a field k. We can think of *points* in X in two ways:

1. Per the discussion in the preliminaries, X as above can be regarded as a topological space. Denoting by X^{cl} the set of closed points, for each $x \in X^{cl}$, there is a local ring $\mathcal{O}_{X,x}$ such that $\mathcal{O}_{X,x}/\mathfrak{m}_x \cong k(x)$, where the residue field $k(x)$ is a finite extension of k by Hilbert's Nullstellensatz. Thus it would be sensible to define the *degree* of x as the index of the extension from k to $k(x)$, denoting as follows

$$\deg(x) := [k(x) : k]$$

2. Alternatively, where K/k, the K-valued points of X can be described as follows. Let $f \in \mathrm{Hom}_{\mathrm{FLD}}(k, K)$, and denote by $X(K)$, the set of points defined to be $\mathrm{Hom}_{\mathrm{Spec}k}(\mathrm{Spec}K, X) =$

$\coprod \mathrm{Hom}_{X\downarrow k}(k(x), K)$. We identify $X(K)$ as the set of *K-valued points.*[1]

In particular, this second approach to points makes considerable sense when considering algebraic extensions K/k. If $f_* \in X(K)$, where $f_* : \mathrm{Spec}(K) \to X$, the point in X is the image of a unique closed point in Spec$K$. Through some elementary hand-waving (wringing?) we can identify that

$$\coprod_{x\in X} \mathrm{Hom}_{X\downarrow k}(k(x), K) = \coprod_{\deg(x)|n} \mathrm{Hom}_{X\downarrow k}(k(x), K)$$

where n is the finite degree of the field extension. This way of thinking about fixed *points* allows us to consider the Galois group $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z}$. So if $\deg(x) = d \leq n$, then the associated stabilizer of any element $x \in X$ will be isomorphic to $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})$. Hence $|\mathrm{Hom}_{X\downarrow k}(k(x), k)| = d$. It follows from this observation that

$$X(K) := \sum_{d|n} d \cdot |\{x \in X^{cl} \mid \deg(x) = d\}| \tag{6.0.1}$$

Moreoever, this approach is sub-additive; if $X = \bigcup^m Y_i$ and each Y_i is a closed subset, then $X(K) = \bigcup^m Y_i(K)$, and crucially, if X is a disjoint sum of Y_i, then $X(K) = \coprod Y_i(K)$ and

$$|X(K)| = \sum_i^m \sum_{d_i|n_i} d_i \cdot |\{x \in Y_i^{cl} \mid \deg(x) = d_i\} \tag{6.0.2}$$

This result is fairly intuitive. Suppose that X is an affine line $\mathbb{A}^n_k$. Then we notice $X(\mathbb{F}_{q^m}) = (\mathbb{F}_{q^m})^n$, and hence $|X(\mathbb{F}_{q^m})| = |\mathbb{F}_{q^m}|^n = q^{nm}$, i.e there are q^{nm} points in $\mathbb{A}^n_k(\mathbb{F}_{q^m})$. Then, since

$$\mathbb{P}^n_k = \mathbb{A}^n_k \coprod \mathbb{P}^{n-1}_k = \ldots = \coprod_{i=0}^n \mathbb{A}^i_k$$

we find that

$$|\mathbb{P}^n(\mathbb{F}_{q^m})| = 1 + q^m + q^{2m} + \ldots + q^{nm} = \sum_{i=0}^n q^{im} \tag{6.0.3}$$

If we consider X_0 to be the n-projective variety over $\mathbb{F}_q$, and X to be the corresponding variety over

[1] That Spec$K$ is trivial is precisely the point; it defines a terminal object, which we can denote by 1, and this is precisely the categorical notion of *element*, or more appropriate, a point in a space.

the algebraic closure $\mathbb{F}$, when we consider the Frobenius mapping $F : X \to X$, defined by $x \mapsto x^q$, we recognize that the hypersurface of X that is fixed by F corresponds to the $\mathbb{A}^i(\mathbb{F}_q)$ for $0 \leq i \leq n$, while in general, the hypersurface fixed by the m^{th}-iterate of the Frobenius F^m corresponds to $\mathbb{A}^{im}(\mathbb{F}_q)$. Thus, we have described the points fixed by F^m, denoted by $N_m = \sum_{i=0}^{n} q^{im}$.

This approach was the most immediately sensible way to approach this problem; the geometry is quite clear, however, it was done without explicit recourse to the ℓ-adic cohomology in counting the fixed points. It is imperative that we check this naive geometric approach is corroborated by the ℓ-adic cohomology that underlies the general proof.

In the interest of the general argument, we revisit the proof by considering that we satisfy the criteria for lifting to characteristic 0. In particular, where R is the corresponding discrete valuation ring with residue field $\mathbb{F}_q$, we take the natural homogeneous $f_i(T_0, \ldots, T_n) \in R[T_0, \ldots, T_n]$ such that modulo $\mathfrak{m}_R$, the f_i generate the homogeneous ideal of $\mathbb{P}^n, (0)$. Moreover, when regarded as polynomials in $K[T_0, \ldots, T_n]$, these f_i define a variety $\mathbb{P}^n(K)$. This allows us to lift $\mathbb{P}^n(\mathbb{F})$ to $\mathbb{P}^n(K)$ for any finite abelian group Λ (and hence, any $\mathbb{Z}/\ell^n\mathbb{Z}$ with $m \in \mathbb{N}$) such that

$$\mathcal{H}^r(\mathbb{P}^n(\mathbb{F}); \mathbb{Z}/\ell^n\mathbb{Z}) \cong \mathcal{H}^r(\mathbb{P}^n(K); \mathbb{Z}/\ell^m\mathbb{Z})$$

and thus, when taking the inverse limit

$$\mathcal{H}^r(\mathbb{P}^n(\mathbb{F}); \mathbb{Z}_\ell) = \varprojlim_m \mathcal{H}^r(\mathbb{P}^n(\mathbb{F}); \mathbb{Z}/\ell^m\mathbb{Z}) \cong \varprojlim_m \mathcal{H}^r(\mathbb{P}^n(K); \mathbb{Z}/\ell^m\mathbb{Z})$$

Furthermore, we can tensor both sides over $\mathbb{Z}_\ell$ by $\mathbb{Q}_\ell$, whence

$$\mathcal{H}^r(\mathbb{P}^n(\mathbb{F}); \mathbb{Q}_\ell) = \varprojlim_m \mathcal{H}^r(\mathbb{P}^n(\mathbb{F}); \mathbb{Z}/\ell^m\mathbb{Z}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \varprojlim_m \mathcal{H}^r(\mathbb{P}^n(K); \mathbb{Z}/\ell^m\mathbb{Z}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

However, as mentioned in the earlier properties of $\ell-$adic cohomology, this is simply $\mathbb{Q}_\ell$ as a 1 dimensional vector space for $r \in \{0, 2, \ldots, 2n\}$, and $\{0\}$ otherwise.

Now, we compute

$$N'_m = \sum (-1)^r \mathrm{Tr}(F^m | \mathcal{H}^r(\mathbb{P}^n(\mathbb{F}_q); \mathbb{Q}_\ell)) \cong \sum_{r=0}^{n} \mathrm{Tr}(F^m | \mathcal{H}^{2r}(\mathbb{P}^n(\mathbb{F}_q); \mathbb{Q}_\ell))$$

In order to do so, we must consider the corresponding generalized Frobenius mapping F^m, for $m \geq 1$, over this vector space. Equipped with this, we can describe the sum of the eigenvalues of F^m acting on by closed subvarieties Z by codimension. First, we note that for any choice of $Z \subset \mathbb{P}^n$ of codimension r, there exists a corresponding $[z] \in \mathcal{H}^{2r}(\mathbb{P}^n; \mathbb{Q}_\ell)$ such that $[z] \neq 0$. When $r = 0$, then F^m acts as [1] on $\mathcal{H}^0(\mathbb{P}^n; \mathbb{Q}_\ell)$. Then for $0 < r < n$, without loss of generality, let Z be the subvariety determined by $\{x_0 = x_1 = \ldots = x_{n-r} = 0\}$. Then the pullback $F^{m*}Z$ consists of q^{mr} lines corresponding to the choices of $q^{m^{th}}$ roots of unity, and so F^m acts on $\mathcal{H}^{2r}(\mathbb{P}^n; \mathbb{Q}_\ell)$ as $[q^{mr}]$. With this established, when codimension $r = n$, then F^m acts on $\mathcal{H}^{2n}(\mathbb{P}^n; \mathbb{Q}_\ell)$ as $[q^{mn}]$. We can then sum accordingly to find that $N'_m = 1 + q^m + \ldots + q^{nm} = N_m$. Thus, we find $N_m = N'_m$ agree. Hence,

$$\begin{aligned}
\zeta(\mathbb{P}^n(\mathbb{F}_q), t) &= \exp(\sum_{m\geq 1} N_m \frac{t^m}{m}) && (6.0.4)\\
&= \exp(\sum_{m\geq 1} (\sum_{i=0}^{n} q^{im}) \frac{t^m}{m}) && (6.0.5)\\
&= \exp(\sum_{i=0}^{n} \sum_{m\geq 1} q^{im} \frac{t^m}{m}) && (6.0.6)\\
&= \prod_{i=0}^{n} \exp(\sum_{m\geq 1} \frac{q^{im}}{m} t^m) && (6.0.7)\\
&= \prod_{i=0}^{n} \exp(-\log(1 - q^i t)) && (6.0.8)\\
&= \prod_{i=0}^{n} (1 - q^i t)^{-1} && (6.0.9)\\
&= \prod_{i=0}^{2n} \left[\exp\left(\sum_{m\geq 1} (\mathrm{Tr}(F^{m*} | \mathcal{H}^i(\mathbb{P}^n(\mathbb{F}_q); \mathbb{Q}_\ell))) \frac{t^m}{m} \right) \right]^{(-1)^m} && (6.0.10)\\
&= \prod_{i=0}^{2n} \left[\exp\left(\sum_{m\geq 1} (-1)^m (\mathrm{Tr}(F^{m*} | \mathcal{H}^i(\mathbb{P}^n(\mathbb{F}_q); \mathbb{Q}_\ell))) \frac{t^m}{m} \right) \right] && (6.0.11)\\
& && (6.0.12)
\end{aligned}$$

$$= \exp\left(\sum_{m\geq 1} N'_m \frac{t^m}{m}\right) \tag{6.0.13}$$

$$= \zeta(\mathbb{P}^n(\mathbb{F}_q), t) \tag{6.0.14}$$

Thus,

$$\zeta(\mathbb{P}^n(\mathbb{F}_q), t) = \frac{1}{(1-t)(1-qt)\cdots(1-q^n t)}$$

since $\sum_{m\geq 1} \frac{(-1)^{m+1}x^m}{m} = \log(1+x)$.

It is clear that this is a rational function as q is integral. Now to verify the functional equation:

$$\begin{aligned}
\zeta(\mathbb{P}^n(\mathbb{F}_q), \frac{1}{q^n t}) &= \frac{1}{(1-\frac{1}{q^n t})\cdot(1-\frac{1}{q^{n-1}t})\cdot\ldots\cdot(1-\frac{1}{t})} \\
&= \frac{(q^n t)(q^{n-1}t)\cdots t}{(-1)^{n+1}(1-q^n t)(1-q^{n-1}t)\cdots(1-t)} \\
&= (-1)^{n+1} q^{n(n+1)/2} t^{n+1} \zeta(\mathbb{P}^n(\mathbb{F}_q), t)
\end{aligned}$$

In particular, with equation (6.0.4), we can infer the analogue of the Riemann hypothesis as well as the Betti numbers, which come to us as the rank of the ordinary cohomology group for the respective complex manifold. That is, for odd dimensions, the rank is 0, and for even dimensions, the rank 1. Thus $\beta_i = \begin{cases} 1 & i \in \{0, 2, \ldots, 2n\} \\ 0 & otherwise \end{cases}$. Thus we can conclude that the Euler characteristic $\chi = n+1$, which we just verified indirectly.

Part III

Some Final Thoughts

Chapter 7

Future Work

As mentioned in the Foreward, this paper is incomplete. Due to the expansive nature of this project, and certain compromises that were made in order to begin laying the proverbial scaffolding for the project, many technical details were omitted. In hindsight, a radically different approach ought to have been taken, such that focus would have been given entirely to individual problems. However, there is at least one advantage to having conducted this survey; the following is a list of specific items that will need to be addressed in order to provide a complete proof within a formal proof verification program, such as `Coq` , or in some language realizing homotopy type theory (`HoTT`):

1. A general survey of the category of groups in `HoTT` ;
2. A general survey of the category rings in `HoTT` ;
3. A general survey of the category of fields in `HoTT` ;
4. A general survey of schemes and varieties with the tools of homotopy type theory, including a proof of Theorem ;
5. A follow up paper including a verification of the proof of Bertini's theorem;
6. A short paper on the Eilenberg-Steenrod axioms in homotopy type theory;
7. A short paper on the Künneth Formula and Poincaré duality, including a proof of the Universal Coefficient theorem;

8. A general survey of abelian sheaf cohomology within homotopy type theory;[1]
9. A short paper on the Chow ring;
10. A short survey of Gysin sequences;
11. A follow up paper to papers focusing on defining the type of Weil cohomology theories;
12. A paper focusing on Lefschetz pencils;
13. A survey focusing on Leray Spectral sequences.
14. A self-contained, and exhaustive paper presenting the proof of the Riemann Hypothesis, although ideally this should be split into the following, far more manageable and comprehensive papers:
    - A paper verifying the geometric reductions;
    - The construction of the desired filtration outlined in Steps 1-3 of section 5.3;
    - A Proof of Lemma 54;
    - A consolidation of these results.

This list is not exhaustive. In some cases, these individuals papers can be produced with little effort from the excised appendices.

[1] While [17] provides a nice overview of two approaches to cohomology in homotopy type theory, the former effectively using truncations, a nice paper performing some explicit calculations would be desirable.

Index

Bibliography

[1] Paulo Aluffi. *Algebra: Chapter 0*. American Mathematical Society, 2009.

[2] Steve Awodey. *Category Theory*. Oxford University Press, second edition, 2010.

[3] Carsten Butz and Ieke Moerdijk. Topological representation of sheaf cohomology of sites, 1996.

[4] P. Deligne, J.F. Boutot, L. Illusie, and J.L. Verdier. Cohomologie etale, 1971. Lecture Notes in Math. 569.

[5] Pierre Deligne. La conjecture de weil i. *Publications Mathématiques de l'IHÉS*, 43:278–308, 1974.

[6] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 82, 1960.

[7] Robert Goldblatt. *Topoi: The Categorial Analysis of Logic*. Dover Publications, Inc., revised second edition edition, 2006.

[8] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[9] Bart Jacobs. *Categorical Logic and Type Theory*, volume 141 of *Studies in Logic and The Foundations of Mathematics*. Elsevier, 1999.

[10] Peter T. Johnstone. *Sketches of An Elephant: A Topos Theory Compendium, Vol I*. Number 43 in Oxford Logic Guides. Oxford Science Publications, 2002.

[11] Peter T. Johnstone. *Sketches of An Elephant: A Topos Theory Compendium, Vol II*. Number 44 in Oxford Logic Guide. Oxford University Press, 2002.

[12] Saunders Mac Lane and Ieke Moerdijk. *Sheaves in Geometry and Logic: A First Introduction To Topos Theory*. Springer, 1992.

[13] Michael Makkai and Gonzalo Reyes. *First Order Categorical Logic*. Lecture Notes In Mathematics. Springer-Verlag, 2008.

[14] James S. Milne. Lectures on etale cohomology (v2.21), 2013. Available at www.jmilne.org/math/.

[15] Kate Ponto and Michael Shulman. Duality and traces for indexed monoidal categories.

[16] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. http://homotopytypetheory.org/book, Institute for Advanced Study, 2013.

[17] Mike Shulman. Cohomology. http://homotopytypetheory.org/2013/07/24/cohomology/, July 2013.