Difference algebraic geometry: Morphisms of difference schemes with an exceptional property

by

Rachael Ann King

Submitted in partial fulfilment of the requirements of the degree of
Doctor of Philosophy

School of Mathematical Sciences
Queen Mary, University of London
United Kingdom

September 2020

Declaration

I, Rachael Ann King, confirm that the research included within this thesis is my own work or that where it has been carried out in collaboration with, or supported by others, that this is duly acknowledged below and my contribution indicated. Previously published material is also acknowledged below.

I attest that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge break any UK law, infringe any third party's copyright or other Intellectual Property Right, or contain any confidential material.

I accept that the College has the right to use plagiarism detection software to check the electronic version of the thesis.

I confirm that this thesis has not been previously submitted for the award of a degree by this or any other university.

Signature: Rachael Ann King

Date: 27$^{\text{th}}$ Sept 2020

Abstract

In this thesis we generalise the theory of exceptional covers of varieties to the context of difference algebraic geometry. We formulate the notion of difference exceptional covers and prove a difference exceptionality criterion analogous to the classical situation. We also obtain a Galois correspondence for difference ring extensions in the style of Borceux-Janelidze.

Along the way we explore the background of exceptional varieties, Grothendieck's Galois categories and discuss a proof of the classical exceptionality criterion. An overview of difference algebraic geometry is given, motivated by the work of Tomašić.

Acknowledgments

First and foremost I would like to thank my supervisor, Ivan Tomašić, for sharing so much of his knowledge and time over the course of this PhD. His patience, honesty and sense of humour have been much appreciated throughout this journey, and this thesis is firmly rooted in his mathematical ideas.
I would also like to thank the School of Mathematical Sciences at QMUL and the broader mathematical community for giving me this opportunity and helping me to navigate the world of academia.

On a personal level I am grateful to my parents, Peter and Sue, for their support throughout my whole academic career and for allowing me the freedom to choose my own path.
I am lucky to have a number of close friends who have counselled and encouraged me over the past few years. I would particularly like to thank Lindsay King for her unwavering positivity, and Elliot Gathercole for his unconditional support.

This work was supported by the EPSRC (1791104).

Contents

List of Figures

Chapter 1

Introduction

1.1 Historical background

1.1.1 Difference algebra

Difference algebra first arose in the early twentieth century alongside differential algebra. Rather than studying structures equipped with a derivation which satisfies the Leibniz rule, the objects of interest here are simply structures together with an endomorphism which is often denoted σ. Motivation for this area of study originally came from considering shifts of arguments of functions, where the difference endomorphism translates the argument by a fixed period. We can consider the field of meromorphic functions on $\mathbb{C}$ as a difference object with $\sigma(f)(z) \mapsto f(z+1)$. The map $D : f \mapsto \sigma(f) - f$ then gives rise to the consideration of finite differences, giving 'difference algebra' its name.

Similarly for any complex number z which is not a negative integer then the Γ function is

a solution to:

$$\sigma(f) = zf.$$

Alternatively if we consider $\sigma(F)_n = F_{n+1}$ then the Fibonacci sequence can be described as the solution of the difference equation

$$\sigma^2(F) = \sigma(F) + F,$$

with initial conditions $F_0 = 0,\ F_1 = 1$.

Difference algebra was developed by Ritt in the 1930s; this work included several papers concerning algebraic difference equations ([RD33], [RR39]). There was much swifter progress in the area of differential algebra which culminated in his influential book published in 1950 [Rit50]. Nevertheless work continued on difference algebra, notably with Babbitt's investigation into extensions of difference fields [Bab62]. In this paper a description is given of some of the pathological compatibility behaviour that difference field extensions can exhibit, along with a decomposition theorem concerning benign extensions.
The first systematic presentation of this subject matter was given by Cohn in 1965 [Coh65] with a more recent account by Levin in 2008 [Lev08]. These books are the standard references for this material and they demonstrate how far the area has diverged from its original analytic background.

Model theoretic interest in difference fields emerged at the end of the 1980s with the development of the theory ACFA ('algebraically closed fields with an automorphism') by van den Dries, Macintyre and Wood. Here the main objects of interest are algebraic closures of finite fields equipped with a power of Frobenius; these are often referred to as difference

fields with Frobenii. Models of ACFA can then be constructed as ultraproducts of these difference fields.

The axiomatisation of ACFA was formalised by Macintyre [Mac97] and Chatzidakis-Hrushovski [CH99] in the late 1990s before it was shown in an unpublished paper by Hrushovski that ACFA is the first order theory of difference fields with Frobenii [Hru04]. A major component of this proof is the generalisation of the Lang-Weil estimates of rational points of varieties over a finite field to the setting of difference algebraic geometry; we will utilise this result in Chapter 6 in our proof of the difference exceptionality criterion.

This model theoretic approach to difference algebra has also found applications in other areas of mathematics, maybe most famously with a new proof of the Manin-Mumford conjecture in arithmetic geometry (Hrushovski, [Hru01]).

More recent developments in difference algebra focus on difference algebraic geometry and Galois theory. Some of these results retain a model theoretic flavour by looking at first order definable sets in the language of difference rings (Tomašić, [Tom16]), whereas others revisit the setting of differential equations in a new light (DiVizio-Hardouin-Wibmer, [DVHW14], [DVHW17]). An overview of progress in the area of difference algebraic groups can be found in Wibmer's habilitation thesis along with many new results [Wib15]. We draw attention to his work on étale difference algebraic groups which complements our own considerations of étale difference algebras in Chapter 6. Notable work has also been conducted by Chatzidakis, DiVizio, Hardouin, Kowalski, Ovchinnikov and Singer.

We will adopt the categorical perspective of difference algebraic geometry developed by Tomašić ([Tom14], [Tom20]).

1.1.2 Exceptional covers

The history of exceptional covers can be traced back to the study of permutation polynomials in the nineteenth century. A polynomial over a finite field is a permutation polynomial if

it induces a bijection on its field of definition. Dickson gave a number theoretic criterion for recognising such polynomials in 1897 [Dic97]; this is often referred to as Hermite's criterion as he noted it in the special case of prime fields in 1856.

Although they will not be the specific focus of this thesis, permutation polynomials have inspired a substantial amount of research in their own right. The computational aspect of generating examples allows for the implementation of methods from computer science, and it is therefore unsurprising that they have found applications in cryptography and coding theory. An overview of results surrounding permutation polynomials can be found in Chapter 7 of Lidl-Niederreiter [LN97] with more recent advances covered in a survey paper by Hou [Hou15]. Examples of investigations into their use in public key cryptography can be seen in Varadharajan [Var88], Singh-Sarma-Saikia [SSS09] and Khachatrian-Kyureghyan [KK17].

There are two ways of defining an exceptional polynomial; the historical definition is that a polynomial f defined over a finite field $\mathbb{F}_q$ is exceptional if the only absolutely irreducible factor of $f(x)-f(y)$ defined over $\mathbb{F}_q$ is $x-y$. The development of this statement can be seen in work by Davenport-Lewis [DL63], MacCluer [Mac67] and Williams [Wil67]. Equivalently a polynomial f defined over $\mathbb{F}_q$ can be said to be exceptional if f is a permutation polynomial over infinitely many extensions of $\mathbb{F}_q$. It is the second definition that we will use throughout this thesis and we will take the first as a criterion for identifying exceptional behaviour. The history of the proof of their equivalence is discussed further in Subsection 3.1.

As in the case of permutation polynomials there have been attempts to generate examples of exceptional polynomials and classify them by degree and order of their field of definition. The Carlitz-Wan conjecture is one result in this direction; we briefly touch on this in Chapter 2 but a comprehensive account of work in this area can be found in Zieve's survey paper [Zie13].

Attention has turned towards generalising exceptionality to algebraic geometry. Both definitions given above can be generalised to give two notions of an exceptional cover. We will focus on a proof of their equivalence given by Fried [Fri74]. This proof holds for endomorphisms of a variety and has since been extended to more general morphisms by Fried-Guralnick-Saxl [FGS93] and Guralnick-Tucker-Zieve [GTZ07]. Fried has also explored the relation between exceptionality and monodromy groups [Fri94].

1.2 Thesis overview

This historical journey brings us to this thesis, in which we develop the theory of exceptional covers in difference algebraic geometry.

Chapter 2 covers relevant preliminary material; we start with early definitions of varieties and the Zariski topology then move towards Grothendieck's formulation of scheme theory, focusing on on rational points, residue fields and properties of morphisms. We also look at Galois covers and define the étale fundamental group as well as decomposition and inertia groups. This includes a discussion of normalisation and function fields.

An exposition of Grothendieck's work on Galois categories is provided. We describe the general correspondence between a Galois category and the category of finite sets with a continuous group action, then use the category of finite étale covers as an illustrative example. This background supports our discussion of the exceptionality criterion in Chapter 3.

Chapter 3 is an exposition of the theory of exceptional covers of varieties. A brief overview of permutation and exceptional polynomials is given, highlighting some results and examples in both cases. We detail the equivalence of two notions of an exceptional cover $f : Y \to X$, one given in terms of bijectivity of rational points over infinitely many extensions and the other given in terms of geometrically irreducible components of the fibre

product $Y \times_X Y$. We take the first as our definition and we call the second the 'exceptionality condition'.
The proof of their equivalence is the main focus of this chapter with a full discussion of the setup of varieties and function fields. We also look at geometric and group-theoretic interpretations of the exceptionality condition.

The exploration of difference algebra begins in Chapter 4. We approach this from a categorical perspective by defining the categories σ-**Set** and G-σ-**Set** and interpreting the notion of connectedness in this context. We contrast this with the definition of a group orbit being σ-closed then discuss results counting σ-closed orbits.
The following section looks more closely at difference fields, defining difference Galois closures and discussing the noncanonical choice of difference structure here. The difference action on the set of connected components of a tensor product of difference fields is then explicitly described.
We next lay the foundations of difference algebraic geometry from a perspective which complements the exposition of algebraic geometry given in Chapter 2. Here we enhance the underlying algebraic geometry and look at how difference rational points of relative schemes interact with the difference action of the base scheme. The chapter concludes by defining a difference Galois cover in a geometric setting and discussing local substitutions of difference rational points.

In Chapter 5 we take a categorical detour to obtain a difference Galois correspondence. Recalling the classical Galois correspondence described in Chapter 2, we utilise a categorical result by Borceux-Janelidze to find an analogous statement in the difference setting. The setup and result is given in full generality; this theory is then applied to the category of difference algebras by identifying relevant objects and morphisms and verifying that they satisfy the required properties. This easily gives a difference Galois correspondence between

a subcategory of difference schemes and the category of finite difference sets with a difference group action.

Chapter 6 brings everything together to formulate and prove a difference exceptionality criterion. Based on a preprint of Tomašić-Zieve [TZ16], we formulate both the definition of exceptional covers and the exceptionality criterion in the difference context and prove an equivalence which generalises the classical situation.
As in Chapter 3 we discuss a geometric interpretation of the difference exceptionality condition. Our final corollary shows that the classical exceptionality criterion can be recovered as a special case of the difference statement. This justifies our claim that the difference formulation of exceptionality is a generalisation of the classical case. We finally give examples of difference exceptional covers obtained from families of permutation polynomials.
This thesis concludes by proposing some avenues for further research, particularly through removing assumptions on the morphism in question.

Chapter 2

Preliminaries

We collect preliminary material for ease of reference throughout the rest of the thesis. This covers the basics of algebraic geometry, Galois covers and Galois categories. The material covered in the first three sections can be found in any standard algebraic geometry textbook; the references used here are Eisenbud-Harris [EH00], Hartshorne [Har77] and Szamuely [Sza09].

2.1 Foundations of algebraic geometry

We cover the older definitions of varieties and coordinate rings for familiarity before discussing the broader context of schemes.

Definition 2.1.1. Let Ω be an algebraically closed field. An **affine n-space over Ω**, denoted $\mathbb{A}^n_\Omega$ or $\mathbb{A}^n$, is the set of all n-tuples of elements of Ω.

A **point** $a \in \mathbb{A}^n$ is an element $a = (a_1, \ldots, a_n)$, where a_i are the **coordinates** of a.

The **polynomial ring in n variables over Ω** is denoted $A = \Omega[x_1, \ldots, x_n]$. Elements of A can be thought of as functions $f : \mathbb{A}^n \to \Omega$ by evaluating $f(a) = f(a_1, \ldots, a_n)$.

Definition 2.1.2. Let $T \subseteq A$. The **zero set of T in $\mathbb{A}^n$**, denoted $Z(T)$, is the set of common zeros of all elements of T, i.e.

$$Z(T) = \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall f \in T\}.$$

Let $X \subseteq \mathbb{A}^n$. The **ideal of X in A**, denoted $I(X)$, is the ideal containing functions in A which vanish on all points of X, i.e.

$$I(X) = \{f \in A \mid f(a) = 0 \ \forall a \in X\}.$$

Definition 2.1.3. The **Zariski topology on** $\mathbb{A}^n$ is defined by taking closed sets to be of the form $Z(T)$ for some $T \subseteq A$. The topology axioms can easily be verified.
An **affine variety** is a closed subset $X \subseteq \mathbb{A}^n$ with the induced Zariski topology.

Definition 2.1.4. Let $X \subseteq \mathbb{A}^n_\Omega$ be an affine variety. The **affine coordinate ring of X**, $\Omega[X]$, is defined as $\Omega[X] = A/I(X)$. This ring can be thought of as the ring of polynomial functions on X.

This approach relies on Ω being an algebraically closed field but we will be interested in working over finite fields. We therefore turn our attention to the richer setting of schemes, first defining sheaves.

Definition 2.1.5. Let X be a topological space. A **sheaf of rings**, $\mathcal{F}$, on X consists of the following data:

1. For every open set $U \subseteq X$, there is a ring $\mathcal{F}(U)$;
2. For every inclusion $V \subseteq U$ of open sets, there is a ring homomorphism $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$.

This data satisfies the conditions:

(i) $\mathcal{F}(\emptyset) = 0$;

(ii) $\rho_{UU} : \mathcal{F}(U) \to \mathcal{F}(U)$ is the identity;

(iii) If $W \subseteq V \subseteq U \subseteq X$ are open subsets, then $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$;

(iv) If $U \subseteq X$ is open, $\{V_i\}$ is an open covering of U and $s \in \mathcal{F}(U)$ is such that $s\restriction_{V_i} = 0$ for all i, then $s = 0$;

(v) If $U \subseteq X$ is open, $\{V_i\}$ is an open covering of U and $s_i \in \mathcal{F}(V_i)$ satisfies $s_i\restriction_{V_i \cap V_j} = s_j\restriction_{V_i \cap V_j}$ for all i, j, then there exists $s \in \mathcal{F}(U)$ such that for all i, $s\restriction_{V_i} = s_i$.

The **stalk of $\mathcal{F}$ at a point** $x \in X$, denoted $\mathcal{F}_x$, is the direct limit of rings $\mathcal{F}(U)$ where U runs over open sets containing x, i.e.

$$\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U).$$

This construction isolates the behaviour of the sheaf at a particular point of X.

Definition 2.1.6. A **ringed space**, $(X, \mathcal{F})$, is a topological space X equipped with a sheaf of rings $\mathcal{F}$.
A **locally ringed space** is a ringed space $(X, \mathcal{F})$ such that for every $x \in X$, the stalk $\mathcal{F}_x$ is a local ring.

We can now define a scheme by introducing the prime spectrum of a ring.

Definition 2.1.7. Let R be a commutative ring. The **spectrum** of R, $\mathrm{Spec}(R)$, is the set of all prime ideals $\mathfrak{p} \lhd R$.
$\mathrm{Spec}(R)$ can be equipped with an adaptation of the Zariski topology: for an ideal $\mathfrak{a} \lhd R$, closed sets are of the form $V(\mathfrak{a}) = \{\mathfrak{p} \lhd R \text{ prime} \mid \mathfrak{a} \subseteq \mathfrak{p}\}$. For $f \in R$, open sets of the form

$D(f) = \{\mathfrak{p} \lhd R \text{ prime} \mid f \notin \mathfrak{p}\}$ define a base for the topology.

$\mathrm{Spec}(R)$ can also be given a structure sheaf $\mathcal{F} = \mathcal{O}$ which is induced from R. For a prime ideal $\mathfrak{p} \lhd R$, let $R_\mathfrak{p}$ denote the localisation of R at $\mathfrak{p}$. Then for an open set $U \subseteq \mathrm{Spec}(R)$, define $\mathcal{O}(U)$ to be the ring of functions $s : U \to \bigsqcup_{\mathfrak{p}\in U} R_\mathfrak{p}$ where each $\mathfrak{p} \in U$ is sent to its corresponding localisation and s is locally a quotient of elements of R. Explicitly:

$$\mathcal{O}(U) \;=\; \Big\{ s : U \to \bigsqcup_{\mathfrak{p}\in U} R_\mathfrak{p} \;\Big|\; \forall \mathfrak{p} \in U,\ s(\mathfrak{p}) \in R_\mathfrak{p},\ \text{and } \exists V \subseteq U \text{ nhood of } \mathfrak{p},$$
$$\exists a, f \in R \text{ such that } \forall \mathfrak{q} \in V, s(\mathfrak{q}) = \frac{a}{f} \in R_\mathfrak{q} \Big\}.$$

Definition 2.1.8. An **affine scheme** is a locally ringed space which is isomorphic to $(\mathrm{Spec}(R), \mathcal{O})$ for some commutative ring R.

A **scheme** is a locally ringed space, $(X, \mathcal{O}_X)$, in which every point has an open neighbourhood U such that $(U, \mathcal{O}_X\restriction_U)$ is an affine scheme. In this situation the sheaf is denoted $\mathcal{F} = \mathcal{O}_X$ and is called the **structure sheaf** of X.

From now on we will omit sheaf notation when discussing schemes, simply writing X in place of $(X, \mathcal{O}_X)$.

There are some useful connections between the structure sheaf on an affine scheme and its associated commutative ring ([Har77], Prop II.2.2).

Proposition 2.1.9. *Let R be a commutative ring and consider the affine scheme* $\mathrm{Spec}(R)$.

(i) For $\mathfrak{p} \lhd R$ prime with corresponding point $x \in \mathrm{Spec}(R)$, there is a local ring isomorphism $\mathcal{O}_{\mathrm{Spec}(R),x} \cong R_\mathfrak{p}$.

(ii) For $f \in R$, there is a ring isomorphism $\mathcal{O}_{\mathrm{Spec}(R)}(D(f)) \cong R_f$.

(iii) There is a ring isomorphism $\mathcal{O}_{\mathrm{Spec}(R)}(\mathrm{Spec}(R)) \cong R$.

This broader framework allows for several types of points.

Definition 2.1.10. Let $X = \mathrm{Spec}(R)$ be an affine scheme.

- A **scheme-theoretic point** corresponds to a prime ideal of R; these are the types of points we have been considering so far. The notation $x \in X$ refers to a scheme-theoretic point unless clearly stated otherwise.
- A **closed point** corresponds to a maximal ideal of R.
- A **generic point**, η, is a scheme-theoretic point such that the Zariski closure of $\{\eta\}$ is X. A generic point exists if and only if X is an irreducible topological space, i.e. if and only if the nilradical of R is a prime ideal.

Definition 2.1.11. Let X, Y be schemes and let $f : Y \to X$ be a continuous map of topological spaces.
The **direct image sheaf of $\mathcal{O}_Y$ on X induced by f**, denoted $f_*\mathcal{O}_Y$, is defined as:

$$(f_*\mathcal{O}_Y)(V) = \mathcal{O}_Y(f^{-1}(V)),$$

for $V \subseteq X$.
The **sheaf morphism induced by f** is denoted:

$$f^{\#} : \mathcal{O}_X \to f_*\mathcal{O}_Y.$$

The **stalk homomorphism induced by f at $y \in Y$**, denoted $f_y^{\#} : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$, is induced by considering the stalk of $f_*\mathcal{O}_Y$ at $f(y)$:

$$\left(f_*\mathcal{O}_Y\right)_{f(y)} = \varinjlim_{V \ni f(y)} f_*\mathcal{O}_Y(V) = \varinjlim_{V \ni f(y)} \mathcal{O}_Y(f^{-1}(V)) \hookrightarrow \varinjlim_{f^{-1}(V) \ni y} \mathcal{O}_Y(f^{-1}(V)) = \mathcal{O}_{Y,y}.$$

Composition then gives:

$$f_y^{\#} : \mathcal{O}_{X,f(y)} \longrightarrow \left(f_*\mathcal{O}_Y\right)_{f(y)} \hookrightarrow \mathcal{O}_{Y,y}.$$

A **morphism of schemes** is a pair:

$$(f, f^{\#}) : (Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X),$$

where $f^{\#}$ is induced by f, and for every $y \in Y$ the induced stalk homomorphisms $f_y^{\#}$ are local, i.e. $\left(f_y^{\#}\right)^{-1}(\mathfrak{m}_y) = \mathfrak{m}_{f(y)}$, where $\mathfrak{m}_y$ is the unique maximal ideal of the stalk $\mathcal{O}_{Y,y}$.
We will suppress the sheaf notation and denote a morphism of schemes by $f : Y \to X$.

We can also consider rational points of a scheme.

Definition 2.1.12. Let X be a scheme.

- For a field F, an **F-rational point** is a morphism $a : \mathrm{Spec}(F) \to X$. Let

  $$X(F) = \mathrm{Hom}_{\mathbf{Sch}}(\mathrm{Spec}(F), X)$$

  denote the **set of F-rational points of a scheme** X.

- A **geometric point** is a rational point with values in an algebraically closed field, i.e. a morphism $\bar{x} : \mathrm{Spec}(\Omega) \to X$.

Definition 2.1.13. Let S be a scheme. A scheme X is **defined over** S or said to be an **S-scheme**, denoted X/S, if it comes equipped with a scheme morphism $X \to S$. This morphism is often called the **structure map**.
If X, Y are both defined over S, then an **S-morphism** is a morphism $f : Y \to X$ which satisfies the following commutative diagram.

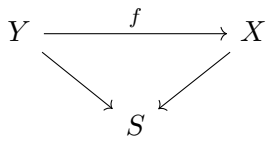

Figure 2.1: An S-morphism

In the case where $S = \mathrm{Spec}(F)$ for a field F, a scheme X is said to be **defined over** F, or an F**-scheme**, and is denoted X/F.

Definition 2.1.14. The **category of schemes**, **Sch**, consists of schemes as objects and scheme morphisms as morphisms.
For a base scheme S, the **category of** S**-schemes**, **Sch**$/S$, is the slice category consisting of schemes defined over S as objects and S-morphisms as morphisms.

We can view $\mathrm{Spec}\colon$ **CRing** $\to$ **Sch** as a contravariant functor from the category of commutative rings to the category of schemes. To see this let $f : R \to T$ be a ring homomorphism and note that we can define a morphism of their corresponding schemes:

$$\begin{array}{rccc} f: & \mathrm{Spec}(T) & \longrightarrow & \mathrm{Spec}(R) \\ & \mathfrak{p} & \longmapsto & f^{-1}(\mathfrak{p}). \end{array}$$

Note that $f^{-1}(\mathfrak{p})$ is a prime ideal of the ring R. We use f to denote both the ring morphism and its associated scheme morphism without confusion.
The categories of affine schemes and commutative rings are in fact anti-equivalent. We can define the **global sections** functor $\Gamma(-, \mathcal{O}_{(-)}) :$ **Sch** $\to$ **CRing** by $\Gamma(X, \mathcal{O}_X) = \mathcal{O}_X(X)$. For a commutative ring R recall from Proposition 2.1.9 that $\mathcal{O}_{\mathrm{Spec}(R)}(\mathrm{Spec}(R)) \cong R$, and Definition 2.1.7 shows that $\mathrm{Spec}(\Gamma(\mathrm{Spec}(R), \mathcal{O}_{\mathrm{Spec}(R)})) \cong \mathrm{Spec}(R)$.

For two rings R, T, we see that

$$\mathrm{Hom}_{\mathbf{Sch}}(\mathrm{Spec}(R), \mathrm{Spec}(T)) \cong \mathrm{Hom}_{\mathbf{CRing}}(T, R).$$

This anti-equivalence lies at the heart of algebraic geometry and allows us to apply algebraic tools to geometric problems.

Definition 2.1.15. For S-schemes $X/S,\ Y/S$, the **fibre product of X and Y over S** in **Sch** is a scheme $X \times_S Y$ together with morphisms

$$X \times_S Y \to X,$$
$$X \times_S Y \to Y,$$

such that the diagram below commutes.

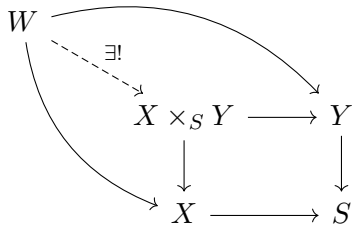

Figure 2.2: The fibre product $X \times_S Y$

This satisfies the universal property that for any scheme W with morphisms $W \to X$, $W \to Y$, there is a unique morphism $W \to X \times_S Y$. Note that this can also be viewed as the product of X/S and Y/S in $\mathbf{Sch}/S$.

If X, Y are two schemes with a morphism $f : Y \to X$, we can take the fibre product of Y with itself over X and denote this $Y \times_X Y$. In this situation the diagonal subscheme can be defined.

Definition 2.1.16. The **diagonal embedding** $\Delta : Y \hookrightarrow Y \times_X Y$ is the unique morphism such that $p_i \circ \Delta = \mathrm{id}_Y$, where p_i denotes the projection maps for $i = 1, 2$.
The **diagonal subscheme**, $\Delta_Y \subseteq Y \times_X Y$, is the subscheme defined as the image of Δ.

Definition 2.1.17. Let X be defined over a field F and let F'/F be a field extension. Then the **base change of X to F'**, denoted $X_{F'}$, is the fibre product $X \times_{\mathrm{Spec}(F)} \mathrm{Spec}(F')$. By abuse of notation this is sometimes written as $X \times_F F'$.

The fibre product construction can also be used to describe fibres of morphisms using rational points.

Definition 2.1.18. Let $f : Y \to X$ be a morphism of schemes and let $x : \mathrm{Spec}(F) \to X$ be an F-rational point of X. The **fibre of f over** x is the fibre product $Y_x = Y \times_X \mathrm{Spec}(F)$ constructed as shown in the diagram below.

$$\begin{array}{ccc} Y_x & \longrightarrow & Y \\ \downarrow & & \downarrow f \\ \mathrm{Spec}(F) & \xrightarrow{x} & X \end{array}$$

Figure 2.3: The fibre of $f : Y \to X$ over x

We conclude this section with the notion of a residue field and its relation to rational points.

Definition 2.1.19. The **residue field** at a point $x \in X$, denoted $\kappa(x)$, is the field obtained by taking the quotient of the stalk at x by its maximal ideal, i.e. $\kappa(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$.
In the case of an affine scheme $\mathrm{Spec}(R)$, the residue field at a point $x \in X$ corresponding to prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ is:

$$\kappa(x) \;=\; \mathrm{Frac}(R/\mathfrak{p}) \;\cong\; R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

For an affine scheme X and for any scheme-theoretic point $x \in X$ we can associate a

corresponding morphism $\mathrm{Spec}(\kappa(x)) \to X$ in the following way. By the definition of the stalk at the point x, we get an induced morphism:

$$\mathcal{O}_X(X) \longrightarrow \mathcal{O}_{X,x} \longrightarrow \kappa(x).$$

By the anti-equivalence of categories given by the Spec and global sections functors this gives a morphism $\mathrm{Spec}(\kappa(x)) \to \mathrm{Spec}(\mathcal{O}_X(X)) = X$.

Lemma 2.1.20. *Let $f : Y \to X$ be a morphism of schemes and let $y \in Y$. Then $\kappa(y)$ is a field extension of $\kappa(f(y))$.*

Proof. The sheaf morphism $f^\#$ induces a morphism of stalks $f^\#_y : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$. Since this a local map, we can quotient out by the maximal ideals on both sides to obtain a morphism $\kappa(f(y)) \to \kappa(y)$. This is injective as it is a field homomorphism so we conclude that $\kappa(y)$ is an extension of $\kappa(f(y))$. □

Definition 2.1.21. Let X be a scheme, let a be an F-rational point of X and let x be a scheme-theoretic point of X. Then a **is located at** x if x is the image of the morphism $a : \mathrm{Spec}(F) \to X$.

Note that there may be several F-rational points located at the same scheme-theoretic point.

If a scheme X is defined over a field F then we can apply Lemma 2.1.20 to see that for any $x \in X$, $\kappa(x)$ is an extension of F. Here it is used that $\mathrm{Spec}(F)$ only has one scheme-theoretic point, $*$, and $\kappa(*) = \mathrm{Frac}(F/*) = F$.
Alternatively for an arbitrary scheme X if there exists $a \in X(F)$ located at $x \in X$, then by Lemma 2.1.20 F is a field extension of $\kappa(x)$ and hence we obtain a morphism $\mathrm{Spec}(F) \to \mathrm{Spec}(\kappa(x))$. Therefore any F-rational point factors through a scheme-theoretic point.

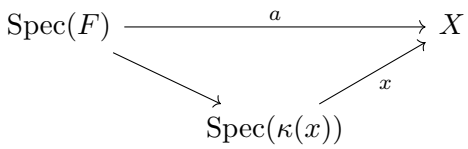

Figure 2.4: An F-rational point factoring through a scheme-theoretic point

Combining these two situations let X be defined over F, let $a \in X(F)$ and let $x \in X$ be the image of a. Then $\kappa(x) = F$ and a is the unique F-rational point located at x.

2.2 Properties of schemes

Now that we have the basics of scheme theory, we discuss several useful properties.

Definition 2.2.1. A scheme X is **reduced** if for every open set $U \subseteq X$, its associated ring $\mathcal{O}_X(U)$ is reduced, i.e. it has no non-zero nilpotent elements. Equivalently a scheme X is reduced if for every $x \in X$, the stalk $\mathcal{O}_{X,x}$ is reduced.

Definition 2.2.2. A scheme X is **irreducible** (resp. **connected**) if its underlying topological space is irreducible (resp. connected). This implies that irreducible schemes are connected.

A scheme X/F is **geometrically irreducible** (resp. **geometrically connected**) if X is irreducible (resp. connected) under any base change, i.e. for any field extension F'/F, the scheme $X_{F'} = X \times_F F'$ is irreducible (resp. connected). Equivalently X is geometrically irreducible if $X_{\bar{F}}$ is irreducible where $\bar{F}$ denotes the algebraic closure of F.

An **irreducible** (resp. **connected**) **component** of a scheme X is a maximal irreducible (resp. connected) subset of X. A scheme can therefore be described uniquely as a union of its irreducible (resp. connected) components.

Note that connected components are disjoint but irreducible components are not necessarily so. However we cannot always describe a scheme X as a coproduct of its connected components as each component is closed but not necessarily open. Spaces where each connected component is open are called **locally connected**; spaces where each point has an irreducible neighbourhood are called **locally irreducible**.

We can consider the **connected components functor**,

$$\pi_0 : \mathbf{Sch} \to \mathbf{Set},$$

which takes a scheme and produces its set of connected components. By slight abuse of

notation we will also apply π_0 to rings and algebras, letting $\pi_0(R)$ mean $\pi_0(\mathrm{Spec}(R))$.

Definition 2.2.3. The **dimension**, d, of a scheme $(X, \mathcal{O}_X)$ is the dimension of its underlying topological space X. Explicitly this is the supremum of all lengths l such that there exists a chain of distinct irreducible closed subsets:

$$\emptyset \neq X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_l \subseteq X.$$

Definition 2.2.4. A scheme X is **integral** if for every open set $U \subseteq X$, its associated ring $\mathcal{O}_X(U)$ is an integral domain. Equivalently a scheme X is integral if it is both reduced and irreducible.

Definition 2.2.5. A scheme X is **normal** if for every $x \in X$, the stalk $\mathcal{O}_{X,x}$ is an integrally closed domain, i.e. $\mathcal{O}_{X,x}$ is an integral domain which is integrally closed in $\mathrm{Frac}(\mathcal{O}_{X,x})$.

Definition 2.2.6. A scheme X is **locally Noetherian** if it can be covered by open affine subsets $\mathrm{Spec}(A_i)$, where each A_i is a Noetherian ring.
A scheme X is **Noetherian** if it can be covered by finitely many $\mathrm{Spec}(A_i)$, where each A_i is Noetherian; therefore X is Noetherian if it is locally Noetherian and quasi-compact.

Proposition 2.2.7. *A Noetherian scheme X has finitely many irreducible components.*

Proof. It is known that a Noetherian topological space has finitely many irreducible components ([Lan02], IX, Thm 5.3). Since the spectrum of a Noetherian ring is a Noetherian topological space and X can be covered by finitely many of these, the result follows. □

We draw attention to the fact that a Noetherian normal scheme is locally irreducible and hence its connected and irreducible components coincide ([GD71], Section 0.2.1.6). We will therefore use these terms interchangeably when we are in this setting.

We will mainly be concerned with morphisms of schemes and will require the following properties.

Definition 2.2.8. A morphism $f : Y \to X$ is **finite** if there exists an open affine covering $\{V_i = \mathrm{Spec}(B_i)\}$ of X such that for all i, $f^{-1}(V_i) = \mathrm{Spec}(A_i)$ where each A_i is a B_i-algebra which is finitely generated as a B_i-module.

A morphism $f : Y \to X$ is **locally of finite type** if there exists an open affine covering $\{V_i = \mathrm{Spec}(B_i)\}$ of X such that for all i, $f^{-1}(V_i)$ has an open affine covering $\{U_{ij} = \mathrm{Spec}(A_{ij})\}$ where each A_{ij} is finitely generated as a B_i-algebra.

A morphism $f : Y \to X$ is **of finite type** if every $f^{-1}(V_i)$ can be covered by finitely many U_{ij}; therefore f is of finite type if it is locally of finite type and quasi-compact.

A morphism $f : Y \to X$ is **quasifinite** if it is locally of finite type and if for all $x \in X$, the fibre $f^{-1}(x)$ is a finite set.

Definition 2.2.9. A morphism $f : Y \to X$ is **separated** if the diagonal embedding $\Delta : Y \hookrightarrow Y \times_X Y$ is a closed immersion.

This provides an algebraic analogue of the Hausdorff property.

Definition 2.2.10. A morphism $f : Y \to X$ is **flat** if for every $y \in Y$, the induced map of stalks $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is a flat ring homomorphism. Recall that a ring homomorphism $\phi : R \to S$ is flat if S is a flat R-module, i.e. if the functor $- \otimes_R S$ preserves exact sequences.

A morphism $f : Y \to X$ is **faithfully flat** if it is both flat and surjective.

Flatness captures the idea of having a "continuously varying" family of fibres where all fibres of the morphism have the same dimension.

Definition 2.2.11. A morphism $f : Y \to X$ is **unramified** if for every $y \in Y$:

$$\mathfrak{m}_{f(y)} \cdot \mathcal{O}_{Y,y} = \mathfrak{m}_y,$$

where $\mathfrak{m}_{f(y)}$ is the maximal ideal of the local ring $\mathcal{O}_{X,f(y)}$, and the residue field extension $\kappa(f(y)) \to \kappa(y)$ is finite and separable.
This definition corresponds to the notion of ramification of prime ideals in algebraic number theory, with the idea that there are no points $x \in X$ such that the fibre Y_x has repeated points.

Definition 2.2.12. A morphism $f : Y \to X$ is **étale** if it is flat and unramified.
A morphism $f : Y \to X$ is **generically étale** if the morphism $f^{-1}(\eta_X) \to \{\eta_X\}$ is étale.
Combining the intuition for flat and unramified morphisms, we see that the definition for étale morphisms provides an analogy to topological covering spaces.

Definition 2.2.13. A morphism $f : Y \to X$ is a **finite étale cover of** X if it is finite and étale. Some authors also require surjectivity, although this is not strictly necessary.

We now see that finite étale covers are preserved under composition and base change. Let $\mathcal{P}$ denote a property of a morphism of schemes.

Definition 2.2.14. A property $\mathcal{P}$ is **preserved under composition** if for any two morphisms $f : Y \to X$ and $g : Z \to Y$ which both satisfy $\mathcal{P}$, their composite $g \circ f : Z \to X$ also satisfies $\mathcal{P}$.
A property $\mathcal{P}$ is **preserved under base change** if for a morphism $f : Y \to X$ satisfying $\mathcal{P}$ and any other morphism $f' : Z \to X$, the base change morphism $Z \times_X Y \to Z$ also satisfies $\mathcal{P}$.

Proposition 2.2.15. *The properties of étaleness and finiteness are preserved under both composition and base change.*

Proposition 2.2.16. *A morphism of étale covers is again étale, i.e. if $Y \to X$, $Z \to X$ are étale then a morphism $Y \to Z$ over X is also étale.*

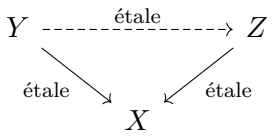

Figure 2.5: Morphisms of étale covers are étale

The results about finiteness can easily be seen from the underlying rings and the results about étaleness can be found in Milne ([Mil80], I, Props 3.3 and 3.6).

The definition of a variety can be reimagined in this framework. Note that the following two definitions capture the same ideas as before but now come equipped with a much richer structure. Let F be a field which is not necessarily algebraically closed.

Definition 2.2.17. Affine n-space over F, $\mathbb{A}^n_F$, is the spectrum of the polynomial ring over F in n variables, i.e. $\mathbb{A}^n_F = \mathrm{Spec}(F[x_1, \ldots, x_n])$.

Definition 2.2.18. A **variety X over F**, denoted X/F, is an integral separated scheme of finite type over $\mathrm{Spec}(F)$.

Definition 2.2.19. Let X/F be a variety. The **function field of X**, denoted $K(X)$, is the stalk at the generic point η, i.e. $K(X) = \mathcal{O}_{X,\eta}$.

Elements of the function field are called rational functions and a substantial amount of geometric information about X is retained in $K(X)$.

Definition 2.2.20. Let X be a variety with function field K and let L be an algebraic field extension of K. The **normalisation of X in L** is the unique normal variety X_L together with an integral morphism $X_L \to X$ such that the function field of X is L.

Proof of existence and uniqueness of X_L can be found in Liu ([Liu02], Prop 1.22). Note that if X is a normal variety then the normalisation of X in its function field K is X itself.

We conclude this section with a useful result on counting rational points of varieties defined over finite fields, which follows from the Weil conjectures ([FK88], Chapter 2, Section 4). This is of particular interest as the definition of exceptionality involves bijections between sets of rational points.

Theorem 2.2.21 (Lang-Weil bound)**.** *Let X be a geometrically irreducible variety of dimension d defined over a finite field $\mathbb{F}_q$. Then there exist constants $C, c > 0$ depending only on the geometric data of X such that:*

$$\left||X(\mathbb{F}_q)| - cq^d\right| < Cq^{d-\frac{1}{2}}.$$

2.3 Galois covers

We will make particular use of Galois covers and their associated groups.

Definition 2.3.1. A scheme Z together with a morphism $\pi : Z \to X$ is a **Galois cover of** X if Z is connected, π is a finite étale cover and the automorphism group $\mathrm{Aut}_X(Z)$ acts transitively on geometric fibres.
Here $\mathrm{Aut}_X(Z)$ denotes the group of scheme automorphisms of Z which preserve π; it is referred to as the **Galois group of** Z/X and is denoted $\mathrm{Gal}(Z/X)$. For any geometric point $\bar{x} \in X(\Omega)$ this group acts on a geometric fibre $Z_{\bar{x}}$ via its action on Z.

Definition 2.3.2. Let $\pi : Z \to X$ be a Galois cover and let $z \in Z$, $x \in X$ such that $\pi(z) = x$. The **decomposition group of** z, denoted $D_{Z/X}(z)$, is the stabiliser of z in $\mathrm{Gal}(Z/X)$, i.e.

$$D_{Z/X}(z) = \{d \in \mathrm{Gal}(Z/X) \mid d \cdot z = z\}.$$

The **inertia group of** z, denoted $I_{Z/X}(z)$, is the kernel of the morphism:

$$D_{Z/X}(z) \to \mathrm{Gal}\left(\kappa(z)/\kappa(x)\right).$$

Let X, Y be varieties and let $f : Y \to X$ be a finite étale morphism. We can construct a finite étale cover of Y which is a Galois cover of X. This is achieved by a theorem attributed to Serre ([Sza09], Prop 5.3.9).

Theorem 2.3.3. *Let $f : Y \to X$ be a finite étale cover of a connected scheme X. Then there exists a morphism $p : Z \to Y$ such that $\pi := f \circ p : Z \to X$ is a Galois cover.*
Moreover if $\pi' : Z' \to X$ is another Galois cover with a morphism $p' : Z' \to Y$, then p'

factors through Z.

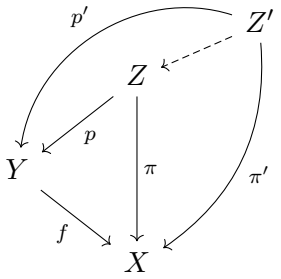

Figure 2.6: Construction of a Galois cover Z

Definition 2.3.4. Let $f : Y \to X$ be a finite étale cover of a connected scheme X. The **Galois closure** of $f : Y \to X$ is the Galois cover Z as constructed in Theorem 2.3.3. By the universal property Z is unique up to a unique isomorphism.

In the case of normal varieties we can also construct the Galois closure via normalisation. Let X, Y be normal varieties with function fields K, L respectively and note that a finite étale cover $Y \to X$ induces a finite separable field extension $K \hookrightarrow L$. Construct the Galois closure of L/K, denoted M, and then define the Galois closure Z to be the normalisation of X in M (Definition 2.2.20).
In this setting X is the normalisation of itself in K and Y is the normalisation of X in L. This allows us to transition between the geometric setup and function field extensions without losing information.

2.4 Galois categories

We describe a general Galois correspondence and illustate it through the example of the category of finite étale covers. This material is originally taken from Grothendieck's SGA1 notes [Gro63] with reference to expository notes by Cadoret [Cad13].

2.4.1 Grothendieck's theory

We first define a Galois category and related notions. Let $\mathcal{C}$ denote a category and let **FSet** denote the category of finite sets. For objects $Y, Z \in \mathcal{C}$, let $\mathrm{Hom}_{\mathcal{C}}(Y, Z)$ denote the set of morphisms from Y to Z in $\mathcal{C}$ and let $\mathrm{Aut}_{\mathcal{C}}(Y)$ denote the group of automorphisms of Y in $\mathcal{C}$.

Definition 2.4.1. A morphism $u \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ is a **strict epimorphism** if the following two conditions hold:

(i) The fibre product $Y \times_Z Y$ with respect to u exists in $\mathcal{C}$;

(ii) Let p_i denote the i^{th} projection $Y \times_Z Y \to Y$ for $i = 1, 2$. Then for any object $Z' \in \mathcal{C}$, the map $- \circ u : \mathrm{Hom}_{\mathcal{C}}(Z, Z') \to \mathrm{Hom}_{\mathcal{C}}(Y, Z')$ is injective and induces a bijection onto the set of all morphisms $\psi \in \mathrm{Hom}_{\mathcal{C}}(Y, Z')$ such that $\psi \circ p_1 = \psi \circ p_2$. This is illustrated in the figure below.

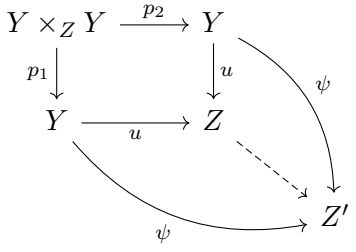

Figure 2.7: A strict epimorphism

Definition 2.4.2. A category $\mathcal{C}$ is a **Galois category** if there exists a covariant functor

$F : \mathcal{C} \to \mathbf{FSet}$ such that the following axioms are satisfied:

(i) $\mathcal{C}$ has a final object $e_{\mathcal{C}}$ and finite fibre products exist in $\mathcal{C}$;

(ii) Finite coproducts exist in $\mathcal{C}$ and categorical quotients by finite groups of automorphisms exist in $\mathcal{C}$;

(iii) Every morphism $u \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ factors as $Y \xrightarrow{u'} Z' \xrightarrow{u''} Z$, where u' is a strict epimorphism and u'' is a monomorphism which is an isomorphism onto a direct summand of Z;

(iv) F sends final objects to final objects and commutes with fibre products;

(v) F commutes with finite coproducts and categorical quotients by finite groups of automorphisms, and sends strict epimorphisms to strict epimorphisms;

(vi) For $u \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, u is an isomorphism if and only if $F(u)$ is an isomorphism.

Definition 2.4.3. Let $\mathcal{C}$ be a Galois category. A functor $F : \mathcal{C} \to \mathbf{FSet}$ satisfying axioms (iv), (v), (vi) is called a **fibre functor for** $\mathcal{C}$. Note that there may be many valid fibre functors associated to a Galois category; for this reason we sometimes denote a Galois category by $(\mathcal{C}, F)$.
Given a Galois category $(\mathcal{C}, F)$ the **fundamental group of** $\mathcal{C}$ **with base point** F, denoted $\pi_1 = \pi_1(\mathcal{C}, F)$, is the automorphism group of F.

Theorem 2.4.4 (Grothendieck's Galois Correspondence)**.** *Let* $\mathcal{C}$ *be a Galois category. Then any fibre functor* F *induces an equivalence of categories* $\mathcal{C} \to \pi_1$**-Set**, *where* π_1**-Set** *denotes the category of finite discrete sets with continuous left* π_1*-action.*

We briefly summarise the proof, which takes advantage of useful properties of morphisms to and from connected objects in $\mathcal{C}$. A connected object Y_0 is a Galois object if $\mathrm{Aut}_{\mathcal{C}}(Y_0)$

acts transitively on $F(Y_0)$ and it is shown that a Galois closure can always be constructed for any connected object.

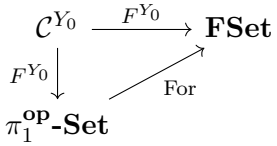

Figure 2.8: Factorisation of fibre functor F^{Y_0} through an equivalence of categories

The fibre functor F is restricted to $F^{Y_0} = F\restriction_{\mathcal{C}^{Y_0}}$, where $\mathcal{C}^{Y_0}$ is the full subcategory consisting of $Y \in \mathcal{C}$ such that there exists a morphism from Y_0 to any connected component of Y. A functor isomorphism is obtained between F^{Y_0} and $\mathrm{Hom}_{\mathcal{C}}(Y_0, -)\restriction_{\mathcal{C}^{Y_0}}$, which gives a factorisation through an equivalence of categories. In the diagram above For denotes the forgetful functor.

The final result is reached by showing that F is strictly pro-representable, i.e. there exists a functor isomorphism between F and $\mathrm{Hom}_{\mathrm{Pro}(\mathcal{C})}(\underline{Y}, -)\restriction_{\mathcal{C}}$, where $\mathrm{Pro}(\mathcal{C})$ is the category whose objects are projective systems with epimorphisms, $\underline{Y}$, in $\mathcal{C}$. A full exposition of the theory underpinning this proof can be found in Cadoret ([Cad13], Section 3).

2.4.2 The category of finite étale covers

It is therefore possible to study a Galois category by looking at the category of finite sets with a continuous action of its associated fundamental group. A classical application of this is to finite étale covers of connected schemes.

Definition 2.4.5. Let X be a connected scheme. The **category of finite étale covers of** X, $\mathbf{F\acute{E}t}_X$, consists of the following objects and morphisms:

- An object is a scheme Y together with a finite étale cover $\phi : Y \to X$;
- For two objects $\phi : Y \to X,\ \psi : Z \to X$, a morphism $u : Y \to Z$ is a morphism of

schemes such that $\phi = \psi \circ u$. By Proposition 2.2.16 u is also étale.

Before it can be verified that $\mathbf{F\acute{E}t}_X$ is a Galois category, a few results and definitions need to be collected. This theorem, originally by Grothendieck, can be found in Milne ([Mil80], Thm 2.17).

Theorem 2.4.6. *Let $u' : Y \to Z'$ be a faithfully flat morphism of schemes of finite type. Then u' is a strict epimorphism.*

The following useful results can be found in Cadoret's exposition ([Cad13], Lemmas 5.6 and 5.12).

Lemma 2.4.7. *If $\mathcal{P}$ is a property of morphisms of schemes which is preserved under composition and arbitrary base change, then $\mathcal{P}$ is preserved under fibre products.*
In particular this holds when $\mathcal{P}$ is the property of being étale (see Prop 2.2.15).

Lemma 2.4.8. *Categorical quotients by finite groups of automorphisms exist in $\mathbf{F\acute{E}t}_X$.*

Definition 2.4.9. For an étale cover $\phi : Y \to X$ the **rank function** $r : X \to \mathbb{Z}_{\geq 0}$ is defined as $r(\phi) = |Y_{\bar{x}}|$, where $\bar{x}$ is a geometric point in X. This is well-defined as all geometric fibres of étale morphisms have the same cardinality.

Proposition 2.4.10. *Let X be a connected scheme and let $\bar{x} \in X(\Omega)$ be a geometric point. Then $\mathbf{F\acute{E}t}_X$ is a Galois category with fibre functor:*

$$\begin{array}{rccc} F_{\bar{x}} : & \boldsymbol{F\acute{E}t}_X & \longrightarrow & \boldsymbol{FSet} \\ & (\phi : Y \to X) & \longmapsto & \lfloor Y_{\bar{x}} \rfloor, \end{array}$$

where $\lfloor Y_{\bar{x}} \rfloor$ is the underlying set of the fibre product scheme constructed from ϕ and $\bar{x}$.

Proof. The six axioms of a Galois category in Definition 2.4.2 must be verified.

(i) The final object is $\mathrm{id}_X : X \to X$ and by Lemma 2.4.7 fibre products exist.

(ii) Lemma 2.4.8 tells us that categorical quotients by finite groups of automorphisms exist. Finite coproducts of schemes are given by disjoint unions where the structure morphism down to X restricts to the finite étale morphism associated to its respective component, so finite coproducts of étale covers are again étale.

(iii) Let $u \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ and define $Z' := \mathrm{Im}(u) \subseteq Z$. Then $u' := u : Y \to Z'$ is faithfully flat (of finite type) and hence is a strict epimorphism by Theorem 2.4.6. We can therefore write $Z = Z' \sqcup (Z \setminus Z')$ and define $u'' : Z' \hookrightarrow Z$ as a monomorphism.

(iv) The final object in $\mathbf{F\acute{E}t}_X$ is id_X and the final object in **FSet** is the singleton $\{*\}$. For $\phi : Y \to X$, we have $F_{\bar{x}}(\phi) = \{*\}$ if and only if $r(\phi) = 1$ if and only if $\phi : Y \xrightarrow{\sim} X$ is an isomorphism. By considering fibre products of sets and using that $F_{\bar{x}}(X) = \{*\}$, it is clear that $F_{\bar{x}}$ commutes with fibre products, i.e.

$$F_{\bar{x}}(Y \times_X Z) \;\cong\; F_{\bar{x}}(Y) \times_{F_{\bar{x}}(X)} F_{\bar{x}}(Z).$$

(v) A strict epimorphism in **FSet** is a surjective map and coproducts are disjoint unions of finite sets. It is therefore clear that $F_{\bar{x}}$ maps strict epimorphisms to strict epimorphisms and commutes with coproducts. It follows that $F_{\bar{x}}$ commutes with categorical quotients by finite groups of automorphisms from the proof of Lemma 2.4.8.

(vi) By functoriality $F_{\bar{x}}$ preserves isomorphisms. Let $u \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ where $\phi : Y \to X$, $\psi : Z \to Y$ are étale covers. Assume $F_{\bar{x}}(u) : F_{\bar{x}}(\phi) \xrightarrow{\sim} F_{\bar{x}}(\psi)$ is an isomorphism. Then u is an étale cover and $r(u) = r(\phi)/r(\psi) = 1$, so u is also an isomorphism.

□

Definition 2.4.11. Let X be a scheme and let $\bar{x} \in X(\Omega)$ be a geometric point. The **étale fundamental group**, denoted $\pi_1(X, \bar{x})$, is the automorphism group of the fibre functor $F_{\bar{x}}$, i.e.

$$\pi_1(X, \bar{x}) \;\cong\; \mathrm{Aut}(F_{\bar{x}}).$$

We can also view the étale fundamental group in terms of Galois covers. Consider a projective system indexed by a directed set I:

$$\{Y_i \to Y_j \mid j < i\},$$

where each Y_i is a Galois cover of X. Then $\pi_1(X, \bar{x})$ is isomorphic to the inverse limit of the automorphism groups of this projective system, i.e.

$$\pi_1(X, \bar{x}) \;\cong\; \varprojlim_{i \in I} \mathrm{Aut}_X(Y_i).$$

Example 2.4.12. If $X = \mathrm{Spec}(F)$ for a field F, then:

$$\pi_1(X, \bar{x}) \cong \mathrm{Gal}(F^{\mathrm{sep}}/F).$$

In the case where X is a geometrically connected scheme over F, $\pi_1(X, \bar{x})$ fits into the short exact sequence:

$$1 \to \pi_1(X \times_F F^{\mathrm{sep}}, \bar{x}) \to \pi_1(X, \bar{x}) \to \mathrm{Gal}(F^{\mathrm{sep}}/F) \to 1.$$

Here $\pi_1(X \times_F F^{\mathrm{sep}}, \bar{x})$ is sometimes referred to as the **geometric fundamental group** and $\pi_1(X, \bar{x})$ as the **arithmetic fundamental group**.

The main result can now be applied to the Galois category $\mathbf{F\acute{E}t}_X$ using the étale fundamental group.

Theorem 2.4.13. *Let X be a connected scheme. There is a one-to-one correspondence between finite étale covers of X and finite sets with a $\pi_1(X, \bar{x})$-action.*

We can now restrict to connected objects by noting that connected objects in the category of π_1**-Set** are finite sets with a transitive group action.

Corollary 2.4.14. *There is a one-to-one correspondence between connected finite étale covers of a connected scheme X and finite sets with a transitive $\pi_1(X, \bar{x})$-action.*

Chapter 3

Exceptional covers of varieties

This chapter discusses a criterion for identifying exceptional covers of varieties. We begin by giving some background on exceptional polynomials, then we state the criterion and fully describe its setup. The exceptionality condition given in the criterion is examined and we explore its geometric and group-theoretic interpretations. The remainder of the chapter follows a proof of Fried [Fri74].

3.1 Permutation and exceptional polynomials

This section provides an overview of permutation and exceptional polynomials. Exceptional polynomials are of interest as they can be related to many areas of mathematics. Initially they were viewed in the context of Weil's bound for the number of solutions to an equation over a finite field [DL63]. This has since developed into broader geometric and group-theoretic connections which we discuss later in this thesis. Building on the applications to cryptography discussed in Subsection 1.1.2, they have also found relevance in finite geometry via the association of planar and perfect nonlinear functions [HMM14].

Let $\mathbb{F}_q$ be a finite field of characteristic p.

Definition 3.1.1. A polynomial $f \in \mathbb{F}_q[x]$ is a **permutation polynomial over** $\mathbb{F}_q$ if the function $f : \mathbb{F}_q \to \mathbb{F}_q$ mapping $a \mapsto f(a)$ is a bijection.

As mentioned in Subsection 1.1.2 an early result classifying permutation polynomials comes from Hermite and Dickson ([LN97], Thm 7.4).

Theorem 3.1.2 (Hermite's Criterion)**.** *A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if the following two conditions hold:*

(i) f has exactly one root in $\mathbb{F}_q$;

(ii) For all integers t such that $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction $f(x)^t \pmod{x^q - x}$ has degree $\leq q-2$.

The following example described by Matthews [Mat94] gives an idea of the type of conditions satisfied by permutation polynomials.

Example 3.1.3. Let q be odd. Then $f_t(x) = 1 + x + \cdots + x^t$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $t \equiv 1 \pmod{p(q-1)}$.

Definition 3.1.4. A polynomial $f \in \mathbb{F}_q[x]$ is an **exceptional polynomial over** $\mathbb{F}_q$ if f is a permutation polynomial over $\mathbb{F}_{q^m}$ for infinitely many extensions $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$.

Note that the definition of exceptionality does not require bijectivity on *all* extensions but on infinitely many.

Proposition 3.1.5. *Let $f \in \mathbb{F}_q[x]$. If f induces a bijection on some extension $\mathbb{F}_{q^m}$, then f induces a bijection on $\mathbb{F}_q$. Therefore if f is an exceptional polynomial over $\mathbb{F}_q$, then f is a permutation polynomial over $\mathbb{F}_q$.*

Proof. If f is bijective over some extension $\mathbb{F}_{q^m}$, then in particular f is injective on $\mathbb{F}_{q^m}$. All of the coefficients of f must be elements of $\mathbb{F}_q$ so $f(\mathbb{F}_q) \subseteq \mathbb{F}_q$. Hence f must also be surjective on $\mathbb{F}_q$. □

There have been attempts to classify the degrees of exceptional polynomials. This began in 1966 with a well-known conjecture of Carlitz ([LM93], P9), which states that if p is odd then the degree of an exceptional polynomial over $\mathbb{F}_q$ must be odd. Wan then proposed a generalisation which was later proved by Lenstra in 1995 [CF95].

Theorem 3.1.6 (Carlitz-Wan Conjecture)**.** *Let* $\gcd(d, q-1) > 1$. *Then there are no exceptional polynomials of degree* d *over* $\mathbb{F}_q$.

There are three standard examples of exceptional polynomials. These are all indecomposable and can be used as building blocks to create further examples ([Zie13], Theorem 8.4.11).

Definition 3.1.7. A polynomial $f \in \mathbb{F}_q[x]$ is **indecomposable** if it cannot be expressed as the composition $f = g \circ h$ of two nonlinear polynomials for $g, h \in \mathbb{F}_q[x]$.

Theorem 3.1.8. *The indecomposable exceptional polynomials over* $\mathbb{F}_q$ *of degree coprime to* q *are precisely the polynomials of the form* $l_1 \circ f \circ l_2$, *where* $l_1, l_2 \in \mathbb{F}_q[x]$ *are linear and* f *takes one of the following forms:*

1. $f(x) = ax + b$, *where* $a \in \mathbb{F}_q^\times$ *and* $b \in \mathbb{F}_q$;
2. $f(x) = x^n$, *where* n *is a prime which does not divide* $q - 1$;
3. $f(x) = D_n(x, a)$, *where* $a \in \mathbb{F}_q^\times$, n *is a prime which does not divide* $q^2 - 1$ *and:*

$$D_n(x,a) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{n} (-a)^i x^{n-2i}.$$

We now describe a criterion for identifying exceptional polynomials over finite fields, although we note that some authors choose to take this as a definition for exceptionality.

Definition 3.1.9. A polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ is **absolutely irreducible** if it is irreducible in $\overline{\mathbb{F}}_p[x, y]$, where $\overline{\mathbb{F}}_p$ denotes the algebraic closure of $\mathbb{F}_p$.

Theorem 3.1.10 (Exceptionality Criterion for Polynomials)**.** *A polynomial $f \in \mathbb{F}_q[x]$ is an exceptional polynomial over $\mathbb{F}_q$ if and only if the only absolutely irreducible factor of $f(x) - f(y)$ defined over $\mathbb{F}_q[x, y]$ is of the form $x - y$.*

Proof. The 'only if' direction can be proved by contradiction using the Lang-Weil bound. This argument can be found at the end of Section 3.4 in a more general form (see page 62). The 'if' direction is proved in two stages. Firstly it is shown that if the condition on absolutely irreducible factors holds, then f is a permutation polynomial over $\mathbb{F}_q$. This was first conjectured by Davenport and Lewis in 1963 [DL63] and was proved by MacCluer in 1966 for the case where $\deg(f) < 2p$ [Mac67]. A proof for the general result with no restrictions on the degree of f was given by Cohen in 1970 [Coh70].
It remains to prove that f is not just a permutation polynomial but is in fact exceptional. Express $f(x) - f(y)$ as the product of its absolutely irreducible factors over $\overline{\mathbb{F}}_p$:

$$f(x) - f(y) \;=\; (x - y) \prod_{i=1}^{r} g_i(x, y),$$

where $(x - y)$ is defined over $\mathbb{F}_q$ and each g_i is defined over a finite extension of $\mathbb{F}_q$. Let $\mathbb{F}_{q^s}$ be the smallest extension such that every g_i is defined over $\mathbb{F}_{q^s}$.
Let m be an integer such that $\gcd(m, s) = 1$ and hence $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^s} = \mathbb{F}_q$. Therefore $x - y$ remains the only absolutely irreducible factor defined over $\mathbb{F}_{q^m}$. Due to the infinitude of primes there are infinitely many m which are coprime to the fixed integer s, and so f is exceptional over $\mathbb{F}_q$. □

3.2 An exceptionality criterion for varieties

The definition of exceptionality can be adapted to the setting of varieties over finite fields by considering rational points over finite fields. This ensures that the bijectivity condition can be mirrored. These results can be found in Fried ([Fri74], Thm 1) and Lidl-Niederreiter ([LN97], Chapter 7, Section 4).
From now on let k denote a finite field, let $\bar{k}$ denote its algebraic closure and let k_m denote the finite extension of k of degree m.

Definition 3.2.1. The automorphism $\varphi_k : \bar{k} \to \bar{k}$ is a power of the Frobenius sending elements to their $|k|^{\text{th}}$ power.

Example 3.2.2. Let $k = \mathbb{F}_p$ and consider φ_k acting on $\overline{\mathbb{F}}_p$. Then φ_k sends all elements to their p^{th} power and fixes $\mathbb{F}_p$.

Definition 3.2.3. Let X, Y be varieties over k and let $f : Y \to X$ be a morphism of k-varieties. Then f is an **exceptional cover** if $f : Y(k_m) \to X(k_m)$ is a bijection for infinitely many extensions k_m of k.

We now state the main results of this chapter.

Theorem 3.2.4. *Let X, Y be normal, geometrically irreducible varieties over k and let $f : Y \to X$ be a quasifinite, generically étale k-morphism. If Δ_Y is the only geometrically irreducible component of $Y \times_X Y$ which is defined over k, then $f : Y(k) \to X(k)$ is surjective.*

Corollary 3.2.5 (Exceptionality Criterion for Varieties)**.** *Assume the same setup as Theorem 3.2.4 and assume that $X = Y$. Then $f : X \to X$ is an exceptional cover if and only if Δ_X is the only geometrically irreducible component of $X \times_X X$ which is defined over k.*

We now set up the situation including a full discussion of its associated function field

diagram. Recall that X, Y be normal, geometrically irreducible varieties over k and that $f : Y \to X$ be a quasifinite, generically étale k-morphism.

Let Z denote the Galois closure of f as constructed in Theorem 2.3.3. Define $\widehat{k}$ to be the relative algebraic closure of k in the function field of Z, i.e. $\widehat{k} = \bar{k} \cap K(Z)$. We can then define $\widehat{X}, \widehat{Y}$ to be the base changes of X, Y to $\widehat{k}$ respectively, i.e.

$$\widehat{X} \;=\; X \times_k \widehat{k}, \qquad \widehat{Y} \;=\; Y \times_k \widehat{k}.$$

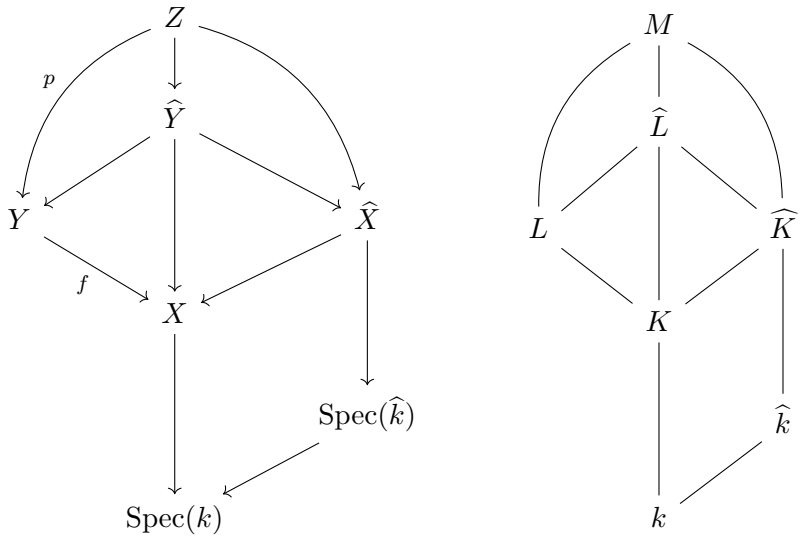

Figure 3.1: Setup of varieties and function fields

Let $K, L, \widehat{K}, \widehat{L}, M$ denote the function fields of $X, Y, \widehat{X}, \widehat{Y}, Z$ respectively. The diagram on the left shows the setup of varieties and the diagram on the right shows the corresponding function fields.

Definition 3.2.6. A field extension K/k is a **regular extension** if it is separable and k is algebraically closed in K, or equivalently if K is linearly disjoint from $\bar{k}$ over k.

We first note that as X is geometrically irreducible over k, the field extension K/k is regular ([FJ08], Cor 10.2.2). By linear disjointness we conclude that $K \otimes_k \widehat{k}$ is a field and:

$$\widehat{K} = K \otimes_k \widehat{k} \;\cong\; K\widehat{k}.$$

Similarly Y is also geometrically irreducible over k, so L/k is regular and we see that:

$$\widehat{L} = L \otimes_k \widehat{k} \;\cong\; L\widehat{k}.$$

By a change of base ([Con], Thm 6.14) we conclude $\widehat{L} \cong L\widehat{K}$.

By assumption L/K is finite, so we know by construction that M/K (and hence also M/L, $M/\widehat{K}$, $M/\widehat{L}$) are finite Galois. We now consider the extension $\widehat{K}/K$.

Lemma 3.2.7. *Assume the setup described in Figure 3.1. Then $\widehat{K}/K$ is Galois and* $\mathrm{Gal}(\widehat{K}/K) \cong \mathrm{Gal}(\widehat{k}/k)$.

Proof. We have already seen that $\widehat{K} \cong K\widehat{k}$, so $\widehat{K}/K$ is Galois as this property is preserved under base change to the compositum. Define the following morphism:

$$\begin{array}{ccc} \mathrm{Gal}(\widehat{K}/K) & \longrightarrow & \mathrm{Gal}(\widehat{k}/k) \\ g & \longmapsto & g{\restriction}_{\widehat{k}}\ , \end{array}$$

where $g{\restriction}_{\widehat{k}}$ is an embedding of $\widehat{k}$ over k and hence is an element of $\mathrm{Gal}(\widehat{k}/k)$. If $g{\restriction}_{\widehat{k}} = \mathrm{id}_{\widehat{k}}$ then since $g{\restriction}_K = \mathrm{id}_K$ we must have $g = \mathrm{id}_{\widehat{K}}$. Therefore the map is injective.
Let $H \subseteq \mathrm{Gal}(\widehat{k}/k)$ denote the image of this restriction morphism and we claim that the fixed field of H is $K \cap \widehat{k} = k$. Clearly any element in H will fix $K \cap \widehat{k}$. Conversely if $\lambda \in \widehat{k}$ is fixed by H then λ must be fixed by $\mathrm{Gal}(\widehat{K}/K)$. Therefore $\lambda \in K$ and hence $\lambda \in K \cap \widehat{k}$. As $\widehat{k}/k$ is finite we conclude that $H = \mathrm{Gal}(\widehat{k}/k)$. □

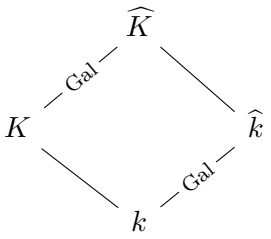

Figure 3.2: Galois extensions inside $\widehat{K}/k$

The extension $\widehat{K}/K$ is finite as it is contained in a finite extension, so the Galois group $\mathrm{Gal}(\widehat{K}/K) \cong \mathrm{Gal}(\widehat{k}/k)$ is cyclic and is generated by the Frobenius morphism φ_k. We therefore have the short exact sequence:

$$1 \to \mathrm{Gal}\left(M/\widehat{K}\right) \to \mathrm{Gal}\left(M/K\right) \to \langle \varphi_k \rangle \to 1. \tag{3.1}$$

Note that $\widehat{k}$ is a finite field.

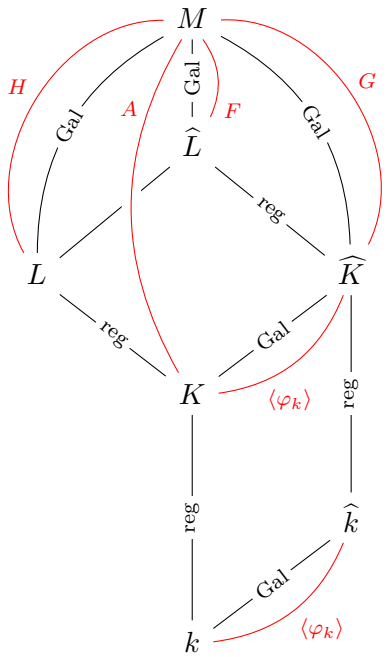

Figure 3.3: Full function field diagram

From now on we will denote $A = \mathrm{Gal}\,(M/K)$, $G = \mathrm{Gal}\,(M/\widehat{K})$, $H = \mathrm{Gal}\,(M/L)$, $F = \mathrm{Gal}\,(M/\widehat{L})$; we use the same group notation in both geometric and algebraic settings without confusion. The function field diagram is redrawn above highlighting this new information with associated Galois groups shown in red.

Since L is a finite separable extension of K, there is a primitive element $\alpha \in L$ which generates L over K. If the degree of L over K is l then there are l distinct roots of the minimal polynomial of α over K. However the extension is not assumed to be Galois so not every root is necessarily contained in L. This motivates the definition of conjugate fields and varieties.

Definition 3.2.8. Let L/K be a finite separable field extension of degree l and let $\alpha \in L$ such that $L = K(\alpha)$.

- Let $\mathcal{S} = \{\alpha_1 = \alpha, \ldots, \alpha_l\}$ denote the roots of the minimal polynomial of α over K.
- The set of **fields conjugate to L over K**, denoted $\{L_1 = L, \ldots, L_l\}$, is the set of fields obtained by adjoining different roots of the minimal polynomial of α to K, i.e. $L_i = K(\alpha_i)$.
  For each i, let $\widehat{L}_i := L_i\widehat{K}$ denote the base change of L_i to $\widehat{K}$.
- The set of **varieties conjugate to Y over X**, denoted $\{Y_1 = Y, \ldots, Y_l\}$, is the set of varieties associated to each conjugate field by normalisation.
  For each i, let $\widehat{Y}_i$ denote the variety associated to $\widehat{L}_i$.
- Since the Galois group A acts transitively on the set of roots $\mathcal{S}$, for each i let $a_i \in A$ such that $a_i \cdot \alpha = \alpha_i$. By slight abuse of notation we also let $a_i \cdot L = L_i$ and $a_i \cdot Y = Y_i$.
- For each i, let $H_i = \mathrm{Gal}(Z/Y_i)$ denote the Galois group associated to the conjugate variety Y_i. Then H_i and $H = H_1$ are conjugate subgroups of A and we can write

$H_i = a_i H a_i^{-1}$.

For each i, let $F_i = \mathrm{Gal}(M/\widehat{L}_i)$ denote the Galois group associated to the conjugate variety $\widehat{Y}_i$.

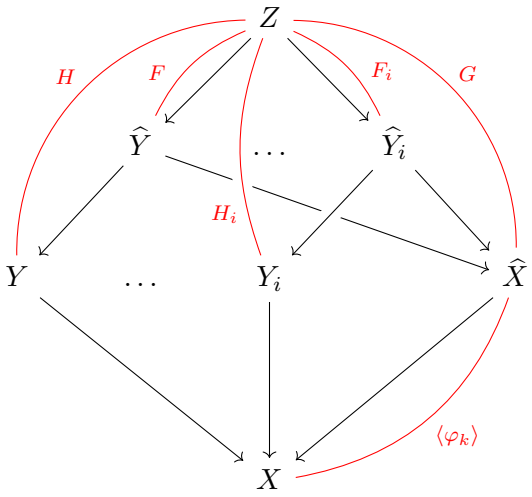

Figure 3.4: Conjugate varieties

3.3 The exceptionality condition

In this section we explore the exceptionality condition given in Theorem 3.2.4. Assume that Δ_Y is the only geometrically connected component of $Y \times_X Y$ which is defined over k. We first discuss a geometric interpretation of this condition before describing a group-theoretic formulation.

Consider the decomposition of $Y \times_X Y$ into all of its geometrically connected components. These are all defined over $\widehat{k}$ and Δ_Y is assumed to be the only one defined over k. An example of this type of behaviour is illustrated in the figure below: the connected components are expressed as $Y \times_X Y = \Delta_Y \cup \bigcup_{i=2}^{m} C_i$ and the geometrically connected components are expressed as $(Y \times_X Y)_{\widehat{k}} = \Delta_Y \cup \bigcup_{j=2}^{n} U_j$.

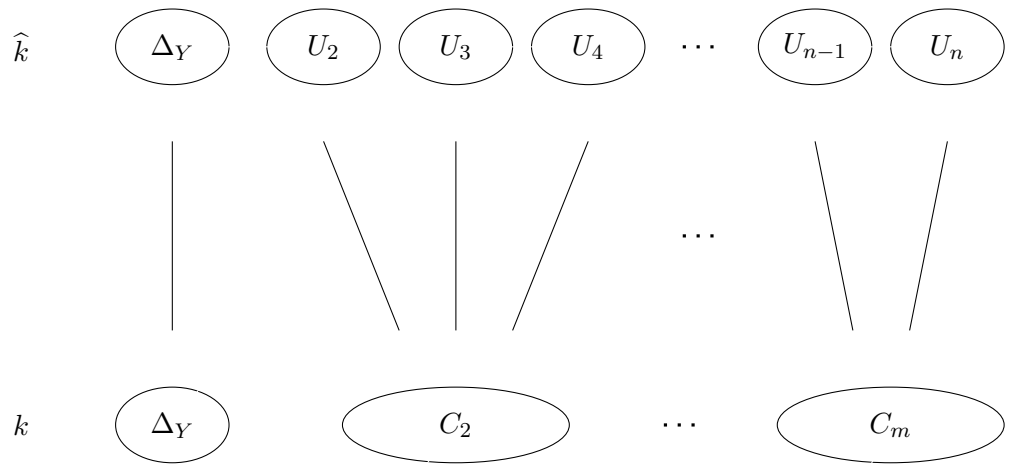

Figure 3.5: Geometrically connected components of $Y \times_X Y$

The Frobenius morphism φ_k induces a permutation of geometrically connected components. As φ_k generates $\mathrm{Gal}(\widehat{k}/k)$ this fixes only those components which are defined over k. The exceptionality condition therefore translates to stating that the only component which is fixed by this permutation is Δ_Y.

We next interpret the condition in terms of group orbits by recalling the category of finite étale covers from Subsection 2.4.2. Recall that A, G are the Galois groups of $Z/X, Z/Y$ respectively.

Lemma 3.3.1. *There is a one-to-one correspondence between connected (resp. geometrically connected) components of $Y \times_X Y$ and A-orbits (resp. G-orbits) of the set $\mathcal{S} \times \mathcal{S}$.*

Proof. Firstly note that if Y is a finite étale cover of X then by Proposition 2.2.15 $Y \times_X Y$ is also a finite étale cover of X. The fibre functor of the Galois category $\mathbf{F\acute{E}t}_X$ with respect to the basepoint $\bar{x} \in X(\bar{k})$ can be extended to the Cartesian product:

$$F_{\bar{x}}(Y \times_X Y) \;\cong\; \big(Y \times_X Y\big)_{\bar{x}}(\bar{k}) \;\cong\; Y_{\bar{x}}(\bar{k}) \times Y_{\bar{x}}(\bar{k}) \;\cong\; F_{\bar{x}}(Y) \times F_{\bar{x}}(Y).$$

As geometric points of $Y_{\bar{x}}$ correspond to k-algebra homomorphisms we can identify $Y_{\bar{x}}(\bar{k})$ with the set of roots $\mathcal{S}$. By applying Corollary 2.4.14 and noting that the action of A on $\mathcal{S} \times \mathcal{S}$ matches the action of $\pi_1(X, \bar{x})$, we have a correspondence between connected components of $Y \times_X Y$ and A-orbits of $\mathcal{S} \times \mathcal{S}$.
Geometrically connected components of $Y \times_X Y$ are connected components of $(Y \times_X Y)_{\bar{k}}$. Here these are all defined over $\widehat{k}$ and G matches the action of $\pi_1(\widehat{X}, \bar{x})$ on $\mathcal{S} \times \mathcal{S}$. We therefore see that there is a correspondence between geometrically connected components of $Y \times_X Y$ and G-orbits of $\mathcal{S} \times \mathcal{S}$. □

It follows that geometrically connected components which are defined over the base field k correspond to common orbits of A and G of the set $\mathcal{S} \times \mathcal{S}$. Since A acts transitively on $\mathcal{S}$ we can describe A-orbits of $\mathcal{S} \times \mathcal{S}$ by basepoints (α_1, α_i) for $i = 1, \ldots, l$, where (α_1, α_1) corresponds to the diagonal component Δ_Y. Note that two basepoints (α_1, α_i), (α_1, α_j) define the same orbit if there exists an element of the stabiliser subgroup $a \in A_{\alpha_1} = H$ such that $a \cdot \alpha_i = \alpha_j$. Therefore we can also think of A-orbits of $\mathcal{S} \times \mathcal{S}$ as H-orbits of $\mathcal{S}$.

An analogous argument shows that we can describe geometrically connected components as F-orbits of $\mathcal{S}$.
The exceptionality condition translates to saying that the orbit corresponding to (α_1, α_1) is the only common orbit of A and G of $\mathcal{S} \times \mathcal{S}$.

We take a short detour to discuss a further group theoretic reformulation of the exceptionality condition. This can be found in Fried-Guralnick-Saxl ([FGS93], Lemma 13.1) although we follow the proof in Guralnick-Tucker-Zieve ([GTZ07], Lemmas 4.2-4.3). We give a general group theoretic lemma and then apply this to the situation where there is a unique common orbit of A and G of $\mathcal{S} \times \mathcal{S}$.

Lemma 3.3.2. *Let A be a finite group acting on a finite set S. Let $G \lhd A$ be a normal subgroup such that A/G is cyclic and let $a \in A$ be such that $A/G = \langle aG \rangle$.*
Then the number of common orbits of A and G of S is:

$$\frac{1}{|G|} \sum_{\beta \in aG} |S^\beta|,$$

where S^β denotes the set of fixed points of β on S.

Proof. Consider A-orbits separately so we may assume A acts transitively on S. We claim that G acts transitively on S if and only if there exists some $g \in G$ such that ag has a fixed point in S.
Assume G acts transitively and let $s \in S$. Then $a \cdot s \in S$ and there exists $g \in G$ such that $g \cdot (a \cdot s) = s$. Then $a \cdot s = ag \cdot (a \cdot s)$ and so the element $a \cdot s$ is fixed by ag.
Conversely assume that ag has a fixed point $s \in S$ and consider the G-orbit $G \cdot s$. Recall that $\langle aG \rangle = A/G$ so any $b \in A$ can be written as $b = a^n \bar{g}$ for some $n \in \mathbb{N}$, $\bar{g} \in G$. Then by using that $ag \cdot s = s$ and that G is normal in A, it can be seen that $G \cdot s$ is also an A-orbit and hence G acts transitively.

Define:

$$\begin{aligned}\mathcal{V} &= \{(\beta, s) \in aG \times S \mid \beta \cdot s = s\},\\ A_s &= \{b \in A \mid b \cdot s = s\},\\ G_s &= \{g \in G \mid g \cdot s = s\}.\end{aligned}$$

Using the above G acts transitively on S if and only if $\mathcal{V}$ is non-empty. We aim to compute the cardinality of $\mathcal{V}$.

We claim that if $\beta \in aG$ satisfies $\beta \cdot s = s$, then $\beta G_s = A_s \cap aG$. Such a β exists based on our assumption of G acting transitively so let $\beta = ag'$ for some (fixed) $g' \in G$. Clearly $\beta G_s \subseteq A_s \cap aG$. Conversely let $ag \in aG$ such that $ag \cdot s = s$. Define $g'' = (g')^{-1}g$ and verify that $ag = ag'g'' = \beta g'' \in \beta G$. It remains to show that g'' fixes s. As both β and ag fix s, we see that:

$$g'' \cdot s \;=\; (g')^{-1}g \cdot s \;=\; (g')^{-1}a^{-1} \cdot s \;=\; (ag')^{-1} \cdot s \;=\; s,$$

and so $A_s \cap aG \subseteq \beta G_s$.

The cardinality of $\mathcal{V}$ can be calculated in two ways. On one hand:

$$\begin{aligned}|\mathcal{V}| &= |A_s \cap aG||S|\\ &= |\beta G_s||S|\\ &= |G_s||S| = |G|.\end{aligned}$$

Alternatively $|\mathcal{V}| = \sum_{\beta \in aG} |S^\beta|$. Equating these we find:

$$\frac{1}{|G|} \sum_{\beta \in aG} |S^\beta| \;=\; 1.$$

Since we assumed that both A and G act transitively the argument can be extended to give the number of common orbits of A and G on S. Let O denote an A-orbit in S and we can then express S as a disjoint union of these. Define:

$$\mathcal{V}_O = \{(\beta, s) \in aG \times O \mid \beta \cdot s = s\},$$

so $|\mathcal{V}_O| = |G|$ if G acts transitively on O and $|\mathcal{V}_O| = 0$ otherwise. Then:

$$\mathcal{V} = \bigsqcup_{O \subseteq S} \mathcal{V}_O,$$
$$|\mathcal{V}| = \sum_{O \subseteq S} |\mathcal{V}_O|,$$

and $|\mathcal{V}|/|G|$ counts the number of common orbits of A and G on S. □

This can be viewed as an adaptation of Burnside's Lemma, which gives the number of G-orbits on S as:

$$\frac{1}{|G|} \sum_{g \in G} |S^g|.$$

To count the number of common orbits of A and G, we see that the sum index must be shifted to the coset aG which satisfies $\langle aG \rangle = A/G$.
Apply this to our setting with Galois groups A, G acting on $\mathcal{S}$. In light of the short exact sequence (3.1), we see that $G \lhd A$ and $A/G \cong \langle \varphi_k \rangle$ is cyclic. We also note that G acts transitively on the set of roots $\mathcal{S}$.

Lemma 3.3.3. *Let A be a finite group acting transitively on a finite set $\mathcal{S}$. Let $G \lhd A$ be a normal subgroup such that A/G is cyclic and G acts transitively on $\mathcal{S}$. Let $a \in A$ be such that $\langle aG \rangle = A/G$. The following are equivalent:*

(1) The only common orbit of A and G on $\mathcal{S} \times \mathcal{S}$ is the diagonal;

(2) Every $\beta \in aG$ has a unique fixed point in $\mathcal{S}$;

(3) Every $\beta \in aG$ has at most one fixed point in $\mathcal{S}$;

(4) Every $\beta \in aG$ has at least one fixed point in $\mathcal{S}$.

Proof. This proof utilises the previous lemma. Clearly (2) implies both (3) and (4). As G acts transitively we see that $\frac{1}{|G|}\sum_{\beta \in aG} |S^\beta| = 1$.
Assume that every $\beta \in aG$ has at most one fixed point, i.e. $|S^\beta| \leq 1$. Then:

$$\frac{1}{|G|}\sum_{\beta \in aG} |S^\beta| \;\leq\; \frac{1}{|G|}|G| \;=\; 1.$$

Equality holds so for every $\beta \in aG$, $|S^\beta| = 1$ and we conclude that (3) implies (2). Similarly (4) implies (2). Next apply the lemma to the set $\mathcal{S} \times \mathcal{S}$. Then there is a unique common orbit of A and G of $\mathcal{S} \times \mathcal{S}$ if and only if:

$$\frac{1}{|G|}\sum_{\beta \in aG} |(\mathcal{S} \times \mathcal{S})^\beta| \;=\; \frac{1}{|G|}\sum_{\beta \in aG} |\mathcal{S}^\beta|^2 \;=\; 1 \;=\; \frac{1}{|G|}\sum_{\beta \in aG} |\mathcal{S}^\beta|.$$

Note that $|\mathcal{S}^\beta|^2 \geq |\mathcal{S}^\beta|$ with equality if and only if $|\mathcal{S}^\beta| = 0$ or 1. Therefore (1) is equivalent to (3). □

3.4 Proof of the classical exceptionality criterion

Recall the setup as described in Figures 3.3 and 3.4. In this section we follow Fried's proof of Theorem 3.2.4 [Fri74]. We then deduce Corollary 3.2.5.
We have seen that the exceptionality condition on connected components can be interpreted in terms of the action of the generating coset of A/G on $\mathcal{S}$. This is useful to keep in mind as we return to the proof of Theorem 3.2.4 with the following definition.

Definition 3.4.1. Let $\widehat{A}$ denote the subgroup of A consisting of elements whose restriction to $\widehat{k}$ generate $\mathrm{Gal}(\widehat{k}/k)$, i.e.

$$\widehat{A} = \{a \in A \mid a|_{\widehat{k}} = \varphi_k\}.$$

Analogously for $i = 1, \ldots, l$, let:

$$\widehat{H}_i = \{h \in H_i \mid h|_{\widehat{k}} = \varphi_k\},$$

where $\widehat{H} = \widehat{H}_1$.

We can also describe $\widehat{A}$ as a coset in A/G and $\widehat{H}_i$ as a coset in H_i/F_i by recalling that $A/G \cong \mathrm{Gal}(\widehat{k}/k)$. An element $a \in A$ is an element of $\widehat{A}$ if and only if $\langle aG \rangle = A/G$, so we can say $\widehat{A} \cong aG$ for any $a \in A$ which generates A/G.
Similarly $h \in H$ is an element of $\widehat{H}_i$ if and only if $\langle hF_i \rangle = H/F_i$, so $\widehat{H}_i \cong hF_i$ for any $h \in H$ which generates H/F_i. This information allows us to understand the cardinality of these groups, which will be useful in the next lemma.

Lemma 3.4.2. *Let $\widehat{A}, \widehat{H}_i$ be as defined above for $i = 1, \ldots l$ and assume that the only A-orbit of $\mathcal{S} \times \mathcal{S}$ which is fixed by the action of φ_k is the orbit corresponding to (α_1, α_1). Then*

$\widehat{A}$ is a disjoint union of $\widehat{H}_i$'s, i.e.

$$\widehat{A} \;=\; \bigsqcup_{i=1}^{l} \widehat{H}_i.$$

Proof. We first show that the $\widehat{H}_i$'s are disjoint. Let $h \in \widehat{H} \cap \widehat{H}_i$ for some $i \neq 1$, so $h\restriction_L = \mathrm{id}_L$, $h\restriction_{L_i} = \mathrm{id}_{L_i}$ and $h\restriction_{\widehat{k}} = \varphi_k$. Then $h \cdot (\alpha_1, \alpha_i) = (\alpha_1, \alpha_i)$; this implies that the orbit with basepoint (α_1, α_i) is also fixed by Frobenius, giving a contradiction. Therefore $\widehat{H} \cap \widehat{H}_i$ is empty.

We next show that the cardinality of both sides is equal. Using the previous discussion on cardinality and disjointness of conjugate groups, we see that $|\widehat{H}_i| = |F_i| = |F|$ and so $|\bigsqcup_{i=1}^{l} \widehat{H}_i| = l|F|$.

We now consider $|\widehat{A}| = |G| = [\widehat{L} : \widehat{K}]|F|$ and use that the extension L/K is regular. This tells us that $[\widehat{L} : \widehat{K}] = [L : K] = l$ ([FJ08], Cor 2.5.2) and so $|\widehat{A}| = l|F|$. The proof is concluded by observing that the right hand side is clearly contained in the left hand side and their cardinalities agree. □

Lemma 3.4.3. *Let $x \in X$ and let $z \in Z_x$. Then there exists $d \in D = D_{Z/X}(z)$ which also lies in $\widehat{A}$.*

Proof. First note that $I_{Z/X}(z) = I \subseteq G$. To see this recall:

$$G = \ker\big(A \to \mathrm{Gal}(\widehat{k}/k)\big),$$
$$I = \ker\big(D \to \mathrm{Gal}(\kappa(z)/k)\big),$$

and that $\widehat{k} \subseteq \kappa(z)$. Therefore if $\tau \in I$ it fixes $\kappa(z)$ and hence must also fix $\widehat{k}$, so $\tau \in G$. We can construct a surjective morphism $\mathrm{Gal}(\kappa(z)/k)) \twoheadrightarrow \mathrm{Gal}(\widehat{k}/k))$ defined by $dI \mapsto dG$.

As D/I is cyclic, there exists $d \in D$ such that $\langle dI \rangle = D/I$. As the morphism of Galois

groups is surjective, we have $\langle dG \rangle = A/G$. Therefore $d \in \widehat{A}$. □

We now combine the previous arguments to complete the proof of Theorem 3.2.4.

Proof. Let $x' \in X(k)$ and let $x \in X$ denote its scheme-theoretic image. By Lemma 3.4.3 there exists $d \in D \cap \widehat{A}$. Assuming the exceptionality condition Lemma 3.4.2 shows that there is a unique $i \in \{1, \ldots, l\}$ such that $d \in \widehat{H}_i$. Therefore $d \in D_{Z/Y_i}(z)$ and by construction d generates $\mathrm{Gal}(\kappa(z)/k)$.

Let $y_i \in Y_i$ be a scheme-theoretic point lying between $z \in Z$ and $x \in X$. We can embed the associated short exact sequences of decomposition and inertia groups as seen in the figure below.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & I_{Z/Y_i}(z) & \longrightarrow & D_{Z/Y_i}(z) & \longrightarrow & \mathrm{Gal}\left(\kappa(z)/\kappa(y_i)\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I & \longrightarrow & D & \longrightarrow & \mathrm{Gal}\left(\kappa(z)/k\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G & \longrightarrow & A & \longrightarrow & \mathrm{Gal}\left(\widehat{k}/k\right) & \longrightarrow & 1
\end{array}$$

Figure 3.6: Relations between short exact sequences

Let $\beta \in \kappa(y_i)$, so $d(\beta) = \beta$. As d generates $\mathrm{Gal}(\kappa(z)/k)$, β must lie in the fixed field of this Galois group and so $\beta \in k$. We conclude that $\kappa(y_i) = k$ and so this scheme-theoretic point corresponds to a rational point $y_i' \in Y_i(k)$. Recalling the conjugation setup from Definition 3.2.8 this can then be translated to obtain $y' \in Y(k)$ which lies above $x' \in X(k)$. We have shown that $f : Y(k) \to X(k)$ is surjective. □

We complete this chapter by proving Corollary 3.2.5.

Proof. The 'only if' direction can be proved using the Lang-Weil bound (Theorem 2.2.21). Note that $(X \times_X X)(k)$ can be interpreted as the set of points $(x_1, x_2) \in X(k) \times X(k)$ such that $f(x_1) = f(x_2)$, and $\Delta_X(k)$ represents the points $(x, x) \in X(k) \times X(k)$.
Assume that the fibre product $X \times_X X$ has another geometrically irreducible component W which is defined over k such that $W \neq \Delta_X$. Let $d = \dim(W)$ and apply Lang-Weil to the geometrically irreducible component W. Then there exist constants $C, c > 0$ such that:

$$\Big||W(k)| - c|k|^d\Big| < C|k|^{d-\frac{1}{2}}.$$

As $|k|$ becomes large, $|k|^{d-\frac{1}{2}} \ll |k|^d$, so $W(k) \neq \emptyset$. It therefore follows that for large finite fields, there exists some rational point in $(X \times_X X)(k)$ which lies in $W(k)$ and hence not $\Delta_X(k)$. This means that f cannot be injective on rational points for large finite fields and therefore not exceptional.
This argument can be applied to the polynomial case (Theorem 3.1.10) by replacing $X \times_X X$ with the variety defined as the zero set of $f(x) - f(y)$ and considering the diagonal as the zero set of $x - y$.

Conversely assume that Δ_X is the only geometrically connected component of $X \times_X X$ which is defined over k. As X is finite dimensional it immediately follows from Theorem 3.2.4 that $X(k) \to X(k)$ is bijective. In order to prove that f is an exceptional cover it remains to show that Δ_X is also the only geometrically connected component of $X \times_X X$ which is defined over k_m for infinitely many m.
We know that all geometrically connected components are defined over $\widehat{k}$, where we let $r = [\widehat{k} : k]$. As in the proof of Theorem 3.1.10, if $\gcd(m, r) = 1$ then Δ_X is the only geometrically connected component defined over k_m. Therefore there are infinitely many extensions k_m such that Δ_X is the only geometrically irreducible component of $X \times_X X$ defined over k_m, and hence such that $f : X(k_m) \to X(k_m)$ is bijective. □

Chapter 4

Difference algebraic geometry

We now lay the foundations of difference algebraic geometry. The first section begins with a discussion of the categories σ-**Set** and G-σ-**Set** then offers both algebraic and geometric perspectives.

Material in Subsections 4.1.1, 4.2.1 and Section 4.3 is adapted from the work of Tomašić ([Tom14], [Tom16]) with reference to classical difference algebra literature ([Lev08], [Wib13]). Material in Subsections 4.1.2, 4.1.3 and 4.2.2 is original to this thesis.

4.1 The categories σ-Set and G-σ-Set

We introduce the framework of difference categories by defining the category σ-**Set** and considering actions of difference groups on difference sets.

4.1.1 Difference group actions

We build σ-**Set** from the familiar category **Set**.

Definition 4.1.1. The **category of difference sets**, σ-**Set**, consists of the following

objects and morphisms:

- An object (S, σ) is a set S together with an endomorphism $\sigma : S \to S$ which we call the difference operator;
- Let $(S, \sigma_S), (T, \sigma_T)$ be two objects. A morphism $f : (S, \sigma_S) \to (T, \sigma_T)$ is a map of the underlying sets such that $\sigma_T \circ f = f \circ \sigma_S$, i.e. the diagram below commutes.

$$\begin{array}{ccc} S & \xrightarrow{f} & T \\ {\scriptstyle \sigma_S}\downarrow & & \downarrow{\scriptstyle \sigma_T} \\ S & \xrightarrow[f]{} & T \end{array}$$

Figure 4.1: Morphism of difference sets

Let σ-**FSet** denote the category of finite difference sets.

We often refer to a difference object without denoting its endomorphism, e.g. $S = (S, \sigma_S)$. In the event that we specifically want to refer to the underlying object it will be explicitly denoted using $\lfloor - \rfloor$ notation: $S = (\lfloor S \rfloor, \sigma_S)$. This does not cause confusion as the meaning should be clear from the context.
Here we do *not* assume that σ is injective or surjective. Objects with an invertible difference operator are called **inversive** and this simplifies many considerations (see [Coh65], [Lev08]). Intuitively we note that $\mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S, T) \subseteq \mathrm{Hom}_{\mathbf{Set}}(S, T)$ due to the extra constraint of the commutative diagram. Every set S can trivially be considered as a difference set (S, id) by equipping with the identity endomorphism.

Definition 4.1.2. For a difference set S, the **fixed set of** S, $\mathrm{Fix}(S)$, is the set of elements which are fixed by the difference action, i.e.

$$\mathrm{Fix}(S) \;=\; \{s \in S \mid \sigma_S(s) = s\}.$$

Definition 4.1.3. A **subobject** U of a difference set S is a subset $U \subseteq S$ such that $\sigma_U = \sigma_S{\restriction}_U$ and $\sigma_U(U) \subseteq U$.
A subobject U is **trivial** if $U = S$ or $U = \emptyset$.

It is important to note here that every subset $U \subseteq S$ is not automatically a subobject: due to our lack of restrictions on σ_S it is possible that for some $u \in U$, $\sigma_U(u) \notin U$. Similarly its complement $S \setminus U$ is not necessarily a subobject.

Example 4.1.4. The set of natural numbers $\mathbb{N}$ together with the 'shift' endomorphism $\sigma_{\mathbb{N}} : n \mapsto n + 1$ is an object of σ**-Set**. Denote this difference set by $\mathbb{N}_+ = (\mathbb{N}, \sigma_{\mathbb{N}})$.
The subset $U = \{1, \ldots, n\}$ is not a subobject as $\sigma_{\mathbb{N}}(n) = n+1 \notin U$. However its complement $\mathbb{N} \setminus U$ is a subobject.

We can consider the categorical Cartesian and fibre products; the underlying constructions occur in the same way and difference structure is defined on top.

Definition 4.1.5. Let S, T, U be difference sets with morphisms $g : S \to U$, $h : T \to U$.

- The **Cartesian product**, $S \times T$, has difference endomorphism $\sigma_S \times \sigma_T$ acting on each component respectively.

- The **fibre product**, $S \times_U T$, has difference endomorphism $\sigma_S \times \sigma_T$ acting on each component respectively. For $s \in S$, $t \in T$ we verify that $(\sigma_S \times \sigma_T)(S \times_U T) \subseteq S \times_U T$:

$$g\big(\sigma_S(s)\big) \;=\; \sigma_U\big(g(s)\big) \;=\; \sigma_U\big(h(t)\big) \;=\; h\big(\sigma_T(t)\big).$$

- The **coproduct**, $S \sqcup T$, has difference endomorphism acting on each component of the disjoint union separately, i.e. $\sigma{\restriction}_S = \sigma_S$, $\sigma{\restriction}_T = \sigma_T$.

Further concrete difference categories can be defined from σ**-Set**: we explicitly show this

for the category of difference groups, σ-**Grp**.

Definition 4.1.6. The **category of difference groups**, σ-**Grp**, consists of group objects in σ-**Set**. Therefore an object in σ-**Grp** is an object $(G, \sigma_G) \in \sigma$-**Set** along with the σ-**Set**-morphisms detailed below.

- There is a morphism $1 : \{*\} \to G$ whose image defines an identity element $1 \in G$, where $(\{*\}, \mathrm{id})$ is the terminal object of σ-**Set**. By definition this satisfies $\sigma_G(1) = 1$.
- There is an inverse morphism $()^{-1} : G \to G$ which satisfies $\sigma_G(g^{-1}) = \big(\sigma_G(g)\big)^{-1}$ for all $g \in G$.
- There is a multiplication morphism $m : G \times G \to G$ which satisfies $\sigma_G(gh) = \sigma_G(g)\sigma_G(h)$ for all $g, h \in G$.

Three additional larger commutative diagrams are also required which express that multiplication is associative and that the images of the identity and inverse morphisms act as identity and inverse elements respectively.

Defining a group object internal to σ-**Set** is equivalent to defining a group G with a group endomorphism σ_G and we can do this analogously for other structures. We will make particular use of difference rings and difference fields.

Definition 4.1.7. A **difference ring**, (R, σ_R), consists of a unital commutative ring R together with a unital ring endomorphism σ_R. The **category of difference rings** is denoted σ-**Ring**.
A **difference field**, (K, σ_K), consists of a field K together with a field endomorphism σ_K. It follows that σ_K is injective.
Let K be a difference field. A K-σ-**algebra**, (A, σ_A), is a K-algebra A together with

endomorphism σ_A where for $\lambda \in K, a \in A$:

$$\sigma_A(\lambda \cdot a) \;=\; \sigma_K(\lambda)\sigma_A(a).$$

The **category of finite dimensional K-σ-algebras** is denoted K-σ-**FAlg**.

We can now consider a difference group acting on a difference set. Here we introduce a 'twisted' notation ${}^{\sigma}()$ for the difference group endomorphism to suggest a relation between the group and the set.

Definition 4.1.8. A **difference group** $(G, {}^{\sigma}())$ **acts on a difference set** (S, σ) if there exists a σ-**Set**-morphism $\mu : G \times S \to S$ where $\mu(g, s) = g \cdot s$. Therefore for all $g \in G, s \in S$, the relation $\sigma(g \cdot s) = {}^{\sigma}g \cdot \sigma(s)$ holds.

$$\begin{array}{ccc} G \times S & \xrightarrow{\mu} & S \\ {\scriptstyle {}^{\sigma}()\times\sigma}\downarrow & & \downarrow{\scriptstyle \sigma} \\ G \times S & \xrightarrow{\mu} & S \end{array}$$

Figure 4.2: Difference group action on a difference set

The following commutative diagrams are also required to ensure that for all $g, h \in G, s \in S$, we have $(gh) \cdot s = g \cdot (h \cdot s)$ and $1 \cdot s = s$. Note that all morphisms are in σ-**Set**.

$$\begin{array}{ccc} G \times G \times S & \xrightarrow{\mathrm{id}\times\mu} & G \times S \\ {\scriptstyle m\times\mathrm{id}}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times S & \xrightarrow[\mu]{} & S \end{array} \qquad\qquad \begin{array}{ccc} \{*\} \times S & & \\ {\scriptstyle 1\times\mathrm{id}}\downarrow & \searrow^{\pi_2} & \\ G \times S & \xrightarrow[\mu]{} & S \end{array}$$

Figure 4.3: Commutative diagrams required for difference group actions

Definition 4.1.9. Let $(G, {}^{\sigma}())$ be a difference group. The **category of difference G-sets**, G-σ-**Set**, consists of difference sets (S, σ) equipped with the action of $(G, {}^{\sigma}())$. Morphisms

in this category are G-equivariant σ-**Set**-morphisms.

In view of the anti-equivalence between algebra and geometry discussed in Section 2.1 (page 24) we can analogously define the action of a difference group on a difference ring. In this case we denote the difference group endomorphism by $()^\sigma$.

Definition 4.1.10. A **difference group** $(G, ()^\sigma)$ **acts on a difference ring** (R, σ) if for all $g \in G$, $r \in R$, the relation $g \cdot \sigma(r) = \sigma(g^\sigma \cdot r)$ holds.

The Cartesian closed property helps us to give another characterisation of group actions.

Definition 4.1.11. A category $\mathcal{C}$ is **Cartesian closed** if for any object $T \in \mathcal{C}$, the product functor $- \times T : \mathcal{C} \to \mathcal{C}$ has a right adjoint. For locally small categories this means that there exists a functor $[T, -] : \mathcal{C} \to \mathcal{C}$ such that the following bijection is natural in all $S, U \in \mathcal{C}$:

$$\mathrm{Hom}_{\mathcal{C}}(S \times T, U) \;\cong\; \mathrm{Hom}_{\mathcal{C}}(S, [T, U]).$$

The category **Set** is Cartesian closed when we take $[T, -] = \mathrm{Hom}_{\mathbf{Set}}(T, -)$. Note that in the category σ-**Set**, the functor $\mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(T, -)$ does not return an object of the category. For $U \in \sigma$-**Set**, $\mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(T, U)$ is a set but not a difference set. We therefore need to find a candidate for a right adjoint functor in this context.

Definition 4.1.12. Let $T, U \in \sigma$-**Set**. The **internal hom** object $[T, U]$ in σ-**Set** is:

$$[T, U] \;=\; \{(f_i)_{i \in \mathbb{N}} \mid f_i \in \mathrm{Hom}_{\mathbf{Set}}(\lfloor T \rfloor, \lfloor U \rfloor),\ \forall i\ f_{i+1} \circ \sigma_T = \sigma_U \circ f_i\}.$$

We can express this information in the commutative diagram below and define a difference

endomorphism τ on this set which we often refer to as a 'shift' morphism:

$$\begin{array}{rccc} \tau: & [T,U] & \longrightarrow & [T,U] \\ & (f_0, f_1, f_2, \dots) & \longmapsto & (f_1, f_2, f_3, \dots)\ . \end{array}$$

$$\begin{array}{ccc} T & \xrightarrow{f_0} & U \\ {\scriptstyle\sigma_T}\downarrow & & \downarrow{\scriptstyle\sigma_U} \\ T & \xrightarrow{f_1} & U \\ {\scriptstyle\sigma_T}\downarrow & & \downarrow{\scriptstyle\sigma_U} \\ T & \xrightarrow{f_2} & U \\ \downarrow & & \downarrow \\ \vdots & & \vdots \end{array}$$

Figure 4.4: The internal hom diagram $[T,U]$

In the case where $T = U$ we can also define the difference group of internal automorphisms $\mathrm{Aut}[T]$, in which every component f_i is an automorphism of $\lfloor T \rfloor$.

Proposition 4.1.13. *Let $S, T, U \in \sigma$-**Set**. The category σ-**Set** is Cartesian closed with the internal hom functor $[T, -]$ being right adjoint to the product functor $- \times T$. Explicitly we have the bijection of sets:*

$$\mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S \times T, U) \ \cong\ \mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S, [T,U]).$$

Proof. Define the following **Set**-morphisms:

- $\Phi : \mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S \times T, U) \to \mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S, [T,U])$ is given by $\Phi(f) = g$, where for $s \in S$, $t \in T$, the i^{th} component of $g(s)$ is $\big(g(s)\big)_i(t) = f\big(\sigma_S^i(s), t\big)$;

- $\Psi : \mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S, [T, U]) \to \mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S \times T, U)$ is given by $\Psi(g) = f$, where for $s \in S$, $t \in T$, $f(s,t) = \big(g(s)\big)_0(t)$.

The required properties below can then easily be verified.

(i) $\Phi(f)(s)$ belongs to the internal hom object, i.e. $\big(g(s)\big)_{i+1} \circ \sigma_T = \sigma_U \circ \big(g(s)\big)_i$.

(ii) $\Phi(f)$ is a σ-**Set**-morphism, i.e. $\tau \circ \Phi(f) = \Phi(f) \circ \sigma_S$.

(iii) $\Psi(g)$ is a σ-**Set**-morphism, i.e. $\sigma_U \circ \Psi(g) = \Psi(g) \circ (\sigma_S \times \sigma_T)$.

(iv) $\Psi\big(\Phi(f)\big) = f$.

(v) $\Phi\big(\Psi(g)\big) = g$.

□

This bijection can be used to describe the difference group action:

$$\mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(G \times S, S) \;\cong\; \mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(G, [S, S]).$$

Here the group action morphism $\mu : G \times S \to S$ is mapped :

$$\begin{array}{rccc} \Phi(\mu): & G & \longrightarrow & [S,S] \\ & g & \longmapsto & (g\cdot -, {}^{\sigma}g\cdot -, {}^{\sigma^2}g\cdot -, \dots)\ . \end{array}$$

In fact for all $g \in G$, we can use the existence of g^{-1} to see that $\Phi(\mu)$ factors through $\mathrm{Aut}[S]$. Therefore giving a difference group action μ is equivalent to giving a homomorphism $G \to \mathrm{Aut}[S]$.

4.1.2 Connected objects

We now discuss competing definitions of connectedness in σ-**Set** and G-σ-**Set**. Connected objects in the category **Set** are just singletons $\{*\}$. For a group G, connected objects in the category G-**Set** are G-orbits. We interpret the notion of connectedness in σ-**Set** and G-σ-**Set**: we present four candidates for the definition, keeping an example in mind to guide us.
Recall the difference set $\mathbb{N}_+$ as described in Example 4.1.4. Intuitively we would expect this to be connected as every natural number lies in the same 'orbit' of $\sigma_{\mathbb{N}}$.

The first two candidates are general categorical definitions whereas the second two are specific to difference categories. Let $S \in \sigma$-**Set**.

1. An object S is connected if for all subobjects $U, V \subseteq S$ such that $S = U \sqcup V$ can be expressed as a (disjoint) coproduct, both U and V are trivial. Recall that a subset U of a difference set S is a subobject if $\sigma(U) \subseteq U$.

2. An object S is connected if the functor $\mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S, -) : \sigma$-**Set** $\to$ **Set** preserves coproducts, i.e. for any collection of objects $Y_i \in \sigma$-**Set** with indexing set I there is a bijection:

$$\mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S, \bigsqcup_{i \in I} Y_i) \;\cong\; \bigsqcup_{i \in I} \mathrm{Hom}_{\sigma\text{-}\mathbf{Set}}(S, Y_i).$$

3. A difference set S is connected if for all $s, t \in S$, $s \sim t$, where the equivalence relation $\sim$ is defined as:

$$s \sim t \iff \exists m, n \in \mathbb{N} \text{ such that } \sigma^m(s) = \sigma^n(t).$$

4. A difference set S is connected if the internal hom functor $[S, -] : \sigma\textbf{-Set} \to \sigma\textbf{-Set}$ preserves coproducts, i.e. for any collection of objects Y_i with indexing set I there is an isomorphism of difference sets:

$$[S, \bigsqcup_{i \in I} Y_i] \cong \bigsqcup_{i \in I} [S, Y_i].$$

We now consider each definition in the context of $\mathbb{N}_+$.

1. Let $U, V \subseteq \mathbb{N}$ such that $\mathbb{N} = U \sqcup V$ and assume they are nontrivial, i.e. there exists $n \in U$, $m \in V$. Without loss of generality we may consider boundary points of the subsets and assume that $m = n + 1$, so $\sigma_{\mathbb{N}}(n) = m$. Therefore $\sigma_U(U) \not\subseteq U$ and hence $\mathbb{N}_+$ is connected with respect to **1**.

2. It is always true that $\bigsqcup_{i \in I} \mathrm{Hom}_{\sigma\textbf{-Set}}(S, Y_i) \subseteq \mathrm{Hom}_{\sigma\textbf{-Set}}(S, \bigsqcup_{i \in I} Y_i)$ so intuitively this definition says that every morphism from S maps into only one coproduct component. Consider a σ**-Set**-morphism $\phi : \mathbb{N} \to Y = \bigsqcup_{i \in I} Y_i$ and let σ_i, σ_Y denote the difference endomorphisms on Y_i, Y respectively, so for all $n \in \mathbb{N}$ we have $\phi(n + 1) = \sigma_Y(\phi(n))$. Assume $\phi(0) \in Y_i$ for some $i \in I$ and then $\phi(1) = \sigma_i(\phi(0)) \in Y_i$. It follows that $\phi(n) \in Y_i$ for all n and hence $\phi : \mathbb{N} \to Y_i$. Therefore $\mathbb{N}_+$ is connected with respect to **2**.

3. It is clear that $\sim$ is an equivalence relation. Let $m, n \in \mathbb{N}$ so without loss of generality we may assume $m \geq n$. Then $\sigma_{\mathbb{N}}^{m-n}(n) = m$ and hence $\mathbb{N}_+$ is connected with respect to **3**.

4. A counterexample can be constructed to show that $\mathbb{N}_+$ is disconnected with respect to **4**. Let $(\phi_j)_{j \in \mathbb{N}} \in [\mathbb{N}, Y_0 \sqcup Y_1]$ such that $\phi_0(0) \in Y_0$, $\phi_0(1) \in Y_1$. We have the freedom to make this assumption: the definition of the internal hom object gives that for all

$n \in \mathbb{N}$, $\phi_1(n+1) = \sigma_Y(\phi_0(n))$ but gives no restriction on $\phi_0(n+1)$. Therefore $(\phi_j)_{j\in\mathbb{N}}$ is not completely contained in either $[\mathbb{N}, Y_0]$ or $[\mathbb{N}, Y_1]$.

These considerations suggest that some of these definitions may be equivalent in σ-**Set**.

Proposition 4.1.14. *Let $S \in \sigma$-**Set**.*

(i) The following are equivalent:

(1) S is connected with respect to **1***;*

(2) S is connected with respect to **2***;*

(3) S is connected with respect to **3***.*

(ii) S is connected with respect to **4** *if and only if $S = (\{*\}, \mathrm{id})$.*

Proof. (i) We prove (1) $\iff$ (3) and (2) $\iff$ (3).

Assume S is connected in the sense of **1**, i.e. it only has trivial subobjects. Let $t \in S$, let $S_t = \{s \mid s \sim t\}$ denote the equivalence class of t and write $S = S_t \sqcup (S \setminus S_t)$.
If $s \in S_t$ then there exist $m, n \in \mathbb{N}$ such that $\sigma^m(s) = \sigma^n(t)$. Then $\sigma^m(\sigma(s)) = \sigma(\sigma^m(s)) = \sigma(\sigma^n(t)) = \sigma^{n+1}(t)$, so $\sigma(s) \in S_t$. Similarly if $s \in S \setminus S_t$ but $\sigma(s) \in S_t$, then there exist $m, n \in \mathbb{N}$ such that $\sigma^m(\sigma(s)) = \sigma^n(t)$ and hence $s \in S_t$. Therefore $\sigma(s) \in S \setminus S_t$ and we have a decomposition into subobjects. By assumption either S_t or $S \setminus S_t$ is trivial and we conclude that $S = S_t$.
Assume S is connected in the sense of **3**. Let $S = U \sqcup V$ and let $s \in U$, $t \in V$. By assumption there exist $m, n \in \mathbb{N}$ such that $\sigma^m(s) = \sigma^n(t)$, and by the definition of subobjects $\sigma^m(s) \in U$ and $\sigma^n(t) \in V$. We get a contradiction so either U or V is empty.

Assume S is connected in the sense of **2**, i.e. the Hom functor preserves coproducts.

Decompose $S = \bigsqcup_{t\in S} S_t$ into equivalence classes with respect to $\sim$, letting $\phi : S \to \bigsqcup_{t\in S} S_t$ be the identity morphism. By assumption for some $t \in S$, ϕ can be identified with a morphism $S \to S_t$, i.e. $S = S_t$.

Assume S is connected in the sense of **3**. Let $\phi : S \to \bigsqcup_{i\in I} Y_i$ and let $\phi(s) \in Y_i$ for some $s \in S$, $i \in I$. Then by the definitions of σ-**Set**-morphisms and subobjects, for all $m \in \mathbb{N}$, $\phi(\sigma^m(s)) = \sigma_i^m(\phi(s)) \in Y_i$. Let $t \neq s \in S$ such that $\phi(t) \in Y_j$ so for all $n \in \mathbb{N}$, $\phi(\sigma^n(t)) = \sigma_j^n(\phi(t)) \in Y_j$. By assumption there exist $m, n \in \mathbb{N}$ such that $\phi(\sigma^n(t)) = \phi(\sigma^m(s)) \in Y_i$ and we conclude that $Y_i = Y_j$.

(ii) Assume S is connected in the sense of **4**. In the simplest case let $|I| = 2$ and let $Y_1 = Y_2 = (\{*\}, \mathrm{id})$. It can easily be seen that $[S, \{*\}] \cong \{*\}$ and so $|[S, \{*\}] \sqcup [S, \{*\}]| = 2$. Elements $(\phi_j)_{j\in\mathbb{N}}$ of the internal hom object $[S, \{*\} \sqcup \{*\}]$ are determined by a combination of the action of ϕ_0 and the difference endomorphism on S. If we assume $|S| \geq 2$ it can be seen that there are at least three distinct combinations and so $[S, \{*\}] \sqcup [S, \{*\}] \neq [S, \{*\} \sqcup \{*\}]$ by a cardinality argument.

Conversely assume that $S = (\{*\}, \mathrm{id})$ and let $(\phi_j)_{j\in\mathbb{N}} \in [\{*\}, \bigsqcup_{i\in I} Y_i]$. Therefore $\sigma_Y \circ \phi_{j-1} = \phi_j$ and so $\sigma_Y^j \circ \phi_0 = \phi_j$. Let $\phi_0(*) \in Y_i$ for some $i \in I$; then $\phi_j(*) = \sigma_i^j(\phi_0(*)) \in Y_i$ and hence $(\phi_j)_{j\in\mathbb{N}} \in [\{*\}, Y_i]$.

□

Definition 4.1.15. Let $S \in \sigma$-**Set**. Then S is σ-**connected** if it satisfies any of the equivalent conditions **1**, **2**, **3**.

We can extend these definitions to the category G-σ-**Set** to find an analogous notion of connectedness. Fix $G \in \sigma$-**Grp** and let $S \in G$-σ-**Set**.

1'. An object S is connected if for all subobjects $U, V \subseteq S$ such that $S = U \sqcup V$ can be expressed as a (disjoint) coproduct, both U and V are trivial. Recall that a subset U

of S is a subobject if $\sigma(U) \subseteq U$ and for all $g \in G$, $g \cdot U \subseteq U$.

2'. An object S is connected if the functor $\mathrm{Hom}_{G\text{-}\sigma\text{-}\mathbf{Set}}(S, -) : G\text{-}\sigma\text{-}\mathbf{Set} \to \mathbf{Set}$ preserves coproducts, i.e. for any collection of objects $Y_i \in G\text{-}\sigma\text{-}\mathbf{Set}$ with indexing set I there is a bijection:

$$\mathrm{Hom}_{G\text{-}\sigma\text{-}\mathbf{Set}}(S, \bigsqcup_{i \in I} Y_i) \;\cong\; \bigsqcup_{i \in I} \mathrm{Hom}_{G\text{-}\sigma\text{-}\mathbf{Set}}(S, Y_i).$$

3'. A G-σ-set S is connected if for all $s, t \in S$, $s \sim_G t$, where the equivalence relation $\sim_G$ is defined as:

$$s \sim_G t \iff \exists m, n \in \mathbb{N},\ \exists g \in G \text{ such that } \sigma^m(s) = g \cdot \sigma^n(t).$$

By making minor alterations to the proof of Proposition 4.1.14 the corresponding result and definition follow.

Proposition 4.1.16. *Let $G \in \sigma$-**Grp** and $S \in G$-σ-**Set**. The following are equivalent:*

(1') S is connected in the sense of **1'**;

(2') S is connected in the sense of **2'**;

(3') S is connected in the sense of **3'**.

Definition 4.1.17. Let $G \in \sigma$-**Grp** and $S \in G$-σ-**Set**. Then S is G-σ-**connected** if it satisfies any of the equivalent conditions **1'**, **2'**, **3'**.

4.1.3 Group orbits with a difference action

We now consider σ-closed orbits of a difference group acting on a difference set. This mirrors the discussion of common orbits of Galois groups in Section 3.3 and we obtain results analogous to Lemmas 3.3.2 and 3.3.3. We then attempt to combine both conditions to consider common σ-closed orbits and highlight the difficulties in doing this. Throughout this section if G is a difference group and S is a difference set then by 'G-orbit' we are referring to the underlying G-orbit on the underlying set, i.e. a $\lfloor G \rfloor$-orbit on $\lfloor S \rfloor$.

Definition 4.1.18. Let $G \in \sigma$**-Grp** and $S \in G$-σ**-Set**. A G-orbit $O \subseteq S$ is σ**-closed** if O is a subobject of S, i.e. if $\sigma(O) \subseteq O$.

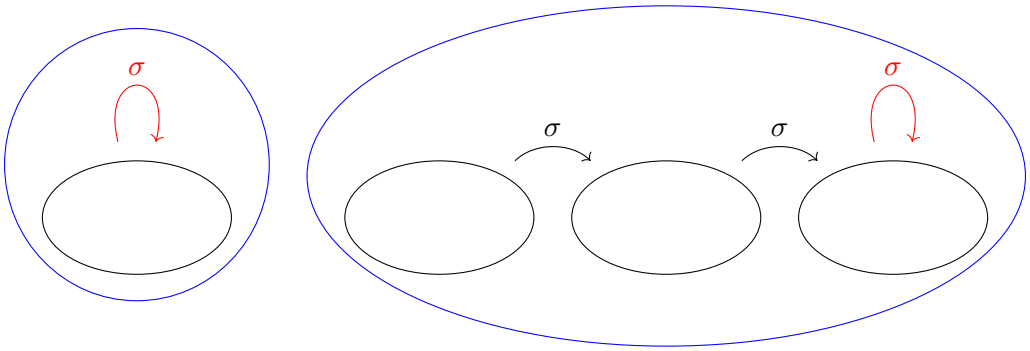

Figure 4.5: σ-closed and G-σ-connected orbits

Note the distinction between the notions of σ-closed and G-σ-connected. For any $s \in S$, $g \in G$, we see that $\sigma(g \cdot s) = {}^{\sigma}g \cdot \sigma(s)$ must lie in the same group orbit as $\sigma(s)$. The difference endomorphism on S therefore induces an action on underlying group orbits; this will not necessarily be a permutation as we do not assume σ to be an automorphism.

An orbit is σ-closed if the induced difference action fixes the orbit, whereas a collection of orbits is G-σ-connected if they are linked by the difference action. This type of behaviour is shown in the figure above with σ-closed orbits highlighted in red and G-σ-connected collections of orbits circled in blue.

Mirroring Chapter 3 let (S, σ) be a finite difference set equipped with the action of a finite difference group $(A, {}^{\sigma}())$. We aim to count the number of σ-closed A-orbits of S.

Definition 4.1.19. A point $s \in S$ is **σ-fixed by** $b \in A$ if $\sigma(s) = b \cdot s$.
Let $s \in S$. The **σ-stabiliser of s in A**, denoted A_s^σ, is the set of elements of A which σ-fix s, i.e.

$$A_s^\sigma = \{b \in A \mid \sigma(s) = b \cdot s\}.$$

In contrast to the usual notion of stabiliser, A_s^σ is only a subset of A rather than a subgroup.
Let $b \in A$. The **σ-fixed set of b in S**, denoted S_σ^b, is the set of points of S which are σ-fixed by b, i.e.

$$S_\sigma^b = \{s \in S \mid \sigma(s) = b \cdot s\}.$$

Note the analogy with fixed point sets used in Lemma 3.3.2. It is also clear that an orbit O is σ-closed if for any $s \in O$, A_s^σ is nonempty.

Proposition 4.1.20. *If $s, t \in S$ lie in the same A-orbit then their σ-stabilisers are σ-conjugate, i.e. there exists $c \in A$ such that ${}^{\sigma}c \cdot A_s^\sigma \cdot c^{-1} = A_t^\sigma$. Therefore $|A_s^\sigma|$ does not depend on the choice of s in a particular orbit.*

Proof. Since s, t lie in the same orbit there exists $c \in A$ such that $c \cdot s = t$. It is then easily verified that there is a bijection:

$$\begin{aligned} A_s^\sigma &\longrightarrow A_t^\sigma \\ b &\longmapsto {}^{\sigma}cbc^{-1} \quad . \end{aligned}$$

□

Proposition 4.1.21. *If an orbit O is σ-closed then for all $s \in O$, $|A_s^\sigma| = |A_s| = \frac{|A|}{|O|}$.*

Proof. Since O is σ-closed there exists $b \in A$ such that $\sigma(s) = b \cdot s$. We then obtain a bijection:

$$\begin{aligned} A_s^\sigma &\longrightarrow A_s \\ c &\longmapsto b^{-1}c \ . \end{aligned}$$

□

The next two lemmas and their proofs are analogous to Lemmas 3.3.2 and 3.3.3.

Lemma 4.1.22. *Let A be a finite difference group acting on a finite difference set S. Then the number of σ-closed A-orbits of S is:*

$$\frac{1}{|A|} \sum_{b \in A} |S_\sigma^b|,$$

where $|S_\sigma^b|$ denotes the σ-fixed set of b in S.

Proof. We first assume that A acts transitively on S, which is trivially σ-closed, and define the characteristic set:

$$\mathcal{V}^\sigma = \{(b, s) \in A \times S \mid \sigma(s) = b \cdot s\}.$$

Its cardinality can be computed as either $\sum_{s \in S} |A_s^\sigma| = \sum_{s \in S} \frac{|A|}{|S|} = |A|$ or $\sum_{b \in A} |S_\sigma^b|$. These can be equated as before to give:

$$\frac{1}{|A|} \sum_{b \in A} |S_\sigma^b| = 1.$$

We now remove the assumption that A acts transitively and extend the argument to an A-orbit O by defining:

$$\mathcal{V}_O^\sigma = \{(b, s) \in A \times O \mid \sigma(s) = b \cdot s\}.$$

Then $|\mathcal{V}_O^\sigma| = |A|$ if O is σ-closed and $|\mathcal{V}_O^\sigma| = 0$ otherwise. This gives that $\mathcal{V}^\sigma$ is the disjoint union of all $\mathcal{V}_O^\sigma$'s and so the number of σ-closed orbits is given by $|\mathcal{V}^\sigma|/|A|$. □

Setting $\sigma = \mathrm{id}$ means that $S_\sigma^b = S^b$ and so Lemma 4.1.22 reduces to Burnside's Lemma for counting the number of orbits in a set.

Lemma 4.1.23. *Let A be a finite difference group acting transitively on a finite difference set S. The following are equivalent:*

(1) The only σ-closed A-orbit of $S \times S$ is the diagonal;

(2) Every $b \in A$ has a unique σ-fixed point in S;

(3) Every $b \in A$ has at most one σ-fixed point in S;

(4) Every $b \in A$ has at least one σ-fixed point in S.

Proof. Clearly (2) implies both (3) and (4). As S is assumed to be an A-orbit it is trivially σ-closed and so $1 = \frac{1}{|A|} \sum_{b \in A} |S_\sigma^b|$. As in the proof of Lemma 3.3.3 we use an inequality argument to show that (3) implies (2) and (4) implies (2).
We now apply the previous lemma to $S \times S$ to see that there is a unique σ-closed orbit of $S \times S$ if and only if $|S_\sigma^b| = 0$ or 1. Therefore (1) is equivalent to (3). □

Here setting $\sigma = \mathrm{id}$ says that the diagonal is the only orbit of $S \times S$ if and only if every group element has a unique fixed point in S. This gives a trivial statement where $|S| = 1$:

if there are distinct elements $s, t \in S$ we can form an element $(s,t) \in S \times S$ which is not in the diagonal orbit. Similarly the identity element of A must have a unique fixed point, forcing there to be a unique element in the set.
Motivated by Section 3.3 we are interested in applying this to difference Galois groups acting on connected components of the difference fibre product $Y \times_X Y$.

Let $G \lhd A$ be finite difference groups which both act transitively on finite difference set S and assume that A/G is cyclic. We have considered A-orbits of $S \times S$ which are either σ-closed or where G also acts transitively. It is natural ask whether it is possible to to combine these two group orbit properties to obtain a result analogous to Lemmas 3.3.3 and 4.1.23. This kind of assumption would correspond to geometrically connected components of $Y \times_X Y$ defined over k which are σ-closed.

Lemma 4.1.24. *Let A be a finite difference group acting on a finite difference set S. Let $G \lhd A$ be a normal difference subgroup such that A/G is cyclic and let $a \in A$ be such that $A/G = \langle aG \rangle$. Let O denote an A-orbit of S.*
Then the number of common orbits of A and G on S which are σ-closed is equal to both of the following expressions:

(i) $$\frac{1}{|A||G|} \sum_{O \subseteq S} \sum_{b \in A} \sum_{\beta \in aG} |O||O_\sigma^b \cap O^\beta|;$$

(ii) $$\frac{1}{|A||G|} \sum_{O \subseteq S} \sum_{b \in A} \sum_{\beta \in aG} |O_\sigma^b||O^\beta|.$$

Proof. If A acts transitively on S then the condition of S being σ-closed is trivially satisfied and we reduce to the situation in Lemma 3.3.2. It is therefore more pertinent in this case to consider orbits $O \subseteq S$. As before we define a characteristic set $\mathcal{W}$ which is nonempty if and only if both conditions are satisfied. Recall that G acts transitively on O if and only if

there exists $\beta \in aG$ with a fixed point in S and define:

$$\mathcal{W} = \{(b, \beta, s) \ \in A \times aG \times O \mid \beta \cdot s = s, \ \sigma(s) = b \cdot s\}.$$

We compute the cardinality of $\mathcal{W}$ in two ways. Firstly:

$$|\mathcal{W}| = \sum_{b \in A} \sum_{\beta \in aG} |O_\sigma^b \cap O^\beta|.$$

Alternatively if we recall the definition of $\mathcal{V}_O$ (page 58) we see that if $\mathcal{W}$ is nonempty its cardinality can be computed as:

$$\begin{aligned} |\mathcal{W}| &= \sum_{s \in O} |\{\beta \in aG \mid \beta \cdot s = s\}||A_s^\sigma| \\ &= |\mathcal{V}_O||A_s^\sigma| \\ &= |G|\frac{|A|}{|O|}. \end{aligned}$$

This contrasts with the previous lemmas where $|\mathcal{V}| = |G|$ and $|\mathcal{V}^\sigma| = |A|$ only depend on the order of the groups. We now see that $|\mathcal{W}|$ depends on the size of the orbit that is being considered; this is where we run into difficulty when extending the action to all A-orbits of S. Nevertheless we can say that O is a common orbit of A and G which is σ-closed if and only if:

$$\frac{|O|}{|A||G|} \sum_{b \in A} \sum_{\beta \in aG} |O_\sigma^b \cap O^\beta| = 1.$$

When we sum over all orbits of S we must be careful not to simplify $\sum_{O \subseteq S} |O| = |S|$ or $\sum_{O \subseteq S} |O_\sigma^b \cap O^\beta| = |S_\sigma^b \cap S^\beta|$. Terms should contribute to this sum if both conditions are satisfied so this identification will result in overcounting. From here we obtain (i) and conclude that this is its simplest form.

The expression (ii) is obtained by multiplying the two relevant characteristic functions:

$$\frac{1}{|G|}\sum_{\beta\in aG}|O^{\beta}| = \begin{cases} 1, & \text{if } G \text{ acts transitively on } O; \\ 0, & \text{otherwise;} \end{cases}$$

$$\frac{1}{|A|}\sum_{b\in A}|O^{b}_{\sigma}| = \begin{cases} 1, & \text{if } O \text{ is } \sigma\text{-closed;} \\ 0, & \text{otherwise.} \end{cases}$$

Again we require both properties to be satisfied by the same orbit so we cannot simplify to $|S^{b}_{\sigma}|$ or $|S^{\beta}|$. Doing so would count orbits which satisfy at least one property and lead to overcounting. □

If we take $\sigma = \mathrm{id}$ we expect to recover Lemma 3.3.2 counting the number of common orbits of A and G. This can indeed be seen by identifying $O^{b}_{\sigma} = O^{b}$ and manipulating each sum. As Lemma 4.1.24 does not give expressions which have the form of averages it is impractical to follow the same style of proof as Lemmas 3.3.3 and 4.1.23. This suggests that if the diagonal is assumed to be the only common orbit of A and G of $S \times S$ which is σ-closed, a reformulation in terms of fixed and σ-fixed points may be more involved.

4.2 Difference algebra

This section explores difference fields in more detail with a particular focus on Galois theory and tensor products of difference fields.

4.2.1 Difference fields

We introduce concepts relevant to difference field Galois theory. Further background can be found in [Lev08] and [Wib13].

Definition 4.2.1. Let L, K be difference fields. L is a **difference field extension** of K if there exists an injective σ-**Ring**-morphism $\iota : K \hookrightarrow L$. As this must satisfy $\sigma_L \circ \iota = \iota \circ \sigma_K$, we can think of σ_L as an extension, or 'lift', of σ_K to L.

Definition 4.2.2. Let K be a difference field. The **fixed field of** K, $\mathrm{Fix}(K, \sigma_K)$, is the subset of K consisting of elements which are fixed by the difference action, i.e.

$$\mathrm{Fix}(K, \sigma_K) = \{\lambda \in K \mid \sigma_K(\lambda) = \lambda\}.$$

It is easily verified that this is indeed a field.

Example 4.2.3. Let $\overline{\mathbb{F}}_p$ denote the algebraic closure of a finite field of characteristic p and let φ_p denote the p^{th} power Frobenius, which acts as an automorphism on $\overline{\mathbb{F}}_p$. Then $\mathrm{Fix}(\overline{\mathbb{F}}_p, \varphi_p) = \mathbb{F}_p$.

We now construct a Galois closure of difference fields following Tomašić ([Tom16], Section 5.3). Let L be a difference field and let $\bar{L}$ denote the algebraic closure of $\lfloor L \rfloor$. We can noncanonically extend σ_L to $\bar{\sigma} : \bar{L} \to \bar{L}$ to obtain a difference field extension ([Coh65], Chapter 7, Cor II to Thm I). The following lemma shows that this allows us to define a difference Galois closure with a choice of difference structure.

Lemma 4.2.4. *Let L/K be a finite algebraic difference field extension and let $\bar{L}$ denote the difference algebraic closure of L with choice of difference structure $\bar{\sigma}$. Let M be the normal closure of L/K in $\bar{L}$. Then $\bar{\sigma}(M) \subseteq M$ and so M is a difference field extension of L with $\sigma_M = \bar{\sigma}|_M$.*

Proof. Let $\alpha \in M$. Then α is a conjugate of some $\alpha_1 \in L$, i.e. if $p \in K[x]$ is the minimal polynomial of α_1 over K then α is also a root of p. Consider $\sigma_M(p)$, which is the minimal polynomial of $\sigma_L(\alpha_1)$. Since $\sigma_L(\alpha_1) \in L$, all roots of $\sigma_M(p)$ must lie in M. Hence $\sigma_M(\alpha) \in M$. □

The Galois extension M/L comes with Galois group $G = \mathrm{Gal}(M/L)$. Then for any $g \in G$, $\sigma_M \circ g$ is also an extension of σ_L to M. We therefore obtain a set of lifts of difference structure.

Definition 4.2.5. Let L/K be a finite separable difference field extension, let M be the normal closure of L/K with choice of difference structure σ_M and let $G = \mathrm{Gal}(M/L)$.
The **difference Galois closure of** L/K is the difference field M, equipped with set of lifts $\Sigma_{M/L} = \sigma_M G$.

Note that if M is the difference Galois closure of L/K with choice of difference structure σ_M, then M/L is a difference Galois extension with set of lifts $\Sigma_{M/L}$ and M/K is a difference Galois extension with set of lifts $\Sigma_{M/K} = \sigma_M A$, where $A = \mathrm{Gal}(M/K)$.

Lemma 4.2.6. *Let M/L be a difference Galois extension with choice of difference structure σ_M and Galois group G. Then G can be equipped with a difference endomorphism*

$$()^\sigma : G \to G.$$

The above lemma shows that we can induce a difference structure on the Galois group ([TW18], Lemma 1.23). For $g \in G$, g^σ is defined as the unique $h \in G$ satisfying $g \circ \sigma = \sigma \circ h$.

4.2.2 Connected components of tensor products of difference fields

We now consider connected components of tensor products of difference fields from an algebraic viewpoint, starting with a classical proposition.

Proposition 4.2.7. *Let L, N be field extensions of K, where L/K algebraic and $L = K(\alpha)$. Let f denote the minimal polynomial of α over K. Then there is an isomorphism of N-algebras:*

$$L \otimes_K N \;\cong\; N[x]/(f).$$

If L/K is separable and $f = \prod_{i \in I} f_i$ is a factorisation of f over N then the Chinese Remainder Theorem gives:

$$L \otimes_K N \;\cong\; N[x]/(f) \;\cong\; \prod_{i \in I} N[x]/(f_i).$$

Recall the connected components functor π_0 from Definition 2.2.2. This proposition therefore tells us that we can identify $\pi_0(L \otimes_K N) \cong I$ as sets.

We now consider difference field extensions and the induced difference action on connected components of their tensor products. The action on $\pi_0(L \otimes_K N)$ is obtained from separate actions on L and N, and we can push this across the isomorphism to obtain the corresponding action on I.

Lemma 4.2.8. *Let L/N be difference field extensions of K where the underlying extension $L = K(\alpha)$ is a finite separable extension of K. Let f denote the minimal polynomial of α over K and let $f = \prod_{i \in I} f_i$ be its factorisation over N. Let $p \in K[x]$ such that $\sigma_L(\alpha) = p(\alpha)$.*

Then there is an isomorphism of difference sets:

$$(\pi_0(L \otimes_K N),\ \sigma_L \otimes \sigma_N) \ \cong\ (I,\ \bar{\sigma}),$$

where $\bar{\sigma} : I \to I$ *is defined as:*

$$\bar{\sigma}(i) = i', \qquad \text{where } f_i \mid \sigma_N(f_{i'}) \circ p.$$

Proof. We first justify that $\bar{\sigma}$ is well-defined. Since α is root of both $\sigma_N(f)\circ p$ and its minimal polynomial f, we see that $f \mid \sigma_N(f) \circ p$ and hence $\prod_{i\in I} f_i \mid \prod_{i\in I} \sigma_N(f_i) \circ p$. Therefore for all $i \in I$ there exists $i' \in I$ such that $f_i \mid \sigma_N(f_{i'}) \circ p$.
Moreover L/K is separable, so for distinct $i, i' \in I$ we see that $\gcd(f_i, f_{i'}) = 1$ and hence $\gcd\left(\sigma_N(f_i) \circ p,\ \sigma_N(f_{i'}) \circ p\right) = 1$. Therefore for all i there exists a unique i' such that $f_i \mid \sigma_N(f_{i'}) \circ p$.

Let f' be the minimal polynomial of $\sigma_L(\alpha)$ over K and let $f' = \prod_{j\in J} f'_j$ be its factorisation over N. The diagram below shows the isomorphisms involved. We explicitly define the highlighted maps.

$$\begin{array}{ccccc}
L \otimes_K N & \xrightarrow{\sim} & N[x]/(f) & \xrightarrow{\sim} & \prod_{i\in I} N[x]/(f_i) \\
\downarrow{\scriptstyle \sigma_L\otimes\sigma_N} & & \downarrow{\scriptstyle \sigma_N} & & \downarrow{\scriptstyle \tau} \\
K(\sigma(\alpha)) \otimes_K N & \xrightarrow{\sim} & N[x]/(f') & \xrightarrow{\sim} & \prod_{j\in J} N[x]/(f'_j) \\
\downarrow & & \downarrow{\scriptstyle -\circ p} & & \downarrow{\scriptstyle \iota} \\
L \otimes_K N & \xrightarrow{\sim} & N[x]/(f) & \xrightarrow{\sim} & \prod_{i\in I} N[x]/(f_i)
\end{array}$$

Figure 4.6: Difference action pushed across isomorphisms

- $\sigma_N : N[x]/(f) \to N[x]/(f')$ applies σ_N to polynomial coefficients. Since $\sigma_L(\alpha)$ is a root of both $\sigma_N(f)$ and its minimal polynomial f', we conclude that $f' \mid \sigma_N(f)$ and

hence the map is well-defined.

- $- \circ p : N[x]/(f') \to N[x]/(f)$ is simply precomposition by p. As above α is a root of both $f' \circ p$ and its minimal polynomial f, so $f \mid f' \circ p$ and the map is well-defined.

- $\tau : \prod_{i \in I} N[x]/(f_i) \to \prod_{j \in J} N[x]/(f'_j)$ is given by $\tau(a)_j = \tau_j(a_{\bar{\tau}(j)})$.
  Here $\bar{\tau} : J \to I$ where $\bar{\tau}(j)$ is the unique index such that $f'_j \mid \sigma_N(f_{\bar{\tau}(j)})$. This is well-defined by separability and induces a morphism $\tau_j : N[x]/(f_{\bar{\tau}(j)}) \to N[x]/(f'_j)$.

- $\iota : \prod_{j \in J} N[x]/(f'_j) \to \prod_{i \in I} N[x]/(f_i)$ is given by $\iota(b)_i = \iota_i(b_{\bar{\iota}(i)})$.
  Here $\bar{\iota} : I \to J$ where $\bar{\iota}(i)$ is the unique index such that $f_i \mid f'_{\bar{\iota}(i)} \circ p$. This is well-defined by separability and induces a morphism $\iota_i : N[x]/(f'_{\bar{\iota}(i)}) \to N[x]/(f_i)$.

These can be put together to see how connected components are moved by the difference action. We define:

$$\sigma : \prod_{i \in I} N[x]/(f_i) \longrightarrow \prod_{i \in I} N[x]/(f_i)$$

given by $\sigma = \iota \circ \tau$. Explicitly $\sigma(a)_i = \sigma_i(a_{\bar{\sigma}(i)})$ where:

$\bar{\sigma} : I \to I$	is defined as	$\bar{\sigma} = \bar{\tau} \circ \bar{\iota}$;
$\sigma_i : N[x]/(f_{\bar{\sigma}(i)}) \to N[x]/(f_i)$	is defined as	$\sigma_i = \iota_i \circ \tau_{\bar{\iota}(i)}$.

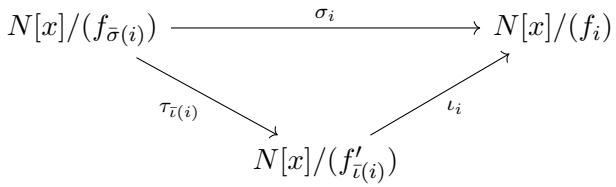

Figure 4.7: The morphism σ_i

By applying definitions we can see that $\bar{\sigma}(i) = \bar{\tau}(\bar{\iota}(i))$ where $f_i \mid f'_{\bar{\iota}(i)} \circ p \mid \sigma_N(f_{\bar{\tau}(\bar{\iota}((i)))}) \circ p$. The morphism σ_i can be visualised in the diagram above. □

Although this difference action seems somewhat convoluted to define we now relate connected components to double cosets and obtain a much simpler description. The idea of associating connected components to group orbits was discussed in Section 3.3; the following lemma enhances this viewpoint.

Lemma 4.2.9. *Let M/K be a difference Galois extension and let L, N be two difference subextensions where L/K is finite separable. Let $A = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$, $F = \mathrm{Gal}(M/N)$ and let $()^\sigma : A \to A$ denote the difference endomorphism on A induced from σ_M. Then there is an isomorphism of difference sets:*

$$(\pi_0(L \otimes_K N),\ \sigma_L \otimes \sigma_N) \ \cong\ (F\backslash A/H,\ \bar{\sigma}),$$

where $F\backslash A/H$ denotes the set of double cosets and $\bar{\sigma}(FaH) = Fa^\sigma H$.

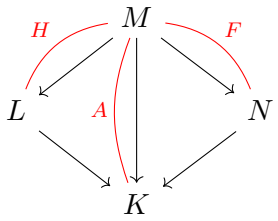

Figure 4.8: Setup of difference field extensions

Proof. As in Lemma 4.2.8 let $L = K(\alpha)$, let f, f' denote the minimal polynomials of $\alpha, \sigma_L(\alpha)$ respectively over K and let $\beta := \sigma_L(\alpha) = p(\alpha)$ for some $p \in K[x]$. Let $f = \prod_{i\in I} f_i$ be its factorisation over N and let $f = (x - \alpha_1)\dots(x - \alpha_l)$ be its factorisation over M where $\alpha_1 = \alpha$.

We therefore have the familiar set of roots $\mathcal{S} = \{\alpha_1, \dots, \alpha_l\}$ and know that A acts trans-

itively on $\mathcal{S}$. We can consider A/H and let $\{a_1, \ldots, a_l\} \subseteq A$ be representatives for each coset. Then $\alpha_i = a_i \cdot \alpha \cong a_i H \cdot \alpha$ mirroring the discussion on page 52.
The factorisation $f = \prod_{i \in I} f_i$ over N corresponds to F-orbits of $\mathcal{S}$ where α, α' are in the same F-orbit if and only if they are roots of the same polynomial f_i. Therefore we see the identification $\pi_0(L \otimes_K N) \cong I \cong F\backslash A/H$.

As in the classical setting, for every i we can consider the conjugate field $L_i = K(\alpha_i)$ (Definition 3.2.8). This comes with an induced difference action $\sigma_{L_i} := a_i \sigma_L a_i^{-1}$ where:

$$\begin{aligned} \sigma_{L_i}(\alpha_i) &= a_i \cdot \sigma_L(a_i^{-1} \cdot \alpha_i) \\ &= a_i \cdot \sigma_L(\alpha) \\ &= a_i \cdot \beta. \end{aligned}$$

In particular $\sigma_{L_1} = \sigma_L$. We introduce the notation $\beta_i := a_i \cdot \beta \in L_i$ and easily see that $\beta_i = p(\alpha_i)$. It remains to determine the induced difference action on $F\backslash A/H$.
The element Fa_iH corresponds to both the component $N[x]/(f_i)$ and the index $i \in I$; we have already shown that $\bar{\sigma}(i) = i'$ where $f_i \mid \sigma_N(f_{i'}) \circ p$. As α_i is a root of f_i it follows that β_i is a root of $\sigma_N(f_{i'})$, i.e. $\beta_i \in \sigma_M(F\alpha_{i'})$. Therefore there exists some $\lambda \in F$ such that $\beta_i = \sigma_M(\lambda \cdot \alpha_{i'}) = \sigma_M(\lambda \cdot a_{i'} \cdot \alpha)$.
On the other hand $\beta_i = a_i \cdot \beta = a_i \cdot \sigma_L(\alpha) = \sigma_M(a_i^\sigma \cdot \alpha)$. As σ_M is a field homomorphism it is injective and we can conclude that $\lambda \cdot a_{i'} \cdot \alpha = a_i^\sigma \cdot \alpha$. The difference action on the double coset space is then given by $\bar{\sigma}(Fa_iH) = Fa_{i'}H = Fa_i^\sigma H$. □

4.3 Foundations of difference algebraic geometry

We enhance the algebraic geometry setting discussed in Chapter 2 by equipping all objects with difference endomorphisms, focusing on affine difference schemes.

4.3.1 Affine difference schemes

Recall that an affine scheme X is isomorphic to $\mathrm{Spec}(R)$ for a commutative ring R.

Definition 4.3.1. The **category of difference schemes**, σ**-Sch**, consists of schemes X together with a scheme endomorphism $\sigma_X : X \to X$. The **category of affine difference schemes**, σ**-AffSch** can be viewed through an equivalence of categories:

$$\sigma\textbf{-AffSch} \;\cong\; (\sigma\textbf{-Ring})^{\mathbf{op}}.$$

As with other difference categories we let $X = (X, \mathcal{O}_X, \sigma_X)$ refer to the difference scheme and may occasionally use $\lfloor X \rfloor = (X, \mathcal{O}_X)$ to explicitly refer to the underlying scheme if necessary.

Definition 4.3.2. A **morphism of difference schemes**, $f : Y \to X$, is a morphism of schemes satisfying $\sigma_X \circ f = f \circ \sigma_Y$.
In the case of affine schemes if $Y = \mathrm{Spec}(R)$, $X = \mathrm{Spec}(T)$, then f corresponds to a σ**-Ring**-morphism $f : T \to R$ satisfying $\sigma_R \circ f = f \circ \sigma_T$. As the categories are anti-equivalent we can use f to denote both morphisms without confusion.

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ {\scriptstyle \sigma_Y}\downarrow & & \downarrow{\scriptstyle \sigma_X} \\ Y & \xrightarrow{f} & X \end{array} \qquad\qquad \begin{array}{ccc} T & \xrightarrow{f} & R \\ {\scriptstyle \sigma_T}\downarrow & & \downarrow{\scriptstyle \sigma_R} \\ T & \xrightarrow{f} & R \end{array}$$

Figure 4.9: Morphism of affine difference schemes

We draw attention to the following definition as it plays a role in our difference exceptionality results. Recall that the difference structure on the fibre product is extended by action on each component (Definition 4.1.5).

Definition 4.3.3. Let X, Y be difference schemes with a morphism $f : Y \to X$. The **diagonal subscheme**, $\Delta_Y \subseteq Y \times_X Y$, is the difference subscheme defined as the image of the **diagonal embedding** $\Delta : Y \hookrightarrow Y \times_X Y$ in σ**-Sch**. It can easily be verified that Δ_Y is a difference subobject.

There are several types of points in a difference scheme (see Definition 2.1.10). The definitions of closed and generic points remain the same but we make slight alterations to the others.

Definition 4.3.4. Let $X = \mathrm{Spec}(R)$ be a difference scheme.

- A **fixed scheme-theoretic point** of X is a point $x \in X$ such that $\sigma_X(x) = x$. The **set of fixed scheme-theoretic points of** X is denoted X^σ.
- For a difference field F, an F**-rational point** is a σ**-Sch**-morphism $a : \mathrm{Spec}(F) \to X$, which therefore satisfies $\sigma_X \circ a = a \circ \sigma_F$.
- For an algebraically closed difference field (Ω, ω), a **geometric point** is a σ**-Sch**-morphism $\bar{x} : \mathrm{Spec}(\Omega) \to X$, which therefore satisfies $\sigma_X \circ \bar{x} = \bar{x} \circ \omega$.

Example 4.3.5. We give an example of a difference scheme modelling a difference equation. Recall the difference equation describing the Fibonacci sequence (page 12). Let $\mathbb{N}^\infty$ denote the difference ring of sequences in $\mathbb{N}$, i.e.

$$\mathbb{N}^\infty \ := \ \{F = (F_0, F_1, F_2, \dots) \mid F_i \in \mathbb{N}\},$$

where $\sigma(F)_n = F_{n+1}$. We then take the difference ring obtained by quotienting by the difference equation $\sigma^2(F) = \sigma(F) + F$:

$$\mathbb{N}^\infty/\langle \sigma^2(F) - \sigma(F) - F \rangle$$
$$= \{(F_0, F_1, F_2, \dots) \mid (F_2, F_3, F_4, \dots) = (F_1, F_2, F_3, \dots) + (F_0, F_1, F_2, \dots)\}.$$

Difference rational points then correspond to solutions of the Fibonacci equation. The original sequence can be recovered by specifying initial conditions.

Definition 4.3.6. Let S be a difference scheme. A difference scheme X is said to be **defined over** S if it comes equipped with a σ-**Sch**-morphism $X \to S$.
The **category of difference schemes over** S is denoted σ-**Sch**$/S$.
Let K be a difference field. The **category of finite affine difference schemes over** K is denoted K-σ-**FAffSch** and we identify:

$$K\text{-}\sigma\text{-}\mathbf{FAffSch} \cong K\text{-}\sigma\text{-}\mathbf{FAlg}^{\mathbf{op}}.$$

If X, Y are both defined over S then a morphism $f : Y \to X$ satisfies the commutative diagram below. Note that the structure maps are required to be σ-**Sch**-morphisms but morphisms of relative difference schemes restrict to the identity on the base as in the usual setting.

This is where we start to see the level of complexity that comes with introducing a difference endomorphism in a relative setting. Let X be a difference scheme defined over a difference field (k, ς), let F be a difference field extension of k and let $a : \mathrm{Spec}(F) \to X$ be an F-rational point of X. Here we cannot conclude that $\sigma_X \circ a \in X(F)$ as it does not restrict to the identity on $\mathrm{Spec}(k)$.
Let X_ς denote the base change of X with respect to $\varsigma : k \to k$. Using the universal property

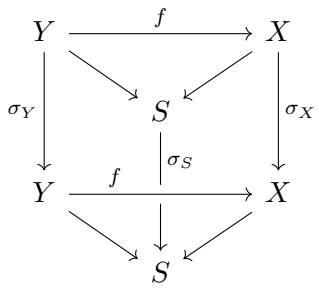

Figure 4.10: Morphism of relative difference schemes

we see from the diagram below that there is a unique morphism $\bar{\sigma} : X \to X_\varsigma$. Here we let π denote the structure map of X and let π_ς denote the structure map of X_ς obtained from the base change construction.

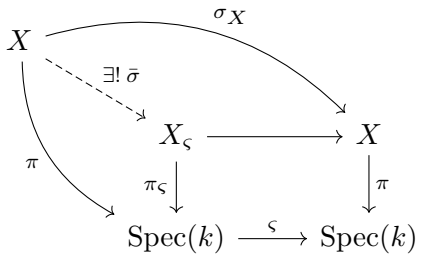

Figure 4.11: Base change of X with respect to ς

Proposition 4.3.7. *Let X be a difference scheme defined over a difference field (k, ς), let F be a difference field extension of k, let $a \in X(F)$ and let $\bar{\sigma} : X \to X_\varsigma$ be constructed as above. Then $\bar{\sigma} \circ a$ is an F-rational point of X_ς.*

Proof. It suffices to prove that $\bar{\sigma} \circ a : \mathrm{Spec}(F) \to X_\varsigma$ is a morphism of relative difference schemes so we must show that it satisfies a commutative diagram analogous to that in Figure 4.10. X_ς has an induced difference morphism which can be found by base changing $\varsigma : \mathrm{Spec}(k) \to \mathrm{Spec}(k)$ with respect to the structure map $\pi_\varsigma : X_\varsigma \to \mathrm{Spec}(k)$. Denote this by $\sigma_\varsigma : X_\varsigma \to X_\varsigma$.

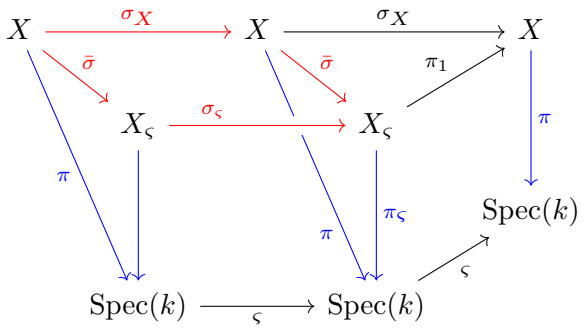

Figure 4.12: $\bar{\sigma} \circ \sigma_X = \sigma_\varsigma \circ \bar{\sigma}$

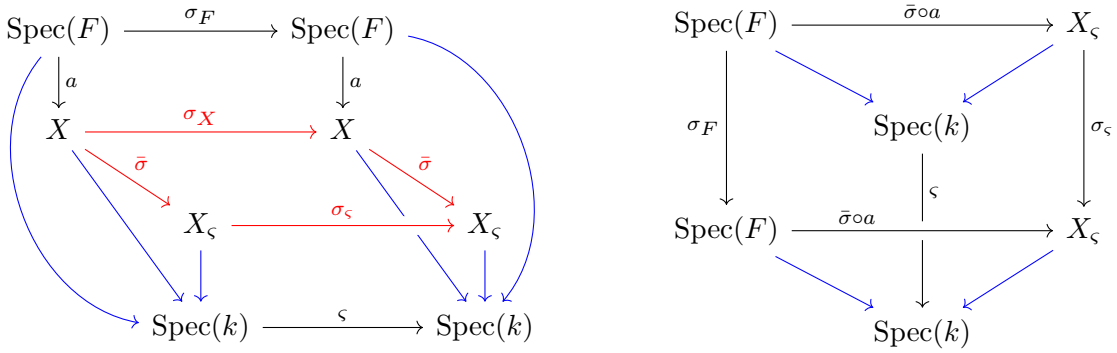

Figure 4.13: $\bar{\sigma} \circ a$ is an F-rational point of X_ς

Figure 4.12 is now built up from the square defining σ_ς by adding $\bar{\sigma} : X \to X_\varsigma$ in two places; we also append a copy of the base change square defining X_ς to allow us to check commutativity. By checking that the outside maps commute we can conclude that $\bar{\sigma} \circ \sigma_X = \sigma_\varsigma \circ \bar{\sigma}$. This square is highlighted in red and structure maps down to k are highlighted in blue for clarity.

Add in the rational point $a : \mathrm{Spec}(F) \to X$ and then extract the required commutative diagram to see that $\bar{\sigma} \circ a$ is an F-rational point of X_ς. This is shown in Figure 4.13. □

We will focus on difference schemes defined over a difference field with identity (k, id) to remove the need for these considerations.

We now revisit residue fields and their relationship to rational points. Let X be a difference scheme and let x be a scheme-theoretic point of $\lfloor X \rfloor$ with residue field $\kappa(x)$. We aim to equip $\kappa(x)$ with a difference endomorphism. We see from Lemma 2.1.20 that $\sigma_X : X \to X$ induces a morphism of stalks $\sigma_x^{\#} : \mathcal{O}_{X,\sigma_X(x)} \to \mathcal{O}_{X,x}$, which in turn induces $\kappa(\sigma_X(x)) \to \kappa(x)$. We therefore conclude that in order to define a difference structure on $\kappa(x)$, the point x must be fixed by σ_X.

Definition 4.3.8. Let X be a difference scheme and let $x \in X^\sigma$, i.e. $\sigma_X(x) = x$. The **residue field** at x, $\kappa(x)$, is the difference field consisting of $\kappa(x)$ together with

$$\sigma^x : \kappa(x) \to \kappa(x),$$

where σ^x denotes the morphism induced from $\sigma_X : X \to X$ via $\sigma_x^{\#} : \mathcal{O}_{X,\sigma_X(x)} \to \mathcal{O}_{X,x}$.

Lemma 4.3.9. *Let F be a difference field (or a difference ring with an injective endomorphism) and let $a \in X(F)$. Then a factors through a fixed scheme-theoretic point, i.e. there exists $x \in X^\sigma$ such that the diagram below commutes.*

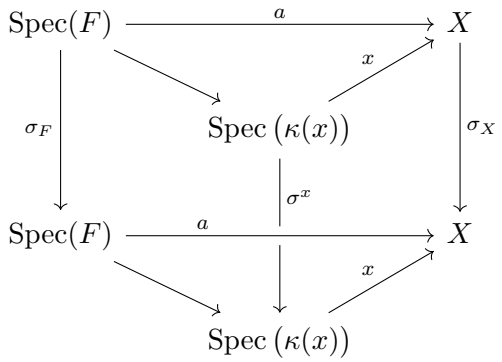

Figure 4.14: Rational point factoring through a fixed scheme-theoretic point

Proof. Let $X = \mathrm{Spec}(R)$ for some difference ring R: our rational point therefore corresponds to a σ-**Ring**-morphism $a : R \to F$ satisfying the diagram below.

$$\begin{array}{ccc} R & \xrightarrow{a} & F \\ {\scriptstyle \sigma_R}\downarrow & & \downarrow{\scriptstyle \sigma_F} \\ R & \xrightarrow[a]{} & F \end{array}$$

Figure 4.15: The rational point a considered in σ-**Ring**

Let $\mathfrak{p} = \ker(a)$ and we claim that $\sigma_R^{-1}(\mathfrak{p}) = \mathfrak{p}$. Let $r \in \sigma_R^{-1}(\mathfrak{p})$ so $\sigma_R(r) \in \mathfrak{p}$. As σ_F is injective we see that $\sigma_F(a(r)) = a(\sigma_R(r)) = 0$ and hence $a(r) = 0$, i.e. $r \in \mathfrak{p}$. Similarly it can be seen that $\mathfrak{p} \subseteq \sigma_R^{-1}(\mathfrak{p})$ by using that σ_F is a homomorphism.
Let x be the scheme-theoretic point in X which corresponds to the prime ideal $\mathfrak{p}$, so $\sigma_X(x) = x$. Then it is clear that a factors through x and that the required diagram commutes. □

We finally introduce the definition of a transformally integral scheme; the parallels between this and the notion of an integral scheme are clear (Definition 2.2.4).

Definition 4.3.10. An element r of a difference ring R is **σ-nilpotent** if there exists $n \in \mathbb{N}$ such that $\sigma^n(r) = 0$.
A difference ring R is **perfectly reduced** if R has no non-zero σ-nilpotents. A difference scheme X is **perfectly reduced** if for every open set $U \subseteq X$, its associated ring $\mathcal{O}_X(U)$ is perfectly reduced.

Definition 4.3.11. A difference scheme X is **transformally integral** if it is algebraically irreducible and perfectly reduced. An affine difference scheme $\mathrm{Spec}(R)$ is therefore transformally integral if R is a domain with no non-zero σ-nilpotents.
A difference scheme X defined over a difference field F is **geometrically transformally integral** if X remains transformally integral under any base change, i.e. for any difference field extension F'/F, the difference scheme $X_{F'} = X \times_F F'$ is transformally integral.

Definition 4.3.12. Let X be a difference scheme defined over a difference field F. For

$x \in X^\sigma$ let $\mathrm{trdeg}_F(\kappa(x))$ denote the transcendence degree of the underlying extension $\kappa(x)/F$.

The **total dimension of X over F**, denoted $\mathrm{dimtot}_F(X)$, is defined as:

$$\mathrm{dimtot}_F(X) := \max_{x \in X^\sigma} \mathrm{trdeg}_F(\kappa(x)).$$

If no maximum exists the total dimension is considered to be infinite.

A generalisation of the Lang-Weil bound (Theorem 2.2.21) has been formulated for difference schemes by Hrushovski. We give a simplified version of this result which will suffice for our purposes but the full statement can be found in the original preprint ([Hru04], Section 10.5, Thm 1B).

Theorem 4.3.13 (Hrushovski's twisted Lang-Weil bound)**.** *Let X be a geometrically transformally integral difference scheme of finite total dimension d over a finite difference field k_o. Then there exists constants $C, c, \mu > 0$ depending only on the geometric data of X such that for every finite field k such that $|k| > c$ and $(\bar{k}, \varphi_k)$ extends k_o:*

$$\left| |X(\bar{k}, \varphi_k)| - \mu |k|^d \right| < C|k|^{d-\frac{1}{2}}.$$

This theorem is easily applied to obtain the following corollary.

Corollary 4.3.14. *Let X be a geometrically transformally integral difference scheme of finite total dimension over a finite difference field k_o. Then for every finite field k such that $|k|$ is large enough and $(\bar{k}, \varphi_k)$ extends k_o, the set $X(\bar{k}, \varphi_k)$ is finite.*

4.3.2 Difference Galois covers and local substitutions

In this section we define difference Galois covers of normal difference schemes, local substitutions for difference rational points and difference Galois closures.

Definition 4.3.15. Let Y, Z be difference schemes. Then $p : Z \to Y$ is a **difference Galois cover** if the underlying morphism $\lfloor Z \rfloor \to \lfloor Y \rfloor$ is a Galois cover (Definition 2.3.1).

This defines a finite Galois cover which will suffice for our purposes, but the more general notion of an infinite Galois cover of finite σ-presentation has also been developed. Further details on this will be discussed in forthcoming work by Tomašić.
We can also define the following sets of difference actions.

Definition 4.3.16. Let Z be a difference scheme with difference set Σ and let $z \in Z$.
The **stabiliser of** z **in** Σ, denoted Σ_z, is defined as:

$$\Sigma_z = \{\tau \in \Sigma \mid \tau(z) = z\}.$$

The **set of residue field morphisms of** z, denoted Σ^z, is defined as:

$$\Sigma^z = \{\tau^z : \kappa(z) \to \kappa(z) \mid \tau \in \Sigma_z\},$$

where τ^z is the residue field morphism given in Definition 4.3.8.

Definition 4.3.17. Let $p : Z \to Y$ be a difference Galois cover with choice of difference structure σ_Z and Galois group G. Let (Ω, ω) be an algebraically closed difference field. Let $\bar{y} \in Y(\Omega, \omega)$ be a difference rational point and let $\bar{z} \in \lfloor Z \rfloor(\Omega)$ be a rational point lying above $\bar{y}$.
The **local** ω**-substitution of** $\bar{z}$ is the element $\tau \in \Sigma$ such that $\tau \circ \bar{z} = \bar{z} \circ \omega$. We can therefore consider $\bar{z} \in Z(\Omega, \omega)$ as a difference rational point.

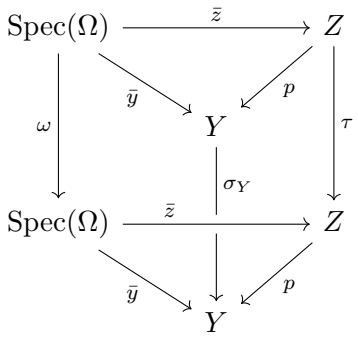

Figure 4.16: Difference rational point $\bar{z} \in Z(\Omega, \omega)$ with local ω-substitution τ

It is easily verified that such a τ exists. As $\bar{z}$ lies above $\bar{y}$ we see that:

$$p\sigma_Z\bar{z} \;=\; \sigma_Y p\bar{z} \;=\; \sigma_Y\bar{y} \;=\; \bar{y}\omega \;=\; p\bar{z}\omega.$$

Therefore there exists $g \in G$ such that $g \cdot \sigma_Z\bar{z} = \bar{z}\omega$ and we select $\tau = g\sigma_Z$.

Proposition 4.3.18. *Assume the setup of Definition 4.3.17. Let $\bar{z}, \bar{z}' \in Z(\Omega, \omega)$ be two lifts of $\bar{y} \in Y(\Omega, \omega)$ and let τ, τ' denote their respective local ω-substitutions. Then τ, τ' are G-conjugate.*

Proof. Since $\bar{z}, \bar{z}'$ lie in the same fibre over $\bar{y}$, there exists $g \in G$ such that $g \cdot \bar{z} = \bar{z}'$. Then:

$$(g^{-1}\tau' g)\bar{z} \;=\; g^{-1}\tau'\bar{z}' \;=\; g^{-1}\bar{z}'\omega \;=\; \bar{z}\omega \;=\; \tau\bar{z}.$$

□

Definition 4.3.19. Assume the setup of Definition 4.3.17. Let $\bar{z} \in Z(\Omega, \omega)$ be a lift of $\bar{y} \in Y(\Omega, \omega)$ with local ω-substitution τ. The **local ω-substitution of** $\bar{y}$ is the G-conjugacy class $[\tau]$.

We will only require the construction of a difference Galois closure in the special case of

normal difference schemes. Note that a generically étale morphism of normal difference schemes corresponds to a finite separable extension of function fields.

Definition 4.3.20. Let X, Y be normal difference schemes and let K, L denote their function fields respectively. Let $f : Y \to X$ be a generically étale morphism which induces a finite separable extension L/K. Let M denote the difference Galois closure of L/K with choice of difference structure σ_M and let $G = \mathrm{Gal}(M/L)$. Let Z denote the normalisation of Y in M with induced difference structure σ_Z.
The **difference Galois closure of** f is the difference scheme Z, equipped with set of lifts $\Sigma_{Z/Y} = G\sigma_Z$.

Note that Z is a difference Galois cover of Y with set of lifts $\Sigma_{Z/Y}$ and a difference Galois cover of X with set of lifts $\Sigma_{Z/X} = A\sigma_Z$, where $A = \mathrm{Gal}(Z/X)$.

Chapter 5

Difference Galois theory

This chapter builds on Grothendieck's Galois theory discussed in Section 2.4. We replicate this in the setting of difference algebraic geometry, utilising a more general categorical theory by Borceux-Janelidze in order to achieve this. We choose a particular setup for this result and obtain a difference Galois correspondence.

5.1 Categorical Galois theory

In this section we describe the categorical Galois correspondence as found in Borceux-Janelidze ([BJ01], Chapter 5). The links between these abstract categorical definitions and the more familiar Galois theoretic correspondence will become clear when we describe a specific application to a difference context in Section 5.2. Throughout we assume that all categories are locally small with pullbacks.

Definition 5.1.1. Let $\mathcal{C}, \mathcal{D}$ be categories and let $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$ be functors. The functor $\mathcal{H}$

is **right adjoint to** $\mathcal{I}$, denoted $\mathcal{I} \dashv \mathcal{H}$, if for all $A \in \mathcal{C}$, $B \in \mathcal{D}$, there is a bijection:

$$\Phi_{A,B} : \ \mathrm{Hom}_{\mathcal{D}}(\mathcal{I}(A), B) \ \xrightarrow{\sim} \ \mathrm{Hom}_{\mathcal{C}}(A, \mathcal{H}(B)).$$

The functors are said to form an **adjunction** and we can define two natural transformations:

$$\begin{aligned} &\eta : \mathrm{Id}_{\mathcal{C}} \to \mathcal{H}\mathcal{I}, && \text{where } \ \eta_A \ := \ \Phi_{A,\mathcal{I}(A)}(\mathrm{id}_{\mathcal{I}(A)}); \\ &\epsilon : \mathcal{I}\mathcal{H} \to \mathrm{Id}_{\mathcal{D}}, && \text{where } \ \epsilon_B \ := \ \Phi^{-1}_{\mathcal{H}(B),B}(\mathrm{id}_{\mathcal{H}(B)}). \end{aligned}$$

Here η, ϵ are the **unit** and **counit** of the adjunction respectively.

Definition 5.1.2. Let $\mathcal{C}$ be a category and let $C \in \mathcal{C}$. The **slice category of $\mathcal{C}$ over** C, denoted $\mathcal{C}/C$, consists of:

- Objects (A, α), where $A \in \mathcal{C}$ and $\alpha \in \mathrm{Hom}_{\mathcal{C}}(A, C)$;
- Morphisms $f : (A, \alpha) \to (B, \beta)$, where $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ such that $\beta \circ f = \alpha$.

The next lemma allows us to consider adjunctions of slice categories without issue. We will implicitly use this throughout the rest of the chapter.

Lemma 5.1.3. *Let $\mathcal{C}$, $\mathcal{D}$ be categories and let $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$ be an adjunction where $\mathcal{H}$ is right adjoint to $\mathcal{I}$. For $C \in \mathcal{C}$ let $\mathcal{C}/C$, $\mathcal{D}/\mathcal{I}(C)$ denote the associated slice categories. Then the induced functors between the slice categories also form an adjunction, i.e.*

$$\begin{aligned} \mathcal{I}_C : \qquad \mathcal{C}/C \qquad &\longrightarrow \qquad \mathcal{D}/\mathcal{I}(C) \\ (A, \alpha) \qquad &\longmapsto \qquad (\mathcal{I}(A), \mathcal{I}(\alpha)) \end{aligned}$$

has a right adjoint functor

$$\begin{array}{lccc} \mathcal{H}_C : & \mathcal{D}/\mathcal{I}(C) & \longrightarrow & \mathcal{C}/C \\ & (B,\beta) & \longmapsto & (Z,\pi_2), \end{array}$$

where (Z,π_2) *is defined by the pullback diagram below.*

$$\begin{array}{ccc} Z & \xrightarrow{\pi_1} & \mathcal{H}(B) \\ {\scriptstyle \pi_2}\downarrow & & \downarrow{\scriptstyle \mathcal{H}(\beta)} \\ C & \xrightarrow[\eta_C]{} & \mathcal{H}\mathcal{I}(C) \end{array}$$

Figure 5.1: Pullback diagram defining Z

Proof. Let $(A,\alpha) \in \mathcal{C}/C$, $(B,\beta) \in \mathcal{D}/\mathcal{I}(C)$. Consider the following diagrams, where the right diagram is obtained by applying $\mathcal{I}$ to the left and adjoining morphisms coming from the universal property of adjunctions and the counit-unit adjunction identity.

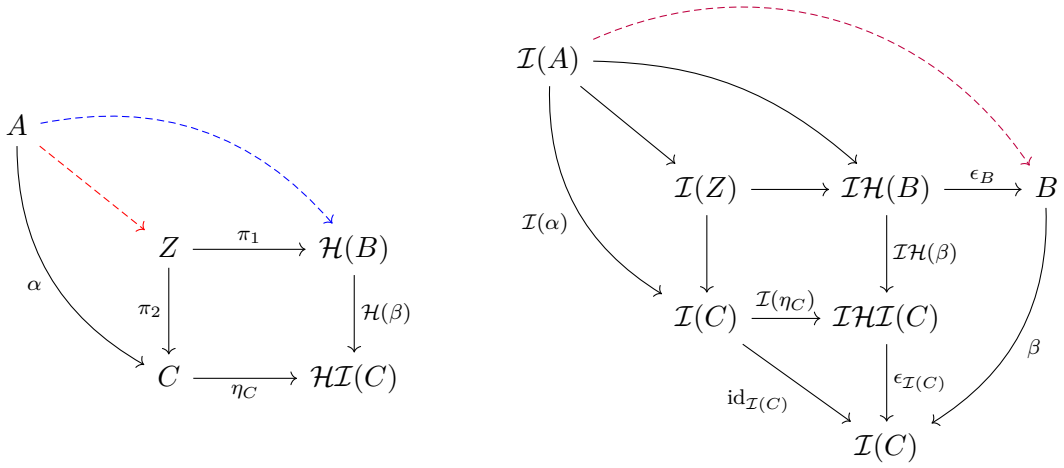

Figure 5.2: The pullback diagram defining Z before and after applying $\mathcal{I}$

Using the underlying adjunction we can then see that $\mathcal{H}_C$ is right adjoint to $\mathcal{I}_C$:

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}/C}\Big((A,\alpha),\mathcal{H}_C(B,\beta)\Big) &= \mathrm{Hom}_{\mathcal{C}/C}\Big((A,\alpha),(Z,\pi_2)\Big)\\ &\cong \mathrm{Hom}_{\mathcal{C}/\mathcal{H}\mathcal{I}(C)}\Big((A,\eta_C\circ\alpha),(\mathcal{H}(B),\mathcal{H}(\beta)\Big)\\ &\cong \mathrm{Hom}_{\mathcal{D}/\mathcal{I}(C)}\Big((\mathcal{I}(A),\mathcal{I}(\alpha)),(B,\beta)\Big)\\ &= \mathrm{Hom}_{\mathcal{D}/\mathcal{I}(C)}\Big(\mathcal{I}_C(A,\alpha),(B,\beta)\Big).\end{aligned}$$

□

We now unpack the notions required to define a monadic functor. Further background on monads can be found in Mac Lane ([ML98], Chapter VI).

Definition 5.1.4. Let $\mathcal{C},\mathcal{D}$ be categories with an adjunction $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$, where $\mathcal{H}$ is right adjoint to $\mathcal{I}$. The **monad induced by** $\mathcal{I}\dashv\mathcal{H}$, denoted $\mathbb{T}$, is a triple $\mathbb{T}=(T,\mu,\eta)$, where:

- $T=\mathcal{H}\circ\mathcal{I}:\ \mathcal{C}\to\mathcal{C}$ is an endofunctor;
- $\mu=\mathcal{H}\epsilon\mathcal{I}:\ TT\to T$;
- η is the unit of the adjunction.

Definition 5.1.5. Let $\mathcal{C},\mathcal{D}$ be categories with an adjunction $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$, where $\mathcal{H}$ is right adjoint to $\mathcal{I}$, and let $\mathbb{T}=(T,\mu,\eta)$ be its induced monad. A **T-algebra** is a pair (A,ν), where:

- A is an object in $\mathcal{C}$;
- $\nu: T(A)\to A$ satisfies the following properties:

  (i) $\nu\circ\mu_A=\nu\circ T(\nu)$;

(ii) $\nu \circ \eta_A = \mathrm{id}_A$.

These properties are shown in the diagrams below.

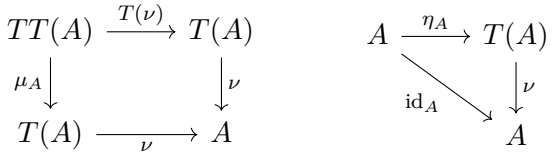

Figure 5.3: Diagrams satisfied by $\nu : T(A) \to A$

The category of T-algebras in $\mathcal{C}$, denoted $\mathcal{C}^{\mathbb{T}}$, is often referred to as the **Eilenberg-Moore category of the monad** $\mathbb{T}$.

Definition 5.1.6. Let $\mathcal{C}, \mathcal{D}$ be categories with an adjunction $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$, where $\mathcal{H}$ is right adjoint to $\mathcal{I}$, and let $\mathbb{T} = (T, \mu, \eta)$ be its induced monad. The **comparison functor**, $\mathcal{K}^{\mathbb{T}}$, is defined as:

$$\begin{array}{lccc} \mathcal{K}^{\mathbb{T}} : & \mathcal{D} & \longrightarrow & \mathcal{C}^{\mathbb{T}} \\ & B & \longmapsto & (\mathcal{H}(B), \mathcal{H}(\epsilon_B)). \end{array}$$

The functor $\mathcal{H} : \mathcal{D} \to \mathcal{C}$ is **monadic** if the comparison functor $\mathcal{K}^{\mathbb{T}}$ defines an equivalence of categories.

This allows us to define split objects and morphisms of relative Galois descent. We now transition into considering slice categories.

Definition 5.1.7. Let $\mathcal{C}$ be a category, let $L, K \in \mathcal{C}$ and let $\varphi : L \to K$ be a $\mathcal{C}$-morphism.

The **pullback functor induced by** φ, denoted $\varphi^* : \mathcal{C}/K \to \mathcal{C}/L$, is defined as:

$$\begin{array}{rccc} \varphi^* : & \mathcal{C}/K & \longrightarrow & \mathcal{C}/L \\ & (A, \alpha) & \longmapsto & (A \times_K L, \varphi^*\alpha), \end{array}$$

where the pullback defining φ^* is shown in the diagram below.

$$\begin{array}{ccc} A \times_K L & \longrightarrow & A \\ {\scriptstyle \varphi^*\alpha}\downarrow & & \downarrow{\scriptstyle \alpha} \\ L & \xrightarrow{\varphi} & K \end{array}$$

Figure 5.4: Pullback diagram defining φ^*

This admits a left adjoint functor, denoted $\varphi_! : \mathcal{C}/L \to \mathcal{C}/K$, defined as:

$$\begin{array}{rccc} \varphi_! : & \mathcal{C}/L & \longrightarrow & \mathcal{C}/K \\ & (B, \beta) & \longmapsto & (B, \varphi \circ \beta) \ . \end{array}$$

Definition 5.1.8. Let $\mathcal{C}, \mathcal{D}$ be categories with an adjunction $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$, where $\mathcal{H}$ is right adjoint to $\mathcal{I}$. Let $L, K \in \mathcal{C}$ and let $\varphi : L \to K$ be a $\mathcal{C}$-morphism. An object $A \in \mathcal{C}/K$ is **split by the morphism** φ if the unit of the adjunction at the object $\varphi^*(A)$ is an isomorphism, i.e.

$$\eta_{\varphi^*(A)} : \ \varphi^*(A) \ \xrightarrow{\sim} \ \mathcal{H}_L\mathcal{I}_L\varphi^*(A).$$

The **category of objects in** $\mathcal{C}/K$ **which are split by** φ is denoted $\mathbf{Spl}_K(\varphi)$.

Definition 5.1.9. Let $\mathcal{C}, \mathcal{D}$ be categories with an adjunction $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$, where $\mathcal{H}$ is right adjoint to $\mathcal{I}$ and the counit ϵ is an isomorphism. Let $L, K \in \mathcal{C}$. A morphism $\varphi : L \to K$ is

of **relative Galois descent** if the following conditions are satisfied:

(i) The pullback functor $\varphi^* : \mathcal{C}/K \to \mathcal{C}/L$ is monadic;

(ii) The counit of the adjunction $\mathcal{I}_L \dashv \mathcal{H}_L$ is an isomorphism, i.e.

$$\epsilon : \mathcal{I}_L\mathcal{H}_L \xrightarrow{\sim} \mathrm{id}_{\mathcal{D}/\mathcal{I}(L)};$$

(iii) For every object $B \in \mathcal{D}/\mathcal{I}(L)$, the object $\varphi_!\mathcal{H}_L(B) \in \mathcal{C}/K$ is split by φ, i.e.

$$\eta_{\varphi_!\mathcal{H}_L(B)} : \ \varphi^*(\varphi_!\mathcal{H}_L(B)) \ \xrightarrow{\sim} \ \mathcal{H}_L\mathcal{I}_L\varphi^*(\varphi_!\mathcal{H}_L(B)).$$

We will fix a morphism of relative Galois descent and consider those objects which are split by it.

The final ingredients required for the main theorem are groupoids internal to the category $\mathcal{D}$ and internal covariant presheaves. Comparing to the previous formulation of Galois categories in Section 2.4, these notions can be seen to correspond to fundamental groups and finite sets equipped with their action.

Definition 5.1.10. Let $\mathcal{C}$, $\mathcal{D}$ be categories and let $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$ be an adjunction where $\mathcal{H}$ is right adjoint to $\mathcal{I}$. Let $L, K \in \mathcal{C}$ and let $\varphi : L \to K$ be a morphism of relative Galois descent in $\mathcal{C}$. The **internal groupoid induced by** φ, denoted $\mathrm{Gal}[\varphi]$, is a groupoid internal to the category $\mathcal{D}$.

Let $L \times_K L$ be the pullback obtained by taking φ in both components. Then $\mathrm{Gal}[\varphi]$ has object-of-objects $\mathcal{I}(L)$ and object-of-morphisms $\mathcal{I}(L \times_K L)$ together with the following morphisms:

- source morphism, $\mathcal{I}(\pi_1)$, where π_1 denotes the first projection $L \times_K L \to L$;
- target morphism, $\mathcal{I}(\pi_2)$, where π_2 denotes the second projection $L \times_K L \to L$;
- identity morphism, $\mathcal{I}(\Delta)$, where Δ denotes the diagonal map $L \to L \times_K L$;
- multiplication morphism, $(\mathcal{I}(p_1), \mathcal{I}(p_4))$, where p_i denotes the i^{th} projection $(L \times_K L) \times_L (L \times_K L) \to L$;
- twisting isomorphism, $\mathcal{I}(\tau)$, where τ switches the components of $L \times_K L$.

The pullback $(L \times_K L) \times_L (L \times_K L)$ is defined using π_1, π_2 as in the diagram below to ensure compatibility of multiplication.

$$\begin{array}{ccc} (L \times_K L) \times_L (L \times_K L) & \longrightarrow & L \times_K L \\ \downarrow & & \downarrow{\scriptstyle \pi_2} \\ L \times_K L & \xrightarrow[\pi_1]{} & L \end{array}$$

Figure 5.5: Pullback diagram defining $(L \times_K L) \times_L (L \times_K L)$

$$\begin{array}{ccccc} & & \overset{\mathcal{I}(\tau)}{\curvearrowright} & & \\ \mathcal{I}(L) & \xrightarrow{\mathcal{I}(\Delta)} & \mathcal{I}(L \times_K L) & \xleftarrow{(\mathcal{I}(p_1),\ \mathcal{I}(p_4))} & \mathcal{I}(L \times_K L) \times_{\mathcal{I}(L)} \mathcal{I}(L \times_K L) \\ & & \mathcal{I}(\pi_1) \downarrow \downarrow \mathcal{I}(\pi_2) & & \\ & & \mathcal{I}(L) & & \end{array}$$

Figure 5.6: The internal groupoid $\mathrm{Gal}[\varphi]$

We can also view the internal groupoid $\mathrm{Gal}[\varphi]$ diagrammatically showing the morphisms listed above.

Definition 5.1.11. Let $\mathcal{C}$, $\mathcal{D}$ be categories and let $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$ be an adjunction where $\mathcal{H}$ is right adjoint to $\mathcal{I}$. Let $L, K \in \mathcal{C}$ and let $\varphi : L \to K$ be a morphism of relative Galois descent in $\mathcal{C}$. An **internal covariant presheaf on the internal groupoid** $\mathrm{Gal}[\varphi]$ is a

triple (F, f, ζ) where:

(i) $F \in \mathcal{D}$;

(ii) $f : F \to \mathcal{I}(L)$ is a morphism in $\mathcal{D}$;

(iii) $\zeta : \mathcal{I}(L \times_K L) \times_{\mathcal{I}(L)} F \to F$ is a morphism in $\mathcal{D}$, where the first square below describes the pullback and the second square commutes.

$$\begin{array}{ccc} \mathcal{I}(L \times_K L) \times_{\mathcal{I}(L)} F & \longrightarrow & \mathcal{I}(L \times_K L) \\ \downarrow & & \downarrow{\scriptstyle \mathcal{I}(\pi_1)} \\ F & \xrightarrow[f]{} & \mathcal{I}(L) \end{array} \qquad \begin{array}{ccc} \mathcal{I}(L \times_K L) \times_{\mathcal{I}(L)} F & \longrightarrow & \mathcal{I}(L \times_K L) \\ {\scriptstyle \zeta}\downarrow & & \downarrow{\scriptstyle \mathcal{I}(\pi_2)} \\ F & \xrightarrow[f]{} & \mathcal{I}(L) \end{array}$$

Figure 5.7: Diagrams characterising $\mathcal{I}(L \times_K L) \times_{\mathcal{I}(L)} F$

The **category of internal covariant presheaves on** $\mathrm{Gal}[\varphi]$ is denoted $\mathcal{D}^{\mathrm{Gal}[\varphi]}$.

We can finally give a Galois correspondence in this adjunction setting ([BJ01], Thm 5.1.24).

Theorem 5.1.12 (Categorical Galois correspondence)**.** *Let $\mathcal{C}, \mathcal{D}$ be categories with an adjunction $\mathcal{C} \underset{\mathcal{H}}{\overset{\mathcal{I}}{\rightleftarrows}} \mathcal{D}$, where $\mathcal{H}$ is right adjoint to $\mathcal{I}$. Let $L, K \in \mathcal{C}$ and let $\varphi : L \to K$ be a morphism of relative Galois descent in $\mathcal{C}$. Then there exists an equivalence of categories between the category of objects of $\mathcal{C}/K$ which are split by φ and the category of internal covariant presheaves in $\mathcal{D}$ on* $\mathrm{Gal}[\varphi]$*, i.e.*

$$\mathbf{Spl}_K(\varphi) \;\cong\; \mathcal{D}^{\mathrm{Gal}[\varphi]}.$$

5.2 A difference Galois correspondence

Let K be a difference field. We now apply the theory in the previous section to the dual category of finite dimensional K-σ-algebras: K-σ-**FAlg**$^{\mathbf{op}} \cong K$-σ-**FAffSch** (Definition 4.3.6). We follow the same structure, identifying the relevant objects and verifying that they satisfy the required conditions.

A general lemma is required. For a category $\mathcal{C}$ the difference category σ-$\mathcal{C}$ can be constructed by equipping all objects with endomorphisms. This is analogous to the construction of σ-**Set** in Section 4.1.

Lemma 5.2.1. *Let $\mathcal{C}$, $\mathcal{D}$ be categories and let $\mathcal{C} \underset{\mathcal{H}_o}{\overset{\mathcal{I}_o}{\rightleftarrows}} \mathcal{D}$ be an adjunction, where $\mathcal{H}_o$ is right adjoint to $\mathcal{I}_o$. Let $\mathcal{I}, \mathcal{H}$ denote the induced functors between the difference categories σ-$\mathcal{C}$ and σ-$\mathcal{D}$, i.e.*

$$\begin{aligned} &\mathcal{I} : \sigma\text{-}\mathcal{C} \to \sigma\text{-}\mathcal{D}, && \text{where } \mathcal{I}(C, \sigma_C) := (\mathcal{I}_o(C), \mathcal{I}_o(\sigma_C)); \\ &\mathcal{H} : \sigma\text{-}\mathcal{D} \to \sigma\text{-}\mathcal{C}, && \text{where } \mathcal{H}(D, \sigma_D) := (\mathcal{H}_o(D), \mathcal{H}_o(\sigma_D)). \end{aligned}$$

Then: *(i) The functor $\mathcal{H}$ is right adjoint to $\mathcal{I}$;*

(ii) Moreover if $\mathcal{H}_o$ is monadic then $\mathcal{H}$ is monadic.

Proof. (i) Let $C \in \mathcal{C}$, $D \in \mathcal{D}$. By assumption we have the following bijection:

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{I}_o(C), D) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(C, \mathcal{H}_o(D)).$$

We can construct the pre- and post-composition functors $- \circ \mathcal{I}_o(\sigma_C)$ and $\sigma_D \circ -$. The difference Hom-set in $\mathcal{D}$ can then be described as the equaliser of these maps:

$$\mathrm{Hom}_{\sigma\text{-}\mathcal{D}}(\mathcal{I}(C), D) = \{f : \mathcal{I}_o(C) \to D \mid f \circ \mathcal{I}_o(\sigma_C) = \sigma_D \circ f\}$$

Similarly we construct $- \circ \sigma_C$, $\mathcal{H}_o(\sigma_D) \circ -$ and see that $\mathrm{Hom}_{\sigma\text{-}\mathcal{C}}(C, \mathcal{H}(D))$ is their equaliser. By the universal property of equalisers we obtain a bijection of difference Hom-sets and see that $\mathcal{I} \dashv \mathcal{H}$. This can be seen in the diagram below.

$$\begin{array}{ccc}
\mathrm{Hom}_{\sigma\text{-}\mathcal{D}}(\mathcal{I}(C), D) & \overset{\sim}{\dashrightarrow} & \mathrm{Hom}_{\sigma\text{-}\mathcal{C}}(C, \mathcal{H}(D)) \\
\Big\downarrow{\scriptstyle \mathrm{eq}} & & \Big\downarrow{\scriptstyle \mathrm{eq}} \\
\mathrm{Hom}_{\mathcal{D}}(\mathcal{I}_o(C), D) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(C, \mathcal{H}_o(D)) \\
{\scriptstyle -\circ\mathcal{I}_o(\sigma_C)}\Big\downarrow\Big\downarrow{\scriptstyle \sigma_D\circ -} & & {\scriptstyle -\circ\sigma_C}\Big\downarrow\Big\downarrow{\scriptstyle \mathcal{H}_o(\sigma_D)\circ -} \\
\mathrm{Hom}_{\mathcal{D}}(\mathcal{I}_o(C), D) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(C, \mathcal{H}_o(D))
\end{array}$$

Figure 5.8: Equalisers of Hom-sets

Define the unit of the adjunction as $\eta = \eta_o$, where:

$$\eta_{(D,\sigma_D)} : (D, \sigma_D) \to (\mathcal{H}_o\mathcal{I}_o(D), \mathcal{H}_o\mathcal{I}_o(\sigma_D)).$$

Similarly define the counit of the adjunction as $\epsilon = \epsilon_o$.

(ii) Construct the monad $\mathbb{T} = (T, \mu, \nu)$ using the adjunction obtained in the first part. Objects of the Eilenberg-Moore category $(\sigma\text{-}\mathcal{C})^{\mathbb{T}}$ are pairs (A, ν), where $A \in \sigma\text{-}\mathcal{C}$ and $\nu = \nu_o : T(A) \to A$. By functoriality we see that σ_A is an endomorphism of (A, ν), i.e. $\sigma_A \circ \nu_o = \nu_o \circ T_o(\sigma_A)$. As the underlying functor $\mathcal{H}_o$ is monadic, we see that:

$$(\sigma\text{-}\mathcal{C})^{\mathbb{T}} \;\cong\; \sigma\text{-}(\mathcal{C}^{\mathbb{T}}) \;\cong\; \sigma\text{-}\mathcal{D}.$$

Therefore $\mathcal{H}$ is monadic.

□

Definition 5.2.2. Let $\mathcal{C} = K\text{-}\sigma\text{-}\mathbf{FAlg}^{\mathbf{op}}$, $\mathcal{D} = \sigma\text{-}\mathbf{FSet}$ and define the functors:

$$\begin{array}{rccc} \mathcal{I}_K: & K\text{-}\sigma\text{-}\mathbf{FAlg}^{\mathbf{op}} & \longrightarrow & \sigma\text{-}\mathbf{FSet} \\ & A & \longmapsto & \pi_0(A); \\ \mathcal{H}_K: & \sigma\text{-}\mathbf{FSet} & \longrightarrow & K\text{-}\sigma\text{-}\mathbf{FAlg}^{\mathbf{op}} \\ & S & \longmapsto & \prod_{s\in S} K_s. \end{array}$$

Here $\pi_0(A)$ denotes the set of connected components of the scheme $\mathrm{Spec}(A)$ (Definition 2.2.2), which is a difference set with difference action induced from σ_A.

Each K_s denotes an isomorphic copy of K indexed by an element of S, so the functor $\mathcal{H}_K(S)$ returns a finite dimensional K-σ-algebra which is viewed as an S-indexed coproduct in $K\text{-}\sigma\text{-}\mathbf{FAlg}^{\mathbf{op}}$. The difference morphism then acts as σ_K on each individual copy of K as well as shuffling with respect to σ_S. For $\lambda = (\lambda_s)_{s\in S} \in \prod_{s\in S} K_s$ this can be explicitly written as:

$$\tilde{\sigma}_S : \prod_{s\in S} K_s \to \prod_{s\in S} K_s, \qquad \text{where } \left(\tilde{\sigma}_S(\lambda)\right)_s := \sigma_K(\lambda_{\sigma_S(s)}).$$

Lemma 5.2.3. *Using the notation introduced in Definition 5.2.2, the functor $\mathcal{H}_K$ is right adjoint to $\mathcal{I}_K$.*

Proof. Consider the functors between the dual category of rings and profinite spaces:

$$\begin{array}{rccc} \mathcal{I}_o: & \mathbf{Ring}^{\mathbf{op}} & \longrightarrow & \mathbf{Prof} \\ & R & \longmapsto & \pi_0(R); \end{array}$$

$$\begin{array}{rccc} \mathcal{H}_o: & \mathbf{Prof} & \longrightarrow & \mathbf{Ring^{op}} \\ & X & \longmapsto & C(X,R), \end{array}$$

where $C(X,R)$ denotes the ring of continuous functions between X and R.
By a result of Borceux-Janelidze ([BJ01], Thm 4.3.2) $\mathcal{H}_o$ is right adjoint to $\mathcal{I}_o$. Using Lemma 5.2.1 (i) we can then construct the functors $\mathcal{I}, \mathcal{H}$ between σ-$\mathbf{Ring^{op}}$ and σ-$\mathbf{Prof}$. We can finally use the identification:

$$K\text{-}\sigma\text{-}\mathbf{Alg^{op}} \;\cong\; \sigma\text{-}\mathbf{Ring^{op}}/K,$$

and apply Lemma 5.1.3 to see that $\mathcal{H}_K$ is right adjoint to $\mathcal{I}_K$. Restricting to the finite dimensional case gives the required adjunction. □

We now identify a morphism of relative Galois descent in K-σ-$\mathbf{FAlg^{op}}$.

Proposition 5.2.4. *Let L/K be a difference field extension such that the underlying field extension is finite Galois with group G. Consider L as an object of K-σ-$\mathbf{FAlg^{op}}$ with structure morphism $\varphi : L \to K$. Then $\varphi : L \to K$ is a morphism of relative Galois descent in K-σ-$\mathbf{FAlg^{op}}$.*

Proof. We check the conditions detailed in Definition 5.1.9.

(i) By a result of Borceux-Janelidze ([BJ01], Cor 4.4.5) the underlying functor

$$\varphi_o^* : K\text{-}\mathbf{Alg^{op}} \to L\text{-}\mathbf{Alg^{op}}$$

is monadic. Therefore Lemma 5.2.1 shows that φ^* is monadic.

(ii) By a result of Borceux-Janelidze ([BJ01], Prop 4.3.3), the underlying counit is an

isomorphism. By functoriality the counit ϵ is therefore a difference isomorphism.

(iii) Let $S \in \sigma$-**FSet**. First note that:

$$\varphi_! \mathcal{H}_L(S) \;=\; \coprod_{s \in S} L_s,$$

where the coproduct is considered as an element of K-σ-$\mathbf{FAlg}^{\mathbf{op}}$. Then as L/K is Galois with group G we have the following isomorphism in L-σ-**FAlg**:

$$L \otimes_K L \;\cong\; \coprod_{g \in G} L_g,$$

where each L_g is a copy of L indexed by an element of G. The difference action on the coproduct is induced from $()^\sigma$ and σ_L analogously to $\tilde{\sigma}_S$ in Definition 5.2.2. Then:

$$\begin{aligned} \varphi^* \varphi_! \mathcal{H}_L(S) \;&=\; \Big(\coprod_{s \in S} L_s \Big) \times_K L \\ &\cong\; \coprod_{s \in S} (L \times_K L)_s \\ &\cong\; \coprod_{s \in S} \Big(\coprod_{g \in G} L_g \Big)_s. \end{aligned}$$

We then easily verify that the object $\varphi_! \mathcal{H}_L(S) \in K$-$\sigma$-$\mathbf{FAlg}^{\mathbf{op}}$ is split by φ:

$$\begin{aligned} \mathcal{H}_L \mathcal{I}_L \varphi^* (\varphi_! \mathcal{H}_L(S)) \;&\cong\; \mathcal{H}_L \mathcal{I}_L \Big(\coprod_{\substack{(s,g) \\ \in S \times G}} L_{(s,g)} \Big) \\ &\cong\; \mathcal{H}_L(S \times G) \\ &\cong\; \coprod_{\substack{(s,g) \\ \in S \times G}} L_{(s,g)} \\ &\cong\; \varphi^* (\varphi_! \mathcal{H}_L(S)). \end{aligned}$$

□

The following definition interprets the categorical definition of a split object in K-σ-$\mathbf{FAlg}^{\mathbf{op}}$.

Definition 5.2.5. A K-σ-algebra A is an **étale K-σ-algebra split by** L if there exists a finite difference set S such that the following is an L-σ-algebra isomorphism:

$$A \otimes_K L \;\cong\; \prod_{s \in S} L_s.$$

Here $A \otimes_K L$ has difference action $\sigma_A \otimes \sigma_L$ and $\prod_{s\in S} L_s$ has difference action $\tilde{\sigma}_S$ as described in Definition 5.2.2.
The **category of étale K-σ-algebras which are split by** L is denoted $\mathbf{Spl}_K(L)$.

We constrast this definition with that of a strongly σ-étale K-σ-algebra given by Tomašić-Wibmer [TW18]. In the strongly σ-étale case $A \otimes_K L$ is σ-reduced, i.e. its difference endomorphism is injective. This is a slightly more restrictive condition.

Proposition 5.2.6. *Let L/K be a difference field extension such that the underlying field extension is finite Galois with group G. Let A be an étale K-σ-algebra split by L. Consider L as an object of K-σ-$\mathbf{FAlg}^{\mathbf{op}}$ with structure morphism $\varphi : L \to K$. Then A is split by φ in the sense of Definition 5.1.8.*
Moreover $\mathbf{Spl}_K(\varphi)$ consists only of étale K-σ-algebras split by L, i.e.

$$\mathbf{Spl}_K(L) \;\cong\; \mathbf{Spl}_K(\varphi).$$

Proof. Assume A is an étale K-σ-algebra split by L. Then there exists a finite difference set S such that we have an isomorphism in L-σ-$\mathbf{FAlg}^{\mathbf{op}}$:

$$\varphi^*(A) \;=\; A \times_K L \;\cong\; \coprod_{s \in S} L_s \;=\; \mathcal{H}_L(S).$$

We can then see that A is split by $\varphi : L \to K$ in the categorical sense:

$$\begin{aligned} \mathcal{H}_L\mathcal{I}_L\varphi^*(A) &\cong \mathcal{H}_L\mathcal{I}_L(\coprod_{s\in S} L_s) \\ &\cong \mathcal{H}_L(S) \\ &\cong \varphi^*(A). \end{aligned}$$

A result of Borceux-Janelidze confirms that this fully describes $\mathbf{Spl}_K(\varphi)$ ([BJ01], Cor 4.7.16), where we use functoriality to obtain the difference case. □

We can find an internal groupoid (Definition 5.1.10) in the category σ-**FSet**.

Proposition 5.2.7. *Let L/K be a difference field extension such that the underlying field extension is finite Galois with group G. Consider G as a difference group with endomorphism ${}^{\sigma}()$ (see Proposition 4.2.6) and consider L as an object of K-σ-$\mathbf{FAlg}^{\mathbf{op}}$ with structure morphism $\varphi : L \to K$. The internal groupoid* $\mathrm{Gal}[\varphi]$ *in* σ-**FSet** *is the difference group* $(G, {}^{\sigma}())$.

Proof. We build the internal groupoid $\mathrm{Gal}[\varphi]$.
This groupoid has object-of-objects $(\pi_0(L), \sigma_L) \cong (\{*\}, \mathrm{id})$. This simplification can be made because L is a field and only has trivial idempotents $0, 1$. We therefore conclude that this will be an internal group rather than an internal groupoid.
$\mathrm{Gal}[\varphi]$ has object-of-morphisms $(\pi_0(L \times_K L), \sigma_L \times \sigma_L) \cong (G, {}^{\sigma}())$. To see this use that the dual of a finite Galois field extension is a G-torsor:

$$\pi_0(L \times_K L) \cong \pi_0(G \times L) \cong G.$$

It can then be verified that multiplication in $\pi_0(L \times_K L)$ can be pushed along this isomorph-

ism chain and agrees with usual multiplication in the group G. The difference structure is mapped along in the same way. We can conclude that $\mathrm{Gal}[\varphi] \cong (G, {}^{\sigma}())$ in this case. □

Internal covariant presheaves on G are triples (S, f, ζ) such that:

- $S \in \sigma$-**FSet**;
- $f : S \to \{*\}$;
- $\zeta : G \times S \to S$.

In this situation $\mathcal{D}^{\mathrm{Gal}[\varphi]} = G$-$\sigma$-**FSet** is the category of finite difference G-sets. The Galois correspondence in this special case can now be described by applying Theorem 5.1.12.

Theorem 5.2.8. *Let L/K be a difference field extension such that the underlying field extension is finite Galois with group G. Consider L as an object of K-σ-$\mathbf{FAlg}^{\mathbf{op}}$ with structure morphism $\varphi : L \to K$ and consider G as a difference group with endomorphism ${}^{\sigma}()$ and .*
Then there is an equivalence of categories:

$$\mathbf{Spl}_K(L) \;\cong\; G\text{-}\sigma\text{-}\mathbf{FSet}.$$

We see how this result mirrors the classical Galois correspondence previously described: the category of finite étale covers has been replaced by the category of finite dimensional étale split difference algebras and finite sets with a fundamental group action have been replaced by finite difference sets with a difference Galois group action.

Chapter 6

Exceptional covers of difference schemes

This chapter presents the main results of this thesis and brings together material from previous chapters to prove our difference exceptionality criterion. We generalise the notion of exceptionality to the context to difference algebraic geometry and obtain a result identifying difference exceptional covers.

The layout of the chapter mirrors that of Chapter 3: we formulate the criterion, discuss its geometric interpretation and give a proof. We recover the classical exceptionality criterion for varieties (Corollary 3.2.5) from the difference version, give some examples and finally suggest directions for future research.

6.1 A difference exceptionality criterion

We now give a definition of a difference exceptional cover and state results analogous to Theorem 3.2.4 and Corollary 3.2.5. Let $k = (k, \mathrm{id})$ be a finite field with trivial difference

operator. Let $\bar{k}$ denote its algebraic closure and fix the following notation:

- Let $\bar{k}_m := (\bar{k}, \varphi_k^m)$, where φ_k is the Frobenius sending elements to their $|k|^{\text{th}}$ power;
- Let $k_m := \text{Fix}(\bar{k}_m)$. In particular $k = k_1$.

Definition 6.1.1. Let X, Y be difference schemes over k and let $f : Y \to X$ be a k-morphism. Then f is a **difference exceptional cover** if $f : Y(\bar{k}_m) \to X(\bar{k}_m)$ is a bijection for infinitely many $m \in \mathbb{N}$.

In the above definition the most interesting case is when X, Y are of finite total dimension, as this ensures that $X(\bar{k}_m), Y(\bar{k}_m)$ are finite for large enough m. We still provide the full definition without restriction for general interest.
For the following theorem recall the construction of a difference Galois closure and its set of lifts from Subsection 4.3.2.

Theorem 6.1.2. *Let X, Y be normal, geometrically transformally integral difference schemes over k and let $f : Y \to X$ be a generically étale k-morphism. Let Z denote the difference Galois closure of f with choice of difference structure σ_Z. Let $\widehat{k}$ denote the relative algebraic closure of k in the difference function field $M = K(Z)$, where $\widehat{k}$ inherits difference structure from the restriction of σ_M.*
If the difference action on the set of connected components of $(Y \times_X Y)_{\widehat{k}} = (Y \times_X Y) \times_k \widehat{k}$ only fixes the component associated to the diagonal Δ_Y, i.e.

$$\left| \text{Fix}\left(\pi_0((Y \times_X Y)_{\widehat{k}})\right) \right| = 1,$$

then for every $m \in \mathbb{N}$ such that $\bar{k}_m$ is a difference field extension of $\widehat{k}$, the morphism $f : Y(\bar{k}_m) \to X(\bar{k}_m)$ is surjective.

Corollary 6.1.3 (Difference Exceptionality Criterion)**.** *Assume the same setup as Theorem*

6.1.2 and assume that $X = Y$ is of finite total dimension. Then $f : X \to X$ is a difference exceptional cover if and only if the difference action on the set of connected components of $(X \times_X X)_{\widehat{k}}$ only fixes the component associated to the diagonal Δ_X.
Moreover the bijectivity condition is satisfied by large enough $m \in \mathbb{N}$ such that $\bar{k}_m$ is a difference field extension of $\widehat{k}$.

These statements generalise the classical situation; we mirror our previous exposition and highlight relevant adaptations.

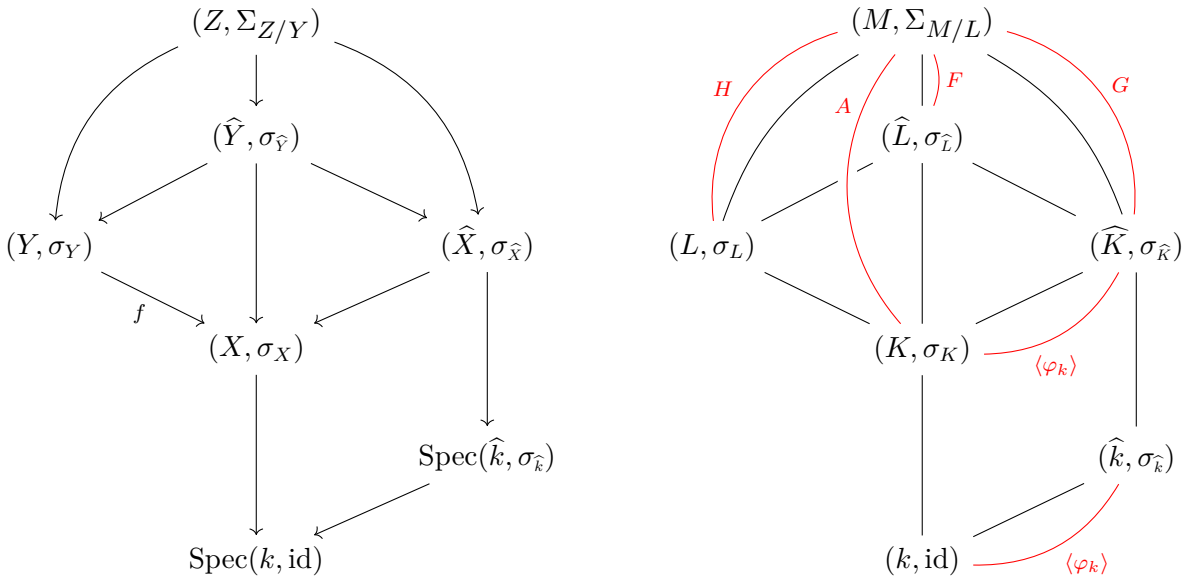

Figure 6.1: Setup of difference varieties and difference function fields

We set up the function fields and look at how to interpret the difference exceptionality condition on fixed points. Recall the function field diagram from Chapter 2 (Figure 3.3): this underlying setup is retained and we enhance it with difference structure.
Recalling Subsection 4.3.2 let Z be the difference Galois closure of f with choice of difference structure σ_Z. We can equip Z with a set of lifts $\Sigma_{Z/Y} = H\sigma_Z$ and induce a difference structure on the associated Galois groups. The diagrams of varieties and function fields are

redrawn in Figure 6.1 explicitly showing the difference structure, with the difference Galois groups shown in red.

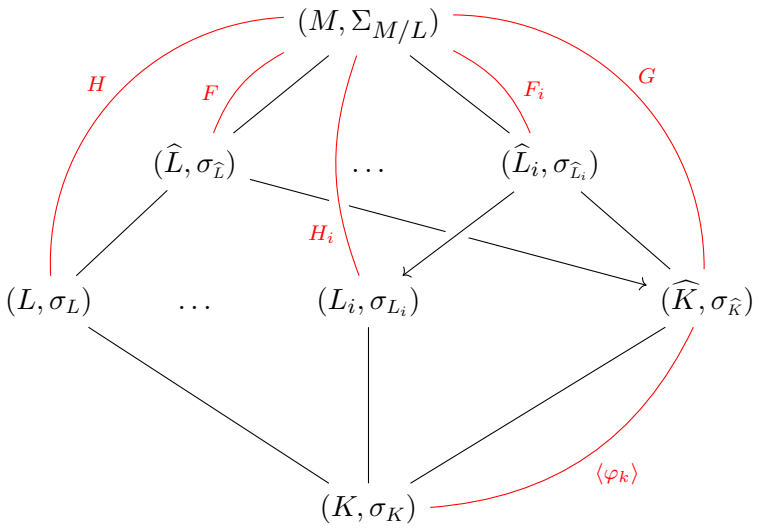

Figure 6.2: Difference conjugate varieties

We also obtain a difference action σ_{L_i} on the conjugate fields and varieties as discussed on page 90. The diagram above enhances Figure 3.4.

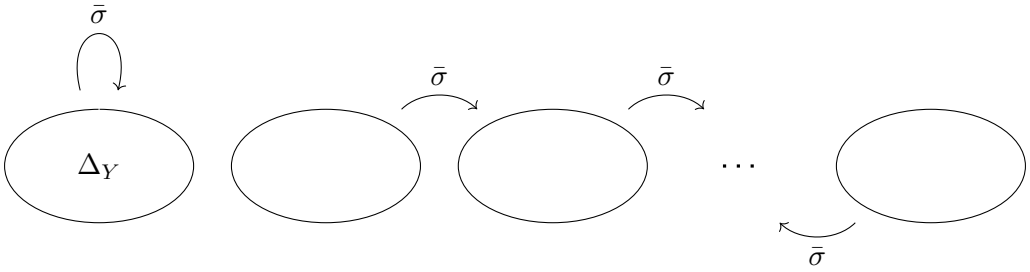

Figure 6.3: The difference exceptionality condition

In Section 3.3 the classical exceptionality condition was interpreted as saying that Δ_Y is the only connected component of $(Y \times_X Y)_{\widehat{k}}$ which is fixed by the induced permutation of the Frobenius φ_k. The difference exceptionality condition generalises this.

Here Δ_Y is the unique component fixed by the induced difference action. An example of this type of behaviour is expressed in the diagram above, where each circle represents a connected component of $(Y \times_X Y)_{\widehat{k}}$ and $\bar{\sigma}$ is the difference action.

We now relate the difference exceptionality condition to tensor products of fields. This will allow us to use Lemmas 4.2.8 and 4.2.9 to explicitly describe the difference action.

Lemma 6.1.4. *Assume the setup described in Figure 6.1. There is a bijection between the set of connected components of* $(Y \times_X Y)_{\widehat{k}}$ *and the set of connected components of* $L \otimes_K \widehat{L}$*, i.e.*

$$\pi_0\big((Y \times_X Y)_{\widehat{k}}\big) \;\cong\; \pi_0(L \otimes_K \widehat{L}).$$

Proof. First note that as our difference schemes are transformally integral, connected components of $(Y \times_X Y)_{\widehat{k}}$ correspond to connected components of $\widehat{k} \otimes_k (L \otimes_K L)$, where $L \otimes_K L$ is considered as a k-algebra. We can then make the following manipulations ([Con], Thm 6.14):

$$\begin{aligned}
\widehat{k} \otimes_k (L \otimes_K L) &\cong (K \otimes_k \widehat{k}) \otimes_K (L \otimes_K L) \\
&\cong \widehat{K} \otimes_K (L \otimes_K L) \\
&\cong (\widehat{K} \otimes_K L) \otimes_{\widehat{K}} (\widehat{K} \otimes_K L) \\
&\cong \widehat{L} \otimes_{\widehat{K}} \widehat{L}.
\end{aligned}$$

Alternatively if we view $\widehat{L}$ as a K-algebra:

$$\begin{aligned}
L \otimes_K \widehat{L} &\cong (\widehat{K} \otimes_K L) \otimes_{\widehat{K}} \widehat{L} \\
&\cong \widehat{L} \otimes_{\widehat{K}} \widehat{L}.
\end{aligned}$$

Combining these we obtain the required bijection:

$$\begin{aligned}\pi_0\big((Y \times_X Y)_{\widehat{k}}\big) &\cong \pi_0\big(\widehat{k} \otimes_k (L \otimes_K L)\big)\\ &\cong \pi_0(\widehat{L} \otimes_{\widehat{K}} \widehat{L})\\ &\cong \pi_0(L \otimes_K \widehat{L}).\end{aligned}$$

□

6.2 Proof of the difference exceptionality criterion

We now prove Theorem 6.1.2 beginning with a description of relevant Σ sets. Assume the setup as described in Figures 6.1 and 6.2.

We switch to the function field setting and for $i = 1, \ldots, l$ let:

$$\Sigma_{M/K} = \sigma_M A, \qquad \Sigma_{M/L_i} = \sigma_M H_i, \qquad \Sigma_{M/\widehat{K}} = \sigma_M G, \qquad \Sigma_{M/\widehat{L_i}} = \sigma_M F_i.$$

Motivated by the definition of $\widehat{A}, \widehat{H_i}$ (Definition 3.4.1) we restrict these sets to their action on $\widehat{K}$.

Definition 6.2.1. Let $\widehat{\Sigma}_{M/K}$ denote the subset of $\Sigma_{M/K}$ consisting of elements whose restriction to $\widehat{K}$ is $\sigma_{\widehat{K}}$, i.e.

$$\widehat{\Sigma}_{M/K} = \{\tau \in \Sigma_{M/K} \mid \tau\restriction_{\widehat{K}} = \sigma_{\widehat{K}}\}.$$

Analogously for $i = 1, \ldots, l$ let:

$$\widehat{\Sigma}_{M/L_i} = \{\tau \in \Sigma_{M/L_i} \mid \tau\restriction_{\widehat{K}} = \sigma_{\widehat{K}}\},$$

where $\widehat{\Sigma}_{M/L_1} = \widehat{\Sigma}_{M/L}$.

As before the cardinality of these sets can be understood via identification with other Σ sets. Linear disjointness allows us to identify $\widehat{\Sigma}_{M/K} = \Sigma_{M/\widehat{K}}$ and $\widehat{\Sigma}_{M/L_i} = \Sigma_{M/\widehat{L_i}}$ and hence deduce that $|\widehat{\Sigma}_{M/K}| = |G|$ and $|\widehat{\Sigma}_{M/L_i}| = |F_i| = |F|$.

Lemma 6.2.2. *Let $\widehat{\Sigma}_{M/K}, \widehat{\Sigma}_{M/L_i}$ be as defined above for $i = 1, \ldots, l$ and assume that*

$|\operatorname{Fix}(\pi_0(L \otimes_K \widehat{L}))| = 1$. *Then* $\widehat{\Sigma}_{M/K}$ *is a disjoint union of* $\widehat{\Sigma}_{M/L_i}$*'s, i.e.*

$$\widehat{\Sigma}_{M/K} \;=\; \bigsqcup_{i=1}^{l} \widehat{\Sigma}_{M/L_i}.$$

Proof. We first show that the $\widehat{\Sigma}_{M/L_i}$'s are disjoint. Recall the set of roots $\mathcal{S}$ (Definition 3.2.8) and the definition of β_i (page 90).
Let $\tau \in \widehat{\Sigma}_{M/L} \cap \widehat{\Sigma}_{M/L_i}$ for some $i \neq 1$. As $\tau \in \Sigma_{M/\widehat{L}}$ we can express $\tau = \sigma_M \lambda$ for some $\lambda \in F$, while $\tau\restriction_{L_i} = \sigma_{L_i}$ implies that $\tau(\alpha_i) = \sigma_{L_i}(\alpha_i) = \beta_i$, i.e. $\tau(a_i \cdot \alpha) = a_i \cdot \sigma_L(\alpha)$. Combining this information:

$$\sigma_M(\lambda a_i \cdot \alpha) \;=\; \tau(a_i \cdot \alpha) \;=\; a_i \cdot \sigma_L(\alpha) \;=\; \sigma_M(a_i^{\sigma} \cdot \alpha).$$

As σ_M is a field homomorphism it must be injective and we can conclude that $\lambda a_i \cdot \alpha = a_i^{\sigma} \cdot \alpha$, i.e. $Fa_iH = Fa_i^{\sigma}H$. We have found $i \neq 1$ which is fixed by the difference action $\bar{\sigma}$ on components as described in Lemma 4.2.9, obtaining a contradiction.
We can reduce to the same cardinality argument as in the proof of Lemma 3.4.2. This follows from noting that $|\widehat{\Sigma}_{M/K}| = |G| = l|F| = |\sqcup_{i=1}^{l} \widehat{\Sigma}_{M/L_i}|$ and that the right hand side is contained in the left hand side. □

We now turn our attention to difference rational points, recalling the theory of local substitutions covered in Subsection 4.3.2.

Lemma 6.2.3. *Let* $m \in \mathbb{N}$ *such that* $\bar{k}_m$ *be a difference field extension of* $\widehat{k}$ *and let* $\bar{x} \in X(\bar{k}_m)$ *be a difference rational point. Then there exists* $\bar{z} \in Z(\bar{k}_m)$ *which lies over* $\bar{x}$ *with local* φ_k^m*-substitution* $\tau \in \widehat{\Sigma}_{Z/X}$.

Proof. By the universal property of the fibre product we can lift $\bar{x} \in X(\bar{k}_m)$ over k to a unique $\widehat{x} \in \widehat{X}(\bar{k}_m)$ over $\widehat{k}$, as shown in the diagram below. As $\widehat{\pi} : Z \to \widehat{X}$ is Galois we can

find $\bar{z} \in Z(\bar{k}_m)$ with local φ_k^m-substitution $\tau \in \Sigma_{Z/\widehat{X}} = \widehat{\Sigma}_{Z/X}$ such that $\widehat{\pi}(\bar{z}) = \widehat{x}$. □

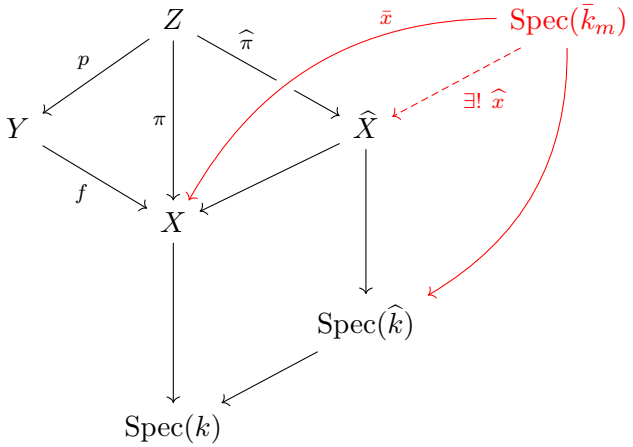

Figure 6.4: Construction of $\widehat{x} \in \widehat{X}(\bar{k}_m)$

We can now prove Theorem 6.1.2 noting that our focus on difference rational points allows for a simpler argument than in the classical case.

Proof. Let $m \in \mathbb{N}$ such that $\bar{k}_m$ is a difference field extension of $\widehat{k}$ and let $\bar{x} \in X(\bar{k}_m)$. By Lemma 6.2.3 there exists $\bar{z} \in Z(\bar{k}_m)$ lying over $\bar{x}$ with local φ_k^m-substitution $\tau \in \widehat{\Sigma}_{Z/X}$. Assuming the difference exceptionality condition holds Lemma 6.2.2 shows that there is a unique $i \in \{1, \ldots, l\}$ such that $\tau \in \widehat{\Sigma}_{Z/Y_i}$. By conjugation we may assume $\tau \in \widehat{\Sigma}_{Z/Y}$. Let $p : Z \to Y$ denote the projection map and define $\bar{y} := p(\bar{z}) \in Y(\bar{k}_m)$ which lies over $\bar{x}$. We have shown that $f : Y(\bar{k}_m) \to X(\bar{k}_m)$ is surjective. □

The proof of Corollary 6.1.3 follows.

Proof. The 'only if' direction of Corollary 6.1.3 requires Hrushovski's twisted Lang-Weil bound (Theorem 4.3.13). As X is of finite total dimension, so is $X \times_X X$. Assume that $W \neq \Delta_X$ is another connected component of $(X \times_X X)_{\widehat{k}}$ which is fixed by the difference

action. The assumption of W being fixed makes it a difference subobject so it is therefore a geometrically transformally integral difference scheme of finite total dimension over $\widehat{k}$. Apply Hrushovski's twisted Lang-Weil bound to W with $k_o = \widehat{k}$. Using the same argument as in the classical case, as m becomes large, $W(\bar{k}_m) \neq \emptyset$ and we obtain a contradiction to the assumption of $f : X(\bar{k}_m) \to X(\bar{k}_m)$ being injective. We therefore require m to be 'large enough' to satisfy this requirement.

The 'if' direction of Corollary 6.1.3 follows easily from the proof of Theorem 6.1.2. If the difference action on the set of connected components of $(X \times_X X)_{\widehat{k}}$ fixes a unique element, we have seen that $f : X(\bar{k}_m) \to X(\bar{k}_m)$ is surjective. As X is of finite total dimension, Corollary 4.3.14 shows that the set $X(\bar{k}_m)$ is finite and so the map is bijective. The proof shows that we can make the same argument for all m such that $\bar{k}_m$ is a difference field extension of $\widehat{k}$, which requires φ_k^m to restrict to $\sigma_{\widehat{k}}$. Recall from the setup described in Section 3.2 that $\widehat{k}$ is a finite field, so $\sigma_{\widehat{k}}$ is a fixed power of Frobenius. There are infinitely such m so we see that f is a difference exceptional cover. □

We verify that the classical exceptionality criterion can be recovered from the difference exceptionality criterion by considering algebraic varieties as difference varieties equipped with the identity endomorphism.

Corollary 6.2.4 (Exceptionality Criterion for Varieties)**.** *Let X be a normal, geometrically irreducible variety over k and let $f : X \to X$ be a quasifinite, generically étale k-morphism. Then $f : X \to X$ is an exceptional cover if and only if Δ_X is the only geometrically irreducible component of $X \times_X X$ which is defined over k.*

Proof. Consider X as a difference scheme over a finite difference field k by setting $\sigma_X = \mathrm{id}_X$ and $\sigma_k = \mathrm{id}_k$. As shown in the diagram below, we first note that a rational point $\bar{x} \in X(\bar{k}_m)$ satisfies $\bar{x} \circ \varphi_k^m = \bar{x}$. Recalling that $\mathrm{Fix}(\bar{k}_m) = k_m$, we can therefore identify

the set of k_m-rational points in $\lfloor X \rfloor$ with the set of difference $\bar{k}_m$-rational points in X, i.e. $\lfloor X \rfloor(k_m) = X(\bar{k}_m)$. The 'only if' direction clearly follows from Corollary 6.1.3.

$$\begin{array}{ccc} \mathrm{Spec}(\bar{k}) & \xrightarrow{\bar{x}} & X \\ {\scriptstyle \varphi_k^m}\downarrow & & \| \\ \mathrm{Spec}(\bar{k}) & \xrightarrow[\bar{x}]{} & X \end{array}$$

Figure 6.5: A difference rational point $\bar{x} \in X(\bar{k}_m)$

Assume that Δ_X is the only geometrically irreducible component of $X \times_X X$ which is defined over k. This translates to saying that Δ_X is the only element of $\pi_0\Big(\big(\lfloor X \rfloor \times_{\lfloor X \rfloor} \lfloor X \rfloor\big)_{\widehat{k}}\Big)$ fixed by the action of the generator of $\mathrm{Gal}(\widehat{k}/k)$. Therefore Corollary 6.1.3 gives that $f : X(\bar{k}_m) \to X(\bar{k}_m)$ is bijective for infinitely many $m \in \mathbb{N}$.

We also see that the extensions k_m for which the bijectivity condition is satisfied are those where φ_k^m restricts to φ_k on $\widehat{k}$. □

6.3 Examples

One way to construct examples of difference exceptional covers is by taking a family of permutation polynomials which naturally fit into the difference language. The following examples come from discussions of Tomašić and Zieve.

Example 6.3.1. Let q be a power of 2. Then it is classically known that:

$$f(x) = x^{2q+1} + x^3 + x$$

is a permutation polynomial over $\mathbb{F}_{2q^2}$. This can be translated to difference geometric language by defining a difference scheme X over $\mathbb{F}_2$ by the difference polynomial:

$$\sigma^2(x^2) = x,$$

and defining a morphism:

$$\begin{array}{cccc} f: & X & \longrightarrow & X \\ & x & \longmapsto & x\sigma_X(x^2) + x^3 + x \ . \end{array}$$

Then for infinitely many powers of 2 we have a bijection:

$$f : X(\overline{\mathbb{F}}_2, \varphi_q) \xrightarrow{\sim} X(\overline{\mathbb{F}}_2, \varphi_q),$$

and so $f : X \to X$ is a difference exceptional cover.

For this example the primary decomposition can be computed using Magma to find polynomial ideals corresponding to connected components of $X \times_X X$. This shows three components: one corresponding to the diagonal and two which are swapped by the difference

action, where all components are defined over $\widehat{k} = k$. This shows that difference exceptionality criterion is satisfied for this example.

Example 6.3.2. Let q be a power of 3. Then it is classically known that:

$$f(x) = x^{6q+3} + x^{3q} - x$$

is a permutation polynomial over $\mathbb{F}_{3q^2}$. As in the previous example we define a difference scheme X over $\mathbb{F}_3$ by the difference polynomial:

$$\sigma^2(x^3) = x,$$

and define a morphism:

$$\begin{array}{cccc} f: & X & \longrightarrow & X \\ & x & \longmapsto & x^3\sigma_X(x^6) + x^3 - x\ . \end{array}$$

Then for infinitely many powers of 2 there is a bijection:

$$f : X(\overline{\mathbb{F}}_3, \varphi_q) \xrightarrow{\sim} X(\overline{\mathbb{F}}_3, \varphi_q),$$

and f is a difference exceptional cover.

6.4 Future directions

We conclude this thesis by suggesting some directions for future work, primarily through removing assumptions and generating more concrete examples. This is an area of research which is very much in its infancy and there are many more paths to explore.

- The difference exceptionality criterion in its current form applies to endomorphisms of difference schemes. An obvious first step in generalisation would be to consider morphisms of distinct difference schemes; a result of this nature has been shown by Lenstra for exceptional covers of varieties ([GTZ07], Prop 4.4).

  This thesis already develops some theory with this direction in mind. The difference Galois correspondence in Chapter 5 gives a translation between difference algebraic geometry and group actions on difference sets, while the considerations of σ-closed group orbits in Chapter 4 lay the framework for an orbit counting-style argument.

- An alternative generalisation is to weaken the assumption of Y being geometrically irreducible; this has resulted in the development of pr-exceptional (possibly reducible exceptional) covers by Fried [Fri05]. The avenues in Section 3 of this paper could be considered in the context of difference algebraic geometry.

  A more ambitious step would be to remove the normality assumption. This would require further progress in difference algebraic geometry to avoid the reliance on difference field arguments. Work in this direction is being undertaken by Tomašić [Tom20] with the development of the Zariski spectrum of difference rings being approached from a topos-theoretic viewpoint.

- Our current examples of difference exceptional covers come from known families of classical permutation polynomials. We may then aim to work in the reverse direction and use the difference exceptionality criterion to generate further examples in the

classical case. This suggests potential for the exploration of links with cryptography and coding theory, which may be appealing to the broader mathematical community.

Appendix A

List of Notation

The following table compiles notation used throughout the thesis together with a brief definition and the page upon which it is introduced.

Notation	**Definition**	**Page**
Ω	An algebraically closed field	18
$\mathrm{Spec}(R)$	The spectrum of a commutative ring R	20
$\mathfrak{p}$	A prime ideal of a commutative ring R	20
$\mathcal{O}_X$	The structure sheaf of a scheme X	21
$f_*\mathcal{O}_X$	The direct image sheaf on Y induced by $f : X \to Y$	22
$f^\#$	The sheaf morphism $f^\# : \mathcal{O}_Y \to f_*\mathcal{O}_X$	22
$X(F)$	The set of F-rational points of a scheme X	23
Δ_Y	The diagonal subscheme $\Delta_Y \subseteq Y \times_X Y$ induced by $f : Y \to X$	26
$\kappa(x)$	The residue field of a scheme-theoretic point x of a scheme X	26

Notation	**Definition**	**Page**
π_0	The 'connected components' functor $\pi_0 : \mathbf{Sch} \to \mathbf{Set}$	29
$K(X)$	The function field of a variety X	33
Z	The Galois closure of $f : Y \to X$	35
$\mathrm{Gal}(Z/X)$	The Galois group of the Galois cover $\pi : Z \to X$	35
$D_{Z/X}(z), I_{Z/X}(z)$	The decomposition and inertia groups respectively of z with respect to Z/X	35
$\pi_1(X, \bar{x})$	The étale fundamental group of a scheme X at a basepoint $\bar{x}$	41
FSet	The category of finite sets	37
$\mathrm{Hom}_{\mathcal{C}}(Y, Z)$	The set of morphisms from Y to Z in a category $\mathcal{C}$	37
$\mathbf{FÉt}_X$	The category of finite étale covers of a connected scheme X	39
$\mathbb{F}_q$	A finite field of characteristic p	45
k	An arbitrary finite field	48
$\bar{k}$	The algebraic closure of k	48
k_m	A field extension of k of degree m	48
φ_k	The Frobenius endomorphism which sending elements to their $\lvert k\rvert^{\text{th}}$ power	48
$\widehat{k}$	The relative algebraic closure of k in $K(Z)$	49
$\widehat{X}, \widehat{Y}$	The base changes of X, Y to $\widehat{k}$ respectively	49
$K, L, \widehat{K}, M$	The function fields of $X, Y, \widehat{X}, Z$ respectively	49
A, G, H, F	The Galois groups of Z over $X, \widehat{X}, Y, \widehat{Y}$ respectively	52
$\mathcal{S}$	The set of roots of the finite separable extension L/K	52
$L_i, \widehat{L}_i$	A field conjugate to $L, \widehat{L}$ over $K, \widehat{K}$ respectively	52
$Y_i, \widehat{Y}_i$	A variety conjugate to $Y, \widehat{Y}$ over $X, \widehat{X}$ respectively	52

Notation	**Definition**	**Page**
a_i	An element $a_i \in A$ such that $a_i \cdot Y = Y_i$	52
H_i, F_i	The Galois groups of Z over $Y_i, \widehat{Y}_i$ respectively	52
$\widehat{A}, \widehat{H}_i$	The subgroups of A, H_i respectively consisting of generators of $\mathrm{Gal}(\widehat{k}/k)$	60
σ**-Set**, σ**-FSet**	The categories of difference sets and finite difference sets respectively	64
$\lfloor S \rfloor$	The underlying object of a difference object S	65
$\mathbb{N}_+$	The set of natural numbers with the shift endomorphism $n \mapsto n+1$	66
σ**-Grp**	The category of difference groups	67
σ**-Ring**	The category of difference rings	67
K-σ**-FAlg**	The category of finite dimensional difference K-algebras over a difference field K	68
${}^{\sigma}()$	The difference endomorphism associated to a group G where G acts on a set (S, σ)	68
G-σ**-Set**	The category of difference sets with the action of a fixed difference group G	68
$()^{\sigma}$	The difference endomorphism associated to a group G where G acts on a ring (R, σ)	69
A_s^{σ}	The σ-stabiliser of a point s in a group A	78
S_{σ}^{b}	The σ-fixed set of a group element b in a set S	78
$\mathrm{Fix}(K, \sigma_K)$	The fixed field of a difference field K	84
$\Sigma_{M/L}$	The set of lifts of σ_L to M where M/L is a difference Galois field extension	85
f_i	A factor of a minimal polynomial $f \in K[x]$ over $\widehat{L}$	86

Notation	**Definition**	**Page**
$(I, \bar{\sigma})$	The difference set corresponding to connected components of $L \otimes_K \widehat{L}$	87
f'_j	A factor of a minimal polynomial $f' \in K[x]$ over $\widehat{L}$	87
X^σ	The set of fixed scheme-theoretic points of a scheme X	92
K-σ-**FAffSch**	The category of finite affine difference schemes over $\mathrm{Spec}(K)$	93
σ^x	A residue field morphism $\sigma^x : \kappa(x) \to \kappa(x)$ for $x \in X^\sigma$	96
Σ_z	The stabiliser of z in Σ	99
Σ^z	The set of induced morphisms on the residue field $\kappa(z)$	99
$\Sigma_{Z/Y}$	The set of lifts of σ_Y to Z where Z/Y is a difference Galois cover	101
$\mathcal{I} \dashv \mathcal{H}$	An adjunction where $\mathcal{H}$ is right adjoint to $\mathcal{I}$	103
η, ϵ	The unit and counit of an adjunction respectively	103
$\mathcal{C}/C$	The slice category of a category $\mathcal{C}$ over an object $C \in \mathcal{C}$	103
$\mathbb{T}$	A monad $\mathbb{T} = (T, \mu, \nu)$ in a category $\mathcal{C}$	105
$\mathcal{C}^\mathbb{T}$	The Eilenberg-Moore category of the monad $\mathbb{T}$	106
$\varphi^*, \varphi_!$	The pullback functor $\varphi^* : \mathcal{C}/K \to \mathcal{C}/L$ induced by a morphism $\varphi : L \to K$ and its left adjoint respectively	107
$\mathbf{Spl}_K(\varphi)$	The category of objects in $\mathcal{C}/K$ split by a morphism $\varphi : L \to K$	107
$\mathrm{Gal}[\varphi]$	The internal groupoid in $\mathcal{D}$ induced by $\varphi : L \to K$	108

Notation	**Definition**	**Page**
$\mathcal{D}^{\mathrm{Gal}[\varphi]}$	The category of internal covariant presheaves in $\mathcal{D}$ on the internal groupoid $\mathrm{Gal}[\varphi]$	110
$\mathcal{I}_K$	The functor $\mathcal{I}_K : K\text{-}\sigma\text{-}\mathbf{FAlg}^{\mathbf{op}} \to \sigma\text{-}\mathbf{FSet}$	112
$\mathcal{H}_K$	The functor $\mathcal{H}_K : \sigma\text{-}\mathbf{FSet} \to K\text{-}\sigma\text{-}\mathbf{FAlg}^{\mathbf{op}}$	113
$\mathbf{Spl}_K(L)$	The category of étale K-σ-algebras split by L	116
$\bar{k}_m$	The difference field $(\bar{k}, \varphi_{\bar{k}}^m)$	120
$\widehat{\Sigma}_{M/K}$	The subset of $\Sigma_{M/K}$ consisting of lifts of $\sigma_{\widehat{K}}$	125

Bibliography

[Bab62] Albert E. Babbitt, Jr. Finitely generated pathological extensions of difference fields. *Trans. Amer. Math. Soc.*, 102:63–81, 1962.

[BJ01] Francis Borceux and George Janelidze. *Galois theories*, volume 72 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2001.

[Cad13] Anna Cadoret. Galois categories. In *Arithmetic and geometry around Galois theory*, volume 304 of *Progr. Math.*, pages 171–246. Birkhäuser/Springer, Basel, 2013.

[CF95] Stephen D. Cohen and Michael D. Fried. Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: an elementary version. *Finite Fields Appl.*, 1(3):372–375, 1995.

[CH99] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.

[Coh65] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.

[Coh70] Stephen D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.

[Con] K. Conrad. Tensor products. Available at: `https://kconrad.math.uconn.edu/blurbs/linmultialg/tensorprod.pdf`. Expository paper.

[Dic97] Leonard Eugene Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. of Math.*, 11(1-6):65–120, 1896/97.

[DL63] H. Davenport and D. J. Lewis. Notes on congruences. I. *Quart. J. Math. Oxford Ser. (2)*, 14:51–60, 1963.

[DVHW14] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference Galois theory of linear differential equations. *Adv. Math.*, 260:1–58, 2014.

[DVHW17] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference algebraic relations among solutions of linear differential equations. *J. Inst. Math. Jussieu*, 16(1):59–119, 2017.

[EH00] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[FGS93] Michael D. Fried, Robert Guralnick, and Jan Saxl. Schur covers and Carlitz's conjecture. *Israel J. Math.*, 82(1-3):157–225, 1993.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[FK88] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné.

[Fri94] Michael D. Fried. Global construction of general exceptional covers with motivation for applications to encoding. In *Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993)*, volume 168 of *Contemp. Math.*, pages 69–100. Amer. Math. Soc., Providence, RI, 1994.

[Fri05] Michael D. Fried. The place of exceptional covers among all Diophantine relations. *Finite Fields Appl.*, 11(3):367–433, 2005.

[Fri74] Michael Fried. On a theorem of MacCluer. *Acta Arith.*, 25:121–126, 1973/74.

[GD71] A. Grothendieck and J. A. Dieudonné. *Eléments de géométrie algébrique. I*, volume 166 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1971.

[Gro63] Alexander Grothendieck. *Revêtements étales et groupe fondamental. Fasc. I: Exposés 1 à 5*, volume 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris, 1963.

[GTZ07] Robert M. Guralnick, Thomas J. Tucker, and Michael E. Zieve. Exceptional covers and bijections on rational points. *Int. Math. Res. Not. IMRN*, (1), 2007.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[HMM14] Fernando Hernando, Gary McGuire, and Francisco Monserrat. On the clas-

sification of exceptional planar functions over $\mathbb{F}_p$. *Geom. Dedicata*, 173:1–35, 2014.

[Hou15] Xiang-dong Hou. Permutation polynomials over finite fields—a survey of recent advances. *Finite Fields Appl.*, 32:82–119, 2015.

[Hru01] Ehud Hrushovski. The Manin-Mumford conjecture and the model theory of difference fields. *Ann. Pure Appl. Logic*, 112(1):43–115, 2001.

[Hru04] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms. `arXiv:math/0406514`, 2004. The most recent version of the paper (2012) is available at: `http://www.ma.huji.ac.il/~ehud/FROB.pdf`.

[KK17] Gurgen Khachatrian and Melsik Kyureghyan. Permutation polynomials and a new public-key encryption. *Discrete Appl. Math.*, 216(part 3):622–626, 2017.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lev08] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LM93] Rudolf Lidl and Gary L. Mullen. Unsolved Problems: When Does a Polynomial over a Finite Field Permute the Elements of the Field?, II. *Amer. Math. Monthly*, 100(1):71–74, 1993.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia*

of Mathematics and its Applications. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[Mac67] C. R. MacCluer. On a conjecture of Davenport and Lewis concerning exceptional polynomials. *Acta Arith*, 12:289–299, 1966/1967.

[Mac97] Angus Macintyre. Generic automorphisms of fields. volume 88, pages 165–180. 1997. Joint AILA-KGS Model Theory Meeting (Florence, 1995).

[Mat94] Rex Matthews. Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field. *Proc. Amer. Math. Soc.*, 120(1):47–51, 1994.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[RD33] J. F. Ritt and J. L. Doob. Systems of Algebraic Difference Equations. *Amer. J. Math.*, 55(1-4):505–514, 1933.

[Rit50] Joseph Fels Ritt. *Differential Algebra*. American Mathematical Society Colloquium Publications, Vol. XXXIII. American Mathematical Society, New York, N. Y., 1950.

[RR39] J. F. Ritt and H. W. Raudenbush, Jr. Ideal theory and algebraic difference equations. *Trans. Amer. Math. Soc.*, 46:445–452, 1939.

[SSS09] Rajesh P Singh, BK Sarma, and Anupam Saikia. Public key cryptography using permutation p-polynomials over finite fields. *IACR Cryptol. ePrint Arch.*, page

208, 2009.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.

[Tom14] Ivan Tomašić. A twisted theorem of Chebotarev. *Proc. Lond. Math. Soc. (3)*, 108(2):291–326, 2014.

[Tom16] Ivan Tomašić. Twisted Galois stratification. *Nagoya Math. J.*, 222(1):1–60, 2016.

[Tom20] Ivan Tomašić. A topos-theoretic view of difference algebra, 2020. Preprint.

[TW18] Ivan Tomašić and Michael Wibmer. Strongly étale difference algebras and Babbitt's decomposition. *J. Algebra*, 504:10–38, 2018.

[TZ16] Ivan Tomašić and Michael E. Zieve. Difference exceptional polynomials, July 2016. Unpublished sketch paper.

[Var88] V Varadharajan. Cryptosystems based on permutation polynomials. *International Journal of Computer Mathematics*, 23(3-4):237–250, 1988.

[Wib13] Michael Wibmer. Algebraic difference equations. Available at: `https://www.math.upenn.edu/~wibmer/AlgebraicDifferenceEquations.pdf`, February 2013. Online lecture notes.

[Wib15] Michael Wibmer. Affine difference algebraic groups. Available at: `https://sites.google.com/view/wibmer/research`, 2015. Habilitation thesis.

[Wil67] Kenneth S. Williams. On extremal polynomials. *Canad. Math. Bull.*, 10:585–594, 1967.

[Zie13] Michael E. Zieve. Exceptional polynomials. In Gary L. Mullen, editor, *Handbook of finite fields*, Discrete Mathematics and its Applications (Boca Raton), chapter 8, pages 236–240. CRC Press, Boca Raton, FL, 2013.