On the Étale Fundamental Group of Schemes over the Natural Numbers

Robert Hendrik Scott Culling

February 2019

A thesis submitted for the degree of Doctor of Philosophy
of the Australian National University

Australian National University

It is necessary that we should demonstrate geometrically, the truth of the same problems which we have explained in numbers.

— Muhammad ibn Musa al-Khwarizmi

For my parents.

Declaration

The work in this thesis is my own except where otherwise stated.

Robert Hendrik Scott Culling

Acknowledgements

I am grateful beyond words to my thesis advisor James Borger. I will be forever thankful for the time he gave, patience he showed, and the wealth of ideas he shared with me. Thank you for introducing me to arithmetic geometry and suggesting such an interesting thesis topic — this has been a wonderful journey which I would not have been able to go on without your support.

While studying at the ANU I benefited from many conversations about algebraic geometry and algebraic number theory (together with many other interesting conversations) with Arnab Saha. These were some of the most enjoyable times in my four years as a PhD student, thank you Arnab. Anand Deopurkar helped me clarify my own ideas on more than one occasion, thank you for your time and help to give me new perspective on this work. Finally, being a student at ANU would not have been nearly as fun without the chance to discuss mathematics with Eloise Hamilton. Thank you Eloise for helping me on so many occasions.

To my partner, Beth Vanderhaven, and parents, Cherry and Graeme Culling, thank you for your unwavering support for my indulgence of my mathematical curiosity. It has been a long time studying and you have always encouraged me to continue and to not give up — thank you for driving me on and providing the means for me to do so.

Last but not least I would like to thank the Australian people for providing my Australian Government Research Training Program (AGRTP) Stipend Scholarship and Australian Government Research Training Program (RTP) Fees

Offsets. Without this kind funding I could not have taken this great opportunity.

Abstract

The aims of the present thesis are to give a concrete description, in the modern language of arithmetic-algebraic geometry, of the Galois theory of Alexander Grothendieck (and the later generation of topos theorists: Micheal Barr, Radu Diaconescu, Peter Johnstone, and Ieke Moerdijk) in the context of the category of semirings, and to calculate the étale fundamental group of the spectrum of a number of semirings including: $\mathbb{B}$, $\mathbb{N}$, and $\mathbb{R}_+$.

In SGA I Grothendieck developed his Galois theory of schemes by classifying the subcategory of locally constant schemes as the category of finite G-sets for some group G — this theory is analogous to both the realization that the category of covering spaces of a topological space X is equivalent to the category of $\pi_1(X)$-sets, where $\pi_1(X)$ is the fundamental group of X, and the Galois theory of finite extensions of a field. Grothendieck himself suggested that this idea should hold in a broader context — for him, this meant the context of toposes. Indeed, later generations of topos theorists proved him correct. It is this theory that we are to apply to the category of affine $\mathbb{N}$-schemes in order to define the étale fundamental group of (the affine $\mathbb{N}$-scheme corresponding to) a semiring — this theory extends Grothendieck's Galois theory of (schemes) rings to the broader category of semirings.

Contents

Chapter 1

Introduction

1.1 Geometry of the Natural Numbers

In this thesis the main objects of consideration are algebraic structures called *semirings*. These objects are the abstract algebraic axiomatization of the basic arithmetic we were taught at school; that is to say, they are derived from the arithmetic of the non-negative integers $\mathbb{N} := \{0, 1, 2, 3, \ldots\}$ which we call the *natural numbers*. Indeed, the natural numbers are the foundation for all other systems of arithmetic. All of the commutative rings of algebraic number theory are *derived* from the natural numbers; the integers are derived from the natural numbers, and the rational numbers are constructed from the integers. Further constructions yield the finite fields, p-adic numbers, and the field of complex numbers. Due to this foundational role of the natural numbers and the axioms of semirings in constructing the basic objects of algebraic number theory it seems right to treat them on the same footing as the more arithmetically well understood algebraic objects, namely *rings*. In particular the extremely fruitful *geometric perspective* of ring theory should be extended to semirings.

Further to this observation of the foundational role of semirings in our understanding of ring theory and higher arithemtic, we now see semirings being used in sophisticated ways to attack deep problems in mathematics. Alain Connes and

Caterina Consani have made extensive use of tropical algebra, tropical geometry, and semirings in their work relating to the Riemann Hypothesis [15, 16, 17]. Tropical geometry is proving to be very influential in classical algebraic geometry by providing new insights and new proofs to old theorems [37]. Semirings, in particular the tropical semiring, play a foundational role in this area. Jeffery and Noah Giansiracusa, motivated by the theory of schemes in classical algebraic geometry, developed a theory of a tropicalisation of a scheme in order to better understand tropical algebraic geometry [19]. This theory of tropical schemes has been investigated further by Diane MacLagan and Felipe Rincón in [36]. Thus it is not only for the sake of applying Grothendieck's geometry of arithmetic to our complete understanding of arithemtic, but a real sense of utility for the broader mathematical community that we approach the arithmetic-algebraic geometry of semirings.

Arithmetic Geometry

Algebra and geometry have interacted prolifically throughout the history of mathematics. Algebraic geometry in the modern sense really began with the work of Richard Dedekind and Heinrich Martin Weber in the algebraic formalization of Bernhard Riemann's ideas relating to algebraic functions of one complex variable [39]. In their ground breaking paper Dedekind and Weber formulated a *duality* connecting algebraic information on the one hand and geometric information on the other. In particular they proved (in the language of today) an equivalence between a certain category of Riemann surfaces and a category of particular algebras over the ring of rational functions in one variable. It is interesting to note the work of Dedekind–Weber was the *first* formal description of Riemann surfaces, as the analysts only came to grips with them much later when the structure of a *manifold* was understood. Of particular relevance to the topic of the present thesis is the fact that Dedekind-Weber had all but proven the category of compact Riemann surfaces over $\mathbb{P}^1_{\mathbb{C}}$ is equivalent to the category of finite étale algebras over $\mathbb{C}(t)$. Precisely, they had shown that each compact Riemann surface can be recovered from its ring of rational functions in one variable — it was this method of constructing a ring from a geometric object and the reconstructing of the geometric object from the ring that was the key insight that sparked algebraic geometry.

This idea, present in the work of Dedekind–Weber, gave the first concrete glimpse of the modern duality between geometric concepts — compact Riemann surfaces — and algebraic concepts — algebras over $\mathbb{C}(t)$. In the years 1880 – 1955 many of the greatest mathematicians of the day worked on understanding and extending these ideas. André Weil, motivated by the growing realization that algebra and geometry are two sides of the same coin and the will to understand equations not over $\mathbb{C}$, but over finite fields $\mathbb{F}_q$, rewrote the foundations of algebraic geometry so as to include equations over *finite fields* [43]. Weil's understanding of the analogy between algebra and geometry was communicated vividly in a letter he wrote to his sister Simoné Weil [44]. In this letter Weil describes an analogy between three seemingly distinct languages; number fields, function fields over finite fields, and compact Riemann surfaces — this analogy between the three theories has been named *Weil's Rosetta Stone* due to its similarity with the Rosetta Stone found in Egypt which connects three ancient languages. This provided a belief that *number fields* should have some geometric behaviour just as algebras over $\mathbb{C}(t)$ (Dedekind–Weber) and finite fields (Weil) both have geometric realizations.

It was Alexander Grothendieck — with the help of Jean Dieudonné, Jean Pierre Serre, Pierre Deligne, and a number of other students at the Institut des Hautes Études Scientifiques — that formulated the precise duality between all *commutative rings with unity* and the category of geometric objects Grothendieck called *affine schèmas*; which was later translated into English as *affine scheme.* This theory was presented in Volumes I - IV of Éléments de Géométrie Algébrique (which we will here after refer to as, EGA)[23]. Grothendieck's theory of schemes has provided algebraic geometers with the complete dictionary between the algebra of commutative unital rings and geometry. Moreover, it has provided algebraic number theorists with a precise language with which they can interpret Weil's Rosetta stone — in this way Grothendieck provided us with the *geometry of arithmetic.*

Arithmetic Geometry over the Natural Numbers

Through the work of Dedekind–Weber, Weil, Grothendieck, and many others we now have a precise language with which we can express the geometry of commutative unital rings. It is clear from the work of Dedekind–Weber that this perspective was immensely helpful for geometers; they were the first mathematicians to give a concrete description of Riemann surfaces. Unsurprisingly the *duality* has also been of great utility to algebraists and number theorists; Oscar Zariski addressed the International Congress of Mathematicians in 1950 with the following remark on the utility of the geometric perspective in commutative algebra

> *"It is undeniably true that the arithmetization of algebraic geometry represents a substantial advance of algebra itself. In helping geometry, modern algebra is helping itself above all. We maintain that abstract algebraic geometry is one of the best things that happened to commutative algebra in a long time."*

Note this was stated *before* the theory of schemes was developed. In light of this service of the theory of schemes to the theory of commutative algebra, we should extend the theory of schemes beyond the category of commutative unital rings to the category of commutative unital *semirings* in the hope of yielding similar insight on the broader theory of semirings. When faced with the task of developing the theory of affine schemes for semirings one has two obvious paths to take when building the foundations of the subject; do we build the theory on the *spectrum of prime ideals and locally ringed spaces*? Or, do we take as foundational the *functor of points*?

Some authors have begun to explore the geometry of semirings from the perspective of Zariski-type topological spaces whose points consist of prime ideals or *prime congruences.* Jaiung Jun's PhD thesis studied, among other objects, semischemes which are locally ringed spaces that are patched together locally from affine semischemes [28]. These affine semischemes are locally ringed spaces whose underlying topological space consists of points corresponding to prime ideals of a semiring and whose topology and structure sheaf is exactly analogous to that of the spectrum of a commutative unital ring as found in EGA. In a later paper Jun recovers the theory of the Cech Cohomology for such objects [29]. In a series of three papers Paul Lescot lays foundations for the algebraic geometry of characteristic one semirings using prime congruences [32, 31, 33]. He shows that this space is different to the topological space defined using prime ideals. Another approach to the geometry of semirings is that of Oliver Lorscheid's *blue schemes* as described in [34, 35].

In 1973 Grothendieck presented a colloquium in which he advocated for the original (topological space of prime ideals) presentation of scheme theory to be abandoned as foundational, in favour of the functorial definition [21]. He stated that any of the "extra baggage" could be extracted later if need be. In their paper "au dessous Spec($\mathbb{Z}$)" Betrand Toën and Michel Vaquié presented a theory of schemes for commutative monoid objects in a symmetric monoidal category; in the case the monoidal category is the category of commutative monoids one obtains the category of commutative unital semirings [41]. Following Grothendieck and Toën-Vaquié we will define an *affine* $\mathbb{N}$*-scheme* to be a *representable functor* from the category of semirings to the category of sets. From this perspective an application of the Yoneda lemma gives us the duality between semirings and affine $\mathbb{N}$-schemes almost for free — this is one of the main advantages to setting up the foundations with functors to sets; the realization of the *space dual to a semiring* is a simple result of category theory.

With the geometric objects at hand, one can begin to ask: how much of the work of Grothendieck carries over to this category of affine $\mathbb{N}$-schemes? What are the counterparts of Éléments de géométrie algébrique (EGA), Séminaire de géométrie algébrique (SGA), and Fondements de la Géometrie Algébrique (FGA)? In Copenhagen during the summer of 2016 (one year after this project had started) Alain Connes and James Borger discussed questions such as these[1]. In particular, they wondered how Grothendieck's theory of the étale fundamental group could best be extended to semirings - More precisely extended to some geometric object associated to a semiring. In short, due to Grothdendieck's category theoretic style, one should believe that *all* of the work in the documents above have natural analogues in the broader world of $\mathbb{N}$-schemes. However this does not tell us how the theories actually work. It is the aim of this thesis to provide a concrete description of Grothendieck's theory of the *étale fundamental group* (i.e. the content of SGA I) in the broader context of affine $\mathbb{N}$-schemes with a language familiar to the modern arithmetic-algebraic geometer, and present the necessary algebraic geometry of affine $\mathbb{N}$-schemes required to make such a theory possible. In the next section we will revisit the fundamental group of a topological space and explain the manner in which Grothendieck reframed the theory so as to make it amenable to the context of schemes.

1.2 Étale Fundamental Groups

Algebraic topologists developed the theory of the fundamental group of a topological space X — denoted $\pi_1(X, p)$ — using the notion of homotopy equivalence classes of loops starting and ending at a point $p \in X$. This provided topologists with a bridge between topological spaces and group theory, thus allowing them to reframe previously intractable problems into the language of group theory, where the problem (hopefully) becomes a lot clearer. Incidentally, this bridge has also helped group theorists attack a number of problems in group theory by

[1]This is commented on further in Remark 4.4.

interpreting their problems geometrically/topologically — in much the same way that schemes have helped commutative ring theorists.

SGA 1 contains Grothendieck's formulation of the fundamental group in the context of schemes [22]. In order for him to associate a fundamental group to a scheme he needed to reframe the definition in a manner free from the use of loops[2]. Whether one chooses to use the functorial point of view that we are taking, or the spectrum of prime ideals, it is not at all clear what a loop in a scheme should be. Happily it was well known that the fundamental group of a topological space could be realised as the group of automorphisms of the universal cover $\tilde{X}$ which permuted fibers above each point $p \in X$ — these automorphisms are known as *deck transformations*. If Y is another covering space of X the group of deck transformations of Y over X is isomorphic to a quotient of $\pi_1(X,p)$ by some subgroup $H \leq \pi_1(X,p)$. Finally, this action of $\pi_1(X,p)$ on the collection of covering spaces of X commutes with morphisms between covering spaces — that is to say, the action of $\pi_1(X,p)$ is functorial. It took Grothendieck to realize that these facts could be pieced together to show $\pi_1(X,p)$ is isomorphic to the *automorphisms of the functor* which pulls back the category of covering spaces over X to the category of covering spaces of the point $p \in X$. In this way Grothendieck reduced the problem of defining a fundamental group for schemes to the problem of defining "covering spaces" of schemes — his solution to this problem was the notion of a *finite étale morphism* of schemes — and the matter of defining the correct notion of point to pull-back to. Grothendieck referred to this automorphism group as the *étale fundamental group* of a scheme. Note: the category of covering spaces over a point is equivalent to the category of sets. This means that the functor which pulls back to the fiber over a point can be considered a functor from the category of covering spaces of X to the category of sets.

[2]This is typical of much of Grothendieck's generalizations of concepts from other parts of mathematics; reframe the idea in a manner amenable to interpretation in the language of category theory and use that *as the definition*.

It was understood that the relationship between the covering spaces of a connected topological space and subgroups of its fundamental group resembled the relationship between field extensions and Galois groups defined by the fundamental theorem of Galois theory. With his theory of the étale fundamental group, Grothendieck was able to provide Galois theory with the geometric interpretation required to realize this resemblance in a concrete manner. We will see how exactly how this happens later in the thesis.

1.3 Galois Categories

At the heart of Grothendieck's reformulation of the theory of the fundamental group is a neat category theoretic presentation. We now know that a fundamental group can be associated to a pair $(\mathbf{C}, \mathcal{F})$, where $\mathbf{C}$ is a (small) category and $\mathcal{F} : \mathbf{C} \to \mathbf{sets}$ is a functor from $\mathbf{C}$ to the category of finite sets, **sets**, such that the pair behave according to the axioms of a *Galois category*. This statement of the axioms of a Galois category is translated directly from Grothendieck [22].

Definition 1.1 (Galois Category)**.** Let $\mathbf{C}$ be a category and $\mathcal{F}$ a covariant functor from $\mathbf{C}$ to **sets**, the category of finite sets. We say that $\mathbf{C}$ is a *Galois category* with *fundamental functor* $\mathcal{F}$ if the following six conditions are satisfied:

(G1) There is a terminal object in $\mathbf{C}$, and the fibred product of any two objects over a third one exists in $\mathbf{C}$.

(G2) Finite sums exist in $\mathbf{C}$, in particular an initial object, and for any object in $\mathbf{C}$ the quotient by a finite group of automorphisms exists.

(G3) Any morphism u in $\mathbf{C}$ can be written as $u = u'u''$, where u'' is an epimorphism and u' a monomorphism. Moreover, any monomorphism $u : X \to Y$ in $\mathbf{C}$ is an isomorphism of X with a direct summand of Y.

(G4) The functor $\mathcal{F}$ transforms terminal objects into terminal objects and commutes with fibred products.

(G5) The functor $\mathcal{F}$ commutes with finite sums, transforms epimorphisms into epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms.

(G6) If u is a morphism in $\mathbf{C}$ such that $\mathcal{F}(u)$ is an isomorphism, then u is an isomorphism. We call such a functor conservative.

Many of the familiar properties of the profinite completetion of the fundamental group of a (sufficiently) connected topological space (resp. the absolute Galois group of a field F) arise from the fact that the (resp. opposite) category of finite covering spaces (resp. finite étale algebras over F) behave according to the above list of axioms; in particular, the fact that the profinite completetion of the fundamental group (resp. absolute Galois group) is a profinite group can be deduced from the above axioms alone *separate from the particular context.* Independence (up to isomorphism) of the choice of base point can also be proven from the axioms of a Galois category, where the fundamental functor acts as the choice of base point. In order to obtain the full fundamental group of a topological space, one can consider all covering spaces (infinite covers included) and the corresponding notion of "Galois category" for such covers — however we will only consider finite covers.

As a result of the abstraction of the core principle behind Galois theory to the realm of category theory, mathematicians have been able to give specific types of categories which have the above properties. Alexander Grothendieck mentioned in Exercise 2.7.5 of [SGA IV, Expose iv, 1971] that his theory of the fundamental group of a scheme will work for the category of *locally constant objects* of an appropriately connected topos. Peter Johnstone has the details of this work spelled out in Section 8.4 of *Topos Theory* [24]. Thus it is well known that such a category of locally constant objects should behave like a Galois category — Galois topos. Furthermore, the Galois theory of toposes has been studied and extended by the following authors: Barr [4, 5]; Barr and Diaconescu [6]; Bunge [12]; Bunge and Moerdijk [13]; André Joyal and Myles Tierney [27]; John Kennison [30], and; Oliva Caramello [14]. In light of this work Galois theory and the theory of the fundamental group is now well understood in the context of toposes. In particular, it is understood that one should get a well behaved Galois-type theory by considering a category of locally constant objects. Therefore, before we even start, we know that our aim is attainable; by defining a topology on the category of affine $\mathbb{N}$-schemes and looking at the subcategory of affine $\mathbb{N}$-schemes that are locally constant, we should — by the work cited above — obtain a Galois category and hence a Galois group. Moreover, with the correct choice of topology this Galois theory of affine $\mathbb{N}$-schemes will recover Grothendieck's theory in the case that the affine $\mathbb{N}$-schemes are the spectrum of a ring.

It should be stated from the outset that the aim of this thesis is to describe the Galois theory of a (topos of objects over a) semiring in terms similar to the geometric exposition of the school of Grothendieck - rather than in the language of topos theory. Moreover, the research of the authors above suggest that this theory will work as it is but an example of their topos theoretic formalization of Galois theory. Since the Galois theory of toposes is well understood we know in advance that we will arrive at a sound theory; it is the exposition in terms of the particular language of semirings that is novel, rather than the existence of such a theory. Furthermore, this thesis will provide the original calculations of a number of fundamental groups of concrete semirings and discuss the relevance of these groups with respect to the category of affine schemes over $\mathbb{Z}$.

In the second chapter of the present thesis we present the definition a semiring and elaborate on a number of the key properties and concepts relating to the algebra of semirings. In the third chapter we give our definition of affine $\mathbb{N}$-scheme and consider the geometry of affine $\mathbb{N}$-schemes. Of note in the third chapter is the Section 3.4 which considers the passage to positive subsemirings in a geometric manner, as glueing "positivity data" to affine schemes over $\mathbb{Z}$. In chapter four we define what we mean by a finite étale morphism and the étale fundamental group of an affine $\mathbb{N}$-scheme. In the penultimate chapter we calculate the étale fundamental group of a number of affine $\mathbb{N}$-schemes. In the final chapter we consider some of the reasons for the results obtained and explore a number of directions for further research.

Chapter 2

Abstract Algebra of Semirings

Semirings are the focus of this thesis. In the present chapter we introduce semirings, study their first properties, and consider a number of examples of semirings. Together with some category theory, the definitions and examples of this chapter will give us a platform from which we can study the geometry of the natural numbers — that is, scheme theory over the natural numbers.

2.1 Semirings: Definitions and Examples

Semirings are abstract objects. However they encode the most basic structures of arithmetic; addition *and* multiplication of whole numbers. In order to do addition and multiplication all one needs is a collection of things (that is, a *set*) which one can add and multiply together. Thus the definition that follows provides the fundamental framework in which one can do arithmetic.

Definition 2.1. A *semiring* is a 5-tuple $(R, +_R, \cdot_R, 0_R, 1_R)$ which consists of: a set, R; associative binary operations $+_R : R \times R \to R$ (which we refer to as addition) and $\times_R : R \times R \to R$ (which we refer to as multiplication) with the following properties

- $\forall a, b \in R \; a +_R b = b +_R a$ [Addition is commutative]

- $\forall a, b \in R \; a \cdot_R b = b \cdot_R a$ [Multiplication is commutative]

- $\forall a, b, c \in R\ a \cdot_R (b + c) = a \cdot_R b +_R a \cdot_R c$ [Multiplication distributes over addition];

and, distinguished (not necessarily distinct) elements of R, 0_R and 1_R, such that: $\forall a \in R\ a +_R 0_R = a$, $0_R \cdot_R a = 0_R$, and $a \cdot_R 1_R = a$.

The distinguished elements 0_R and 1_R will be referred to as the additive and (resp.) multiplicative identities of the corresponding semiring.

Remark 2.2. One should note that there are some differences in definitions throughout the literature on semirings. For instance, some authors do not require semirings to have the distinguished elements 0_R or 1_R. Similarly, some authors do not require the binary operation of multiplication to be commutative. In this thesis we are primarily motivated by arithmetic (number theoretic) topics, and here most of the semirings that arise are commutative. Indeed, we will only consider unital commutative semirings — that is, semirings with commutative multiplication and a multiplicative identity.

Remark 2.3. Many of the definitions in this thesis come from Johnathon S. Golan's text *Semirings and their Applications*. In this text Golan presents the theory of semirings (including noncommutative semirings) and a number of their applications [20].

We will make liberal use of the following abuses of notation: a semiring will be denoted by its set, often leaving the binary operations $+_R$ and $\cdot_R$ as implied and the subscripts on $+_R$, $\cdot_R$, 0_R, and 1_R will be dropped.

Example 2.4. The natural numbers, $\mathbb{N} := \{0, 1, 2, 3, \dots\}$ with their standard addition and multiplication form a semiring.

Example 2.5. If R is a semiring in which $0_R = 1_R$, then every element of the semiring is equal to 0_R. In which case we say R is the zero-semiring. We will denote the zero-semiring by $\mathbf{0}$.

Example 2.6 (Ring)**.** One may define a *ring* as a 5-tuple $(R, +_R, \cdot_R, 0_R, 1_R)$ such that (i) the 5-tuple forms a semiring, and (ii) $\forall a \in R\ \exists b \in R$ such that $a+b = 0_R$. Thus, every ring is a semiring.

Again, one must remark that there are differences in the definition of a ring in the literature. As before, one need not assume the existence of 0_R, 1_R, nor that multiplication is commutative. However, in this thesis a ring will be as defined in the example. Namely, commutative in both operations, with identities, and existence of additive inverses. Indeed these conditions are required for usual scheme theory, so in order to stay consistent with that theory we are required to make this definition.

Definition 2.7 (Subsemiring)**.** If $R = (R, +, \cdot, 0_R, 1_R)$ is a semiring and $S \subseteq R$ is a subset closed under $+$, $\cdot$, with identities $0_S = 0_R$ and $1_S = 1_R$, then we say S is a subsemiring of the semiring R.

Example 2.8 (Positivity)**.** One can find semirings within $\mathbb{R}$ by making use of its natural order. Precisely, given any sub(semi)ring R of $\mathbb{R}$, one can pick out the *positive* (elements greater than or equal to 0) subset of R. This subset will form a subsemiring of $\mathbb{R}$. We will denote this subsemiring $R_+ := \{r \in R \mid r \geq 0\}$. For example the subset of positive rational numbers, $\mathbb{Q}_+$, form a semiring. Moreover, the natural numbers arise in this manner as $\mathbb{N} = \mathbb{Z}_+$.

Example 2.9. The *Boolean semiring*, denoted $\mathbb{B}$, is defined on the set $\{0, 1\}$ by declaring $1 + 1 = 1$. Notice, every other addition and multiplication is already defined by the axioms of a semiring. This seemingly unassuming semiring will play a key role later chapters.

Example 2.10 (Tropical Semiring, $\mathbb{T}$)**.** In this example we define the *tropical real numbers* which are appearing across mathematics with great effect; in particular they are doing a lot of work, and provide a lot of promise, in algebraic geometry. The process by which we arrive at the tropical real numbers $\mathbb{T}$ is often referred to as *Maslov dequantization* [37].

This process begins with the observation that, for each $t \in \mathbb{R}_{>0}\backslash\{1\}$, the map $\log_t : \mathbb{R}_+ \to \mathbb{R} \cup \{-\infty\}$ does not form a homomorphism with the standard operations on $\mathbb{R} \cup \{-\infty\}$. However, we can force it to be a homomorphism by letting it *induce* the following operations on $\mathbb{R} \cup \{-\infty\}$ — for each $t \in \mathbb{R}_{>0}\backslash\{1\}$ $x \oplus_t y := \log_t(t^x + t^y)$ and $x \otimes_t y := x + y$. We note the element $-\infty$ behaves as expected; namely, for each $y \in \mathbb{R} \cup \{-\infty\}$ we define $-\infty \oplus_t y := y$ and $-\infty \otimes_t y := -\infty$. This process determines a family of semirings (for each $t \in \mathbb{R}$) consisting of $(\mathbb{R} \cup \{-\infty\}, \oplus_t, \otimes_t, -\infty, 0)$.

This continuum of semirings depends on the parameter $t \in \mathbb{R}_{>0}\backslash\{1\}$. One might wonder: what is the semiring *at infinity*? That is, what happens in the limit $t \to \infty$. In order to see the behaviour in this limit, let us first observe the following inequalities

$$\max(x, y) \leq x + y \leq 2\max(x, y).$$

In particular, for $t \geq 1$

$$\max(t^x, t^y) \leq t^x + t^y \leq 2\max(t^x, t^y).$$

Moreover, for each $t > 1$ the function $\log_t$ is strictly increasing, therefore

$$\max(x, y) \leq x \oplus_t y \leq \log_t(2) + \max(x, y).$$

Now we can see that as $t \to \infty$, $\log_t(2) \to 0$ and $x \oplus_t y \to \max(x, y)$. Therefore we conclude that the limit of this family of semirings as $t \to \infty$ is the semiring $\mathbb{T} := (\mathbb{R} \cup \{-\infty\}, \max(\ ,\ ), +, -\infty, 0)$. We note, for each $x \in \mathbb{R} \cup \{-\infty\}$ we have $\max(x, -\infty) = x$ and hence that $-\infty$ really is the additive identity of this semiring. We call this semiring the *tropical semiring* and henceforth denote it $\mathbb{T}$. In this context we may refer to max as *tropical sum* and + as *tropical multiplication*. Note: the tropical numbers are often referred to as $\mathbb{R}_{\max}$ and they have a number of sub-semifields arising from the additive sub-groups of $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ which are explored in [42].

2.2 First Properties of Semirings

In this section we explore a number of the basic properties of semirings and some of the ways to construct new semirings from old. This section consists of definitions from Johnathon S. Golan's *Semirings and their Applications* [20].

Definition 2.11 (Zero Sum Free)**.** If R is a semiring such that $\forall a \neq 0 \in R$ the equation $x + a = 0$ does not have a solution, then we say R is zero sum free.

If R is a non-zero ring, then R can't be zero sum free. Zero sum free semirings are often referred to as *strict* semirings in the literature.

Example 2.12. The natural numbers are zero sum free. Indeed, all subsemirings of the reals of the form R_+ (see Example 2.8) are zero sum free.

Definition 2.13 (Cancellative)**.** We say that a semiring R is (additively) cancellative if for each $a, b, c \in R$, we have $a + b = c + b$ implies $a = c$.

Note that a semiring is addtively cancellative if and only if it can be mapped injectively into a ring. Zero sum free semirings can be cancellative — just as being an integral domain does not imply the existence of multiplicative inverses.

Example 2.14. The natural numbers are cancellative. As are all $R_+ \subseteq \mathbb{R}$.

The following definition is the multiplicative version of the previous definition.

Definition 2.15 (Integral Domains)**.** We say that a non-zero semiring R is an integral domain if for each $a, b, c \in R$, and $b \neq 0$ we have $a \cdot b = c \cdot b$ implies $a = c$.

Definition 2.16 (Semifield)**.** If R is an integral domain, then we say R is a semifield if for every $a \neq 0 \in R$, there exists an element b such that $ab = 1$.

If R is a semifield and $a \in R$ such that there exists a $b \in R$ where $ab = 1$, then b is unique in this respect. As such, we will denote it $a^{-1} := b$. Moreover, this relationship is symmetric in a and b.

Definition 2.17 (Polynomial Semiring)**.** If R is a semiring, then we can define the semiring of *polynomials with coefficients in* R as follows

$$\mathcal{P} := \left(\bigoplus_{\mathbb{N}} R, +, \times \right)$$

such that for each $u = (u_i)_{i \in \mathbb{N}}$ and $v = (v_j)_{j \in \mathbb{N}}$ there exist elements $s = (s_k)_{k \in \mathbb{N}}$ and $t = (t_\ell)_{\ell \in \mathbb{N}}$

$$\begin{aligned} u + v &:= s, \text{ where } s_k := u_k + v_k \\ u \times v &:= t, \text{ where } t_\ell := \sum_{i+j=\ell} u_i v_j. \end{aligned}$$

If $f = (f_i)_{i \in \mathbb{N}}$ is an element of $\mathcal{P}$ we will denote it $f(x) := \sum_{f_i \neq 0} f_i x^i$, where x is some choice of indeterminate symbol and (under this identification) we will denote the semiring of polynomials with coefficients in R as $R[x]$.

If $R[x]$ is the polynomial ring over R in the indeterminate x, then we will denote $(R[x])[y] = R[x, y]$ and refer to it is as the polynomial ring in 2 indeterminate symbols over R. By induction we may similarly define the semiring $R[x_1, \ldots x_n]$ of polynomials in finitely many indeterminate symbols. Moreover, we may allow the case of infinitely many indeterminate x_i with each polynomial only being a sum of products of finitely many of them.

Example 2.18. If R is an integral domain, then $R[x]$ (and, by induction $R[x_1, \ldots x_n]$ for each integer n) is an integral domain.

If R, R' are semirings, then the product set $R \times R'$ with component-wise operations forms a semiring, we call this the product semiring. In general if $(R_i)_{i \in I}$ is any family of semirings indexed by a set I, we can form the product set indexed by I and this will also form a semiring under component-wise operations. Semirings of this form will be extremely important in the later chapters of this thesis. In particular, we need to know how to recognise when a semiring can be written in this form. The key ingredients are *idempotent elements* of semirings.

Definition 2.19 (Idempotents)**.** If $e \in R$ is an element of R such that $e^2 = e$, then we say that e is an *idempotent* of R. If $e \neq 0$ or 1, then we say that e is a *non-trivial idempotent* of R.

If R is a ring, then the existence of a non-trivial idempotent is enough to prove that $R \cong R_1 \times R_2$, for some non-zero rings R_1, R_2. However, the next example shows this is *not* the case for semirings.

Example 2.20. The second octant in $\mathbb{R}^2$ i.e. $A := \{(x, y) \in \mathbb{R}^2_+ \mid y \geq x\}$ is a semiring. This semiring has the non-trivial idempotent $e := (0, 1)$. However A does *not* decompose into a product of semirings. Intuitively, this is because $1 - e \notin A$. In fact, we know that this semiring does not have any zero-divisors, therefore it can't have any such family of orthogonal elements.

It is still true that a product of some finite number, n, of semirings contains a family of n idempotents $(e_i)_{i=1}^n$ which sum to the identity and multiply (in the semiring) as $e_i e_j = \delta_{ij} e_i$ — these are the elements with a 1 in the i-th column and 0 else where. We will see that the converse is also true.

Definition 2.21 (Connected Semiring)**.** Let $R \neq 0$ be a semiring. If there exists a finite set I such that $|I| \geq 2$ and a family $(e_i)_{i \in I}$ of non-trivial idempotents in R with the following properties (i) $e_i e_j = \delta_{ij} e_i$, and (ii) $\sum_I e_i = 1_R$, then we say R is *disconnected*. If the only family of idempotents with properties (i) and (ii) is $\{0, 1\}$ and $0 \neq 1$, then we say R is *connected*. We will refer to a family of idempotents with property (i) as being *mutually orthogonal*.

Definition 2.22 (Standard Idempotents)**.** If I is a finite set indexing a family $(R_i)_{i \in I}$ of semirings R_i, then the product $\prod_{i \in I} R_i$ contains the family of idempotents $(e_i)_{i \in I}$ where $e_j = (\delta_{ij})_{i \in I}$. We will refer to the family $(e_i)_{i \in I}$ of idempotents as the *standard idempotents* of the product $\prod_{i \in I} R_i$.

These are the often referred to as the *standard basis vectors* when each $R_i = k$ is a fixed field for every $i \in I$.

2.3 Morphisms of Semirings

Since the introduction of category theory mathematicians have come to understand that in order to understand an object X it is important to understand objects which "relate" to X — that is, to understand the ambient category in which X lives. In this section we define semiring homomorphisms, thus providing the manner in which semirings relate to one and other and as such defining the ambient category that we are interested in.

Definition 2.23. If R and S are semirings, then a *semiring homomorphism* from R to S is a set map $\varphi : R \to S$ with the following properties: $\varphi(x +_R y) = \varphi(x) +_S \varphi(y)$; $\varphi(x \cdot_R y) = \varphi(x) \cdot_S \varphi(y)$; $\varphi(0_R) = 0_S$; and, $\varphi(1_R) = 1_S$.

If $\varphi : R \to S$ is a semiring homomorphism and there exists a semiring homomorphism $\psi : S \to R$ such that $\psi \circ \varphi = \mathrm{id}_R$ and $\varphi \circ \psi = \mathrm{id}_S$, then we say that φ (and ψ) is a semiring isomorphism. In this case we say S and R are *isomorphic* and denote this relation $S \cong R$.

Remark 2.24. If R is a ring, then $\varphi(0_R) = 0_S$ can be derived from the other properties of a ring homomorphism. This proof makes explicit use of additive inverses and as such does not prove this property holds for such maps of semirings. Indeed the existence of the morphism $f : \mathbf{0} \to \mathbb{B}$ where $0 \mapsto 1$ proves that this must be required in the definition.

Example 2.25. The set map $\varphi : \mathbb{N} \to \mathbb{B}$ which sends $0 \mapsto 0$ and for each $x \neq 0$, $x \mapsto 1$ is a semiring homomorphism. Moreover if $R \subseteq \mathbb{R}$ is a subsemiring of the real numbers, then $\varphi : R_+ \to \mathbb{B}$ which sends $0 \mapsto 0$ and non-zero elements to 1 is a semiring homomorphism.

Theorem 2.26. *If R is a zero sum free integral domain, then the map $\varphi : R \to \mathbb{B}$ where $\varphi(0) = 0$ and for each non-zero $x \in R$, $\varphi(x) = 1$ is a semiring homomorphism.*

Proof. Let $x, y \in R$. If (wlog) $x = 0$, then $\varphi(x+y) = \varphi(y)$ and $\varphi(x)+\varphi(y) = \varphi(y)$. Also $\varphi(xy) = \varphi(0) = 0$ and $\varphi(x)\varphi(y) = 0$. Let us assume both x and y are non-zero. In this case, (as R is zero sum free) $x + y \neq 0$, so $\varphi(x + y) = 1$. Moreover $\varphi(x) + \varphi(y) = 1 + 1 = 1$. Similarly, $\varphi(xy) = 1$ since R is an integral domain and $\varphi(x)\varphi(y) = 1$. Therefore the map φ is a semiring homomorphism. ■

Example 2.27 (No Maps from $\mathbb{Z}$ to $\mathbb{B}$)**.** If $\varphi : \mathbb{Z} \to \mathbb{B}$ is a semiring homomorphism, then it must send the additive and multiplicative identities (respectively) of $\mathbb{Z}$ to the additive and multiplicative identities of $\mathbb{B}$; that is, $\varphi(0) = 0$ and $\varphi(1) = 1$. However, this means $\varphi(1 + (-1)) = 0$ and $1 + \varphi(-1) = 0$. This system has no solution in $\mathbb{B}$. Therefore no such semiring homomorphism can exist.

Example 2.28. If $\varphi : \mathbb{N} \to \mathbb{B}$ is defined as in Example 2.25, then the kernel is trivial — only $0 \in \mathbb{N}$ is sent to $0 \in \mathbb{B}$. However, the morphism is far from injective! The preimage of 1 has infinite cardinality. For this reason we will not make use of the notion of kernel of a semiring homomorphism in this thesis.

Theorem 2.29. *If R is a semiring, then R is disconnected if and only if there exists a finite set, I, such that $|I| \geq 2$ and for every $i \in I$ non-zero semirings R_i such that $R \cong \prod_I R_i$.*

Proof. If R is isomorphic to a finite product of semirings R_i, then the standard idempotents form a family of idempotents which are (i) mutually orthogonal, and (ii) sum to unity. So R is disconnected. If R is disconnected, then there exists a finite set I (with at least two elements) and a family of idempotents $(e_i)_{i \in I}$ such that (i) $e_i e_j = \delta_{ij} e_i$, and (ii) $\sum_I e_i = 1_R$. For each $i \in I$ observe $Re_i := \{re_i \mid r \in R\}$ is a semiring with multiplicative identity e_i. Denote $R_i := Re_i$. We can define a semiring homomorphism $\varphi : R \to \prod_I Re_i$ by $r \mapsto (re_i)_{i \in I}$. This homomorphism has the inverse $\psi : \prod_I R_i \to R$ which maps $(r_i e_i)_{i \in I} \mapsto \sum_I r_i e_i$. ■

Example 2.30. Theorem 2.29 gives us the tools to give another proof that the semiring $A := \{(x, y) \in \mathbb{R}^2_+ \mid y \geq x\}$ in Example 2.20 does not decompose as a product. Indeed the only idempotents of A are $(0, 0), (1, 1)$, and $(1, 0)$. No collection of these constitute a family of mutually orthogonal non-trivial idempotents which sum to unity. Therefore A is *not* disconnected. Note: the proof of the existence of one non-trivial idempotent in a semiring R is *not enough* to conclude that R splits as a (non-trivial) product; contrary to the case for commutative rings.

It will be essential for us to understand morphisms between products of semirings in order to really understand finite étale morphisms later in the thesis. We will take some time now to study some of the important lemmata relating to such morphisms of semirings.

Lemma 2.31. *If R is a semiring, N a finite set, $f : R^N \to R$ an R-algebra homomorphism, and $\{e_i \mid i \in N\} \subseteq R^N$ the family of standard idempotents, then each of the following hold*

(i) If $e_i \neq e_j$ and $f(e_i) = f(e_j)$, then $f(e_i) = f(e_j) = 0$.

(ii) $N' := \{r \in R \mid r \neq 0 \text{ and } \exists i \in N : r = f(e_i)\} \subseteq R$ is an orthonormal family of idempotents in R.

(iii) $R \cong \prod_{r \in N'} Rr$.

Proof. In order to prove (i) consider multiplying both sides of the equation $f(e_i) = f(e_j)$ by $f(e_i)$. It follows $f(e_i) = f(e_i e_j) = f(0) = 0$. Moreover, by assumption, $f(e_i) = f(e_j) = 0$. Before we prove (ii) let us first note: if $r \in N'$, then there exists *precisely one* $e_i \in R^N$ which maps to it. For, if there were two (distinct) e_i, e_ℓ mapping to r, then by (i) $r = 0$.

In order to prove N' is an orthonormal family of idempotents it must be shown that the $r \in N'$ are idempotents, mutually orthogonal, and sum to unity. Images of idempotents are idempotents. Orthogonality can be seen from the following equations: for each $r \neq s \in N'$ we have $rs = f(e_j)f(e_\ell) = f(e_j e_\ell) = f(0) = 0$. Recall the sum of the $e_i \in R^N$ is unity, therefore $f(\sum_N e_i) = f(1) = 1$. Consider the term $f(\sum_N e_i)$. Since f is a homomorphism we see that $f(\sum_N e_i) = \sum_N f(e_i)$. Some of the e_i will get sent to 0, however the image of those elements which do not get sent to 0 are precisely the $r \in N'$. Thus, $\sum_{r \in N} r = 1$ as required. Theorem 2.29 proves the third part of this lemma. ■

After we have discussed quotient semirings we will present another version of this lemma in terms of quotients of R, rather than the semirings Rr.

2.4 Congruence Classes and Quotients

In this section we formally describe how semirings can be constructed as quotients of other semirings by *congruence relations*; these are precisely the type of equivalence relations that allow the operations of the semiring to descend to the quotient. Of note is the fact that ideals do *not* play a prominent role in the quotients of semirings in general, as they do with rings. James Borger [10] and Golan [20] both describe congruence relations and their corresponding quotients.

Recall that an equivalence relation on a set S can be considered as a subset of $S \times S$ in the following manner: if $\sim$ is an equivalence on S, then all relations $a \sim b$, for $a, b \in S$, correspond to pairs $(a, b) \in S \times S$. We make use of this idea in the following definition of a congruence relation.

Definition 2.32 (Congruence Relation)**.** If R is a semiring, then a *congruence relation on* R, denoted $\sim$, is an equivalence relation which, as a subset of $R \times R$, is a semiring. The collection of congruence classes of R under $\sim$ is denoted $R/\sim$.

We will refer to the congruence relation which equates an element $r \in R$ with itself, and only itself, as the *trivial congruence relation.* As a subset of $R \times R$ the trivial congruence relation corresponds to the diagonal $\Delta := \{(r, r) \mid r \in R\}$.

Theorem 2.33 (Quotient Semirings)**.** *If R is a semiring and $\sim$ is a congruence relation on R, then the set of equivalence classes $R/\sim$ forms a semiring with the operations* $[r] + [s] := [r + s]$ *and* $[r] \cdot [s] := [r \cdot s]$.

Proof. In order to prove this we need to prove that $+$ and $\cdot$ as given in the statement of theorem are well defined, and that they have identities. Suppose $r \sim r'$ and $s \sim s'$ are equivalences under the congruence relation. We are required to prove $[r] + [s] = [r'] + [s']$ and $[r] \cdot [s] = [r \cdot s]$.

Let $S_\sim \subseteq R \times R$ denote the congruence relation as a subsemiring of $R \times R$. This means $(r, r') \in S_\sim$ and $(s, s') \in S_\sim$. Since $S_\sim$ is a semiring, we know $(r, r') + (s, s') = (r + s, r' + s') \in S_\sim$. However, this implies $r + s \sim r' + s'$ and $[r]+[s] = [r']+[s']$. Similarly, $(r, r') \cdot (s, s') = (rs, r's') \in S_\sim$, so $[r] \cdot [s] = [r'] \cdot [s']$.

The congruence classes generated by the additive and multiplicative identities, [0] and [1], are the additive and multiplicative identities (resp.) for the addition and multiplication on the set $R/\sim$. ■

Remark 2.34. If R is a *ring*, then quotienting R by a congruence relation is equivalent to "quotienting by an ideal". In particular, if $I \subseteq R$ is an ideal of R, then we can define an equivalence relation, $\sim_I$, on R in the following way: $\forall a, b \in R$, we say $a \sim_I b$ if and only if $a - b \in I$. From a congruence relation, $\sim$, on R one may obtain an ideal $I_\sim := \{r \in R \mid r \sim 0\}$. If R is a ring, then these two processes are inverses of one another; that is to say, ideals and congruence relations are in bijection with one another. This bijection makes calculations with quotients *very convenient.*

If R is a *semiring* and I is an ideal of R, then these processes are not inverses. That is to say congruence relations are not in bijection with ideals.

Definition 2.35 (Simple Semirings)**.** If R is a semiring that has precisely two congruence relations, then we say R is simple.

Example 2.36. The only semiring which is both simple and zero sum free is $\mathbb{B}$ [20].

Definition 2.37 (Maximal Congruence Relations)**.** If $\sim$ is a congruence relation on a semiring R such that $R/\sim$ is simple, then we say $\sim$ is a maximal congruence relation.

All fields are simple semirings. However, there are some semifields which are *not* simple. For example, the positive rational numbers $\mathbb{Q}_+$ is not a simple semiring; for there is a surjective homomorphism $f : \mathbb{Q}_+ \to \mathbb{B}$ which is determined by $0 \mapsto 0$ and $1 \mapsto 1$.

Definition 2.38 (Quotient by a Single Relation)**.** If R is a semiring and (a, b) is an element of $R \times R$, then we denote the *smallest congruence relation on R defined by* (a, b):$=\sim_{(a,b)}$ and the corresponding quotient semiring $R/\langle a = b\rangle := R/\sim_{(a,b)}$.

The smallest congruence relation on R exists due to the fact that the intersection of subsemirings (in this case subsemirings of $R \times R$) is again a subsemiring and the intersection of a subequivalence relations is again an equivalence relation. Thus the interection of congruence relations is again a congruence relation.

Remark 2.39. In order to obtain the smallest subsemiring of $R \times R$ containing (a, b) that is reflexive and symmetric it suffices to take the diagonal (for reflexivity) and all polynomials of the form $\sum_{i=0}^{n}(r_i, r_i)(a, b)^i$ and $\sum_{i=0}^{n}(r_i, r_i)(b, a)^i$.

One might then ask: If $S_\sim \subseteq R \times R$ is a reflexive symmetric subsemiring of $R \times R$, is $S_\sim$ necessarily transitive? — no. Consider the reflexive symmetric semiring of $\mathbb{N} \times \mathbb{N}$ generated by the element $(1, 2)$. This contains $(1, 2)$ and $(2, 3)$. But it cannot contain $(1, 3)$. For this reason one must further close $S_\sim$ under transitivity. That is, include all transitive relations.

If $((a_i, b_i))_{i\in I}$ is a family of elements in $R \times R$, then we can consider the smallest congruence relation of $R \times R$ that contains each of the elements (a_i, b_i) and denote this $\sim_{((a_i,b_i))_{i\in I}}$. We denote the corresponding *quotient semiring of R generated by the* (a_i, b_i) as $R/\langle a_1 = b_1, \ldots, a_i = b_i, \ldots\rangle := R/\sim_{((a_i,b_i))_{i\in I}}$.

Example 2.40 ($\mathbb{B}$ as a Quotient of $\mathbb{N}$)**.** The Boolean semiring, $\mathbb{B}$, can be realised as the quotient of $\mathbb{N}$ by the (smallest congruence relation generated by the) element $(1, 2)$. Let the subsemiring of $\mathbb{N} \times \mathbb{N}$ corresponding to this congruence relation be denoted $S_\sim$. Since $S_\sim$ is (i) a semiring (ii) symmetric, it contains polynomials in $(1, 2)$ and $(2, 1)$. The only other elements it contains are the "closures under transitivity". None of these elements have a 0 in precisely one of their entries; this follows from the fact that $\mathbb{N}$ is a zero sum free integral domain. Therefore, $(0, n) \notin S_\sim$ if $n \neq 0$. In particular, $(0, 1) \notin S_\sim$.

Thus $\mathbb{N}/\langle 1 = 2\rangle$ contains precisely two congruence clases; namely, [0] and [1]. Moreover, the induced operations are precisely the operations of the Boolean numbers. Therefore this quotient semiring is isomorphic to $\mathbb{B}$ under the isomorphism $[0] \mapsto 0$ and $[1] \mapsto 1$.

For use later in the thesis we state a theorem from Johnathon Golan's *Semirings and Their Applications* which relates to *simple* semirings; We will return to this theorem and its corollary in Chapter 4 to discuss its geometric content.

Theorem 2.41 (Golan). *If R is a non-zero semiring having no nontrivial proper congruence relations, then either $R = \mathbb{B}$ or R is a field.*

Corollary 2.42. *If R is a non-zero semiring, then there exists a semiring homomorphism from R to $\mathbb{B}$ or a field.*

Congruence relations and polynomial semirings allow us to give *presentations* of semirings over other semirings. That is, we can represent a semiring as being generated by a number of *generators* and *relations*.

Definition 2.43 (Presentations of Semirings). Let R, A be semirings. If I, N are sets and $(f_i)_{i\in I}$ and $(g_i)_{i\in I}$ are families of polynomials in the polynomial semiring $R[x_n \mid n \in N]$ such that there exists an isomorphism

$$\varphi : \frac{R[x_n \mid n \in N]}{\langle f_i = g_i \mid i \in I\rangle} \to A$$

then we say the data $((x_n)_{n\in N}, \langle f_i = g_i \mid i \in I\rangle, \varphi)$ is a *presentation of A over R.* If N can be taken to be a finite set, then we say A is *finitely generated over R.* If both I and N can be taken to be finite sets, then we say A is *finitely presented over R.*

Example 2.44 (Presentation of the Integers over the Naturals). The ring of integers has the following finite presentation over the natural numbers
$\mathbb{Z} \cong \mathbb{N}[x]/\langle x + 1 = 0\rangle$. If we define $\tilde{f} : \mathbb{N}[x] \to \mathbb{Z}$ by mapping $x \mapsto -1$, then f descends to a surjective homomorphism $f : \mathbb{N}[x]/\langle x+1 = 0\rangle \to \mathbb{Z}$. Moreover the unique map out of the integers $g : \mathbb{Z} \to \mathbb{N}[x]/\langle x + 1 = 0\rangle$ is the inverse of f.

The next lemma reformulates Lemma 2.31 in terms of quotient semirings and presentations.

Lemma 2.45. *If R is a semiring, N a finite set, with $f : R^N \to R$ an R-algebra homomorphism, $\{e_i \mid i \in N\} \subseteq R^N$ the family of standard idempotents, and $N' := \{r \in R \mid r \neq 0 \text{ and } \exists i \in N : r = f(e_i)\} \subseteq R$, then the morphism*

$$\varphi : R \to \prod_{r \in N'} \frac{R}{\langle r = 1 \rangle}$$

defined by mapping $x \mapsto (xr)_{r \in N'}$ is an isomorphism.

Proof. In light of Lemma 2.31 it suffices to prove: $\forall r \in N'\ Rr \cong R/\langle r = 1 \rangle$. In order to prove this we define a morphism $\overline{\psi} : R \to Rr$ by mapping $x \mapsto rx$ and show this descends to an isomorphism on the quotient.

As this morphism is surjective, it suffices to prove that it descends to the quotient. Denote by $\tilde{E}$ the symmetric and reflexive closure of $\langle (r, 1) \rangle \subseteq R \times R$. Let us first suppose $(x, y) \in \tilde{E}$. This implies there exist $s_i, t_j \in R$ such that $(x, y) = \sum_{i=0}^{k} (s_i, s_i)(r, 1) + \sum_{j=0}^{\ell} (t_j, t_j)(1, r)$. That is to say $x = \sum_{i=0}^{k} (s_i r) + \sum_{j=0}^{\ell} t_j$ and $y = \sum_{i=0}^{k} s_i + \sum_{j=0}^{\ell} t_j r$. If we apply $\overline{\psi}$ to both sides we see:

$$\overline{\psi}(x) = \overline{\psi}\left(\sum_{i=0}^{k} s_i r + \sum_{j=0}^{\ell} t_j\right) = \sum_{i=0}^{k} s_i \overline{\psi(r)} + \sum_{j=0}^{\ell} t_j \overline{\psi(r)} = \sum_{i=0}^{k} s_i + \sum_{j=0}^{\ell} t_j$$

$$\overline{\psi}(y) = \overline{\psi}\left(\sum_{i=0}^{k} s_i + \sum_{j=0}^{\ell} t_j r\right) = \sum_{i=0}^{k} s_i \overline{\psi(r)} + \sum_{j=0}^{\ell} t_j \overline{\psi(r)} = \sum_{i=0}^{k} s_i + \sum_{j=0}^{\ell} t_j$$

This calculation uses the fact that $\overline{\psi(r)} = r^2 = r$, which is the identity on Rr. This proves that if (x, y) are in $\tilde{E}$, then $\overline{\psi}$ maps them to the same element. In order to prove $\overline{\psi}$ descends to the quotient, we need to check elements agree if they are in the transitive closure of this set, which we denote E. If $(u, v) \in E$, this implies there exists $t \in R$ such that $(u, t), (t, v) \in \tilde{E}$. As we know $\overline{\psi}$ agrees on elements upto $\tilde{E}$ we may conclude $\overline{\psi}(u) = \overline{\psi}(t) = \overline{\psi}(v)$. Therefore $\overline{\psi}$ descends to a morphism $\psi : R/\langle r = 1 \rangle \to Rr$. Injectivity follows in a similar manner to our proof that ψ is well defined. Therefore ψ is an isomorphism.

∎

2.5 Modules over Semirings

In ring theory modules over a ring R are an important tool for studying the structure of R itself and studying the geometry of $\mathrm{Spec}(R)$. The same is true for semirings. This section introduces *modules over a semiring* and some of their properties.

Definition 2.46 (R-module)**.** If R is a semiring and M is a commutative monoid with a bilinear map $R \times M \to M$ which maps $(r, m) \mapsto rm$ and has the following associativity property: $\forall r, s \in R$ and $m \in M$ $(rs)m = r(sm)$, then we say M is an R-module.

We refer to the bilinear map as *multiplication by* R, or *the action of* R *on* M. We often suppress the fact that the multiplication by R is a bilinear map in our notation, and simply denote it, for each $r \in R$ and $m \in M$, as rm.

Remark 2.47. If R is a semiring and M is a monoid, then giving an R-module structure to M is equivalent to giving a semiring homomorphism $f : R \to \mathrm{End}(M)$. However, $\mathrm{End}(M)$ is, in general, *not* a *commutative* semiring.

Definition 2.48 (R-module Homomorphism)**.** Let R be a semiring and M, N be R-modules. If $\varphi : M \to N$ is a homomorphism of monoids, then we say φ is an R-module homomorphism if $\forall r \in R$ and $m \in M$, $\varphi(r \cdot m) = r \cdot \varphi(m)$. Where, $r \cdot m$ denotes the R-module action of R on M and $r \cdot \varphi(m)$ denotes the R-module action of R on N.

Definition 2.49 (Sub-R-module)**.** If R is a semiring and M is an R-module, then any submonoid $N \subseteq M$ that is closed under the action of R is called a *sub* R*-module of* M.

Example 2.50. If R is a semiring, then it is in fact a monoid under addition and, separately, multiplication. However, the natural action of R on the multiplicative monoid does *not* in general form an R-module, for the action does not distribute over the operation (multiplication) of the monoid.

Definition 2.51 (Ideals of Semirings)**.** If R is a semiring and $M \subseteq R$ is a sub-R-module of the additive R-module, then we say that M is an *ideal* of the semiring R.

Example 2.52. If R is a semiring and $r \in R$, then $\langle r \rangle := \{x \in R \mid \exists a \in R\ x = ra\}$ is a sub-R-module of R. We call this the *principal ideal generated by* r.

Lemma 2.53. *If* $e, e' \in R$ *are idempotents and* $\langle e \rangle = \langle e' \rangle$*, then* $e = e'$*.*

Proof. Since $\langle e \rangle = \langle e' \rangle$ we know $e' \in \langle e \rangle$ which implies there exists an $r \in R$ such that $e' = re$. Similarly, there exists an $r' \in R$ such that $e = r'e'$. Together these equations imply $r'e' \cdot e' = ee' = re \cdot e$. Which implies $r'e' = re$. Thus by choice of r, r' we conclude $e = e'$. ∎

Example 2.54. If M, M' are R-modules, then the product set $M \times M$ has a natural module structure where multiplication by r on an element (m, m') is simply given by component-wise multiplication from the respective module structures; that is to say, $r \cdot (m, m') = (rm, rm')$. We will often refer to this as the diagonal action of R on the product $M \times M'$. By extension, we can form any product indexed by any set I and define the module structure component wise.

If F is a field, then all modules (i.e. vector spaces) over F are free by the axiom of choice. The following example proves this is *not* the case for *semifields*.

Example 2.55. Let $M := \{(x, y) \mid x > 0 \text{ and } y > 0\} \cup \{(0, 0)\} \subseteq \mathbb{R}^2$. This is an $\mathbb{R}_+$-module, which is *not* free. If this were free, then it would be generated by two distinct vectors — for any three (or more) distinct non-zero elements are necessarily dependent. However, given only two vectors one could never obtain elements outside the $\mathbb{R}_+$ cone of them. Therefore M can't be free.

Example 2.56. The Boolean semiring, $\mathbb{B}$, is principally generated as a module over $\mathbb{N}$. However it is not freely generated.

Quotients of R-modules are also an important tool for the study of R-modules. We present the relevant definitions for the formal study of quotients of R-modules.

Intuitively, the idea is much the same as for semirings; however, instead of requiring the equivalence relation E on an R-module M to be a sub-semiring of $M \times M$, we simply require it to be a sub-R-module — indeed, a semiring structure has not been defined on M and hence can't be expected of a congruence relation in $M \times M$.

Definition 2.57 (Equivalence Relation on an R-module)**.** Let R be a semiring and M be an R-module. An R-module equivalence relation, E, on M is a sub-R-module $E \subseteq M \times M$ that is also an equivalence relation.

Theorem 2.58 (Quotient R-modules)**.** *If R is a semiring, M an R-module, and E an R-module equivalence relation on M, then the set of equivalence classes of M under E, denoted M/E, forms an R-module under the following operations: $\forall a, b \in M \ r \in R, \ \ [a] \cdot [b] := [ab]$ and $r[a] := [ra]$.*

With quotients of R-modules defined we may now define the *tensor product* of two R-modules. An important construction which will be used extensively in the study of the geometry of semirings.

Definition 2.59 (Tensor Product of R-modules)**.** Let M and N be R-modules. Let E denote the equivalence relation on the free R-module $\bigoplus_{M \times N} R$ given by the following relations:

$$\forall\, m, m' \in M \;\forall\, n \in N \quad (m + m', n) = (m, n) + (m', n)$$

$$\forall\, n, n' \in N \;\forall\, m \in M \quad (m, n + n') = (m, n) + (m, n')$$

$$\forall\, r \in R \;\forall\, m \in M \;\forall\, n \in N \quad (r \cdot m, n) = (m, r \cdot n) = r(m, n)$$

$$(0_M, b) = 0$$

$$(a, 0_N) = 0$$

Since M, N are R-modules, the quotient $\bigoplus_{M \times N} R/E$ comes equipped with a natural R-module structure. We denote the quotient R-module, $M \otimes_R N := \bigoplus_{M \times N} R/E$ and denote congruence classes of $(m, n) \in M \times N$ as $m \otimes n \in M \otimes_R N$.

The relations defined in the previous definition are really defined on the basis elements $e_{(m,n)}$ of the free R-module $\bigoplus_{M\times N} R$. However, we have abused notation and identify each basis element with its index.

Remark 2.60. For a fixed R-module M the endofunctor

$$\mathrm{Hom}_{\mathbf{Mod}_R}(M,-) : \mathbf{Mod}_R \to \mathbf{Mod}_R$$

has a left adjoint given by the tensor product

$$M \otimes_R - : \mathbf{Mod}_R \to \mathbf{Mod}_R.$$

This means for each choice of R-module M, N, and P the following sets of homomorphisms are equal $\mathrm{Hom}_{\mathbf{Mod}_R}(M \otimes_R N, P) = \mathrm{Hom}_{\mathbf{Mod}_R}(N, \mathrm{Hom}_{\mathbf{Mod}_R}(M, P))$. Furthermore, since $\mathrm{Hom}_{\mathbf{Mod}_R}(N, \mathrm{Hom}_{\mathbf{Mod}_R}(M, P)) = \mathrm{Bil}_{\mathbf{Mod}_R}(M \times N, P)$ — the module of R bilinear maps — we may conclude that a homomorphism $M \otimes_R N \to P$ is equivalent to a *bilinear homomorphism* $M \times N \to P$. In fact $M \otimes_R N$ is the universal such object i.e. $M \otimes_R N$ is the coproduct of M, N in the category of R-modules [10].

It will be important for us to understand the behaviour of products of finitely many semirings and modules over such products of semirings. For now we will state a number of lemmata pertaining to such objects which we can call on later in the thesis.

Lemma 2.61. *If $R = \prod_{i=1}^n R_i$ is a product of semirings R_i and M is an R-module, then $M \cong \oplus_{i=1}^n M_i$ where M_i is an R_i-module.*

Proof. In fact we can say precisely what each M_i is, namely

$$M_i := \{m \in M \mid e_i m = m\}.$$

This should be expected as e_i is the identity of R_i. First we note, if $m \in M$, then $m = m \cdot 1 = m(\sum_{i=1}^n e_i) = \sum_{i=1}^n e_i x$. Since $e_i \cdot e_i x = e_i x$, we know $e_i x \in M_i$. Moreover, if $x \in M_i$ and $x \in M_j$ for $i \neq j$, then $e_i x = x = e_j x$. If we multiply through by e_j, then we see $e_j e_i x = e_j x = x$ i.e. $0 = x$. Therefore $M \cong \oplus_{i=1}^n M_i$, as required. ∎

Moreover the morphisms between modules over product semirings also break up into morphisms which act componentwise according to the decomposition given in Lemma 2.61.

Lemma 2.62. *If $R = \prod_{i=1}^{n} R_i$ is a product of R-algebras R_i and $f : M \to N$ is morphism of R-modules, then (i) $M \cong \oplus_{i=1}^{n} M_i$ and $N \cong \oplus_{i=1}^{n} N_i$, and (ii) $f = \oplus_{i=1}^{n} f_i$, for R_i-module homomorphisms $f_i : M_i \to N_i$.*

Proof. Part (i) is the content of Lemma 2.61. Again, we can explicitly define the required data. If $x_i \in M_i$, then we define $f_i(x_i) := f(x_i)$. Since the M_i are submodules, this is well defined. ■

2.6 Algebras over Semirings

An algebra over a ring R is (intuitively) another ring A whose elements can be multiplied by elements of R. Moreover, one typically requires that for each $a \in A$ (i) $0_R \times a = 0_A$ and (ii) $1_R \times a = a$. Morphisms of semirings allow us to *formally* define what it means for A to be an algebra over R.

Definition 2.63. If R and A are semirings and $\varphi : R \to A$ is a semiring homomorphism, then we say the pair (A, φ) is an R-algebra.

If (A, φ) is an R-algebra, then we refer to φ as the *structure morphism* of the R-algebra. We will often simply refer to (A, φ) by A, and leave the structure morphism implied. Instead of saying A is an R-algebra, we may instead say A is an algebra over R.

Remark 2.64. Indeed this does let us multiply elements of A by elements of R. We define this multiplication in the following way: for each $r \in R$ and $a \in A$, we may define $r \times a := \varphi(r)a$. Since φ is a semiring homomorphism both 0_R and 1_R act as required in the introduction to this section.

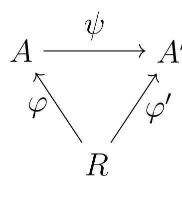
Example 2.65. Every semiring R is an R-algebra over itself via the identity homomorphism.

Example 2.66. If R is a semiring and $R[x_1, \ldots, x_n]$ the polynomial in n indeterminates with coefficients in R, then the set map $\varphi : R \to R[x_1, \ldots, x_n]$ which sends each $r \in R$ to the constant polynomial $r \in R[x_1, \ldots, x_n]$, is a semiring homomorphism and therefore defines a structure morphism for $R[x_1, \ldots, x_n]$ over R.

Example 2.67. Theorem 2.26 specifies a structure morphism for $\mathbb{B}$ over each zero sum free semiring. Thus, the Booleans are an algebra over all zero sum free semirings. This will be important later as it allows us to guarantee a $\mathbb{B}$-point for some $\mathbb{N}$-schemes.

Example 2.68 (Semirings are $\mathbb{N}$-algebras)**.** If A is a semiring, then there is a *unique* semiring homomorphism $\varphi : \mathbb{N} \to A$ which maps $1 \mapsto 1_A$. This follows from the fact that the image of 0 and 1 are determined, and the image of 1 determines the image of each $n > 1$ in $\mathbb{N}$. Moreover, this induced map is a semiring homomorphism. This implies that every semiring is an algebra over $\mathbb{N}$ *in a unique way.* For this reason we will often refer to semirings as $\mathbb{N}$-algebras.

Definition 2.69. If (A, φ) and (A', φ') are R-algebras, then an R-algebra homomorphism between them is a semiring homomorphism $\psi : A \to A'$ such that the following diagram commutes



That is to say, $\psi \circ \varphi = \varphi'$

Example 2.70. If R is a semiring and $(A, \varphi), (A', \varphi')$ are R-algebras, then the semiring homomorphism $\psi : R \to A \times A'$ determined by $r \mapsto (\varphi(r), \varphi'(r))$, defines the R-algebra $(A \times A', \psi)$.

Definition 2.71 (Presentations of R-Algebras)**.** Let R be a semiring and A an R-algebra. If I, N are sets and $(f_i)_{i\in I}$ and $(g_i)_{i\in I}$ are families of polynomials in the polynomial semiring $R[x_n \mid n \in N]$ such that there exists an isomorphism

$$\varphi : \frac{R[x_n \mid n \in N]}{\langle f_i = g_i \mid i \in I\rangle} \to A$$

of R-algebras, then we say the data $((x_n)_{n\in N}, \langle f_i = g_i \mid i \in I\rangle, \varphi)$ is a *presentation of A as an R-algebra.* If N is a finite set, then we say A is *a finitely generated R-algebra.* If both I and N are finite sets, then we say A is *a finitely presented R-algebra.*

If R is a semiring and (A, φ), (B, ψ) are R-algebras, then we can construct another R-algebra out of them, which we call the *tensor product of A and B over R*, or simply the tensor product of A and B.

Definition 2.72 (Tensor Product of R-algebras)**.** If (A, φ) and (B, ψ) are algebras over a semiring R, then the tensor product $A \otimes_R B$ is the R-module spanned by elements of the form $a \otimes b$ for $a \in A$ and $b \in B$ with the following relations

$$\forall\, a, a' \in A\ \forall\, b \in B \quad (a + a') \otimes b = a \otimes b + a' \otimes b$$

$$\forall\, b, b' \in B\ \forall\, a \in A \quad a \otimes (b + b') = a \otimes b + a \otimes b'$$

$$\forall\, r \in R\ \forall\, a \in A\ \forall\, b \in B \quad \varphi(r)a \otimes b = a \otimes \psi(r)b = r(a \otimes b)$$

$$0_A \otimes b = 0$$

$$a \otimes 0_B = 0.$$

In this way see $A \otimes_R B$ is a quotient of $\bigoplus_{M\times N} R$ and the congruence relation generated by those relations given above. Moreover, the multiplication from algebra structures extends to $A\otimes_R B$ in the following way $(a\otimes b)(a'\otimes b') := aa'\otimes bb'$, thus $A \otimes_R B$ is in fact a semiring. Finally the morphism $f : R \to A \otimes_R B$ which sends $r \mapsto \varphi(r) \otimes 1 = 1 \otimes \psi(r) = r(1 \otimes 1)$ makes $(A \otimes_R B, f)$ and R-algebra.

Note that the morphism $a \mapsto a \otimes 1$ from $A \to A \otimes_R B$ is a semiring homomorphism, as $0_A \otimes 1_B = 0_{A\otimes_R B} \in A \otimes_R B$. Similarly, the map $b \mapsto 1 \otimes b$ from

$B \to A \otimes_R B$ is also a semiring homomorphism. Not all elements of $A \otimes_R B$ are of the form $a \otimes b$. In general, $x \in A \otimes_R B$ is of the form $x = \sum_{i=1}^{n} a_i \otimes b_i$. Elements of the form $a \otimes b$ are called *elementary tensors*.

Remark 2.73. Similarly to Remark 2.60 we note that this tensor product of R-algebras A, B has the following universal property: if $f : A \to C$ and $g : B \to C$ are R-algebra homomorphisms, then there exists a *unique* R-algebra homomorphism $h : A \otimes_R B \to C$ which commutes with f, g and the morphisms $A \to A \otimes_R B$ and $B \to A \otimes_R B$. Tensor product is the coproduct in the category of R-algebras [10].

Example 2.74 (Useful Tool for Calculating Tensor Products.)**.** If A is an R-algebra with a presentation

$$A \cong \frac{R[x_n \mid n \in N]}{\langle f_i = g_i \mid i \in I \rangle}$$

and C is another R-algebra, then the tensor product $A \otimes_R C$ has the following presentation

$$A \otimes_R C \cong \frac{C[x_n \mid n \in N]}{\langle f_i = g_i \mid i \in I \rangle}$$

where the polynomials f_i and g_i are interpreted with coefficients in C via the structure morphism of the R-algebra C.

Lemma 2.75. *If $\sigma \in S_{|N|}$ is an element of the permutation group on a finite set N, then σ induces an R-algebra automorphism $f_\sigma : R^N \to R^N$ by permuting N. If A is an R-algebra, then (i) $R^N \otimes_R A \cong A^N$ and (ii) $f_\sigma \otimes \mathrm{id}_A : A^N \to A^N$ permutes the elements of N via σ.*

2.7 Categories of Semirings

Category theory provides an excellent framework for thinking about mathematics and is an indispensable tool for understanding mathematical objects and their relations to each other. In this section we introduce the category of semirings and study the properties of this category. We note that James Borger [10] proves much of what is to follow about the category of semirings.

Definition 2.76 (Category of Semirings)**.** Let $\mathbf{Alg}_{\mathbb{N}}$ denote the category whose class of objects is the class of all semirings and, for each pair of objects R, R', the morphisms between them are the set of semiring homomorphisms $\mathrm{Hom}_{\mathbf{Alg}_{\mathbb{N}}}(R, R')$.

This notation is used due to the observation in Example 2.68; that every semiring is an $\mathbb{N}$-algebra in a unique way. This is another way of saying $\mathbb{N}$ is the *initial object* in the category of semirings.

Definition 2.77 (Category of R-algebras)**.** If R is a semiring, then let $\mathbf{Alg}_R$ denote the category whose class of objects is the class of all R-algebras and, for each pair of objects A, A', the morphisms between them are the set of R-algebra homomorphisms $\mathrm{Hom}_{\mathbf{Alg}_R}(A, A')$.

Example 2.78 (Characteristic One)**.** It is often said that a semiring R has characteristic one if for all $r \in R$ the equation $r + r = r$ holds [32]. In particular, $1 + 1 = 1$ in such a semiring. In the context of the previous definition, this naturally places all semirings of characteristic one inside $\mathbf{Alg}_{\mathbb{B}}$. That is to say, all semirings of characterisitic one are algebras over the Booleans.

When given a category, such as $\mathbf{Alg}_{\mathbb{N}}$, there are a number of natural operations under which one can ask if $\mathbf{Alg}_{\mathbb{N}}$ is closed. These properties include products and coproducts. More generally, one can ask if $\mathbf{Alg}_{\mathbb{N}}$ is closed under limits and colimits. Simply one might ask if a category is *complete* and/or *cocomplete*.

Lemma 2.79. *If R is a semiring and A, A' are R-algebras, then $A \times A'$ has the universal property of the product in $\mathbf{Alg}_R$. Moreover, $A \otimes_R A'$ has the universal property of the coproduct in $\mathbf{Alg}_R$.*

Proof. The product in the category of R-algebras can be computed in the underlying category of sets. Indeed the product set $A \times A'$ equipped with component wise operations and the projection maps $\pi_1 : A \times A' \to A$ and $\pi_2 : A \times A' \to A'$

form the triple $(A \times A', \pi_1, \pi_2)$, which has the universal property of the product in the category of R-algebras. That the tensor product is the coproduct follows from Remark 2.60. ■

Corollary 2.80. *If R is a semiring, then $\mathbf{Alg}_R$ is closed under finite products and coproducts.*

One can ask if $\mathbf{Alg}_R$ has equalizers of every pair of morphisms $\varphi, \psi : A \to B$. Again, $\mathbf{Alg}_R$ does have limits.

Theorem 2.81. *If A and B are objects in $\mathbf{Alg}_R$ and $\varphi, \psi \in \mathrm{Hom}_{\mathbf{Alg}_R}(A, B)$, then the equalizer and coequalizer of φ, ψ exist in $\mathbf{Alg}_R$.*

Proof. The equalizer is simply the subsemiring $E := \{a \in A \mid \varphi(a) = \psi(a)\}$ with the inclusion morphism $i : E \hookrightarrow A$. While the coequalizer of the pair φ ψ is the quotient of B by the congruence relation generated by the elements $(\varphi(a), \psi(a)) \in B \times B$. ■

So far we know for each semiring R the category $\mathbf{Alg}_R$ has finite products, coproducts, equalizers, and coequalizers. Therefore we may conclude on the basis of results from category theory, for each semiring R the category $\mathbf{Alg}_R$ is finitely complete and finitely cocomplete category [8]. This also means the opposite category ${\mathbf{Alg}_R}^{op}$ is both finitely complete and finitely cocomplete.

In the following lemmata we identify the sets M^N and $\mathrm{Hom}_{\mathbf{sets}}(N, M)$. In particular we index an element R^{M^N} with set maps $\alpha : N \to M$.

Lemma 2.82. *If R is an $\mathbb{N}$-algebra and M, N are finite sets, then the morphism*

$$\theta : \left(R^M\right)^{\otimes N} \to R^{M^N}$$

defined on elementary tensors to send $(r_i^1)_{i \in M} \otimes \cdots \otimes (r_i^n)_{i \in M} \mapsto x = (x_\alpha)_{\alpha \in M^N}$ where, $x_\alpha := \prod_{j \in N} r^j_{\alpha(j)}$ is an R-algebra isomorphism.

Proof. In order to define a morphism out of a tensor product it suffices to define a morphism out of each of the factors in the tensor product. Similarly, in order to define a morphism into a product it suffices to define a morphism into each factor. Therefore we first define for each $\alpha \in M^N = \mathrm{Hom}_{\mathbf{sets}}(N, M)$ the morphisms

$$\theta_{\alpha,j} : R^M \to R$$

by mapping $(r_i)_{i\in M} \mapsto r_{\alpha(j)}$ i.e. $\theta_{\alpha,j}$ is projection onto the $\alpha(j)$th factor. Piecing these together gives, by the universal properties of maps out of a tensor product, R-algebra homomorphisms for each $\alpha \in M^N$

$$\theta_\alpha : (R^M)^{\otimes N} \to R$$

by maping $(r_i^1)_{i\in M} \otimes \cdots \otimes (r_i^n)_{i\in M} \mapsto \prod_{j\in N} \theta_{\alpha,j}((r_i^j))_{i\in M} = \prod_{j\in N} r^j_{\alpha(j)}$. Finally the universal property for morphisms into a product yield the morphism claimed in the statement of the lemma.

■

Lemma 2.83. *If R is an $\mathbb{N}$-algebra and M, N are finite sets, then the morphism*

$$\eta : \mathrm{Hom}_{\mathbf{Alg}_R}(R^M, R^N) \to \mathrm{Hom}_{\mathbf{Alg}_R}((R^M)^{\otimes N}, R)$$

defined by $f \mapsto \pi_1 f \otimes \pi_2 f \otimes \cdots \otimes \pi_n f$ is an isomorphism of sets.

Proof. This is a restatement of the universal property of tensor products. ■

Lemma 2.84. *If R is an $\mathbb{N}$-algebra, M, N finite sets, and $\alpha : N \to M$ a morphism of finite sets, then α induces a morphism $f_\alpha : R^M \to R^N$ by mapping $r \mapsto s = (s_j)_{j\in N}$ where $s_j = r_{\alpha(j)}$.*

Proof. That this is a homorphism follows from the universal property of morphisms into a product. It is constructed from the N morphisms which project onto the $\alpha(j)$th factor. ■

Remark 2.85. If $\alpha : N \to M$ is a map between finite sets N, M, then f_α can be defined as in Lemma 2.84. Furthermore, we can use α to define the morphism $\pi_\alpha : R^{M^N} \to R$ as the projection onto the α-th factor. We will now prove $\eta(f_\alpha) = \pi_\alpha \circ \theta$. That is to say, f_α is sent to π_α under the following chain of isomorphisms $\mathrm{Hom}_{\mathbf{Alg}_R}(R^M, R^N) \cong \mathrm{Hom}_{\mathbf{Alg}_R}((R^M)^{\otimes N}, R) \cong \mathrm{Hom}_{\mathbf{Alg}_R}(R^{M^N}, R)$. It suffices to check how these morphisms act on elementary tensors. On the one hand $\eta(f_\alpha)(((r_i^1)_{i\in M} \otimes \cdots \otimes (r_i^n)_{i\in M})) = (\pi_1(f_\alpha)(r_i^1)_{i\in M}) \otimes \cdots \otimes \pi_1(f_\alpha)(r_i^n)_{i\in M})) = r^1_{\alpha(1)} \cdots r^n_\alpha(n) = \prod_{j\in N} r^j_{\alpha(j)}$. On the other hand Lemma 2.83 shows $\pi_\alpha \circ \theta(((r_i^1)_{i\in M} \otimes \cdots \otimes (r_i^n)_{i\in M})) = \prod_{j\in N} r^n_{\alpha(n)}$. So we see these maps are equal.

Lemma 2.86. *Let I be a finite set indexing a family $(R_i)_{i\in I}$ of $\mathbb{N}$-algebras R_i and $\pi_j : \prod_{i\in I} R_i \to R_j$ denote the projection onto the jth component.*
If $f : \prod_{i\in I} R_i \to A$ is an $\mathbb{N}$-algebra homomorphism, then (i) $A \cong \prod_{i\in I} A_i$ for some $\mathbb{N}$-algebras A_i and (ii) the morphism $\mathrm{id} \otimes \pi_j A \to A \otimes_R R_j$ induced by the tensor product commutes with the projection $\pi'_j : A \to A_i$ in the following way $\mathrm{id} \otimes \pi_j = \pi'_j \circ g$, where $g : A \to \prod_i A_i$ is the isomorphism from (i).

Proof. In fact (i) follows from Lemma 2.45. It remains to prove the morphism $\mathrm{id} \otimes \pi_j$ acts as claimed. This morphism is the pull back of π_j in the following diagram of R-algebras.

$$\begin{array}{ccc} A & \xrightarrow{\mathrm{id}\otimes\pi_j} & A \otimes_R R_j \\ \uparrow & & \uparrow \\ R & \xrightarrow[\pi_j]{} & R_j \end{array}$$

Given the presentation $R \cong R_i$ where $R_i = R/(e_i = 1)$ and $(e_i)_{i\in I}$ are orthogonal idempotents that sum to unity, π_j acts by mapping $e_j \mapsto 1$. In fact all of the other idempotents $e_i \neq e_j$ are forced to vanish under π_j. Moreover, the base change is $A \otimes_R R_j \cong A/(f(e_j) = 1)$. The commutativity of the pushout diagram implies that $\mathrm{id} \otimes \pi_j$ maps $f(e_j) \mapsto 1$ and sends the rest of the elements $f(e_i) \mapsto 0$ for $e_i \neq e_j$. Therefore the map is nothing but the projection onto the component $A_j = A/(f(e_j) = 1)$, as claimed.

■

Given a semiring R one can also construct the category of R-modules. This is an important tool in the study of the algebra, and geometry, of rings. Therefore we should consider its uses in our work on the geometry of semirings.

Definition 2.87 (Category of R-modules)**.** If R is a semiring, then let $\mathbf{Mod}_R$ denote the category whose class of objects is the class of R-modules and for each pair of objects M, M' the morphisms between them are the set of R-module homomorphisms $\mathrm{Hom}_{\mathbf{Mod}_R}(A, A')$.

Remark 2.88. Just as $\mathbf{Alg}_{\mathbb{N}}$ is equivalent to the category of semirings, so is $\mathbf{Mod}_{\mathbb{N}}$ equivalent to the category of (commutative) monoids. Therefore, when referring to the category of (commutative) monoids, we will use the notation $\mathbf{Mod}_{\mathbb{N}}$.

For each semiring, R, the category $\mathbf{Mod}_R$ is both complete and cocomplete. This follows in an analogous manner to the argument given above for the completeness and cocompleteness of $\mathbf{Alg}_R$.

Given a semiring R and an R-module, M, one obtains a functor $M \otimes_R - : \mathbf{Mod}_R \to \mathbf{Mod}_R$. This functor acts, on objects, by sending an R-module $N \mapsto M \otimes_R N$. This functor has a right adjoint, namely, $\mathrm{Hom}_{\mathbf{Mod}_R}(M, -)$. This functor takes $N \mapsto \mathrm{Hom}_{\mathbf{Mod}_R}(M, N)$ the R-module of R-module homomorphisms from M to N. However $M \otimes_R -$ does *not* (in general) have a left adjoint and as such fails to preserve all finite limits. This motivates the following definition.

Definition 2.89 (Flat R-module)**.** If R is a semiring and M an R-module, then we say M is a flat R-module if the functor $M \otimes_R - : \mathbf{Mod}_R \to \mathbf{Mod}_R$ preserves finite limits.

Remark 2.90 (Flatness is the Same as Classical Definition)**.** For each R-module M the functor $- \otimes_R M$ is right exact — preserves surjective morphisms. In ring theory one would say M is flat if it is also left exact, preserves injective morphisms. That is to say M is flat if $M \otimes_R -$ preserves exact sequences. This turns out to be the same as our definition above. Preservation of all finite limits is equivalent to the preservation of all finite products and equalizers. Tensor products always preserve finite products. Thus, in order for $M \otimes_R -$ to preserve all finite limits it is sufficient to check that it preserves all equalizers.

As mentioned earlier in the thesis ideals (kernels) play less of a role in the theory of semirings. It is for this reason that we do not define flatness directly in terms of preservation of short exact sequences as is done in module theory over rings.

Example 2.91. If M is a free R-module, then M is flat. In particular, R is flat over itself.

Example 2.92. If R is a field, then every R-module is flat. This follows from the fact that all modules over a field are a filtered colimit of their finitely generated submodules. Moreover, these submodules are finite dimensional vector spaces. Therefore each module over a field is a filtered colimit of (free and hence) flat modules, and hence is itself flat.

Definition 2.93 (Flat R-Algebra)**.** If R is a semiring and A is an R-algebra, then we say A is a flat R-algebra if the underlying R-module structure of A is a flat R-module.

Example 2.94 (Additive Localization is Not Flat)**.** In this example we will show $\mathbb{Z}$ is *not flat* over $\mathbb{N}$. Consider the diagram of $\mathbb{N}$-modules $0, + : \mathbb{N}^2 \to \mathbb{N}$, where 0 corresponds to the 0-map and + corresponds to the $\mathbb{N}$-module morphism which sums the entries of the pair $(a, b) \in \mathbb{N}^2$. Since $\mathbb{N}$ is zero sum free, the equalizer of this diagram is the trivial module $\mathbf{0}$.

If we tensor with $\mathbb{Z}$, then the equalizer is the sub-module $M = \{(a, -a)\} \subseteq \mathbb{Z}^2$. This is non-zero and hence not isomorphic to $\mathbf{0} \otimes_{\mathbb{N}} \mathbb{Z} \cong \mathbf{0}$. Therefore, tensoring with $\mathbb{Z}$ does not preserve *all* equalizers i.e. does not preserve all finite limits.

Remark 2.95. In commutative ring theory we often consider the process of (multiplicatively) inverting an element $x \in R$ thus forming the ring $R[\frac{1}{x}]$. We call this process (multiplicative) localization. This process yields a morphism $R \to R[\frac{1}{x}]$ which is *always* flat.

In commutative semiring theory we also have the option of *additively* inverting elements. Let us call the process of adding the additive inverse of an element *additive localization.* Example 2.94 proves additive localization is *not* in general flat. Borger proved the following more general statement.

Theorem 2.96 (Borger, 2010)**.** *Let A be a zero sum free $\mathbb{N}$-algebra, and let M be a flat A-algebra. Then M is zero sum free. In particular, the zero module* (0) *is the only flat A-module which is a group under addition, and the map $A \to \mathbb{Z} \otimes_{\mathbb{N}} A$ is flat if and only if $\mathbb{Z} \otimes_N A = 0$.*

Lemma 2.97. *If R is a zero sum free $\mathbb{N}$-algebra, A is a flat R-algebra, and $\varphi : R \to \mathbb{B}$ is the morphism which sends all non-zero elements $r \in R$ to $1 \in \mathbb{B}$, then the kernel of the induced map $\varphi_A : A \to A \otimes_R \mathbb{B}$, is trivial.*

Proof. Since R is zero sum free we can realise the kernel of φ as the pull-back of the following diagram of R-modules

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & \mathbb{B} \\ & & \uparrow \\ & & 0 \end{array}$$

Similarly the kernel of φ_A is the base change of this diagram along the structure morphism $R \to A$. We know the kernel of φ_A must also be trivial as the structure morphism is flat, and any finite limit must be preserved along such a flat base change. ∎

To finish this chapter we will prove that all projection morphisms $\pi_j : \prod_{i \in I} R_i \to R_j$ for I a finite set, are flat. That is, R_j is flat as an $\prod_{i \in I} R_i$-module under the morphism π_j. In order to get the idea of why this is true we consider the following extended example of the case I is a set with two elements.

Example 2.98. If $R = R_1 \times R_2$ and M is an R-module such that $M \cong M_1 \oplus M_2$, for R_i-modules M_i. We can define the congruence relation $\langle (e_2, 0) \rangle$ on R. This induces a congruence relation on the R-module M. What is the quotient of M by the induced congruence relation?

Since $e_2 = 0$ in the quotient, we know that the smallest congruence relation on M it generates is the congruence generated by *all* elements of the form $(e_2 m, 0)$. Since it has to be symmetric we need all elements of the form $(0, e_2 m)$. Closing under transitivity yields all elements of the form $(e_2 m, e_2 n)$. This yields the submonoid $(0 \oplus M_2) \oplus (0 \oplus M_2) \subseteq M^2$. It is the smallest congruence relation generated by all the elements $(e_2 m, 0)$. Similarly, if we consider the congruence relation generated by $e_1 = 0$, then we would get the submonoid $(M_1 \oplus 0) \oplus (M_1 \oplus 0) \subseteq M^2$.

Each element of $m \in M$ can be written uniquely as $m = xe_1 + ye_2$, for some $x, y \in M$. In the previous paragraph we gave an explicit account of each element in the congruence relation defined by $(e_2, 0)$. We saw that every element of M_2 is in the same congruence class and that every element of M_1 is in a distinct congruence class. Thus the congruence class of m is $[m] = [xe_1]$. Therefore we see $M/\langle e_2 = 0 \rangle = M_1$. Similarly, $M/\langle e_1 = 0 \rangle = M_2$.

If $R = \prod_{i \in I} R_i$, then for each $j \in I$ the factor R_j is isomorphic to the following quotient $R_j \cong R/\langle e_j = 1, (e_i = 0)_{i \neq j} \rangle$. It follows from this presentation for R_j and the work in the previous example that the base change of $M = \bigoplus_{i \in I} M_i$ along $\pi_j : R \to R_j$ is:

$$\begin{aligned} M \otimes_R R_j &= M \otimes_R R/\langle e_j = 1, (e_i = 0)_{i \neq j} \rangle \\ &= M/\langle e_j = 1, (e_i = 0)_{i \neq j} \rangle \\ &= M_j \end{aligned}$$

Lemma 2.99. *If $R \cong \prod_{i=1}^n R_i$ where R_i are $\mathbb{N}$-algebra, then for each j the morphism $\pi_j : R \to R_j$ is flat.*

Proof. It suffices to prove any equalizer of R-modules remains an equalizer diagram after extension of scalars along each π_j. If we are given the equalizer diagram

$$E \dashrightarrow M \underset{g}{\overset{f}{\rightrightarrows}} N.$$

Lemma 2.61 and Lemma 2.62 tell us the following is a commutative diagram of R-modules.

$$\begin{array}{ccccc}
E & \dashrightarrow & M & \underset{g}{\overset{f}{\rightrightarrows}} & N \\
\downarrow \wr & & \downarrow \wr & & \downarrow \wr \\
\bigoplus_{i\in I} E_i & \dashrightarrow & \bigoplus_{i\in I} M_i & \underset{\oplus g_i}{\overset{\oplus f_i}{\rightrightarrows}} & \bigoplus_{i\in I} N_i.
\end{array}$$

Furthermore we know the base change along the morphism $\pi_j : R \to R_j$ produces the following

$$\begin{array}{ccccc}
(\bigoplus E_i) \otimes_R R_j & \dashrightarrow & (\bigoplus M_i) \otimes_R R_j & \underset{\oplus g_i}{\overset{\oplus f_i}{\rightrightarrows}} & (\bigoplus N_i) \otimes_R R_j. \\
\downarrow \wr & & \downarrow \wr & & \downarrow \wr \\
E_j & \dashrightarrow & M_j & \underset{g_j}{\overset{f_j}{\rightrightarrows}} & N_j.
\end{array}$$

Moreover the arrow on the bottom diagram is an equalizer precisely because of the way f and g decompose to act on the components of M. Therefore extending scalars along $\pi_j : R \to R_j$ does preserve equalizers and hence each R_j is a flat R-module. ■

Lemma 2.100. *If $R \cong \prod_{i=1}^{n} R_i$ where R_i are $\mathbb{N}$-algebras, then the family $(\pi_i : R \to R_i)_{i=1}^{n}$ reflects isomorphisms.*

Proof. If $f : M \to N$ is an R-module homomorphism, then Lemma 2.62 shows f can be decomposed into $(f_i)_{i=1}^{n}$, where $f_i : M_i \to N_i$. If we assume each f_i is an isomorphism, then we know that f itself must be an isomorphism. Therefore this family reflects isomorphisms. ■

Chapter 3

Algebraic Geometry of Semirings

Just as algebraic geometry helped algebraists understand commutative unital ring theory, so it should help us understand commutative unital semirings. This chapter of the thesis develops the geometric picture of the arithmetic of semirings. We introduce affine $\mathbb{N}$-schemes and explore some of their first properties. In order to study the fundamental group of $\mathbb{N}$-schemes we are required to introduce a (Grothendieck) topology on (the category of) affine $\mathbb{N}$-schemes. In fact the notion of an $\mathbb{N}$-scheme is not novel to this thesis. Betrand Toën and Michel Vaquiè introduced the notion of an $\mathbb{N}$-scheme (in the sense we will discuss for the remainder of this thesis) in their paper *Au-dessous de* $\mathrm{Spec}(\mathbb{Z})$ [41]. For Toën and Vaquiè an $\mathbb{N}$-scheme was but one example of a more general class of objects, for us $\mathbb{N}$-schemes will be the explicit focus of our considerations.

3.1 Affine $\mathbb{N}$-schemes

In the modern algebraic geometry of schemes, there are two approaches to the foundation of the subject; building affine schemes out of the spectrum of prime ideals and equipping a structure sheaf, or foregoing the topological space and considering only the functor of points. Thus when considering the extension of this idea to the category $\mathbf{Alg}_{\mathbb{N}}$ one must make a choice, at least at first, about which direction to take when formulating the foundations of the subject.

It seems much of the work in the former approach is done by the structure sheaf of the locally-ringed space. One is then lead to think that there could be an approach which does not bother with the underlying topological space. Indeed, Grothendieck himself advocated for the latter approach to the foundations of algebraic geometry [21]. In this thesis we take the latter approach. We forgo the idea of an underlying topological space and *define* our “semiring-schemes” as certain *functors of points*.

Definition 3.1 (Affine $\mathbb{N}$-Scheme)**.** If $X : \mathbf{Alg}_{\mathbb{N}} \to \mathbf{Sets}$ is a representable functor from the category of $\mathbb{N}$-algebras to the category of sets, then we say X is an *affine* $\mathbb{N}$*-scheme.*

We will often drop the word affine and refer just to $\mathbb{N}$-schemes. In this thesis *all* $\mathbb{N}$-schemes are *affine* $\mathbb{N}$-schemes.

Definition 3.2 (Affine n-Space)**.** If R is an $\mathbb{N}$-algebra, then we denote $\mathbb{A}^n_R := \operatorname{Spec}(R[x_1, \dots, x_n])$ and refer to this $\mathbb{N}$-scheme as *affine n-space over R.* In the special cases (i) $n = 1$, we refer to $\mathbb{A}^1_R$ as the *affine line over R*, and (ii) $n = 2$, we refer to $\mathbb{A}^2_R$ as the *affine plane over R.*

Remark 3.3. Given an $\mathbb{N}$-algebra, C, we will often refer to the C-points of $\mathbb{A}^n_{\mathbb{N}}$. This is simplified greatly under the following identification:
$\mathbb{A}^n_{\mathbb{N}}(C) = C^n$. This identification is justified, as a homomorphism from $\mathbb{N}[x_1, \dots, x_n]$ to an $\mathbb{N}$-algebra C is determined by the choice of images of the x_i in C. Indeed, each choice of an image of x_i specifies a morphism uniquely. In this way we make the identification $\operatorname{Hom}_{\mathbf{Alg}_{\mathbb{N}}}(\mathbb{N}[x_1, \dots, x_n], C) = C^n$.

Example 3.4 (Empty $\mathbb{N}$-Scheme)**.** If C is an $\mathbb{N}$-algebra, then we can ask for the C-points of the $\mathbb{N}$-scheme $\operatorname{Spec}(0)$. If $C \neq 0$, then $\operatorname{Spec}(0)(C) = \emptyset$. If $C = 0$, then $\operatorname{Spec}(0)(C) = \{\star\}$. For this reason we make the following denotation $\emptyset := \operatorname{Spec}(0)$ and we call this the *empty* $\mathbb{N}$*-scheme.*

3.2 Morphisms of Affine $\mathbb{N}$-Schemes

Definition 3.5. If X, Y are affine $\mathbb{N}$-schemes, then we refer to natural transformations between them as *morphisms of* $\mathbb{N}$*-schemes*.

Remark 3.6. The Yoneda lemma implies the natural transformations between affine $\mathbb{N}$-schemes are in bijection with (determined uniquely by) morphisms between the objects ($\mathbb{N}$-algebras) representing the affine schemes.

Note: if $f : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ is a morphism of affine $\mathbb{N}$-schemes, then we may refer to the induced morphism between $\mathbb{N}$-algebras as $f^* : B \to A$. We denote the category of affine $\mathbb{N}$-schemes with $\mathbb{N}$-scheme morphisms (natural transformations of functors) between them as $\mathbf{Aff}_{\mathbb{N}}$.

Remark 3.7 (Geometry is Coarithmetic)**.** The Yoneda lemma implies the following equivalence of categories $\mathbf{Aff}_{\mathbb{N}} = \mathbf{Alg}_{\mathbb{N}}{}^{\mathrm{op}}$, thus realizing (affine) algebraic geometry as little more than an application of the category theoretic philosophy of dualizability. Just as every limit has a notion of *co*limit, every category has a *co*category. That is, every category has an opposite category. Algebraic geometry is thus the dual of algebra.

Remark 3.8 (Notation in $\mathbf{Aff}_{\mathbb{N}}$)**.** We denote the image of an $\mathbb{N}$-algebra, R, under the Yoneda embedding $Y : \mathbf{Alg}_{\mathbb{N}} \to \mathbf{Aff}_{\mathbb{N}}$ as $\mathrm{Spec}(R) := \mathrm{Hom}_{\mathbf{Alg}_{\mathbb{N}}}(R, -)$. If $\varphi : A \to B$ is a morphism of $\mathbb{N}$-algebras, then φ gives rise to a morphism $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$.

It will be useful for us to know whether an affine $\mathbb{N}$-scheme can be realised as an affine scheme over $\mathrm{Spec}(\mathbb{Z})$; that is, whether or not it is an affine scheme in the usual sense, or it is a genuine (not ring) semiring. In order to do this we can appeal to the following result of Borger-Grinberg [11]. Golan's Theorem 2.41 (as stated in this thesis) features in the proof given by Borger-Grinberg. In some sense the following theorem should be considered a geometric interpretation of Theorem 2.41.

Theorem 3.9 (Borger-Grinberg 2015). *If A is an $\mathbb{N}$-algebra and $X := \mathrm{Spec}(A)$, then $X \in \mathbf{Aff}_{\mathbb{Z}}$ if and only if $X(\mathbb{B}) = \emptyset$.*

Proof. See Borger-Grinberg 2015 [11]. ■

Given an affine $\mathbb{N}$-scheme $X : \mathbf{Alg}_{\mathbb{N}} \to \mathbf{Sets}$, is it possible to retrieve the underlying $\mathbb{N}$-algebra? Yes. It is done in the same manner as one would retrieve the coordinate ring from a (classical) algebraic variety, simply take the $\mathbb{N}$-scheme morphisms between X and the affine line, $\mathbb{A}^1_{\mathbb{N}}$.

Definition 3.10 (Function Algebra of an ℕ-Scheme). Let X be an object in $\mathbf{Aff}_{\mathbb{N}}$ and denote the set $\mathcal{O}(X) := \mathrm{Hom}_{\mathbf{Aff}_{\mathbb{N}}}(X, \mathbb{A}^1_{\mathbb{N}})$. This set can be equipped with an $\mathbb{N}$-algebra structure. In order to define the sum and product of these natural transformations of functors, we need only say how they act on algebras, C, in $\mathbf{Alg}_{\mathbb{N}}$. For this definition we identify $\mathbb{A}^1_{\mathbb{N}}(C) = C$. If $f, g \in \mathcal{O}(X)$, then

- $(f+g)(C) : X(C) \to C$, such that $\forall a \in X(C) :\ a \mapsto f(a) + g(a)$
- $(f \cdot g)(C) : X(C) \to C$, such that $\forall a \in X(C) :\ a \mapsto f(a) \cdot g(a)$

As additive and multiplicative identities we have the morphisms $0_{\mathcal{O}_X}$ and $1_{\mathcal{O}_X}$ defined on objects, C, of $\mathbf{Alg}_{\mathbb{N}}$ in the following manner:

- $0_{\mathcal{O}_X}(C) : X(C) \to C$, such that $\forall a \in X(C) :\ a \mapsto 0_C$
- $1_{\mathcal{O}_X}(C) : X(C) \to C$, such that $\forall a \in X(C) :\ a \mapsto 1_C$

We call this $\mathbb{N}$-algebra the *function algebra* of the affine $\mathbb{N}$-scheme X.

Lemma 3.11. *If R is an $\mathbb{N}$-algebra and $X = \mathrm{Spec}(R)$, then $\mathcal{O}(X) \cong R$.*

Proof. In this case we have $\mathcal{O}(X) := \mathrm{Hom}_{\mathbf{Aff}_{\mathbb{N}}}(\mathrm{Spec}(R), \mathbb{A}^1_{\mathbb{N}})$. Furthermore this is defined to be $\mathrm{Hom}_{\mathbf{Aff}_{\mathbb{N}}}(\mathrm{Spec}(R), \mathbb{A}^1_{\mathbb{N}}) := \mathrm{Hom}_{\mathbf{Alg}_{\mathbb{N}}}(\mathbb{N}[x], R)$. Given a natural transformation $\eta : \mathrm{Spec}(R) \to \mathbb{A}^1_{\mathbb{N}}$, we need to construct an element of R. We will do this by identifying $\mathrm{Hom}_{\mathbf{Alg}_{\mathbb{N}}}(\mathbb{N}[x], R) = R$ as in Remark 3.3. It is the Yoneda lemma that gives us this morphism: $F : \mathcal{O}(X) \to R$ which maps $\eta \mapsto \eta_R(\mathrm{id}_R)(x)$, where x is the indeterminate in the polynomial algebra $\mathbb{N}[x]$. The content of the Yoneda lemma is the fact that this map is bijective. We are left to show it is in fact a homomorphism of semirings.

If $\eta, \mu \in \mathcal{O}(X)$, then $(\eta + \mu)(R)(f) = \eta(R)(f) + \mu(R)(f)$, by definition. From which it follows that $(\eta+\mu)(R)(\mathrm{id}_R) = \eta(R)(\mathrm{id}_R) + \mu(R)(\mathrm{id}_R)$. Therefore $F(\eta) + F(\mu) = \eta(R)(\mathrm{id}_R)(x) + \mu(R)(\mathrm{id}_R)(x) = (\eta + \mu)(R)(\mathrm{id}_R)(x) = F(\eta + \mu)$. Similarly one sees that F respects the multiplication structures on both $\mathbb{N}$-algebras. Finally, because $0_{\mathcal{O}_X}$ maps everything to 0, it maps $x \in \mathbb{N}[x]$ to 0. Similarly for $1_{\mathcal{O}_X}$. Therefore, the bijection from the Yoneda embedding is an isomorphism of $\mathbb{N}$-algebras.

■

The assignment of $X \mapsto \mathcal{O}(X)$ forms a contravariant functor, which we denote $\mathcal{O}(-) : \mathbf{Aff}_{\mathbb{N}} \to \mathbf{Alg}_{\mathbb{N}}$. Moreover, $\mathrm{Spec}(-)$ and $\mathcal{O}(-)$ form *explicit* (anti-) equivalences of the categories $\mathbf{Alg}_{\mathbb{N}}$ and $\mathbf{Aff}_{\mathbb{N}}$.

Since the category $\mathbf{Alg}_{\mathbb{N}}$ is complete and cocomplete, so too is $\mathbf{Aff}_{\mathbb{N}}$. Although the following constructions are simply duals of those given in Chapter 2, we will spell them out and give them their own notation. Each of the following definitions are duals of those given Chapter 2; products of $\mathbb{N}$-algebras and coproducts of affine $\mathbb{N}$-schemes, and vice-versa. First we dualize the notion of an R-algebra.

Definition 3.12. If R is an $\mathbb{N}$-algebra, and (A, φ^*) is an R-algebra, then we say $\varphi : \mathrm{Spec}(A) \to \mathrm{Spec}(R)$ *is a scheme over* $\mathrm{Spec}(R)$.

The category of all $\mathbb{N}$-schemes over $\mathrm{Spec}(R)$, with morphisms which respect the morphisms to $\mathrm{Spec}(R)$, is denoted $\mathbf{Aff}_R$. Moreover, this category is (anti)-equivalent to the category $\mathbf{Alg}_R$. At times, we may refer to $\mathbb{N}$-schemes over $\mathrm{Spec}(R)$ as R-schemes. Note: this does not conflict with the original notation of $\mathbb{N}$-schemes, as every R-scheme is an $\mathbb{N}$-scheme in a unique way. Thus $\mathbb{N}$-schemes as defined in Definition 3.1 are *exactly the same as* "$\mathbb{N}$-schemes over $\mathrm{Spec}(\mathbb{N})$".

If R is an $\mathbb{N}$-algebra and A, B are R-algebras, then the coproduct of the corresponding R-schemes is given by $\mathrm{Spec}(A) \coprod \mathrm{Spec}(B) \cong \mathrm{Spec}(A \times B)$. Since

A and B are R-algebras, we can take the tensor product of A and B over R. In $\mathbf{Aff}_R$ this corresponds to $\mathrm{Spec}(A) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(B) \cong \mathrm{Spec}(A \otimes_R B)$, which we refer to as the (fibered) product of the affine $\mathbb{N}$-schemes over X.

Definition 3.13 (Base Change Along a Morphism)**.** Let $X = \mathrm{Spec}(R)$ be an affine $\mathbb{N}$-scheme. If $f : Y \to X$ is an R-scheme and $g : Z \to X$ is another R-scheme, then we can consider the following diagram:

$$\begin{array}{ccc} Y & \longleftarrow & Y \times_X Z \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g^*(f)} \\ X & \underset{g}{\longleftarrow} & Z \end{array}$$

We refer $g^*(f) : Y \times_X Z \to Z$ as the *base change of f along g.*

We may denote the corresponding scheme as $Y_Z := Y \times_X Z$. The phrases *pull back of f along g* and *pull back of Y along Z* will be used interchangeably with base change of f along g.

Remark 3.14. Let $X = \mathrm{Spec}(R)$ and $Z = \mathrm{Spec}(A)$. If $f : Z \to X$ is a scheme over X, then base change along Z defines a functor $- \times_X Z : \mathbf{Aff}_R \to \mathbf{Aff}_A$. It takes schemes over X to schemes over Z. This idea will be important for us later in the thesis. This is the geometric dual of the tensor functor $- \otimes_R A : \mathbf{Alg}_R \to \mathbf{Alg}_A$.

Definition 3.15 (Flat Map of Affine ℕ-schemes)**.** If $f : Y \to X$ is a morphism of affine $\mathbb{N}$-schemes and the induced algebra $f^* : \mathcal{O}(X) \to \mathcal{O}(Y)$ is flat, then we say $f : Y \to X$ is a *flat map of* $\mathbb{N}$*-schemes.*

Dual to the pullback (base change) construction is the *pushout* construction. This is often considered analogous to glueing $\mathbb{N}$-schemes together along a common (up to isomorphism) "sub-ℕ-scheme".

Definition 3.16 (Pushout of a Diagram)**.** If X, Y, and Z are objects in a category $\mathbf{C}$ with $f : X \to Y$ and $g : X \to Z$ between them, then the pushout (if it exists in $\mathbf{C}$) is an object $Y \sqcup_X Z$ with morphisms $i_Y : Y \to Y \sqcup_X Z$ and $i_Z : Z \to Y \sqcup_X Z$ which, together, satisfy the following universal property;

$$\begin{array}{ccc} Y & \longrightarrow & Y \sqcup_X Z \\ {\scriptstyle f}\uparrow & & \uparrow \\ X & \underset{g}{\longrightarrow} & Z \end{array}$$

For each object T in $\mathbf{C}$, if $f' : Y \to T$ and $g' : Z \to T$ are morphisms in $\mathbf{C}$, then there exists a unique morphism $i : Y \sqcup_X Z \to T$ such that $f' = i \circ i_Y$ and $g' = i \circ i_Z$.

For each semiring R the category $\mathbf{Aff}_R$ has pushouts given by the spectrum of the pull back of the corresponding diagram of R-algebras.

3.3 Finiteness Conditions on Affine $\mathbb{N}$-Schemes

If X is an affine $\mathbb{N}$-scheme, then it is isomorphic to a $\mathbb{N}$-scheme of the form $X = \mathrm{Spec}(R)$. Moreover, if $Y \cong \mathrm{Spec}(A)$ is an affine $\mathbb{N}$-scheme over X, then we can ask for a presentation of A as an R-algebra. Dual to the notion of finitely generated and finitely presented algebras are *morphisms of finite type* and *finitely presented morphisms*.

Definition 3.17 (Finiteness Conditions of Morphisms)**.** If $X = \mathrm{Spec}(R)$ is an affine $\mathbb{N}$-scheme and $f : \mathrm{Spec}(A) \to \mathrm{Spec}(R)$ is an affine $\mathbb{N}$-scheme over X, then we say f is of *finite type* if A is finitely generated as an R-algebra. If A is finitely presented as an R-algebra, then we say f is a *finitely presented morphism*.

Example 3.18. Let R be an $\mathbb{N}$-algebra and A be an R-algebra. Suppose further that A has the following presentation:

$$A = \frac{R[x_1, \ldots, x_n]}{\langle f_1 = g_1, \ldots, f_m = g_m \rangle}$$

where the f_i and g_i are polynomials in $R[x_1, \dots x_n]$. If $g : \mathrm{Spec}(C) \to \mathrm{Spec}(R)$ is an R-scheme, then the pull back of $\mathrm{Spec}(A)$ along $\mathrm{Spec}(C)$ is isomorphic to the following C-scheme

$$\mathrm{Spec}(A) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(C) \cong \mathrm{Spec}\left(\frac{C[x_1, \dots, x_n]}{\langle f_1 = g_1, \dots, f_m = g_m \rangle}\right)$$

where the fi and g_i are interpreted as polynomials with coefficients in C via the structure morphism of the R-algebra, C. Therefore we see, in this case, pulling back along an affine $\mathbb{N}$-scheme simply changes the coefficients of the presentation and hence preserves the property of being finitely presented.

As mentioned in Chapter 2 finite generation and finite presentation are relative properties. They are defined over some fixed base $\mathrm{Spec}(R)$.

3.4 Positive Cones of Affine Schemes

We will now consider an interesting family of examples of this glueing (pushout) construction. It will provide a geometric way of thinking about positivity and the passage from the natural numbers to the integers.

Example 3.19. In this example we consider the pushout of the following diagram of $\mathbb{N}$-schemes; which we interpret as gluing $\mathrm{Spec}(\mathbb{R}_+)$ to $\mathrm{Spec}(\mathbb{Z})$.

$$\begin{array}{ccc} \mathrm{Spec}(\mathbb{R}_+) & \longrightarrow & \mathrm{Spec}(\mathbb{R}_+) \sqcup_{\mathrm{Spec}(\mathbb{R})} \mathrm{Spec}(\mathbb{Z}) \\ \uparrow & & \uparrow \\ \mathrm{Spec}(\mathbb{R}) & \longrightarrow & \mathrm{Spec}(\mathbb{Z}) \end{array}$$

Dual to this diagram is the corresponding pullback of $\mathbb{N}$-algebras. Since all of the morphisms are injective morphisms of $\mathbb{N}$-algebras, the pullback is given by the intersection of $\mathbb{R}_+$ and $\mathbb{Z}$ in $\mathbb{R}$ i.e. $\mathbb{R}_+ \times_{\mathbb{R}} \mathbb{Z} \cong \mathbb{N}$ and as affine $\mathbb{N}$-schemes we see $\mathrm{Spec}(\mathbb{N}) \cong \mathrm{Spec}(\mathbb{R}_+) \coprod_{\mathrm{Spec}(\mathbb{R})} \mathrm{Spec}(\mathbb{Z})$.

Example 3.20 (Positive Cone over an Affine $\mathbb{N}$-scheme)**.** The glueing of $\mathrm{Spec}(\mathbb{R}_+)$ to $\mathrm{Spec}(\mathbb{Z})$ in Example 3.19 is not special to $\mathrm{Spec}(\mathbb{Z})$. As long as an affine $\mathbb{N}$-scheme X has a $\mathrm{Spec}(\mathbb{R})$ point, then we may perform this glueing construction. If X is an affine $\mathbb{N}$-scheme such that $p \in X(\mathbb{R})$, then let us denote $X_p^+ := \mathrm{Spec}(\mathbb{R}_+) \sqcup_{\mathrm{Spec}(\mathbb{R})} X$. Note this construction depends upon the choice of point in $X(\mathbb{R})$. In this notation we see that there is only one $p \in \mathrm{Spec}(\mathbb{Z})(\mathbb{R})$ and at this point $\mathrm{Spec}(\mathbb{N}) = \mathrm{Spec}(\mathbb{Z})_p^+$. We will refer to X_p^+ as the *positive cone of* X.

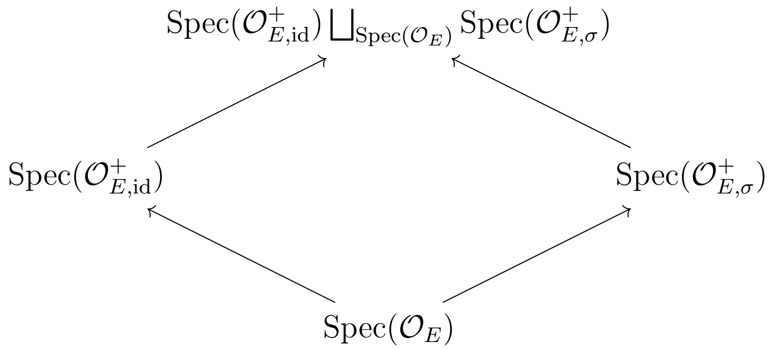
Remark 3.21 (Positive Cones are not in $\mathbf{Aff}_{\mathbb{Z}}$)**.** By construction the positive cone of an affine $\mathbb{N}$-scheme X (with an $\mathbb{R}$ point) necessarily has a $\mathbb{B}$-point coming from the attachment of $\mathbb{R}_+$. This implies X_p^+ is not the spectrum of a ring.

Example 3.22 (Positive Cones of Rings of Integers)**.** Further to constructing the positive cone over the spectrum of a number field with a real place, we can construct the positive cone over the corresponding ring of integers (or any order inside the number field). If $E : \mathbb{Q}$ is a real finite separable extension and $\mathcal{O}_E$ denotes the ring of integers in E, then there is (in general) more than one embedding $p : \mathcal{O}_E \to \mathbb{R}$, each of which will give a different sub-semiring $\mathcal{O}_{E,p}^+ \subseteq \mathcal{O}_E$.

In order to obtain a subsemiring which does not depend upon the embedding, we consider taking the intersection of all $\mathcal{O}_{E,p}^+$ inside $\mathcal{O}_E$. Geometrically this corresponds to glueing each of the $\mathbb{N}$-schemes $\mathrm{Spec}(\mathcal{O}_{E,p}^+)$ together along the structure morphisms to $\mathrm{Spec}(\mathcal{O}_E)$.

Example 3.23. If $E := \mathbb{Q}(\sqrt{2})$, then $\mathcal{O}_E = \mathbb{Z}[\sqrt{2}]$. Note $E/\mathbb{Q}$ is a Galois extension with Galois group $\mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, where $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. Therefore there are precisely two real embeddings, which we denote with the same symbols as the elements of the Galois group, namely id and σ. With these real embeddings we obtain the following $\mathbb{N}$-algebras: $\mathcal{O}_{E,\mathrm{id}}^+ := \{a+b\sqrt{2} \mid a+b\sqrt{2} \geq 0\}$ and $\mathcal{O}_{E,\sigma}^+ := \{a + b\sqrt{2} \mid a - b\sqrt{2} \geq 0\}$.

If we glue these along the morphisms $\mathrm{Spec}(\mathcal{O}_E) \to \mathrm{Spec}(\mathcal{O}_{E,\sigma}^+)$ and $\mathrm{Spec}(\mathcal{O}_E) \to \mathrm{Spec}(\mathcal{O}_{E,\sigma}^+)$ we obtain a new $\mathbb{N}$-scheme



In fact this $\mathbb{N}$-scheme is affine and represented by the $\mathbb{N}$-algebra:

$$\mathcal{O}_E^{++} := \{a + b\sqrt{2} \mid \forall \varphi \in \mathrm{Gal}(E/\mathbb{Q})\ \varphi(a + b\sqrt{2}) \geq 0\}$$

which we call the *totally positive* subsemiring of $\mathcal{O}_E$. Notice that this depends only on E and not any specific embedding $p : E \to \mathbb{R}$.

Definition 3.24 (Totally Positive Semiring)**.** If $E/\mathbb{Q}$ is a real finite extension and $S := \mathrm{Hom}_{\mathbf{Alg}_{\mathbb{Q}}}(E, \mathbb{R})$, then we define the *totally positive sub semifield of E* to be $E^{++} := \{x \in E \mid \forall \varphi \in S\ \varphi(x) \geq 0\}$ and the *totally positive sub semiring of $\mathcal{O}_E$* to be $\mathcal{O}_E^{++} := \{x \in \mathcal{O}_E \mid \forall \varphi \in S\ \varphi(x) \geq 0\}$.

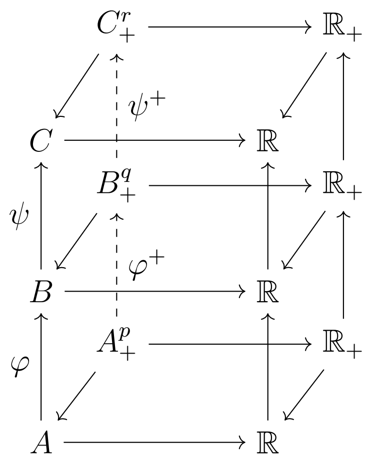
If we are given a morphism of affine $\mathbb{N}$-schemes $f : Y \to X$ such that X, Y have real points $p \in X(\mathbb{R})$ and $q \in Y(\mathbb{R})$, then do we always obtain a *natural* morphism $f_+ : Y_q^+ \to X_p^+$? In general, the answer is no. However, if the point q sits over the point p, then we do obtain a natural morphism $f_+ : Y_q^+ \to X_p^+$. This is the geometric interpretation of the following theorem. We use the following notation in the statement of the next theorem: For any semiring R, let $\mathbf{Alg}^R$ denote the category with (i) objects defined to be pairs (A, p), where A is an $\mathbb{N}$-algebra and $p : A \to R$ is an $\mathbb{N}$-algebra homomorphism, and (ii) a morphism between pairs $\varphi : (A, p) \to (B, q)$ is an $\mathbb{N}$-algebra homomorphism $\varphi : A \to B$ such that $q \circ \varphi = p$.

Theorem 3.25. *If we define the map $+ : \mathbf{Alg}^{\mathbb{R}} \to \mathbf{Alg}^{\mathbb{R}_+}$ which maps $(A, p) \mapsto A_+^p := A \times_{\mathbb{R}} \mathbb{R}_+$, then this can be extended to a functor by mapping $\varphi : (A, p) \to (B, q)$ to the morphism $+(\varphi) : A_+^p \to B_+^q$ defined by $(a, r) \mapsto (\varphi(a), r)$.*

Proof. We note the fibre product that defines A_+^p is given by the pull back of the following diagram

$$\begin{array}{ccc} \mathbb{R}_+ & \longleftarrow & A_+ \\ \downarrow & & \downarrow \\ \mathbb{R} & \longleftarrow & A \end{array}$$

In particular $A_+^p = \{(a, r) \in A \times \mathbb{R}_+ \mid p(a) \geq 0\}$. If we are given a morphism $\varphi : (A, p) \to (B, q)$ and a morphism $\psi : (B, q) \to (C, r)$, then we can fit this data into the diagram



In order for this assignment to define a functor we have to say what $\varphi_+ := +(\varphi)$ is for each morphism $\varphi : (A, p) \to (B, \psi)$ and check that the assignment behaves well with respect to composition. We define $+(\varphi) : A_+^p \to B_+^q$ to be the map which sends $(a, r) \mapsto (\varphi(a), r)$. In order to check this is well defined, we need only check $q(\varphi(a)) \geq 0$. However, we know $q \circ \varphi = p$ (as we are only considering morphisms of algebras whose $\mathbb{R}$-points commute) and therefore $q(\varphi(a)) = p(a) \geq 0$ as $(a, r) \in A_+^p$. It is routine to check $\psi_+ \circ \varphi_+ = (\psi \circ \varphi)_+$. ■

3.5 Topologies on $\mathbf{Aff}_{\mathbb{N}}$

This thesis aims to develop the theory of the étale fundamental group of an affine $\mathbb{N}$-scheme in a manner analogous to that of Grothendieck and Artin in SGA 4.

In order to do so we need an algebraic analog of a covering space of a topological space. That is to say, we need to define "locally trivial" morphisms of $\mathbb{N}$-schemes. In this section we make precise what we are to mean by "locally".

In the study of topological spaces one refers to a topology on the space in order to define things locally. Topologies on a space consist of an assignment of *subsets* of the space. However, we have given up any genuine notion of topological space in our study of affine $\mathbb{N}$-schemes. Our approach has been largely determined by the philosophy of category theory; objects are determined by the morphisms to them. This suggests that we should consider our "opens" — previously, inclusions $i : U \hookrightarrow X$ of subsets — simply as *any* morphism $f : Y \to X$ in $\mathbf{Aff}_{\mathbb{N}}$.

In the definition of a covering space and the notion of a sheaf, it is the notion of an *open covering* of the base space that is important. We can talk about a "cover" without actually specifying a topology. An open cover of a topological space is a jointly surjective family (indexed by a set I) of "open sets" $(U_i \hookrightarrow X)_{i \in I}$.

Definition 3.26 (Grothendieck Topology)**.** Let X be an object of a category $\mathcal{C}$. A covering family of X is a class of families of morphisms $\{(U_i \to X)_{i\in I}\}$, in the category $\mathcal{C}$, denoted $\mathrm{Cov}(X)$. A *Grothendieck topology* on a category $\mathcal{C}$ is an assignment of a collection[1] $\mathrm{Cov}(X)$ for each object X in $\mathcal{C}$ such that the following properties are satisfied:

(i) If $V \to X$ is an isomorphism, then $(V \to X) \in \mathrm{Cov}(X)$

(ii) If $(W_i \to X)_{i\in I}$ is in $\mathrm{Cov}(X)$ and $Y \to X$ is any arrow in $\mathbf{Aff}_R$, then $(W_i \times_X Y \to Y)_{i\in I}$ is in $\mathrm{Cov}(Y)$.

(iii) If $(W_i \to X)_{i\in I}$ is in $\mathrm{Cov}(X)$ and $(V_{ij} \to W_i)_{j\in J_i}$ is in $\mathrm{Cov}(W_i)$ for each $i \in I$, then the compositions $(V_{ij} \to W_i \to X)_{i\in I, j\in J_i}$ are in $\mathrm{Cov}(X)$.

When specifiying, or referring to, a Grothendieck topology on a category we will drop the word Grothendieck and simply refer to it is as a *topology* on the

[1]In general $\mathrm{Cov}(X)$ will *not* be a set. Indeed the collection of all one element covers is too big to be a set. However, we will not address these set theoretic issues in this thesis.

category.

Remark 3.27. In *Sketches of an Elephent* (Sketches) Peter Johnstone uses the term *coverage* for what we have defined to be a Grothendieck topology [25, 26]. Thus we depart from his notation in two ways. First we retain the use of the word topology from Grothendieck's original exposition of the idea, instead of using Johnstone's term coverage. Coverages as defined in Sketches are equivalent to the topologies we defined above. Secondly, we use Grothendieck's name in our definition, whereas Johnstone requires of a Grothendieck coverage that each family must in fact consist of *sieves*, special types of coverages. For the purposes of our work coverages are sufficient and provide good geometric intuition without clouding the idea with too much detail, so we will not make use sieves. Note: Lemma 2.1.3 on p. 538 of Sketches proves a functor $X : \mathcal{C}^{op} \to \mathbf{Set}$ is sheaf for a coverage if and only if it is a sheaf for the sieve generated by a coverage. This vindicates our choice as the main objects of study for arithmetic algebraic geometers are sheaves on a particular site [26].

Before we introduce the main topology on the category $\mathbf{Aff}_R$ that we will use for the remainder of the thesis, we need one more definition.

Definition 3.28 (Faithful Family)**.** If R is an $\mathbb{N}$-algebra, I a set, and $(f_i : R \to C_i)_{i \in I}$ is family of morphisms of R-algebras with the following property for each morphism $g : M \to N$ of R-modules:

(P) if for each $i \in I$ the morphism of C_i-modules $g \otimes \mathrm{id} : M \otimes_R C_i \to N \otimes_R C_i$ is an isomorphism, then the original morphism $g : M \to N$ must be an isomorphism,

We say the family of R-algebras $(f_i : R \to C_i)_{i \in I}$ is a *faithful family* of R-algebras. If $(f_i : U_i \to X)_{i \in I}$ is a family of morphisms of affine $\mathbb{N}$-schemes, then we say it is a faithful family if the corresponding family of $\mathcal{O}(X)$-algebras is a faithful family.

Lemma 3.29. *Let* $X = \mathrm{Spec}(R)$ *be an object in* $\mathbf{Aff}_{\mathbb{N}}$*. Let* $\mathrm{Cov}(X)$ *denote collection of all families of morphisms* $(\varphi_i : W_i \to X)_{i \in I}$ *in* $\mathbf{Aff}_{\mathbb{N}}$ *with the following properties*

(1) each $\varphi_i : W_i \to X$ is flat

(2) the collection of all φ_i is faithful.

In this case Cov(X) has the following properties

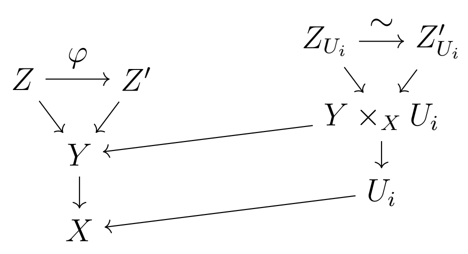
(i) If $V \to X$ is an isomorphism, then $(V \to X) \in \mathrm{Cov}(X)$

(ii) If $(W_i \to X)_{i\in I}$ is in $\mathrm{Cov}(X)$ and $Y \to X$ is any arrow in $\mathbf{Aff}_R$, then $(W_i \times_X Y \to Y)_{i\in I}$ is in $\mathrm{Cov}(Y)$.

(iii) If $(W_i \to X)_{i\in I}$ is in $\mathrm{Cov}(X)$ and $(V_{ij} \to W_i)_{j\in J_i}$ is in $\mathrm{Cov}(W_i)$ for each $i \in I$, then the compositions $(V_{ij} \to W_i \to X)_{i\in I, j\in J_i}$ are in $\mathrm{Cov}(X)$.

Proof. Isomorphisms $V \to X$ are flat and reflect isomorphisms. Recall that a morphism is flat if it preserves finite limits, so the composition of two flat morphisms is certainly flat. Moreover, the composition of two faithful families of morphisms is also faithful. The crux of this lemma is proving that the pull-back of a faithful family $(U_i \to X)_{i\in I}$ along a morphism $Y \to X$ remains faithful over Y.

If $(U_i \to X)_{i\in I}$ is a faithfully-flat family over X and $Y \to X$ is an affine $\mathbb{N}$-scheme over X, then we may obtain a family of flat (since flatness is preserved along base-changes) morphisms $(Y \times_X U_i \to Y)_{i\in I}$. Let $\varphi : Z \to Z'$ be a morphism of $\mathbb{N}$-schemes over Y such that for each $i \in I$ the base change of φ along $Y \times_X U_i \to Y$ is an isomorphism of affine $\mathbb{N}$-schemes. It suffices to show that φ is an isomorphism.



If we consider Z, Z' as schemes over X by post-composing with the structure morphism $Y \to X$, and further consider φ as a morphism of affine $\mathbb{N}$-schemes over X, then the diagram above makes it clear that each isomorphism $Z_{U_i} \to Z'_{U_i}$ arises from the pull-back along each morphism $U_i \to X$ as schemes over X. Therefore the fact that the family is faithfully flat over X implies $\varphi : Z \to Z'$ is an isomorphism of $\mathbb{N}$-schemes over X. However, this implies that it must in fact be an isomorphism of $\mathbb{N}$-schemes over Y. Therefore the family $(Y \times_X U_i \to Y)_{i\in I}$ does reflect isomorphisms. ■

Definition 3.30 (Flat Topology)**.** If R is an $\mathbb{N}$-algebra, $X := \mathrm{Spec}(R)$, and I is a set, then the collections $\mathrm{Cov}(X)$ of families $(\varphi_i : W_i \to X)_{i\in I}$ such that (i) each $\varphi_i : W_i \to X$ is flat, and (ii) the collection of all φ_i is faithful, forms a Grothendieck topology on $\mathbf{Aff}_R$. We refer to this as the *flat topology*.

In the context of schemes over the integers, there are two topologies which are closely related to the flat topology; both of which are obtained by imposing some finiteness hypotheses on the covers of the flat topology. These related topologies can also be defined in the broader context of affine $\mathbb{N}$-schemes. We give these definitions now.

Definition 3.31 (*fpqc* Topology)**.** If R is an $\mathbb{N}$-algebra, $X := \mathrm{Spec}(R)$, and I is a set, then the collections $\mathrm{Cov}(X)$ of families $(\varphi_i : W_i \to X)_{i\in I}$ such that (i) each $\varphi_i : W_i \to X$ is flat, and (ii) there exists a finite subset $J \subseteq I$ such that the family $(\varphi_j : W_j \to X)_{j\in J}$ faithful, forms a Grothendieck topology on $\mathbf{Aff}_R$. We refer to this as the *fpqc topology*.

Definition 3.31 of an *fpqc* topology and the proof that such covers form a topology can be found in [41].

Definition 3.32 (*fppf* Topology)**.** If R is an $\mathbb{N}$-algebra, $X := \mathrm{Spec}(R)$, and I is a set, then the collections $\mathrm{Cov}(X)$ of families $(\varphi_i : W_i \to X)_{i\in I}$ such that (i) each family is faithfully flat, and (ii) each morphism φ_i is finitely presented, forms a Grothendieck topology on $\mathbf{Aff}_R$. We refer to this as the *fppf topology*.

We already know that the flat topology is a topology. Therefore in order to prove that the *fppf* topology is a Grothendieck topology it suffices to show the axioms of a cover behave well with respect to finite presentations. Any isomorphism of $\mathbb{N}$-algebras is finitely presented. Moreover, the composition of finitely presented algebras is also finitely presented. Therefore it remains to determine whether the pull-back of finitely presented algebra is finitely presented; this follows from Example 2.74.

Remark 3.33. Notice that the *fpqc* and *fppf* topologies are both defined to be flat topologies with *extra* structure. Because of this, just as we would say in the study of topological spaces, we refer to the flat topology on $\mathbf{Aff}_{\mathbb{N}}$ as being a finer topology than both the *fpqc* and the *fppf* topology.

If X is an affine scheme over Spec($\mathbb{Z}$), then the quasi-compactness of X in the Zariski topology and the Zariski-open image of finitely presented morphisms allows us to conclude that any *fppf* cover is in fact an *fpqc* cover. However we don't (yet) have these results for schemes over Spec($\mathbb{N}$).

Question: If X is an affine $\mathbb{N}$-scheme and $(U_i \to X)_{i \in I}$ is an *fppf* cover of X, then is $(U_i \to X)_{i \in I}$ necessarily an *fpqc* cover of X? That is to say, is there a finite subset $J \subseteq I$ which is faithful over X?

In this thesis we will often refer to phenomena happening "locally" on an affine $\mathbb{N}$-scheme. This means the phenomena happens after pulling back along some covering family of the affine $\mathbb{N}$-scheme; either one of the three topologies defined above can be used to consider this type of "local" behaviour. Moreover, many properties of affine $\mathbb{N}$-schemes and the morphisms between them can be checked locally; that is to say, we can check whether the property, P, of an (or, a morphism of) affine $\mathbb{N}$-scheme(s) holds after pulling-back along a covering family from one of the previous topologies.

For us the key sense of locality for property checking will be "flat-local". We say a property P of a morphism $f : Y \to X$ is *flat-local* if it can be checked after pulling-back along a flat covering family of X. Notice that due to the relative fineness of the flat, fpqc, and fppf topologies a flat local property can be checked after passing to an fpqc or fppf covering family, as they are both flat covers. The next lemma proves that flatness is a flat, and hence fpqc and fppf, local property.

Lemma 3.34 (Flatness is Flat Local)**.** *If $f : Y \to X$ is a morphism of affine $\mathbb{N}$-schemes and $(U_i \to X)_{i\in I}$ is a flat cover of X, then Y is flat over X if and only if each $Y \times_X U_i \to U_i$ is a flat morphism of $\mathbb{N}$-schemes.*

Proof. Let $X = \operatorname{Spec}(R)$ and $Y = \operatorname{Spec}(A)$ and $f^* : R \to A$ be the structure morphism of the R-algebra A. Furthermore, we may assume $U_i = \operatorname{Spec}(C_i)$ for some flat R-algebras C_i. With this notation we may consider the following diagram in $\mathbf{Alg}_R$.

$$\begin{array}{ccc} A & \xrightarrow{\text{flat}} & A \otimes_R C_i \\ \uparrow & & \uparrow \text{flat} \\ R & \xrightarrow[\text{flat}]{} & C_i \end{array}$$

The morphisms $R \to C_i$ are flat by definition and the morphisms $A \to A \otimes_R C_i$ are flat since these are a base change of the flat maps $R \to C_i$. Finally, the morphisms $C_i \to A \otimes_R C_i$ are flat by assumption. Furthermore the families $(R \to C_i)_{i\in I}$ and $(A \to A \otimes_R C_i)_{i\in I}$ are faithful. The latter family is faithful as it is the base change of a faithful family.

Let us suppose the following is an equalizer diagram of R-modules

$$E \dashrightarrow M \rightrightarrows N \qquad (\star)$$

We want to show the diagram obtained by extending scalars along $f^* : R \to A$

$$\begin{array}{ccccc} E' & \dashrightarrow & A \otimes_R M & \rightrightarrows & A \otimes_R N \\ \uparrow g & & & & \\ A \otimes_R E & & & & \end{array} \qquad (\star\star)$$

is an equalizer diagram. We have denoted the equalizer of this diagram E'. In this case there is a morphism $g : A \otimes_R E \to E'$. We will prove that this morphism becomes an isomorphism after extending scalars further along the faithful flat cocover $(A \to A \otimes_R C_i)_{i \in I}$ and hence itself must be an isomorphism. Extending scalars this way around the commutative diagram is equivalent to extending scalars first along $R \to C_i$ and then $C_i \to A \otimes_R C_i$. Since each of these morphisms are flat, they preserve the equalizer of $(\star)$. Extending scalars in this way yields $(E \otimes_R A) \otimes_R C_i$ as the equalizer. Therefore $E' \otimes_A (A \otimes_R C_i) \cong (E \otimes_R A) \otimes_R C_i$, as these are the equalizers obtained by extending scalars around both branches of the commutative diagram. Finally we note $A \otimes_R E$ becomes, along the extension $A \to A \otimes_R C_i$, $(A \otimes_R E) \otimes_A (A \otimes_R C_i) \cong (E \otimes_R A) \otimes_R C_i$. This proves E' and $A \otimes_R E$ become isomorphic after extending scalars along a flat cocover and hence themselves must be isomorphic. Thus A does preserve the equalizer and hence is a flat R-algebra. ■

The following remark is an aside to the main goal of the present thesis, but an important note for further studies into the arithemtic algebraic geometry of $\mathbb{N}$-algebras. All new terms will not be defined here, but references will be given for the topics considered.

Remark 3.35. Given a category $\mathcal{C}$ and a Grothendieck topology τ, the pair $(\mathcal{C}, \tau)$ is referred to as a *site*. With this structure one can define the notion of a sheaf on a site as certain functors $F : \mathcal{C}^{op} \to \mathbf{set}$ with a glueing condition: sections can be glued together from local (in the sense of the topology τ) sections [26]. The category of all such sheaves on a site form a Grothendieck topos. Toposes are well behaved, **set**-like categories. One of the revelations following Grothendieck's work is that arithemtic algebraic geometry is best considered as happening inside the topos of sheaves on the étale (or fpqc, or fppf) site.

In *Au-dessous de Spec($\mathbb{Z}$)* Toën–Vaquiè explore these ideas in a broader setting which includes the category of $\mathbb{N}$-algebras. They define a Zariski topology and an fpqc topology on $\mathbf{Aff}_{\mathbb{N}}$ analogous to that for schemes over $\mathbb{Z}$. Furthermore they prove each affine $\mathbb{N}$-scheme is naturally a sheaf on the fpqc site $(\mathbf{Aff}_{\mathbb{N}}, \tau_{fpqc})$ and glue these together along the Zariski topology to form non-affine $\mathbb{N}$-schemes.[2] In this way we can see that the topos theoretic formalism of the study of schemes over $\mathbb{Z}$ carries over naturally to the broader context of schemes over $\mathbb{N}$.

Before we move on to the study of finite étale morphisms of $\mathbb{N}$-schemes we will present some results about the local nature of particular morphisms of $\mathbb{N}$-schemes.

Definition 3.36 (Idempotent Immersion)**.** If N is a finite set, $R = \prod_{i\in N} R_i$ is a product of finitely many $\mathbb{N}$-algebras R_i, and $\pi_j : \prod_{i\in N} R_i \to R_j$ is the projection onto R_j, then we refer to the corresponding map of $\mathbb{N}$-schemes $\pi_j^* : \mathrm{Spec}(R_j) \to \coprod_{i\in N} \mathrm{Spec}(R_i)$ as *idempotent immersions.*

Remark 3.37. Lemma 2.99 tells us that idempotent immersions are flat morphisms of $\mathbb{N}$-schemes.

In the next lemma we will prove that the property of being an idempotent immersion can be checked *flat locally*[3].

Lemma 3.38. *If R, A are $\mathbb{N}$-algebras and $f : R \to A$ is an $\mathbb{N}$-algebra homomorphism, then $f : R \to A$ is an idempotent immersion if and only if there exists a flat cocover $(i_\alpha : R \to C_\alpha)_{\alpha\in S}$ such that $f|_\alpha : C_\alpha \to A \otimes_R C_\alpha$ is an idempotent immersion.*

Proof. Let $A_\alpha := A \otimes_R C_\alpha$, $C_{\alpha\beta} := C_\alpha \otimes_R C_\beta$, and $A_{\alpha\beta} := A \otimes_R C_{\alpha\beta}$. Let us first suppose that each $f_\alpha : C_\alpha \to A_\alpha$ is an idempotent immersion. This means (i) for each $\alpha \in S$ there exists a finite set T_α and a family of idempotents $(e_i^\alpha)_{i\in T_\alpha} \subseteq C_\alpha$

[2]It is known that the flat topology, as defined in this thesis, is not subcanonical. That is, there are representable functors which are *not sheaves* for the flat topology. Angelo Vistoli provides an example in Remark 2.56 of [2]. So it is necessary to use the *fpqc* topology over the *flat* topology when developing sheaf theory and the theory of non-affine $\mathbb{N}$-schemes.

[3]If a property is flat local, then it is also fpqc and fppf local. We will leave this assumed from now on. When ever a property is shown to be flat local, we know that it is both fpqc and fppf local.

such that they are mutually orthogonal and sum to unity in C_α, which implies (ii) for each $\alpha \in S$ we have $C_\alpha = \prod_{i \in T_\alpha} B_i^\alpha$, where $B_i^\alpha = C_\alpha/(e_i^\alpha = 1)$, and finally (iii) there exists $j \in T_\alpha$ such that $A_\alpha = B_j^\alpha$ and $f_\alpha = \pi_j^\alpha : \prod_{i \in T_\alpha} B_i^\alpha \to B_j^\alpha$.

For each $\alpha \in S$ we have distinguished idempotents $e_\alpha := e_j^\alpha$ and $\overline{e_\alpha} := \sum_{i \neq j} e_i^\alpha$ in C_α, which generate distinguished sub-C_α-modules $I_\alpha := \langle e_\alpha \rangle$ and $\overline{I_\alpha} := \langle \overline{e_\alpha} \rangle$. In fact these distinguished sub-modules arise as the equalizers of the following diagrams

$$I_\alpha \longrightarrow C_\alpha \underset{0}{\overset{\theta}{\rightrightarrows}} C_\alpha.$$

where the morphism of C_α-modules θ is defined by $\theta(e_\alpha) = 0$ and sending the other generating idempotents to themselves. Furthermore, $\overline{I_\alpha}$ is the equalizer of the following diagram

$$\overline{I_\alpha} \longrightarrow C_\alpha \underset{0}{\overset{\pi_j^\alpha}{\rightrightarrows}} B_j^\alpha.$$

In order to prove f is an idempotent immersion we need to prove there is an idempotent in R onto which f projects. To do this we will prove that the constructions of e_α and $\overline{e_\alpha}$ descend to R. In order to do this it suffices to show these constructions are stable under refinement — since they generate *sub-C_α-modules* of C_α (for each α) we do not need to check any cocycle condition in order to glue the modules together.

Over each C_α we have I_α and $\overline{I_\alpha}$ and over $C_{\alpha\beta}$ we have (by the analogous construction) $I_{\alpha\beta}$ and $\overline{I_{\alpha\beta}}$. In fact the diagrams that each $I_{\alpha\beta}$ are equalizers of are precisely the base-change along $C_\alpha \to C_{\alpha\beta}$ of the diagram for which I_α is the equalizer of. Since the morphism $C_\alpha \to C_{\alpha\beta}$ is flat - by definition of the C_α forming a cocover of R - we know that the equalizers must be preserved under base change. Therefore for each $\alpha, \beta \in S$ we know $I_{\alpha\beta} = I_\alpha \otimes_{C_\alpha} C_{\alpha\beta}$, hence $\langle e_{\alpha\beta} \rangle = \langle e_\alpha \rangle \subseteq C_{\alpha\beta}$. Similarly, $\alpha, \beta \in S$ we know $\overline{I_{\alpha\beta}} = \overline{I_\alpha} \otimes_{C_\alpha} C_{\alpha\beta}$, hence $\langle \overline{e_{\alpha\beta}} \rangle = \langle \overline{e_\alpha} \rangle \subseteq C_{\alpha\beta}$. Lemma 2.53 proves $e_{\alpha\beta} = e_\alpha$ and $\overline{e_{\alpha\beta}} = \overline{e_\alpha}$.

Since the idempotents agree at $C_{\alpha\beta}$ they descend to elements $e, \overline{e} \in R$ - It remains to show they are idempotents and $f : R \to A$ acts by projection onto e. In order to do this we note that the morphism $g : R \to R/\langle e = 1\rangle \times R/\langle \overline{e} = 1\rangle$ becomes an isomorphism over the faithful cover of C_α, thus it must itself be an isomorphism. Hence $e, \overline{e}$ are orthogonal idempotents which sum to unity. In order to show f is an idempotent immersion, we need only note the commutativity of the following diagram, as this proves that f must project onto e.

$$\begin{array}{ccc} A & \longrightarrow & \prod_{\alpha \in S} A_\alpha \\ f \uparrow & & \uparrow \prod f_\alpha \\ R & \longrightarrow & \prod_{\alpha \in S} C_\alpha \end{array}$$

Therefore we may conclude that if f is flat locally an idempotent immersion, then it is globally. ■

Chapter 4

Finite Étale Morphisms

This chapter presents one of the main theorems of this thesis: that of the existence and structure of the étale fundamental group of an affine $\mathbb{N}$-scheme. In the introduction of this thesis we discussed the ingredients required to formulate this theory; a notion of covering space and a notion of point. Initially this chapter provides these ideas to build the necessary framework. In the final sections of the current chapter we define the étale fundamental group of an affine $\mathbb{N}$-scheme, discuss a number of its properties, and consider some examples coming from algebraic number theory.

4.1 Finite Étale Morphisms

In this section we formalise the phrase *"category of covering spaces"* of an affine $\mathbb{N}$-scheme. Recall that a morphism $f : Y \to X$ of topological spaces is a *finite* covering space if there exists an open cover $(U_i \to X)_{i \in I}$ and *finite* sets N_i for each $i \in I$ such that $Y \times_X U_i \cong \coprod_{N_i} U_i$. Indeed the diagram below

$$\begin{array}{ccc} Y & \longleftarrow & Y \times_X U_i \cong \coprod_{N_i} U_i \\ \downarrow & & \downarrow \\ X & \longleftarrow & U_i \end{array}$$

represents this behaviour when interpreted in the category of topological spaces. All that is required of us is to interpret this diagram in the category of affine $\mathbb{N}$-schemes. In particular, we need to specify what it is that we mean by an "open cover" of an affine $\mathbb{N}$-scheme X. In the literature on schemes over $\mathrm{Spec}(\mathbb{Z})$ the property of a morphism $f : Y \to X$ being étale is typically defined point-wise on the base scheme X: either using differentiation [38] or ramification of fibers [40]. These point-wise definitions are not immediately available to us from our functorial point of view of affine schemes over the natural numbers. However, one can show this point-wise definition of finite étale for schemes over $\mathrm{Spec}(\mathbb{Z})$ is equivalent to saying there is an *fppf* cover $(U_i \to X)_{i \in I}$ of X such that for each $i \in I$ we have an isomorphism $Y \times_X U_i \cong \coprod_{N_i} U_i$ (Proposition 5.2.9 p 155. [40]). That is to say, we can interpret the diagram on the previous page by saying an "open cover of X" is an *fppf* coverage of X.

Definition 4.1 (Finite Étale Morphism)**.** Let $f : Y \to X$ be a morphism of affine $\mathbb{N}$-schemes. If there exists an element $(U_i \to X)_{i \in I}$ of the fppf topology on $\mathbf{Aff}_{\mathbb{N}}$ and finite sets N_i for each $i \in I$ such that $Y \times_X U_i \cong \coprod_{N_i} U_i$ as U_i-schemes, then we say that $f : Y \to X$ is a finite étale morphism.

If $f : Y \to X$ is a finite étale morphism, then we may say Y is finite étale over X. Or we may refer to the morphism f itself and say f is a finite étale morphism of affine $\mathbb{N}$-schemes. If $Y \to X$ is of the form $Y \cong \coprod_N X$ for some set N, then we say that Y is totally split over X. Thus, further to our choice of notations, we may refer to finite étale morphisms as *fppf locally totally split morphisms*, or *locally totally split morphisms*. We denote the subcategory of affine $\mathbb{N}$-schemes over X with objects as finite étale morphisms over X and all morphisms between them by $\mathbf{F\acute{E}t}_X$.

Example 4.2. If X, Y are affine schemes over $\mathrm{Spec}(\mathbb{Z})$, then a morphism of affine $\mathbb{N}$-schemes $f : Y \to X$ is finite étale in the sense of Definition 4.1 if and only if it is finite étale in the sense of Grothendieck's original definition. This is shown in, for example, Proposition 5.2.9 in [40].

Example 4.3. If $X = \mathrm{Spec}(R)$ is an affine $\mathbb{N}$-scheme and $Y \cong \coprod_N X$, for some finite set N, then the morphism $f : Y \to X$ induced by the R-algebra morphism $f^* : R \to R^N$ is a finite étale morphism. Indeed this morphism is already totally split, so it remains totally split along the fppf cover $(\mathrm{id} : X \to X)$.

Section 4.2 contains many more examples of finite étale morphisms. For now we will make a few remarks about the choice of definition and then move onto study properties of finite étale morphisms.

Remark 4.4. It was mentioned in the introduction that Connes and Borger had discussed how the theory of the fundamental group could extend to semirings and semiring-schemes. Connes suggested (following Bhargav Bhatt and Peter Scholze in [7]) that a map $f : Y \to X$ should be considered étale if both f and $\Delta : Y \to Y \times_X Y$ are flat and Y is finitely presented over X. Indeed, a finite étale map (as defined in this thesis) has this property, as flatness is flat local, and this property is satisfied locally. It would be interesting to know if these are equivalent definitions.

Remark 4.5. Chapter 3 introduced three different topologies on $\mathbf{Aff}_{\mathbb{N}}$. Our definition of finite étale follows the definition over $\mathrm{Spec}(\mathbb{Z})$. However, it begs the question: does the choice of topology matter? We could instead interpret "open cover" of X to mean the existence of a *flat* coverage of X or an *fpqc* coverage of X. For each (including the choice we made) of these choices we obtain, a priori, three different notions of finite étale and hence three different categories. Which would result in three different étale fundamental groups. Thus we ask: are the étale fundamental groups obtained from the three topologies on $\mathbf{Aff}_{\mathbb{N}}$ isomorphic?

Given the natural duality between $\mathbf{Aff}_{\mathbb{N}}$ and $\mathbf{Alg}_{\mathbb{N}}$ it makes sense to consider what this picture looks like in the opposite category. The definition that follows is the dual of the previous definition; but the difference in notation and terminology is helpful to have at hand.

Definition 4.6 (Finite Étale Algebra)**.** Let $f : R \to A$ be an R-algebra. If there exists an element $(U_i \to \mathrm{Spec}(R))_{i \in I}$ of the fppf topology on $\mathbf{Aff}_{\mathbb{N}}$ and finite sets N_i for each $i \in I$ such that $A \otimes_R \mathcal{O}(U_i) \cong \prod_{N_i} \mathcal{O}(U_i)$, then we say that $f^* : R \to A$ is a finite étale R-algebra.

Similarly, we may refer to finite étale R-algebras $f : R \to A$ by saying A is finite étale over R. Or, that the structure morphism f is a finite étale morphism. Of course, because these definitions are duals of one another, we know if $f : Y \to X$ is a finite étale morphism of $\mathbb{N}$-schemes, then the induced morphism $f^* : \mathcal{O}(X) \to \mathcal{O}(Y)$ is a finite étale $\mathcal{O}(X)$-algebra. Moreover, if $f^* : R \to A$ is a finite étale R-algebra, then the induced morphism $f : \mathrm{Spec}(A) \to \mathrm{Spec}(R)$ is a finite étale morphism $\mathbb{N}$-schemes. If R is an $\mathbb{N}$-algebra, then we denote the category of finite étale algebras $\mathbf{F\acute{E}t}_R := {\mathbf{F\acute{E}t}_{\mathrm{Spec}(R)}}^{\mathrm{op}}$. Note: one refers to the subscript to know whether or not the morphisms are to be interpreted as algebra morphisms or R-scheme morphisms.

Remark 4.7 (Finite Étale Implies Flat)**.** Since finite étale morphisms are fppf locally totally split, they are flat locally totally split, and hence flat locally free. In particular, they are flat locally *flat*, since all free modules are flat. Moreover, Lemma 3.34 tells us flatness is a flat local property, therefore all finite étale algebras are flat algebras.

In order to understand the structure of $\mathbf{F\acute{E}t}_X$ for some affine $\mathbb{N}$-scheme X we first will give a number of lemmata related to finite étale morphisms and the morphisms between them.

Lemma 4.8 (Finite Étale Stable Under Base Change)**.** *If $f : Y \to X$ is a finite étale cover of X and $g : Z \to X$ is any morphism of affine $\mathbb{N}$-schemes, then $Y \times_X Z \to Z$ is a finite étale cover.*

Proof. If $(h_i : U_i \to X)_{i \in I}$ is the fppf cover of X over which Y splits, then the pull back of this cover $(h_i \times \mathrm{id}_Z : U_i \times_X Z \to Z)_{i \in I}$ is an fppf cover of Z over which $Y \times_X Z$ will split. ■

Lemma 4.9 (Finite Étale Flat Local on Base)**.** *If $f : Y \to X$ is a morphism of $\mathbb{N}$-schemes and $(g_i : U_i \to X)_{i\in I}$ is a fppf cover of X, then $f : Y \to X$ is a finite étale morphism if and only if, for each $i \in I$, the morphisms $f_i : Y \times_X U_i \to U_i$ are finite étale.*

Proof. If each f_i is a finite étale morphism, then there exist fppf covers $(h_{ij} : W_{ij} \to U_i)_{j\in J_i}$ over which each of the morphisms f_i become totally split. Since compositions of fppf covers form fppf covers, this means there exists a fppf cover of X over which the morphism $f : Y \to X$ becomes totally split i.e. Y is finite étale over X. ■

Lemma 4.10. *If X is an affine $\mathbb{N}$-scheme and $\varphi : \coprod_N X \to \coprod_M X$ is a morphism of $\mathbb{N}$-schemes induced by a set map $\tilde{\varphi} : N \to M$, then φ is a finite étale morphism.*

Proof. Since the property of being finite étale is flat local on the target we may pull back along the fppf cover $(m : X \to \coprod_M X)_{m\in M}$ in order to check whether or not the morphism is finite étale; Lemma 2.99 and Lemma 2.100 tell us this a fppf cover. Indeed, over the m^{th} component we simply get $\tilde{\varphi}^{-1}(m)$ copies of X over X. Thus each of the pull backs are finite étale. Therefore the original morphism must be finite étale. ■

In a similar vein we see piecing together finite étale morphisms gives us finite étale morphisms.

Lemma 4.11. *If $(f_i : Y_i \to X_i)_{i\in I}$ is a family of finite étale covers index by a finite set I, then the induced morphism $\coprod_{i\in I} f_i : \coprod_{i\in I} Y_i \to \coprod_{i\in I} X_i$ is a finite étale morphism.*

Proof. Lemma 4.9 says it suffices to consider the question over some fppf cover of X. Indeed the family $(g_j : X_j \to \coprod_{i\in I} X_i)_{j\in I}$ is (by Lemma 2.99 and Lemma 2.100) an fppf cover of $\coprod_{i\in I} X_i$. Pulling $\coprod_{i\in I} f_i$ back along each of these yields a finite étale morphism. Therefore the original morphism must in fact be finite étale. ■

Remark 4.12. The converse of this lemma is true. If $\coprod_{i \in I} f_i : \coprod_{i\in I} Y_i \to \coprod_{i \in I} X_i$ is finite étale, then each f_j for $j \in I$ is finite étale. Each f_j can be realized as a pull-back of the coproduct of the f_j i.e. a pull-back of a finite étale map. Therefore each f_j is finite étale.

If R_1, R_2 are $\mathbb{N}$-algebras, then there are two projection morphisms $\pi_1^* : R_1 \times R_2 \to R_1$ and $\pi_2^* : R_1 \times R_2 \to R_2$. In the opposite category these morphisms $\pi_i : \mathrm{Spec}(R_i) \to \mathrm{Spec}(R_1) \coprod \mathrm{Spec}(R_2)$ will be referred to as *idempotent immersions*. In general one can consider any finite family R_i indexed by a finite set I and the corresponding projection morphisms, these too are said to be idempotent immersions. Next we will prove idempotent immersions are finite étale.

Lemma 4.13. *If $(X_i)_{i\in I}$ are a collection affine $\mathbb{N}$-schemes, then the morphisms $X_j \to \coprod_{i\in I} X_i$ are finite étale.*

Proof. Observe $(f_j : X_j \to \coprod_{i\in I} X_i)_{j\in I}$ is an fppf cover of $\coprod_{i\in I} X_i$. Since the property of being finite étale is flat local on the target, it suffices to check whether a given f_j is finite étale after pulling back along each f_ℓ.

Since each X_i is affine we know there are $\mathbb{N}$-algebras R_i such that $X \cong \mathrm{Spec}(R_i)$. In the opposite category $f_j^* : \prod_I R_i \to R_j$ is the projection onto the jth component. In order to determine whether or not f_j^* is finite étale after pull back to f_ℓ we need to determine the pushout of the following diagram

$$\begin{array}{ccc} R_j & \dashrightarrow & R_j \otimes_{\prod_I R_i} R_\ell \\ \uparrow & & \uparrow \\ \prod_I R_i & \longrightarrow & R_\ell \end{array}$$

In the case that $j \neq \ell$ one need only consider the image of the the element $e_j = (0, 0, \ldots 1, \ldots, 0)$ which is 1 in the *jth* column and 0 else where, under both paths to the pushout. On the other hand, via R_j the element e_j is sent to the multiplicative identity; the other way it is sent to the additive identity. Therefore, in the pushout, $1 = 0$. In the case $j \neq \ell$ the pushout is 0. In particular, it is finite étale over R_ℓ.

It remains to consider the case $j = \ell$. By the universal property of pushouts, a morphism $R_j \otimes_{\prod_I R_i} R_j \to C$, to some (test object) algebra C, is equivalent to giving two morphisms $\alpha : R_j \to C$ and $\beta : R_j \to C$ such that $\alpha \circ f_j^* = \beta \circ f_j^*$. Claim: α must be equal to β. For, if $\alpha \neq \beta$, then there exists an $x \in R_j$ such that $\alpha(x) \neq \beta(x)$. This implies, by the surjectivity of f_j^*, that there exists a $y \in \prod_I R_i$ such that $x = f_j^*(y)$ and hence $\alpha(f_j^*(y)) \neq \beta(f_j^*(y))$, contradicting the choice of α, β. That is to say, a morphism out of the tensor product, is the same thing as a morphism out of R_j. Yoneda lemma allows us to conclude $R_j \cong R_j \otimes_{\prod_I R_i} R_j$. In particular, the pullback of f_j^* is finite étale. Finally, we may conclude that the original, idempotent immersion, is finite étale. ■

Next we prove that compositions of finite étale morphisms are themselves finite étale. First we deal with a special case, and then prove that the special case implies the general.

Lemma 4.14. *If $f : Y \to \coprod_I X$ is finite étale and $\triangle : \coprod_I X \to X$ is the morphism of $\mathbb{N}$-schemes induced by the diagonal, then the composition $Y \to X$ is finite étale.*

Proof. Since f is finite étale, there exists an fppf covering family of $\coprod_I X$ given by $(g_k : U_k \to \coprod_I X)_{k \in K}$ over which Y splits, $Y \times_{\coprod_I X} U_k \cong \coprod_{N_k} U_k$. Note the family $(\triangle \circ g_k : U_k \to X)_{k \in K}$ is an fppf family — this follows from the fact that it is a composition of fppf covering families. In fact, Y splits over this family

$$\begin{aligned} Y \times_X U_k &\cong \left(Y \times_{\coprod_I X} \coprod_I X \right) \times_X U_k \\ &\cong Y \times_{\coprod_I X} \left(\coprod_I X \times_X U_k \right) \\ &\cong Y \times_{\coprod_I X} \left(\coprod_I U_k \right) \\ &\cong \coprod_I \left(\coprod_{N_k} U_k \right). \end{aligned}$$

Therefore we may conclude the composition of the given morphisms $\triangle \circ f : Y \to X$ is finite étale. ■

Lemma 4.15. *If $f : Z \to Y$ and $g : Y \to X$ are finite étale morphisms of affine $\mathbb{N}$-schemes, then the composition $g \circ f : Z \to X$ is a finite étale morphism.*

Proof. We are free to choose an fppf cover $(h_i : U_i \to X)$ over which Y splits into $Y \times_X U_i \cong \coprod_{N_i} U_i$, for some finite sets N_i. If we pull f and g back along each h_i we see $f \times \mathrm{id} : Z \times_X U_i \to \coprod_{N_i} U_i$ is a finite étale morphism. Since finite étale is a flat local property, it suffices to show that the composition of the pull backs of f, g are finite étale. However this is precisely what the previous lemma tells us. Therefore, the composition $g \circ f$ of finite étale morphisms is finite étale. ■

Later we will need to deal with quotients by group actions and other details of that require a finer understanding of the local nature of a morphism between two finite étale covers of a fixed affine $\mathbb{N}$-scheme. The main problem we have to overcome is the following: despite the fact that for each morphism of finite étale $\mathbb{N}$-schemes over X, $f : Y \to Z$, there exists a cover of X which trivializes Y and Z, we don't yet know that f itself can be trivialized. That is to say, we don't know that f pulls back to a morphism between the sheets of the finite étale covers. This behaviour is illustrated in the following example:

Example 4.16 (Can't Assume Morphism is Trivial)**.** Let $X := \mathrm{Spec}(R) \coprod \mathrm{Spec}(R)$ be an affine $\mathbb{N}$-scheme. We can define the following morphism $f : X \to \coprod_2 X$

which is *not* induced by a morphism from the singleton to the set with 2 elements. This map is defined (in the algebra category) by mapping $((1,1),(0,0)) \mapsto (1,0)$ and $((0,0),(1,1)) \mapsto (0,1)$. This induces a morphism $f : X \to \coprod_2 X$ which is not defined by a morphism from the one sheet of X into some sheet of $\coprod_2 X$.

In order to get around this problem Grothendieck proves that one can always refine the cover further in order to obtain a cover over which this cannot happen [22]. However, his proof makes explicit use of the Zariski topology, which we have not encorporated into our development of affine $\mathbb{N}$-schemes. We will now prove that we *can* always make such a refinement..

Let $X = \mathrm{Spec}(R)$ be an affine $\mathbb{N}$-scheme, with $f : Y \to Z$ a morphism of finite étale covers of X, and $(g_i : U_i \to X)_{i \in I}$ be an fppf cover of X over which $Y \times_X U_i \cong \coprod_{N_i} U_i$ and $Z \times_X U_i \cong \coprod_{M_i} U_i$, for some *finite sets* N_i and M_i. We will now prove that we can refine this cover so that f acts by mapping sheets to sheets; that is to say f is locally induced by a map of sets.

For now let us fix an $i \in I$ and denote $U := U_i$, $N := N_i$, and $M := M_i$. So we have a morphism $f := f_i : \coprod_N U \to \coprod_M U$. This induces a morphism $f' : U \to \coprod_{M^N} U$. Furthermore, since U is an affine $\mathbb{N}$-scheme over X we know $U \cong \mathrm{Spec}(A)$ for some finitely presented R-algebra A, therefore f' is induced by an R-algebra morphism $f'^* : A^{M^N} \to A$. Lemma 2.45 provides us with a decomposition of A into a product of quotient semirings $A \cong \prod_{M^N} A_\alpha$, where we have forgone the subset defined in Lemma 2.45 and left in the possibility that some of the quotients give the 0 semiring. In particular, $A_\alpha := A/\langle f'^*(e_\alpha) = 1 \rangle$. Notice the A_α are finite quotients of a finitely presented R-algebra, and hence are themselves finitely presented over R. Let us denote $E_\alpha := \mathrm{Spec}(A_\alpha)$. These E_α should be thought of as the locus over which f is given by the set map $\alpha : N \to M$.

Since $U \cong \coprod_\alpha E_\alpha$, we may conclude on the basis of Lemma 2.99 that each morphism $E_\alpha \to U$ is flat. Lemma 2.100 also tells us that the family is faithful. Therefore we know that $(E_\alpha \to U)_\alpha$ is an fppf cover. Moreover, we know that compositions of covers are covers, therefore the collection of all E^i_α form an fppf cover of X.

In order to prove this cover splits f in the desired way, let us fix a morphism $\beta : \coprod_N U \to \coprod_M U$ which *is induced by a morphism* $\tilde{\beta} : N \to M$. As before this yields a morphism $\beta^* : A^{M^N} \to A$. Furthermore, following Remark 2.85 we know that this morphism is equivalent to the projection onto the β^{th} component which we denote π_β - we are making explicit use of the identification $M^N = \mathrm{Hom}_{\mathbf{sets}}(N, M)$. In order to prove the given cover does split f, it suffices to show f and β become equal after pull-back to E_β. In other words, it suffices to prove the identity $i : \coprod_N E_\beta \to \coprod_N E_\beta$ is the equalizer of the diagram

$$\coprod_N E_\beta \xrightarrow{\ \mathrm{id}\ } \coprod_N E_\beta \underset{\beta}{\overset{f}{\rightrightarrows}} \coprod_M E_\beta. \qquad (\dagger)$$

In order to prove that this diagram is an equalizer diagram we will consider the corresponding coequalizer diagram in the opposite category (the category of algebras) which can be seen to be equivalent by (the Yoneda lemma and) the following bijections of sets

$$\begin{aligned}\mathrm{Hom}_{\mathbf{Alg_A}}\left(\prod_M A, \prod_N A\right) &= \prod_N \mathrm{Hom}_{\mathbf{Alg_A}}\left(\prod_M A, A\right)\\ &= \mathrm{Hom}_{\mathbf{Alg_A}}\left(\left(\prod_M A\right)^{\otimes N}, A\right)\\ &= \mathrm{Hom}_{\mathbf{Alg_A}}\left(\prod_{M^N} A, A\right).\end{aligned}$$

These equivalences lead to us to prove that the following is a coequalizer diagram in the category of A-algebras.

$$A_\beta \longleftarrow A \underset{\pi_\beta}{\overset{f^*}{\leftleftarrows}} \prod_{M^N} A.$$

Let us denote the coequalizer $\mathcal{O}(E)$. We will now prove that it is isomorphic to A_β. By definition the coequalizer is given by the following quotient

$$\mathcal{O}(E) := \frac{A}{(f^*(e_\alpha) = \pi_\beta(e_\alpha))_{\alpha \in M^N}}.$$

Lemma 2.45 gives us a decomposition for the semiring A which we substitute to obtain

$$\frac{\prod_{\gamma\in M^N}\frac{A}{(f^*(e_\gamma)=1)}}{(f^*(e_\alpha)=\pi_\beta(e_\alpha))_{\alpha\in M^N}}.$$

Which further simplifies as

$$\prod_{\gamma\in M^N}\frac{A}{(f^*(e_\alpha)=\pi_\beta(e_\alpha),f^*(e_\gamma)=1)_{\alpha\in M^N}}.$$

It remains to determine each factor of this product of semirings.

1. First let us consider the case $\gamma=\beta$, then the equivalence relation is given by the following family of relations:

   $$(f^*(e_\alpha)=\pi_\beta(e_\alpha),f^*(e_\beta)=1)_{\alpha\in M^N}.$$

   If $\alpha=\beta$, then $f^*(e_\beta)=1$ determines the relation $f^*(e_\beta)=\pi_\beta(e_\alpha)$. Similarly, in the case $\alpha\neq\beta$, the relation $f^*(e_\beta)=1$ determines the other relationships. Therefore each $f^*(e_\alpha)=\pi_\beta(e_\alpha)$ is redundant. Therefore we see the factor corresponding to $\gamma=\beta$ is precisely the semiring A_β derived above.

2. Now let us find the quotient in the case $\gamma\neq\beta$. This case is also split into the subcases $\alpha=\beta$ and $\alpha\neq\beta$. In the case $\alpha=\beta$ the family of equivalence relations is :

   $$(f^*(e_\alpha)=\pi_\beta(e_\alpha),f^*(e_\gamma)=1)_{\alpha\in M^N}.$$

   Since $\pi_\beta(\alpha)=1$ in this case, we see $f^*(e_\alpha)=1$ and $f^*(e_\gamma)=1$. As $\alpha=\beta\neq\gamma_0$, we conclude $1=f^*(e_\alpha)f^*(e_\gamma)=f^*(e_\alpha e_\gamma)=0$ is an element of the family of equivalence relations. Thus the corresponding quotient is isomorphic to the 0 semiring. Finally, if $\alpha\neq\beta$, then the family of relations defining this quotient is:

   $$(f^*(e_\alpha)=0,f^*(e_\gamma)=1)_{\alpha\in M^N}$$

   As α ranges over all elements of M^N, we know the relation $1=0$ is in the family and hence the quotient is the 0 semiring.

Therefore we may conclude $\mathcal{O}(E) = A_\beta$. Furthermore, the correpsonding diagram of $\mathbb{N}$-schemes

$$\coprod_N E_\beta \overset{i}{\dashrightarrow} \coprod_N U \underset{\beta}{\overset{f}{\rightrightarrows}} \coprod_M U. \qquad (\star)$$

is an equalizer diagram. In order to conclude that the original diagram (†) is an equalizer it suffices to notice that it is the pullback of $(\star)$ along the *flat* morphism $E_\beta \to U$. Since the morphism is flat, the equalizer is preserved. Therefore the equalizer of (†) is $\coprod_N E_\beta$, as required. We now know that for a given morphism $f : Y \to Z$ of finite étale schemes over X, there exists an fppf cover of X over which Y and Z split and f is given by mapping sheets over Y to sheets over Z i.e. the morphism f is determined by a set map. We state this formally in the next lemma.

Lemma 4.17. *If $i_Y : Y \to X$ and $i_Z : Z \to X$ are finite étale morphisms and $f : Y \to Z$ is a morphism of schemes over X, then there exists an fppf cover $(h_i : U_i \to X)_{i\in I}$ and families of finite sets $(N_i)_{i\in I}$ and $(M_i)_{i\in I}$ such that for each $j \in I$, (i) $Y \times_X U_j \cong \coprod_{N_j} U_j$ (ii) $Z \times_X U_j \cong \coprod_{M_j} U_j$ and (iii) $f \times \mathrm{id}$ is equivalent to a morphism induced by a set map $\alpha_j : N_j \to M_j$.*

Proof. This follows from the case where $S = \{\star\}$ is the one-point set given above, since the property of a morphism being totally split is stable under pullback. Thus we can always take a common refinement to obtain the desired cover. ■

This fact about the local nature of morphisms between finite étale covers allows us to prove the following lemmata which are indispensable in the proof of the main theorem of this chapter; the first of which states that morphisms between finite étale covers X are themselves finite étale.

Lemma 4.18. *If $f : Y \to X$ and $g : Z \to X$ are finite étale covers of X and $h : Y \to Z$ is a morphism of affine $\mathbb{N}$-schemes such that $f = gh$, then h is a finite étale morphism i.e. Y is a finite étale cover of Z.*

Proof. Since h is flat locally given by a set map, Lemma 4.10 allows us to conclude h is flat locally finite étale. Moreover, this means h is finite étale. ■

Before we move onto some examples of finite étale morphisms over specific affine $\mathbb{N}$-schemes we record an observation about the nature of the fppf cover that splits an affine $\mathbb{N}$-scheme over (the spectrum of) a *ring*.

Remark 4.19. If $X = \mathrm{Spec}(R)$ is the spectrum of a ring R (with no idempotents i.e. X is connected) and $f : Y \to X$ is finite étale over X, then we may simplify the fppf cover $(U_i \to X)_{i \in I}$ which splits affine scheme Y. Since each of the morphisms $U_i \to X$ are finitely presented, their image in X (which we denote as U_i) is a Zariski open subscheme of X. Furthermore, as X is an affine scheme we know that each open cover has some finite subcover. Therefore only finitely many of the fppf covers of X are required to form an fppf coverage of X. Thus we may restrict to considering $(U_j \to X)_{j \in J}$ for some *finite subset* $J \subseteq I$. In fact we can take the coproduct of these finitely many U_j to form a single finitely presented affine scheme $U = \coprod_J U_j$ and the associated fppf coverage $(U \to X)$. This one morphism is flat, finitely presented, and splits the morphism $f : Y \to X$. In light of this we see that in the case $f : Y \to X$ is a morphism over a connected affine scheme X, it suffices to consider fppf coverages consisting of one morphism when determining whether or not f is finite étale.

4.2 Examples

Example 4.20 (Finite Étale Morphisms over $\mathrm{Spec}(\mathbb{B})$)**.** Suppose the morphism of affine $\mathbb{N}$-schemes $f : X \to \mathrm{Spec}(\mathbb{B})$ is a non-empty finite étale $\mathbb{B}$-scheme — if X is empty, then X is isomorphic to the empty coproduct of copies of $\mathrm{Spec}(\mathbb{B})$. This means there exists an fppf cover $(g_i : U_i \to \mathrm{Spec}(\mathbb{B}))_{i \in I}$ over which f becomes trivial. Since the g_i form a faithful cover, there exists $j \in I$ such that $U_j \neq \emptyset$. Golan's theorem (Theorem 2.41) tells us there exists a morphism $x : \mathrm{Spec}(\mathbb{B}) \to$

U_j — there can be no such map from the spectrum of a field, as this would correspond to a semiring map from $\mathbb{B}$ to a field.

$$\begin{array}{ccccc} X & \longleftarrow & \coprod_{N_j} U_j & \longleftarrow & \coprod_{N_j} \mathrm{Spec}(\mathbb{B}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{B}) & \longleftarrow & U_j & \longleftarrow & \mathrm{Spec}(\mathbb{B}) \end{array}$$

The composition along the bottom (the identity) is an isomorphism, therefore the top row must also be an isomorphism. It follows that $X \cong \coprod_{N_j} \mathrm{Spec}(\mathbb{B})$; that is to say, X is totally split. Therefore all affine $\mathbb{N}$-schemes that are finite étale over $\mathrm{Spec}(\mathbb{B})$ are totally split.

Example 4.21 (Finite Étale over a Field)**.** Let F be a field and the morphism $f : \mathrm{Spec}(A) \to \mathrm{Spec}(F)$ be a finite étale morphism, then $A \cong \prod_{i=1}^{n} E_i$, where E_i/F are finite separable extensions of F.

In order to prove this we first we note that a finite étale morphism must in fact be finitely generated. That is to say, A is a finite dimensional vector space over F — Remark 4.19 allows us to assume the cover which splits $\mathrm{Spec}(A)$ consists of *one* morphism $g : U \to \mathrm{Spec}(F)$, where $U = \mathrm{Spec}(C)$ for a non-zero finitely presented F-algebra. Moreover, this implies $A \otimes_F C \cong C^N$ is a finite dimensional F-algebra and hence $A \hookrightarrow C^N$ must also be a finite dimensional F-algebra. All finite dimensional algebras over a field F are of the following form

$$A \cong \prod_{i=1}^{n} A/\mathfrak{m}_i^N.$$

Considering the following diagram shows all finite étale algebras must embed inside a reduced ring and hence themselves must be reduced

$$\begin{array}{ccccc} A & \longrightarrow & \prod_N C & \longrightarrow & \prod_N C_{\mathrm{red}} \\ \uparrow & & \uparrow & & \uparrow \\ F & \longrightarrow & C & \longrightarrow & C_{\mathrm{red}} \end{array}$$

Since F is a field and $C_{\text{red}} \neq 0$, we know $F \to C_{\text{red}}$ is injective. Moreover, A is flat over F, therefore the morphism $A \to \prod_N C_{\text{red}}$ is also injective. Therefore A is a reduced ring. This implies $N = 1$ and hence $A \cong \prod_{i=1}^n A/\mathfrak{m}_i$. It remains to prove each of these field extensions of F are in fact separable. It suffices to show each $A/\mathfrak{m}_j \otimes_F \overline{F} \cong \prod_{I_j} \overline{F}$, for some finite set I_j, where $\overline{F}$ is an algebraic closure of F. In order to prove this is the case, consider the following diagram of F-algebras

$$\begin{array}{ccccc}
A/\mathfrak{m}_j & \longrightarrow & C/\mathfrak{m}_j & \longrightarrow & \prod_{I_j} \overline{F} \\
\uparrow & & \uparrow & & \uparrow \\
\prod_N A/\mathfrak{m}_i & \longrightarrow & \prod_N C/\mathfrak{m}_i & \longrightarrow & \prod_M \overline{F} \\
\uparrow & & \uparrow & & \uparrow \\
F & \longrightarrow & C & \longrightarrow & \overline{F}
\end{array}$$

Since C is finitely presented over F, Hilbert's Nullstellansatz guarantees us a morphism $C \to \overline{F}$, which is the map given in the preceding diagram. Each square in the above diagram is a pushout (tensor product), in particular, we obtain the required isomorphism $A/\mathfrak{m}_j \otimes_F \overline{F} \cong \prod_{I_j} \overline{F}$ for some finite set I_j. In fact, I_j is isomorphic to the number of roots in $\overline{F}$ of the polynomials that generate the maximal ideal $\mathfrak{m}_j$ in C. Therefore each $A/\mathfrak{m}_i$ is a finite separable extension of F and A is a product of finite separable extensions of F.

Remark 4.22. The fact that A is finitely presented over F in Example 4.21 is true more broadly. If A is finite étale over a ring R, then A must in fact be finitely presented over R. This can be shown by proving finite presentation descends along faithfully flat covers.

Example 4.23 (Finite Étale over the Integers)**.** If $\mathrm{Spec}(A) \to \mathrm{Spec}(\mathbb{Z})$ is a finite étale morphism, then $A \cong \prod_N \mathbb{Z}$, for some finite set N. In particular, if A is connected, then $A \cong \mathbb{Z}$.

Indeed, if we assume $A \neq \mathbb{Z}$ is a non-zero connected finite étale algebra over $\mathbb{Z}$, then it is a finitely generated $\mathbb{Z}$-module. Moreover, by extending scalars along the flat injective morphism $\mathbb{Z} \to \mathbb{Q}$, we see (following Example 4.21) A is a subring of $A_{\mathbb{Q}} = \prod_N E_i$, for number fields E_i. As A is connected and non-zero, we know $|N| = 1$. Therefore, all connected non-zero finite étale algebras A over $\mathbb{Z}$ are orders in a number field i.e. there exists an order $\mathcal{O}$ in a number field E such that $A \cong \mathcal{O} \subseteq E$. Minkowski's theorem implies there that there exists at least one prime $p \in \mathbb{Z}$ which ramifies in $\mathcal{O}$. This implies $A \otimes_{\mathbb{Z}} \mathbb{F}_p$ contains nilpotent elements, and hence is *not* finite étale over $\mathbb{F}_p$. This contradicts the fact that being finite étale is preserved along any base change. Therefore, A can't be finite étale over $\mathbb{Z}$. So the only connected finite étale algebras over $\mathbb{Z}$ is $\mathbb{Z}$ itself.

4.3 Geometric Points

With the notion of (covering space) finite étale morphism in hand, all that remains to develop the étale fundamental group of an $\mathbb{N}$-scheme is to define what we mean by a "point". Euclid was clear when he said a point is *that which has no part*; interpreting this in the language of $\mathbb{N}$-schemes a point should be something that has no non-trivial quotients/congruence relations. Theorem 2.41 tells us that the only affine $\mathbb{N}$-schemes with this property are $\mathrm{Spec}(k)$, for k a field, and $\mathrm{Spec}(\mathbb{B})$.

However, this is not enough for our purposes. Points should be *simply connected*, that is to say, they should not have any non-trivial covering spaces. Example 4.21 shows us that fields *can* have non-trivial finite étale covers, thus we should not expect all fields to act exactly like points. For this reason we restrict the denotation of point to *separably closed fields*. Notice, Example 4.20 shows the Boolean semiring *does* not have any non-trivial finite étale covers, so this too should be considered a point. We make this discussion precise with the following definition.

Definition 4.24 (Geometric Morphism)**.** Let X be an affine $\mathbb{N}$-scheme. If p is a simple affine $\mathbb{N}$-scheme with no non-trivial finite étale morphisms and $i : p \to X$ is a morphism of affine $\mathbb{N}$-schemes, then we say (p, i) is a *geometric morphism* *into X.*

We will often refer to a geometric morphism $i : p \to X$ simply as a (geometric) point of X, or we may refer to the $\mathbb{N}$-scheme p itself as a (geometric) point of X. However the following remark suggests we should be cautious when using this abbreviation.

Example 4.25. The affine $\mathbb{N}$-scheme $\mathrm{Spec}(\mathbb{B})$ has a unique (up-to unique isomorphism) point determined by the identity morphism of $\mathbb{N}$-algebras $i : \mathbb{B} \to \mathbb{B}$.

Remark 4.26. Recall that we have defined an $\mathbb{N}$-scheme to be a functor from the category of $\mathbb{N}$-algebras to the category of sets. Given an $\mathbb{N}$-scheme X and an $\mathbb{N}$-algebra C, we refer to the elements of the set $X(C)$ as C-points. This sense of point is a broader sense to that of a point in the sense of Definition 4.24. Geometric morphisms are elements of $X(\mathbb{B})$ and $X(\overline{k})$, for $\overline{k}$ a separably closed field.

We have singled out these special geometric morphisms as they are morphisms that provide the notion of point required in the development of the étale fundamental group. Indeed, the following theorem proves such a morphism provides us with the functor to **sets** (finite sets) that we require. More generally, it proves the category of finite étale morphisms over any affine $\mathbb{N}$-scheme, X, is equivalent to the category of sets if all finite étale morphisms over X are trivial.

Lemma 4.27. *If $X = \mathrm{Spec}(R)$ is a non-empty affine $\mathbb{N}$-scheme such that all finite étale covers of X are of the form $f : \coprod_N X \to X$, for some finite set N, then the functors*

$$\mathrm{Hom}_{\mathbf{FEt}_X{}^{\mathrm{op}}}(-, R) : \mathbf{FEt}_X{}^{\mathrm{op}} \to \mathbf{sets}$$
$$\mathrm{Hom}_{\mathbf{sets}}(-, R) : \mathbf{sets} \to \mathbf{FEt}_X{}^{\mathrm{op}}$$

together with the natural isomorphisms

$$\eta : \mathrm{id}_{\mathbf{FEt}_X{}^{\mathrm{op}}} \to \mathrm{Hom}_{\mathbf{sets}}(-, R) \circ \mathrm{Hom}_{\mathbf{FEt}_X}(-, R)$$
$$\varepsilon : \mathrm{id}_{\mathbf{sets}} \to \mathrm{Hom}_{\mathbf{FEt}_X}(-, R) \circ \mathrm{Hom}_{\mathbf{sets}}(-, R)$$

which are defined, on objects, by the following collection of morphisms

$$\eta(A) : A \to \mathrm{Hom}_{\mathbf{sets}}(\mathrm{Hom}_{\mathbf{FEt}_X{}^{\mathrm{op}}}(A, R), R)$$
$$\text{where, } a \mapsto \mathrm{ev}_a := [f \mapsto f(a)]$$
$$\varepsilon(S) : S \to \mathrm{Hom}_{\mathbf{FEt}_X{}^{\mathrm{op}}}(\mathrm{Hom}_{\mathbf{sets}}(S, R), R)$$
$$\text{where, } s \mapsto \mathrm{ev}_s := [f \mapsto f(s)]$$

constitute an (anti) equivalence of the category of finite étale covers of X ($\mathbf{FEt}_X$) and finite sets ($\mathbf{sets}$).

Proof. We need the non-empty assumption: for if $X = \emptyset$, then all finite étale $\mathbb{N}$-schemes over X are isomorphic to X. Therefore the category of them is not **sets**. Most of the detail is given in the definition of the functors and natural transformations, unpacking these yields the result. We need the totally split assumption in order for the functors to be essentially surjective. However, we will prove the not immediately obvious fact that for a finite set $S \in \mathbf{set}$, the set of homomorphisms $\mathrm{Hom}_{\mathbf{set}}(S, R)$ is a finite étale R-algebra. In fact, we will prove $\mathrm{Hom}_{\mathbf{set}}(S, R) \cong R^S$.

First we note the algebra structure on these functions is given by componentwise addition and multiplication. In particular this means the additive identity is given by $\forall s \in S : s \mapsto 0_R$ while the multiplicative identity is given by $\forall s \in S : s \mapsto 1_R$. In order to prove that this algebra is isomorphic to R^S it suffices to find a family of orthogonal idempotents that generate the R-algebra of functions and sum to the identity function. The elements of this family of functions are defined in the following manner:

$$\forall s \in S \ e_s : S \to R \ \ e_s(t) := \delta_{st}.$$

If $s \neq t$, then $e_s e_t(x) = \delta_{sx}\delta_{tx} = 0$, since one of the delta functions must vanish. Hence $s \neq t$ implies $e_s e_t = 0$ i.e. these functions are orthogonal. Each of these functions are idempotents, for $e_s^2(x) = e_s(x)e_s(x) = \delta_{sx}\delta_{sx} = \delta_{sx} = e_s(x)$. If we sum the entire family $(e_s)_{s\in S}$ we obtain the identity function $s \mapsto 1_R$ - If $x \in S$, then $(\sum_S e_s)(x) = \sum_S(e_s(x)) = \delta_{xx} = 1_R$. All of the terms in the sum vanish, except for the term $e_x(x)$ corresponding to $s = x$ in the summation index. Finally, the family can be seen to generate *as an R-algebra* the entire set of functions. For each function $f : S \to R$, we know $f(t) = r_{f,t} \in R$. With this notation at hand we know $f = \sum_{s\in S} r_{f,s}e_s$, and hence that the family $(e_s)_{s\in S}$ is generates (over R) the algebra $\mathrm{Hom}_{\mathbf{sets}}(S, R)$. ■

Since geometric points satisfy the hypotheses of Lemma 4.27 we know that pulling back to the category of finite étale morphisms over a fixed affine ℕ-scheme X along such a point does provide us with a functor to **sets**.

Remark 4.28 (ℕ-Schemes and the 𝔹 point)**.** We return now to Theorem 2.41 to discuss its geometric interpretation. When we broaden our category to include the (opposite of the) category semirings we might ask: how many (geometric) points does this extension add? Theorem 2.41 and Example 4.20 tell us that we only add *one* point by doing this extension. Namely, the (spectrum of the) Boolean semiring 𝔹. This suggests the Boolean semiring 𝔹 is central to the geometry of semirings, in particular, the natural numbers; it marks the difference between those affine ℕ-schemes over $\mathrm{Spec}(\mathbb{Z})$ and those which do not live over $\mathrm{Spec}(\mathbb{Z})$.

4.4 Étale Fundamental Group of an ℕ-Scheme

We are now in a position to define the étale fundamental group of a connected affine ℕ-scheme at a point (geometric morphism) $x : p \to X$.

Definition 4.29 (Étale Fundamental Group of an ℕ-Scheme)**.**

If X is an affine ℕ-scheme and $x : p \to X$ is a geometric morphism to X, then we obtain the following functor: $- \times_X p : \mathbf{FEt}_X \to \mathbf{sets}$. We define the *étale fundamental group of X at the point p* to be $\pi_1^{\text{Ét}}(X,p) := \mathrm{Aut}(- \times_X p)$ the automorphism group of the functor $- \times_X p : \mathbf{FEt}_X \to \mathbf{sets}$.

Naturally we hope that this group has many of the properties of the Galois group of a field — pro-finiteness — or the fundamental group of a topological space — independence (up to canonical isomorphism) of choice of geometric (base) point. In the next section we will see that the group $\pi_1^{\text{Ét}}(X,p)$ behaves as hoped and that these properties are a result of the fact that the pair $(\mathbf{FEt}_X, - \times_X p)$, forms a *Galois category.*

4.5 Galois Category

Grothendieck's work on the étale fundamental group culminated in a category theoretic characterisation of the phenomena of covering spaces and their relation to the fundamental group. This statement of the axioms of a Galois category is translated, from the original French, directly from Grothendieck's exposition [22].

Definition 4.30 (Galois Category)**.** Let $\mathbf{C}$ be a category and $\mathscr{F}$ a covariant functor from $\mathbf{C}$ to **sets**, the category of finite sets. We say that $\mathbf{C}$ is a *Galois category* with *fundamental functor* $\mathscr{F}$ if the following six conditions are satisfied:

(G1) There is a terminal object in $\mathbf{C}$, and the fibred product of any two objects over a third one exists in $\mathbf{C}$.

(G2) Finite sums exist in $\mathbf{C}$, in particular an initial object, and for any object in $\mathbf{C}$ the quotient by a finite group of automorphisms exists.

(G3) Any morphism u in $\mathbf{C}$ can be written as $u = u'u''$, where u'' is an epimorphism and u' a monomorphism. Moreover, any monomorphism $u : X \to Y$ in $\mathbf{C}$ is an isomorphism of X with a direct summand of Y.

(G4) The functor $\mathscr{F}$ transforms terminal objects into terminal objects and commutes with fibred products.

(G5) The functor $\mathscr{F}$ commutes with finite sums, transforms epimorphisms into epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms.

(G6) If u is a morphism in $\mathbf{C}$ such that $\mathscr{F}(u)$ is an isomorphism, then u is an isomorphism. We call such a functor conservative.

Since Grothendieck first introduced these axioms category theorists have deepened their understanding of category theory. In light of this deeper understanding, we now have a simpler more concise expression of (some of) these axioms in terms of (co)completeness and exactness properties of functors. In order to make some of the axioms more concise we may restate them as follows (G1) $\mathbf{C}$ is *finitely complete* (G4) $\mathscr{F}$ *preserves finite limits*, and (G6) $\mathscr{F}$ *reflects isomorphisms.* Francis Borceux's *Handbook of Categorical Algebra 1: Basic Category Theory* can be consulted for proofs that these restatements are equivalent than the axioms of Grothendieck.

The next theorem is a theorem of Grothendieck. It characterises Galois categories and allows us to deduce a lot about finite étale morphisms simply from the fact that they (together with a choice of geometric morphism) form a Galois category. Grothendieck first proved this theorem in [22]. However, the version stated here is from Hendrik Lenstra [1].

Theorem 4.31 (Grothendieck, SGA I)**.** *Let* $\mathbf{C}$ *be an essentially small Galois category with fundamental functor* $\mathcal{F}$*. Then we have:*

(a) $H : \mathbf{C} \to \mathrm{Aut}(\mathcal{F}) - \mathbf{sets}$ *(defined below) is an equivalence of categories*

(b) If π *is a profinite group such that the categories* $\mathbf{C}$ *and* π-**sets** *are equivalent by an equivalence that, when composed with the forgetful functor* π-**sets**, *yields the functor* $\mathcal{F}$*, then* π *is canonically isomorphic to* $\mathrm{Aut}(\mathcal{F})$.

(c) If $\mathcal{F}'$ *is a second fundamental functor on* $\mathbf{C}$*, then* F *and* F' *are isomorphic*

(d) *If* π *is a profinite group such that the categories* $\mathbf{C}$ *and* π-**sets** *are equivalent, then there is an isomorphism of profinite groups* $\pi \cong \mathrm{Aut}(\mathcal{F})$ *that is canonically determined up to an inner automorphism of* $\mathrm{Aut}(\mathcal{F})$*.*

Proof. For a proof of this theorem the reader may consult Grothendieck [22] or Lenstra [1]. ■

In the above theorem $H : \mathbf{C} \to \mathrm{Aut}(\mathcal{F}) - \mathbf{sets}$ is defined in the same way as the fundamental functor, except we remember the action by $\mathrm{Aut}(\mathcal{F})$ on the sets. Since this theorem is stated in terms of a general Galois category, we will restate a number of statements from the theorem in the context of finite étale morphisms over a connected affine $\mathbb{N}$-scheme. We will do this in the form of the following corollaries of Theorem 4.31 of Grothendieck.

Corollary 4.32. *If* X *is a connected affine* $\mathbb{N}$*-scheme with two geometric points* $i : p \to X$ *and* $i' : p' \to X$*, then* $\pi_1^{\text{Ét}}(X, p) \cong \pi_1^{\text{Ét}}(X, p')$*.*

Next we develop the idea of the *rank of an étale morphism.* Intuitively, for a finite étale morphism $f : Y \to X$ and a geometric point $i : p \to X$, the rank corresponds to the size of the set $Y \times_X p$ i.e. size of the fiber. If X is connected, this should be *constant.* This is a useful tool for proving a given morphism is *not* finite étale — if different fibers have different sizes, then the morphism can't be finite étale.

Corollary 4.33. *Let* X *be an affine* $\mathbb{N}$*-scheme with geometric points* $i : p \to X$ *and* $i' : p' \to X$ *and* $f : Y \to X$ *be a finite étale morphism such that* $Y_p \cong \coprod_{N_p} p$ *and* $Y_{p'} \cong \coprod_{N_{p'}} p'$*. If* X *is a connected affine* $\mathbb{N}$*-scheme, then* $N_p \cong N_{p'}$*.*

Proof. From each geometric point i, i' we obtain fiber functors F_p and $F_{p'}$. Property (c) of Grothendieck's theorem says $F_p \cong F_{p'}$. Therefore, there exists an isomorphism $F_p(Y) \cong F_{p'}(Y)$. That is to say, the underlying morphism of finite sets is an isomorphism. ■

With this result in hand we may define the degree of a finite étale morphism over a connected affine $\mathbb{N}$-scheme X. Inuitively speaking one should view the degree of a finite étale morphism as the "number of sheets of the cover of X". We pick this out by looking at the "number of points in each fiber above a (geometric morphism) point of the base X". Precisely, we define it by pulling back along a geometric morphism.

Definition 4.34 (Degree of Finite Étale Morphism)**.** If X is a connected affine $\mathbb{N}$-scheme, $i : p \to X$ is a geometric point of X, and Y is finite étale over X such that $Y_p \cong \coprod_{N_p} p$, then we define the *degree of* Y *over* X to be $\deg_X(Y) := |N_p|$.

The degree of a finite étale morphism over a *connected* affine $\mathbb{N}$-scheme X does *not* depend on the choice of geometric point of X. This follows from Corollary 4.33 of Grothendieck's theorem.

4.6 Special Case: Trivial Galois Group

The following theorem states that the triviality of the étale fundamental group of an $\mathbb{N}$-scheme X is equivalent to the fact that all finite étale morphisms over X are *globally* totally split.

Theorem 4.35 (Trivial Galois Group)**.** *If X is a connected affine $\mathbb{N}$-scheme and $i : p \to X$ a geometric morphism of X, then $\pi_1^{\text{Ét}}(X, p) = 0$ if and only if each finite étale $\mathbb{N}$-scheme over X is totally split.*

Proof. If $\pi_1^{\text{Ét}}(X, p) = 0$, then $\mathbf{FEt}_X = \mathbf{sets}$, as the group action is trivial. Lemma 4.27 proves that each finite étale $\mathbb{N}$-scheme over X is totally split. Lemma 4.27 also proves the opposite direction - Since the category is equivalent to sets, the action of $\pi_1^{\text{Ét}}(X, p)$ must be trivial on all objects i.e. the fundamental group $\pi_1^{\text{Ét}}(X, p) = 0$ must be trivial.

∎

Notation: If X is a connected affine $\mathbb{N}$-scheme with trivial étale fundamental group, then we say X is *simply connected*. This is consistent with the notion of a simply connected topological space as a topological space is simply connected if and only if its fundamental group is trivial.

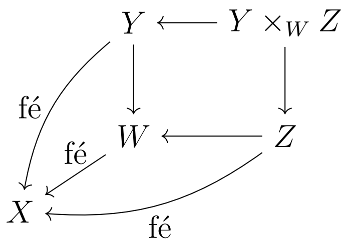
4.7 Main Theorem: $\mathbf{FEt}_X$ is a Galois Category

In this section we prove all pairs $(\mathbf{FEt}_X, p)$, for X a connected affine $\mathbb{N}$-scheme and p a geometric point of X form a Galois category. We will prove that each of the six axioms of a Galois category hold one at a time.

Galois Category Axiom 1

Lemma 4.36 ($\mathbf{FEt}_X$ Finitely Complete (G1))**.** *If X is an affine $\mathbb{N}$-scheme, then $\mathbf{FEt}_X$ is finitely complete.*

Proof. In order to prove $\mathbf{FEt}_X$ is finitely complete it suffices to prove (i) $\mathbf{FEt}_X$ has a terminal object, and (ii) fibred products exist in $\mathbf{FEt}_X$. It is clear that X is the terminal object of $\mathbf{FEt}_X$, so we need only show that fibred products exist. In order to determine whether or not the fibred product of two finite étale covers over another is again finite étale we refer to the following diagram:



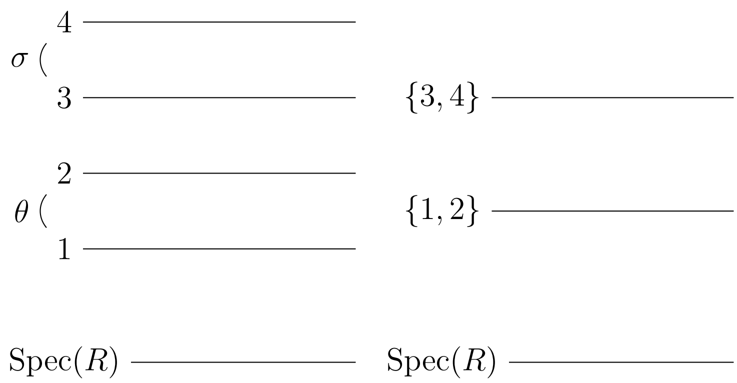
If W, Y, and Z are finite étale over an affine $\mathbb{N}$-scheme X, then in order to prove $Y \times_W Z$ is finite étale over X it suffices to prove $Y \to W$ equiv. $Z \to W$ are finite étale; since compositions of finite étale morphisms are finite étale. Lemma 4.18 tells us that $Y \to W$ and $Z \to W$ are finite étale. Therefore $Y \times_W Z$ is finite étale over X. It follows that the category of finite étale morphisms over a fixed affine $\mathbb{N}$-scheme X is finitely complete. ∎

Galois Category Axiom 2

The initial object of $\mathbf{FEt}_X$ is $\emptyset$ the empty scheme. Moreover finite sums in the category of $\mathbb{N}$-schemes correspond to the product of the corresponding semirings; the product of finite étale morphisms are finite étale. Therefore, in order to prove (G2) holds it remains to show quotients by finite groups of automorphisms exist in $\mathbf{FEt}_X$.

Let us first consider the case that $X = \coprod_N \operatorname{Spec}(R)$ for some $\mathbb{N}$-algebra R and G acts via permutations on the set N; that is to say we might as well assume $G \leq S_N$. Once we have dealt with this case we will reduce the general theorem to this result. In the opposite category this case corresponds to taking the invariants of the G action on R^N; where the action on N induces an action on the standard idempotents $e_1, e_2, \ldots, e_n$. We can partition the set of idempotents into the *orbits* of the action of G. Moreover, *the sum of all the elements in a given orbit is fixed by the action of* G. This fact allows us to describe the subalgebra of invariants in the following manner: the morphism $\varphi : (R^N)^G \to R^{N/G}$, which maps an element $x = \sum_N r_i e_i \in (R^N)^G \mapsto \sum_{N/G} r_i e_{\text{orb}}$, where $e_{\text{orb}(i)}$ denotes the standard idempotents of $R^{N/G}$ indexed by the orbits in N/G, is an isomorphism. Note that since $x \in (R^N)^G$ we know that $r_i = r_j$ for each $i, j \in orb(i)$. In particular, the subalgebra of invariants is isomorphic to a finite number of copies of R i.e. it is finite étale over R. To help get an understanding of what is going on, let us consider an explicit example.

Example 4.37. Let $X := \coprod_4 \operatorname{Spec}(R)$ for some $\mathbb{N}$-algebra, R. Moreover, let $G := \{e, \sigma, \theta, \sigma\theta\}$ be a group of automorphisms of X which act on the set of 4 elements; here σ swaps 2 elements of the set with 4 elements and θ swaps the other two. The following diagram gives a sketch representation of what is happening to X under the action of these elements.



On the left we see how the group G acts on $X = \coprod_4 \mathrm{Spec}(R)$. The picture on the right represents the quotient under the action of H where the equivalent branches (elements of an orbit) have become equal; in particular, note that the quotient is still totally split.

Lemma 4.38. *If $f : Y \to X$ is a finite étale morphism and $G \leq \mathrm{Aut}(Y)$ is a finite group of automorphisms of Y as an affine $\mathbb{N}$-scheme over X, then Y/G is finite étale over X.*

Proof. Let $(f_i : U_i \to X)_{i \in I}$ be an fppf cover of X over which Y becomes totally split. Lemma 4.17 allows us to assume that the automorphisms act as a subgroup of the permutation group of the finite sets N_i, where $Y \times_X U_i \cong \coprod_{N_i} U_i$.

We will now prove that this same fppf cover of X suffices in trivializing Y/G. Recall quotienting out by the action of a finite group is a finite colimit in the category of affine $\mathbb{N}$-schemes. Moreover, each U_i is flat over X thus pulling back along each U_i preserves the finite colimit; that is to say $Y/G \times_X U_i \cong (Y \times_X U_i)/G$. Furthermore, $Y \times_X U_i \cong \coprod_{N_i} U_i$, where the action of G is by a permutation of the finite set N_i. It follows that $Y/G \times_X U_i \cong \coprod_{N_i/G} U_i$. Thus Y/G is finite étale over X, as required. ■

Galois Category Axiom 3

If $f : Y \to Z$ is a morphism of finite étale covers of a fixed affine $\mathbb{N}$-scheme X, then we know there exists a cover $(g_i : U_i \to X)$ and families $(N_i)_{i \in I}$ and $(M_i)_{i \in I}$

indexed by a set I over which $Y \times_X U_i \cong \coprod_{N_i} U_i$, $Z \times_X U_i \cong \coprod_{M_i} U_i$, and f_i is induced by the action of a set map $\tilde{f}_i : N_i \to M_i$. In the opposite category of $\mathcal{O}(X)$-algebras, this morphism decomposes as $\mathcal{O}(Z) \to f^*(\mathcal{O}(Z)) \to \mathcal{O}(Y)$, where the left morphism f'' is a surjection (hence epimorphism) and f' is injective (hence a monomorphism). In fact, $f^*(\mathcal{O}(Z))$ splits over the same fppf cover of U_i and hence is finite étale over $\mathcal{O}(X)$. Precisely, we see the space split as $\mathrm{Spec}(f^*(\mathcal{O}(Z))) \times_X U_i \cong \coprod_{\tilde{f}_i(N_i)} U_i$. Therefore, every morphism splits into an epimorphism and monomorphism as required.

Furthermore, let us assume f is a monomorphism. Since f is a morphism between finite étale covers of X, Lemma 4.18 shows us f itself is a finite étale morphism. Therefore we have reduced to proving the following: if $f : Y \to X$ is an monomorphism and a finite étale morphism, then it is necessarily an isomorphism of Y with a direct summand of X. In the opposite category we know there exists an fppf cocover $(g_i^* : \mathcal{O}(X) \to C_i)_{i \in I}$ over which $\mathcal{O}(Y)$ becomes totally split. Pulling f^* back along each of these morphisms yields an epimorphism $C_i \to C_i^{N_i}$.

Lemma 4.39. *If $R \to R^N$ is an epimorphic R-algebra morphism, then N is either (i) the empty set $\emptyset$, or (ii) a singleton $\{\emptyset\}$.*

Proof. If N is not one of the claimed sets, then R^N has non-trivial automorphisms which fix R. This contradicts the property of being an epimorphism, thus N must have at most one element. ■

Lemma 4.39 implies that f^* is fppf locally an idempotent projection and hence that f is fppf locally an idempotent immersion. Lemma **??** allows us to conclude that f itself must be an idempotent immersion. Therefore we see that all monomorphisms $f : Y \to Z$ of finite étale morphisms are in fact isomorphisms of Y with a direct summand of Z. Thus the category $\mathbf{FEt}_X$ does satisfy axiom (G3) of a Galois category.

Galois Category Axiom 4

The fundamental functor is the composition of the functors: $- \times_X p$, where p is a geometric point, and an equivalence of categories $\mathbf{FEt}_p \cong \mathbf{sets}$. Therefore it corresponds to the fibred product. Since fibered products commute with fibered products we know that the fundamental functor will commute with fibered products. In order to satisfy (G4) the fundamental functor must also send the terminal object to the terminal object in set; however, this is true because $\mathrm{Spec}(R) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(\overline{k}) \cong \mathrm{Spec}(\overline{k})$ which is the terminal object in $\mathbf{FEt}_{\mathrm{Spec}(\overline{k})}$. This is also true if the geometric point is $\mathrm{Spec}(\mathbb{B})$. Note that the equivalence of categories that is composed with this pull-back must send terminal objects to terminal objects.

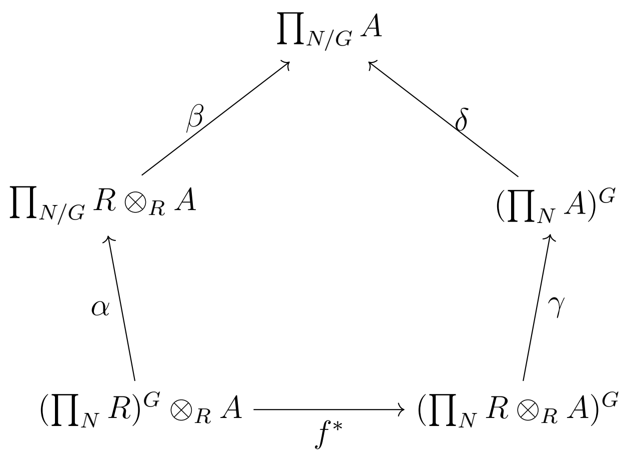
Galois Category Axiom 5

Since the tensor product commutes with finite products of $\mathbb{N}$-algebras we know that the fundamental functor will commute with finite sums of finite étale covers. If $h : Y \to Z$ is an epimorphism of finite étale covers of X, we know that there must be a cover $(f_i : U_i \to X)_{i \in I}$ over which Y and Z split. Moreover we may assume h is *trivial* over this cover i.e. given by a set map. Since the cover is flat, pulling back along it preserves epimorphisms, therefore h_i is still an epimorphism and hence so is the corresponding map of sets.

In order to prove that the fundamental functor commutes with passage to quotient by the action of a finite group G of automorphisms of a finite étale cover $Y \to X$, it suffices to prove that passage to such a quotient commutes with *any* pull back. We will prove that this is true when $Y = \coprod_N X$ and reduce the general case to this totally split instance.

Lemma 4.40. *If $X = \mathrm{Spec}(R)$ and $Z = \mathrm{Spec}(A)$ are affine $\mathbb{N}$-schemes, N is a finite set, $g : \coprod_N X \to X$ is the codiagonal map and $h : Z \to X$ is a morphism of affine $\mathbb{N}$-schemes, and G is a finite group of automorphisms which acts via permutation of N, then the natural map $(\coprod_N X \times_X Z)/G \to (\coprod_N X)/G \times_X Z$ is an isomorphism.*

Proof. In the opposite category the morphism in the statement of the lemma $f : (\coprod_N X \times_X Z)/G \to (\coprod_N X)/G \times_X Z$ is given by $f^* : (R^N)^G \otimes_R A \to (R^N \otimes_R A)^G$ where $(r_i)_{i\in N} \otimes a \mapsto (r_i)_{i\in N} \otimes a$. This is well defined as the action of G on $(R^N \otimes_R A)^G$ is only on the R^N components of the tensors. In order to prove that this is an isomorphism we will do the following (i) construct maps $\alpha, \beta, \gamma, \delta$ as shown in the pentagon below (ii) prove this pentagon commutes (iii) show each of $\alpha, \beta, \gamma, \delta$ to be isomorphisms. This will allow us to conclude that f^* must also be an isomorphism, as the commutativity will give $\beta\alpha = \delta\gamma f^*$ while the fact that $\alpha, \beta, \gamma, \delta$ are all isomorphisms allows us to conclude $f^* = \gamma^{-1}\delta^{-1}\beta\alpha$ is an isomorphism.



When defining these morphisms we use denote the orbit of $j \in N$ under the action of G as $\mathrm{orb}(j)$ in the quotient N/G. With this notation we define the morphisms of the pentagon as follows.

$$\alpha : (r_i)_{i\in N} \otimes a \mapsto (r_i)_{\mathrm{orb}(i)\in N/G} \otimes a$$

$$\beta : (r_{\mathrm{orb}(i)})_{\mathrm{orb}(i)\in N/G} \otimes a \mapsto (r_{\mathrm{orb}(i)}a)_{\mathrm{orb}(i)\in N/G}$$

$$\gamma : (r_i)_{i\in N} \otimes a \mapsto (r_i a)_{i\in N}$$

$$\delta : (a_i)_{i\in N} \mapsto (a_i)_{\mathrm{orb}(i)\in N/G}$$

First we must say why α and δ are in fact well-defined; in particular, if it is the case that $\mathrm{orb}(i) = \mathrm{orb}(j)$, why is it that $r_i = r_j$ in R? and similarly for δ and A.

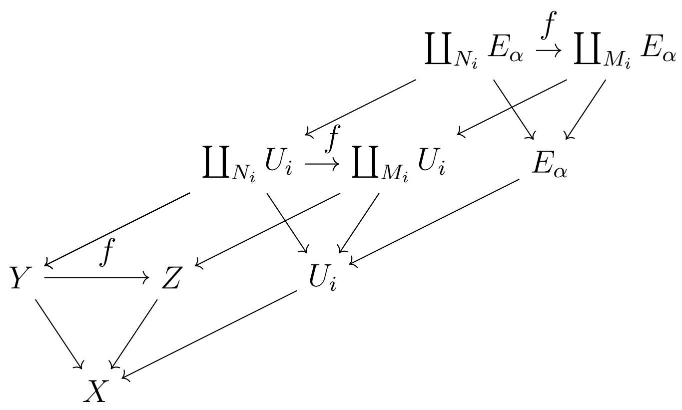
This is necessarily true as α and δ are defined as maps out of the sub-algebra of invariants under the action of G. Thus, if the ith component of an element (r_i) is mapped to the jth, then the $r_i = r_j$, else the element would not be invariant under the action. We have given the action of morphisms out of a tensor product only on the elementary tensors. The full definition is the linear extension to non-elementary tensors. In order to see that this diagram commutes we first calculate the image of the following elementary tensor $\beta\alpha((r_i)_{i\in N} \otimes a) = (r_{\mathrm{orb}(i)}a)_{\mathrm{orb}(i)\in N/G}$. Starting from $(\prod_N R)^G \otimes_R A$ and following the morphisms in the other direction yields $\delta\gamma f^*((r_i)_{i\in N} \otimes a) = \delta\gamma((r_i)_{i\in N} \otimes a) = (r_{\mathrm{orb}(i)}a)_{\mathrm{orb}(i)\in N/G}$. Thus we see that this diagram does commute i.e. $\beta\alpha = \delta\gamma f^*$. It remains to prove each of these morphisms are in fact isomorphisms.

First we note that α and δ are isomorphisms because they are induced by the isomorphism $(R^N)^G \cong R^{N/G}$ that we deduced leading up to Lemma 4.38. On the other hand β and γ are isomorphisms because they are induced by the isomorphism of R-algebras $\prod_S R \otimes_R A \cong \prod_S A$ which sends $(r_s)_{s\in S} \otimes a \mapsto (ar_s)_{s\in S}$. Therefore $\alpha, \beta, \gamma, \delta$ are each isomorphisms and as a result we may conclude that f^* is also an isomorphism. ■

It remains to reduce the global case to this totally split theorem. However, this follows from the fact that Y is *flat* locally totally split. Since the pull back to the totally split case is a flat pull back it commutes with passage to the quotient by a finite group of automorphisms — pull back along flat morphisms commute with all finite colimits. Lemma 4.40 proves f is flat locally an isomorphism and hence that f itself must be an isomorphism.

Galois Category Axiom 6

Let $X = \mathrm{Spec}(R)$ be an $\mathbb{N}$-scheme, with $f : Y \to Z$ a morphism of finite étale morphisms over X, and $(g_i : U_i \to X)_{i\in I}$ be an fppf cover of X over which $Y \times_X U_i \cong \coprod_{N_i} U_i$ and $Z \times_X U_i \cong \coprod_{M_i} U_i$, for some *finite sets* N_i and M_i and $S_i := \mathrm{Hom}_{\mathbf{sets}}(N_i, M_i)$. Lemma 4.17 allows us to give, for each $i \in I$, a family $(E_\alpha \to U_i)_{\alpha\in S_i}$ such that we have $U_i \cong \coprod_{\alpha\in S_i} E_\alpha$.



Finally, we saw that f and the map induced by α *become equal when pull-backed to each* E_α. Now we observe that f is an isomorphism over E_α if and only if $\alpha : N_i \to M_i$ is a bijection on sets. With this observation we make the following definition

$$\mathrm{Isom}(f_i) := \coprod_{\alpha \in \mathrm{Bij}} E_\alpha,$$

where Bij$\subseteq$ Hom(N_i, M_i) is the subset of bijections of sets $N_i \to M_i$. We refer to each Isom(f_i) as *the isomorphism locus of* f *in* U_i. Similarly, we make the definition

$$\neg\mathrm{Isom}(f_i) := \coprod_{\alpha \notin \mathrm{Bij}} E_\alpha.$$

If $\neg$Isom$(f_i) = \emptyset$, then f_i will be an isomorphism when pulled back to it, otherwise we can think of this as the locus in U_i over which f_i is *not* an isomorphism.

In order to complete the this construction, we will employ the machinery of faithfully flat descent of modules, which we will not review here. One can refer to [9, 10] for discussions on faithfully flat descent for modules of rings and semirings, respectively. We have constructed an isomorphism locus for each f_i *locally*, in order to complete our proof we need to show that this construction descends to X. Since each Isom(f_i) is constructed out of the E^i_α (Note we have introduced the superscript $i \in I$ to keep track of the U_i in which E^i_α and Isom(f_i) is in), it suffices to prove that each of these descend to X. As these $E^i_\alpha \to U_i$ are subobjects of U_i, the condition for descent to X is that their construction is stable under refinement of the cover $(U_i \to X)_{i \in I}$. We do not need to check a cocycle condition when glueing subobjects, as there is only one way they can be isomorphic. For each $i \in I$ and $\alpha \in \mathrm{Hom}_{\mathbf{sets}}(N_i, M_i)$ the affine $\mathbb{N}$-scheme E^i_α is the equalizer of the following diagram

$$E^i_\alpha \dashrightarrow U_i \underset{i_\beta}{\overset{f}{\rightrightarrows}} \textstyle\prod_{M_i^{N_i}} U_i. \ (\dagger)$$

Over the refinement of the cover $U_{ij} := U_i \times_X U_j$ we can perfom the analogous construction

$$E^{ij}_\alpha \dashrightarrow U_{ij} \underset{i_\beta}{\overset{f}{\rightrightarrows}} \textstyle\prod_{M_i^{N_i}} U_{ij}. \ (\star)$$

Now we need to prove $E^i_\alpha \times_{U_i} U_{ij} \cong E^{ij}_\alpha$. Notice that the second diagram $(\star)$ can be obtained from $(\dagger)$ by a flat base change along the morphism $U_{ij} \to U_i$. Therefore the isomorphism follows from the fact that these objects are constructed as limits and $U_{ij} \to U_i$ is flat morphism of affine $\mathbb{N}$-schemes and therefore must preserve the limits. Thus the conditions for descent are satisfied. In conclusion we know that for a given morphism $f : Y \to Z$ of finite étale $\mathbb{N}$-schemes over X, there are subobjects $\mathrm{Isom}(f)$ and $\neg\mathrm{Isom}(f)$ of X such that $X = \mathrm{Isom}(f) \coprod \neg\mathrm{Isom}(f)$. Furthermore, when pulled back along $\mathrm{Isom}(f) \to X$, the given morphism f becomes an isomorphism. Now if we assume X is *connected*, we know one of these components must in fact be empty. Furthermore, under the assumption f is an isomorphism at a geometric point (i.e. after applying the fundamental functor) we conclude $i : p \to X$ must factor through $\mathrm{Isom}(f)$, else it would factor through $\neg\mathrm{Isom}(f)$ and hence f would not become an isomorphism over p. Therefore $\neg\mathrm{Isom}(f) = \emptyset$ and $X \cong \mathrm{Isom}(f)$. We see the fundamental functor reflects isomorphisms of finite étale covers over a *connected* affine $\mathbb{N}$-scheme.

Theorem 4.41 ($\mathbf{FEt}_X$ is Galois). *If X is a connected affine $\mathbb{N}$-scheme, p is a geometric point of X, and $F : \mathbf{FEt}_X \to \mathbf{sets}$ is the fundamental functor derived from p, then the pair $(\mathbf{FEt}_X, F)$ is a Galois category.*

Proof. The proof of this theorem is the content of the present section under the headings Galois Category Axiom 1 - 6. ■

Corollary 4.42. *If X is a connected affine $\mathbb{N}$-scheme with two geometric points $i : p \to X$ and $i' : p' \to X$, then $\pi_1^{\text{Ét}}(X, p) \cong \pi_1^{\text{Ét}}(X, p')$.*

Proof. This follows from the theorem of Grothendieck presented in this thesis as Theorem 4.31. ■

Chapter 5

Calculating the Étale Fundamental Group

In this final chapter of the thesis we calculate the étale fundamental group of a number of affine $\mathbb{N}$-schemes. We will calculate the étale fundamental group of the following $\mathbb{N}$-schemes; $\mathrm{Spec}(\mathbb{B})$, $\mathrm{Spec}(\mathbb{R}_+)$, and $\mathrm{Spec}(\mathbb{N})$. Note these are all connected, so these calculations will be independent of choice of base point. We will also calculate the étale fundamental group of $\mathrm{Spec}(E)^p_+$ and $\mathrm{Spec}(E_{++})$ for each real number field $E/\mathbb{Q}$ and each $p \in \mathrm{Hom}_{\mathbf{Alg}_{\mathbb{Q}}}(E, \mathbb{R})$. We use the fact that the étale fundamental group of an $\mathbb{N}$-scheme, X, classifies the $\mathbb{N}$-schemes finite étale over X in order to calculate the group. Indeed, we give explicit characterisations of the finite étale morphisms over each of these $\mathbb{N}$-schemes and deduce the étale fundamental group from that characterisation.

Following Remark 4.5 we observe that the choice of topology may change the notion of finite étale and hence change the resulting étale fundamental group. It is worth noting that due to the nature of the calculations below, none of the results obtained are dependent upon this choice of topology. We find that all étale fundamental groups are trivial in the flat topology and hence must be trivial in the coarser fpqc and fppf topologies. Therefore the results of this section are *independent* of the open question in Remark 4.5.

5.1 Boolean Semiring: $\mathbb{B}$

In Example 4.20 we proved every finite étale morphism over $\mathrm{Spec}(\mathbb{B})$ is of the form $\coprod_N \mathrm{Spec}(\mathbb{B})$ for some finite set N. Theorem 4.35 allows us to conclude $\pi_1^{\text{Ét}}(\mathrm{Spec}(\mathbb{B})) = 0$.

Theorem 5.1 (Étale Fundamental Group of $\mathbb{B}$). *If A is a finite étale $\mathbb{B}$-algebra, then there exists a finite set $N := N(A)$ such that $A \cong \prod_N \mathbb{B}$ i.e. $\pi_1^{\text{Ét}}(\mathrm{Spec}(\mathbb{B}), p) = 0$ for the unique (up to unique isomorphism) geometric point p of $\mathrm{Spec}(\mathbb{B})$.*

In some sense the remainder of our calculations will rely on this fact. We discuss a possible reason for this in the following remark.

Remark 5.2. In his paper *Finite Extensions of* $\mathbb{Z}_{\max}$ [42] Jeffery Tolliver shows that there are no finite intermediate semifield extensions between $\mathbb{B}$ and $\mathbb{Z}_{\max}$. This result is of a similar flavour to Theorem 5.1, as one might expect that any non-trivial finite extension of semifields should be a finite étale algebra.

Furthermore, it is shown (Corollary 3.9 of [42]) that there is an infinite family of intermediate finite extensions between $\mathbb{Z}_{\max} \subseteq \mathbb{R}_{\max}$. It has yet to be determined whether these extensions are finite étale in the sense of the present thesis. The remainder of this chapter will show that finite extensions of semifields need not be finite étale algebras, as one might expect from ring theory. So determining whether Tolliver's finite extensions of $\mathbb{Z}_{\max}$ are finite étale is an interesting question that should be pursued.

Remark 5.3 (Hensel's Lemma at the ∞ Place)**.** Remark 4.28 considers extending Hensel's analogy between p-adic numbers and functions of one complex variable (Riemann surfaces). To put this in more concrete terms we would like to consider the consequences of the suggestion that the ∞-adic integers are defined to be $\mathbb{Z}_\infty := \mathbb{R}_+$ and the residue field at infinity, $\mathbb{F}_\infty := \mathbb{B}$. In particular, we could wonder how Hensel's lemma extends to the infinite place. Hensel's lemma characterises the conditions under which zeroes of polynomials in $\mathbb{Z}_p[x]$ can be lifted from zeroes of the polynomials when reduced modulo p i.e. lifted from solutions to the corresponding polynomial in $\mathbb{F}_p[x]$. Extending this to the infinite place with our definitions one might wonder when solutions to equations of the form $f(x) = g(x)$ for $f, g \in \mathbb{R}_+[x]$ can be lifted from the corresponding equations $\overline{f}(x) = \overline{g}(x)$ where $\overline{f}, \overline{g}$ are the image of f, g in $\mathbb{B}[x]$.

Determining whether an algebra is totally split is equivalent to finding an orthonormal family of idempotents (finite orthogonal family which sums to unity) in the algebra. Idempotents are simply solutions to the equation $x^2 = x$. Therefore if one wishes to determine whether or not an algebra is finite étale over e.g. $\mathbb{R}_+$ it may be enough to lift idempotents from the base change to $\mathbb{B}$. Indeed, this is how our calculations below work in practise. In this way, we see that, to some extent, Hensel's lemma *does* extend to ∞ with our definitions; at least to the extent that we can lift idempotents i.e. solutions to $x^2 = x$.

5.2 Subalgebras of Real Number Fields

In this section we prove the étale fundamental group of $\mathrm{Spec}(E)^p_+$ and $\mathrm{Spec}(E_{++})$ are trivial, for $E/\mathbb{Q}$ a real number field and each $p \in \mathrm{Hom}_{\mathbf{Alg}_\mathbb{Q}}(E, \mathbb{R})$. Our strategy for these $\mathbb{N}$-algebras is to the use the fact (Lemma 4.8) that the property of being finite étale is stable under base change and therefore that $A_\mathbb{B}$ is finite étale over $\mathbb{B}$ whenever A is finite étale over an $\mathbb{N}$-algebra with a $\mathbb{B}$ point. Explicitly, since $A_\mathbb{B}$ is finite étale over $\mathbb{B}$ it is totally split. Inspired by Hensel's lemma we will prove that we can lift the idempotents of $A_\mathbb{B}$ to A and thus prove A is totally split. Given a totally real number field E over $\mathbb{Q}$ (including $\mathbb{Q}$ itself) we can form the following diagram, which we will reference frequently throughout this chapter.

$$
\begin{array}{ccccccc}
 & & & A_{\mathbb{B}} & & & \\
 & & \nearrow & \uparrow & & & \\
A & \longrightarrow & A_{E^p_+} & \longrightarrow & A_E & \longrightarrow & A_{\mathbb{C}} \\
\text{fé}\uparrow & & \uparrow & \mathbb{B} & \uparrow & & \uparrow \\
 & & & \nearrow & & & \\
E_{++} & \longrightarrow & E^p_+ & \longrightarrow & E & \longrightarrow & \mathbb{C} \\
\uparrow & & & & & & \\
\mathbb{Q}_+ & & & & & &
\end{array}
\qquad (\star)
$$

Note in the case $E = \mathbb{Q}$ the diagram $(\star)$ simplifies as $\mathbb{Q}_+ = \mathbb{Q}_{++}$. If A is assumed to be finite étale over E_{++}, then all of the base changes in $(\star)$ are also finite étale over their respective bases. Since $A_{\mathbb{B}}$ is finite étale over $\mathbb{B}$, we know $A_{\mathbb{B}} \cong \mathbb{B}^N$ for some finite set N. We will prove that all such A are in fact totally split, and will do some by lifting the idempotents from $A_{\mathbb{B}}$ to A.

In this section let us fix a finite étale algebra $f : E_{++} \to A$, where f is the morphism $E_{++} \to A$ in $(\star)$. We will prove $A \cong E_{++}^N$, for some finite set N. In order to do so we require a few observations relating to the information in $(\star)$. First, since E_{++} is a subalgebra of E, we know (by the flatness of A) that A is a subalgebra of A_E. Moreover, since A_E is finite étale over E (a field) we know $A_E \cong \prod_M E_i$ for i in some finite set M and $E_i : E$ finite separable extensions of E. On the other hand we can consider the base change $A_{\mathbb{B}}$ which is finite étale over $\mathbb{B}$. Theorem 5.1 tells us $A_{\mathbb{B}} \cong \mathbb{B}^N$, for some finite set N. Let us denote the "standard basis vectors" of $\mathbb{B}^N$ by e_i. Following Remark 5.3 we hope to lift these idempotents $(e_i)_{i\in N} \subseteq A_{\mathbb{B}}$ to A. Since the morphism $\psi : A \to A_{\mathbb{B}}$ is the base change of a surjective morphism, it is surjective. Moreover, Lemma 2.97 tells us the preimage $\psi^{-1}(0) = \{0\}$. Let us choose a lift $\tilde{e_i} \in A$ for each $e_i \in A_{\mathbb{B}}$. First, let us determine that the $\tilde{e_i}$ are mutually orthogonal; $\psi(\tilde{e_i}\tilde{e_j}) = \psi(\tilde{e_i})\psi(\tilde{e_j}) = e_i e_j = 0$, for $i \neq j$. Since the preimage $\psi^{-1}(0) = \{0\}$, it follows $\tilde{e_i}\tilde{e_j} = 0$. We conclude A contains a family $(\tilde{e_i})_{i\in N}$ of mutually orthogonal elements.

To summarise, we have so far deduced A is a subalgebra of $A_E \cong \prod_M E_i$ with N *non-zero mutually orthogonal elements.* Next we show A contains N mutually orthogonal *idempotents.* The following lemma proves this is a consequence of a more general result.

Lemma 5.4. *Let D be an integral domain and T be a finite set indexing a family of non-zero elements $(f^\alpha)_{\alpha\in T}$ in D^N, for some finite set N. If f_i^α denotes the i^{th} component of f^α, then let $S_\alpha := \{j \in N \mid f_j^\alpha \neq 0\}$. If $\alpha \neq \beta \in T$ and $f^\alpha f^\beta = 0$, then $S_\alpha \cap S_\beta = \emptyset$. Furthermore, if $|T| = |N|$, then $\forall\alpha \in T$ $|S_\alpha| = 1$.*

Proof. Fix an $\alpha \in S$. Since $f^\alpha \neq 0$, there exists a $j \in N$ such that $f_j^\alpha \neq 0$ i.e. $S_\alpha \neq \emptyset$. For each $\beta \neq \alpha$, $f^\alpha f^\beta = 0$, which implies, for each $\beta \neq \alpha$, $f_j^\alpha f_j^\beta = 0 \in D$ — as D is an integral domain, we may conclude for each $\beta \neq \alpha$ and $j \in S_\alpha$, $f_j^\beta = 0$ — which means $S_\alpha \cap S_\beta = \emptyset$.

Since $S_\alpha \cap S_\beta = \emptyset$ we know $|\cup_\alpha S_\alpha| = \sum_\alpha |S_\alpha|$ and $|N| \geq |\cup_\alpha S_\alpha|$. Piecing these facts together proves $|N| \geq |\cup_\alpha S_\alpha| = \sum_\alpha |S_\alpha| \geq |T|$. Therefore, under the assumption $|N| = |T|$, we may conclude $\sum_\alpha |S_\alpha| = |T|$ and hence $\forall\alpha \in T$ $|S_\alpha| = 1$. ■

This implies that each f^α is supported in precisely one component. Hence each f^α lies on one of the axes in D^N. This is summarised in the following corollary.

Corollary 5.5. *If D, T, N, $(f^\alpha)_{\alpha\in T}$ are as in Lemma 5.4, and $|N| = |T|$, then $\forall\alpha \in T$ $\exists i \in N$ and $d_i \in D$ such that $f^\alpha = d_i e_i$ where e_i is the i^{th} standard idempotent of D^N.*

Corollary 5.5 allows us to conclude the lifts $\tilde{e_i} \in A$ are of the form $\tilde{e_i} = d_i\overline{e_i}$, where $(\overline{e_i})_{i\in N} \subseteq \prod_M E_i$ are N of the standard basis vectors and $d_i \in E_i$. In particular we note $|N| \leq |M|$. On the other hand $A_{\mathbb{C}} = (\prod_M E_i) \otimes_E \mathbb{C} \cong \mathbb{C}^{\sum_M [E_i:E]}$. Since E is connected Corollary 4.33 implies $|N| = \sum_M [E_i : E]$. Since $|N| \leq |M|$ and $|N| = \sum_M [E_i : E]$ we know $\forall i \in M$ $[E_i : E] = 1$ and $|N| = |M|$. So we have $A \subseteq \prod_N E$ with $|N|$ elements $\tilde{e_i} = d_i\overline{e_i}$ positioned on the N axes. In general the $d_i \in E$, but $d_i^2 \in E_{++}$. It follows for each $i \in N$ since we know $\frac{1}{d_i^2}\tilde{e_i}^2 \in A$. We may conclude each of the following elements $\frac{1}{d_i^2}\tilde{e_i}^2 = \frac{d_i^2\overline{e_i}^2}{d_i^2} = \overline{e_i} \in A$. Since A is an E_{++} algebra, the existence of the idempotents $\overline{e_i} \in A$ implies there is a morphism $i : E_{++}^N \hookrightarrow A$. Note: this is a morphism of algebras finite étale over E_{++}. Thus we may check whether or not it is an isomorphism *after* pulling back to the point $\mathbb{C}$ — this is axiom (G6) of the axioms of a Galois category. After pulling back to $\mathbb{C}$ we obtain an injective (by axiom (G5) of a Galois category) morphism $i_{\mathbb{C}} : \mathbb{C}^N \hookrightarrow \mathbb{C}^N$ of finite dimensional vector spaces. Consequently $i_{\mathbb{C}}$ is an isomorphism of vector spaces and therefore the original morphism i must in fact be an isomorphism. In conclusion, all algebras $f : E_{++} \to A$ which are finite étale are of the form $A \cong \prod_N E_{++}$ for some finite set N.

Theorem 5.6 (Étale Fundamental Group of E_{++})**.** *If $E : \mathbb{Q}$ is a real finite Galois extension and A is a finite étale E_{++}-algebra, then there exists a finite set $N := N(A)$ such that $A \cong \prod_N E_{++}$ i.e the étale fundamental group is* $\pi_1^{\text{Ét}}(\operatorname{Spec}(E_{++}), p) = 0$ *for each geometric point p of* $\operatorname{Spec}(E_{++})$.

Furthermore, we can swap E_+^p for E_{++} in this argument to obtain the following theorem.

Theorem 5.7 (Étale Fundamental Group of E_+)**.** *If $E : \mathbb{Q}$ is a real finite Galois extension, $q : E \to \mathbb{R}$ is a morphism of $\mathbb{N}$-algebras, and A is a finite étale E_+^q-algebra, then there exists a finite set $N := N(A)$ such that $A \cong \prod_N E_+^q$ i.e. the étale fundamental group is $\pi_1^{\text{Ét}}(\operatorname{Spec}(E)_+^q, p) = 0$ for each geometric point p of* $\operatorname{Spec}(E)_+^q$.

It should be noted that Theorem 5.6 and Theorem 5.7 might highlight a weakness in this theory of the étale fundamental group for $\mathbb{N}$-schemes. The passage from E to E_+^p and E_{++} annhilate the entire absolute Galois group $\operatorname{Gal}(E)$. This idea is disucussed at the end of the thesis in Section 5.5.

5.3 Positive Real Numbers: $\mathbb{R}_+$

We may adapt the diagram $(\star)$ given in the previous section to see that the entire argument (with small changes) holds in the case of algebras finite étale over $\mathbb{R}_+$.

$$\begin{array}{ccccccc} A_{\mathbb{B}} & \longleftarrow & A & \longrightarrow & A_{\mathbb{R}} & \longrightarrow & A_{\mathbb{C}} \\ {\scriptstyle \text{fé}}\uparrow & & {\scriptstyle \text{fé}}\uparrow & & {\scriptstyle \text{fé}}\uparrow & & {\scriptstyle \text{fé}}\uparrow \\ \mathbb{B} & \longleftarrow & \mathbb{R}_+ & \longrightarrow & \mathbb{R} & \longrightarrow & \mathbb{C} \end{array} \qquad (\star)$$

The Boolean and complex point interact in the same manner to prove $A \subseteq \mathbb{R}^N$, where N is the rank of the finite étale algebra A. Similarly, the idempotents lift to orthogonal elements which we scale to prove there is an injective morphism $i : \mathbb{R}_+^N \hookrightarrow A$. Which we show is an isomorphism over $\mathbb{C}$, thus is itself an isomorphism.

Theorem 5.8 (Étale Fundamental Group of $\mathbb{R}_+$)**.** *If A is a finite étale $\mathbb{R}_+$-algebra, then there exists a finite set $N := N(A)$ such that $A \cong \prod_N \mathbb{R}_+$ i.e. the étale fundamental group is $\pi_1^{\text{Ét}}(\text{Spec}(\mathbb{R}_+), p) = 0$ for each geometric point p of $\text{Spec}(\mathbb{R}_+)$.*

Remark 5.9. This method generalizes (at least) to zerosum free semifields. Every zerosum free semifield lives inside an (algebraically closed) field and has a map to $\mathbb{B}$; thus the argument given for $\mathbb{R}_+$ above can be used for these types of semirings.

5.4 The Natural Numbers: $\mathbb{N}$

In order to calculate the étale fundamental group of the natural numbers, we use the following diagram to develop a geometric heuristic for how the argument should be laid out. The natural numbers $\mathbb{N}$ are the pull back of the following diagram:

$$\begin{array}{ccc} \mathbb{Z} & & \\ \downarrow & & \\ \mathbb{R} & \longleftarrow & \mathbb{R}_+ \end{array}$$

In other words $\mathbb{N} = \mathbb{Z} \times_{\mathbb{R}} \mathbb{R}_+$. Geometrically speaking, this diagram is more illuminating

$$\begin{array}{ccc} \operatorname{Spec}(\mathbb{Z}) & \longrightarrow & \operatorname{Spec}(\mathbb{N}) \\ \uparrow & & \uparrow \\ \operatorname{Spec}(\mathbb{R}) & \longrightarrow & \operatorname{Spec}(\mathbb{R}_+) \end{array}$$

As it is now clear that $\operatorname{Spec}(\mathbb{N})$ can be constructed by glueing $\operatorname{Spec}(\mathbb{Z})$ and $\operatorname{Spec}(\mathbb{R}_+)$ along their common "subscheme" $\operatorname{Spec}(\mathbb{R})$. This heuristic suggests $\operatorname{Spec}(\mathbb{N})$ is the result of glueing two "simply connected" spaces ($\operatorname{Spec}(\mathbb{Z})$ and $\operatorname{Spec}(\mathbb{R}_+)$ have trivial (étale) fundamental group) along a connected ($\operatorname{Spec}(\mathbb{R})$ is connected) subspace. In algebraic topology such a construction must necessarily be simply connected i.e. we should expect $\mathbb{N}$ to have trivial étale fundamental group.

Theorem 5.10 (Étale Fundamental Group of ℕ)**.** *If A is a finite étale $\mathbb{N}$-algebra, then there exists a finite set $N := N(A)$ such that $A \cong \prod_N \mathbb{N}$ and hence $\pi_1^{\text{Ét}}(\operatorname{Spec}(\mathbb{N}), p) = 0$ for each geometric point p of $\operatorname{Spec}(\mathbb{N})$.*

Proof. Let $f : \mathbb{N} \to A$ be a finite étale algebra. Recall the natural numbers can be presented as the following finite limit $\mathbb{N} = \mathbb{Z} \times_{\mathbb{R}} \mathbb{R}_+$. We can use the flatness of A over $\mathbb{N}$ to give the following presentation of A:

$$\begin{aligned} A &\cong \mathbb{N} \otimes_{\mathbb{N}} A \\ &\cong (\mathbb{Z} \times_{\mathbb{R}} \mathbb{R}_+) \otimes_{\mathbb{N}} A \\ &\cong (\mathbb{Z} \otimes_{\mathbb{N}} A) \times_{(\mathbb{R} \otimes_{\mathbb{N}} A)} (\mathbb{R}_+ \otimes_{\mathbb{N}} A) \qquad (\star) \end{aligned}$$

We use the flatness of A in distributing the tensor product over the *finite* limit presentation of $\mathbb{N}$. Since $\mathbb{Z}$ and $\mathbb{R}_+$ are simply connected, we know $\mathbb{Z} \otimes_{\mathbb{N}} A = \mathbb{Z}^T$ and $\mathbb{R}_+ \otimes_{\mathbb{N}} A = \mathbb{R}_+^S$. In fact, Corollary 4.33 allows us to conclude there is a bijection $\varphi : S \to T$. Also, by extending scalars one sees $\mathbb{R} \otimes_{\mathbb{N}} A \cong \mathbb{R}^T$. Plugging this into $(\star)$ yields

$$A = \mathbb{Z}^T \times_{\mathbb{R}^T} \mathbb{R}_+^T$$

which is naturally isomorphic to $A = \mathbb{N}^T$. Therefore each finite étale $\mathbb{N}$-algebra is a finite product of copies of $\mathbb{N}$. ■

5.5 Searching for a Non-Trivial Example

All of our calculations have so far yielded only $\mathbb{N}$-schemes with *trivial* étale fundamental group. In this section we discuss some reasons for this and where we might be able to find an $\mathbb{N}$-scheme (which is *not* an affine $\mathbb{Z}$-scheme) which has a non-trivial finite étale cover and hence a non-trivial étale fundamental group.

In Example 3.20 of Chapter 3 we introduced the positive cone of an affine $\mathbb{N}$-scheme X with a real point $p \in X(\mathbb{R})$ — recall that this scheme over X is constructed by glueing the positive real numbers to X at a real point. We denote this affine $\mathbb{N}$-scheme X_p^+. This generalized the construction of Spec($\mathbb{N}$) from Spec($\mathbb{Z}$) and Spec(E_+) from Spec(E), where $E : \mathbb{Q}$ is a totally real finite separable extension of $\mathbb{Q}$. When we constructed the positive cone over Spec($\mathbb{Q}$), Spec(E), and Spec($\mathbb{R}$) we obtained a simply connected affine $\mathbb{N}$-scheme. Notice each of these affine $\mathbb{N}$-schemes originally have *non-trivial* étale fundamental group, but when we attached the positive reals (the Booelan point) to the chosen real point of these schemes, the result is a simply connected affine $\mathbb{N}$-scheme. It is interesting to consider how general this behaviour might be. So far we have only considered schemes of dimension 0, as well as the 1 dimensional scheme Spec($\mathbb{Z}$). In order to see if this phenomena generalizes, we should first consider what happens to schemes of higher dimension.

It is certainly not true that all semirings have trivial étale fundamental group, as there are many rings (which are semirings) which have non-trivial étale fundamental group. One might then ask if all non-ring semirings have only trivial finite étale morphisms? Theorem 3.9 tells us this is equivalent to asking if every semiring with a morphism to the Booleans has only trivial étale finite étale morphisms. Again examples like $A := \mathbb{R} \times \mathbb{B}$ tell us this is not true, as the non-triviality of the finite étale morphisms of $\mathbb{R}$ will give non-trivial finite étale morphisms over A. What about if we restrict to *connected* semirings? Even then one could imagine glueing $\mathbb{A}^1_{\mathbb{R}}$ and $(\mathbb{A}^1_{\mathbb{R}})^q_+$ at a common point $p \in \mathbb{A}^1_{\mathbb{R}}$ which is different from q and obtaining non-trivial finite étale morphisms from the $\mathbb{A}^1_{\mathbb{R}}$ component. Let us say an affine $\mathbb{N}$-scheme $X = \mathrm{Spec}(A)$ is *integral* if A has no zero divisors.

Question: Does there exist an integral affine $\mathbb{N}$-scheme X which satisfies the following conditions (i) $X(\mathbb{B}) \neq \emptyset$ and (ii) $\pi_1^{\text{Ét}}(X, p) \neq 0$?

Unfortunately an answer to this question could not be given before the deadline of the thesis.

Chapter 6

Concluding Remarks

In this chapter we will discuss some of the possible geometric interpretations for the phenomena observed in the calculations of the previous chapter and a number of possible directions for future research into the arithmetic algebraic geometry of $\mathbb{N}$ and algebras over $\mathbb{N}$.

Attaching Positivity Information and Higher Homotopy Theory

It seems that the passage to the positive cone annihilates information in the étale fundamental group — the highly non-trivial fundamental group of $\mathrm{Spec}(\mathbb{Q})$ becomes the trivial fundamental group of $\mathrm{Spec}(\mathbb{Q}_+)$. In algebraic topology this behaviour is often observed when glueing spaces together. However, there are often residual effects in the *higher homotopy groups* of the spaces that are being glued together. This phenomena suggests that in order for us to obtain a better understanding of the consequences of glueing $\mathrm{Spec}(\mathbb{R}_+)$ and $\mathrm{Spec}(\mathbb{B})$ to schemes with real points, we should consider not just the étale fundamental group, but the higher homotopy groups of the $\mathbb{N}$-schemes. Micheal Artin and Barry Mazur have developed a theory of higher homotopy types of schemes [3]. Eric Friedlander has also given another approach to this idea [18]. All of this suggests that one of the next steps in this program should be to consider their work in the broader context of $\mathbb{N}$-schemes and calculate the higher homotomopy groups of the affine $\mathbb{N}$-schemes considered in Chapter 5.

What would this require? The work of Artin-Mazur requires the full theory of schemes, so we would have to say what we mean by a non-affine $\mathbb{N}$-scheme; glueing affine $\mathbb{N}$-schemes together with particular topology, and considering functors which are locally affine in the same topology. We have already remarked that the flat topology is not appropriate for this work, as sheaves on the flat site are not well-behaved. In particular the flat topology is not subcanonical. Moreover, Artin-Mazur require not only require the notion of finite étale, but étale as well. Thus this more general notion would need to be developed in the broader context. Perhaps it is the definition suggested by Connes in Remark 4.4 that would be the appropriate definition of étale for such an étale topology.

Different Definition of Finite Étale?

In light of the fact that the étale fundamental group of a number field $E/\mathbb{Q}$ is annhilated when passing to either E_+ for some point p, or E_{++}, one might wonder whether the definition of finite étale that we gave is incorrect. It seems like an honest generalization of Grothendieck's definition, but perhaps we need a broader category of objects in order to encapsulate all of the behaviour of these positive completions. Or not, perhaps this is the "proper behaviour" of these affine $\mathbb{N}$-schemes.

It was mentioned earlier in Remark 4.4 that Alain Connes has suggested that a morphism $f : R \to A$ should be said to be étale if both f and $\Delta : A \otimes_R A \to A$ are flat. I am not sure if this (+ the necessary finite generation as an R-module condition) is equivalent to the definition of finite étale that is given in this thesis. Perhaps the category of such objects is strictly larger and hence has non-trivial objects. This would imply the corresponding étale fundamental group is in fact *non-trivial.* It would be interesting to know if this is true. Or if the correct definition of finite étale should be something else altogether. Further research will be done to answer this question.

The Geometry of p-adic Numbers and the Boolean Point

In Remark **??** we suggested Spec($\mathbb{N}$) behaves like it is the compactification of Spec($\mathbb{Z}$). In particular, we used the analogy of Weil's Rosetta stone to suggest that Spec($\mathbb{Z}$) is missing a point and that Spec($\mathbb{N}$) has that missing point. Moreover, we noticed, with further comment in Remark 4.28, that extending the theory of schemes to the category of semirings adds *precisely one more point*; precisely, Spec($\mathbb{B}$) is the only geometric point of Spec($\mathbb{N}$) which does not come from Spec($\mathbb{Z}$). This idea suggests the centrality of Spec($\mathbb{B}$) in the geometry of semirings (including rings) and therefore we should consider its relation to the rest of the category of $\mathbb{N}$-schemes in the future.

In particular the narrative of this analogy suggests that the Booleans behave a lot like $\mathbb{F}_\infty$; that is, in a manner similar to the relationship between $\mathbb{F}_p$ and $\mathbb{Z}_p \subseteq \mathbb{Q}_p$. Research along these lines will help elucidate the extent to which this analogy should be taken seriously. For example, one might consider the relationship between $\mathbb{B}$ and $\mathbb{R}_+$. In order to calculate the étale fundamental group of Spec($\mathbb{R}_+$) we lifted idempotents from $\mathbb{B}$ to $\mathbb{R}_+$; this could be considered similar to the way one can lift solutions from $\mathbb{F}_p$ to $\mathbb{Z}_p$. From this suggestion we make the following denotation; $\mathbb{F}_\infty := \mathbb{B}$ and $\mathbb{Z}_\infty := \mathbb{R}_+$. Research should be carried to test this analogy; results at the finite primes should be considered in this context of the *infinite prime*. **Q:** to what extent does *Hensel's Lifting Lemma* extend to this context? We can lift idempotents, but can we lift solutions to other equations? **Q:** the ring of p-adic numbers can be obtained from the finite field $\mathbb{F}_p$ by an application of the p-typical Witt vector functor; is there a "natural" manner in which we can define an ∞-typical Witt vector functor which constructs $\mathbb{R}_+$ out $\mathbb{B}$? Alternatively, is there a natural way to piece together $\mathbb{B}$, $\mathbb{R}_+$, and $\mathbb{R}$ in a manner similar to the relationship between $\mathbb{F}_p$, $\mathbb{Z}_p$, and $\mathbb{Q}_p$?

Bibliography

[1] Galois theory for schemes. https://websites.math.leidenuniv.nl/algebra/. Accessed: 12^{th} of February 2019.

[2] Notes on grothendieck topologies fibered categories and descent. http://homepage.sns.it/vistoli/. Accessed: 14^{th} of February 2019.

[3] Artin, M., and Mazur, B. *Etale Homotopy.* Springer-Verlag Berlin, Heidelberg, 1969.

[4] Barr, M. Abstract Galois Theory. *Journal Of Pure and Applied Algebra.* (1980).

[5] Barr, M. Abstract Galois Theory II. *Journal Of Pure and Applied Algebra.* (1982).

[6] Barr, M., and Diaconescu, R. On Locally Simply Connected Toposes and Their Fundamental Groups. *Colloque Sur Les Categories Dedie A Charles Ehresmann.* (1980).

[7] Bhatt, B., and Scholze, P. The pro-étale topology for schemes. *Astérisque 369* (2015).

[8] Borceux, F. *Handbook of Categorical Algebra 1.* Cambridge University Press, 1994.

[9] Borceux, F. *Handbook of Categorical Algebra 2.* Cambridge University Press, 1995.

[10] Borger, J. Witt vectors, semirings, and total positivity. Absolute Arithmetic and $\mathbb{F}_1$ Geometry. *EMS Publishing House* (2016).

[11] Borger, J., and Grinberg, D. Boolean Witt vectors and an integral Edrei-Thoma theorem. *Selecta Mathematica* (2016), pp 595–629.

[12] Bunge, M. Galois Groupoids and Covering Morphisms in Topos Theory. *Fields Institute Communications 43, AMS* (2004).

[13] Bunge, M., and Moerdijk, I. On the Construction of the Grothendieck Fundamental Group of a Topos by Paths. *Journal of Pure and Applied Algebra* (1996).

[14] Caramello, O. Topological Galois Theory. *Advances in Mathematics 291* (2016), pp 646–695.

[15] Connes, A., and Consani, C. The arithmetic site. *Comptes Rendus Mathematique Volume 352, Issue 12* (2014), pp 971–975.

[16] Connes, A., and Consani, C. Geometry of the Arithmetic Site. *Advances in Mathematics 291* (2016), pp 274–329.

[17] Connes, A., and Consani, C. The Scaling Site. *Comptes Rendus Mathematique. Volume 354, Issue 1* (2016), pp 1–6.

[18] Friedlander, E. M. *Etale Homotopy of Simplicial Schemes.* Princeton University Press, 1982.

[19] Giansiracusa, J., and Giansiracusa, N. Equations of tropical varieties. *Duke Mathematical Journal* (2016), 3379–3433.

[20] Golan, J. S. *Semirings and their Applications.* Kluwer Academic Publishers, 1999.

[21] Grothendieck, A. Lecture Notes: Introduction to Functorial Algebraic Geometry. *Summer School in Buffalo. Lecture notes written by Frederico Gaeta.*

[22] Grothendieck, A. *Revêtements étales et groupe fondamental (SGA 1)*, vol. 224 of *Lecture notes in mathematics.* Springer-Verlag, 1971.

[23] Grothendieck, A., and Dieudonn, J. Éléments de géométrie algébrique I - IV. *Publications Mathématiques de l'IHÉS* (1961).

[24] Johnstone, P. T. *Topos Theory.* Academic Press 1977, 1977.

[25] Johnstone, P. T. *Sketches of an Elephant, Volume 1.* Clarendon Press, Oxford, 2002.

[26] Johnstone, P. T. *Sketches of an Elephant, Volume 2.* Clarendon Press, Oxford, 2002.

[27] Joyal, A., and Tierney, M. *An Extension of the Galois Theory of Grothendieck.* Memoirs of the American Mathematical Society, 1984.

[28] Jun, J. *Algebraic geometry over semi-structures and hyper-structures of characteristic one.* PhD thesis, The John Hopkins University, 2015.

[29] Jun, J. Cech Cohomology of Semiring Schemes. *ArXiv e-prints* (Mar. 2015).

[30] Kennison, J. F. The Fundamental Localic Groupoid of a Topos. *Journal of Pure and Applied Algebra* (1991).

[31] Lescot, P. Algèbre absolue. *Ann. Sci. Math. Québec. Volume 33*, pp 63–82.

[32] Lescot, P. Algèbre absolue II - Ideals and Spectra. *Journal of Pure and Applied Algebra 215(7)* (2011), pp 1782–1790.

[33] Lescot, P. Absolute Algebra III - The saturated spectrum. *Journal of Pure and Applied Algebra 216(5)* (2013), pp 1004–1015.

[34] Lorscheid, O. The geometry of blueprints. Part I: Algebraic background and scheme theory. *Advances in Mathematics 229(3)* (2012), pp 1804–1846.

[35] Lorscheid, O. The geometry of blueprints. Part II: Tits-Weyl models of algebraic groups. *Forum Math. Sigma 6, e20* (2018).

[36] Maclagan, D., and Rincón, F. Tropical schemes, tropical cycles, and valuated matroids. *arXiv e-prints* (Jan. 2014), arXiv:1401.4654.

[37] Maclagan, D., and Sturmfels, B. *Introduction to Tropical Geometry*, vol. 161 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2015.

[38] Mumford, D. *The Red Book of Varieties and Schemes*. Springer-Verlag Berlin, Heidelberg, 1999.

[39] Stillwell, J. *Theory of Algebraic Functions of One Variable History of Mathematics Sources, Translated and Introduced by John Stillwell*. American Mathematical Society, 2012.

[40] Szamuely, T. *Galois Groups and Fundamental Groups*. Cambridge University Press, 2009.

[41] Toën, B., and Vaquiè, M. Au-dessous de Spec(Z). *Journal of K-Theory 3(3)* (2009), pp 437 – 500.

[42] Tolliver, J. Finite extensions of $\mathbb{Z}_{\max}$, 2014.

[43] Weil, A. *Foundations of Algebraic Geometry*. American Mathematical Society, 1946.

[44] Weil, A. A 1940 Letter of André Weil on Analogy in Mathematics. *Notices of the American Mathematical Society, Volume 52, No. 3* (2005).