Twisted Galois stratification
TOMASIC, I

© 2011 Académie des sciences.

For additional information about this publication click this link.
http://qmro.qmul.ac.uk/xmlui/handle/123456789/12506

Information about this research object was correct at the time of download; we occasionally make corrections to records, please therefore check the published record when citing. For more information contact scholarlycommunications@qmul.ac.uk
TWISTED GALOIS STRATIFICATION

IVAN TOMAŠIĆ

Abstract. We prove a direct image theorem stating that the direct image of a Galois formula by a morphism of difference schemes is equivalent to a Galois formula over fields with powers of Frobenius. As a consequence, we obtain an effective quantifier elimination procedure and a precise algebraic-geometric description of definable sets over fields with Frobenii in terms of twisted Galois formulae associated with finite Galois covers of difference schemes.

Contents

1. Introduction 2
2. Generalised difference algebra and geometry 4
2.1. Difference structures 4
2.2. Difference spectra 6
2.3. Difference schemes 6
2.4. Galois covers 8
3. Local study of difference schemes and their morphisms 9
3.1. Difference schemes vs. pro-algebraic varieties 9
3.2. Local Properties 15
3.3. Etale morphisms of difference schemes 18
3.4. Etale Galois covers 20
3.5. Transformal separability 22
4. Bi-fibered structure of the category of difference schemes 22
5. Babbitt’s decomposition 25
5.1. Non-abelian difference Galois cohomology 25
5.2. Benign extensions and Babbitt’s theorem 26
5.3. Galois closure 28
5.4. Ampleness of finite difference structures 29
6. Effective difference algebraic geometry 32
7. Galois stratification 34
7.1. Galois stratifications and Galois formulae 34
7.2. Direct Image Theorems 36
7.3. Quantifier elimination for Galois formulae 42
References 44

Date: May 6, 2016.
Key words and phrases. difference scheme, Galois stratification, Galois formula, Frobenius automorphism, ACFA.
1. Introduction

Galois stratification, originally developed through work of Fried, Haran, Jarden and Sacerdote ([14], [11], [13]), provides an explicit arithmetic-geometric description of definable sets over finite fields in terms of Galois formulae associated to Galois covers of algebraic varieties. When compared to the earlier work of Ax [2], made more explicit by Kiefe [19], which showed that every formula in the language of rings is equivalent to a formula with a single (bounded) existential quantifier, the fundamental achievement of the Galois stratification was the effective (in fact primitive recursive) nature of its quantifier elimination procedure. Moreover, the precise description of formulae in terms of Galois covers was particularly well-suited for applications of geometric and number-theoretic nature, for example in Fried’s work on Davenport’s problem [12]. In our opinion, the most impressive application was in the work of Denef and Loeser on arithmetic motivic integration in [8]. They assign a Chow motive to a Galois formula, thus extending the consideration of algebraic-geometric invariants of algebraic varieties to arbitrary first-order formulae.

We develop the theory of twisted Galois stratification in order to describe first-order definable sets in the language of difference rings over algebraic closures of finite fields equipped with powers of the Frobenius automorphism. A (normal) Galois stratification on a difference scheme \((X, \sigma)\) is a datum

\[ \mathcal{A} = \langle X, Z_i/X_i, C_i \mid i \in I \rangle, \]

where \(X_i, i \in I\) is a partition of \(X\) into finitely many normal locally closed difference subschemes of \(X\), each \((Z_i, \Sigma_i) \to (X_i, \sigma)\) is a Galois cover with some group \((G_i, \tilde{\Sigma}_i)\) and \(C_i\) is a conjugacy domain in \(\Sigma_i\), with all these notions defined in Section 2. The Galois formula associated with \(\mathcal{A}\) is the realisation subfunctor \(\tilde{\mathcal{A}}\) of \(X\) defined by the assignment

\[ \tilde{\mathcal{A}}(F, \varphi) = \bigcup_{i \in I} \{ x \in X_i(F, \varphi) : \varphi_x \subseteq C_i \} \subseteq X(F, \varphi), \]

where \((F, \varphi)\) is an algebraically closed difference field and the conjugacy class \(\varphi_x \subseteq \Sigma\) is the local \(\varphi\)-substitution at \(x\), see [3.44]. Our principal result in its algebraic-geometric incarnation is the following direct image theorem, stating that a direct image of a Galois formula by a morphism of finite transformal type is equivalent to a Galois formula over fields with Frobenius. Equivalently, the class of Galois formulae over fields with Frobenius is closed under taking direct images by morphisms of finite transformal type (the precise statement is 7.12).

**Theorem 1.1.** Let \(f : (X, \sigma) \to (Y, \sigma)\) be a morphism of finite transformal type (over a suitable base), and let \(\mathcal{A}\) be a Galois stratification on \(X\). We can effectively compute a Galois stratification \(\mathcal{B}\) on \(Y\) such that for all (suitable) \((\bar{\mathbb{F}}_p, \varphi)\) with a high enough power of Frobenius \(\varphi\),

\[ f(\tilde{\mathcal{A}}(\bar{\mathbb{F}}_p, \varphi)) = \tilde{\mathcal{B}}(\bar{\mathbb{F}}_p, \varphi). \]

A model-theoretic restatement of the above theorem is that fields with Frobenius allow quantifier elimination in the language of Galois formulae. In other words, any definable set over fields with powers of Frobenius can be described by a Galois formula (the precise statement is 7.15).
Theorem 1.2. Let $\theta(x_1, \ldots, x_n)$ be a first-order formula in the language of difference rings (with suitable parameters). We can effectively compute a Galois stratification $A$ of the difference affine $n$-space such that for all (suitable) $(\bar{F}_p, \varphi)$ with a high enough power of Frobenius $\varphi$,

$$\theta(\bar{F}_p, \varphi) = \tilde{A}(\bar{F}_p, \varphi).$$

Conversely, every Galois formula is equivalent to a first-order formula in the language of difference rings over algebraically closed difference fields.

Historically speaking, the comparison of our result to the known model-theoretic quantifier elimination result found by Macintyre [21] and greatly refined in modern terms by Chatzidakis and Hrushovski [6], is parallel to the relation between the work of Fried-Sacerdote and the work of Ax mentioned above. The logic quantifier elimination [6, 1.6] states that any formula $\theta(x_1, \ldots, x_n)$ in the language of difference rings is equivalent, modulo the theory ACFA of existentially closed difference fields, to a Boolean combination of formulae of the form

$$\exists y \psi(y; x_1, \ldots, x_n),$$

where $\psi$ is quantifier free, and $\psi(y; x_1, \ldots, x_n)$ implies that $y$ satisfies a nonzero polynomial whose coefficients are $\sigma$-polynomials in $x_1, \ldots, x_n$, i.e., the single existential quantifier is bounded. The proof uses the compactness theorem and, although recursive, such quantifier elimination proceeds by unbounded searches and it is far from being primitive recursive or effective in a suitable sense of the word.

The main achievements of our paper are:

1. the fine quantifier elimination, our Galois formulae being associated with finite Galois covers of difference schemes, whereas the covers associated with the logic quantifier elimination are in general only quasi-finite, with possibly infinite algebraic extensions of function fields;
2. the effectivity of our quantifier elimination procedure, the proof of the direct image theorem being fundamentally algorithmic and algebraic-geometric in nature.

We show that our quantifier elimination and the decision procedure for fields with Frobenii are $\dagger$-primitive recursive, i.e., primitive-recursive reducible to basic operations in difference algebra, as detailed in Section 6. Given that some of the most elementary constructions in difference algebra are not known to be primitive recursive themselves, the strength of the hybrid notion of $\dagger$-primitive recursiveness is strongly dependent on future developments in the field of effective/constructive difference algebra. For that reason, we developed a coarser theory of direct Galois stratification (in the sense of [10]), to show that the logic quantifier elimination is outright primitive recursive in [23]. Needless to say, while it may be possible to start with the model-theoretic quantifier elimination and deduce the precise form of 1.2 (in fact 7.17), taking this route would be missing the point.

The statement 1.2 is over fields with Frobenii and that is why we must refer to the present author’s Chebotarev Lemma [24, 4.28] which uses the difficult paper [18] on twisted Lang-Weil estimates, proving the earlier conjecture of [21] that ACFA is the elementary theory of fields with Frobenii. This is the only use of the main result of [18] in this paper, and the remaining references to [18] are mostly foundational lemmas. However, our Galois stratification procedure works over existentially closed difference fields unconditionally, without the use of [18], see 7.17.
One of the biggest challenges was the correct formulation of the result and even a suitable definition of a Galois cover, which already requires the full power of the theory of generalised difference schemes developed in [24], since the category of strict difference schemes has no reasonable Galois actions, covers or quotients. One clear advantage of the description of the definable sets in terms of (twisted) Galois stratifications is our ability to reduce considerations regarding points on definable sets to calculations of various character sums, as expounded in [24]. Since the style of our proof is reminiscent of many a direct image theorem from algebraic geometry, our results should appeal to algebraic geometers and number theorists and we expect more diophantine applications to follow.

Our approach to the proof of 1.1 (in fact of 7.12) is more geometric and conceptual than those of [14], [11], [13] in the classical case. The proof from [22] in the algebraic case uses the theory of the étale fundamental group in a rather sophisticated way, which is not available in the difference scenario. However, by performing a ‘baby’ Stein factorisation at the start of our procedure, the only remnant of that theory is the short exact sequence for the étale fundamental group, in which case we can ‘manually’ keep track of what happens at the level of finite Galois covers. From this point of view, even if we were to eliminate all the difference language, our line of proof would still yield an essentially new proof in the classical case. Here, on the other hand, we must treat several genuinely new difference phenomena which do not arise in the algebraic case. Key ingredients include Babbitt’s decomposition theorem 5.12 and our Chebotarev lemma [24, 4.28].

The foundation of the theory of generalised difference schemes has been laid in [24]. We give a gist of it in Section 2 and we develop the framework even further in Section 4.

In the course of the proof, we use local properties of difference schemes previously unknown in difference algebraic geometry, developed in Section 3. It must be emphasised that our theory is almost orthogonal to the various notions of smoothness that appear in G. Giabicani’s thesis [15], see 3.31.

En route to the main theorem, we encounter another merit of working in the context of generalised difference schemes, a difference version of Chevalley’s theorem 7.7 which gives a sufficient condition for the image of a morphism of difference schemes of finite transfromal type to contain a dense open set. Wibmer gives a similar result by generalising difference algebra in a slightly different direction [26].

The author would like to thank Michael Fried, Angus Macintyre, Thomas Scanlon and Michael Wibmer for fruitful discussions on the topic of this paper, and to Zoe Chatzidakis for pointing out the importance of Babbitt’s decomposition and for helping to improve a preliminary version of the paper. We gratefully acknowledge the hospitality of IHES Paris and MPIM Bonn, where significant parts of the paper were produced.

2. Generalised difference algebra and geometry

In this section we give a summary of the theory of generalised difference schemes from [24]. The familiarity with this work is crucial and we often refer to numerous technical results from [24] we were not able to include here. However, the reader acquainted with [18] may be able to follow the subsequent developments that refer to ordinary difference schemes.

2.1. Difference structures.
Definition 2.1. Let us consider the category $\text{Diff}$ as follows. An object of $\text{Diff}$ is a set $\Sigma$, equipped with a map $\Sigma \times \Sigma \rightarrow \Sigma$, $(\sigma, \tau) \mapsto \sigma \circ \tau$ such that:

1. $\sigma \circ \sigma = \sigma$;
2. $(\sigma \circ \tau) \circ \upsilon = (\sigma \circ \upsilon) \circ (\tau \circ \upsilon)$ for all $\sigma, \tau, \upsilon \in \Sigma$.

A morphism $\phi : \Sigma \rightarrow T$ is a function such that for all $\sigma, \tau \in \Sigma$,

$$\phi(\sigma \circ \tau) = \phi(\sigma) \circ \phi(\tau).$$

Inherently, for every $\sigma \in \Sigma$, the map $(\cdot) \circ \sigma : \Sigma \rightarrow \Sigma$ is a $\text{Diff}$-morphism.

Definition 2.2. The difference category of locally ringed spaces has objects of form $(X, \Sigma)$, where $(X, O_X)$ is a locally ringed space, and $\Sigma$ is a set of endomorphisms of $X$ such that there exists a function $\Sigma \times \Sigma \rightarrow \Sigma$, $(\sigma, \tau) \mapsto \tau \sigma$ with:

1. for every $\sigma, \tau \in \Sigma$,

$$\tau \sigma \circ \tau = \tau \circ \sigma;$$

2. $(\Sigma, (\sigma, \tau) \mapsto \tau \sigma)$ is an object of $\text{Diff}$.

A morphism $(\varphi, \tau(\cdot)) : (X, \Sigma) \rightarrow (Y, T)$ consists of a $\text{Diff}$-morphism $\tau(\cdot) : \Sigma \rightarrow T$ and a morphism of locally ringed spaces $\varphi : X \rightarrow Y$ such that for every $\sigma \in \Sigma$,

$$\tau \sigma \circ \varphi = \varphi \circ \sigma.$$

Definition 2.3. The category of difference rings has objects of form $(A, \Sigma)$, where $A$ is a commutative ring with identity and $\Sigma$ is a set of endomorphisms $A \rightarrow A$ such that there exists a function $\Sigma \times \Sigma \rightarrow \Sigma$, $(\sigma, \tau) \mapsto \tau \sigma$ with:

1. for every $\sigma, \tau \in \Sigma$,

$$\tau \sigma \circ \tau = \tau \circ \sigma;$$

2. $(\Sigma, (\sigma, \tau) \mapsto \tau \sigma)$ is an object of $\text{Diff}$.

A morphism $\varphi : (B, T) \rightarrow (A, \Sigma)$ consists of a $\text{Diff}$-morphism $(\cdot) \varphi : \Sigma \rightarrow T$ and a ring homomorphism $\varphi : B \rightarrow A$ and a such that

$$\varphi \circ \sigma \varphi = \sigma \circ \varphi.$$

Definition 2.4. Each difference ring $(A, \Sigma)$ has a natural action of the free semigroup $(\Sigma)$ generated by $\Sigma$, as well as the rig $\mathbb{N}[\Sigma] = \mathbb{N}[\langle \Sigma \rangle]$ of positive integer combinations of elements of $(\Sigma)$. The difference ring localisation of $A$ at $f \in A$ is $A_{f \Sigma} = \{ \nu f : \nu \in \mathbb{N}[\Sigma] \}^{-1} A$.

Definition 2.5. A difference ring $(A, \Sigma)$ is called

1. strong, or $\Sigma$-reduced, if all endomorphisms in $\Sigma$ are injective;
2. inversive, if every $\sigma \in \Sigma$ is an automorphism of $A$;
3. almost-strict, if there exist a finite subgroup $G$ of $\text{Aut}(A, \Sigma)$, an element $\sigma \in \Sigma$ and a group homomorphism $(\cdot) \sigma : G \rightarrow G$ such that $\Sigma = \sigma G$, and for all $g \in G$, $\sigma g = \sigma g\sigma$. Consequently, the difference structure is given by

$$(\sigma g)^{(\sigma h)} = \sigma(h^{-1} g)^{\sigma}. h.$$

Every strong difference ring $(A, \Sigma)$ with $\Sigma$ finite and every $(\cdot) \sigma : \Sigma \rightarrow \Sigma$ bijective has an inversive closure.

Definition 2.6. Let $I$ be an ideal in a difference ring $(A, \Sigma)$. We say that:

1. $I$ is a $\Sigma$-ideal if $\sigma(I) \subseteq I$ for every $\sigma \in \Sigma$;
2. $I$ is $\Sigma$-reflexive if $\sigma^{-1}(I) = I$ for every $\sigma \in \Sigma$;
3. $I$ is $\Sigma$-well-mixed if $ab \in I$ implies $a \sigma(b) \in I$ for any $\sigma \in \Sigma$.
4. A itself is well-mixed if the zero ideal is;
5. $I$ is $\Sigma$-perfect if for every $\sigma \in \Sigma$, $a \sigma a \in I$ implies $a$ and $\sigma a$ are both in $I$.
6. $A$ is a transmorphic domain if $(A, \Sigma)$ is strong and $A$ is a domain.

2.2. Difference spectra.

Definition 2.7. Let $(R, \Sigma)$ be a difference ring. We consider each of the following subsets of $\text{Spec}(R)$ as locally ringed spaces with the Zariski topology and the structure sheaves induced from $\text{Spec}(R)$:

1. $\text{Spec}^\sigma(R) = \{ p \in \text{Spec}(R) : \sigma^{-1}(p) = p \}$, for any $\sigma \in \Sigma$;
2. $\text{Spec}^\Sigma(R) = \bigcup_{\sigma \in \Sigma} \text{Spec}^\sigma(R)$.

In discussions of induced topology, we use the notation $V^\sigma(I), D^\sigma(I), V^\Sigma(I), D^\Sigma(I)$, for the traces of $V(I)$ and $D(I)$ on $\text{Spec}^\sigma(R), \text{Spec}^\Sigma(R)$, respectively.

Writing $X = \text{Spec}^\Sigma(R)$, bearing in mind that for $\sigma, \tau \in \Sigma$,

$$a^\sigma(\text{Spec}^\tau(R)) \subseteq \text{Spec}^{\tau^\sigma}(R),$$

each $\sigma \in \Sigma$ induces the morphism of locally ringed spaces $(a^\sigma, \tilde{\sigma}) : (X, O_X) \to (X, O_X)$. Consequently, the locally ringed space $(X, O_X)$ is equipped with a set of endomorphisms of locally ringed spaces

$$a^\Sigma = \{(a^\sigma, \tilde{\sigma}) : \sigma \in \Sigma\},$$

which is closed under ‘conjugation’ through the relation $a^\sigma(\tau) = (\tau^\sigma)^*(a^\tau)$, making $(\text{Spec}^\Sigma(R), O_{\text{Spec}^\Sigma(R)}, a^\Sigma)$ into a difference locally ringed space.

Similarly, a morphism $\varphi : (S, T) \to (R, \Sigma)$ of difference rings satisfies

$$a^\varphi(\text{Spec}^\sigma(R)) \subseteq \text{Spec}^{\sigma^\varphi}(S),$$

and it gives rise to a morphism in the difference category of locally ringed spaces

$$(a^\varphi, \tilde{\varphi}, a^\varphi^\sigma) : (\text{Spec}^\Sigma(R), a^\Sigma) \to (\text{Spec}^T(S), a^T).$$

This makes $\text{Spec}$ into a contravariant functor from the category of difference rings to the difference category of locally ringed spaces which respects the difference structure.

Fact 2.8. Let $(A, \Sigma)$ be a well-mixed difference ring with finite $\Sigma$ so that $X = \text{Spec}^\Sigma(A)$ is quasi-compact.

1. The canonical morphism $i : A \to \bar{A} = H^0(X) = O_X(X)$ is injective and induces an isomorphism of difference schemes

$$(a^i, i) : \text{Spec}^\Sigma(\bar{A}) \sim \to \text{Spec}^\Sigma(A).$$

2. Consequently, the functor $H^0$ is left adjoint to $\text{Spec}$.

2.3. Difference schemes.

Definition 2.9. (1) An affine difference scheme is an object $(X, O_X, \Sigma)$ of the difference category of locally ringed spaces, which is isomorphic to $\text{Spec}^\Sigma(A)$ for some difference ring $(A, \Sigma)$.

(2) A difference scheme is an object $(X, O_X, \Sigma)$ of the difference category of locally ringed spaces, which is locally an affine difference scheme.

(3) A morphism of difference schemes $(X, O_X, \Sigma) \to (Y, O_Y, T)$ is just a morphism in the difference category of locally ringed spaces.
Definition 2.10. Let \((X, \Sigma)\) be a difference scheme and \(x \in X\) a point. Let
\[
\Sigma_x = \{ \sigma \in \Sigma : \sigma(x) = x \}, \quad \Sigma^*_x = \{ \sigma^*_x : \sigma \in \Sigma_x \}, \quad \text{and} \quad \Sigma^x = \{ \sigma^x : \sigma \in \Sigma_x \},
\]
where \(\sigma^x : k(x) \to k(x)\) is induced by the local morphism \(\sigma^x_0 : \mathcal{O}_x \to \mathcal{O}_x\) associated with each \(\sigma \in \Sigma_x\). This yields a difference local ring \((\mathcal{O}_x, \Sigma^*_x)\) with difference residue field \((k(x), \Sigma^x)\).

Definition 2.11. A difference scheme \((X, \mathcal{O}_X, \Sigma)\) is said to be:

1. reduced, if the nilradical of each \(\mathcal{O}_x\) is trivial;
2. perfectly reduced, if the perfect closure of 0 in each \(\mathcal{O}_x\) is trivial;
3. irreducible (resp. connected) if its underlying topological space is;
4. integral (resp. transformally integral) if it is irreducible and reduced (resp. perfectly reduced);
5. well-mixed, if each \(\mathcal{O}_x\) is well-mixed.

We often work in a relative setting, over a chosen base scheme \((S, \Sigma_0)\) or a base difference ring \((R, \Sigma_0)\). An \(S\)-scheme is a difference scheme morphism \((X, \Sigma) \to (S, \Sigma_0)\), and morphisms between \(S\)-difference schemes are required to preserve the structural morphisms to \(S\). Similarly, an \((R, \Sigma_0)\)-difference scheme is locally of the form \(\text{Spec}^\Sigma(A)\), for a difference \((R, \Sigma_0)\)-algebra \((A, \Sigma)\), and morphisms are required to locally preserve the \((R, \Sigma_0)\)-algebra structure.

Definition 2.12. Let \((X, \Sigma)\) be a difference scheme and \((K, \varphi)\) a difference field. The set of \((K, \varphi)\)-rational points of \((X, \Sigma)\) is the set
\[
\text{Hom}(\text{Spec}^\Sigma(K), (X, \Sigma)).
\]

In a relative setting, the points are required to factor through the base. A geometric point of a difference scheme is a point with values in an algebraically closed difference field.

In order for a fibre product \((X_1, \Sigma_1) \times_{(S, \Sigma_0)} (X_2, \Sigma)\) to exist, the factors have to be compatible in a suitable sense. However, this technical difficulty is largely overcome by the framework of generalised difference schemes and we can ensure that all the products we form in subsequent sections are compatible.

Definition 2.13. Let \((X, \Sigma) \to (S, \Sigma_0)\) be a morphism of difference schemes, considered as a family parametrized by \(S\). Let \((K, \varphi)\) be a difference field and let \(s \in (S, \Sigma_0)(K, \varphi)\). The fibre \(X_s\) is the \((K, \varphi)\)-difference scheme obtained by base change via the morphism \(s : \text{Spec}^\varphi(K) \to (S, \Sigma_0)\),
\[
(X_s, \Sigma_s) = (X, \Sigma) \times_{(S, \Sigma_0)} \text{Spec}^\varphi(K).
\]

Let \(P\) be a property of difference schemes. If \((X, \Sigma) \to (S, \Sigma_0)\) is a difference scheme over a given base, we shall say that \(X\) is geometrically \(P\), if every base change of \(X\) has the property \(P\).

Definition 2.14. Let \((R, \Sigma_0)\) be a difference ring.

1. An \((R, \Sigma_0)\)-algebra \((A, \Sigma)\) is of finite \(\Sigma\)-type if there exist elements \(a_1, \ldots, a_n\) in \(A\) such that \(A = R[a_1, \ldots, a_n]_{\Sigma} = R[\nu a_1, \ldots, \nu a_n : \nu \in (\Sigma)]\).
2. An \((R, \Sigma_0)\)-difference scheme \((X, \Sigma)\) is of finite \(\Sigma\)-type, or of finite transformal type if it is a finite union of affine difference schemes of the form \(\text{Spec}^\Sigma(A)\), where \((A, \Sigma)\) is of finite \(\Sigma\)-type over \((R, \Sigma_0)\).
A morphism \( f : (X, \Sigma) \to (Y, \Sigma_0) \) is of finite \( \Sigma \)-type if \( Y \) is a finite union of open affine subsets \( V_i = \text{Spec}^{\Sigma_0}(R_i) \) such that for each \( i \), \( f^{-1}(V_i) \) is of finite \( \Sigma \)-type over \((R_i, \Sigma_0)\).

A morphism \( f : (X, \Sigma) \to (Y, \Sigma_0) \) is integral (resp. finite) if \( Y \) is a finite union of open affine subsets \( V_i = \text{Spec}^{\Sigma_0}(R_i) \) such that for each \( i \), \( f^{-1}(V_i) \) is \( \text{Spec}^{\Sigma}(A_i) \), where \( A_i \) is integral (resp. finite) over \( R_i \).

**Definition 2.15.** A difference ring \((R, \Sigma)\) is Ritt if it has the ascending chain condition on \( \Sigma \)-perfect ideals.

It is classically known ([7]) that every difference ring of finite \( \sigma \)-type over a Ritt difference ring is Ritt, or, equivalently, that difference schemes of finite \( \sigma \)-type over a Ritt difference ring are topologically Noetherian. Moreover, a perfectly reduced difference scheme decomposes into transformally integral components.

In the generalised context, we have the following.

**Fact 2.16.** Let \((S, \Sigma)\) be an almost-strict algebra of finite \( \Sigma \)-type over a Ritt ring \((R, \sigma_0)\), and \( \Sigma \) finite. Then \( \text{Spec}^\Sigma(S) \) is topologically Noetherian and \( S \) has an ascending chain condition on ideals which are perfect with respect to any \( \sigma \in \Sigma \).

### 2.4. Galois covers

**Definition 2.17.** A difference group \((G, \Sigma)\) is a group \( G \), together with a \( \text{Diff} \)-structure \( \Sigma \) of group endomorphisms satisfying the properties from 2.2 (more precisely, it is an object of the difference category over the category of groups in the sense of 2.2).

We say that a group \((G, \Sigma)\) acts (on the left) by automorphisms on a ring \((A, \Sigma)\), if every \( \sigma \in \Sigma \) corresponds to an endomorphism \( (\cdot)\sigma \in \Sigma \) of \( G \) so that, for every \( g \in G \) and \( \sigma, \tau \in \Sigma \),

\[(g^\tau)^\sigma = (g^\sigma)^\tau,\]

and, in \( \text{End}(A) \), we have the relation

\[g\sigma = \sigma g^\sigma.\]

We invite the reader to formulate dual axioms for an action of a difference group \((G, \Sigma_0)\) on a locally ringed space \((X, \Sigma)\), where each \( \sigma \in \Sigma \) corresponds to an endomorphism \( \sigma() \in \Sigma_0 \) of \( G \).

**Remark 2.18.** If \((G, \Sigma)\) acts on \((A, \Sigma)\), then \((^\sigma G, \Sigma_0)\) acts on \((X, ^\sigma \Sigma) = \text{Spec}^{^\sigma \Sigma}(A)\) for \( \Sigma_0 = \{ ^\sigma() : \sigma \in \Sigma \} \).

**Notation 2.19.** Identifying the two difference groups from the remark, by a slight abuse of notation, we henceforth write \( \bar{\Sigma} \) for either of \( \Sigma, \Sigma_0 \), so that we can think of a difference group \((G, \bar{\Sigma})\) acting both on algebraic and geometric objects.

**Lemma 2.20.** Let \((A, \sigma)\) be a transformal domain. Suppose that a finite group \( G \) acts on \( A \) so that, writing \( B = A^G \), we have \( \sigma(B) \subseteq B \). Let \( \bar{\sigma} = \sigma |_B \). Then there exists a homomorphism \( (\cdot)^\sigma : G \to G \) satisfying \( g\sigma = \sigma g^\sigma \) for \( g \in G \), making \((A, \Sigma)\), for \( \Sigma = \sigma G \), into an almost-strict extension of \((B, \bar{\Sigma})\) with automorphism group \((G, \bar{\Sigma})\), where \( \bar{\Sigma} = \{ (\cdot)^\tau : \tau \in \Sigma \} \).

**Proof.** For a \( g \in G \), consider \( f_1 = j\sigma, f_2 = jg\sigma \), where \( j \) injects \( A \) into its fraction field. Since \( \sigma(B) \subseteq B \), we verify that \( f_1 |_B = f_2 |_B \), so \([5, \text{V}, \S 2.3, \text{Corollaire 1}]\) yields a \( h \in G \) such that \( f_2 = f_1h \). By injectivity of \( j \), we get \( g\sigma = \sigma h \). Since \( \sigma \) is injective, \( h \) is unique and we can write \( h = g^\sigma \). \( \square \)
Corollary 2.21. Let \((K, \bar{\sigma}) \to (L, \sigma)\) be a difference field extension where \(L/K\) is Galois with group \(G\). Let \(\Sigma\) be the set of all lifts of \(\bar{\sigma}\) to \(L\). Then \(\Sigma = \sigma G\) and we have endomorphisms \(\tilde{\Sigma} = \{\tau^\tau : \tau \in \Sigma\}\) of \(G\) such that \((G, \tilde{\Sigma})\) is the group of automorphisms of \((L, \Sigma)\) over \((K, \bar{\sigma})\).

Proposition 2.22. Suppose a finite group \((G, \Sigma)\) acts on the left on a difference ring \((A, \Sigma)\), and \(\Sigma G = \Sigma\). Consequently, \(G\) acts on the right on \(X = \text{Spec}^\Sigma(A)\) via \(x.g = a^g(x)\). Let \((B, \Sigma) = A^G\) be the subring of invariants of \(A\), \(Y = \text{Spec}^\Sigma(B)\) and let \(p : (X, a^\Sigma) \to (Y, a^\Sigma)\) be the canonical \((G\text{-invariant})\) morphism. Then the following holds.

1. \(A\) is integral over \(B\).
2. The morphism \(p\) is surjective, its fibres are \(G\)-orbits and the topology of \(Y\) is the quotient of the topology of \(X\).
3. Let \(x \in X\), \(y = p(x)\). Write \(G_x\) for the stabiliser of \(x\) and \(\Sigma_x = \{\sigma \in \Sigma : a^\sigma(x) = x\}\) (we used \(a^\Sigma_x = a^\Sigma(x)\) in 2.10). Let \(\tilde{\Sigma}_x = \{\sigma^\tau : \tau \in \Sigma_x\}\) and \(\tilde{\Sigma}_x = \{\sigma^\tau : \sigma \in \Sigma_x\}\), where \(\sigma^\tau : k(x) \to k(y)\) is induced by \(\sigma^\tau : \tilde{\Sigma}_x \to \tilde{\Sigma}_x\) for every \(\sigma \in \Sigma_x\). Then \((k(x))\) is a quasi-Galois algebraic extension of \(k(y)\) and the canonical map

\[
(G_x, \tilde{\Sigma}_x) \to \left(\text{Gal}(k(x)/k(y)), \tilde{\Sigma}_x\right)
\]

is surjective.
4. The natural homomorphism \(\mathcal{O}_Y \to (p_*, \mathcal{O}_X)^G\) is an isomorphism.
5. \((Y, \Sigma)\) is a quotient difference scheme of \((X, \Sigma)\) by \(G\).

Definition 2.23. Let \((X, \Sigma)\) be a difference scheme with a finite group of automorphisms \((G, \Sigma)\) such that \(G\Sigma = \Sigma\) and let \(p : (X, \Sigma) \to (Y, T)\) be an affine invariant morphism inducing \(\mathcal{O}_Y \xrightarrow{\sim} (p_*, \mathcal{O}_X)^G\). In this case, the morphism \(p\) is called a Galois cover of \((Y, T)\) with group \((G, \Sigma)\).

If \(p\) is a Galois cover, it can be shown that \((Y, T)\) is isomorphic to the quotient difference scheme \((X, \Sigma)/(G, \Sigma)\) and the conclusions 1, 2, 3 of 2.22 still hold.

3. LOCAL STUDY OF DIFFERENCE SCHEMES AND THEIR MORPHISMS

3.1. Difference schemes vs. pro-algebraic varieties. One of the most important ideas in the study of difference algebraic geometry was the realisation that there is a translation mechanism between the language of difference schemes and that of algebraic correspondences, or, more generally, systems of prolongations associated with a difference scheme.

We would like to be able to reduce the study of certain local properties of difference schemes to the study of known properties of algebraic schemes through systems of prolongations. In order to achieve this goal, we must be able to speak about difference subvarieties of ordinary algebraic varieties, which is achieved by defining a difference scheme associated to a scheme.

Proposition 3.1 ([18]). Let \((R, \varsigma)\) be a difference ring. The forgetful functor from the category of difference \((R, \varsigma)\)-algebras to the category of \(R\)-algebras has a left adjoint \([\varsigma]_R\), i.e., for every \(R\)-algebra \(A\) we have a homomorphism \(A \to [\varsigma]_R A\) inducing the functorial isomorphism

\[
\text{Hom}_{(R, \varsigma)}([\varsigma]_RA, (C, \sigma)) = \text{Hom}_R(A, C),
\]
for every \((R, \varsigma)\)-algebra \((C, \sigma)\).

Proof. Let us write \(A_{\varsigma^i} = A \otimes_R R\), where the morphism \(R \to R\) is \(\varsigma^i\), and let \(\sigma_{i,j} : A_{\varsigma^i} \to A_{\varsigma^j}\) be the induced \(\varsigma^{j-i}\)-linear homomorphisms, for \(i \leq j\). Writing

\[A_n = \bigotimes_{i \leq n} A_{\varsigma^i},\]

where the tensor product is taken over \(R\), and

\[\sigma_n : A_n \to A_{n+1}\]

for the natural \(\varsigma\)-homomorphisms induced by the \(\sigma_{i,i+1}\), we obtain a system \(A_n\) of \(R\)-algebras directed by inclusions \(A_n \to A_{n+1}\). The direct limit \((|\varsigma|_RA, \sigma)\) of \(A_n\) and \(\sigma_n\) is clearly a difference \((R, \varsigma)\)-algebra, and the inclusion \(\iota : A \to |\varsigma|_RA\) is obtained by identifying \(A\) with \(A_0\).

We need to show that every \(R\)-homomorphism \(\varphi : A \to C\) to an \((R, \varsigma)\)-algebra \((C, \sigma)\) lifts uniquely to a \((R, \varsigma)\)-homomorphism \(\tilde{\varphi} : (|\varsigma|_RA, \sigma) \to (C, \sigma)\) such that \(\varphi = \tilde{\varphi}\iota\). By the universal property of tensor products, the diagram

\[\begin{array}{ccc}
C & \xrightarrow{\sigma^i} & C \\
\downarrow{\varphi} & & \downarrow{\varphi} \\
A & \xrightarrow{\sigma_{0,1}} & A_{\varsigma^1} \\
\downarrow & & \downarrow \\
R & \xrightarrow{\varsigma^1} & R
\end{array}\]

yields a unique \(\varphi : A_{\varsigma^i} \to C\), and subsequently \(\tilde{\varphi}_n = \bigotimes_{i \leq n} \varphi_i : A_n \to C\). Passing to the limit, we obtain \(\tilde{\varphi} : |\varsigma|_RA \to C\) with the required properties. □

**Proposition 3.2** (LS). Let \((R, \varsigma)\) be a difference ring and let \(X\) be an (algebraic) scheme over \(R\). The functor from the category of difference \((R, \varsigma)\)-schemes to the category of sets, \((Z, \sigma) \mapsto \text{Hom}_R(Z, X)\) (morphisms of locally \(R\)-ringed spaces) is representable. More precisely, the universal morphism \([|\varsigma|_RA, \sigma]X \to X\) of locally \(R\)-ringed spaces induces a functorial isomorphism

\[\text{Hom}_R(Z, X) \cong \text{Hom}_{(R, \varsigma)}((Z, \sigma), [|\varsigma|_RA], X),\]

for every \((R, \sigma)\)-difference scheme \((Z, \sigma)\).

Proof. Let us prove the affine case. Suppose \(X = \text{Spec}(A)\), \(Z = \text{Spec}^\sigma(C)\) for a well-mixed difference ring \((C, \sigma)\) and let \(f : Z \to X\) be a morphism of locally ringed spaces. By taking global sections of the corresponding sheaf morphism, we derive a ring homomorphism \(\varphi : A \to C = \mathcal{O}_Z(Z)\) so that, in view of \(2.8\) \(f\) is the restriction of \(\varphi : \text{Spec}(C) \to \text{Spec}(A)\) to \(\text{Spec}(C)\). Using \(3.1\) there is a unique lift \((|\varsigma|_R, \sigma) \to (C, \sigma)\) of \(\varphi\), which gives the required difference scheme morphism

\[Z \to \text{Spec}^\sigma(|\varsigma|_RA) = [|\varsigma|_RA], X.\]

Suppose now that \(X\) is an \(R\)-scheme and \((Z, \sigma)\) is a closed \((R, \varsigma)\)-difference subscheme of \([|\varsigma|_RA]X\). For ease of notation, let us write \(S = \text{Spec}(R)\). Writing \(X_{\varsigma^1}\) for the base change \(X \times_S S\) via the morphism \(\varsigma^1 : S \to S\), it is clear that the
\( \zeta^i \)-linear morphism \( \sigma^i : [\zeta]_RX \to [\zeta]_RX \) defines an \( R \)-morphism \( [\zeta]_RX \to X_{\zeta^i} \) and thus we deduce a morphism
\[
Z \hookrightarrow [\zeta]_RX \to X \times X_\zeta \times \cdots \times X_{\zeta^n} =: X[n).
\]
We denote the scheme-theoretic image of this map by \( Z[n] \), obtaining a closed \( R \)-subscheme \( Z[n] \hookrightarrow X[n] \) for every \( n \), called the \( n \)-th Zariski closure of the difference scheme \( Z \) in \( X \). Although the projective limit \( Z[\infty] \) of the \( Z[n] \) can be viewed as a scheme, we will find it most illuminating to view it as a pro-(scheme of finite type).

The maps \( X_{\zeta^{i+1}} \to X_{\zeta^i} \) induce the maps \( \sigma_n : X[n+1] \to X[n] \) and thus \( X[\infty] \) is equipped with an endomorphism \( \sigma \), which is the limit of \( \sigma_n \). In this context, \( [\zeta]_RX \) is the fixed point scheme of \( \sigma \) on \( X[\infty] \).

We say that \( Z \) is weakly Zariski dense in \( X \) if \( Z[0] = X \). Note that it can happen that \( Z \) is weakly Zariski dense in \( X \) but the set of points of \( Z \) is not Zariski dense in \( X \).

Let us now start with a difference scheme \( (X, \sigma) \) of finite \( \sigma \)-type over \( (R, \zeta) \) and build a system of ‘prolongations’ of \( X \) in which \( X \) is weakly Zariski dense by construction. We shall describe the procedure for an affine difference scheme \( (X, \sigma) = \text{Spec}^\sigma(A) \), where \( A = R[a] \sigma \) is an \( (R, \zeta) \)-algebra of finite \( \sigma \)-type, generated by a tuple \( a \in A \).

If we write \( A_n := R[a, \sigma a, \ldots, \sigma^n a] \), we have inclusions \( A_n \hookrightarrow A_{n+1} \) and maps \( \sigma_n : A_n \to A_{n+1} \) induced by \( \sigma \), so that \( (A, \sigma) \) is the direct limit of the \( A_n \) and the \( \sigma_n \). We obtain the following diagram for \( X_n = \text{Spec}(A_n) \).

\[
\begin{array}{ccccccc}
S & \hookrightarrow & X_0 & \hookrightarrow & X_1 & \hookrightarrow & X_2 & \hookrightarrow & \cdots \\
\downarrow \zeta & & \downarrow \sigma_0 & & \downarrow \sigma_1 & & \downarrow \sigma_2 & & \\
S & \hookrightarrow & X_{0\zeta} & \hookrightarrow & X_{1\zeta} & \hookrightarrow & X_{2\zeta} & \hookrightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
X_0 & \hookrightarrow & X_1 & \hookrightarrow & X_2 & \hookrightarrow & X_3 & \hookrightarrow & \cdots 
\end{array}
\]

By construction, we have closed immersions \( X_1 \hookrightarrow X_0 \times_S X_{0\zeta} \) and \( X_{n+1} \hookrightarrow X_n \times_{X_{n-1}\zeta} X_{n\zeta} \) for \( n \geq 1 \), and we conclude that we have written \( (X, \sigma) \) as a weakly Zariski dense difference subscheme of \( X_0 \).

**Lemma 3.3** (Preparation Lemma). With above notation, if \( A \) and \( R \) are formally integral, by \( \sigma \)-localising \( A \) and \( R \) we can arrange that morphisms
\[
X_{n+1} \to X_n \times_{X_{n-1}\zeta} X_{n\zeta} \to X_n \times_{X_{n-1}} X_n
\]
are isomorphisms for \( n \geq 1 \) and that \( X \) is a Zariski dense difference subscheme of \( X_0 \).

**Proof.** Let \( K \) be the fraction field of \( R \). By combining the statements 5.2.10, 5.2.11, 5.2.12 from [20], modulo a \( \zeta \)-localisation of \( R \), we can find a new tuple of generators \( a = bc \) so that, writing \( \sigma^i(a) = a_i = bc_i \) and \( L_n = K(a_0, \ldots, a_n) \) for the fraction field of \( A_n \), we have that for \( n \geq 1 \),

1. \( b_n \) is algebraically independent over \( L_{n-1} \), and
2. \( [L_n : L_{n-1}(b_n)] = [L_{n+1} : L_n(b_{n+1})] \).
Given a diagram

\[
\begin{array}{ccc}
  k & \rightarrow & B \\
  \sigma & \downarrow & \sigma \\
  C & \rightarrow & K
\end{array}
\]

of sub-\(k\)-algebras \(B, C\) of a difference field \((K, \sigma)\), we shall say that \(B\) is \(\sigma\)-linearly disjoint from \(C\) over \(k\) if whenever \(\{\beta_1, \ldots, \beta_r\} \subseteq B\) is linearly independent over \(k\), then \(\{\sigma(\beta_1), \ldots, \sigma(\beta_r)\}\) is linearly independent over \(C\). This is equivalent to the injectivity of the natural map \(B \otimes_k C \rightarrow \sigma(B)C\).

Using [1], we see that \(L_{n-1}(b_n)\) is \(\sigma\)-linearly disjoint from \(L_n\) over \(L_{n-1}\), and using [2] we deduce that \(L_n\) is \(\sigma\)-linearly disjoint from \(L_n(b_{n+1})\) over \(L_{n-1}(b_n)\). By transitivity of \(\sigma\)-linear disjointness, it follows from the diagram

\[
\cdots \rightarrow L_{n-1} \rightarrow L_{n-1}(b_n) \rightarrow L_n \rightarrow \cdots
\]

\[
\cdots \rightarrow L_n \rightarrow L_n(b_{n+1}) \rightarrow L_{n+1} \rightarrow \cdots
\]

that \(L_n\) is \(\sigma\)-linearly disjoint from \(L_n\) over \(L_{n-1}\) for all \(n \geq 1\).

Now, using generic flatness [16, Théorème 6.9.2], by \(\sigma\)-localising \(A\) (by an element of \(A_0\)) we may assume that \(\pi_{10} : A_0 \rightarrow A_1\) and \(\sigma_0 : A_0 \rightarrow A_1\) are flat (i.e., \(A_1\) is a flat \(A_0\)-module both via \(\pi_{10}\) and \(\sigma_0\)), so \(A_1 \otimes_{A_0} A_1\) is a flat \(A_0\) module. Thus the natural morphism

\[
(A_1 \otimes_{A_0} A_1) \rightarrow L_0 \otimes_{A_0} (A_1 \otimes_{A_0} A_1)
\]

is injective, the kernel in general being the \(A_0\)-torsion of \(A_1 \otimes_{A_0} A_1\), which we thoughtfully made trivial. Moreover, by linear disjointness guaranteed by the construction,

\[
L_0 \otimes_{A_0} (A_1 \otimes_{A_0} A_1) = (L_0 \otimes_{A_0} A_1) \otimes_{L_0} (L_0 \otimes_{A_0} A_1)
\]

\[
= L_0[A_1] \otimes_{L_0} L_0[A_1] \rightarrow L_0[A_1, \sigma(A_1)] = L_0[A_2]
\]

is injective. We conclude that \(A_1 \otimes_{A_0} A_1 \rightarrow A_2\) is injective and thus bijective by the construction, and that both \(\pi_{21} : A_1 \rightarrow A_2\) and \(\sigma_1 : A_1 \rightarrow A_2\) are flat. This is all we need to proceed by induction and prove that all

\[
A_n \otimes_{A_{n-1}} A_n \rightarrow A_n \otimes_{A_{n-1}} A_n \rightarrow A_{n+1}
\]

are isomorphisms. Note, if we are happy to finish with the associated morphisms being just closed immersions which are generically isomorphisms, we can skip the ‘generic flatness’ step and we do not need to localise \(A\) but only \(R\). □

**Definition 3.4.** Let \(P\) be a property of scheme morphisms of finite type. Consider the following permanence properties of \(P\):

1. (Composite). A composite of morphisms with property \(P\) has property \(P\).
2. (Base change). If \(X \rightarrow Y\) has \(P\), and \(Z \rightarrow Y\) is arbitrary, then \(X \times_Y Z \rightarrow Z\) has \(P\).
3. (Open embedding). If \(X \rightarrow Y\) has \(P\), and \(U \hookrightarrow X\), then \(U \rightarrow Y\) has \(P\).
4. (Genericity in the target). If \(f : X \rightarrow Y\) (with \(Y\) integral) is generically \(P\), there is a localisation \(Y'\) of \(Y\) such that \(f \mid f^{-1}(Y')\) is \(P\).
(4) (Genericity in the source). If \( f : X \to Y \) (with \( Y \) integral) is generically \( P \), there is a localisation \( X' \) of \( X \) and \( Y' \) of \( Y \) such that \( f \upharpoonright X' \cap f^{-1}(Y') \) is \( P \).

We say that \( P \) is hereditary if it has properties (1)–(3). It is hereditarily generic in the target (resp. source), if it is hereditary with property (4) (resp. (4')). The property \( P \) is strongly hereditary if in addition,

(5) (SH). If \( g \circ f \) and \( g \) have \( P \), then \( f \) has \( P \).

**Definition 3.5.**

(1) Let \((X, \sigma)\) be an \((R, \sigma)\)-difference scheme of finite \( \sigma \)-type. We say that \((X, \sigma)\) has the property \( \sigma \)-pro-\( P \), if there exists a prolongation sequence \( X_n \) as above for \( X \) such that all the structure maps \( X_n \to \text{Spec}(R) \) have the property \( P \).

(2) Let \( P \) be a property of scheme morphisms of finite type. Let \( f : (X, \sigma) \to (Y, \sigma) \) be a morphism of finite \( \sigma \)-type. We say that \( f \) has the property \( \sigma \)-pro-\( P \), if for every open affine \( V = \text{Spec}^\sigma(R) \) in \( Y \), the scheme \( f^{-1}(V) \) has the property \( \sigma \)-pro-\( P \).

(3) Let \( P \) be a property of morphisms of schemes of finite type. Let \( f : (X, \sigma) \to (Y, \sigma) \) be a morphism of schemes of finite \( \sigma \)-type (over a common base). We say that \( f \) has the property \( \sigma \)-pro-\( P \), if there exists a prolongation sequence \( f_n : X_n \to Y_n \) for \( f \) such that all the maps \( f_n \) have the property \( P \).

**Remark 3.6.** Suppose \( P \) is strongly hereditary.

(1) If \((X, \sigma)\) is \( \sigma \)-pro-\( P \), then all the connecting morphisms \( X_{n+1} \to X_n \) have the property \( P \).

(2) If a morphism \( f : (X, \sigma) \to (Y, \sigma) \) of schemes of finite \( \sigma \)-type (over some common base) is \( \sigma \)-pro-\( P \), and \((Y, \sigma)\) is \( \sigma \)-pro-\( P \), then \((X, \sigma)\) is \( \sigma \)-pro-\( P \).

**Proposition 3.7.**

(1) Let \( P \) be a property of scheme morphisms of finite type which is hereditarily generic in the source/target. Then the property \( \sigma \)-pro-\( P \) is \( \sigma \)-generic in the source. In other words, if \( f : (X, \sigma) \to (Y, \sigma) \) is a morphism of finite \( \sigma \)-type between transformally integral schemes which is generically \( \sigma \)-pro-\( P \), then there exists a \( \sigma \)-localisation \( X' \) of \( X \) and \( Y' \) of \( Y \) such that \( f \upharpoonright X' \) is \( \sigma \)-pro-\( P \) above \( Y' \), i.e., \( f \upharpoonright X' \cap f^{-1}(Y') \) is \( \sigma \)-pro-\( P \).

(2) The same statement applies when \( P \) is a (target/source) hereditarily generic property of morphisms of schemes of finite type and \( f : (X, \sigma) \to (Y, \sigma) \) is a morphism of transformally integral schemes of finite \( \sigma \)-type.

**Proof.** Let us prove (2), the proof of (1) being strictly easier. We shall assume the reader has constructed, upon a \( \sigma \)-localisation of the source, the relevant diagram of prolongations for \( f_n : X_n \to Y_n \) using the Preparation Lemma 3.3. In the case of genericity in the target, by using (G), modulo a \( \sigma \)-localisation of \( Y \) we can assume that \( X_0 \to Y_0 \) has \( P \). Using (G) and (O), by \( \sigma \)-localising \( X \) by an element of \( X_0 \) we can assume that \( X_1 \to X_0 \) also has \( P \).

In the case of genericity in the source, using (G), by a \( \sigma \)-localisation of \( X \) and \( Y \) we can assume that \( X_0 \to Y_0 \) has \( P \). Using (G) again, we need to \( \sigma \)-localise \( X \) further to make \( X_1 \to X_0 \) have the property \( P \). Using (O), the new \( X_0 \to Y_0 \) still has \( P \), but we lose the exact \( \sigma \)-generation in terms of fibre products to the extent that \( X_{n+1} \to X_n \times_{X_{n-1}} X_{n-1} \) are no longer isomorphisms for \( n \geq 1 \), but only open immersions.

We proceed by induction. Assuming that \( X_{n-1} \to Y_{n-1} \) and \( X_n \to X_{n-1} \) have \( P \), using (C), we get that \( X_n \to Y_n \) has \( P \). Moreover, using (BC), we obtain that

[4] (Genericity in the source). If \( f : X \to Y \) (with \( Y \) integral) is generically \( P \), there is a localisation \( X' \) of \( X \) and \( Y' \) of \( Y \) such that \( f \upharpoonright X' \cap f^{-1}(Y') \) is \( P \).
Lemma 3.14. \(X \times_{X_{n-1}} X_n \to X_n\) has \(P\). By (O) and the fact that \(X_{n+1} \hookrightarrow X_n \times_{X_{n-1}} X_n\) for \(n \geq 1\), we can deduce that \(X_{n+1} \to X_n\) also has \(P\), which keeps the induction going.

Let us note that, in case of a property strongly hereditarily generic in the target, if the preparation lemma could be improved so that we need only localise the base, then we could prove that \(\sigma\)-\(P\) is \(\sigma\)-generic in the target. \(\square\)

Corollary 3.8. Let \(f : (X, \sigma) \to (Y, \sigma)\) be a morphism of finite \(\sigma\)-type between transformally integral schemes.

1. If \(f\) is separable then there is a \(\sigma\)-localisation \(X'\) of \(X\) and \(Y'\) of \(Y\) such that \(f \mid X' \cap f^{-1}(Y')\) is \(\sigma\)-pro-smooth.
2. If \(f\) is separable algebraic, then there is a \(\sigma\)-localisation \(X'\) of \(X\) and \(Y'\) of \(Y\) such that \(f \mid X' \cap f^{-1}(Y')\) is \(\sigma\)-pro-\(\acute{e}\)tale.

Corollary 3.9. Let \((X, \sigma)\) be a transformally integral separable difference scheme of finite \(\sigma\)-type over \((R, \sigma)\). There is a \(\sigma\)-localisation \(X'\) of \(X\) and \(R'\) of \(R\) such that \(X'/R'\) is normal (in the sense of 3.27).

Proof. By Corollary 3.8 take a \(\sigma\)-localisation \(X'/R'\) which is \(\sigma\)-pro-smooth. \(\square\)

Definition 3.10. Given a difference polynomial ring \(P = R[\bar{x}]\Sigma\) over \((R, \varsigma)\), let us write \(P_1 = R[\bar{x}, \Sigma \bar{x}_1, \ldots, \Sigma \bar{x}_n] \subseteq P\). We shall say that an \((R, \varsigma)\)-algebra \((A, \Sigma)\) of finite \(\Sigma\)-type is directly presented if there exists an \((R, \varsigma)\)-epimorphism from some \(\Sigma\)-polynomial ring \(h : (P, \Sigma) \to (A, \Sigma)\) whose kernel \(I\) is \(\Sigma\)-generated by \(I \cap P_1\).

An affine difference scheme is directly presented over \((R, \varsigma)\) if it is the spectrum of a directly presented \((R, \varsigma)\)-algebra.

Remark 3.11. Let \(h : R[\bar{x}]_{\sigma} \to (A, \sigma)\) be a direct presentation of \((A, \sigma)\) over \((R, \varsigma)\). Let \(a = h(x)\) be an associated choice of \(\sigma\)-generators of \(A\), and let \(A_0\) be the projective system of Zariski closures constructed above. Then clearly \((A, \sigma)\) can be reconstructed from the morphisms \(A_0 \hookrightarrow A_1 \leftarrow A_0\). Similarly, \(X = \text{Spec}^\sigma(A)\) is ‘presented’ by the algebraic correspondence \(X_0 \leftarrow X_1 \to X_{0\varsigma}\) over \(R\). Conversely, for every closed immersion \(X_1 \to X_0 \times X_{0\varsigma}\) of \(R\)-schemes \(X_0, X_1\), Hrushovski [18] gives a construction of the associated directly presented difference scheme.

In [20], we consider directly presented difference schemes \((X, \Sigma)\) associated with a collection of algebraic correspondences \(X_0 \leftarrow X_1 \to X_{0\varsigma}\), for \(\sigma \in \Sigma\).

Definition 3.12. Let \((X, \Sigma)\) be a directly presented difference scheme over \((R, \varsigma)\) associated with algebraic correspondences \(X_0 \leftarrow X_1 \to X_{0\varsigma}\), for \(\sigma \in \Sigma\), and let \(P\) be a property of \(R\)-algebraic schemes. We say that \(X\) is directly \(P\), if \(X_0, X_1\) and \(X_{0\varsigma}\) have the property \(P\).

Definition 3.13. With notation of Definition 3.12, a difference scheme \((X, \Sigma)\) is said to be directly geometrically transformally integral if it is directly geometrically integral and \(\pi_1, \pi_2(\sigma)\) are dominant, for all \(\sigma \in \Sigma\).

Lemma 3.14. Let \(f : (Y, \sigma) \to (S, \varsigma)\) be a morphism of finite \(\sigma\)-type of transformally integral difference schemes whose generic fibre is geometrically transformally integral. Then there is a \(\sigma\)-localisation \(Y'\) of \(Y\) such that \(f \mid Y'\) has directly geometrically transformally integral fibres.
Proof. The Preparation Lemma \[3.3\] shows that, modulo a localisation, \(Y\) can be made directly presented over \(S\). Writing \(\eta\) for the generic point of \(S\), \(Y_\eta\) is assumed to be geometrically transformally integral, so \(Y_{0,\eta}, Y_{1,\eta}\) and \(Y_{0,\kappa,\eta} = Y_{0,\kappa,\eta}\) are geometrically integral and the relevant projections are all dominant. Using the constructibility of the property of being geometrically integral \([1\, \text{Tag 055G}]\), as well as the dominance of a morphism, we can \(\zeta\)-localise \(S\) to obtain that every fibre \(Y_s\) is directly transformally integral. \(\square\)

Lemma 3.15. Let \((X, \Sigma) \to (Y, \sigma)\) be an étale Galois cover of transformally integral difference schemes of finite transformal type over \((S, \zeta)\) such that the generic fibres of \(X\) and \(Y\) over \(S\) are geometrically transformally integral. Then there exist localisations \(X'\) of \(X\), \(Y'\) of \(Y\) and \(S'\) of \(S\) such that for every \(s \in S'\), the fibres \(X'_s\) and \(Y'_s\) are directly geometrically transformally integral and

\[
\text{Gal}(X'_s/Y'_s) = \text{Gal}(X'/Y').
\]

Proof. It is an exercise in dealing with constructible properties of algebraic schemes and correspondences to find an ad hoc proof of this claim. We offer a more conceptual proof, referring to the techniques of \[23\]. By a localisation, we may assume that \(X \to Y\) is a direct Galois cover whose direct Galois group equals \(\text{Gal}(X/Y)\). Using the assumption on the generic fibres, by a further localisation and \[3.14\] we can achieve that the fibres \(X_s\) and \(Y_s\) are directly geometrically transformally integral and then the direct Galois groups of \(X_s/Y_s\) and \(X/S\) obviously coincide. By the construction, the direct Galois groups are in fact Galois groups and we are done. \(\square\)

3.2. Local Properties. This subsection is mostly concerned with the question of whether it is reasonable to expect that if a property holds locally, at every point of a fixed point spectrum of a difference ring, then it also holds globally.

Definition 3.16. Let \((M, \sigma)\) be an \((A, \sigma)\)-module and let \((N, \sigma)\) be a submodule.

1. We say that \((M, \sigma)\) is well-mixed if \(am = 0\) implies \(\sigma(a)m = 0\) for all \(a \in A, m \in M\).

2. We say that \((N, \sigma)\) is a well-mixed submodule of \((M, \sigma)\) if the module \(M/N\) is well-mixed.

Clearly \((M, \sigma)\) is well-mixed if and only if the annihilator \(\text{Ann}(m)\) of any \(m \in M\) is a well-mixed \(\sigma\)-ideal in \((A, \sigma)\). Indeed, if \(ab \in \text{Ann}(m)\), then \(a(bm) = 0\) so \(\sigma(a)(bm) = (\sigma(a)b)m = 0\) and \(\sigma(a)b \in \text{Ann}(m)\).

Moreover, since the intersection of well-mixed submodules is well-mixed and \(M\) is trivially a well-mixed submodule of itself, for every submodule \((N, \sigma)\) of \((M, \sigma)\) there exists a smallest well-mixed submodule \([N]_w\) containing \(N\). Thus \([0]_w\) is the smallest well-mixed submodule of \((M, \sigma)\) associated with the largest well-mixed quotient \(M_w\) of \(M\).

Proposition 3.17. Let \((M, \sigma)\) be a well-mixed \((A, \sigma)\)-module. The following are equivalent.

1. \(M = 0\);
2. \(M_p = 0\) for every \(p \in \text{Spec}^\sigma(A)\);
3. \(M_p = 0\) for every \(p\) maximal in \(\text{Spec}^\sigma(A)\).
Proof: It is clear that (1) implies (2) and (2) implies (3). Suppose that (3) holds but \( M \neq 0 \). Let \( x \in M \setminus \{0\} \) and let \( a = \text{Ann}(x) \). Then \( a \neq (1) \) is well-mixed and, by [24, 2.21], \( V^\sigma(a) \neq \emptyset \). Choose a maximal \( p \) in \( V^\sigma(a) \). Since \( x/1 = 0 \) in \( M_p \), there exists an \( a \notin p \) such that \( ax = 0 \), which is in contradiction with \( \text{Ann}(x) \subseteq p \). □

Corollary 3.18. Let \((M,\sigma)\) be an \((A,\sigma)\)-module. If \( M_p = 0 \) for every \( p \in \text{Spec}^\sigma(A) \), then \( M_w = 0 \).

The above can be sharpened as follows.

Proposition 3.19. Let \((M,\sigma)\) be an \((A,\sigma)\)-module. If \((M_p)_w = 0 \) for every \( p \) maximal in \( \text{Spec}^\sigma(A) \), then \( M_w = 0 \).

Proof. Using the universal properties of localisation and passing to well-mixed quotients, as well as the fact that localisation is an exact functor, we construct a commutative diagram

\[
\begin{array}{ccc}
M & \xrightarrow{\psi} & M_p \\
\pi \downarrow & & \pi' \downarrow \\
M_w & \xrightarrow{\alpha} & (M_p)_w \\
\psi' \downarrow & \beta \downarrow & \\ \\
& & (M_w)_p
\end{array}
\]

in which \( \pi \) and \( \pi' \) are surjective, so we conclude that \( \pi_p \) and \( \beta \) are also surjective. Therefore, \((M_p)_w = 0\) implies that \((M_w)_p = 0\) and we finish by 3.17 □

Proposition 3.20. Let \( \phi : (M,\sigma) \to (N,\sigma) \) be an \((A,\sigma)\)-module homomorphism and assume that \((M,\sigma)\) is well-mixed. The following are equivalent.

1. \( \phi \) is injective;
2. \( \phi_p : M_p \to N_p \) is injective for every \( p \in \text{Spec}^\sigma(A) \).
3. \( \phi_p : M_p \to N_p \) is injective for every \( p \) maximal in \( \text{Spec}^\sigma(A) \).

Proof. \( (1) \Rightarrow (2) \). If \( 0 \to M \to N \) is exact, since localisation is exact, we get that \( 0 \to M_p \to N_p \) is also exact. \( (2) \Rightarrow (3) \) is trivial.

\( (3) \Rightarrow (1) \). Let \( M' = \ker \phi \). Then \( 0 \to M' \to M \to N \) is exact so \( 0 \to M'_p \to M_p \to N_p \) is exact for every \( p \in \text{Spec}^\sigma(A) \). By assumption, \( M'_p = 0 \) for every \( p \in \text{Spec}^\sigma(A) \). Since \( M' \) is well-mixed (as a submodule of \( M \) ), by 3.17 we conclude that \( M' = 0 \). □

We shall say that an \((A,\sigma)\)-module homomorphism \( \phi : (M,\sigma) \to (N,\sigma) \) is almost surjective, if \( [\text{im}(\phi)]_w = N \) (or, equivalently, if \( \text{coker}(\phi)_w = 0 \)).

Proposition 3.21. Let \( \phi : (M,\sigma) \to (N,\sigma) \) be an \((A,\sigma)\)-module homomorphism. If \( \phi_p : M_p \to N_p \) is almost surjective for every \( p \) maximal in \( \text{Spec}^\sigma(A) \), then \( \phi \) is almost surjective.

Proof. Let \( N' = \text{coker}(\phi) \). Then \( M \to N \to N' \to 0 \) is exact, and by localisation \( M_p \to N_p \to N'_p \to 0 \) is exact for every \( p \in \text{Spec}^\sigma(A) \). By assumption, \((N'_p)_w = 0\) for all \( p \) maximal in \( \text{Spec}^\sigma(A) \) and 3.19 implies that \( N'_w = 0 \). □
Lemma 3.22 ([10], 6.4). Let $M$ and $N$ be $A$-modules and suppose $N$ is generated by \( \{ n_i \} \). Then every element of $M \otimes_A N$ can be written as $\sum_i m_i \otimes n_i$ with finitely many nonzero $m_i$ and $\sum_i m_i \otimes n_i = 0$ in $M \otimes_A N$ if and only if there exist $m'_i \in M$ and $a_{ij} \in A$ such that for every $i$, 
\[
\sum_j a_{ij} m'_j = m_i
\]
and for every $j$, 
\[
\sum_i a_{ij} n_i = 0.
\]

Proposition 3.23. Let $(M, \sigma)$ and $(N, \sigma)$ be $(A, \sigma)$-modules with $(N, \sigma)$ well-mixed. Then $(M, \sigma) \otimes_{(A, \sigma)} (N, \sigma)$ is well-mixed.

Proof. Pick a set of generators $\{ n_i \}$ for $N$. Suppose $b \sum_i m_i \otimes n_i = 0$. Then $\sum_i m_i \otimes bn_i = 0$ so Lemma 3.22 implies the existence of $m'_i \in M$ and $a_{ij} \in A$ such that for every $i$, $\sum_j a_{ij} m'_j = m_i$ and for every $j$, $0 = \sum_i a_{ij} n_i = b \sum_i a_{ij} n_i$. Since the latter holds in $(N, \sigma)$ which is well-mixed, we get that $0 = \sigma(b) \sum_i a_{ij} n_i = \sum_i a_{ij} \sigma(b) n_i$. Using Lemma 3.22 again, it follows that $\sigma(b) \sum_i m_i \otimes n_i = \sum_i m_i \otimes \sigma(b) n_i = 0$. \qed

Proposition 3.24. Let $(M, \sigma)$ be a well-mixed $(A, \sigma)$-module. The following are equivalent.

1. $M$ is a flat $A$-module.
2. $M_p$ is a flat $A_p$-module for every $p \in \text{Spec}^\sigma(A)$.
3. $M_p$ is a flat $A_p$-module for every $p$ maximal in $\text{Spec}^\sigma(A)$.

Proof. (1) $\Rightarrow$ (2). Assuming (1), it is classically known that $M_p$ is a flat $A_p$ module for every prime $p$. (2) $\Rightarrow$ (3) is trivial.

(3) $\Rightarrow$ (1). Let $(N, \sigma) \rightarrow (P, \sigma)$ be injective. Then $N_p \rightarrow P_p$ is injective for every $p \in \text{Spec}^\sigma(A)$. By assumption, $N_p \otimes_{A_p} M_p \rightarrow P_p \otimes_{A_p} M_p$ is injective and thus $(N \otimes_A M)_p \rightarrow (P \otimes_A M)_p$ is injective for all $p$ maximal in $\text{Spec}^\sigma(A)$. Since $N \otimes_A M$ is well-mixed by Proposition 3.23 Proposition 3.20 implies that $N \otimes_A M \rightarrow P \otimes_A M$ is injective. \qed

Remark 3.25. Let $(A, \sigma) \rightarrow (B, \sigma)$ be a homomorphism of well-mixed difference rings such that $B$ is a flat $A$-module and denote by $A$ and $B$ the rings of global sections of $\text{Spec}^\sigma(A)$ and $\text{Spec}^\sigma(B)$. We can consider $B$ as an $A$-module via the morphism $A \rightarrow A \rightarrow B$ as in (2.8) and we can conclude that $B$ is flat over $A$. Indeed, $B$ is well-mixed, and we know that $\text{Spec}^\sigma(B) \simeq \text{Spec}^\sigma(B)$ and $B_p \simeq B_p$, which suffices to apply 3.24.

Proposition 3.26. Let $(A, \sigma)$ be a transformal domain. If $A_p$ is normal for every $p$ maximal in $\text{Spec}^\sigma(A)$, then $A$ is almost normal in the sense that there is a normal transformal domain $C$ with $[A]_w = C$.

Proof. Let $K$ be the fraction field of $A$, let $C$ be the integral closure of $A$ in $K$ and denote by $\phi : A \rightarrow C$ the inclusion. By assumption, each $\phi_p$ is surjective, so it implies that $\phi$ is almost surjective and thus $[A]_w = C$. \qed

Definition 3.27. A difference scheme $(X, \Sigma)$ is said to be normal if every local ring $\mathcal{O}_x$, for $x \in X$, is normal.
3.3. Étale morphisms of difference schemes.

**Definition 3.28.** A morphism \((R, \sigma) \to (S, \sigma)\) is formally smooth (resp. formally unramified, formally étale), if for every solid commutative diagram

\[
\begin{array}{ccc}
(S, \sigma) & \to & A/I \\
\downarrow & & \downarrow \\
(R, \sigma) & \to & (A, \sigma)
\end{array}
\]

with \(I\) a difference ideal satisfying \(I^2 = 0\), there exists at least one (resp. at most one, exactly one) dashed arrow making the diagram commutative.

Recall that a morphism of rings \(R \to S\) is defined to be formally smooth, formally unramified or formally étale by using exactly the same universal property in the category of commutative rings, omitting the difference structure.

**Lemma 3.29.** If \((R, \sigma) \to (S, \sigma)\) is formally smooth, then \(R \to S\) is formally smooth.

**Proof.** Let \((P, \sigma) \to (S, \sigma)\) be a surjective \((R, \sigma)\)-algebra morphism from a difference polynomial ring \(P\), and let \(J\) be the kernel, which is a difference ideal. Consider the above diagram for \(A = P/J^2\) and \(I\) generated by \(J\). By formal smoothness, we obtain a (difference) morphism \(S \to P/J^2\) which is a right inverse to the surjection \(P/J^2 \to S\), and thus \(R \to S\) is formally smooth using [1, 00TL]. \(\square\)

**Remark 3.30.** For a difference \((R, \sigma)\)-algebra \((S, \sigma)\), the module of relative differentials \(\Omega_{S/R}\) naturally classifies \(R\)-derivations that commute with \(\sigma\). Indeed, if we let \(J\) be the kernel of the multiplication map \(S \otimes_R S \to S\), it is known that \(\Omega_{S/R} \cong J/J^2\). However, in this context \(J\) is a difference ideal and \(J/J^2\) comes equipped with a natural difference structure, which entails in particular that the universal \(R\)-derivation \(d : S \to \Omega_{S/R}\) satisfies

\[d\sigma = \sigma d.\]

**Remark 3.31.** The above is in contrast with the various notions of smoothness developed in Giabicani’s thesis [15]. With clear intent to apply his theory to the case where \(\sigma\) is a power of the Frobenius automorphism, he postulates \(d\sigma = 0\). Another fundamental difference is that étale morphisms in our context as developed below are of relative total dimension 0, whereas in Giabicani’s context they are of relative transversal dimension 0.

**Remark 3.32.** If \((B, \sigma)\) is an \((A, \sigma)\)-algebra of finite \(\sigma\)-type, the second exact sequence for differentials implies that \(\Omega_{B/A}\) is a finitely \(\sigma\)-generated \((B, \sigma)\)-module.

**Lemma 3.33.** Given a difference morphism \((R, \sigma) \to (S, \sigma)\), the following statements are equivalent:

1. \((R, \sigma) \to (S, \sigma)\) is formally unramified;
2. \(R \to S\) is formally unramified;
3. \(\Omega_{S/R} = 0\).

**Proof.** In view of [3.30], since \(d\sigma = \sigma d\), the classical proof of the equivalence of [2] and [3] also works for the equivalence of [1] and [3]. \(\square\)
Corollary 3.34. Let \((R, \sigma) \to (S, \sigma)\) be a morphism. The following are equivalent:

1. \((R, \sigma) \to (S, \sigma)\) is almost formally unramified in the sense that 
\((\Omega_{S/R})_{\text{tr}} = 0\);
2. for every \(q \in \text{Spec}^{\sigma}(S)\) lying over \(p = q \cap R\), \((R_p, \sigma) \to (S_q, \sigma)\) is formally unramified;
3. for every \(q \in \text{Spec}^{\sigma}(S)\) lying over \(p = q \cap R\), \(R_p \to S_q\) is formally unramified.

Proof. Straightforward from \ref{3.19} applied to the \((S, \sigma)\)-module \(\Omega_{S/R}\). \hfill \Box

Corollary 3.35. A morphism \((R, \sigma) \to (S, \sigma)\) is formally étale if and only if \(R \to S\) is formally étale.

Proof. If \((R, \sigma) \to (S, \sigma)\) is formally étale, it is both formally smooth and formally unramified. By \ref{3.29}, \(R \to S\) is formally smooth, and by \ref{3.33} it is formally unramified, and therefore it is formally étale. The converse follows by a lengthy (although elementary) diagram chase, as noted in a discussion with M. Wibmer. \hfill \Box

Definition 3.36. A morphism \((R, \sigma) \to (S, \sigma)\) is smooth (resp. unramified, étale), if it is of finite \(\sigma\)-type and formally smooth (resp. formally unramified, formally étale).

Proposition 3.37. If \((R, \sigma) \to (S, \sigma)\) is \(\sigma\)-pro-étale, then \((R, \sigma) \to (S, \sigma)\) is étale.

Proof. Assuming that \((S, \sigma)\) is \(\sigma\)-pro-étale over \((R, \sigma)\), we can find a system of \(S_i\) directed by inclusions \(S_i \hookrightarrow S_{i+1}\) and homomorphisms \(\sigma_i : S_i \to S_{i+1}\) such that \((S, \sigma)\) is the direct limit of the \(S_i\) and the \(\sigma_i\), as in Subsection \ref{3.1} where \(R \to S_i\) are étale. Suppose we have a situation from \ref{3.28} and write \(\bar{A} = A/I\), \(\bar{\sigma} : \bar{A} \to \bar{A}\) for the endomorphism induced by \(\sigma : A \to A\), and denote the morphism \((S, \sigma) \to (\bar{A}, \bar{\sigma})\) by \(f\). We obtain the solid part of the diagram

\[
\begin{array}{ccc}
S_i & \xrightarrow{f_{i+1}} & A_{i+1} \\
\sigma_i & \downarrow & \sigma_{i+1} \\
S_{i+1} & \xrightarrow{\bar{f}_{i+1}} & \bar{A} \\
\sigma_{i+1} & \downarrow & \bar{\sigma} \\
A_{i+1} & \xrightarrow{\bar{\sigma}} & \bar{A} \\
\end{array}
\]

where \(f_i\) denotes the restriction of \(f\) to \(S_i\). The dashed arrows represent the unique lifts \(\bar{f}_i : S_i \to A_{i+1}\) of \(f_i\). Since both \(\bar{f}_{i+1} \sigma_i\) and \(\sigma \bar{f}_i\) are lifts of \(f_{i+1} \sigma_i = \sigma f_i\), by étaleness of \(R \to S_i\) we deduce that \(\bar{f}_{i+1} \sigma_i = \sigma \bar{f}_i\), which yields a unique lift \(\bar{f} : (S, \sigma) \to (A, \sigma)\) of \(f\) in the limit. \hfill \Box

Definition 3.38. A morphism \(f : (X, \Sigma) \to (Y, \sigma)\) is called smooth (resp. unramified, étale), if it is of finite transformal type and for every \(x \in X\) and every \(\tau \in \Sigma_x\), the morphism \((\mathcal{O}_{f(x)}, \sigma) \to (\mathcal{O}_x, \tau)\) is smooth (resp. unramified, étale).

Remark 3.39. A morphism \(f : (X, \Sigma) \to (Y, \sigma)\) of finite transformal type is unramified (resp. étale) if and only if for every \(x \in X\) there exists an (affine) open neighbourhood on which \(f\) is modelled by an unramified (resp. étale) morphism of difference rings. More precisely, if a morphism \((R, \sigma) \to (S, \sigma)\) is unramified (resp.
étale) at some \( q \in \text{Spec}^\sigma(S) \) lying over \( p = q \cap R \), then there is a \( g \notin q \) such that the \( \sigma \)-localisation \( (R, \sigma) \to (S_q, \sigma) \) is unramified (resp. étale).

The above ‘openness’ statement for the property of being unramified is obvious from \( \text{3.33} \) and \( \text{3.32} \). For étaleness, it follows from \( \text{3.32} \) and the Jacobian criterion for smoothness which states the following. Let \((A, \sigma)\) be a difference ring, \((B, \sigma)\) a formally smooth \((A, \sigma)\)-algebra, \( J \) a reflexive difference ideal of \( B \) and let \( C = B/J \). Then \((C, \sigma)\) is a formally smooth \((A, \sigma)\)-algebra if and only if the natural morphism of difference modules

\[
\delta : J/J^2 \to \Omega_{B/A} \otimes_B C
\]

is left-invertible. We omit the details of the proof since these results will not be used in the sequel. However, a generic étaleness result can be deduced by combining \( \text{3.8} \) with \( \text{3.37} \).

3.4. Étale Galois covers. In view of Babbitt’s decomposition discussed in the next section, many considerations reduce to a study of unramified or étale morphisms with stronger finiteness assumptions such as quasi-finiteness or finiteness, and we will make every effort to explicitly state them when possible.

Suppose \((G, \Sigma)\) acts on \((X, \Sigma)\). For \( x \in X \), the decomposition group at \( x \) is the stabiliser \( G_d(x) = G_x \) of \( x \). With the notation of \( \text{2.22} \) \((G_d(x), \Sigma_x)\) acts on \((k(x), \Sigma^x)\) and the inertia group \( G_i(x) \) at \( x \) is the set of elements of \( G_d(x) \) which act trivially on \( k(x) \).

If \((X, \Sigma) \to (Y, T)\) is a Galois cover with group \((G, \Sigma)\), and \((F, \varphi)\) is an algebraically closed difference field, we have that \( Y(F, \varphi) \simeq X(F, \varphi)/G \). Moreover, if \( x \) is the locus of \( \bar{x} \in X(F, \varphi) \), the stabiliser of \( \bar{x} \) in \( G \) is exactly the inertia group \( G_i(x) \).

**Proposition 3.40.** Suppose that \((X, \Sigma) \to (Y, T)\) is a Galois cover of difference schemes of finite transformal type over a difference field \((k, \sigma)\) with group \((G, \Sigma)\). If \( G_i(x) = (e) \) for all \( x \in X \), the natural projection \((X, \Sigma) \to (Y, T)\) is finite étale.

**Proof.** Since the assertion is local, we may assume that \( X \) is affine and that we are in the situation of \( \text{2.22} \). Suppose \( X = \text{Spec}^\Sigma\!(A) \) and that \((G, \Sigma)\) acts on \((A, \Sigma)\). By assumption, there is a finite tuple \( a \in A \) so that \( A = k[a]_\Sigma \). Writing \( \bar{a} = \{ ga : g \in G \} \), we have that \( A = k[\bar{a}]_\Sigma \) for any choice of \( \sigma \in \Sigma \). Then \( G \) acts on each \( A_n = k[\bar{a}, \sigma_1, \ldots, \sigma^n \bar{a}] \), and we can form \( B_n = A_n^G \). We have \( A = \lim \rightarrow_n A_n \) and \( B = A^G = \lim \rightarrow_n B_n \) and we have formed a projective limit of Galois covers \( p_n : X_n \to Y_n \) such that \( X \to Y \) is obtained by taking the \( \Sigma \)-fixed points of the ambient Galois cover \( \lim \rightarrow_n X_n \to \lim \rightarrow_n Y_n \). Let \( x \in X \) and write \( x_n \) for the projection of \( x \) in \( X_n \). Since \( G_i(x) = (e) \), we have that \( G_i(x_n) = (e) \) for all \( n \), so by the known result for Galois covers of locally Noetherian schemes it follows that \( p_n \) is étale at \( x_n \). By compatibility of formal étaleness with limits, we conclude that \( X \to Y \) is étale at \( x \).

**Corollary 3.41.** Suppose \((X, \Sigma)\) is integral and that \((G, \Sigma)\) acts faithfully. Then \( X \to X/G \) is étale if and only if all the inertia groups of points of \( X \) are trivial.

**Proof.** By the previous result, it suffices to show that if the quotient morphism is étale at \( x \in X \), then \( G_i(x) = (e) \). Take an \( x \in X \) with \( p : X \to X/G \) étale. We can easily reduce to the case where \( G_i(x) = G \) and \( k(x) = k(p(x)) \). Note, since \( X \) is integral and \( G \) is faithful on \( X \), then \( G \) is also faithful on \( \mathcal{O}_x \). However, the
classical proof works for the finite local étale extension $O_{p(x)} \to O_x$ and shows that $G = (e)$.

**Definition 3.42.** A difference scheme $(X, \Sigma)$ is faithful if $\Sigma$ acts faithfully on geometric points of $X$ in the sense that, for every geometric point $a \in X(F, \varphi)$, and $\sigma, \sigma' \in \Sigma$, the relation $\sigma a = \sigma' a$ implies $\sigma = \sigma'$.

**Corollary 3.43.** Suppose $(Y, T)$ is faithful, and that $p : (X, \Sigma) \to (Y, T)$ is an étale almost direct Galois cover of transformally integral difference schemes. Then $(X, \Sigma)$ is also faithful.

Thus, if $(X, \Sigma) \to (Y, \sigma)$ is an étale Galois cover of a strict difference scheme, then $(X, \Sigma)$ is automatically faithful. Since most generalised difference schemes that appear in the later sections will in fact be Galois covers of a strict difference scheme, we shall not need to discuss faithfulness outside this section.

When $(X, \Sigma)$ is faithful and $a \in X(F, \varphi)$ is a geometric point, we define the local $\varphi$-substitution $\varphi_a$ at $a$ as the unique element $\varphi_a \in \Sigma_x$ satisfying

$$\varphi_a a = a \varphi.$$  

In other words, if $a$ is localised at $x \in X$, then $\varphi_a$ is the element of $\Sigma_x$ corresponding (via the conclusion of Theorem 2.23) to the image $\varphi^a$ of $\varphi$ by the morphism of difference structure $(\varphi^a) : \{ \varphi \} \to \Sigma^a$. Note, when we have a Galois cover $\pi : (X, \Sigma) \to (Y, T)$ of faithful difference schemes with group $(G, \Sigma)$, and $\pi(a) = \pi(a') = b \in Y(F, \varphi)$, there exists a $g \in G$ with $a' = ga$ and

$$\varphi_a a = a \varphi = g^{-1} a' \varphi = g^{-1} \varphi_d a' = g^{-1} \varphi_d ga,$$

so we conclude that $\varphi_a$ and $\varphi_{a'}$ are $G$-conjugate. Therefore, the following definition is meaningful.

**Definition 3.44.** The local $\varphi$-substitution at $b$ is the $G$-conjugacy class $\varphi_b = \varphi_b^{X/Y}$ of any $\varphi_a$ with $\pi(a) = b$.

Alternatively, let $\pi(X, \Sigma) \to (Y, T)$ be an étale Galois cover, and fix a section $T \to \Sigma$ and a geometric point $b \in Y(F, \varphi)$. Writing $\hat{\sigma} \in \Sigma$ for the image of $\varphi^b \in \Sigma_b$, we define the twisted local $\varphi$-substitution at $a \in X(F, \varphi)$ with $\pi(a) = b$, to be the unique element $\hat{\varphi}_a \in G_a(x)$ with the property

$$\hat{\varphi}_a \hat{\sigma} a = a \varphi.$$

As explained above, for $\pi(a) = \pi(a') = b$, there is a $g \in G$ such that

$$\hat{\varphi}_a \hat{\sigma} = g^{-1} \hat{\varphi}_a' \hat{\sigma} g = g^{-1} \hat{\varphi}_a' \hat{\sigma} g \hat{\sigma},$$

so we can make the following definition.

**Definition 3.45.** The twisted $\varphi$-substitution $\hat{\varphi}_b$ at $b \in Y(F, \varphi)$ is the $\hat{\sigma}(\cdot)$-conjugacy class in $G$ of any $\hat{\varphi}_a$ with $\pi(a) = b$.

The previous two definitions are equivalent for an étale Galois cover of faithful difference schemes via the relation $\varphi_a = \hat{\varphi}_a \hat{\sigma}$.

In the special case when $F = \bar{k}$ is the algebraic closure of a finite field $k$ and $\varphi = \varphi_k$ is the Frobenius automorphism generating $\text{Gal}(\bar{k}/k)$, and $b \in Y(\bar{k}, \varphi_k)$ is a $(\bar{k}, \varphi_k)$-rational point, we obtain the local Frobenius substitution at $b$, denoted by $\varphi_{k,b}$ when considered as a conjugacy class in $\Sigma$, or $\hat{\varphi}_{k,b}$ when considered as a twisted conjugacy class in $G$. 
3.5. **Transformal separability.** The following definition generalises the notion of \( \sigma \)-separable extensions of difference fields from [18] and [9].

**Definition 3.46.** (1) An algebra \((A, \Sigma)\) over a difference field \((k, \sigma)\) is \(\Sigma\)-separable, if \((A, \Sigma) \otimes_{(k, \sigma)} (k', \sigma)\) is \(\Sigma\)-reduced/strong for every difference field extension \((k', \sigma)\) of \((k, \sigma)\).

(2) A morphism \((X, \Sigma) \rightarrow (Y, \sigma)\) of finite transformal type is **transformally separable**, if every fibre \(X_y\) is a finite union of difference spectra of transformally separable \((k(y), \sigma^{(y)})\)-algebras, for \(y \in Y\).

(3) A difference field extension \((L, \Sigma)\) of \((k, \sigma)\) is \(\tau\)-radicial (for \(\tau \in \Sigma\)), if for every \(\alpha \in L\), there exists a natural number \(n\) with \(\tau^n \alpha \in k\). It is \(\Sigma\)-radicial, if it is \(\tau\)-radicial for every \(\tau \in \Sigma\).

(4) A morphism \(f : (X, \sigma) \rightarrow (Y, \sigma)\) is \(\sigma\)-radicial if it is injective as a map of topological spaces, and for every \(x \in X\), the difference field extension \((k(f(x)), \sigma^{f(x)}) \rightarrow (k(x), \sigma^x)\) is transformally radicial.

**Proposition 3.47.** Any difference field extension \((k, \sigma) \rightarrow (L, \sigma)\) of finite \(\sigma\)-type factors as \((k, \sigma) \rightarrow (L_0, \sigma) \rightarrow (L, \sigma)\), where \(L_0\) is \(\sigma\)-separable over \(k\), and \(L\) is \(\sigma\)-radicial over \(L_0\).

**Proof.** A sub-extension \((E, \sigma)\) is \(\sigma\)-separable over \(k\) if and only if it is linearly disjoint from the inversive closure of \(k^{\text{inv}}\) over \(k\). By [15, 3.2.9], there is a natural number \(r\) such that \(L_0 = k\sigma^r(L)\) is linearly disjoint from \(k^{\text{inv}}\) over \(k\), i.e., such that \(L_0\) is \(\sigma\)-separable over \(k\).

**Remark 3.48.** A transformally radicial morphism \((X, \sigma) \rightarrow (Y, \sigma)\) induces an injection \(X(F, \varphi) \rightarrow Y(F, \varphi)\) for every difference field \((F, \varphi)\). If \((F, \varphi)\) is inversive, the induced map is bijective.

**Remark 3.49.** Let \((k, \sigma) \rightarrow (L, \Sigma)\) be a difference field extension with \(L/k\) Galois. In view of [2.21], \(L\) is \(\tau\)-separable (resp. \(\tau\)-radicial) over \(k\) for some \(\tau \in \Sigma\) if and only if \(L\) is \(\Sigma\)-separable (resp. \(\Sigma\)-radicial) over \(k\).

**Lemma 3.50.** Let \((k, \sigma) \rightarrow (L, \sigma)\) be a separable, \(\sigma\)-separable difference field extension, and let \(L_0\) be the relative algebraic closure of \(k\) in \(L\). Then \(L\) is regular \(\sigma\)-separable over \(L_0\).

**Proof.** By [4] Cor. 3, A.V.119], \(L/L_0\) is separable and therefore regular. Note, since \(L_0\) is algebraic over \(k\), we have that \(L_0^{\text{inv}}\) is algebraic over \(k^{\text{inv}}\). Hence, given that \(L\) is linearly disjoint from \(k^{\text{inv}}\), we deduce that \(L\) is free from \(L_0^{\text{inv}}\) over \(L_0\), so [4] Cor. 1, A.V.137] yields that \(L\) is linearly disjoint from \(L_0^{\text{inv}}\) over \(L_0\).

### 4. Bi-fibered structure of the category of difference schemes

**Definition 4.1** (Pullback). Let \((Y, T)\) be a difference scheme and let \(\psi : \Sigma \rightarrow T\) be a \(\text{Diff}\)-morphism. The **pullback** of \(Y\) with respect to \(\psi\) is defined as

\[
\psi^* Y = \cup_{\sigma \in \Sigma} Y^{\psi(\sigma)},
\]

with its induced structure as a \(\Sigma\)-difference scheme, with \(\sigma \in \Sigma\) acting as \(\psi(\sigma)\) on \(Y\). There is a natural morphism

\[
\psi^* Y \rightarrow Y.
\]
Definition 4.2. Let \((X_0, \Sigma_0)\) be a difference scheme and let \(\iota : \Sigma_0 \hookrightarrow \Sigma\) be an inclusion of almost-strict difference structures, i.e., \(\Sigma_0 = H\sigma, \Sigma = G\sigma\), and we have a homomorphism \(\tau() : G \to G\), so that \(H\) is a subgroup of \(G\) with \(\tau(H) = H\). Note that in this geometric situation, we have properties dual to those of 2.5(3), namely \(\sigma g = g\sigma\) and \((h\sigma)(g\sigma) = h\sigma(g h^{-1})\sigma\), for \(g, h \in G\).

For \(\sigma_i = g_i\sigma \in \Sigma, i = 0, 1, 2\), we introduce the notation \(\sigma^{\sigma_1, \sigma_2}_0 = g_1^{-1} g_0 \sigma g_2\sigma\).

Let \(g_i, i \in I\) be the representatives of \(G/H\), and \(\tau_i = g_i\sigma \in \Sigma\). For each \(\tau \in \Sigma\), and each \(\tau_i\), there is a unique \(\tau_{j}\) with \(\tau_{j}\tau_i \in \Sigma_0\). The assignment \(i \mapsto j\) defines a permutation \(\bar{\tau}\) of \(I\). Consider the space \(\coprod_{i \in I} X_i\), where each \(X_i\) is a copy of \(X_0\) (that should be thought of as \(g_i X_0\)) and \(\tau \in \Sigma\) takes \(X_i\) to \(X_{\bar{\tau}(i)}\), and acts as \(\tau^{\tau_i} \tau_{j} \in \Sigma_0\) on the associated copy of \(X_0\). In view of the fact that \(\bar{\tau}(i) = i\) if and only if \(\tau_{j}\tau_i = \tau_{\bar{\tau}(i)} \in \Sigma_0\), the underlying space of the (coproduct) pushforward is

\[
\iota_* X_0 = \bigcup_{\tau \in \Sigma} \left(\coprod_{i \in I} X_i\right)^{\tau} = \coprod_{i \in I} \bigcup_{\tau_{j} \in \Sigma_0} X_0^{\tau_{j}},
\]

and the action of \(\Sigma\) is inherited from \(\prod_{i \in I} X_i\).

There is a natural (inclusion) morphism 

\((X_0, \Sigma_0) \to (\iota_* X_0, \Sigma)\).

Definition 4.3. Let \((X_0, \Sigma_0)\) be a difference scheme and let \(\iota : \Sigma_0 \hookrightarrow \Sigma\) and \(I\) satisfy the assumptions of 4.2. Consider the space

\(\prod_{i \in I} X_i\),

where each \(X_i\) is a copy of \(X_0\) (that should be thought of as \(g_i X_0\)) and \(\tau \in \Sigma\) takes \(X_i\) to \(X_{\bar{\tau}(i)}\), and acts as \(\tau^{\tau_i} \tau_{j} \in \Sigma_0\) on the associated copy of \(X_0\). In view of the fact that \(\bar{\tau}(i) = i\) if and only if \(\tau_{j}\tau_i = \tau_{\bar{\tau}(i)} \in \Sigma_0\), the underlying space of the (product) pushforward is

\[
\iota! X_0 = \bigcup_{\tau \in \Sigma} \left(\prod_{i \in I} X_i\right)^{\tau} = \prod_{i \in I} \bigcup_{\tau_{j} \in \Sigma_0} X_0^{\tau_{j}},
\]

and the action of \(\Sigma\) is inherited from \(\prod_{i \in I} X_i\).

There is a natural morphism projecting onto the first factor

\(\iota^* \iota! X_0 \to X_0\).

Definitions 4.2 and 4.3 can also be made sense of in the context of full difference structures \(\Sigma\), recall 2.6.

Definition 4.4. Let \((X, \Sigma)\) be a difference scheme and let \(\pi : \Sigma \to T\) be a \(\text{Diff}\)-morphism such that there exists a finite group \(K\) acting faithfully on \(\Sigma\) such that \(\pi\) is in fact the canonical projection \(\Sigma \to \Sigma/K = T\). We define

\[
\pi_* (X, \Sigma) = (X, \Sigma)/K,
\]
considered as a $T$-difference scheme. There is an obvious quotient morphism

$$(X, \Sigma) \to (\pi_*X, T).$$

**Remark 4.5.** Let $\pi : \Sigma \to T$ be as in [4,4]. We shall not need the functor $\pi_!$ in the sequel, but we give an idea of its construction on an affine model. Let $(R, \Sigma)$ be a difference algebra over a difference field $(k, \varphi)$. Let

$$\pi!R = R_K = k \otimes_{k[K]} R$$

be the ring of $K$-coinvariants, with its natural $T$-action. Both natural morphisms $R \to k \otimes_{k[K]} R$ and $k \otimes_{k[K]} R \to R$ are used to prove the required adjunction below.

**Definition 4.6.** Let $(X, \Sigma)$ be a difference scheme and let $\psi : \Sigma \to T$ be a Diff-morphism which is a composite of Diff-morphisms satisfying the requirements of [4,2] or [4,4]. We define

$$\psi_*X = \psi_1 \cdots \psi_n X \quad \text{and} \quad \psi!X = \psi_1! \cdots \psi_n! X$$

and there are obvious natural morphisms

$$X \to \psi_*X \quad \text{and} \quad X \to \psi!X.$$

**Theorem 4.7.** Let $\psi : \Sigma \to T$ be a Diff-morphism as in [4,6].

1. The functor $\psi_*$ is left adjoint to $\psi^*$, i.e.,

$$\text{Hom}_\Sigma(X, \psi^*Y) \simeq \text{Hom}_T(\psi_*X, Y),$$

functorially in $(X, \Sigma)$ and $(Y, T)$.

2. The functor $\psi!$ is right adjoint to $\psi^*$, i.e.,

$$\text{Hom}_\Sigma(\psi^*Y, X) \simeq \text{Hom}_T(Y, \psi!X),$$

functorially in $(X, \Sigma)$ and $(Y, T)$.

**Proof.** (1) Suppose we have a difference scheme $(X, \Sigma)$ and $\iota : \Sigma_0 \to \Sigma$ satisfies the assumptions of [4,2]. Writing $(X_0, \Sigma_0) = \iota^*X$ and adopting the notation from loc. cit., there is a natural morphism $\iota_*\iota^*X \to X$, induced by the morphism $\prod_i X_i \to X$, taking the $i$-th copy of $X_0$ to $g_i(X_0)$. Since $\iota^*\iota^*Y$ is a disjoint union of copies of $(Y, \Sigma_0)$, an obvious morphism $(Y, \Sigma_0) \to \iota^*\iota^*Y$ is the inclusion onto the first copy. This makes it easy to verify that the resulting adjunctions

$$\iota_*\iota^* \to 1 \quad \text{and} \quad 1 \to \iota^*\iota_*$$

indeed satisfy the required unit-counit identities for the required adjunction to hold. When $\pi : \Sigma \to T$ satisfies the requirements of [4,4], $\pi_*\pi^*$ is an isomorphism and $1 \to \pi^*\pi_*$ is essentially the quotient morphism, so the unit-counit relations are easily verified.

(2) With the above notation, a natural morphism $X \to \iota_!\iota^*X$ is obtained as a restriction of the twisted diagonal embedding $X \to \prod_i X_i$, where the $X_i$ are copies of $X$ and the morphism is $x \mapsto (g_i(x))$. For $(Y, \Sigma_0)$, a natural morphism $\iota^*\iota_1Y \to Y$ is the projection on the first factor, $\iota^*\iota_1Y$ being a direct product of copies of $(Y, \Sigma)$. It is just a formality to verify that the resulting adjunctions

$$1 \to \iota_!\iota^* \quad \text{and} \quad \iota^*\iota_1 \to 1$$

are as required. 

\(\square\)
**Remark 4.8.** The construction from 4.3 can be adapted to a relative setting. In addition to the data from 4.3, suppose we have a difference scheme \((Y, \Sigma)\) and a morphism \(X_0 \to \iota^* Y\). We carry out an analogous construction on the fibre product of the \(X_i\) over \(Y\), where \(X_i = X_0 \times_Y Y\) as in the diagram
\[
\begin{array}{c}
X_i \longrightarrow Y \\
\downarrow \tau_i \\
X_0 \longrightarrow \iota^* Y \\
\end{array}
\]
which yields a difference scheme \((\iota_!(X_0/Y), \Sigma)\) satisfying
\[
\text{Hom}_{(Y, \Sigma)}(\iota^* Z, X_0) \cong \text{Hom}_{(Y, \Sigma)}(Z, \iota(X_0/Y)),
\]
for any difference scheme \((Z, \Sigma)\) over \((Y, \Sigma)\).

**Remark 4.9.** As hinted in [24, 2.10], the functor \((X, \Sigma) \mapsto \Sigma) makes the category of difference schemes into a (split) fibered category over \(\text{Diff}\).

In Grothendieck’s terminology from [17], the existence of left adjoints for the pullback functors makes the category of almost strict difference schemes into a (split) bi-fibered category over the category of almost strict difference structures. The author is uncertain on the nomenclature of (split) fibrations in which the pullback functors come with right adjoints as well.

### 5. Babbitt’s decomposition

#### 5.1. Non-abelian difference Galois cohomology.

**Definition 5.1.** Let \((G, \Sigma)\) be a difference group. Recall [2.17], for every \(\sigma \in \Sigma\) we have a group endomorphism (\(\cdot^\sigma : G \to G\) such that for every \(g \in G\) and \(\sigma, \tau \in \Sigma\),
\[
(g^\tau)^{\sigma^\tau} = (g^\sigma)^\tau.
\]

We let \(H^0(\Sigma, G) = G^\Sigma = \{g \in G : g^\sigma = g \text{ for all } \sigma \in \Sigma\}\). A cocycle is a map \(a : \Sigma \to G\) such that
\[
a(\sigma)^\tau = a(\tau)^{\sigma^\tau} a(\sigma^{\tau}) a(\tau)^{-1}.
\]

Two cycles \(a\) and \(b\) are cohomologous, if there exists a \(g \in G\) such that
\[
b(\sigma) = g^{\sigma} a(\sigma) g^{-1}.
\]

The cohomology set \(H^1(\Sigma, G)\) is the pointed set of equivalence classes of cocycles by the relation of being cohomologous, equipped with the distinguished class of the unit cocycle.

**Proposition 5.2.** Every short exact sequence of \(\text{Diff}\)-groups
\[
1 \to (H, \Sigma) \to (G, \Sigma) \to (\bar{G}, \Sigma) \to 1
\]
gives rise to a long exact cohomology sequence
\[
1 \to H^0(\Sigma, H) \to H^0(\Sigma, G) \to H^0(\Sigma, \bar{G}) \to \to H^1(\Sigma, H) \to H^1(\Sigma, G) \to H^1(\Sigma, \bar{G}).
\]

The proof consists of a number of lengthy but routine verifications similar to the proof of an analogous result in classical group/semigroup/rack cohomology.
Remark 5.3. In the case \( \Sigma = \{ \sigma \} \), \( H^1(\{ \sigma \}, G) \) is just the set of \( \{ \sigma \} \)-conjugacy classes in \( G \), so clearly the last arrow in 5.2 is surjective.

Let \((K, \Sigma_0) \rightarrow (L, \Sigma)\) be a separable quasi-Galois extension with a surjective structure morphism \( \pi : \Sigma \rightarrow \Sigma_0 \) and let \( G = \text{Gal}(L/K) \). The morphism \( \pi \) extends to the set \( \hat{\Sigma} \) consisting of all lifts of elements of \( \Sigma_0 \) to \( L \) by the rule \( \pi(\sigma) = \sigma \upharpoonright K \).

As in 2.21, for any \( \sigma, \tau \in \hat{\Sigma} \) such that \( \pi(\sigma) = \pi(\tau) \), there exists a (unique) \( g \in G \) with \( \tau = \sigma g \). For each \( \tau \in \Sigma \) this yields a homomorphism \((\tau) : G \rightarrow G\) such that \( g\tau = \tau g^\tau \),

which makes \( G \) into a \( \text{Diff} \)-group \((G, \Sigma)\).

Suppose now \((L, \Sigma')\) is another extension of \((K, \Sigma_0)\), with \( \Sigma' \subseteq \hat{\Sigma} \) and let \( \iota : \Sigma \rightarrow \Sigma' \) be a surjective \( \text{Diff} \)-morphism with the property \( \pi \iota = \pi \). It is easily verified that maps \( a : \Sigma \rightarrow G \) satisfying

\[
\iota(\sigma) = \sigma a(\sigma)
\]
correspond to cocycles, and that cocycles \( a_1, a_2 \) corresponding to isomorphic extensions \((L, \Sigma_1), (L, \Sigma_2)\) of \((K, \Sigma_0)\) are cohomologous. We draw the following conclusion.

Remark 5.4. The cohomology set \( H^1(\Sigma, \text{Gal}(L/K)) \) classifies the above family of difference field extensions of \((K, \Sigma_0)\) up to isomorphism.

5.2. Benign extensions and Babbitt’s theorem.

**Definition 5.5.** A morphism \((S, \sigma) \rightarrow (R, \sigma)\) of difference rings is called **benign** if there exists a quasifinite \( S \rightarrow R_0 \) such that \((R, \sigma)\) is isomorphic to \([\sigma]_S R_0\) over \((S, \sigma)\). In other words, writing \( R_{i+1} = R_i \otimes_S S \) for \( i \geq 0 \) (where the morphism \( S \rightarrow S \) is \( \sigma \)), \((R, \sigma)\) is the (limit) tensor product of the \( R_i \) and the canonical morphisms \( \sigma_i : R_i \rightarrow R_{i+1} \) over \( S \). The morphism is **proper benign** if, additionally, \( R \) is (algebraically) integral over \( S \).

In the **benign Galois** case, \( R_0 \) is Galois over \( S \) with group \( G_0 \) and the Galois group \( \text{Gal}(R/S) = \text{Gal}(k(R)/k(S)) = (G, (\sigma)^\circ) \) is isomorphic to the direct product of \( G_i = \text{Gal}(R_i/S) \) and \((\sigma)^\circ \) ‘shifts’ from \( G_i \) to \( G_{i+1} \).

In view of such a specific form of \( G \), we get that for any \( h, h' \in G \) there is a \( g \in G \) such that \( h' = g^\sigma hg^{-1} \), i.e., \( h \) and \( h' \) are \((\sigma)^\circ\)-conjugate, proving the following.

**Lemma 5.7.** The (non-abelian) difference cohomology \( H^1(\{ \sigma \}, G) = 1 \).

**Lemma 5.8.** If \( R \) is proper benign over \( S \), then for any \( y \in \text{Spec}^\sigma(S) \), any algebraically closed difference field \((F, \varphi)\) extending \((k(y), (\sigma)^\circ)\), any \( \bar{y} \in (S, \sigma)(F, \varphi) \) above \( y \) and any \( g \in G \), there exists an \( \bar{x} \in (R, g\sigma)(F, \varphi) \) lifting \( \bar{y} \).

**Proof.** By 5.4, all \((R, g\sigma), g \in G \) are isomorphic over \((S, \sigma)\), so it suffices to treat the case of \((R, \sigma)\).

Let \( R_i \) be as in 5.3. By the integrality assumption, all the \( R_i \) are finite over \( S \).

Let \( \bar{y} : (S, \sigma) \rightarrow (F, \varphi) \). Since \( R_0 \) is finite over \( S \) and \( F \) is algebraically closed, we can find some \( \bar{x}_0 : R_0 \rightarrow F \) above \( \bar{y} \). By the universal property 3.1 of \( \bar{R} = [\sigma]_S R_0 \), there exists an \( \bar{x} : (R, \sigma) \rightarrow (F, \sigma) \) extending \( \bar{x}_0 \) and consequently \( \bar{y} \).

\( \square \)
Lemma 5.9. Let \((\tau \in \text{alent})\) two difference schemes (Definition 5.10. \(\bar{\Sigma}\)).

(1) A morphism \((\psi, (\psi^0)) : (S, T) \to (R, \Sigma)\) of almost-strict difference rings is ben\(\text{i\,n}\) if for some (or equivalently, for all) \(\sigma \in \Sigma\), the morphism \((S, \sigma^0) \to (R, \sigma)\) is ben\(\text{i\,n}\).

(2) A morphism \((X, \Sigma) \to (Y, T)\) of almost-strict difference schemes is ben\(\text{i\,n}\) if it is affine and above each open affine subset of \(Y\) it is modelled by a fixed-point spectrum of a ben\(\text{i\,n}\) morphism of rings.

(3) In the situation of [2], the morphism is proper ben\(\text{i\,n}\), if the relevant difference ring extensions are proper ben\(\text{i\,n}\).

An immediate consequence of 5.1 is the following.

Lemma 5.9. Let \((X, \Sigma) \to (Y, T)\) be a proper ben\(\text{i\,n}\) Galois morphism. For any \(\tau \in T\) and \(\sigma \in \Sigma\) mapping to \(\tau\), any \(y \in Y^\tau\), any algebraically closed difference field \((F, \varphi)\) extending \((k(y), \tau^0)\), any \(\bar{y} \in Y^\tau(F, \varphi)\) above \(y\), there exists an \(\bar{x} \in X^\sigma(F, \varphi)\) lifting \(\bar{y}\).

Definition 5.10. Two difference schemes \((X_1, \Sigma_1)\) and \((X_2, \Sigma_2)\) are called equivalent, written \((X_1, \Sigma_1) \simeq (X_2, \Sigma_2)\), if they have isomorphic inversive closures, \((X_1^{\text{inv}}, \Sigma_1^{\text{inv}}) \simeq (X_2^{\text{inv}}, \Sigma_2^{\text{inv}})\).

The following is a slight refinement of a fundamental theorem from [3], showing how to use it for not necessarily inversive difference fields.

Lemma 5.11 (Babbitt’s Theorem). Let \((K, \sigma) \to (L, \sigma)\) be a separable \(\sigma\)-separable quasi-Galois extension of finite \(\sigma\)-type. Then we have a tower

\[
(K, \sigma) \to (L_0, \sigma) \to (L_1, \sigma) \to \cdots \to (L_n, \sigma) \simeq (L, \sigma)
\]

of difference field extensions with \(L_0/K\) finite and all \(L_{i+1}/L_i\) ben\(\text{i\,n}\) for \(i \geq 0\).

Proof. Let us remark that, if \(F/K\) is \(\sigma\)-separable, and \(F^{\text{inv}} = K^{\text{inv}}(a)_{\sigma}\) for some \(a = a_1, \ldots, a_n\), then there is an \(r \geq 0\) such that \(F = K(a^{\sigma r})_{\sigma}\).

The original theorem from [3] gives that, writing \(\hat{L} = K^{\text{inv}}L\), and \(L_0\) for the core of \(K^{\text{inv}}\) in \(\hat{L}\), there exist \(u_1, \ldots, u_n \in \hat{L}\) such that \(\hat{L} \simeq \hat{L}_0(u_1, \ldots, u_n)_{\sigma}\) and for every \(0 \leq i \leq n - 1\), \(L_0(u_1, \ldots, u_{i+1})_{\sigma}\) is a ben\(\text{i\,n}\) extension of \(L_0(u_1, \ldots, u_i)_{\sigma}\) with normal minimal generator \(u_{i+1}\).

It is known that \(L_0\) is inversive, so using the above remark for \(F = \hat{L}_0\), we deduce that \(\hat{L}_0 = L_K\), the core of \(K\) in \(L\). Bearing in mind that \(L \simeq \hat{L}\), we produce the required decomposition.

Babbitt’s theorem on algebraic extensions of difference fields has the following consequence in our terminology, providing a deep structure theorem.

Theorem 5.12 (Babbitt’s decomposition). Any generically étale quasi-Galois \(\sigma\)-separable morphism of finite transformally affine integral normal affine almost-strict difference schemes factorizes as

\[
(X, \Sigma) \simeq (X_n, \Sigma_n) \to \cdots \to (X_1, \Sigma_1) \to (X_0, \Sigma_0) \to (Y, T),
\]

where \((X_0, \Sigma_0) \to (Y, T)\) is generically finite étale quasi-Galois and for \(i \geq 0\), \((X_{i+1}, \Sigma_{i+1}) \to (X_i, \Sigma_i)\) is ben\(\text{i\,n}\) Galois. Modulo a transformally localisation of \(Y\), we can achieve that \((X_0, \Sigma_0) \to (Y, T)\) is finite étale quasi-Galois, and that \(X_{i+1} \to X_i\) are étale proper ben\(\text{i\,n}\) Galois.
Proof. By applying Babbitt’s theorem 5.11 to the extension of difference function fields \((k(Y),\tau) \to (k(X),\sigma)\) for a suitable choice of \(\sigma\) and \(\tau\) we obtain a tower of difference field extensions

\[(k(Y),\tau) \to (L_0,\sigma) \to (L_1,\sigma) \cdots \to (L_n,\sigma) \simeq (k(X),\sigma),\]

where \(L_0/k(Y)\) is finite and each \((L_{i+1},\sigma)/(L_i,\sigma)\) is benign for \(i \geq 0\). We let \(\Sigma_i\) be the \(\text{Diff}\)-structure obtained as a restriction of \(\Sigma\) from \(L_n\) to \(L_i\). Let \((X_i,\Sigma_i)\) be the normalisation of \((Y,T)\) in \((L_i,\Sigma_i)\). It is clear from [21, 2.5] that by a transformal localisation we can achieve that \(X_0 \to Y\) is finite étale and it remains to show that each \(X_{i+1} \to X_i\) can be made étale benign, which is granted by the following lemma.

\[\square\]

Lemma 5.13. Let \((R,\sigma)\) be a normal transformal domain with fraction field \((K,\sigma)\) and let \((K,\sigma) \to (L,\sigma)\) be a benign extension of difference fields such that \(L\) is the composite of the linearly disjoint subfields \(L_i = \sigma^i(0)\) where \(L_0\) is a fraction field of an étale \(R\)-algebra \(A_0\). Then the normalisation of \(R\) in \(L\) is the (limit) tensor product of the \(A_{0\sigma^i}\) over \(R\) and thus benign over \(R\).

Proof. Since \(A_0\) is étale over \(R\) so is any \(A_{0\sigma^i}\), and any tensor product of those is therefore \(R\)-torsion-free and the conclusion follows from linear disjointness in the spirit of the proof of 3.3. \[\square\]

5.3. Galois closure.

Lemma 5.14. Let \((K,\sigma) \to (L,\sigma) \to (F,\tilde{\sigma})\) be a tower of difference field extensions with \(L/K\) algebraic, and suppose that the quasi-Galois (normal) closure \(\tilde{L}\) of \(L\) over \(K\) is contained in \(F\). Then \(\tilde{\sigma}(\tilde{L}) \subseteq \tilde{L}\) and \((\tilde{L},\tilde{\sigma})\) is a difference field extension of \((L,\sigma)\), where \(\tilde{\sigma} = \tilde{\sigma} \mid _{\tilde{L}}\).

Proof. If \(\alpha \in \tilde{L}\), then it is a conjugate of some \(\alpha_0 \in L\). In other words, the minimal polynomial \(f \in K[t]\) of \(\alpha_0\) over \(K\) splits as \(f(t) = (t - \alpha_0)(t - \alpha_1) \cdots (t - \alpha_n)\), for \(\alpha_i \in \tilde{L}\), and \(\alpha\) is one of the \(\alpha_i\). Then \(f^{\sigma}(t) = (t - \sigma\alpha_0)(t - \tilde{\sigma}\alpha_1) \cdots (t - \tilde{\sigma}\alpha_n)\) is the minimal polynomial of \(\sigma\alpha_0\), which is again in \(L\), so \(\alpha_i\) are its conjugates and therefore they lie in \(L\).

\[\square\]

Remark 5.15. Cohn remarks in [7, Chapter 7, no. 16] that the algebraic closure \(\tilde{L}\) of \(L\) can always be equipped with an endomorphism \(\tilde{\sigma}\) so that \((\tilde{L},\tilde{\sigma})\) extends \((L,\sigma)\). Thus (considering \((\tilde{L},\tilde{\sigma})\) in the role of \((F,\tilde{\sigma})\) above), the quasi-Galois closure \(\tilde{L}\) can always be made (non-canonically) into a difference field extension of \((L,\sigma)\).

Definition 5.16. Suppose \((L,\sigma)\) is a separable extension of \((K,\sigma)\), and let \((\tilde{L},\tilde{\sigma})\) be a choice of a difference structure on the quasi-Galois closure of \(L\) over \(K\). The diagram

\[
\begin{array}{ccc}
(L,\sigma) & \xrightarrow{\ell^*} & (\tilde{L},\tilde{\sigma}) \\
\downarrow & & \downarrow \\
(K,\sigma) & \xrightarrow{\ell^*} & (\tilde{L},\tilde{\sigma})
\end{array}
\]

is called the Galois closure of \((L,\sigma)\) over \((K,\sigma)\), where \(\Sigma\) is the set of all lifts of \(\sigma\) from \(K\) to \(\tilde{L}\), and \(\tilde{\Sigma} \subseteq \Sigma\) is the set of all lifts of \(\sigma\) from \(L\) to \(\tilde{L}\). In fact, \(\Sigma = \tilde{\sigma}\text{Gal}(\tilde{L}/K)\), and \(\tilde{\Sigma} = \tilde{\sigma}\text{Gal}(\tilde{L}/L)\).
Proposition 5.17 (The universal property of Galois closure). Let \((L, \sigma)\) be a separable extension of \((K, \sigma)\), and suppose \((F, \Sigma_F)\) is Galois over \((K, \sigma)\) such that there is a \(\tilde{\sigma} \in \Sigma_F\) with \((F, \tilde{\sigma})\) extending \((L, \sigma)\). Then there are extensions \((\tilde{L}, \tilde{\Sigma}) \to (F, \Sigma_F)\) and \((\hat{L}, \hat{\Sigma}) \to (F, \Sigma_F)\), where \(\tilde{\Sigma} = \{\tau \in \Sigma_F : \tau \mid_L = \sigma\}\).

Proof. By the universal property of (algebraic) Galois closure, \(\tilde{L} \subseteq F\) and \(F/\tilde{L}\) is Galois. Let \(\bar{\sigma} \in \Sigma_F\) be an endomorphism such that \(\bar{\sigma} \mid_L = \sigma\). By 5.14, \(\tilde{\sigma} = \bar{\sigma} \mid_{\tilde{L}} \in \tilde{\Sigma}\), and we know that \(\Sigma = \tilde{\sigma} \text{Gal}(\tilde{L}/K), \Sigma_F = \bar{\sigma} \text{Gal}(F/K)\) and that

\[
1 \to \text{Gal}(F/\tilde{L}) \to \text{Gal}(F/K) \to \text{Gal}(\tilde{L}/K) \to 1
\]
is exact, so the restriction map \(\Sigma_F \to \Sigma\) is onto, giving the inclusion \((\tilde{L}, \tilde{\Sigma}) \to (F, \Sigma_F)\). Similarly we get the inclusion \((\hat{L}, \hat{\Sigma}) \to (F, \hat{\Sigma})\). \(\square\)

Definition 5.18. Let \((X, \sigma) \to (Y, \sigma)\) be a generically étale \(\sigma\)-separable finite morphism of transformally integral normal difference schemes, and denote by \((K, \sigma) \to (L, \sigma)\) the corresponding extension of function fields, let \((\tilde{L}, \tilde{\Sigma})\) and \(\hat{\Sigma}\) be as in 5.16 (\(\Sigma\) is finite in this case), and write \(\iota : \hat{\Sigma} \hookrightarrow \Sigma\). Let \((\hat{X}, \hat{\Sigma})\) be the normalisation of \(Y\) in \((\tilde{L}, \tilde{\Sigma})\), and let \(\hat{X} = \iota^* X\). The Galois closure of \(X\) over \(Y\) is the resulting diagram

\[
\begin{array}{ccc}
\hat{X} & \to & \hat{X} \\
\downarrow & & \downarrow \\
X & \to & Y
\end{array}
\]
in which the vertical arrows are Galois covers.

5.4. Ampleness of finite difference structures. A geometric motivation for the study of generalised difference geometry was the quest for a framework that gives rise to a suitable notion of a Galois cover. Intuitively, a morphism \((K, \sigma) \to (L, \sigma)\) of difference fields with \(K \to L\) Galois is not a Galois extension in the category of difference rings. Instead, one should consider the extension \((K, \sigma) \to (L, \hat{\Sigma})\) where \(\hat{\Sigma}\) is the set of all lifts of \(\sigma\) to \(L\). Even in the common case where \(L\) is algebraic of finite \(\sigma\)-type over \(K\), this typically involves a consideration of a profinite structure \(\hat{\Sigma}\). This certainly works, but falls beyond the scope of the present paper.

The aim of the following string of results is to show that, for most purposes in difference algebraic geometry, it suffices to consider difference rings and fields (and schemes) with finite difference structures.

Lemma 5.19. Let \((L_0, \sigma) \to (L, \sigma)\) be a coreless extension of an inversive difference field \(L_0\) (i.e., the core of \(L_0\) in \(L\) is \(L_0\)). Then

\[
H^1((\sigma)^*, \text{Gal}(L/L_0)) = 1.
\]

Proof. Using Babbitt’s decomposition, let

\[
(L_0, \sigma) \to (L_1, \sigma) \cdots \to (L_n, \sigma) \simeq (L, \sigma),
\]

be a tower of benign difference field extensions. By 5.6, \(H^1((\sigma)^*, \text{Gal}(L_{i+1}/L_i)) = 1\) for all \(i \geq 0\). It is straightforward now to prove that \(H^1((\sigma)^*, \text{Gal}(L_{i}/L_0)) = 1\) by
induction, using the long exact sequence for difference cohomology associated with the short exact sequence

$$1 \to \text{Gal}(L_{i+1}/L_i) \to \text{Gal}(L_{i+1}/L_0) \to \text{Gal}(L_i/L_0).$$

In particular, we have that $H^1((\sigma)^r, \text{Gal}(L_n/L_0)) = 1$. By analogous considerations, we obtain $H^1((\sigma)^r, \text{Gal}(L_n^{\text{inv}}/L_0)) = 1$.

If $g \in \text{Gal}(L^{\text{inv}}/L)^\sigma$, then also $g^{\sigma^r} = g$ for every $r$. For $x \in L^{\text{inv}}$, choose $r$ so that $\sigma^r(x) \in L$, and then $g^{\sigma^r}x = \sigma^r x$, so $g(x) = g^{\sigma^r}(x) = x$, and thus $g$ is the identity. We conclude that $\text{Gal}(L^{\text{inv}}/L)^\sigma = 1$.

Using the fact that $L^{\text{inv}} = L_n^{\text{inv}}$, the cohomology long exact sequence (extended by \[.3\] associated with $L$, $H$ becomes

$$1 \to \text{Gal}(L^{\text{inv}}/L) \to \text{Gal}(L^{\text{inv}}/L_0) \to \text{Gal}(L/L_0) \to 1$$

becomes

$$1 \to 1 \to \text{Gal}(L^{\text{inv}}/L_0)^\sigma \to \text{Gal}(L/L_0)^\sigma \to H^1((\sigma)^r, L^{\text{inv}}/L) \to 1 \to H^1((\sigma)^r, L/L_0) \to 1,$$

whence we conclude that $H^1((\sigma)^r, L/L_0) = 1$, and, since $\text{Gal}(L/L_0)^\sigma$ is finite as a $\sigma$-Galois group of an algebraic extension of finite $\sigma$-type, that all the remaining terms are finite.

**Lemma 5.20.** Let $(K, \sigma) \to (L, \tilde{\sigma})$ be a separable $\sigma$-separable quasi-Galois extension of finite $\tilde{\sigma}$-type. Let $L_0 = L_K$ be the core of $K$ in $L$. The exact sequence

$$1 \to \text{Gal}(L/L_0) \to \text{Gal}(L/K) \to \text{Gal}(L_0/K) \to 1$$

is nearly split in the sense that there exists a finite $(\sigma)$-invariant subgroup $G_1$ of $\text{Gal}(L/K)$ which maps onto $\text{Gal}(L_0/K)$.

Moreover, the set of isomorphism classes of all lifts of $\sigma$ from $K$ to $L$ is in one-to-one correspondence with the set of isomorphism classes of lifts of $\sigma$ from $K$ to $L_0$ and $G_1$ can be chosen so that $\sigma G_1$ contains a set of representatives for those isomorphism classes.

**Proof.** The assumption that $L$ is $\sigma$-separable allows us to assume that $K$ is inversive, and then $L_0$ is inversive by \[.7\] Chapter 7, no. 15. Let us introduce the shorthand notation $H = \text{Gal}(L_1/L_0)$, $G = \text{Gal}(L_1/K)$, $G_0 = \text{Gal}(L_0/K)$, and let us denote by $\Phi$ the operator $(\sigma)^n : G \to G$, where $n$ is the order of $(\sigma)$ on $G_0$.

Using \[.19\] we get that $H^1((\sigma)^r, H) = 1$ and $H^1(\Phi, H) = 1$ so the long exact sequences (from \[.3\] for (non-abelian) difference cohomology become

(1) $$1 \to H^\sigma \to G^\sigma \to G_0^\sigma \to 1 \to H^1((\sigma)^r, G) \to H^1((\sigma)^r, G_0) \to 1$$

and

(2) $$1 \to H^\Phi \to G^\Phi \to G_0 \to 1 \to H^1(\Phi, G) \to H^1(\Phi, G_0).$$

Since $H^\Phi$ is finite, \[.2\] implies that $G^\Phi$ is a finite subgroup of $G$ that maps onto $G_0$. But \[.1\] shows that $H^1((\sigma)^r, G) \cong H^1((\sigma)^r, G_0)$ and thus $G^\Phi$ also maps onto $H^1((\sigma)^r, G)$, which proves the ‘moreover’ clause by \[.4\] \hfill □
**Definition 5.21.** Let \((K, T) \to (F, \Sigma)\) be an extension of difference fields with finite structures \(T\) and \(\Sigma\), and let \((L, \Sigma)\) be the relative algebraic closure of \(K\) in \(F\). We say that an extension \((K, T) \to (F, \Sigma)\) is a weak difference cover if \(L/K\) is Galois and \(\Sigma\) contains a (finite) set of representatives of the isomorphism classes of lifts of all \(\tau \in T\) to \(L\).

**Definition 5.22.** Let \((K, \sigma) \to (L, \sigma)\) be a separable algebraic \(\sigma\)-separable extension of difference fields of finite \(\sigma\)-type. Let \((\tilde{L}, \Sigma)\) be the Galois closure of \((L, \sigma)\) over \((K, \sigma)\) as in 5.16. Note that \(\Sigma\) will often be infinite. We use 5.20 to find \((\tilde{L}, \Sigma_0)\) where the finite \(\Sigma_0 \subseteq \Sigma\) represents all lifts of \(\sigma\) from \(K\) to \(\tilde{L}\), and we let \(\iota : \Sigma_0 \to \Sigma\) be the data associated with the quasi-Galois closure \(\iota^* \tilde{X}\) of \(\tilde{Y}\) over \(Y\). We obtain a diagram

\[
\begin{align*}
\iota^* \tilde{X} & \longrightarrow \tilde{X} \\
X & \longrightarrow Y
\end{align*}
\]

in which the vertical arrows are weak generic covers, called the (generic) weak Galois closure of \(X\) over \(Y\).

**Proposition 5.25.** Let \((X, \sigma) \to (Y, \sigma)\) be a generically dominant generically smooth morphism of integral normal almost strict difference schemes. Then it can be subsumed in a generic weak cover in the sense that there exists a diagram

\[
\begin{align*}
X_0 & \longrightarrow \tilde{X} \\
X & \longrightarrow Y
\end{align*}
\]

where \((X_0, \Sigma_0) \to (X, \sigma)\) and \((\tilde{X}, \Sigma) \to (Y, \sigma)\) are generic weak covers.

**Proof.** Let \((L, \sigma)\) be the relative algebraic closure of \(k(Y)\) inside \(k(X)\), and let \(\tilde{Y}\) be the normalisation of \(Y\) in \(L\). As in 5.24, let \((\tilde{Y}, \Sigma), \iota : \Sigma_0 \to \Sigma\) be the data associated with the quasi-Galois closure \(\iota^* Y\) of \(\tilde{Y}\) over \(Y\), and let \((X_0, \Sigma_0) = \)
The diagram obtained using [4.8]

\[
\begin{array}{c}
X \\ \downarrow \\ Y
\end{array}
\quad \xrightarrow{\sigma} \quad
\begin{array}{c}
X_0 \\ \uparrow \\ \downarrow
\end{array}
\quad \xrightarrow{\iota(X_0/Y)}
\quad
\begin{array}{c}
\iota^*Y \\ \downarrow
\end{array}
\quad \xrightarrow{\sigma} \quad
\begin{array}{c}
\tilde{Y} \\ \downarrow
\end{array}
\quad \xrightarrow{\sigma} \quad
\begin{array}{c}
Y
\end{array}
\]

shows the required statement with \( \tilde{X} = \iota(X_0/Y) \) in a very explicit way. \( \square \)

6. Effective difference algebraic geometry

As mentioned in the Introduction, one of the main benefits of our Galois stratification procedure is that it makes the quantifier elimination and decision procedures for fields with Frobenii effective in an adequate sense of the word to be expounded in this section.

Ideally, we would like to prove that it makes those procedures primitive recursive, which would represent a significant improvement on the known results [21], [6], [18], where it was shown that the decision procedure is recursive.

Unfortunately, due to the underdeveloped state of constructive difference algebra, and the lack of algorithms for relevant operations with difference polynomial ideals, all we can do at the moment is to show that our Galois stratification procedure is primitive recursive reducible to a number of oracles for basic operations in difference algebra, which we hope will be shown to be primitive recursive themselves.

For a reader critical of this hybrid notion of effectiveness, let us mention that we have developed the theory of Galois stratification in the context of directly presented difference schemes, and the resulting quantifier elimination, equivalent in power to the logic quantifier elimination but coarser than the one in the present paper, is shown to be unconditionally primitive recursive in [23]. As is often the case in difference and differential algebra, a coarser result turns out to be more effective.

**Definition 6.1.** A ring \((R, \sigma)\) is said to be effectively presented, if it has a finite \(\sigma\)-presentation over \(\mathbb{Z}\), with its generators and relations explicitly given.

The following is a list of elementary operations on effectively presented rings that we shall have recourse to in the sequel.

- \((\dagger_1)\) Given a difference ideal \(I\) in a difference polynomial ring over an effectively presented difference field, find its minimal associated \(\sigma\)-primes, i.e., find an irredundant decomposition \(\{I\}_\sigma = p_1 \cap \cdots \cap p_n\) (as in [24, 2.45]).
- \((\dagger_2)\) Given an extension \((K, \sigma) \rightarrow (L, \sigma)\) of effectively presented difference fields of finite \(\sigma\)-type, compute the relative algebraic closure of \(K\) in \(L\).
- \((\dagger_3)\) In the situation of \((\dagger_2)\), compute a decomposition into a \(\sigma\)-separable and \(\sigma\)-radicial part as in [3.47].
- \((\dagger_4)\) Given an \(\sigma\)-separable Galois extension \((K, \sigma) \rightarrow (L, \sigma)\) of effectively presented difference fields of finite \(\sigma\)-type, compute its Babbitt’s decomposition (as in [5.11]).
(†₅) For an effectively presented integrally closed domain \((R, \sigma)\) with fraction field \((K, \sigma)\), and an extension \((L, \sigma)\) of \((K, \sigma)\) of finite \(\sigma\)-type, find the integral closure \((S, \sigma)\) of \(R\) in \(L\), and compute the \(\sigma\)-localisation \((R', \sigma)\) of \(R\) so that the corresponding \(S'\) is of finite \(\sigma\)-type over \(R'\) ([23] 2.56).

(†₆) Given an effectively presented morphism \(f : (R, \sigma) \to (S, \sigma)\) of effectively presented difference rings and a suitable property \(P\) of scheme morphisms, if \(f\) is generically \(\sigma\)-pro-\(P\), compute the \(\sigma\)-localisations \(R'\) of \(R\) and \(S'\) of \(S\) such that \((R', \sigma) \to (S', \sigma)\) is \(\sigma\)-pro-\(P\) (in particular, we need effective versions of \([3.3] 3.14\) and \([3.9]\)).

(†₇) Given an algebraic extension \((K, \sigma) \to (L, \sigma)\) of effectively presented difference fields of finite \(\sigma\)-type, compute the quasi-Galois closure of \(L\) over \(K\).

(†₈) For a finite Galois extension \((K, \sigma) \to (L, \Sigma)\) of effectively presented difference fields, establish an effective correspondence between the intermediate field extensions and subgroups of the Galois group.

(†₉) Effective Twisted Lang-Weil estimate. In the situation of [23] 4.2, compute explicitly the constant \(C\) and the localisation \(S'\) of \(S\).

**Definition 6.2.** We define \(\dagger\)-**primitive recursive functions** as functions primitive recursive reducible to basic operations in Difference Algebraic Geometry as detailed by the following axioms.

Basic \(\dagger\)-primitive recursive functions are:

1. *Constant* functions, *Successor* function \(S\), coordinate *Projections*;
2. *Elementary operations* in difference algebraic geometry \([1.1] [1.9]\).

More complex \(\dagger\)-primitive recursive functions are built using:

3. *Composition.* If \(f\) is an \(n\)-ary \(\dagger\)-primitive recursive function, and \(g_1, \ldots, g_n\) are \(m\)-ary \(\dagger\)-primitive recursive function, then
   \[
   h(x_1, \ldots, x_m) = f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m))
   \]
   is \(\dagger\)-primitive recursive.

4. *Primitive recursion.* Suppose \(f\) is an \(n\)-ary and \(g\) is an \((n+2)\)-ary \(\dagger\)-primitive recursive function. The function \(h\), defined by
   \[
   h(0, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)
   
   h(S(y), x_1, \ldots, x_n) = g(y, h(y, x_1, \ldots, x_n), x_1, \ldots, x_n)
   \]
   is \(\dagger\)-primitive recursive.

*Remark 6.3.* The operations \([1.6] [1.9]\) are primitive recursive.

**Proof.** In view of the constructive nature of proofs of \([3.3] 3.7\) \([3.8] 3.14\) \([3.9]\) the fact that the operation \([1.6]\) is primitive recursive will follow from the existence of the classical primitive recursive procedure for finding a localisation satisfying the property \(P\) at the start of the prolongation sequence.

The operation \([1.7]\) is primitive recursive because the construction of quasi-Galois closure is primitive recursive in the algebraic case. Indeed, if \(L = K(a_1, \ldots, a_n)\), and \(K(b_1, \ldots, b_m)\) is the quasi-Galois closure of \(K(a_1, \ldots, a_n)\), then \(K(b_1, \ldots, b_m)\) is the quasi-Galois closure of \(L\).

Since the operation \([1.8]\) only deals with finite Galois extensions, it follows that it is primitive recursive by the discussion in [11].
Regarding [13], Hrushovski indicates in the ‘Decidability’ subsection following [18, 13.2] that it is effective, showing how to explicitly compute the constants for the error term.

Conjecture 6.4. All the operations [13] are primitive recursive. The notions of primitive recursive and †-primitive recursive coincide.

7. Galois stratification

7.1. Galois stratifications and Galois formulae.

Definition 7.1. Let \((X, \sigma)\) be an \((S, \sigma)\)-difference scheme. It is often useful to consider its realisation functor \(\tilde{X}\). For each \(s \in S\) and each algebraically closed difference field \((F, \varphi)\) extending \((k(s), \sigma^s)\),

\[\tilde{X}(s, (F, \varphi)) = X_s(F, \varphi)\]

An \((S, \sigma)\)-subassignment of \(X\) is any subfunctor \(F\) of \(\tilde{X}\). Namely, for any \((s, (F, \varphi))\) as above,

\[F(s, (F, \varphi)) \subseteq X_s(F, \varphi),\]

and for any \(u : (s, (F, \varphi)) \to (s', (F', \varphi'))\), \(F(u)\) is the restriction of \(\tilde{X}(u)\) to \(F(s, (F, \varphi))\).

Definition 7.2. Let \((S, \sigma)\) be a difference scheme and let \((X, \sigma)\) be a difference scheme over \((S, \sigma)\). A normal (twisted) Galois stratification \(A = \langle X, Z_i/X_i, C_i | i \in I \rangle\) of \((X, \sigma)\) over \((S, \sigma)\) is a partition of \((X, \sigma)\) into a finite set of transformally integral normal \(\sigma\)-locally closed difference \((S, \sigma)\)-subvarieties \((X_i, \sigma)\) of \((X, \sigma)\), each equipped with a transformally integral étale Galois cover \((Z_i, \Sigma_i)/(X_i, \sigma)\) with group \((G_i, \tilde{\Sigma}_i)\), and \(C_i\) is a ‘conjugacy domain’ in \(\Sigma_i\).

A normal Galois stratification is effectively given, if the base \((S, \sigma)\) and all the pieces \(Z_i, X_i\) are affine with effectively presented coordinate rings (i.e., of finite \(\sigma\)-presentation over \(Z\)).

Definition 7.3. We define the (twisted) Galois formula over \((S, \sigma)\) associated with the above stratification \(A\) to be its realisation subassignment \(\tilde{A}\) of \(X\). Given a point \(s \in S\) and an algebraically closed difference field \((F, \varphi)\) extending \((k(s), \sigma^s)\),

\[\tilde{A}(s, (F, \varphi)) = A_s(F, \varphi) = \bigcup_i \{ x \in X_{i,s}(F, \varphi) | \varphi^Z_{X_i/X_i} x \subseteq C_i \},\]

where \(\varphi^Z_{X_i/X_i}\) denotes the local \(\varphi\)-substitution at \(x\), see 3.44.

It can be beneficial to think of the Galois formula associated with \(A\) and a given parameter \(s \in S\) as of the formal expression

\[\theta(t; s) \equiv \{ t \in X_s \mid \ar(t) \subseteq \con(A) \},\]

whose interpretation in any given \((F, \varphi)\) extending \((k(s), \sigma^s)\) is given above. Namely, the ‘Artin symbol’ \(\ar(t)\) of a point \(x \in X_{i,s}(F, \varphi)\) is interpreted as \(\ar(x) = \varphi_x\), the local \(\varphi\)-substitution at \(x\) with respect to the cover \(Z_i/X_i\), and \(\con(A)\) at \(x\) becomes the appropriate \(C_i\).
Remark 7.4. If we fix a lift \( \sigma_i \in \Sigma_i \) of \( \sigma \) for each \( i \) as in 3.45, the above data is equivalent to fixing for each \( i \) a \( \sigma_i \)-equivalent to fixing for each \( i \) a \( \sigma_i \)-conjugacy domain \( \hat{C}_i \) in \( G_i \), i.e., a union of \( \sigma_i \)-conjugacy classes in \( G_i \). This justifies the adjective ‘twisted’ used alongside ‘stratification’. Clearly,

\[
A_s(F, \varphi) = \bigcup_i \{ x \in X_{i,s}(F, \varphi) \mid \varphi_{x}^{Z_i/X_i} \subseteq \hat{C}_i \}.
\]

Definition 7.5. Let \( f : (X, \sigma) \to (Y, \sigma) \) be an \( (S, \varphi) \)-morphism, let \( A = \langle X, Z_i/X_i, C_i \rangle \) be an \( (S, \sigma) \)-Galois stratification on \( X \) and let \( B = \langle Y, W_j/Y_j, D_j \rangle \) be an \( (S, \sigma) \)-Galois stratification on \( Y \).

1. Given étale Galois \( (S, \varphi) \)-covers \( (Z_i', \Sigma_i') \to (X_i, \sigma) \) that dominate \( Z_i/X_i \), and writing \( \pi_i : \Sigma_i' \to \Sigma_i \) for the relevant \( \text{Diff} \)-morphisms, the inflation of \( A \) with respect to covers \( Z_i'/X_i \) is defined as

\[
A'_s(F, \varphi) = A_s(F, \varphi).
\]

It has the property that for every \( s \in S \), and every algebraically closed \((F, \varphi)\) extending \( (k(s), \sigma^s) \),

\[
A'_s(F, \varphi) = A_s(F, \varphi).
\]

2. Suppose we are given a further stratification of each \( X_i \) into finitely many integral, normal, locally closed \( (S, \sigma) \)-subschemas \( X_{ij} \). For each \( i,j \), let \( Z_{ij} \) be a connected component of \( (Z_i, \Sigma_i) \times_{(X_i, \sigma)} (X_{ij}, \sigma) \), and let \( D_{ij} \) be its decomposition subgroup in \( Z_i/X_i \). Moreover, let \( \Sigma_{ij} = \{ \sigma \in \Sigma_i : \sigma Z_{ij} = Z_{ij} \} \) and write \( \iota_{ij} : \Sigma_{ij} \hookrightarrow \Sigma_i \). Then \( (Z_{ij}, T_{ij}) \to (X_{ij}, \sigma) \) is a Galois cover over \( (S, \sigma) \) with group \( (D_{ij}, \Sigma_{ij}) \).

The refinement of \( A \) to the stratification \( \{ X_{ij} \} \) of \( X \) is defined as

\[
A'_s(F, \varphi) = A_s(F, \varphi).
\]

It has the property that for every \( s \in S \), and every algebraically closed \((F, \varphi)\) extending \( (k(s), \sigma^s) \),

\[
A'_s(F, \varphi) = A_s(F, \varphi).
\]

3. Let \( Z_j \) be a component of \( (X, \sigma) \times_{(Y, \sigma)} (W_j, T_j) \), and let \( D_{Z_j} \) be its decomposition subgroup in \( W_j/Y_j \). Moreover, let \( T_{Z_j} = \{ \tau \in T_j : \tau Z_j = Z_j \} \) and write \( \iota_{Z_j} : T_{Z_j} \hookrightarrow T_j \). Then \( (Z_j, T_{Z_j}) \to (X_j, \sigma) \) is a Galois cover with group \( (D_{Z_j}, T_{Z_j}) \).

The pullback \( f^*B \) of \( B \) with respect to \( f \) is defined as a refinement of

\[
\langle X, Z_j/X_j, \iota_{Z_j}^{-1}(D_j) \rangle
\]

to a normal refinement (non-canonical, found by 3.9) of the stratification \( X_j \) of \( X \). It has the property that for every \( s \in S \), and every algebraically closed \((F, \varphi)\) extending \( (k(s), \sigma^s) \),

\[
f^*B_s(F, \varphi) = f_s^{-1}(B_s(F, \varphi)).
\]

Definition 7.6. Let \( (X, \sigma) \) be an \( (S, \sigma) \)-difference scheme. The class of \( (S, \sigma) \)-Galois formulae on \( X \) has a Boolean algebra structure as follows.

(1) \( \perp_X = \langle X, X/X, \emptyset \rangle \), \( \top_X = \langle X, X/X, \{ \sigma \} \rangle \).

For Galois formulae on \( X \) given by \( A \) and \( B \), upon a refinement and an inflation we may assume that \( A = \langle X, Z_i/X_i, C_i \rangle \) and \( B = \langle X, Z_i/X_i, D_i \rangle \), with \( C_i, D_i \subseteq \Sigma_i \).
7.2. Direct Image Theorems. The following result can be considered as a differ-
ence version of Chevalley’s theorem stating that a direct image of a constructible
set by a scheme morphism of finite presentation is again constructible.

Proposition 7.7. Let $\pi : (X, \Sigma) \to (Y, T)$ be a generic weak cover of finite trans-
formal type. Then $\pi(X)$ contains a dense open subset of $Y$. If $\pi$ is effective-
ly presented, we can compute it in a $\dagger$-primitive recursive way.

Proof. It is enough to consider the case when $T = \{\sigma\}$.

Using 3.47, we can factorise $\pi$ as a composite of a radicial (purely inseparable),
radicial and a separable $\sigma$-separable morphism. The cases of radicial or $\sigma$-radicial
$\pi$ are dealt with using 3.48, so we reduce to the case of separable $\sigma$-separable $\pi$. In
the effective situation, this requires (1).

By $\sigma$-localising (3.8), we may assume that $\pi$ is a $\sigma$-pro-smooth morphism between
normal difference schemes. This is $\dagger$-primitive recursive by (1). By considering the
normalisation $\hat{Y}$ in the relative algebraic closure of $k(Y)$ inside $k(X)$, we obtain a
baby Stein factorisation $(X, \Sigma) \to (\hat{Y}, \hat{\Sigma}) \to (Y, \sigma)$, where the first map has ge-
ometrically transformally integral generic fibre (by 3.50), and the second is generically
$\sigma$-pro-étale $\sigma$-separable, with $k(\hat{Y})/k(Y)$ Galois by definition of weak covers.

By localising further using 3.14, we may assume that all the fibres of the first mor-
phism are directly transformally integral and consequently non-empty, so the first
morphism is surjective, and we can restrict our attention to the second morphism.
These steps are $\dagger$-primitive recursive by (1).

Using 3.8 by another localisation we restrict to the case where $(\hat{Y}, \hat{\Sigma}) \to (Y, \sigma)$ is
$\sigma$-pro-étale $\sigma$-separable. Applying Babbitt’s decomposition 5.12 to $(\hat{Y}, \hat{\Sigma}) \to (Y, \sigma)$
and a further localisation if necessary, we obtain a tower

$$\hat{Y} \simeq Y_n \to \cdots \to Y_1 \to Y_0 \to Y,$$

with $(Y_0, \Sigma_0) \to (Y, \sigma)$ finite Galois and all $Y_{i+1} \to Y_i$ proper benign, for $i \geq 0$. In
the effective case, all this can be achieved in a $\dagger$-primitive recursive way, using (1).

The first morphism is a Galois cover and therefore surjective by 2.22 and its generalisations, and proper benign morphisms are clearly surjective. Thus, we con-
clude that $\pi$ can be made surjective upon a finite $\sigma$-localisation, which is
enough to deduce the required statement. \hfill $\Box$

Definition 7.8. Let $(S, \sigma)$ be a normal integral difference scheme of finite $\sigma$-type
over $\mathbb{Z}$, and let $(X, \sigma)$ be an $(S, \sigma)$-difference scheme. Let $\mathcal{F}$ and $\mathcal{F}'$
be $(S, \sigma)$-subassignments of $X$ and let $m$ be a positive integer. We shall write

$$\mathcal{F} \equiv_{S}^{\text{Frob}, m} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$ and
$|k| \geq m$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$ and
$|k| \geq m$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$ and
$|k| \geq m$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$ and
$|k| \geq m$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$ and
$|k| \geq m$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$ and
$|k| \geq m$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$ and
$|k| \geq m$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)\text{ and } k$.

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

We say that $\mathcal{F}$ and $\mathcal{F}'$ are equivalent modulo fields with Frobenii over $S$ and write

$$\mathcal{F} \equiv_{S}^{\text{Frob}} \mathcal{F'},$$

if for every closed $s \in S$, every finite field $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)\text{ and } k$.
if \( \mathcal{F} \equiv_{S}^{\text{Frob}, m} \mathcal{F}' \) for some \( m \). We write \( \mathcal{F} \equiv_{S} \mathcal{F}' \), if the two subassignments agree over all algebraically closed difference fields.

**Definition 7.9.** Let \( f : (X, \sigma) \to (Y, \sigma) \) be a morphism of \((S, \sigma)\)-difference schemes and let \( \mathcal{A} \) be Galois stratification on \( X \). For \( s \in S \) and \((F, \varphi)\) an algebraically closed difference field extending \((k(s), \sigma^s)\), we define a subassignment \( f_{\mathcal{A}} \mathcal{A} \) of \( Y \) by the rule

\[
 f_{\mathcal{A}}(s, (F, \varphi)) = (f_{\mathcal{A}})_s(F, \varphi) = f_s(\mathcal{A}_s(F, \varphi)) \subseteq Y_s(F, \varphi).
\]

When \( \mathcal{A} \) is associated with a Galois formula \( \chi(x; s) \equiv \{ x \in X_s \mid \ar(x) \subseteq \text{con}(\mathcal{A}) \} \), it can be identified with an expression

\[
 \iota(y; s) \equiv \{ y \in Y_s \mid \exists x \; \chi(x; s), f_s(x) = y \},
\]

which justifies the notation somewhat.

**Lemma 7.10.** Suppose that

\[
 \begin{array}{ccc}
 Z & \xrightarrow{f} & Y \\
 | & \downarrow \varphi_z & \\
 X & \xrightarrow{f} & Y
 \end{array}
\]

is a triangle of étale Galois covers. We have an exact sequence of groups with operators

\[
 1 \to \text{Gal}(Z/X) \to \text{Gal}(Z/Y) \to \text{Gal}(X/Y) \to 1.
\]

Let \( C_0 \subseteq \Sigma_Z \) be a \( \text{Gal}(Z/X) \)-conjugacy domain, and let \( C \) be the \( \text{Gal}(Z/Y) \)-conjugacy domain induced by \( C_0 \). Then

\[
 f_{\mathcal{A}}(Z/X, C_0) \equiv \langle Z/Y, C \rangle^*.
\]

**Proof.** For the nontrivial inclusion, let \((F, \varphi)\) be an arbitrary algebraically closed difference field containing the field of definition of \( Y \), and suppose \( y \in \langle Z/Y, C \rangle(F, \varphi) \). There exists a \( z \in Z(F, \varphi) \) such that \( z \mapsto y \) and

\[
 \varphi_z \in C = \bigcup_{g \in \text{Gal}(Z/Y)} C_0^g,
\]

so let \( \varphi_z \in C_0^g \). Then \( \varphi^{-1}_z \in C_0 \), so the image \( x \) of \( g^{-1}z \) in \( X \) witnesses \( f(x) = y \) and \( x \in \langle Z/X, C_0 \rangle(F, \varphi) \). \( \square \)

**Lemma 7.11.** Let \((X, \sigma) \to (Y, \sigma)\) be a finite étale morphism of normal difference schemes, let \((Z, \Sigma_Z) \to (Y, \sigma)\) be a Galois cover, and let \( \hat{Z} = \iota^*Z \) be a difference scheme obtained by restricting the difference structure via some \( \iota : \Sigma_{\hat{Z}} \hookrightarrow \Sigma_Z \) so that \( \hat{Z} \to X \) is a Galois cover. Let \( C \) be a \( \text{Gal}(\hat{Z}/X) \)-conjugacy class in \( \Sigma_Z \). Then

\[
 f_{\mathcal{A}}(\hat{Z}/X, C) \equiv \langle Z/Y, \iota_*C \rangle^*,
\]

where \( \iota_*C \) is the smallest \( \text{Gal}(Z/Y) \)-conjugacy domain in \( \Sigma_Z \) containing \( \iota(C) \).

**Proof.** The diagram

\[
 \begin{array}{ccc}
 & \hat{Z} & \\
 & \downarrow & \Rightarrow \\
 & \hat{X} & \\
 \Rightarrow & \Rightarrow & \Rightarrow \\
 X & \xrightarrow{f} & Y
 \end{array}
\]
shows the situation following the insertion of the Galois closure of $X$ over $Y$. Starting with a Gal($\hat{Z}/X$)-conjugacy class $C$ in $\hat{\Sigma}$, we can consider it as a Gal($\hat{Z}/X$)-conjugacy domain $C'$, and write $C''$ for $C'$ considered in $\hat{Z}$, so that $\hat{C} = \iota_C C$ is the Gal($Z/Y$)-conjugacy domain induced by $C''$. Using (7.10) we have that $\hat{f}_3(\hat{Z}/\hat{X},C') = (Z/Y,\hat{C})$. Thus
\[ f_3(\hat{Z}/X,C) \equiv f_3\circ f_3(\hat{Z}/\hat{X},C') \equiv f_3(\hat{Z}/\hat{X},C') \equiv \hat{f}_3(\hat{Z}/\hat{X},C') \equiv (Z/Y,\hat{C}). \]

The main result of this paper is the following direct image theorem, stating that the class of Galois formulae over fields with Frobenii is closed under taking images by $f_3$.

**Theorem 7.12.** Let $(S,\sigma)$ be a difference scheme of finite $\sigma$-type over $Z$ and let $f: (X,\sigma) \to (Y,\sigma)$ be a morphism of $(S,\sigma)$-difference schemes of finite $\sigma$-type. For every Galois formula $A$ of $X$, the subassignment $f_3 A$ is $Frob_S$-equivalent to a Galois formula on $Y$, i.e., there exists a Galois formula $B$ on $Y$ such that
\[ f_3 A \equiv_{Frob_S} B. \]
When $A$ is effectively given, a $\dagger$-primitive recursive procedure yields an effectively given $B$ and a constant $m > 0$ such that
\[ f_3 A \equiv_{Frob_S,m} B. \]

**Proof.** The proof is by devissage, or noetherian induction, whereby in each step we calculate the direct image on a dense open piece and postpone the calculation on the ‘bad locus’ complement to the next step. At the end of the procedure, we will have obtained the image of each piece of the domain as a Galois stratification supported on a locally closed piece of the codomain. To finish, we extend all of these trivially to produce Galois formulae on the whole of $Y$, and we take their disjunction to represent the total image as a Galois formula.

In order to show that the procedure is $\dagger$-primitive recursive in the effective case, we must argue that our noetherian induction procedure can be rewritten in terms of bounded loops. This is a consequence of the fact that our devissage is controlled (unlike arbitrary noetherian induction algorithms, which are notoriously far from being primitive recursive). Indeed, in each step the ‘lower-dimensional bad locus’ can be computed explicitly and its degree/complexity can be bounded, and, even though the number of its components may be very large, it can be computed by the $\dagger$-oracles such as (7.11). Thus, even though the algorithm is written down as a devissage argument for convenience, the main control loop can in fact be bounded.

Given that we are interested in points with values in difference fields, we may assume that $X$ and $Y$ are perfectly reduced, so we can decompose them into transformally integral components using (7.11) and we can thus reduce to the case where $X$ and $Y$ are transformally integral.

By splitting off the radicial and $\sigma$-radicial part as in the proof of (7.7) we may assume that $f$ is separable $\sigma$-separable. In the effective case, we use (7.13) and after a possible refinement of $A$, we obtain stratifications $X_i$ and $Y_j$ into transformally integral normal locally closed $(S,\sigma)$-subschemes of $X$ and $Y$ such that for every $i$ there exists a $j$ with $f(X_i) \subseteq Y_j$ and $f_i := f \mid_{X_i}: (X_i,\sigma) \to (Y_j,\sigma)$ is
σ-pro-smooth σ-separable. This can be done in a †-primitive recursive way, using (1) and the effective case of 7.7.

By the philosophy of the proof, we can restrict our attention to one of the $f_i$, so we disregard the index $i$ and write $f : (X, \sigma) \to (Y, \sigma)$ in place of $f_i$, and we may assume that $A$ on $X$ is basic, $A = \langle Z/X, C \rangle$, where $(Z, \Sigma_Z)/(X, \sigma)$ is a transformally integral Galois cover with group $(G, \Sigma_Z)$ and $C$ is a $G$-conjugacy domain in $\Sigma_Z$.

By considering the normalisation $\tilde{Y}$ in the relative algebraic closure of $k(Y)$ inside $k(X)$, we obtain a baby Stein factorisation $(X, \sigma) \to (\tilde{Y}, \sigma) \to (Y, \sigma)$, where the first morphism has generically geometrically transformally integral fibres (by 3.50), and the second is generically σ-pro-étale σ-separable. In the effective situation, this requires (1).

Thus, we can split our considerations into two cases.

**Case 1.** We have a morphism $f : (X, \sigma) \to (Y, \sigma)$ of transformally integral $(S, \sigma)$-schemes whose generic fibre is geometrically transformally integral, and $(Z, \Sigma_Z)/(X, \sigma)$ is étale Galois with $Z$ transformally integral.

Let $(W, \Sigma_W)$ be the normalisation of $(Y, \sigma)$ in the relative algebraic closure of $k(Y)$ in $(k(Z), \Sigma_Z)$, in the effective case calculated by (1) and (1). Then $(W, \Sigma_W)$ is a Galois cover of $(Y, \sigma)$. Writing $(W_X, \Sigma_{W_X}) = (X, \sigma) \times_{(Y, \sigma)} (W, \Sigma_W)$, we obtain an exact sequence

$$1 \to \text{Gal}(Z/W_X) \to \text{Gal}(Z/X) \to \text{Gal}(W/Y) \to 1,$$

(3)

together with a $\text{Diff}$-quotient morphism

$$\pi : \Sigma_Z \to \Sigma_Z/\text{Gal}(Z/W_X) = \Sigma_W.$$

By a σ-localisation, using 3.14 and 3.15 we may assume that

(i) $W$ is transformally integral and $(W, \Sigma_W)/(Y, \sigma)$ is étale Galois;
(ii) $f$ and $Z \to W$ (and consequently $W_X \to W$) have directly geometrically transformally integral fibres;
(iii) $\text{Gal}(Z_w/W_w) = \text{Gal}(Z/W_X)$ for all fibres $Z_w$ of $Z \to W$ and $W_w$ of $W_X \to W$ above $w \in W$.

This is effective by (1) and (1).

Let $D = \pi_s(C)$ be the image of $C$ in $\Sigma_W$, computed by (1) and we claim that

$$f_\exists(Z/X, C) \equiv_{\text{PROB}} \langle W/Y, D \rangle,$$

i.e., for all closed $s \in S$, all large enough $k$ with $(\bar{k}, \varphi_k)$ extending $(k(s), \sigma^s)$,

$$\{ y \in Y_s(\bar{k}, \varphi_k) \mid \exists x \in X_s(\bar{k}, \varphi_k), \varphi_{k,x} \in C, f_s(x) = y \} = \{ y \in Y_s(\bar{k}, \varphi_k) \mid \varphi_{k,y} \in D \}.$$

(4)

A routine verification of the left to right inclusion needs no assumptions on the size of $k$. Conversely, let $y \in Y_s(\bar{k}, \varphi_k)$, $\varphi_{k,y} \in D_0 \subseteq D$. Pick some $y'$ in the fibre of $W/Y$ above $y$ with $\varphi_{k,y'} \in D_0$. Let us denote by $y \in Y_s$, $y' \in W_s$ the loci of $\tilde{y}$ and $\tilde{y}'$, $\tilde{y} = \text{Spec}^{\sigma^s}(k(y))$, $\tilde{y}' = \text{Spec}^{\Sigma^{\sigma^s}}(k(y'))$ (where $\Sigma^{\sigma^s}$ is shorthand for $\Sigma^{\sigma^s}$).
and consider the diagram

```
\begin{diagram}
  Z_y' & \rightarrow & X_y' \\
  \downarrow & & \downarrow \\
  W_X & \rightarrow & W \\
  \downarrow & & \downarrow \\
  X & \rightarrow & Y \\
\end{diagram}
```

where \((X_y, \sigma_y) = (X, \sigma) \times_{(Y, \sigma)} (\tilde{y}, \sigma_y')\) is the fibre of \(X\) above \(y\), \((X_y', \Sigma_y') = (W_X, \Sigma_W) \times_{(W, \Sigma_W)} (\tilde{y}', \Sigma_y')\) is the fibre of \(W_X\) above \(y'\), and

\[(Z_y', \Sigma_y') = (Z, \Sigma_Z) \times_{(W_X, \Sigma_W)} (X_y', \Sigma_y') = (Z, \Sigma_Z) \times_{(W, \Sigma_W)} (\tilde{y}', \Sigma_y')\]

is the fibre of \(Z\) above \(y'\). By construction, \(Z_y'\) is directly geometrically transformally integral and \(\text{Gal}(Z_y'/X_y') \cong \text{Gal}(Z/W_X)\). In the diagram with exact rows

\[
1 \rightarrow \text{Gal}(Z_y'/X_y') \rightarrow \text{Gal}(Z_y'/X_y) \rightarrow \text{Gal}(\tilde{y}'/\tilde{y}) \rightarrow 1 \\
1 \rightarrow \text{Gal}(Z/W_X) \rightarrow \text{Gal}(Z/X) \rightarrow \text{Gal}(W/Y) \rightarrow 1
\]

the left vertical arrow is an isomorphism and \(\text{Gal}(\tilde{y}'/\tilde{y}) = \text{Gal}(k(y')/k(y))\). It follows that \(\text{Gal}(Z_y'/X_y) = \text{Gal}(Z/X) \times_{\text{Gal}(W/Y)} \text{Gal}(\tilde{y}'/\tilde{y})\) and we get a Cartesian diagram of difference structures:

```
\begin{diagram}
  \Sigma_{y'} & \rightarrow & \Sigma_y' \\
  \downarrow & & \downarrow \\
  \Sigma_Z & \rightarrow & \Sigma_{y'} \\
\end{diagram}
```

Thus we can find a conjugacy domain \(C' \subseteq \Sigma_{y'}\) which maps into \(C\) in \(\Sigma_Z\) (and eventually to \(D_0 \subseteq \Sigma_W\), as well as onto \(\varphi_k\). It suffices to find an \(x \in X_y(k, \varphi_k)\) with \(\varphi_{k,x} \subseteq C'\) with respect to the cover \(Z_y'/X_y\), and this is possible for large enough \(k\) by Twisted Chebotarev [24, 4.28]. The relevant bound for the size of \(k\) can be calculated by (11a).

**Case 2.** The morphism \(f : (X, \sigma) \rightarrow (Y, \sigma)\) is generically \(\sigma\)-pro-´etale \(\sigma\)-separable of transformally integral \((S, \sigma)\)-schemes.

Using [5.24] the generic weak Galois closure of \(X\) over \(Y\) consists of generic weak covers \(r : (X, \tilde{\Sigma}) \rightarrow (X, \sigma)\) and \(\tilde{X} \rightarrow Y\) such that \(h = fr : (\tilde{X}, \tilde{\Sigma}) \rightarrow (Y, \sigma)\) is quasi-Galois. By [3.8 and 7.7] modulo a \(\sigma\)-localisation, we may assume that \(f\) is \(\sigma\)-pro-´etale and that \(h\) strictly dominates \(f\), i.e., that the morphism \(r\) is surjective. Then

\[f_3A \equiv f_3r_3r^*A \equiv h_3r^*A,\]
so it is enough to show that the direct image by \( h_\Sigma \) of a Galois formula \( B = i^*A \) is again Galois. In the effective case, we can do this via \( \{ t_2 \} \{ \{ t_3 \} \{ t_4 \} \{ t_5 \} \{ t_6 \} \). For each \( \sigma \in \Sigma \), let \( h_\sigma \) be the inclusion \( \{ \sigma \} \hookrightarrow \Sigma \), let \( X^\sigma = i_\sigma^* X \) and let \( i_\sigma : X^\sigma \to X \) be the natural morphism. Writing \( B^\sigma = i_\sigma^* B \) and \( h^\sigma = h_i \sigma \colon X^\sigma \to Y \), it is easily verified that
\[
h_\Sigma \equiv \bigvee_{\sigma \in \Sigma} h_\sigma^* B^\sigma,
\]
so we can reduce the consideration to morphisms of ordinary difference schemes.

In other words, we may assume that the original \( f : (X, \sigma) \to (Y, \sigma) \) is \( \sigma \)-pro-étale quasi-Galois \( \sigma \)-separable, so we can benefit from Babbitt’s decomposition. Indeed, modulo a localisation, \( \{ t_4 \} \{ t_5 \} \{ t_6 \} \) yields a decomposition of \( f \) as
\[
(X, \sigma) \simeq (X_n, \sigma) \to \cdots \to (X_1, \sigma) \to (X_0, \sigma) \to (Y, \sigma),
\]
with \( (X_0, \sigma) \to (Y, \sigma) \) finite étale quasi-Galois, and for \( i \geq 0 \), \( (X_{i+1}, \sigma) \to (X_i, \sigma) \) étale benign quasi-Galois. This can be achieved in a \( \dagger \)-primitive recursive way by using \( [t_4] \) and \( [t_5] \).

We can therefore reduce to two subcases as follows.

**Case 2(a).** The morphism \( f : (X, \sigma) \to (Y, \sigma) \) is finite étale. We are given a Galois cover \( (Z, \Sigma) \to (X, \sigma) \) and a Gal\((Z/X)\)-conjugacy domain \( C \) in \( \Sigma \).

The Galois closure \( \{ t_7 \} \{ t_8 \} \) of a finite étale morphism consists of Galois covers \( (r, \rho) : (\bar{Z}, \bar{\Sigma}) \to (Z, \Sigma) \) and \( (\bar{Z}, \bar{\Sigma}) \to (Y, \sigma) \), as well as a morphism \( (\bar{Z}, \bar{\Sigma}) \to (\bar{Z}, \bar{\Sigma}) \) arising by restriction of structure via \( i : \Sigma \hookrightarrow \bar{\Sigma} \).

Thus, using inflation and \( \{ t_7 \} \{ t_8 \} \)
\[f_\bar{\Sigma} \langle Z/X, C \rangle \equiv f_\bar{\Sigma} \langle Z/X, \rho^{-1} C \rangle \equiv \langle \bar{Z}/Y, \iota_* \rho^{-1} C \rangle.\]
The relevant calculations in the effective case are performed using \( [t_2] \) and \( [t_5] \).

**Case 2(b).** The morphism \( f : (X, \sigma) \to (Y, \sigma) \) is proper benign étale quasi-Galois. We are given a Galois cover \( (Z, \Sigma_Z) \to (X, \sigma) \) and a conjugacy domain \( C \) in \( \Sigma_Z \).

The weak generic Galois closure \( \{ t_9 \} \{ t_8 \} \) of \( Z \) over \( Y \) consists of weak generic covers \( Z \to Z \) and \( \bar{Z} \to Y \). Since \( Z \) is a finite Galois cover of \( X \) and \( X \) is quasi-Galois over \( Y \), it follows that \( \bar{Z} \) is a finite Galois cover of \( X \). Thus, using inflation we can replace \( Z \) by \( \bar{Z} \) and assume that the original \( Z \) is in fact quasi-Galois over \( Y \).

Babbitt’s decomposition \( \{ t_4 \} \{ t_5 \} \{ t_6 \} \) applied to \( Z/Y \) yields a sequence
\[
(Z, \Sigma_Z) \simeq (Z_n, \Sigma_n) \to \cdots \to (Z_1, \Sigma_1) \to (Z_0, \Sigma_0) = (W, \Sigma_W) \to (Y, \sigma)
\]
where \((W, \Sigma_W)/(Y, \sigma)\) can be assumed to be a finite étale Galois cover and \( Z_{i+1}/Z_i \) is benign for \( i \geq 0 \). Since \( k(X) \) is linearly disjoint from \( k(W) \) over \( k(Y) \), we obtain an exact sequence of the form \( \{ t_4 \} \) again, and we have the corresponding Diff-morphism \( \pi : \Sigma_Z \to \Sigma_W/Gal(Z/W_X) = \Sigma_W \). Let \( D = \pi_* C \) be the image of \( C \) in \( \Sigma_W \), and we claim that \( \{ t_4 \} \) holds for any \( s \) closed in \( S \) and \( (k, \varphi_k) \) extending \( (k(s), \varphi_s) \). To see the non-trivial inclusion, let \( y \) be an element of the right hand side and let \( z_0 \in W = Z_0 \) such that \( z_0 \to y \) and \( \varphi_k, z_0 \in D \). Using the property \( \{ t_9 \} \{ t_8 \} \) repeatedly, we can lift \( z_0 \) through the ‘stack’ of benign extensions \( Z_{i+1}/Z_i \) to a point \( z \in Z^\sigma(k, \varphi_k) \) with \( \tilde{\sigma} \in C \), and then the image \( x = x \) of \( z \) in \( X_s \) has the properties \( \varphi_k, x \sim \tilde{\sigma} \in C \) and \( f(x) = y \). This case is \( \dagger \)-primitive recursive by \( [t_2] \) \( [t_3] \) \( [t_6] \) \( [t_8] \).
Corollary 7.13. With assumptions of 7.12 it makes sense to define a subassignment
\[ f_\varphi A \equiv^{\text{Frob}}_S \neg f_\varphi(\neg A), \]
and it is again a Galois formula on \( Y \).

7.3. Quantifier elimination for Galois formulae. Let \((R, \sigma)\) be an integral normal difference ring of finite \( \sigma \)-type over \( \mathbb{Z} \), and let \((S, \sigma) = \text{Spec}^\sigma(R)\).

Definition 7.14. (1) A first-order formula over \((S, \sigma)\) is a first-order expression built in the usual way starting from terms which are difference polynomials with coefficients in \((R, \sigma)\). If \(x_1, \ldots, x_n\) are the free variables of a formula \(\theta\), and \(r_1, \ldots, r_m \in R\) are all the coefficients of all polynomials appearing as terms of \(\theta\), we can express this dependence by writing
\[ \theta(x_1, \ldots, x_n; r_1, \ldots, r_n), \]
where the \(r_i\) are thought of as parameters of \(\theta\).

(2) An \((R, \sigma)\)-formula \(\theta(x_1, \ldots, x_n; r_1, \ldots, r_n)\) gives rise to a subassignment \(\tilde{\theta}\) of \(\mathbb{A}_n(S, \sigma)\) by the following procedure. Let \(s \in S\), and let \((F, \varphi)\) be an algebraically closed difference field extending \((k(s), \sigma^s)\). Taking the images of the \(r_i\) by the composite
\[ (R, \sigma) \to (O_{S,s}, \sigma^s_1) \to (k(s), \sigma^s) \to (F, \varphi), \]
we obtain an honest first-order formula in the language of difference rings on the field \((F, \varphi)\), and we take its set of realizations to be the value
\[ \tilde{\theta}(s, (F, \varphi)) \subseteq \mathbb{A}_n(F, \varphi). \]

(3) An \((S, \sigma)\)-subassignment \(\mathcal{F}\) of \(\mathbb{A}_n(S, \sigma)\) is called definable if there exists a first-order formula \(\theta(x_1, \ldots, x_n)\) over \((R, \sigma)\) such that \(\mathcal{F} = \tilde{\theta}\).

Theorem 7.15 (Quantifier elimination for fields with Frobenii). The class of definable \((S, \sigma)\)-subassignments is equal to the class of \((S, \sigma)\)-Galois formulae modulo the relation \(\equiv^{\text{Frob}}_S\), i.e., with respect to fields with Frobenii over \( S \). The quantifier elimination procedure is \(\dagger\)-primitive recursive.

Proof. Let us show by induction on the complexity of a first-order formula that every \((S, \sigma)\)-formula in the language of rings \(\theta(x_1, \ldots, x_n)\) is equivalent to a Galois formula on \(\mathbb{A}_n(S, \sigma)\):

(1) If \(\theta(x_1, \ldots, x_n)\) is a positive atomic formula, it is given by a difference-polynomial equation \(P(x_1, \ldots, x_n) = 0\), which cuts out a closed difference subscheme \(Z\) of \(\mathbb{A}_n(S, \sigma)\). We can stratify the affine space into normal locally closed pieces \(X_i\) such that each piece is either completely in \(Z\) or in its complement. For each \(X_i\), we choose a trivial Galois cover \((X_i, \sigma) \to (X_i, \sigma)\), and we let \(C_i = \{\sigma\}\) when \(X_i \subseteq Z\), and \(C_i = 0\) otherwise. Then \(\mathcal{A} = \langle \mathbb{A}_S^n, X_i / X_i, C_i \rangle\) has the property that
\[ \tilde{\theta} \equiv \tilde{A} \]

(2) If \(\theta(\bar{x}) = \theta_1(\bar{x}_1) \land \theta_2(\bar{x}_2)\), where it is assumed that \(\bar{x}\) is the union of variables in \(\bar{x}_1\) and \(\bar{x}_2\), we choose the corresponding projections \(p_i : \mathbb{A}^{[\bar{x}]} \to \mathbb{A}^{[\bar{x}_i]}\). By induction hypothesis, we can find Galois formulae \(\mathcal{A}_i\) on \(\mathbb{A}^{[\bar{x}_i]}\) such that \(\theta_i \equiv^{\text{Frob}}_S \mathcal{A}_i\). Then
\[ \theta \equiv^{\text{Frob}}_S p^*_1 \mathcal{A}_1 \land p^*_2 \mathcal{A}_2. \]
(3) If \( \theta = \theta_1 \lor \theta_2 \), we proceed analogously to the previous step.
(4) If \( \theta = \neg \theta' \), and \( \theta' \equiv^{\text{Frob}}_S A \), then
\[
\theta \equiv^{\text{Frob}}_S \neg A.
\]

(5) If \( \theta(x_2, \ldots, x_n) = \exists x_1 \theta'(x_1, x_2, \ldots, x_n) \), and \( \theta' \equiv^{\text{Frob}}_S A \) on \( \mathbb{A}^n \), writing \( x_1 \) for the projection \( \mathbb{A}^n \to \mathbb{A}^{n-1} \) to the variables \( x_2, \ldots, x_n \), we have that
\[
\theta \equiv_S \exists x_1 \theta' \equiv^{\text{Frob}}_S x_1 \exists A,
\]
which is Galois by \( \ref{7.12} \).

(6) If \( \theta = \forall x_1 \theta' \), and \( \theta' \equiv^{\text{Frob}}_S A \), then
\[
\theta \equiv_S \forall x_1 \theta' \equiv^{\text{Frob}}_S x_1 \forall y A,
\]
which is Galois by \( \ref{7.13} \).

We have checked all cases so the induction is complete. Note that working over fields with Frobenius is only crucial in steps \([6] \) and \([8] \).

Conversely, suppose we have a Galois stratification \( \mathcal{A} = \langle \mathbb{A}^n_{(S, \sigma)}, Z_i / X_i, C_i \rangle \). By refining it further, we may assume that each Galois cover \( (Z_i, \Sigma_i) \to (X_i, \sigma) \) with group \( (G, \Sigma) \) is embedded in some affine space, in the sense that \( Z_i \) is embedded in some \( \mathbb{A}^n_{Z_i} \), and all automorphisms corresponding to elements of \( G \) are restrictions of difference rational endomorphisms of \( \mathbb{A}^n_{Z_i} \) to \( Z_i \), and the canonical projection \( Z_i \to X_i \) is a restriction of difference rational morphism \( \mathbb{A}^n_{Z_i} \to \mathbb{A}^n_{Z_i} \). Then, if \( C_i \) is the conjugacy class of some element \( \sigma_i \in \Sigma \), the set
\[
\{ x \in X_i : \text{ar}(x) \subseteq C_i \} = \{ x \in X_i : \exists z \in Z_i^{\sigma_i}, z \mapsto x \}
\]
is clearly expressible (working over algebraically closed difference fields) in a first-order way using an existential formula in the language of difference rings. When \( C_i \) is a union of conjugacy classes, we take the disjunction of the corresponding difference ring formulae. \( \square \)

Let \( T_\infty \) be the set of first-order sentences true in difference fields \((\bar{k}, \varphi_k)\) with \( k \) a sufficiently large finite field.

**Corollary 7.16.** The theory \( T_\infty \) is decidable by a \( \uparrow \)-primitive recursive procedure. Moreover, for each first-order sentence \( \theta \in T_\infty \) a \( \uparrow \)-primitive recursive procedure can compute the (finite) list of exceptional finite fields \( k \) such that \( \theta \) does not hold in \((\bar{k}, \varphi_k)\).

**Proof.** The quantifier elimination procedure produces a Galois stratification \( \mathcal{A} \) on the base \( S = \text{Spec}(\mathbb{Z}) \) and a constant \( m \) such that for every \( p \in S \), and every \( k \) of characteristic \( p \) with \( |k| \geq m \), \( \theta(\bar{k}, \varphi_k) = A(\bar{k}, \varphi_k) \). The stratification \( \mathcal{A} \) stipulates the existence of a localisation \( S' = \mathbb{Z}[1/N] \) of \( S \), a Galois cover \( Z / S' \) and a conjugacy class \( C \) in \( \text{Gal}(Z / S') \) such that, for \( p \in S' \) (i.e., for \( p \) not dividing \( N \)), and \( k \) of characteristic \( p \) with \( |k| \geq m \), \( \theta \) holds in \((\bar{k}, \varphi_k)\) if and only if \( \varphi_k \in C \). By (the classical) Chebotarev’s density theorem, this can hold for all but finitely many \( p \) if and only if \( C = \text{Gal}(Z / S') \), which can be effectively checked by \( \ref{7.14} \).

For each field \((\bar{k}, \varphi_k)\) with characteristic of \( k \) dividing \( N \), or \( |k| < m \), once we interpret \( \sigma \) as the Frobenius \( \varphi_k \) with \( \varphi_k(\alpha) = \alpha^{|k|} \), the formula \( \theta \) can be treated as a formula in the language of rings, which can be decided by the well-known primitive recursive decision procedure for the algebraically closed field \( \bar{k} \). \( \square \)
A model-theoretic restatement of the above theorem would say that the theory $T_\infty$ of fields with Frobenii allows quantifier elimination down to the class of Galois formulae. Given that $T_\infty$ happens to be \cite{18}, the theory of existentially closed difference fields (ACFA), let us state an appropriate analogue of the above result.

We must emphasise that the statement below can be obtained unconditionally, i.e., without appealing to \cite{18}, by replacing the use of \cite{24, 4.2} in the present paper by the use of existentially-closedness of models of ACFA (i.e., by the use of the ‘ACFA-axiom’). This will be done in a separate paper \cite{25}.

**Theorem 7.17.** Let $(k, \sigma)$ be a difference field. Let $\psi(x) = \psi(x; s)$ be a first order formula in the language of difference rings in variables $x = x_1, \ldots, x_n$ with parameters $s$ from $k$. There exists a Galois stratification $\mathcal{A}$ of the difference affine $n$-space over $k$ such that for every model $(F, \varphi)$ of ACFA which extends $(k, \sigma)$,

$$\psi(F, \varphi) = \mathcal{A}(F, \varphi).$$

**References**


Ivan Tomasić, School of Mathematical Sciences, Queen Mary University of London, London, E1 4NS, United Kingdom, Tel: +44 7985428862, Fax: +44 2078827684
E-mail address: i.tomasic@qmul.ac.uk