Nagoya Math. J., **222**(1) (2016), 1–60
DOI 10.1017/nmj.2016.9

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 formulas associated with finite Galois covers of difference schemes.

CONTENTS

§1. Introduction

Galois stratification, originally developed through work of Fried, Haran, Jarden and Sacerdote [13], [14], [12], provides an explicit arithmetic–geometric description of definable sets over finite fields in terms of Galois formulas 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

Received November 8, 2012. Accepted February 22, 2015.
2010 Mathematics subject classification. Primary 03C60, 11G25; Secondary 14G10, 14G15.

precise description of formulas 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 [11]. 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 formulas.

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, σ) 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 Σ_i, with all these notions defined in Section 2. The *Galois formula* associated with $\mathcal{A}$ is the realization 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, φ) is an algebraically closed difference field and the conjugacy class $\varphi_x \subseteq \Sigma$ is the local φ-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 Frobenii. Equivalently, the class of Galois formulas over fields with Frobenii 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 φ,*

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

A model-theoretic restatement of the above theorem is that fields with Frobenii allow *quantifier elimination* in the language of Galois formulas. In

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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 $\theta(x_1, \dots, x_n)$ be a first-order formula in the language of difference rings (with suitable parameters). We can effectively compute a Galois stratification $\mathcal{A}$ of the difference affine n-space such that for all (suitable) $(\bar{\mathbb{F}}_p, \varphi)$ with a high enough power of Frobenius φ,*

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

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 $\theta(x_1, \dots, x_n)$ in the language of difference rings is equivalent, modulo the theory ACFA of existentially closed difference fields, to a Boolean combination of formulas of the form

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

where ψ is quantifier free, and $\psi(y; x_1, \dots, x_n)$ implies that y satisfies a nonzero polynomial whose coefficients are σ-polynomials in $x_1, \dots, x_n$, that is, 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 formulas being associated with *finite* Galois covers of difference schemes, whereas the covers associated with the logic quantifier elimination are in general only quasifinite, 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 †-*primitive recursive*, that is, primitive recursive

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

reducible to basic operations in difference algebraic geometry, 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 †-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 3.10), 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 *generalized 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 [13], [14], [12] 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 factorization 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,

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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 generalized 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 emphasized that our theory is almost orthogonal to the various notions of smoothness that appear in Giabicani's thesis [15] (see 3.31).

En route to the main theorem, we encounter another merit of working in the context of generalized 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 transformal type to contain a dense open set. Wibmer gives a similar result by generalizing difference algebra in a slightly different direction [26].

§2. Generalized difference algebra and geometry

In this section, we give a summary of the theory of generalized 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 *Diff* as follows. An object of *Diff* is a set Σ, equipped with a map $\Sigma \times \Sigma \to \Sigma$, $(\sigma, \tau) \mapsto \sigma \triangleleft \tau$ such that:

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

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

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

Inherently, for every $\sigma \in \Sigma$, the map $() \triangleleft \sigma : \Sigma \to \Sigma$ is a *Diff*-morphism.

DEFINITION 2.2. The *difference category of locally ringed spaces* has objects of form (X, Σ), where $(X, \mathcal{O}_X)$ is a locally ringed space, and Σ is

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

a set of endomorphisms of X such that there exists a function $\Sigma \times \Sigma \to \Sigma$, $(\sigma, \tau) \mapsto {}^{\tau}\sigma$ 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 *Diff*.

A morphism $(\varphi, {}^{\varphi}()) : (X, \Sigma) \to (Y, T)$ consists of a *Diff*-morphism ${}^{\varphi}() : \Sigma \to T$ and a morphism of locally ringed spaces $\varphi : X \to Y$ such that for every $\sigma \in \Sigma$,
$$ {}^{\varphi}\sigma \circ \varphi = \varphi \circ \sigma. $$

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

(1) for every $\sigma, \tau \in \Sigma$,
$$ \tau \circ \sigma^{\tau} = \sigma \circ \tau; $$
(2) $(\Sigma, (\sigma, \tau) \mapsto \sigma^{\tau})$ is an object of *Diff*.

A morphism $\varphi : (B, T) \to (A, \Sigma)$ consists of a *Diff*-morphism $()^{\varphi} : \Sigma \to T$ and a ring homomorphism $\varphi : B \to A$ such that
$$ \varphi \circ \sigma^{\varphi} = \sigma \circ \varphi. $$

Definition 2.4. Each difference ring (A, Σ) has a natural action of the free semigroup $\langle \Sigma \rangle$ generated by Σ, as well as the ring $\mathbb{N}[\Sigma] = \mathbb{N}[\langle \Sigma \rangle]$ of positive integer combinations of elements of $\langle \Sigma \rangle$. The *difference ring localization* 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, Σ) is called

(1) *strong*, or Σ-*reduced*, if all endomorphisms in Σ 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 $\mathrm{Aut}(A, \Sigma)$, an element $\sigma \in \Sigma$ and a group homomorphism $()^{\sigma} : G \to G$ such that $\Sigma = \sigma G$, and for all $g \in G$, $g\sigma = \sigma g^{\sigma}$. Consequently, the difference structure is given by
$$ (\sigma g)^{(\sigma h)} = \sigma (h^{-1} g)^{\sigma}\, h. $$

Every strong difference ring (A, Σ) with Σ finite and every $()^{\sigma} : \Sigma \to \Sigma$ bijective has an *inversive closure*.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

DEFINITION 2.6. Let I be an ideal in a difference ring (A, Σ). We say that:

(1) I is a Σ-*ideal* if $\sigma(I) \subseteq I$ for every $\sigma \in \Sigma$;
(2) I is Σ-*reflexive* if $\sigma^{-1}(I) = I$ for every $\sigma \in \Sigma$;
(3) I is Σ-*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 Σ-*perfect* if for every $\sigma \in \Sigma$, $a\,\sigma a \in I$ implies a and σa are both in I;
(6) A is a *transformal domain* if (A, Σ) is strong and A is a domain.

2.2 Difference spectra

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

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

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 $\mathrm{Spec}^{\sigma}(R)$, $\mathrm{Spec}^{\Sigma}(R)$, respectively.

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

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

each $\sigma \in \Sigma$ induces the morphism of locally ringed spaces $({}^{a}\sigma, \tilde{\sigma}) : (X, \mathcal{O}_X) \to (X, \mathcal{O}_X)$. Consequently, the locally ringed space $(X, \mathcal{O}_X)$ 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 ${}^{a}(\tau^{\sigma}) = {}^{({}^{a}\sigma)}({}^{a}\tau)$, making $(\mathrm{Spec}^{\Sigma}(R), \mathcal{O}_{\mathrm{Spec}^{\Sigma}(R)}, {}^{a}\Sigma)$ into a difference locally ringed space.

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

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

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

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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

This makes 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, Σ) be a well-mixed difference ring with finite Σ so that $X = \mathrm{Spec}^{\Sigma}(A)$ is quasicompact.

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

$$({}^a i, \tilde{\imath}) : \mathrm{Spec}^{\Sigma}(\bar{A}) \xrightarrow{\sim} \mathrm{Spec}^{\Sigma}(A).$$

(2) Consequently, the functor H^0 is left adjoint to Spec.

2.3 Difference schemes

DEFINITION 2.9.

(1) An *affine difference scheme* is an object $(X, \mathcal{O}_X, \Sigma)$ of the difference category of locally ringed spaces, which is isomorphic to $\mathrm{Spec}^{\Sigma}(A)$ for some difference ring (A, Σ).
(2) A *difference scheme* is an object $(X, \mathcal{O}_X, \Sigma)$ of the difference category of locally ringed spaces, which is locally an affine difference scheme.
(3) A *morphism of difference schemes* $(X, \mathcal{O}_X, \Sigma) \to (Y, \mathcal{O}_Y, T)$ is just a morphism in the difference category of locally ringed spaces.

DEFINITION 2.10. Let (X, Σ) be a difference scheme and $x \in X$ a point. Let

$$\Sigma_x = \{\sigma \in \Sigma : \sigma(x) = x\}, \quad \Sigma_x^\sharp = \{\sigma_x^\sharp : \sigma \in \Sigma_x\}, \quad \text{and} \quad \Sigma^x = \{\sigma^x : \sigma \in \Sigma_x\},$$

where $\sigma^x : \mathbf{k}(x) \to \mathbf{k}(x)$ is induced by the local morphism $\sigma_x^\sharp : \mathcal{O}_x \to \mathcal{O}_x$ associated with each $\sigma \in \Sigma_x$. This yields a difference *local ring* $(\mathcal{O}_x, \Sigma_x^\sharp)$ with difference *residue field* $(\mathbf{k}(x), \Sigma^x)$.

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.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

We often work in a relative setting, over a chosen base scheme (S, Σ_0) or a base difference ring (R, Σ_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, Σ_0)-*difference scheme* is locally of the form $\mathrm{Spec}^{\Sigma}(A)$, for a difference (R, Σ_0)-algebra (A, Σ), and morphisms are required to locally preserve the (R, Σ_0)-algebra structure.

DEFINITION 2.12. Let (X, Σ) be a difference scheme and (K, φ) a difference field. The set of (K, φ)-*rational points* of (X, Σ) is the set

$$\mathrm{Hom}(\mathrm{Spec}^{\varphi}(K), (X, \Sigma)).$$

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 fiber 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 generalized 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, φ) be a difference field and let $s \in (S, \Sigma_0)(K, \varphi)$. The *fiber* X_s is the (K, φ)-difference scheme obtained by base change via the morphism $s : \mathrm{Spec}^{\varphi}(K) \to (S, \Sigma_0)$,

$$(X_s, \Sigma_s) = (X, \Sigma) \times_{(S,\Sigma_0)} \mathrm{Spec}^{\varphi}(K).$$

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, Σ_0) be a difference ring.

(1) An (R, Σ_0)-algebra (A, Σ) is of *finite* Σ-*type* if there exist elements $a_1, \ldots, a_n$ in A such that $A = R[a_1, \ldots, a_n]_{\Sigma} = R[\nu a_1, \ldots, \nu a_n : \nu \in \langle \Sigma \rangle]$.
(2) An (R, Σ_0)-difference scheme (X, Σ) is of *finite* Σ-*type*, or of *finite transformal type* if it is a finite union of affine difference schemes of the form $\mathrm{Spec}^{\Sigma}(A)$, where (A, Σ) is of finite Σ-type over (R, Σ_0).

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

(3) A morphism $f : (X, \Sigma) \to (Y, \Sigma_0)$ is *of finite* Σ*-type* if Y is a finite union of open affine subsets $V_i = \mathrm{Spec}^{\Sigma_0}(R_i)$ such that for each i, $f^{-1}(V_i)$ is of finite Σ-type over (R_i, Σ_0).
(4) A morphism $f : (X, \Sigma) \to (Y, \Sigma_0)$ is *integral* (resp. *finite*) if Y is a finite union of open affine subsets $V_i = \mathrm{Spec}^{\Sigma_0}(R_i)$ such that for each i, $f^{-1}(V_i)$ is $\mathrm{Spec}^{\Sigma}(A_i)$, where A_i is integral (resp. finite) over R_i.

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

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

In the generalized context, we have the following.

Fact 2.16. Let (S, Σ) be an almost-strict algebra of finite Σ-type over a Ritt ring (R, σ_0), and Σ finite. Then $\mathrm{Spec}^{\Sigma}(S)$ 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, Σ) is a group G, together with a *Diff*-structure Σ 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 [24, 2.2]).

We say that a group $(G, {}_{\llcorner}\Sigma)$ *acts* (on the left) by automorphisms on a ring (A, Σ), if every $\sigma \in \Sigma$ corresponds to an endomorphism $()^{\sigma} \in {}_{\llcorner}\Sigma$ of G so that, for every $g \in G$ and $\sigma, \tau \in \Sigma$,

$$(g^{\tau})^{\sigma^{\tau}} = (g^{\sigma})^{\tau},$$

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

$$g\sigma = \sigma g^{\sigma}.$$

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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

REMARK 2.18. If $(G, \lrcorner\Sigma)$ acts on (A, Σ), then $({}^aG, \Sigma_\lrcorner)$ acts on $(X, {}^a\Sigma) = \mathrm{Spec}^{\Sigma}(A)$ for $\Sigma_\lrcorner = \left\{{}^a\sigma() : \sigma \in \Sigma\right\}$.

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

LEMMA 2.20. *Let (A, σ) 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 $\bar{\sigma} = \sigma \restriction_B$. Then there exists a homomorphism $()^\sigma : G \to G$ satisfying $g\sigma = \sigma g^\sigma$ for $g \in G$, making (A, Σ), for $\Sigma = \sigma G$, into an almost-strict extension of $(B, \bar{\sigma})$ with automorphism group $(G, \tilde{\Sigma})$, where $\tilde{\Sigma} = \{()^\tau : \tau \in \Sigma\}$.*

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 $f_1 \restriction_B = f_2 \restriction_B$, so [5, V, Section 2.3, Corollaire 1] yields a $h \in G$ such that $f_2 = f_1 h$. By injectivity of j, we get $g\sigma = \sigma h$. Since σ is injective, h is unique and we can write $h = g^\sigma$. □

COROLLARY 2.21. *Let $(K, \bar{\sigma}) \to (L, \sigma)$ be a difference field extension where L/K is Galois with group G. Let Σ be the set of all lifts of $\bar{\sigma}$ to L. Then $\Sigma = \sigma G$ and we have endomorphisms $\tilde{\Sigma} = \{()^\tau : \tau \in \Sigma\}$ of G such that $(G, \tilde{\Sigma})$ is the group of automorphisms of (L, Σ) over $(K, \bar{\sigma})$.*

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

(1) *A is integral over B.*
(2) *The morphism p is surjective, its fibers 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 stabilizer of x and $\Sigma_x = \{\sigma \in \Sigma : {}^a\sigma(x) = x\}$ (we used ${}^a\Sigma_x = {}^a(\Sigma_x)$ in 2.10). Let $\tilde{\Sigma}_x = \{()^\sigma \in \tilde{\Sigma} : \sigma \in \Sigma_x\}$ and $\tilde{\Sigma}^x = \{()^{\sigma^x} : \sigma \in \Sigma_x\}$, where $\sigma^x : \mathbf{k}(x) \to \mathbf{k}(x)$ is induced by $\sigma_x^\sharp : \mathcal{O}_x \to \mathcal{O}_x$ for every $\sigma \in \Sigma_x$. Then $\mathbf{k}(x)$ is a quasi-Galois algebraic extension of $\mathbf{k}(y)$ and the canonical map*

$$(G_x, \tilde{\Sigma}_x) \to \left(\mathrm{Gal}(\mathbf{k}(x)/\mathbf{k}(y)), \tilde{\Sigma}^x\right)$$

is surjective.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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

DEFINITION 2.23. Let (X, Σ) be a difference scheme with a finite group of automorphisms $(G, \tilde{\Sigma})$ 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 $(G, \tilde{\Sigma})$.

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

§3. Local study of difference schemes and their morphisms

3.1 Difference schemes versus pro-algebraic varieties

One of the most important ideas in the study of difference algebraic geometry was the realization 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, ς) *be a difference ring. The forgetful functor from the category of difference* (R, ς)*-algebras to the category of* R*-algebras has a left adjoint* $[\varsigma]_R$*, that is, for every* R*-algebra* A *we have a homomorphism* $A \to [\varsigma]_R A$ *inducing the functorial isomorphism*

$$\mathrm{Hom}_{(R,\varsigma)}([\varsigma]_R A, (C, \sigma)) = \mathrm{Hom}_R(A, C),$$

for every (R, ς)*-algebra* (C, σ).

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

$$A_n = \bigotimes_{i \leqslant n} A_{\varsigma^i},$$

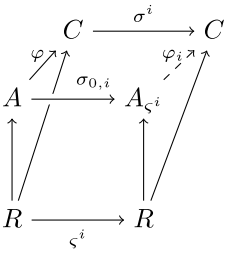
where the tensor product is taken over R, and

$$\sigma_n : A_n \to A_{n+1}$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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

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



yields a unique $\varphi_i : A_{\varsigma^i} \to C$, and subsequently $\tilde{\varphi}_n = \bigotimes_{i \leqslant n} \varphi_i : A_n \to C$. Passing to the limit, we obtain $\tilde{\varphi} : [\varsigma]_R A \to C$ with the required properties. □

PROPOSITION 3.2. [18] *Let (R,ς) be a difference ring and let X be an (algebraic) scheme over R. The functor from the category of difference (R,ς)-schemes to the category of sets, $(Z,\sigma) \mapsto \mathrm{Hom}_R(Z,X)$ (morphisms of locally R-ringed spaces) is representable. More precisely, the universal morphism $[\varsigma]_R X \to X$ of locally R-ringed spaces induces a functorial isomorphism*

$$\mathrm{Hom}_R(Z,X) = \mathrm{Hom}_{(R,\varsigma)}((Z,\sigma),[\sigma]_R X),$$

for every (R,σ)-difference scheme (Z,σ).

Proof. Let us prove the affine case. Suppose $X = \mathrm{Spec}(A)$, $Z = \mathrm{Spec}^\sigma(C)$ for a well-mixed difference ring (C,σ) 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 $\varphi : A \to \bar{C} = \mathcal{O}_Z(Z)$ so that, in view of 2.8 f is the restriction of ${}^a\varphi : \mathrm{Spec}(\bar{C}) \to \mathrm{Spec}(A)$ to $\mathrm{Spec}^\sigma(\bar{C})$. Using 3.1, there is a unique lift $([\varsigma]_R, \sigma) \to (\bar{C},\sigma)$ of φ, which gives the required difference scheme morphism

$$Z \to \mathrm{Spec}^\sigma([\varsigma]_R A) = [\varsigma]_R X. \qquad \square$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

Suppose now that X is an R-scheme and (Z,σ) is a closed (R,ς)-difference subscheme of $[\varsigma]_R X$. For ease of notation, let us write $S=\mathrm{Spec}(R)$. Writing X_{ς^i} for the base change $X\times_S S$ via the morphism $\varsigma^i : S\to S$, it is clear that the ς^i-linear morphism $\sigma^i : [\varsigma]_R X\to [\varsigma]_R X$ defines an R-morphism $[\varsigma]_R X\to X_{\varsigma^i}$ and thus we deduce a morphism

$$Z\hookrightarrow [\varsigma]_R X\to X\times X_\varsigma\times\cdots\times X_{\varsigma^n}=:X[n].$$

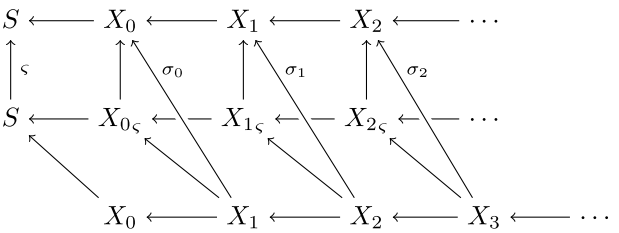
We denote the scheme-theoretic image of this map by $Z[n]$, obtaining a closed R-subscheme $Z[n]\hookrightarrow X[n]$ for every n, called the nth *Zariski closure of the difference scheme Z in X*. Although the projective limit $Z[\infty]$ of the $Z[n]$ can be viewed as a scheme, we find it most illuminating to view it as a pro-(scheme of finite type).

The maps $X_{\varsigma^{i+1}}\to X_{\varsigma^i}$ induce the maps $\sigma_n : X[n+1]\to X[n]$ and thus $X[\infty]$ is equipped with an endomorphism σ, which is the limit of σ_n. In this context, $[\varsigma]_R X$ is the fixed-point scheme of σ 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,σ) of finite σ-type over (R,ς) 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 $(X,\sigma)=\mathrm{Spec}^\sigma(A)$, where $A=R[a]_\sigma$ is an (R,ς)-algebra of finite σ-type, generated by a tuple $a\in A$.

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



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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

LEMMA 3.3. (Preparation Lemma) *With above notation, if A and R are transformally integral, by σ-localizing A and R we can arrange that morphisms*

$$X_{n+1} \to X_n \times_{X_{n-1_\varsigma}} X_{n\varsigma} \to X_n \times_{X_{n-1}} X_n$$

are isomorphisms for $n \geqslant 1$ 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 ς-localization of R, we can find a new tuple of generators $a = bc$ so that, writing $\sigma^i(a) = a_i = b_i c_i$ and $L_n = K(a_0, \ldots, a_n)$ for the fraction field of A_n, we have that for $n \geqslant 1$,

(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

$$\begin{array}{ccc} k & \longrightarrow & B \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ C & \longrightarrow & K \end{array}$$

of sub-k-algebras B, C of a difference field (K, σ), we shall say that B is σ-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 $B \otimes_k C \to \sigma(B)C$.

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

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & L_{n-1} & \longrightarrow & L_{n-1}(b_n) & \longrightarrow & L_n & \longrightarrow & \cdots \\ & & & {\scriptstyle\sigma}\searrow & & {\scriptstyle\sigma}\searrow & & {\scriptstyle\sigma}\searrow & \\ & & \cdots & \longrightarrow & L_n & \longrightarrow & L_n(b_{n+1}) & \longrightarrow & L_{n+1} \longrightarrow \cdots \end{array}$$

that L_n is σ-linearly disjoint from L_n over L_{n-1} for all $n \geqslant 1$.

Now, using generic flatness [16, Théorème 6.9.2], by σ-localizing A (by an element of A_0) we may assume that $\pi_{10} : A_0 \to A_1$ and $\sigma_0 : A_0 \to A_1$ are flat (i.e., A_1 is a flat A_0-module both via π_{10} and σ_0), so $A_1 \otimes_{A_0} A_1$ is a flat A_0 module. Thus the natural morphism

$$(A_1 \otimes_{A_0} A_1) \to L_0 \otimes_{A_0} (A_1 \otimes_{A_0} A_1)$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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,

$$\begin{aligned} L_0 \otimes_{A_0} (A_1 \otimes_{A_0} A_1) &= (L_0 \otimes_{A_0} A_1) \otimes_{L_0} (L_0 \otimes_{A_0} A_1) \\ &= L_0[A_1] \otimes_{L_0} L_0[A_1] \to L_0[A_1, \sigma(A_1)] \\ &= L_0[A_2] \end{aligned}$$

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

$$A_n \otimes_{A_{n-1}} A_n \to A_n \otimes_{A_{n-1_\varsigma}} A_{n_\varsigma} \to A_{n+1}$$

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 localize 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 $X \to Y$ has P, and $Z \to Y$ is arbitrary, then the morphism $X \times_Y Z \to Z$ has P.
(3) (Open embedding). If $X \to Y$ has P, and $U \hookrightarrow X$, then $U \to Y$ has P.
(4) (Genericity in the target). If $f : X \to Y$ (with Y integral) is generically P, there is a localization Y' of Y such that $f \restriction f^{-1}(Y')$ is P.

(4′) (Genericity in the source). If $f : X \to Y$ (with Y integral) is generically P, there is a localization X' of X and Y' of Y such that the morphism $f \restriction X' \cap f^{-1}(Y')$ 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.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

DEFINITION 3.5.

(1) Let (X, σ) be an (R, σ)-difference scheme of finite σ-type. We say that (X, σ) has the property *σ-pro-P*, if there exists a prolongation sequence X_n as above for X such that all the structure maps $X_n \to \mathrm{Spec}(R)$ 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 σ-type. We say that f has the property *σ-pro-P*, if for every open affine $V = \mathrm{Spec}^{\sigma}(R)$ in Y, the scheme $f^{-1}(V)$ has the property σ-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 σ-type (over a common base). We say that f has the property *σ-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, σ) is σ-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 σ-type (over some common base) is σ-pro-P, and (Y, σ) is σ-pro-P, then (X, σ) is σ-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 σ-pro-P is σ-generic in the source. In other words, if $f : (X, \sigma) \to (Y, \sigma)$ is a morphism of finite σ-type between transformally integral schemes which is generically σ-pro-P, then there exists a σ-localization X' of X and Y' of Y such that $f \restriction X'$ is σ-pro-P above Y', that is, $f \restriction X' \cap f^{-1}(Y')$ is σ-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 σ-type.*

Proof. Let us prove (2), the proof of (1) being strictly easier. We shall assume the reader has constructed, upon a σ-localization 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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

σ-localization of Y we can assume that $X_0 \to Y_0$ has P. Using (G) and (O), by σ-localizing 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 σ-localization of X and Y we can assume that $X_0 \to Y_0$ has P. Using (G) again, we need to σ-localize 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 σ-generation in terms of fiber products to the extent that $X_{n+1} \to X_n \times_{X_{n-1_\varsigma}} X_{n_\varsigma}$ are no longer isomorphisms for $n \geqslant 1$, 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 $X_n \times_{X_{n-1}} X_n \to X_n$ has P. By (O) and the fact that $X_{n+1} \hookrightarrow X_n \times_{X_{n-1}} X_n$ for $n \geqslant 1$, 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 localize the base, then we could prove that σ-pro-P is σ-generic in the target. □

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

(1) *If f is separable then there is a σ-localization X' of X and Y' of Y such that $f \restriction X' \cap f^{-1}(Y')$ is σ-pro-smooth.*
(2) *If f is separable algebraic, then there is a σ-localization X' of X and Y' of Y such that $f \restriction X' \cap f^{-1}(Y')$ is σ-pro-étale.*

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

Proof. By 3.8, take a σ-localization X'/R' which is σ-pro-smooth. □

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

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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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

In [23], we consider directly presented difference schemes (X, Σ) associated with a collection of algebraic correspondences $X_0 \overset{\pi_1}{\longleftarrow} X_1 \overset{\pi_2(\sigma)}{\longrightarrow} X_{0\varsigma}$, for $\sigma \in \Sigma$.

DEFINITION 3.12. Let (X, Σ) be a directly presented difference scheme over (R, ς) associated with algebraic correspondences $X_0 \overset{\pi_1}{\longleftarrow} X_1 \overset{\pi_2(\sigma)}{\longrightarrow} X_{0\varsigma}$, 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 3.12, a difference scheme (X, Σ) is said to be *directly geometrically transformally integral* if it is directly geometrically integral and π_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 σ-type of transformally integral difference schemes whose generic fiber is geometrically transformally integral. Then there is a σ-localization Y' of Y, Y' of Y such that $f \restriction_{Y'} : Y' \to S'$ has directly geometrically transformally integral fibers.*

Proof. The Preparation Lemma 3.3 shows that, modulo a localization, Y can be made directly presented over S. Writing η for the generic point of S, Y_η is assumed to be geometrically transformally integral, so $Y_{0,\eta}$, $Y_{1,\eta}$ and $Y_{0\varsigma,\eta} = Y_{0,\varsigma\eta}$ are geometrically integral and the relevant projections are all dominant. Using the constructibility of the property of being geometrically integral [1, Tag 055G], as well as the dominance of a morphism, we can ς-localize S to obtain that every fiber Y_s is directly transformally integral. □

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, ς) such that the generic fibers of X and Y over S are geometrically transformally integral. Then there exist localizations X' of X, Y' of Y and S' of S such that for every $s \in S'$, the fibers X'_s and Y'_s are directly geometrically transformally*

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

integral and

$$\mathrm{Gal}(X'_s/Y'_s) = \mathrm{Gal}(X'/Y').$$

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 localization, we may assume that $X \to Y$ is a *direct Galois cover* whose direct Galois group equals $\mathrm{Gal}(X/Y)$. Using the assumption on the generic fibers, by a further localization and 3.14 we can achieve that the fibers 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. □

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, σ) be an (A, σ)-module and let (N, σ) be a submodule.

(1) We say that (M, σ) is *well-mixed* if $am = 0$ implies $\sigma(a)m = 0$ for all $a \in A$, $m \in M$.
(2) We say that (N, σ) is a *well-mixed submodule* of (M, σ) if the module M/N is well-mixed.

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

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, σ) of (M, σ) there exists a smallest well-mixed submodule $[N]_w$ containing N. Thus $[0]_w$ is the smallest well-mixed submodule of (M, σ) associated with the largest well-mixed quotient M_w of M.

PROPOSITION 3.17. *Let (M, σ) be a well-mixed (A, σ)-module. The following are equivalent.*

(1) $M = 0$;
(2) $M_{\mathfrak{p}} = 0$ *for every* $\mathfrak{p} \in \mathrm{Spec}^{\sigma}(A)$;
(3) $M_{\mathfrak{p}} = 0$ *for every* $\mathfrak{p}$ *maximal in* $\mathrm{Spec}^{\sigma}(A)$.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

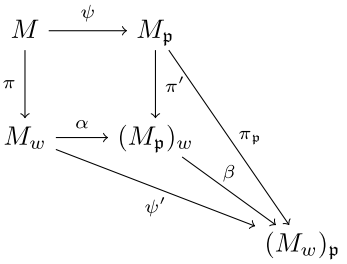
Proof. It is clear that (1) implies (2) and (2) implies (3). Suppose that (3) holds but $M \neq 0$. Let $x \in M \setminus \{0\}$ and let $\mathfrak{a} = \mathrm{Ann}(x)$. Then $\mathfrak{a} \neq (1)$ is well-mixed and, by [24, 2.21], $V^\sigma(\mathfrak{a}) \neq \emptyset$. Choose a maximal $\mathfrak{p}$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

COROLLARY 3.18. *Let (M, σ) be an (A, σ)-module. If $M_\mathfrak{p} = 0$ for every $\mathfrak{p} \in \mathrm{Spec}^\sigma(A)$, then $M_w = 0$.*

The above can be sharpened as follows.

PROPOSITION 3.19. *Let (M, σ) be an (A, σ)-module. If $(M_\mathfrak{p})_w = 0$ for every $\mathfrak{p}$ maximal in $\mathrm{Spec}^\sigma(A)$, then $M_w = 0$.*

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



in which π and π' are surjective, so we conclude that $\pi_\mathfrak{p}$ and β are also surjective. Therefore, $(M_\mathfrak{p})_w = 0$ implies that $(M_w)_\mathfrak{p} = 0$ and we finish by 3.17. □

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

(1) *ϕ is injective;*
(2) *$\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for every $\mathfrak{p} \in \mathrm{Spec}^\sigma(A)$;*
(3) *$\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for every $\mathfrak{p}$ maximal in $\mathrm{Spec}^\sigma(A)$.*

Proof. (1) ⇒ (2). If $0 \to M \to N$ is exact, since localization is exact, we get that $0 \to M_\mathfrak{p} \to N_\mathfrak{p}$ is also exact. (2) ⇒ (3) is trivial.

(3) ⇒ (1). Let $M' = \ker \phi$. Then $0 \to M' \to M \to N$ is exact so $0 \to M'_\mathfrak{p} \to M_\mathfrak{p} \to N_\mathfrak{p}$ is exact for every $\mathfrak{p} \in \mathrm{Spec}^\sigma(A)$. By assumption, $M'_\mathfrak{p} = 0$ for every

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

$\mathfrak{p} \in \mathrm{Spec}^\sigma(A)$. Since M' is well-mixed (as a submodule of M), by 3.17 we conclude that $M' = 0$. □

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

PROPOSITION 3.21. *Let $\phi : (M, \sigma) \to (N, \sigma)$ be an (A, σ)-module homomorphism. If $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is almost surjective for every $\mathfrak{p}$ maximal in $\mathrm{Spec}^\sigma(A)$, then ϕ is almost surjective.*

Proof. Let $N' = \mathrm{coker}(\phi)$. Then $M \to N \to N' \to 0$ is exact, and by localization $M_\mathfrak{p} \to N_\mathfrak{p} \to N'_p \to 0$ is exact for every $\mathfrak{p} \in \mathrm{Spec}^\sigma(A)$. By assumption, $(N'_\mathfrak{p})_w = 0$ for all $\mathfrak{p}$ maximal in $\mathrm{Spec}^\sigma(A)$ 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 $m'_j \in M$ 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, σ) and (N, σ) be (A, σ)-modules with (N, σ) 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 3.22 implies the existence of $m'_j \in M$ and $a_{ij} \in A$ such that for every i, $\sum_j a_{ij} m'_j = m_i$ and for every j, $0 = \sum_i a_{ij} bn_i = b \sum_i a_{ij} n_i$. Since the latter holds in (N, σ) 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 3.22 again, it follows that $\sigma(b) \sum_i m_i \otimes n_i = \sum_i m_i \otimes \sigma(b) n_i = 0$. □

PROPOSITION 3.24. *Let (M, σ) be a well-mixed (A, σ)-module. The following are equivalent.*

(1) *M is a flat A-module.*
(2) *$M_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module for every $\mathfrak{p} \in \mathrm{Spec}^\sigma(A)$.*
(3) *$M_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module for every $\mathfrak{p}$ maximal in $\mathrm{Spec}^\sigma(A)$.*

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

Proof. (1) ⇒ (2). Assuming (i), it is classically known that $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$ module for every prime $\mathfrak{p}$. (2) ⇒ (3) is trivial.

(3) ⇒ (1). Let $(N,\sigma)\to(P,\sigma)$ be injective. Then $N_{\mathfrak{p}}\to P_{\mathfrak{p}}$ is injective for every $\mathfrak{p}\in\operatorname{Spec}^{\sigma}(A)$. By assumption, $N_{\mathfrak{p}}\otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}\to P_{\mathfrak{p}}\otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$ is injective and thus $(N\otimes_A M)_{\mathfrak{p}}\to(P\otimes_A M)_{\mathfrak{p}}$ is injective for all $\mathfrak{p}$ maximal in $\operatorname{Spec}^{\sigma}(A)$. Since $N\otimes_A M$ is well-mixed by 3.23, Proposition 3.20 implies that $N\otimes_A M\to P\otimes_A M$ is injective. □

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

PROPOSITION 3.26. *Let (A,σ) be a transformal domain. If $A_{\mathfrak{p}}$ is normal for every $\mathfrak{p}$ maximal in $\operatorname{Spec}^{\sigma}(A)$, 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 $\phi:A\hookrightarrow C$ the inclusion. By assumption, each $\phi_{\mathfrak{p}}$ is surjective, so 3.21 implies that ϕ is almost surjective and thus $[A]_w=C$. □

DEFINITION 3.27. A difference scheme (X,Σ) 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

$$\begin{array}{ccc}(S,\sigma) & \longrightarrow & A/I\\ \uparrow & \nearrow & \uparrow\\ (R,\sigma) & \longrightarrow & (A,\sigma)\end{array}$$

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.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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,σ)-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]. □

REMARK 3.30. For a difference (R,σ)-algebra (S,σ), the module of relative differentials $\Omega_{S/R}$ naturally classifies R-derivations that commute with σ. Indeed, if we let J be the kernel of the multiplication map $S\otimes_R S\to S$, it is known that $\Omega_{S/R}\simeq J/J^2$. 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 σ 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 transformal dimension 0.

REMARK 3.32. If (B,σ) is an (A,σ)-algebra of finite σ-type, the second exact sequence for differentials implies that $\Omega_{B/A}$ is a finitely σ-generated (B,σ)-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). □

COROLLARY 3.34. *Let $(R,\sigma)\to(S,\sigma)$ be a morphism. The following are equivalent:*

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

(1) $(R,\sigma)\to(S,\sigma)$ *is almost formally unramified in the sense that* $(\Omega_{S/R})_w=0$*;*
(2) *for every* $\mathfrak{q}\in\mathrm{Spec}^\sigma(S)$ *lying over* $\mathfrak{p}=\mathfrak{q}\cap R$, $(R_\mathfrak{p},\sigma)\to(S_\mathfrak{q},\sigma)$ *is formally unramified;*
(3) *for every* $\mathfrak{q}\in\mathrm{Spec}^\sigma(S)$ *lying over* $\mathfrak{p}=\mathfrak{q}\cap R$, $R_\mathfrak{p}\to S_\mathfrak{q}$ *is formally unramified.*

Proof. Straightforward from 3.19 applied to the (S,σ)-module $\Omega_{S/R}$. □

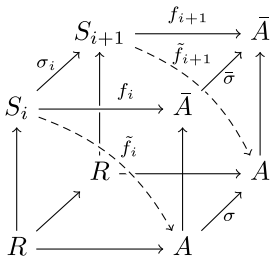
COROLLARY 3.35. *A morphism* $(R,\sigma)\to(S,\sigma)$ *is formally étale if and only if* $R\to S$ *is formally étale.*

Proof. If $(R,\sigma)\to(S,\sigma)$ is formally étale, it is both formally smooth and formally unramified. By 3.29, $R\to S$ is formally smooth, and by 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. □

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

PROPOSITION 3.37. *If* $(R,\sigma)\to(S,\sigma)$ *is* σ*-pro-étale, then* $(R,\sigma)\to(S,\sigma)$ *is étale.*

Proof. Assuming that (S,σ) is σ-pro-étale over (R,σ), 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,σ) is the direct limit of the S_i and the σ_i, as in Subsection 3.1, where all $R\to S_i$ are étale. Suppose we have a situation from 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



where f_i denotes the restriction of f to S_i. The dashed arrows represent the unique lifts $\tilde{f}_i: S_i\to A$ of f_i. Since both $\tilde{f}_{i+1}\sigma_i$ and $\sigma\tilde{f}_i$ are lifts of

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

$f_{i+1}\sigma_i = \bar{\sigma} f_i$, by étaleness of $R \to S_i$ we deduce that $\tilde{f}_{i+1}\sigma_i = \sigma \tilde{f}_i$, which yields a unique lift $\tilde{f} : (S, \sigma) \to (A, \sigma)$ of f in the limit. □

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 neighborhood on which f is modeled 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 $\mathfrak{q} \in \mathrm{Spec}^{\sigma}(S)$ lying over $\mathfrak{p} = \mathfrak{q} \cap R$, then there is a $g \notin \mathfrak{q}$ such that the σ-localization $(R, \sigma) \to (S_g, \sigma)$ is unramified (resp. étale).

The above "openness" statement for the property of being unramified is obvious from 3.33 and 3.32. For étaleness, it follows from 3.32 and the *Jacobian criterion* for smoothness which states the following. Let (A, σ) be a difference ring, (B, σ) a formally smooth (A, σ)-algebra, J a reflexive difference ideal of B and let $C = B/J$. Then (C, σ) is a formally smooth (A, σ)-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 3.8 with 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 quasifiniteness or finiteness, and we make every effort to explicitly state them when possible.

Suppose $(G, \tilde{\Sigma})$ acts on (X, Σ). For $x \in X$, the *decomposition group* at x is the stabilizer $G_d(x) = G_x$ of x. With the notation of 2.22, $(G_d(x), \tilde{\Sigma}_x)$ acts on $(\mathbf{k}(x), \Sigma^x)$ and the *inertia group* $G_i(x)$ at x is the set of elements of $G_d(x)$ which act trivially on $\mathbf{k}(x)$.

If $(X, \Sigma) \to (Y, T)$ is a Galois cover with group $(G, \tilde{\Sigma})$, and (F, φ) 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 stabilizer of $\bar{x}$ in G is exactly the inertia group $G_i(x)$.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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, σ) with group $(G, \tilde{\Sigma})$. 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 2.22. Suppose $X = \mathrm{Spec}^{\Sigma}(A)$ and that $(G, \tilde{\Sigma})$ acts on (A, Σ). 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 $A_n = k[\bar{a}, \sigma\bar{a}, \ldots, \sigma^n\bar{a}]$, and we can form $B_n = A_n^G$. We have $A = \varinjlim_n A_n$ and $B = A^G = \varinjlim_n B_n$ 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 Σ-fixed points of the ambient Galois cover $\varprojlim_n X_n \to \varprojlim_n Y_n$. 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, Σ) is integral and that $(G, \tilde{\Sigma})$ 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 $\mathbf{k}(x) = \mathbf{k}(p(x))$. 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 $\mathcal{O}_{p(x)} \to \mathcal{O}_x$ and shows that $G = (e)$. □

DEFINITION 3.42. A difference scheme (X, Σ) is *faithful* if Σ 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, Σ) is also faithful.*

Thus, if $(X, \Sigma) \to (Y, \sigma)$ is an étale Galois cover of a strict difference scheme, then (X, Σ) is automatically faithful. Since most generalized 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.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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

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

In other words, if a is localized at $x \in X$, then φ_a is the element of Σ_x corresponding (via the conclusion of 2.22(3)) to the image φ^a of φ by the morphism of difference structure $()^a : \{\varphi\} \to \Sigma^x$. Note, when we have a Galois cover $\pi : (X, \Sigma) \to (Y, T)$ of faithful difference schemes with group $(G, \tilde{\Sigma})$, and $\pi(a) = \pi(a') = b \in Y(F, \varphi)$, there exists a $g \in G$ with $a' = ga$ and

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

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

DEFINITION 3.44. The *local φ-substitution at b* is the G-conjugacy class $\varphi_b = \varphi_b^{X/Y}$ of any φ_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 $\tilde{\sigma} \in \Sigma$ for the image of $\varphi^b \in \Sigma_0$, we define the *twisted* local φ-substitution at $a \in X(F, \varphi)$ with $\pi(a) = b$, to be the unique element $\dot{\varphi}_a \in G_d(x)$ with the property

$$\dot{\varphi}_a \tilde{\sigma} a = a\varphi.$$

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

$$\dot{\varphi}_a \tilde{\sigma} = g^{-1}\dot{\varphi}_{a'}\tilde{\sigma}g = g^{-1}\dot{\varphi}_{a'}\,{}^{\tilde{\sigma}}g\,\tilde{\sigma},$$

so we can make the following definition.

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

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

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 $\mathrm{Gal}(\bar{k}/k)$, 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 Σ, or $\dot{\varphi}_{k,b}$ when considered as a twisted conjugacy class in G.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

3.5 Transformal separability

The following definition generalizes the notion of σ-separable extensions of difference fields from [18] and [9].

DEFINITION 3.46.

(1) An algebra (A, Σ) over a difference field (k, σ) is Σ-separable, if $(A, \Sigma) \otimes_{(k,\sigma)} (k', \sigma)$ is Σ-reduced/strong for every difference field extension (k', σ) of (k, σ).
(2) A morphism $(X, \Sigma) \to (Y, \sigma)$ of finite transformal type is *transformally separable*, if every fiber X_y is a finite union of difference spectra of transformally separable $(\mathbf{k}(y), \sigma^y)$-algebras, for $y \in Y$.
(3) A difference field extension (L, Σ) of (k, σ) is *τ-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 *Σ-radicial*, if it is τ-radicial for every $\tau \in \Sigma$.
(4) A morphism $f : (X, \sigma) \to (Y, \sigma)$ is *σ-radicial* if it is injective as a map of topological spaces, and for every $x \in X$, the difference field extension $(\mathbf{k}(f(x)), \sigma^{f(x)}) \to (\mathbf{k}(x), \sigma^x)$ is transformally radicial.

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

Proof. A subextension (E, σ) is σ-separable over k if and only if it is linearly disjoint from the inversive closure of k^{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^{inv} over k, that is, such that L_0 is σ-separable over k. □

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

REMARK 3.49. Let $(k, \sigma) \to (L, \Sigma)$ be a difference field extension with L/k Galois. In view of 2.21, L is τ-separable (resp. τ-radicial) over k for some $\tau \in \Sigma$ if and only if L is Σ-separable (resp. Σ-radicial) over k.

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

Proof. By [4, Corollary 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^{inv} is algebraic

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

over k^{inv}. Hence, given that L is linearly disjoint from k^{inv}, we deduce that L s free from L_0^{inv} over L_0, so [4, Corollary 1, A.V.137] yields that L is linearly disjoint from L_0^{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 $\psi : \Sigma \to T$ be a *Diff*-morphism. The *pullback* of Y with respect to ψ is defined as

$$\psi^* Y = \bigcup_{\sigma \in \Sigma} Y^{\psi(\sigma)},$$

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

$$\psi^* Y \to Y.$$

DEFINITION 4.2. Let (X_0, Σ_0) be a difference scheme and let $\iota : \Sigma_0 \hookrightarrow \Sigma$ be an inclusion of almost-strict difference structures, that is, $\Sigma_0 = H\sigma$, $\Sigma = G\sigma$, and we have a homomorphism ${}^{\sigma}(\,) : G \to G$, so that H is a subgroup of G with ${}^{\sigma}(H) = H$. Note that in this geometric situation, we have properties dual to those of 2.5(3), namely $\sigma g = {}^{\sigma} g \sigma$ and ${}^{(h\sigma)}(g\sigma) = h\, {}^{\sigma}(gh^{-1})\sigma$, for $g, h \in G$.

For $\sigma_i = g_i \sigma \in \Sigma$, $i = 0, 1, 2$, we introduce the notation

$$\sigma_0^{\sigma_1, \sigma_2} = g_1^{-1} g_0\, {}^{\sigma} g_2\, \sigma.$$

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 τ_i, there is a unique τ_j with $\tau^{\tau_j, \tau_i} \in \Sigma_0$. 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 $\tau^{\tau_{\bar{\tau}(i)}, \tau_i} \in \Sigma_0$ on the associated copy of X_0. In view of the fact that $\bar{\tau}(i) = i$ if and only if $\tau^{\tau_i, \tau_i} = \tau^{g_i} \in \Sigma_0$, the underlying space of the (coproduct) pushforward is

$$\iota_* X_0 = \bigcup_{\tau \in \Sigma} \Big(\coprod_{i \in I} X_i \Big)^{\tau} = \coprod_i \bigcup_{\tau^{g_i} \in \Sigma_0} X_0^{\tau^{g_i}},$$

and the action of Σ is inherited from $\coprod_{i \in I} X_i$.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

There is a natural (inclusion) morphism

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

DEFINITION 4.3. Let (X_0, Σ_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, which can be identified with X_0^I, the space of functions $f : I \to \coprod_{i \in I} X_i$ with the property $f(i) \in X_i$. The action is defined via

$$(\tau f)(\bar{\tau}(i)) = \tau^{\tau_{\bar{\tau}(i)}, \tau_i}(f(i)).$$

The underlying space of the (product) pushforward is

$$\iota_! X_0 = \bigcup_{\tau \in \Sigma} \Big(\prod_{i \in I} X_i \Big)^{\tau},$$

and the action of Σ 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 Σ, recall [24, 2.6].

DEFINITION 4.4. Let (X, Σ) be a difference scheme and let $\pi : \Sigma \to T$ be a *Diff*-morphism such that there exists a finite group K acting faithfully on Σ such that π 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, Σ) be a difference algebra over a difference field (k, φ). 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.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

DEFINITION 4.6. Let (X, Σ) 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, $\psi = \psi_1 \circ \cdots \psi_n$. We define

$$\psi_* X = \psi_{1*} \cdots \psi_{n*} X \quad \text{and} \quad \psi_! X = \psi_{1!} \cdots \psi_{n!} X.$$

THEOREM 4.7. *Let $\psi : \Sigma \to T$ be a Diff-morphism as in 4.6.*

(1) *The functor ψ_* is left adjoint to ψ^*, that is,*

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

functorially in (X, Σ) and (Y, T).

(2) *The functor $\psi_!$ is right adjoint to ψ^*, that is,*

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

functorially in (X, Σ) and (Y, T).

Proof. **(1)** Suppose we have a difference scheme (X, Σ) and $\iota : \Sigma_0 \hookrightarrow \Sigma$ satisfies the assumptions of 4.2. Writing $(X_0, \Sigma_0) = \iota^* X$ and adopting the above notation, there is a natural morphism $\iota_* \iota^* X \to X$, induced by the morphism $\coprod_i X_i \to X$, taking the ith copy of X_0 to $g_i(X_0)$. Since $\iota^* \iota_* Y$ is a disjoint union of copies of (Y, Σ_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, $\pi_* \pi^* \to 1$ 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, Σ_0), a natural morphism $\iota^* \iota_! Y \to Y$ is the projection on the first factor, $\iota^* \iota_! Y$ being a direct product of copies of (Y, Σ). It is just a formality to verify that the resulting adjunctions

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

are as required. □

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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, Σ) and a morphism $X_0 \to \iota^* Y$. We carry out an analogous construction on the fiber product of the X_i over Y, where $X_i = X_0 \times_Y Y$ as in the diagram

$$\begin{array}{ccccc} X_i & \longrightarrow & & & Y \\ \downarrow & & & & \downarrow{\scriptstyle \tau_i} \\ X_0 & \longrightarrow & \iota^* Y & \longrightarrow & Y \end{array}$$

which yields a difference scheme $(\iota_!(X_0/Y), \Sigma)$ satisfying

$$\mathrm{Hom}_{(\iota^* Y, \Sigma_0)}(\iota^* Z, X_0) \simeq \mathrm{Hom}_{(Y,\Sigma)}(Z, \iota_!(X_0/Y)),$$

for any difference scheme (Z, Σ) over (Y, Σ).

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 *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 Nonabelian difference Galois cohomology

DEFINITION 5.1. Let (G, Σ) be a difference group. Recall (2.17), for every $\sigma \in \Sigma$ we have a group endomorphism $()^\sigma : G \to G$ 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

$$b(\sigma) = g^\sigma \, a(\sigma) g^{-1}.$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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 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 $(K, \Sigma_0) \to (L, \Sigma)$ be a separable quasi-Galois extension with a surjective structure morphism $\pi : \Sigma \to \Sigma_0$ and let $G = \mathrm{Gal}(L/K)$. The morphism π extends to the set $\hat{\Sigma}$ consisting of all lifts of elements of Σ_0 to L by the rule $\pi(\sigma) = \sigma \restriction K$.

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 $()^\tau : G \to G$ such that

$$g\tau = \tau g^\tau,$$

which makes G into a *Diff*-group (G, Σ).

Suppose now (L, Σ') is another extension of (K, Σ_0), with $(\Sigma' \subseteq \hat{\Sigma})$ and let $\iota : \Sigma \to \Sigma'$ be a surjective *Diff*-morphism with the property $\pi\iota = \pi$. It is easily verified that maps $a : \Sigma \to G$ satisfying

$$\iota(\sigma) = \sigma a(\sigma)$$

correspond to cocycles, and that cocycles a_1, a_2 corresponding to isomorphic extensions (L, Σ_1), (L, Σ_2) of (K, Σ_0) are cohomologous. We draw the following conclusion.

REMARK 5.4. The cohomology set $H^1(\Sigma, \mathrm{Gal}(L/K))$ classifies the above family of difference field extensions of (K, Σ_0) up to isomorphism.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

5.2 Benign extensions and Babbitt's theorem

DEFINITION 5.5. A morphism $(S,\sigma)\to(R,\sigma)$ of difference rings is called *benign* if there exists a quasifinite $S\to R_0$ such that (R,σ) is isomorphic to $[\sigma]_S R_0$ over (S,σ). In other words, writing $R_{i+1}=R_i\otimes_S S$ for $i\geqslant 0$ (where the morphism $S\to S$ is σ), (R,σ) is the (limit) tensor product of the R_i and the canonical morphisms $\sigma_i: R_i\to R_{i+1}$ over S. The morphism is *proper benign* if, in addition, 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 $\mathrm{Gal}(R/S)=\mathrm{Gal}(\mathbf{k}(R)/\mathbf{k}(S))=(G,()^\sigma)$ is isomorphic to the direct product of $G_i=\mathrm{Gal}(R_i/S)$ and $()^\sigma$ "shifts" from G_i to G_{i+1}.

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

LEMMA 5.6. *The (nonabelian) difference cohomology* $H^1(()^\sigma,G)=1$.

LEMMA 5.7. *If R is proper benign over S, then for any $y\in\mathrm{Spec}^\sigma(S)$, any algebraically closed difference field (F,φ) extending $(\mathbf{k}(y),\sigma^y)$, 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 5.6 and 5.4, all $(R,\sigma g)$, $g\in G$ are isomorphic over (S,σ), so it suffices to treat the case of (R,σ).

Let R_i be as in 5.5. By the integrality assumption, all the R_i are finite over S. Let $\bar{y}:(S,\sigma)\to(F,\varphi)$. Since R_0 is finite over S and F is algebraically closed, we can find some $\bar{x}_0: R_0\to F$ above $\bar{y}$. By the universal property 3.1 of $R=[\sigma]_S R_0$, there exists an $\bar{x}:(R,\sigma)\to(F,\sigma)$ extending $\bar{x}_0$ and consequently $\bar{y}$. □

DEFINITION 5.8.

(1) A morphism $(\psi,()^\psi):(S,T)\to(R,\Sigma)$ of almost-strict difference rings is *benign* if for some (or equivalently, for all) $\sigma\in\Sigma$, the morphism $(S,\sigma^\psi)\to(R,\sigma)$ is benign.
(2) A morphism $(X,\Sigma)\to(Y,T)$ of almost-strict difference schemes is *benign* if it is affine and above each open affine subset of Y it is modeled by a fixed-point spectrum of a benign morphism of rings.
(3) In the situation of (2), the morphism is *proper benign*, if the relevant difference ring extensions are proper benign.

An immediate consequence of 5.7 is the following.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

LEMMA 5.9. *Let $(X, \Sigma) \to (Y, T)$ be a proper benign Galois morphism. For any $\tau \in T$ and $\sigma \in \Sigma$ mapping to τ, any $y \in Y^\tau$, any algebraically closed difference field (F, φ) extending $(\mathbf{k}(y), \tau^y)$, 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, Σ_1) and (X_2, Σ_2) are called *equivalent*, written $(X_1, \Sigma_1) \simeq (X_2, \Sigma_2)$, if they have isomorphic inversive closures, $(X_1^{\mathrm{inv}}, \Sigma_1^{\mathrm{inv}}) \cong (X_2^{\mathrm{inv}}, \Sigma_2^{\mathrm{inv}})$.

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 σ-separable quasi-Galois extension of finite σ-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 benign for $i \geqslant 0$.

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

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

It is known that $\tilde{L}_0$ is inversive, so using the above remark for $F = \tilde{L}_0$, we deduce that $\tilde{L}_0 = L_K$, the core of K in L. Bearing in mind that $L \simeq \tilde{L}$, 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 σ-separable morphism of finite transformal type $(X, \Sigma) \to (Y, T)$ of transformally 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 $i \geqslant 0$, $(X_{i+1}, \Sigma_{i+1}) \to (X_i, \Sigma_i)$ is benign Galois. Modulo a transformal localization

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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 benign Galois.

Proof. By applying Babbitt's theorem 5.11 to the extension of difference function fields $(\mathbf{k}(Y), \tau) \to (\mathbf{k}(X), \sigma)$ for a suitable choice of σ and τ we obtain a tower of difference field extensions

$$(\mathbf{k}(Y), \tau) \to (L_0, \sigma) \to (L_1, \sigma) \cdots \to (L_n, \sigma) \simeq (\mathbf{k}(X), \sigma),$$

where $L_0/\mathbf{k}(Y)$ is finite and each $(L_{i+1}, \sigma)/(L_i, \sigma)$ is benign for $i \geqslant 0$. We let Σ_i be the *Diff*-structure obtained as a restriction of Σ from L_n to L_i. Let (X_i, Σ_i) be the normalization of (Y, T) in (L_i, Σ_i). It is clear from [24, 2.56] that by a transformal localization 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. □

LEMMA 5.13. *Let (R, σ) be a normal transformal domain with fraction field (K, σ) 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 $L_i = \sigma^i(L_0)$ where L_0 is a fraction field of an étale R-algebra A_0. Then the normalization 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. □

5.3 Galois closure

LEMMA 5.14. *Let $(K, \sigma) \to (L, \sigma) \to (F, \bar{\sigma})$ 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 $\bar{\sigma}(\tilde{L}) \subseteq \tilde{L}$ and $(\tilde{L}, \tilde{\sigma})$ is a difference field extension of (L, σ), where $\tilde{\sigma} = \bar{\sigma} \restriction_{\tilde{L}}$.*

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 α_0 over K splits as $f(t) = (t - \alpha_0)(t - \alpha_1) \cdots (t - \alpha_n)$, for $\alpha_i \in \tilde{L}$, and α is one of the α_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 $\tilde{\alpha}_i$ are its conjugates and therefore they lie in $\tilde{L}$. □

REMARK 5.15. Cohn remarks in [7, Chapter 7, no. 16] that the algebraic closure $\bar{L}$ of L can always be equipped with an endomorphism $\tilde{\sigma}$ so that $(\bar{L}, \tilde{\sigma})$ extends (L, σ). Thus (considering $(\bar{L}, \bar{\sigma})$ in the role of $(F, \bar{\sigma})$ above),

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

the quasi-Galois closure $\tilde{L}$ can always be made (noncanonically) into a difference field extension of (L, σ).

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

$$\begin{array}{ccc} (\tilde{L}, \mathring{\Sigma}) & \longleftarrow & (\tilde{L}, \Sigma) \\ \uparrow & & \uparrow \\ (L, \sigma) & \nwarrow & \\ & & (K, \sigma) \end{array}$$

is called the *Galois closure* of (L, σ) over (K, σ), where Σ is the set of all lifts of σ from K to $\tilde{L}$, and $\mathring{\Sigma} \subseteq \Sigma$ is the set of all lifts of σ from L to $\tilde{L}$. In fact, $\Sigma = \tilde{\sigma}\mathrm{Gal}(\tilde{L}/K)$, and $\mathring{\Sigma} = \tilde{\sigma}\mathrm{Gal}(\tilde{L}/L)$.

PROPOSITION 5.17. (The universal property of Galois closure) *Let (L, σ) be a separable extension of (K, σ), and suppose (F, Σ_F) is Galois over (K, σ) such that there is a $\bar{\sigma} \in \Sigma_F$ with $(F, \bar{\sigma})$ extending (L, σ). Then there are extensions $(\tilde{L}, \Sigma) \to (F, \Sigma_F)$ and $(\tilde{L}, \mathring{\Sigma}) \to (F, \mathring{\Sigma}_F)$, where $\mathring{\Sigma}_F = \{\tau \in \Sigma_F : \tau \restriction_L = \sigma\}$.*

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 $\bar{\sigma} \restriction_L = \sigma$. By 5.14, $\tilde{\sigma} = \bar{\sigma} \restriction_{\tilde{L}} \in \mathring{\Sigma}$, and we know that $\Sigma = \tilde{\sigma}\mathrm{Gal}(\tilde{L}/K)$, $\Sigma_F = \bar{\sigma}\mathrm{Gal}(F/K)$ and that

$$1 \to \mathrm{Gal}(F/\tilde{L}) \to \mathrm{Gal}(F/K) \to \mathrm{Gal}(\tilde{L}/K) \to 1$$

is exact, so the restriction map $\Sigma_F \to \Sigma$ is onto, giving the inclusion $(\tilde{L}, \Sigma) \to (F, \Sigma_F)$. Similarly we get the inclusion $(\tilde{L}, \mathring{\Sigma}) \to (F, \mathring{\Sigma}_F)$. □

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

$$\begin{array}{ccc} \mathring{\tilde{X}} & \longrightarrow & \tilde{X} \\ \downarrow & & \downarrow \\ X & \searrow & Y \end{array}$$

in which the vertical arrows are Galois covers.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

5.4 Ampleness of finite difference structures

A geometric motivation for the study of generalized 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 σ to L. Even in the common case where L is algebraic of finite σ-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*

$$H^1((\,)^\sigma,\mathrm{Gal}(L/L_0))=1.$$

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, $H^1((\,)^\sigma,\mathrm{Gal}(L_{i+1}/L_i))=1$ for all $i\geqslant 0$. It is straightforward now to prove that $H^1((\,)^\sigma,\mathrm{Gal}(L_i/L_0))=1$ by induction, using the long exact sequence for difference cohomology associated with the short exact sequence

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

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

If $g\in\mathrm{Gal}(L^{\mathrm{inv}}/L)^\sigma$, then also $g^{\sigma^r}=g$ for every r. For $x\in L^{\mathrm{inv}}$, 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 $\mathrm{Gal}(L^{\mathrm{inv}}/L)^\sigma=1$.

Using the fact that $L^{\mathrm{inv}}=L_n^{\mathrm{inv}}$, the cohomology long exact sequence (extended by 5.3) associated with

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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

becomes

$$1 \to 1 \to \mathrm{Gal}(L_1^{\mathrm{inv}}/L_0)^\sigma \to \mathrm{Gal}(L/L_0)^\sigma \to \\ \to H^1(()^\sigma, L^{\mathrm{inv}}/L) \to 1 \to H^1(()^\sigma, L/L_0) \to 1,$$

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

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

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

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

Moreover, the set of isomorphism classes of all lifts of σ from K to L is in one-to-one correspondence with the set of isomorphism classes of lifts of σ from K to L_0 and G_1 can be chosen so that σG_1 contains a set of representatives for those isomorphism classes.

Proof. The assumption that L is σ-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 $H = \mathrm{Gal}(L_1/L_0)$, $G = \mathrm{Gal}(L_1/K)$, $G_0 = \mathrm{Gal}(L_0/K)$, and let us denote by Φ the operator $()^{\sigma^n} : G \to G$, where n is the order of $()^\sigma$ on G_0.

Using 5.19, we get that $H^1(()^\sigma, H) = 1$ and $H^1(\Phi, H) = 1$ so the long exact sequences (from 5.3) for (nonabelian) difference cohomology become

$$1 \to H^\sigma \to G^\sigma \to G_0^\sigma \to 1 \to H^1(()^\sigma, G) \to H^1(()^\sigma, G_0) \to 1 \tag{1}$$

and

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

Since H^Φ is finite, (2) implies that G^Φ is a finite subgroup of G that maps onto G_0. But (1) shows that $H^1(()^\sigma, G) \cong H^1(()^\sigma, G_0)$ and thus G^Φ also maps onto $H^1(()^\sigma, G)$, which proves the "moreover" clause by 5.4. □

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

DEFINITION 5.21. Let $(K,T)\to(F,\Sigma)$ be an extension of difference fields with finite structures T and Σ, and let (L,Σ) 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 Σ 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 σ-separable extension of difference fields of finite σ-type. Let $(\tilde{L},\Sigma)$ be the Galois closure of (L,σ) over (K,σ) as in 5.16. Note that Σ 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 σ from K to $\tilde{L}$, and we let $\mathring{\Sigma}_0=\{\tau\in\Sigma_0:\tau\restriction_L=\sigma\}$. Then $(K,\sigma)\to(\tilde{L},\Sigma_0)$ and $(L,\sigma)\to(\tilde{L},\mathring{\Sigma}_0)$ are weak difference covers and the associated diagram is called the *weak Galois closure* of (L,σ) over (K,σ).

DEFINITION 5.23. Let $(X,\Sigma)\to(Y,T)$ be a dominant morphism of transformally integral difference schemes. We shall say that it is a *generic weak cover* if the corresponding inclusion of function fields $(\mathbf{k}(Y),T)\to(\mathbf{k}(X),\Sigma)$ is a weak difference cover of fields.

DEFINITION 5.24. Let $(X,\sigma)\to(Y,\sigma)$ be a generically étale σ-separable morphism of transformally integral normal difference schemes, and denote by $(K,\sigma)\to(L,\sigma)$ the corresponding extension of function fields, let $(\tilde{L},\Sigma_0)$ and $\mathring{\Sigma}_0$ be as in 5.22, and write $\iota:\mathring{\Sigma}_0\hookrightarrow\Sigma_0$. Let $(\tilde{X},\Sigma_0)$ be the normalization of Y in $(\tilde{L},\Sigma_0)$. We obtain a diagram

$$\begin{array}{ccc}\iota^*\tilde{X} & \longrightarrow & \tilde{X}\\ \downarrow & & \downarrow\\ X & \searrow & Y\end{array}$$

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*

$$\begin{array}{ccc}X_0 & \longrightarrow & \tilde{X}\\ \downarrow & & \downarrow\\ X & \searrow & Y\end{array}$$

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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

Proof. Let (L, σ) be the relative algebraic closure of $\mathbf{k}(Y)$ inside $\mathbf{k}(X)$, and let $\bar{Y}$ be the normalization 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 $\iota^*\tilde{Y}$ of $\bar{Y}$ over Y, and let $(X_0, \Sigma_0) = (X, \sigma) \times_{(Y,\sigma)} (\iota^*\tilde{Y}, \Sigma_0)$. The diagram obtained using 4.8

$$\begin{array}{ccccc} X & \longleftarrow & X_0 & \longrightarrow & \iota_!(X_0/\tilde{Y}) \\ \downarrow & & \downarrow & & \downarrow \\ \tilde{Y} & \longleftarrow & \iota^*\tilde{Y} & \longrightarrow & \tilde{Y} \\ & \searrow & \downarrow & \swarrow & \\ & & Y & & \end{array}$$

shows the required statement with $\tilde{X} = \iota_!(X_0/\tilde{Y})$ in a very explicit way. □

§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.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

DEFINITION 6.1. A ring (R, σ) is said to be *effectively presented*, if it has a finite σ-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 σ-primes, that is, find an irredundant decomposition $\{I\}_\sigma = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ (as in [24, 2.45]).

($\dagger_2$) Given an extension $(K, \sigma) \to (L, \sigma)$ of effectively presented difference fields of finite σ-type, compute the relative algebraic closure of K in L.

($\dagger_3$) In the situation of ($\dagger_2$), compute a decomposition into a σ-separable and σ-radicial part as in 3.47.

($\dagger_4$) Given an σ-separable Galois extension $(K, \sigma) \to (L, \sigma)$ of effectively presented difference fields of finite σ-type, compute its Babbitt's decomposition (as in 5.11).

($\dagger_5$) For an effectively presented integrally closed domain (R, σ) with fraction field (K, σ), and an extension (L, σ) of (K, σ) of finite σ-type, find the integral closure (S, σ) of R in L, and compute the σ-localization (R', σ) of R so that the corresponding S' is of finite σ-type over R' [24, 2.56].

($\dagger_6$) 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 σ-pro-P, compute the σ-localizations R' of R and S' of S such that $(R', \sigma) \to (S', \sigma)$ is σ-pro-P (in particular, we need effective versions of 3.8, 3.14 and 3.9).

($\dagger_7$) Given an algebraic extension $(K, \sigma) \to (L, \sigma)$ of effectively presented difference fields of finite σ-type, compute the quasi-Galois closure of L over K.

($\dagger_8$) 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.

($\dagger_9$) Effective Twisted Lang–Weil estimate. In the situation of [24, 4.2], compute explicitly the constant C and the localization S' of S.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

DEFINITION 6.2. We define †-*primitive recursive functions* as functions primitive recursive reducible to basic operations in Difference Algebraic Geometry as detailed by the following axioms.

Basic †-primitive recursive functions are:

(1) *Constant* functions, *Successor* function S, coordinate *Projections*;
(2) Elementary operations in *difference algebraic geometry* ($\dagger_1$)–($\dagger_9$).

More complex †-primitive recursive functions are built using:

(3) *Composition.* If f is an n-ary †-primitive recursive function, and $g_1, \ldots, g_n$ are m-ary †-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 †-primitive recursive.

(3) *Primitive recursion.* Suppose f is an n-ary and g is an $(n+2)$-ary †-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 †-primitive recursive.

REMARK 6.3. The operations ($\dagger_6$)–($\dagger_9$) 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 ($\dagger_6$) is primitive recursive will follow from the existence of the classical primitive recursive procedure for finding a localization satisfying the property P at the start of the prolongation sequence.

The operation ($\dagger_7$) is primitive recursive because the construction of quasi-Galois closure is primitive recursive in the algebraic case. Indeed, if $L = K(a_1, \ldots, a_n)_\sigma$, and $K(b_1, \ldots, b_m)$ is the quasi-Galois closure of $K(a_1, \ldots, a_n)$, then $K(b_1, \ldots, b_m)_\sigma$ is the quasi-Galois closure of L.

Since the operation ($\dagger_8$) only deals with finite Galois extensions, it follows that it is primitive recursive by the discussion in [14].

Regarding ($\dagger_9$), 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 ($\dagger_1$)–($\dagger_5$) are primitive recursive. The notions of *primitive recursive* and †-*primitive recursive* coincide.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

§7. Galois stratification

7.1 Galois stratifications and Galois formulas

DEFINITION 7.1. Let (X, σ) be an (S, σ)-difference scheme. It is often useful to consider its *realization functor* $\tilde{X}$. For each $s \in S$ and each algebraically closed difference field (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

$$\tilde{X}(s, (F, \varphi)) = X_s(F, \varphi).$$

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

$$\mathcal{F}(s, (F, \varphi)) \subseteq X_s(F, \varphi),$$

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

DEFINITION 7.2. Let (S, σ) be a difference scheme and let (X, σ) be a difference scheme over (S, σ). A *normal (twisted) Galois stratification*

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

of (X, σ) over (S, σ) is a partition of (X, σ) into a finite set of transformally integral normal σ-locally closed difference (S, σ)-subvarieties (X_i, σ) of (X, σ), 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 Σ_i.

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

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

$$\tilde{\mathcal{A}}(s, (F, \varphi)) = \mathcal{A}_s(F, \varphi) = \bigcup_i \{x \in X_{i,s}(F, \varphi) \mid \varphi_x^{Z_i/X_i} \subseteq C_i\},$$

where $\varphi_x^{Z_i/X_i}$ denotes the local φ-substitution at x (see 3.44).

It can be beneficial to think of the Galois formula associated with $\mathcal{A}$ and a given *parameter* $s \in S$ as of the formal expression

$$\theta(t; s) \equiv \{t \in X_s \mid \mathrm{ar}(t) \subseteq \mathrm{con}(\mathcal{A})\},$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

whose *interpretation* in any given (F, φ) extending $(\mathbf{k}(s), \sigma^s)$ is given above. Namely, the "Artin symbol" $\mathrm{ar}(t)$ of a point $x \in X_{i,s}(F, \varphi)$ is interpreted as $\mathrm{ar}(x) = \varphi_x$, the local φ-substitution at x with respect to the cover Z_i/X_i, and $\mathrm{con}(\mathcal{A})$ at x becomes the appropriate C_i.

REMARK 7.4. If we fix a lift $\sigma_i \in \Sigma_i$ of σ for each i as in 3.45, the above data is equivalent to fixing for each i a ${}^{\sigma_i}()$-conjugacy domain $\dot{C}_i$ in G_i, that is, a union of ${}^{\sigma_i}()$-conjugacy classes in G_i. This justifies the adjective "twisted" used alongside "stratification". Clearly,

$$\mathcal{A}_s(F, \varphi) = \bigcup_i \{x \in X_{i,s}(F, \varphi) \mid \dot{\varphi}_x^{Z_i/X_i} \subseteq \dot{C}_i\}.$$

DEFINITION 7.5. Let $f : (X, \sigma) \to (Y, \sigma)$ be an (S, φ)-morphism, let $\mathcal{A} = \langle X, Z_i/X_i, C_i\rangle$ be an (S, σ)-Galois stratification on X and let $\mathcal{B} = \langle Y, W_j/Y_j, D_j\rangle$ be an (S, σ)-Galois stratification on Y.

(1) Given étale Galois (S, φ)-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 *Diff*-morphisms, the *inflation of* $\mathcal{A}$ *with respect to covers* Z_i'/X_i is defined as

$$\mathcal{A}' = \langle X, Z_i'/X_i, \pi_i^{-1}(C_i)\rangle.$$

It has the property that for every $s \in S$, and every algebraically closed (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

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

(2) Suppose we are given a further stratification of each X_i into finitely many integral, normal, locally closed (S, σ)-subschemes 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, σ) with group $(D_{ij}, \tilde{\Sigma}_{ij})$.
The *refinement of* $\mathcal{A}$ *to the stratification* $\{X_{ij}\}$ *of* X is defined as

$$\mathcal{A}' = \langle X, Z_{ij}/X_{ij}, \iota_{ij}^{-1}(C_i)\rangle.$$

It has the property that for every $s \in S$, and every algebraically closed (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

(3) Let Z_j be a component of $(X,\sigma)\times_{(Y,\sigma)}(W_j,T)$, 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 $\iota_j:T_{Z_j}\hookrightarrow T_j$. Then $(Z_j,T_{Z_j})\to(X_j,\sigma)=f^{-1}(Y_j)$ is a Galois cover with group $(D_{Z_j},\tilde{T}_{Z_j})$.
The *pullback* $f^*\mathcal{B}$ of $\mathcal{B}$ with respect to f is defined as a refinement of

$$\langle X, Z_j/X_j, \iota_j^{-1}(D_j)\rangle$$

to a normal refinement (noncanonical, 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,φ) extending $(\mathbf{k}(s),\sigma^s)$,

$$f^*\mathcal{B}_s(F,\varphi)=f_s^{-1}(\mathcal{B}_s(F,\varphi)).$$

DEFINITION 7.6. Let (X,σ) be an (S,σ)-difference scheme. The class of (S,σ)-Galois formulas on X has a *Boolean algebra* structure as follows.

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

For Galois formulas on X given by $\mathcal{A}$ and $\mathcal{B}$, upon a refinement and an inflation we may assume that $\mathcal{A}=\langle X,Z_i/X_i,C_i\rangle$ and $\mathcal{B}=\langle X,Z_i/X_i,D_i\rangle$, with $C_i,D_i\subseteq\Sigma_i$.

(2) $\mathcal{A}\wedge\mathcal{B}=\langle X,Z_i/X_i,C_i\cap D_i\rangle$.

(3) $\mathcal{A}\vee\mathcal{B}=\langle X,Z_i/X_i,C_i\cup D_i\rangle$.

(4) $\neg\mathcal{A}=\langle X,Z_i/X_i,\Sigma_i\setminus C_i\rangle$.

7.2 Direct image theorems

The following result can be considered as a difference 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 $f:(X,\Sigma)\to(Y,T)$ be a generic weak cover of finite transformal type. Then $f(X)$ contains a dense open subset of Y. If f is effectively 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 factorize f as a composite of a radicial (purely inseparable), σ-radicial and a separable σ-separable morphism. The cases of radicial or σ-radicial f are dealt with using 3.48, so we reduce to the case of separable σ-separable f. In the effective situation, this requires ($\dagger_3$).

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

By σ-localizing (3.8), we may assume that f is a σ-pro-smooth morphism between normal difference schemes. This is †-primitive recursive by ($\dagger_9$). By considering the normalization $\tilde{Y}$ in the relative algebraic closure of $\mathbf{k}(Y)$ inside $\mathbf{k}(X)$, we obtain a baby Stein factorization $(X,\Sigma)\to(\tilde{Y},\tilde{\Sigma})\to(Y,\sigma)$, where the first map has geometrically transformally integral generic fiber (by 3.50), and the second is generically σ-pro-étale σ-separable, with $\mathbf{k}(\tilde{Y})/\mathbf{k}(Y)$ Galois by definition of weak covers.

By localizing further using 3.14, we may assume that all the fibers of the first morphism are directly transformally integral and consequently nonempty, so the first morphism is surjective, and we can restrict our attention to the second morphism. These steps are †-primitive recursive by ($\dagger_2$), ($\dagger_5$), ($\dagger_6$).

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

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

with $(Y_0,\Sigma_0)\to(Y,\sigma)$ finite Galois and all $Y_{i+1}\to Y_i$ proper benign, for $i\geqslant 0$. In the effective case, all this can be achieved in a †-primitive recursive way, using ($\dagger_6$), ($\dagger_4$), ($\dagger_5$). The first morphism is a Galois cover and therefore surjective by 2.22 and its generalizations, and proper benign morphisms are clearly surjective. Thus, we conclude that f can be made surjective upon a finite σ-localization, which is enough to deduce the required statement. □

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

$$\mathcal{F}\equiv_S^{\mathrm{FROB},m}\mathcal{F}',$$

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

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

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

$$\mathcal{F}\equiv_S^{\mathrm{FROB}}\mathcal{F}',$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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, σ)-difference schemes and let $\mathcal{A}$ be Galois stratification on X. For $s \in S$ and (F, φ) an algebraically closed difference field extending $(\mathbf{k}(s), \sigma^s)$, we define a subassignment $f_\exists \mathcal{A}$ of Y by the rule

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

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

$$\upsilon(y; s) \equiv \{y \in Y_s \mid \exists x \ \chi(x; s), f_s(x) = y\},$$

which justifies the notation somewhat.

LEMMA 7.10. *Suppose that*

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

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

$$f_\exists \langle Z/X, C_0 \rangle \equiv \langle Z/Y, C \rangle^{\sim}.$$

Proof. For the nontrivial inclusion, let (F, φ) 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 $\varphi_{g^{-1}z} \in C_0$, so the image x of $g^{-1}z$ in X witnesses $f(x) = y$ and $x \in \langle Z/X, C_0 \rangle(F, \varphi)$. ∎

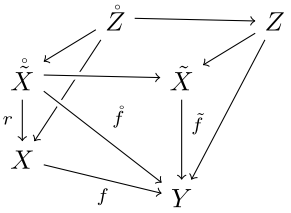
https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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 $\mathring{Z}=\iota^*Z$ be a difference scheme obtained by restricting the difference structure via some $\iota:\mathring{\Sigma}_Z\hookrightarrow\Sigma_Z$ so that $\mathring{Z}\to X$ is a Galois cover. Let C be a $\mathrm{Gal}(\mathring{Z}/X)$-conjugacy class in $\mathring{\Sigma}_Z$. Then*

$$f_\exists\langle\mathring{Z}/X,C\rangle\equiv\langle Z/Y,\iota_*C\rangle^{\sim},$$

where ι_*C is the smallest $\mathrm{Gal}(Z/Y)$-conjugacy domain in Σ_Z containing $\iota(C)$.

Proof. The diagram



shows the situation following the insertion of the Galois closure of X over Y. Starting with a $\mathrm{Gal}(\mathring{Z}/X)$-conjugacy class C in $\mathring{\Sigma}_Z$, we can consider it as a $\mathrm{Gal}(\mathring{Z}/\mathring{X})$-conjugacy domain C', and write C'' for C' considered in $Z/\tilde{X}$, so that $\tilde{C}=\iota_*C$ is the $\mathrm{Gal}(Z/Y)$-conjugacy domain induced by C''. Using 7.10, we have that $\tilde{f}_\exists\langle Z/\tilde{X},C''\rangle\equiv\langle Z/Y,\tilde{C}\rangle$ and $r_\exists\langle\mathring{Z}/\mathring{\tilde{X}},C'\rangle\equiv\langle\mathring{Z}/X,C\rangle$. Thus

$$\begin{aligned}f_\exists\langle\mathring{Z}/X,C\rangle&\equiv f_\exists r_\exists\langle\mathring{Z}/\mathring{\tilde{X}},C'\rangle\\&\equiv\mathring{f}_\exists\langle\mathring{Z}/\mathring{\tilde{X}},C'\rangle\\&\equiv\tilde{f}_\exists\langle Z/\tilde{X},C''\rangle\\&\equiv\langle Z/Y,\tilde{C}\rangle^{\sim}.\end{aligned}$$

∎

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

THEOREM 7.12. *Let (S,σ) be a difference scheme of finite σ-type over $\mathbb{Z}$ and let $f:(X,\sigma)\to(Y,\sigma)$ be a morphism of (S,σ)-difference schemes of finite σ-type. For every Galois formula $\mathcal{A}$ of X, the subassignment $f_\exists\mathcal{A}$ is $\equiv_S^{\mathrm{FROB}}$-equivalent to a Galois formula on Y, that is, there exists a Galois*

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

formula $\mathcal{B}$ *on* Y *such that*

$$f_{\exists}\mathcal{A} \equiv_S^{\text{FROB}} \mathcal{B}.$$

When $\mathcal{A}$ *is effectively given, a* †*-primitive recursive procedure yields an effectively given* $\mathcal{B}$ *and a constant* $m > 0$ *such that*

$$f_{\exists}\mathcal{A} \equiv_S^{\text{FROB},m} \mathcal{B}.$$

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 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 formulas 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 †-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 †-oracles such as ($\dagger_1$). 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 ($\dagger_1$), and we can thus reduce to the case where X and Y are transformally integral.

By splitting off the radicial and σ-radicial part as in the proof of 7.7, we may assume that f is separable σ-separable. In the effective case, we use ($\dagger_3$).

Thus, by a Noetherian induction trick using generic σ-pro-smoothness 3.8 and 7.7, after a possible refinement of $\mathcal{A}$, we obtain stratifications X_i and Y_j into transformally integral normal locally closed (S, σ)-subschemes of X and Y such that for every i there exists a j with $f(X_i) \subseteq Y_j$ and $f_i := f \restriction_{X_i} : (X_i, \sigma) \to (Y_j, \sigma)$ is σ-pro-smooth σ-separable. This can be done in a †-primitive recursive way, using ($\dagger_6$) and the effective case of 7.7.

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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 $\mathcal{A}$ on X is basic, $\mathcal{A} = \langle Z/X, C\rangle$, where $(Z, \Sigma_Z)/(X, \sigma)$ is a transformally integral Galois cover with group $(G, \tilde{\Sigma}_Z)$ and C is a G-conjugacy domain in Σ_Z.

By considering the normalization $\tilde{Y}$ in the relative algebraic closure of $\mathbf{k}(Y)$ inside $\mathbf{k}(X)$, we obtain a baby Stein factorization $(X, \sigma) \to (\tilde{Y}, \sigma) \to (Y, \sigma)$, where the first morphism has generically geometrically transformally integral fibers (by 3.50), and the second is generically σ-pro-étale σ-separable. In the effective situation, this requires ($\dagger_2$).

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, σ)-schemes whose generic fiber is geometrically transformally integral, and $(Z, \Sigma_Z)/(X, \sigma)$ is étale Galois with Z transformally integral.

Let (W, Σ_W) be the normalization of (Y, σ) in the relative algebraic closure of $\mathbf{k}(Y)$ in $(\mathbf{k}(Z), \Sigma_Z)$, in the effective case calculated by ($\dagger_2$) and ($\dagger_5$). Then (W, Σ_W) is a Galois cover of (Y, σ). Writing $(W_X, \Sigma_{W_X}) = (X, \sigma) \times_{(Y,\sigma)} (W, \Sigma_W)$, we obtain an exact sequence

$$1 \to \mathrm{Gal}(Z/W_X) \to \mathrm{Gal}(Z/X) \to \mathrm{Gal}(W/Y) \to 1, \tag{3}$$

together with a *Diff*-quotient morphism

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

By a σ-localization, 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 fibers;
(iii) $\mathrm{Gal}(Z_w/W_w) = \mathrm{Gal}(Z/W_X)$ for all fibers Z_w of $Z \to W$ and W_w of $W_X \to W$ above $w \in W$.

This is effective by ($\dagger_5$), ($\dagger_6$) and ($\dagger_8$).

Let $D = \pi_*(C)$ be the image of C in Σ_W, computed by ($\dagger_8$), and we claim that

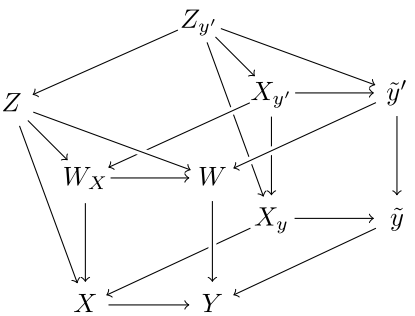
$$f_\exists\langle Z/X, C\rangle \underset{S}{=}^{\text{Frob}} \langle W/Y, D\rangle^{\sim},$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

that is, for all closed $s \in S$, all large enough k with $(\bar{k}, \varphi_k)$ extending $(\mathbf{k}(s), \sigma^s)$,

$$\begin{aligned} &\{y \in Y_s(\bar{k}, \varphi_k) \mid \exists x \in X_s(\bar{k}, \varphi_k), \varphi_{k,x} \in C, f_s(x) = y\} \\ &\quad = \{y \in Y_s(\bar{k}, \varphi_k) \mid \varphi_{k,y} \in D\}. \end{aligned} \tag{4}$$

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



where $(X_y, \sigma_y) = (X, \sigma) \times_{(Y,\sigma)} (\tilde{y}, \sigma^y)$ is the fiber of X above y, $(X_{y'}, \Sigma_{y'}) = (W_X, \Sigma_{W_X}) \times_{(W,\Sigma_W)} (\tilde{y}', \Sigma^{y'})$ is the fiber of W_X above y', and

$$(Z_{y'}, \Sigma_{y'}) = (Z, \Sigma_Z) \times_{(W_X, \Sigma_{W_X})} (X_{y'}, \Sigma_{y'}) = (Z, \Sigma_Z) \times_{(W,\Sigma_W)} (\tilde{y}', \Sigma^{y'})$$

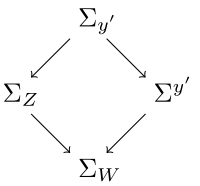
is the fiber of Z above y'. By construction, $Z_{y'}$ is directly geometrically transformally integral and $\mathrm{Gal}(Z_{y'}/X_{y'}) \cong \mathrm{Gal}(Z/W_X)$. In the diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(Z_{y'}/X_{y'}) & \longrightarrow & \mathrm{Gal}(Z_{y'}/X_y) & \longrightarrow & \mathrm{Gal}(\tilde{y}'/\tilde{y}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Gal}(Z/W_X) & \longrightarrow & \mathrm{Gal}(Z/X) & \longrightarrow & \mathrm{Gal}(W/Y) & \longrightarrow & 1 \end{array}$$

the left vertical arrow is an isomorphism and $\mathrm{Gal}(\tilde{y}'/\tilde{y}) = \mathrm{Gal}(\mathbf{k}(y')/\mathbf{k}(y))$. It follows that $\mathrm{Gal}(Z_{y'}/X_y) = \mathrm{Gal}(Z/X) \times_{\mathrm{Gal}(W/Y)} \mathrm{Gal}(\tilde{y}'/\tilde{y})$ and we get a

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

Cartesian diagram of difference structures:



Thus we can find a conjugacy domain $C' \subseteq \Sigma_{y'}$ which maps into C in Σ_Z (and eventually to $D_0 \subseteq \Sigma_W$), as well as onto φ_k. It suffices to find an $x \in X_y(\bar{k}, \varphi_k)$ 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 (†9).

Case 2. The morphism $f : (X, \sigma) \to (Y, \sigma)$ is generically σ-pro-étale σ-separable of transformally integral (S, σ)-schemes.

Using 5.24, the generic weak Galois closure of X over Y consists of generic weak covers $r : (\mathring{X}, \mathring{\Sigma}) \to (X, \sigma)$ and $\tilde{X} \to Y$ such that $h = fr : (\mathring{X}, \mathring{\Sigma}) \to (Y, \sigma)$ is quasi-Galois. By 3.8 and 7.7, modulo a σ-localization, we may assume that f is σ-pro-étale and that h strictly dominates f, that is, that the morphism r is surjective. Then

$$f_\exists \mathcal{A} \equiv f_\exists r_\exists r^* \mathcal{A} \equiv h_\exists r^* \mathcal{A},$$

so it is enough to show that the direct image by $h_\exists$ of a Galois formula $\mathcal{B} = r^*\mathcal{A}$ is again Galois. In the effective case, we can do this via (†5), (†6), (†7).

For each $\sigma \in \mathring{\Sigma}$, let ι_σ be the inclusion $\{\sigma\} \hookrightarrow \mathring{\Sigma}$, let $\mathring{X}^\sigma = \iota_\sigma^* \mathring{X}$ and let $i_\sigma : \mathring{X}^\sigma \to \mathring{X}$ be the natural morphism. Writing $\mathcal{B}^\sigma = i_\sigma^* \mathcal{B}$ and $h^\sigma = h i_\sigma : \mathring{X}^\sigma \to Y$, it is easily verified that

$$h_\exists \mathcal{B} \equiv \bigvee_{\sigma \in \mathring{\Sigma}} h^\sigma_\exists \mathcal{B}^\sigma,$$

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 σ-pro-étale quasi-Galois σ-separable, so we can benefit from Babbitt's decomposition. Indeed, modulo a localization, 5.12 yields a decomposition of f as

$$(X, \sigma) \simeq (X_n, \sigma) \to \cdots \to (X_1, \sigma) \to (X_0, \sigma) \to (Y, \sigma),$$

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

with $(X_0, \sigma) \to (Y, \sigma)$ finite étale quasi-Galois, and for $i \geqslant 0$, $(X_{i+1}, \sigma) \to (X_i, \sigma)$ étale benign quasi-Galois. This can be achieved in a †-primitive recursive way by using ($\dagger_4$) and ($\dagger_5$).

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 $\mathrm{Gal}(Z/X)$-conjugacy class C in Σ.

The Galois closure (5.18) of a finite étale morphism consists of Galois covers $(r, \rho) : (\mathring{Z}, \mathring{\Sigma}) \to (Z, \Sigma)$ and $(\tilde{Z}, \tilde{\Sigma}) \to (Y, \sigma)$, as well as a morphism $(\mathring{Z}, \mathring{\Sigma}) \to (\tilde{Z}, \tilde{\Sigma})$ arising by restriction of structure via $\iota : \mathring{\Sigma} \hookrightarrow \tilde{\Sigma}$.

Thus, using inflation and 7.11,

$$f_\exists \langle Z/X, C\rangle \equiv f_\exists \langle \mathring{Z}/X, \rho^{-1}C\rangle \equiv \langle \tilde{Z}/Y, \iota_*\rho^{-1}C\rangle.$$

The relevant calculations in the effective case are performed using ($\dagger_7$) and ($\dagger_8$).

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 Σ_Z. The weak generic Galois closure (5.24) of Z over Y consists of weak generic covers $\mathring{Z} \to Z$ and $\tilde{Z} \to Y$. Since Z is a finite Galois cover of X and X is quasi-Galois over Y, it follows that $\mathring{Z}$ is a *finite* Galois cover of X. Thus, using inflation we can replace Z by $\mathring{Z}$ and assume that the original Z is in fact quasi-Galois over Y.

Babbitt's decomposition 5.12 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 $i \geqslant 0$. Since $\mathbf{k}(X)$ is linearly disjoint from $\mathbf{k}(W)$ over $\mathbf{k}(Y)$, we obtain an exact sequence of the form (3) again, and we have the corresponding *Diff*-morphism $\pi : \Sigma_Z \to \Sigma_Z/\mathrm{Gal}(Z/W_X) = \Sigma_W$. Let $D = \pi_* C$ be the image of C in Σ_W, and we claim that (4) holds for any s closed in S and $(\bar{k}, \varphi_k)$ extending $(\mathbf{k}(s), \varphi_s)$. To see the nontrivial inclusion, let y be an element of the right-hand side and let $z_0 \in W = Z_0$ such that $z_0 \mapsto y$ and $\varphi_{k,z_0} \in D$. Using the property 5.9 repeatedly, we can lift z_0 through the "stack" of benign extensions Z_{i+1}/Z_i to a point $z \in Z^{\tilde{\sigma}}(\bar{k}, \varphi_k)$ with $\tilde{\sigma} \in C$, and then the image x of z in X_s has the properties $\varphi_{k,x} \sim \tilde{\sigma} \in C$ and $f(x) = y$. This case is †-primitive recursive by ($\dagger_2$), ($\dagger_5$), ($\dagger_6$), ($\dagger_8$). □

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

COROLLARY 7.13. *With assumptions of 7.12, it makes sense to define a subassignment*

$$f_\forall \mathcal{A} \equiv_S^{\text{FROB}} \neg f_\exists(\neg \mathcal{A}),$$

and it is again a Galois formula on Y.

7.3 Quantifier elimination for Galois formulas

Let (R, σ) be an integral normal difference ring of finite σ-type over $\mathbb{Z}$, and let $(S, \sigma) = \mathrm{Spec}^\sigma(R)$.

DEFINITION 7.14.

(1) A *first-order formula* over (S, σ) is a first-order expression built in the usual way starting from terms which are difference polynomials with coefficients in (R, σ). If $x_1, \ldots, x_n$ are the free variables of a formula θ, and $r_1, \ldots, r_m \in R$ are all the coefficients of all polynomials appearing as terms of θ, 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 θ.

(2) An (R, σ)-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, φ) be an algebraically closed difference field extending $(\mathbf{k}(s), \varphi^s)$. Taking the images of the r_i by the composite

$$(R, \sigma) \to (\mathcal{O}_{S,s}, \sigma_s^\sharp) \to (\mathbf{k}(s), \sigma^s) \to (F, \varphi),$$

we obtain an honest first-order formula in the language of difference rings on the field (F, φ), and we take its set of realizations to be the value

$$\tilde{\theta}(s, (F, \varphi)) \subseteq \mathbb{A}^n_s(F, \varphi).$$

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

THEOREM 7.15. (Quantifier elimination for fields with Frobenii) *The class of definable (S, σ)-subassignments is equal to the class of (S, σ)-Galois formulas modulo the relation $\equiv_S^{\text{FROB}}$, that is, with respect to fields with Frobenii over S. The quantifier elimination procedure is †-primitive recursive.*

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

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

(1) If $\theta(x_1,\dots,x_n)$ is a positive atomic formula, it is given by a difference-polynomial equation $P(x_1,\dots,x_n)=0$, 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 $C_i=\emptyset$ otherwise. Then $\mathcal{A}=\langle \mathbb{A}^n_S, X_i/X_i, C_i\rangle$ has the property that
$$\tilde{\theta}\equiv\tilde{\mathcal{A}}.$$

(2) If $\theta(\bar{x})=\theta_1(\bar{x}_1)\wedge\theta_2(\bar{x}_2)$, 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 formulas $\mathcal{A}_i$ on $\mathbb{A}^{|\bar{x}_i|}$ such that $\theta_i\equiv^{\mathrm{FROB}}_S\mathcal{A}_i$. Then
$$\theta\equiv^{\mathrm{FROB}}_S p_1^*\mathcal{A}_1\wedge p_2^*\mathcal{A}_2.$$

(3) If $\theta=\theta_1\vee\theta_2$, we proceed analogously to the previous step.

(4) If $\theta=\neg\theta'$, and $\theta'\equiv^{\mathrm{FROB}}_S\mathcal{A}$, then
$$\theta\equiv^{\mathrm{FROB}}_S\neg\mathcal{A}.$$

(5) If $\theta(x_2,\dots,x_n)=\exists x_1\theta'(x_1,x_2,\dots,x_n)$, and $\theta'\equiv^{\mathrm{FROB}}_S\mathcal{A}$ on $\mathbb{A}^n$, writing x_1 for the projection $\mathbb{A}^n\to\mathbb{A}^{n-1}$ to the variables $x_2,\dots,x_n$, we have that
$$\theta\equiv_S\exists x_1\theta'\equiv^{\mathrm{FROB}}_S x_{1\exists}\mathcal{A},$$
which is Galois by 7.12.

(6) If $\theta=\forall x_1\theta'$, and $\theta'\equiv^{\mathrm{FROB}}_S\mathcal{A}$, then
$$\theta\equiv_S\forall x_1\theta'\equiv^{\mathrm{FROB}}_S x_{1\forall}\mathcal{A},$$
which is Galois by 7.13.

We have checked all cases so the induction is complete. Note that working over fields with Frobenii is only crucial in steps (5) and (6).

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

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

$(Z_i, \Sigma_i) \to (X_i, \sigma)$ with group $(G, \tilde{\Sigma})$ is embedded in some affine space, in the sense that Z_i is embedded in some $\mathbb{A}^m_S$, and all automorphisms corresponding to elements of G are restrictions of difference rational endomorphisms of $\mathbb{A}^m_S$ to Z_i, and the canonical projection $Z_i \to X_i$ is a restriction of difference rational morphism $\mathbb{A}^m_S \to \mathbb{A}^n_S$. Then, if C_i is the conjugacy class of some element $\sigma_i \in \Sigma$, the set

$$\{x \in X_i : \mathrm{ar}(x) \subseteq C_i\} = \{x \in X_i : \exists z \in Z_i^{\sigma_i}, z \mapsto x\}$$

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 formulas. □

Let T_∞ 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_∞ is decidable by a †-primitive recursive procedure. Moreover, for each first-order sentence $\theta \in T_\infty$ a †-primitive recursive procedure can compute the (finite) list of exceptional finite fields k such that θ does not hold in $(\bar{k}, \varphi_k)$.*

Proof. The quantifier elimination procedure produces a Galois stratification $\mathcal{A}$ on the base $S = \mathrm{Spec}(\mathbb{Z})$ and a constant m such that for every $p \in S$, and every k of characteristic p with $|k| \geqslant m$, $\theta(\bar{k}, \varphi_k) = \mathcal{A}(\bar{k}, \varphi_k)$. The stratification $\mathcal{A}$ stipulates the existence of a localization $S' = \mathbb{Z}[1/N]$ of S, a Galois cover Z/S' and a conjugacy class C in $\mathrm{Gal}(Z/S')$ such that, for $p \in S'$ (i.e., for p not dividing N), and k of characteristic p with $|k| \geqslant m$, θ 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 $C = \mathrm{Gal}(Z/S')$, which can be effectively checked by (†8).

For each field $(\bar{k}, \varphi_k)$ with characteristic of k dividing N, or $|k| < m$, once we interpret σ as the Frobenius φ_k with $\varphi_k(\alpha) = \alpha^{|k|}$, the formula θ 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 $\bar{k}$. □

A model-theoretic restatement of the above theorem would say that the theory T_∞ of fields with Frobenii allows quantifier elimination down to the class of Galois formulas. Given that T_∞ happens to be [18] the theory of

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press

existentially closed difference fields (ACFA), let us state an appropriate analog of the above result.

We must emphasize that the statement below can be obtained unconditionally, that is, without appealing to [18], by replacing the use of [24, 4.2] in the present paper by the use of existential closedness of models of ACFA (i.e., by the use of the "ACFA-axiom"). This will be done in a separate paper [25].

THEOREM 7.17. *Let (k, σ) 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, φ) of ACFA which extends (k, σ),*

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

Acknowledgments. 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 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.

REFERENCES

[1] The Stacks Project Authors. Stacks Project. http://stacks.math.columbia.edu.
[2] James Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271.
[3] A. E. Babbitt Jr., *Finitely generated pathological extensions of difference fields*, Trans. Amer. Math. Soc. **102** (1962), 63–81.
[4] N. Bourbaki, *Éléments de mathématique. Algèbre. Chapitre 4: Polynomes et fractions rationnelles. Chapitre 5: Corps commutatifs. Actualités Scientifiques et Industrielles, No. 1102,* Deuxième édition, Hermann, Paris, 1959.
[5] N. Bourbaki, *Éléments de mathématique. Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations. Actualités Scientifiques et Industrielles, No. 1308*, Hermann, Paris, 1964.
[6] Z. Chatzidakis and E. Hrushovski, *Model theory of difference fields*, Trans. Amer. Math. Soc. **351**(8) (1999), 2997–3071.
[7] R. M. Cohn, *Difference Algebra*, Interscience Publishers John Wiley & Sons, New York–London–Sydney, 1965.
[8] J. Denef and F. Loeser, *Definable sets, motives and p-adic integrals*, J. Amer. Math. Soc. **14**(2) (2001), 429–469; (electronic).
[9] L. Di Vizio, C. Hardouin and M. Wibmer, *Difference Galois theory of linear differential equations*, Adv. Math. **260** (2014), 1–58.

[10] D. Eisenbud, *Commutative Algebra*, Graduate Texts in Mathematics **150**, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.
[11] M. D. Fried, *Variables separated equations: strikingly different roles for the branch cycle lemma and the finite simple group classification*, Sci. China Math. **55**(1) (2012), 1–72.
[12] M. D. Fried, D. Haran and M. Jarden, *Effective counting of the points of definable sets over finite fields*, Israel J. Math. **85**(1–3) (1994), 103–133.
[13] M. D. Fried and M. Jarden, *Field Arithmetic*, third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics **11**, Springer-Verlag, Berlin, 2008, Revised by Jarden.
[14] M. Fried and G. Sacerdote, *Solving Diophantine problems over all residue class fields of a number field and all finite fields*, Ann. of Math. (2) **104**(2) (1976), 203–233.
[15] G. Giabicani, Théorie de l'intersection en géométrie aux différences. PhD Thesis, École Polytechnique, Paris, 2011.
[16] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Publ. Math. Inst. Hautes Études Sci. (24) (1965).
[17] A. Grothendieck, "*Séminaire de géométrie algébrique du Bois Marie 1960–61*", in *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) **3**, Société Mathématique de France, Paris, 2003, Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math. **224**, Springer, Berlin; (50 #7129)].
[18] E. Hrushovski, The elementary theory of the Frobenius automorphisms. arXiv:math /0406514, 2004. The most recent version of the paper (2012) is available at http://www.ma.huji.ac.il/∼ehud/FROB.pdf.
[19] C. Kiefe, *Sets definable over finite fields: their zeta-functions*, Trans. Amer. Math. Soc. **223** (1976), 45–59.
[20] A. Levin, *Difference Algebra*, Algebra and Applications **8**, Springer, New York, 2008.
[21] A. Macintyre, *Generic automorphisms of fields*, Ann. Pure Appl. Logic **88**(2–3) (1997), 165–180; Joint AILA-KGS Model Theory Meeting (Florence, 1995).
[22] J. Nicaise, *Relative motives and the theory of pseudo-finite fields*, Int. Math. Res. Pap. IMRP **70**(1) (2007), Art. ID rpm001.
[23] I. Tomašić, *Direct twisted Galois stratification*, preprint, 2014, arXiv:1412.8066, submitted.
[24] I. Tomašić, *A twisted theorem of Chebotarev*, Proc. Lond. Math. Soc. (3) **108**(2) (2014), 291–326.
[25] I. Tomašić, *Galois stratification and ACFA*, Ann. Pure Appl. Logic **166**(5) (2015), 639–663.
[26] M. Wibmer, *A Chevalley theorem for difference equations*, Math. Ann. **354**(4) (2012), 1369–1396.

Ivan Tomašić
School of Mathematical Sciences
Queen Mary University of London
London E1 4NS
United Kingdom
i.tomasic@qmul.ac.uk

https://doi.org/10.1017/nmj.2016.9 Published online by Cambridge University Press