GALOIS STRATIFICATION AND ACFA

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 modulo the theory ACFA of existentially closed difference fields. As a consequence, we obtain an *effective* quantifier elimination procedure and a precise algebraic-geometric description of definable sets over existentially closed difference fields in terms of twisted Galois formulae associated with finite Galois difference ring/scheme covers.

Contents

1. Introduction

Results. We develop the theory of *twisted Galois stratification* in order to study first-order definable sets in the language of *difference rings* over existentially closed difference fields. A (normal) *Galois stratification* on a difference scheme (X, σ) is a datum

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

where X_i, $i \in I$ is a partition of X into finitely many normal locally closed difference subschemes of X, each $(C_i, \Sigma_i)/(X_i, \sigma)$ is a finite Galois difference ring/scheme

Date: January 11, 2015.

2000 *Mathematics Subject Classification.* Primary 03C60, 11G25. Secondary 11U09, 14G15, 39A14.

Key words and phrases. difference scheme, Galois stratification, Galois formula, Frobenius automorphism, ACFA.

cover with some group $(G_i, \tilde{\Sigma})$ and Γ_i is a conjugacy domain in Σ_i, as defined in Subsection 3.1. The *Galois formula* associated with $\mathcal{A}$ is the realisation subfunctor $\tilde{\mathcal{A}}$ of X defined by the assignment

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

where (F,φ) is an algebraically closed difference field and the conjugacy class $\varphi_x \subseteq \Sigma$ is the local φ-substitution at x, as expounded in Subsection 3.2.

From an algebraic-geometric point of view, our main result 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 existentially closed difference fields (a precise statement is 3.23 in conjunction with 4.5). In order to capture the idea that the computation of direct images is *effective* in a suitable sense, we develop the notion of *†(k)-primitive recursive functions* which, intuitively, correspond to functions primitively recursively reducible to basic operations with difference polynomial ideals over a primitive recursive difference field (k,σ), see Section 4.

Theorem 1.1. *Let $f : (X,\sigma) \to (Y,\sigma)$ be a morphism of finite transformal type over a difference field (k,σ), and let $\mathcal{A}$ be a Galois stratification on X. There exists a Galois stratification $\mathcal{B}$ on Y such that for all existentially closed difference fields (F,φ) extending (k,σ),*

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

When (k,σ) is primitive recursive and $\mathcal{A}$ is effectively given, a †(k)-primitive recursive procedure can compute an effectively given $\mathcal{B}$ as above.

From a model-theoretic point of view, our main result is that the theory ACFA of existentially closed difference fields allows *quantifier elimination* in the language of Galois formulae. In other words, every definable set over an existentially closed difference field is equivalent to a Galois formula (a precise statement is 3.26).

Theorem 1.2. *Let $\theta(x_1,\ldots,x_n)$ be a first-order formula in the language of difference rings with parameters in a difference field (k,σ). There exists a Galois stratification $\mathcal{A}$ of the difference affine n-space such that for all existentially closed difference field (F,φ) extending (k,σ),*

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

Conversely, every Galois formula is equivalent to a first-order formula in the language of difference rings over algebraically closed difference fields. When (k,σ) is primitive recursive, the quantifier elimination procedure is †(k)-primitive recursive.

To summarise, our main achievements are:

- *Fine quantifier elimination,* a precise description of definable sets in terms of *Galois formulae*, well-suited for algebraic-geometric and number-theoretic applications.
- *Effectivity* of the quantifier elimination. We present a constructive algorithm for quantifier elimination in ACFA, primitive recursive reducible to methods of difference algebraic geometry via the direct image theorem 1.1.

Although the phenomenon is not yet fully understood, it is empirically evident that there are few finite Galois covers of difference schemes orthogonal to the fixed field.

Thus, Galois stratification in ACFA may possess an even greater classifying power than that over pseudofinite fields.

Historical overview. Galois stratification has been originally developed in the context of pseudofinite fields by Fried, Haran, Jarden and Sacerdote ([10], [7], [9]). Earlier work of Ax [1], explicated by Kiefe [13], showed that every formula $\theta(x_1, \ldots, x_n)$ in the language of rings is equivalent to a Boolean combination of formulae of the form

$$\exists y \ f(y; x_1, \ldots, x_n) = 0,$$

where f is a polynomial. Galois stratification procedure gave a more explicit description of definable sets over pseudofinite fields in terms of Galois formulae associated with Galois covers of algebraic varieties, and the benefits were twofold. On the one hand, it afforded an *effective* (primitive recursive) quantifier elimination procedure. On the other, the precise description of formulae in terms of Galois covers was particularly useful for applications of geometric and number-theoretic nature, for example in Fried's work on Davenport's problem [8], as well as the impressive work of Denef and Loeser on arithmetic motivic integration in [6], where the authors assign a Chow motive to a Galois formula, extending the consideration of algebraic-geometric invariants of algebraic varieties to arbitrary first-order formulae over pseudofinite fields.

In the framework of existentially closed difference fields, the relation of our work to the known model-theoretic quantifier elimination found by Macintyre [15] and greatly refined in modern terms by Chatzidakis and Hrushovski [4], is analogous to the relation between the work of Fried-Sacerdote and the work of Ax and Kiefe mentioned above. Macintyre and Chatzidakis-Hrushovski show that any formula $\theta(x_1, \ldots, x_n)$ in the language of difference rings is equivalent, modulo the theory ACFA, to a disjunction $\varphi(x_1, \ldots, x_n)$ of formulae of the form

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

where ψ is quantifier free, and $\psi(y; x_1, \ldots, x_n)$ implies that y satisfies a nonzero polynomial whose coefficients are σ-polynomials in $x_1, \ldots, x_n$, i.e., the single existential quantifier is bounded.

We should emphasise that our quantifier elimination down to Galois formulae is *finer* than the model-theoretic quantifier elimination, in the sense that it describes definable sets in terms of *finite* Galois covers, whereas the covers associated with the bounded $\exists_1$-formulae from the logical quantifier elimination may correspond to infinitary quasifinite covers of difference schemes (with finite fibres).

In terms of effectivity, the model-theoretic proof of the decidability of ACFA uses the compactness theorem, and, although recursive, the quantifier elimination is far from being effective. Indeed, in order to eliminate the quantifiers from a formula $\theta(x_1, \ldots, x_n)$, one would have to perform a search through all formulas $\varphi(x_1, \ldots, x_n)$ of the above form, and for each φ, one would have to perform an indefinite search through all proofs to decide whether $ACFA$ proves

$$\forall x_1 \cdots \forall x_n \theta(x_1, \ldots, x_n) \leftrightarrow \varphi(x_1, \ldots, x_n).$$

Our quantifier elimination procedure through the direct image theorem 1.1 is a much more focused algorithm which reduces the calculation to basic operations with difference polynomial ideals, and we dub it †-primitive recursive.

Motivated by the desire to find an outright primitive quantifier elimination procedure for ACFA, we developed a coarser theory of *direct* Galois stratification in [18],

equivalent in power to the model-theoretic quantifier elimination. It shows that the logic quantifier elimination for ACFA is *primitive recursive*, and that ACFA is decidable using a primitive recursive procedure. To summarise, *fine quantifier elimination* is †-primitive recursive, while the coarser *logic quantifier elimination* is primitive recursive.

Methodology. The first major obstacle in this work was the fact that the category of *strict/ordinary* difference schemes has no reasonable Galois actions, covers or quotients. Thus, in order to formulate a suitable notion of a *Galois cover*, we had to develop *generalised difference algebra* in [19].

In the paper [17] we develop Galois stratification over algebraic closures of finite fields with powers of Frobenius. There, we make full use of the power of *generalised difference schemes* from [19]. In the present paper, however, acknowledging the fact that learning that theory may be an obstacle for a reader already familiar with the theory of ordinary or strict difference schemes as in [12], [14], [11], we make every effort to replace any use of generalised difference schemes by algebraic techniques. In particular, we replace the use of Galois covers of difference schemes $(X, \Sigma) \to (Y, \sigma)$ by the use of ring/scheme covers $(C, \Sigma)/(Y, \sigma)$, where (Y, σ) is an ordinary difference scheme. One awkward consequence of this approach is that we cannot discuss a tower of ring/scheme covers, and this forces us to digress into a study of *infinite* Galois theory, even though our main results show with hindsight that only finite Galois covers are relevant.

As a consequence, the proof of 1.1 (in fact of 3.23) is different to the one from [17], and it runs even smoother in certain cases. In both papers, our approach is more geometric and conceptual than those of [10], [7], [9], and [16] in the classical case of Galois stratification over pseudofinite fields.

Our trick is to perform a rudimentary form of Stein factorisation at the start of the procedure, which significantly simplifies matters. In fact, by eliminating the difference considerations from our procedure, we would obtain an essentially new procedure in the classical case of pseudofinite fields. On the other hand, we must treat several genuinely new difference phenomena which do not arise in the algebraic case, the key ingredient being Babbitt's decomposition theorem 2.26.

We shall freely use the theory of generalised difference schemes and their local properties as developed in [19] and [17]. Nevertheless, we provide a quick guide through the most relevant prerequisites, as well as some complements, in Section 2.

The author would like to express his gratitude to Michael Fried and Thomas Scanlon for fruitful discussions on the topic of this paper, to Angus Macintyre, who encouraged the development of Galois stratification in ACFA, and to Zoe Chatzidakis for pointing out the importance of Babbitt's decomposition.

2. Generalised difference algebra and geometry

The detailed treatment of generalised difference algebraic geometry can be found in [19] and [17]. In the interest of brevity, this section is intended as a 'Leitfäden' through that work rather than a complete account.

2.1. **Generalised 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 $\Sigma \times \Sigma \to \Sigma$, $(\sigma, \tau) \mapsto \sigma^\tau$ such that $\sigma^\sigma = \sigma$.

A morphism $()^{\varphi} : \Sigma \to T$ is a function such that for all $\sigma, \tau \in \Sigma$,

$$(\sigma^{\tau})^{\varphi} = (\sigma^{\varphi})^{(\tau^{\varphi})}.$$

A *Diff*-object is called *regular*, if $()^{\sigma} : \Sigma \to \Sigma$ is bijective for every $\sigma \in \Sigma$.

Definition 2.2. Let us define the category of *generalised difference rings,* which can be thought of as a category of 'representations' of $Diff^{op}$-objects in rings. The objects are of form (A, Σ), where A is a commutative ring with identity, and Σ is a set of endomorphisms $A \to A$ such that:

(1) for every $\sigma, \tau \in \Sigma$, there exists a unique $\sigma^{\tau} \in \Sigma$ with
$$\tau \circ \sigma^{\tau} = \sigma \circ \tau;$$
(2) $(\Sigma, (\cdot)^{(\cdot)})$ is an object of *Diff*;
(3) for every $\sigma \in \Sigma$, $()^{\sigma} : \Sigma \to \Sigma$ is a *Diff*-morphism.

A morphism $\varphi : (B, T) \to (A, \Sigma)$ consists of an $\mathcal{A}$-morphism $\varphi : B \to A$ and a map $()^{\varphi} : \Sigma \to T$ such that

$$\varphi \circ \sigma^{\varphi} = \sigma \circ \varphi.$$

Moreover, we require that

$$(\tau^{\sigma})^{\varphi} = (\tau^{\varphi})^{(\sigma^{\varphi})}.$$

Our desired objects of study are *strong* (or Σ-*reduced*) generalised difference rings (A, Σ), where all $\sigma \in \Sigma$ are injective. Certain operations, such as tensor products to be studied below, do not preserve injectivity, so we need to remain vigilant as we progress into more complex considerations.

A difference ring (A, Σ) is *inversive*, if all $\sigma \in \Sigma$ are bijective. Every strong regular (A, Σ) has an *inversive closure* $(A^{\mathrm{inv}}, \Sigma^{\mathrm{inv}})$ ([19, 2.9]).

We shall say that (A, Σ) is *nearly-strict*, if there exists a group G of automorphisms of (A, Σ) such that $\Sigma \subseteq G\sigma$ for some $\sigma \in \Sigma$.

Moreover, we say that (A, Σ) is a *transformal domain* if A is a domain with (A, Σ) strong.

Definition 2.3. Two difference rings (A_1, Σ) and (A_2, Σ) are called *equivalent*, written $(A_1, \Sigma) \simeq (A_2, \Sigma)$, if their inversive closures are isomorphic, $(A_1^{\mathrm{inv}}, \Sigma^{\mathrm{inv}}) \cong (A_2^{\mathrm{inv}}, \Sigma^{\mathrm{inv}})$.

Definition 2.4. Let (A, Σ) be a difference ring. We shall consider the following subsets of $\mathrm{Spec}(A)$:

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

A detailed study of those sets as locally ringed spaces with the Zariski topology and the structure sheaves induced from $\mathrm{Spec}(A)$ is carried out in [19]. It is particularly well-behaved for *well-mixed* difference rings (A, Σ), in which $ab = 0$ implies $a\sigma(b) = 0$ for any $\sigma \in \Sigma$. Let us just mention that by an (affine) *ordinary (or strict) difference scheme* we will mean a locally ringed space $\mathrm{Spec}^{\sigma}(A)$ for a well-mixed (A, σ).

Remark 2.5. It is proved in [19, 2.23] that every difference scheme morphism $\mathrm{Spec}^{T}(B) \to \mathrm{Spec}^{\Sigma}(A)$ can be realised as the fixed-point spectrum of a difference ring morphism $(A, \Sigma) \to (\bar{B}, T)$, where $\bar{B}$ is closely associated to B and $\mathrm{Spec}^{T}(\bar{B}) \simeq \mathrm{Spec}^{T}(B)$. The situation is weaker than for algebraic schemes where

we have an equivalence of categories between the categories of affine schemes and commutative rings with identity. Nevertheless, we are still able to transfer the considerations from geometry into algebra and vice-versa. Moreover, even the finiteness properties from 2.11 can be preserved in this process, as shown in [19, 2.41].

Remark 2.6. For an element $\sigma \in \Sigma$, let us write ${}^a\sigma$ for the map $\mathrm{Spec}(A) \to \mathrm{Spec}(A)$ defined by ${}^a\sigma(\mathfrak{p}) = \sigma^{-1}(\mathfrak{p})$. Note that for an arbitrary $\tau \in \Sigma$,

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

so each $\sigma \in \Sigma$ induces a map ${}^a\sigma : \mathrm{Spec}^\Sigma(A) \to \mathrm{Spec}^\Sigma(A)$.

Definition 2.7. (1) Let (A, Σ) be an algebra over a difference field (k, σ). Let (F, φ) be a difference field extension of (k, σ). We will use the notation

$$(A, \Sigma)(F, \varphi) = \mathrm{Hom}_{(k,\sigma)}((A, \Sigma), (F, \varphi)).$$

(2) Let $(X, \sigma) = \mathrm{Spec}^\sigma(A)$ be an affine difference scheme over a difference field (k, σ). We may assume that (A, σ) is a (k, σ)-algebra, and let (F, φ) be a difference field extension of (k, σ). The set of (F, φ)-rational points of (X, σ), written $X(F, \varphi)$, is the set of all (k, σ)-morphisms $\mathrm{Spec}^\varphi(F) \to (X, \sigma)$. By 2.5, it can be identified with $(A, \sigma)(F, \varphi)$.

2.2. **Products and compatibility.** Suppose that we have morphisms $(B, \Sigma) \to (A_i, \Sigma_i)$ where the structure morphisms $\Sigma_i \to \Sigma$ are surjective. It is shown in [19, 2.35, 2.34] that the coordinate ring corresponding to the fibre product of associated difference schemes is

$$(A_1 \otimes_B A_2)_w,$$

the largest well-mixed quotient of $A_1 \otimes_B A_2$ with the difference structure induced by $\Sigma_1 \times_\Sigma \Sigma_2$.

One of the main difficulties with (fibre) products in the difference framework is the possibility that such a product of non-zero difference rings can be trivial.

Lemma 2.8 ([11, 1.9.7])**.** *Let $(K, \sigma) \to (L_i, \sigma_i)$, $i = 1, 2$, be two difference field extensions. The following statements are equivalent:*

(1) L_1/K and L_2/K are compatible*, i.e., they can be embedded in a common difference field extension of K;*
(2) $(L_1 \otimes_K L_2, \sigma_1 \otimes \sigma_2)_w \neq 0$;
(3) $\mathrm{Spec}^{\sigma_1}(L_1) \times_{\mathrm{Spec}^\sigma(K)} \mathrm{Spec}^{\sigma_2}(L_2) \neq \emptyset$.

Thus, before taking any fibre product, we have to worry about compatibility. To our advantage, the only two types of situation where we take the fibre products in our proof of 3.23 are handled by the following discussion.

Remark 2.9. Suppose that we have morphisms $(B, \sigma) \to (A_i, \Sigma_i)$ of transformal domains.

(1) If $B \to A_1$ is a regular extension which corresponds to a morphism with geometrically directly transformally integral fibres (defined in 2.14), then $(A_1 \otimes_B A_2, \Sigma_1 \times_\sigma \Sigma_2)$ is geometrically directly transformally integral (and therefore non-empty by 2.29).
(2) If $(B, \sigma) \to (A_2, \Sigma_2)$ is a Galois extension with group $(G, \tilde{\Sigma}_2)$ as in 3.1, $\mathrm{Spec}^{\Sigma_1 \times_\sigma \Sigma_2}(A_1 \otimes_B A_2)$ is not empty. If all the rings are Ritt with Σ_i finite (see 2.16, 2.17), pick a minimal prime $\mathfrak{p}$ inside and then $(A_1, \Sigma_1) \to$

$(A_1 \otimes_B A_2/\mathfrak{p}, \Sigma_\mathfrak{p})$ is a Galois extension with group $(D_\mathfrak{p}, \tilde{\Sigma}_\mathfrak{p})$, where $D_\mathfrak{p} = \{g \in G : g^{-1}(\mathfrak{p}) = \mathfrak{p}\}$ and $\Sigma_\mathfrak{p} = \{\sigma \in \Sigma_1 \times_\sigma \Sigma_2 : \sigma^{-1}(\mathfrak{p}) = \mathfrak{p}\}$. It should be thought of as a *component* of the resulting fibre.

Proof. A well-known result of [2] states that extensions L_1/K and L_2/K are compatible if and only if their cores are compatible. In the first case, the core of $\mathbf{k}(A_1)/\mathbf{k}(B)$ is trivial. In the second case, since the restriction of Σ_2 to the core of $\mathbf{k}(A_2)/\mathbf{k}(B)$ consists of all the extensions of σ to $\mathbf{k}(A_2)$, for each element of Σ_1 there will be an element of Σ_2 compatible with it. □

Definition 2.10. A property of difference schemes is said to hold *geometrically*, if it is preserved by an arbitrary base change.

2.3. **Finiteness properties.**

Definition 2.11. Let (R, σ) be a difference ring.

(1) An (R, σ)-algebra (A, Σ) is of *finite* Σ*-type* if there exist elements $a_1, \ldots, a_n$ in A such that $A = R[a_1, \ldots, a_n]_\Sigma = R[\nu a_1, \ldots, \nu a_n : \nu \in \langle\Sigma\rangle]$, where $\langle\Sigma\rangle$ is the free semigroup generated by Σ.
(2) An (R, σ)-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).
(3) A morphism $f : (X, \sigma) \to (Y, \sigma)$ is *of finite* σ*-type* if Y is a finite union of open affine subsets $V_i = \mathrm{Spec}^\sigma(R_i)$ such that for each i, $f^{-1}(V_i)$ is of finite σ-type over (R_i, σ).
(4) A morphism $f : (X, \sigma) \to (Y, \sigma)$ is *finite* if Y is a finite union of open affine subsets $V_i = \mathrm{Spec}^\sigma(R_i)$ such that for each i, $f^{-1}(V_i)$ is $\mathrm{Spec}^\sigma(A_i)$, where A_i is finite over R_i.
(5) Given a difference polynomial ring $P = R[\bar{x}]_\Sigma$ over (R, σ), let $P_0 = R[\bar{x}]$ and $P_1 = R[\bar{x}, \Sigma\bar{x}] \subseteq P$. 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 $I \cap P_1$.

Definition 2.12. Let (A, σ) be of finite σ-type over a difference field (k, σ). For any choice of a tuple of σ-generators a of (A, σ), we can consider the associated sequence of prolongations $A_i = k[a, \ldots, \sigma^i a]$ and associated homomorphisms $\pi_i : A_i \hookrightarrow A_{i+1}$, and $\sigma_i : A_i \to A_{i+1}$ satisfying

$$\sigma_{i+1}\pi_i = \pi_{i+1}\sigma_i, \quad i \in \mathbb{N},$$

so that $(A, \sigma) = \varinjlim_i \langle A_i, \sigma_i; \pi_i\rangle$.

When we have a morphism $f : (A, \sigma) \to (B, \sigma)$ of (k, σ)-algebras of finite σ-type, it is possible to choose the generators in such a way that f becomes the limit of $f_i : A_i \to B_i$.

(1) Let P be a property of algebras of finite type over k. We say that (A, σ) is σ*-pro-*P, if we can choose a prolongation sequence so that each A_i has the property P.
(2) Let Q be a property of homomorphisms of algebras of finite type over k. We say that $f : (A, \sigma) \to (B, \sigma)$ is σ*-pro-*P, if we can choose prolongation sequences so that each $f_i : A_i \to B_i$ has the property Q.

We make analogous definitions for the associated (morphisms of) difference schemes.

Fact 2.13 ([17, 3.8, 3.9])**.** *Let $(A,\sigma) \to (B,\sigma)$ be a morphism of transformal domains of finite σ-type over a difference field (k,σ).*

(1) If it is separable, we can find finite σ-localisations A' of A and B' of B so that $(A',\sigma) \to (B',\sigma)$ is σ-pro-smooth.
(2) If it is separable algebraic, we can find finite σ-localisations A' of A and B' of B so that $(A',\sigma) \to (B',\sigma)$ is σ-pro-étale.
(3) If (A,σ) is separable over (k,σ), we can find a finite σ-localisation (A',σ) of A which is normal.

Definition 2.11(5) can be extended to difference schemes ([12]) and it is related to the folklore notion of the difference scheme defined by a correspondence W between an algebraic scheme V over (k,σ) and its σ-twist V_σ, whose (F,σ)-points are

$$\{a \in V(F) : (a,\sigma(a)) \in W\}.$$

In [18], we study the properties of direct presentations of generalised difference schemes at length, reconfirming the invaluable role they play in the study of difference geometry.

Definition 2.14. Suppose $h : (P,\Sigma) \to (A,\Sigma)$ is a direct presentation. Then (A,Σ) is called *directly integral*, if $A_0 = h(P_0)$ and $A_1 = h(P_1)$ are integral. It is *directly transformally integral* if it is directly integral, and all $\sigma : A_0 \to A_1$, $\sigma \in \Sigma$ are injective.

Fact 2.15 ([12, Sect. 4.7],[17, 3.14])**.** *Let $(R,\sigma) \to (A,\sigma)$ be a morphism of finite σ-type.*

(1) We can find a σ-localisation (A',σ) of A which is directly presented over R.
(2) If (R,σ) and (A,σ) are transformal domains and the generic fibre of $(R,\sigma) \to (A,\sigma)$ is geometrically transformally integral, then we can σ-localise R and A to get that the fibres A_s, $s \in (R,\sigma)(F,\varphi)$ are geometrically directly transformally integral.

Recall that a Σ-ideal I is Σ-*perfect* if for every $\sigma \in \Sigma$, $aa^\sigma \in I$ implies a and a^σ are both in I.

Definition 2.16. A difference ring (A,Σ) is *Ritt* if it has the ascending chain condition on Σ-perfect ideals.

Cohn proved in ([5]) 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. We can generalise these considerations as follows.

Fact 2.17 ([19, 2.46])**.** *Let (A,Σ) be an nearly-strict algebra of finite Σ-type over a Ritt difference ring (R,σ), and suppose Σ is finite. Then $\mathrm{Spec}^\Sigma(A)$ is topologically Noetherian and S has an ascending chain condition on ideals which are σ-perfect for any $\sigma \in \Sigma$.*

2.4. **Babbitt's decomposition.** This subsection consists mainly of (re)statements of relevant results from [17] so we omit the proofs.

Definition 2.18. Let $(K,\sigma) \to (L,\sigma)$ be a separable difference field extension. The *core* of L over K is the union of all difference field subextensions (L_0,σ) with $[L_0 : K]$ finite.

It is shown in [5] that, when $(K,\sigma) \to (L,\sigma)$ is of finite σ-type, the core of L over K is a finite extension of K.

Proposition 2.19 ([12, Sect. 4.3])**.** *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 $[\varsigma]_R$, i.e., 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).

We omit the proof, but briefly recall the construction of $[\varsigma]_R A$ in notation of [17]. 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 $i \le j$. Writing

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

where the tensor product is taken over R, and

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

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.

Definition 2.20. A morphism $(S,\sigma) \to (R,\sigma)$ of integral 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 $i \ge 0$ (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.

It is *proper benign*, if each R_i is integral over S. It is *benign Galois*, if R_0 is Galois over S.

Remark 2.21. Suppose that $(R,\sigma) \simeq [\sigma]_S R_0$ is benign Galois over (S,σ) and let $G_0 = \mathrm{Gal}(R_0/S)$. Then the Galois group $\mathrm{Gal}(R/S) = \mathrm{Gal}(\mathbf{k}(R)/\mathbf{k}(S)) = (G, ()^\sigma)$, in the sense of 3.1, is isomorphic to the direct product of copies $G_i = \mathrm{Gal}(R_i/S)$ of G_0 and the operator $()^\sigma$ 'shifts' from G_i to G_{i+1}.

It follows that any two elements h, h' of G are $()^\sigma$*-conjugate,* i.e., there is a $g \in G$ such that $h' = g^{-1} h g^\sigma$.

Remark 2.22. Babbitt's original definition [2] calls a quasi-Galois (normal) algebraic extension $(K,\sigma) \to (L,\sigma)$ of finite σ-type benign, if there exists an $\alpha \in L$ such that L is σ-generated by α over K and $[K(\alpha) : K]$ equals the *limit degree* of L/K, which is the eventual degree of L_{i+1}/L_i, where $L_i = K(\alpha, \ldots, \sigma^i\alpha)$. This condition is equivalent to saying that L is the composite of linearly disjoint fields $K(\sigma^i\alpha) = L_{0\sigma^i}$ over K, where $L_{0\sigma^i} = L_0 \otimes_K K$ is the twist of L_0 via $\sigma^i : K \to K$. Through the well-known relationship of linear disjointness and tensor product of fields, this is equivalent to L being the limit tensor product of the $L_{0\sigma^i}$ over K, i.e., $(L,\sigma) = [\sigma]_K[L_0]$. Thus, our definition extends the classical one.

The following is an easy consequence of 2.21.

Lemma 2.23. *Let $(S,\sigma) \to (R,\sigma)$ be a proper benign Galois extension of (k,σ)-algebras. For any algebraically closed difference field (F,φ) extending (k,σ), any $\bar{y} \in (S,\sigma)(F,\varphi)$ and any $g \in \mathrm{Gal}(R/S)$, there exists an $\bar{x} \in (R,\sigma g)(F,\varphi)$ lifting $\bar{y}$.*

Definition 2.24. A morphism $(\psi,()^{\psi}) : (S,T) \to (R,\Sigma)$ of difference rings is *benign* if for all $\sigma \in \Sigma$, the morphism $(S,\sigma^{\psi}) \to (R,\sigma)$ is benign.

The fundamental theorem of [2] is stated for an extension of *inversive* difference fields. We note that it can be applied to a σ-separable extension of arbitrary difference fields. Recall that an extension $(K,\sigma) \to (L,\sigma)$ is called *σ-separable* when L is linearly disjoint from K^{inv} over K.

Fact 2.25 (Babbitt's Theorem, [2])**.** *Let $(K,\sigma) \to (L,\sigma)$ be a σ-separable 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 where L_0 is the core of L over K (and thus L_0/K is finite) and all L_{i+1}/L_i are benign for $i \geq 0$.

Using normalisation techniques, we lift Babbitt's theorem to a deep structure theorem about difference ring extensions.

Fact 2.26 (Babbitt's decomposition, [17, 5.12])**.** *Every (generically) separable quasi-Galois Σ-separable morphism of finite transformal type $(S,\sigma) \to (R,\Sigma)$ of normal (integrally closed) nearly-strict transformal domains factorizes as*

$$(S,\sigma) \to (R_0,\Sigma_0) \to (R_1,\Sigma_1) \to \cdots (R_n,\Sigma_n) \simeq (R,\Sigma),$$

where $(S,\sigma) \to (R_0,\Sigma_0)$ is generically finite separable quasi-Galois and for $i \geq 0$, $(R_i,\Sigma_i) \to (R_{i+1},\Sigma_{i+1})$ is benign Galois. Modulo a transformal localisation of S, we can achieve that $(S,\sigma) \to (R_0,\Sigma_0)$ is finite étale quasi-Galois, and that $R_i \to R_{i+1}$ are étale benign Galois.

Definition 2.27. Let $(S,\tau) \to (R,\Sigma)$ be a morphism of transformal domains, and let (L,Σ) be the relative algebraic closure of $(\mathbf{k}(S),\tau)$ in $(\mathbf{k}(R),\Sigma)$. We shall say that it is a *generic weak cover* extension if $(\mathbf{k}(S),\tau) \to (L,\Sigma)$ is (algebraically) Galois, and Σ is a *finite* set containing the representatives of the isomorphism classes of lifts of τ to $\mathbf{k}(R)$.

Generic difference covering extensions are abundant, i.e., any reasonable morphism can be subsumed in a generic difference covering extension in the technical sense of [17, 5.25].

2.5. **Existentially closed difference fields.**

Fact 2.28 ([15],[4])**.** *The first-order theory of difference fields has a model-companion called* ACFA*. It axiomatises existentially closed difference fields. In fact, the axiom scheme is obtained by translating the following statements into the first-order language of difference rings. A difference field (F,φ) is existentially closed whenever*

1. *F is algebraically closed;*
2. *φ is an automorphism;*
3. *for all F-algebraic varieties V and $W \hookrightarrow V \times V_{\varphi}$ projecting dominantly on V and V_{φ}, there is a point $a \in V(F)$ such that $(a,\varphi(a)) \in W$.*

In the sequel, we shall frequently consider a difference field (k,σ) and a class of existentially closed difference fields extending it. We shall write ACFA_k for its first-order theory.

Many subsequent developments go through for algebraically closed difference fields and do not require the field to be existentially closed. We shall be precise about this.

Lemma 2.29. *Let (X,σ) be a difference scheme of finite transformal type over (k,σ), and let (F,σ) be an existentially closed difference field extending (k,σ).*

(1) If X is directly geometrically transformally integral then it has an (F,φ)-point, i.e.,

$$X(F,\sigma)\neq\emptyset.$$

(2) If X is well-mixed then

$$X(F,\sigma)\neq\emptyset.$$

(3) The natural morphism

$$X(F,\varphi)\to X,$$

which maps a geometric point $\bar{x}\in X(F,\varphi)$ to its locus $x\in X$, is surjective on closed points of X.

Proof. In view of the terminology fixed in 2.11(5), the statement (1) is precisely the ACFA-axiom from 2.28. For (2), we can reduce to the case $X=\mathrm{Spec}^\sigma(R)$ for (R,σ) well-mixed of finite transformal type over k, say $R=k[x_1,\ldots,x_n]_\sigma$. Since R is well-mixed, it is known ([12], [14, 2.2.4], [19, 2.21]) that $\mathrm{Spec}^\sigma(R)\neq\emptyset$ so we can choose an element $\mathfrak{p}$ in it. Since R is of finite σ-type, it is Ritt ([5]) and thus $\mathfrak{p}$ can be perfectly generated by finitely many elements, $f_1,\ldots,f_r\in R$, say. Clearly, $f_i=P_i(x_1,\ldots,x_n)$ for some difference polynomial P_i over k. Since (F,σ) is existentially closed, the system $P_1=\cdots=P_n=0$ has a solution in F, which yields a geometric point localised at $\mathfrak{p}$. The statement (3) is obvious. □

3. Galois stratification

3.1. **Difference ring/scheme covers.** One of the disadvantages of our approach which avoids the use of generalised difference schemes is that it forces us into an excursion into the theory of infinite Galois covers of difference rings. Although the final results tell us that only finite Galois covers are relevant in the theory of Galois stratification, several proofs pass through auxiliary infinite covers. We note that [19] and [17] *never* discuss infinite Galois covers in an essential way.

Definition 3.1. Let (C,σ) be of finite σ-type over a difference field (k,σ). We will say that a profinite group $(G,()^\sigma)$ with a continuous endomorphism $()^\sigma:G\to G$ acts *continuously* on (C,σ) if:

(1) there exists a finite tuple c of σ-generators of C such that, $(C,\sigma)=k[c]_\sigma=\varinjlim\langle C_i,\sigma_i;\pi_i\rangle$, where $C_i=k[c,\ldots,\sigma^i c]$, $\pi_i:C_i\hookrightarrow C_{i+1}$ and $\sigma_i:C_i\to C_{i+1}$ satisfy

$$\sigma_{i+1}\pi_i=\pi_{i+1}\sigma_i,\quad i\in\mathbb{N};$$

(2) for every i, we have a finite group G_i acting on C_i, and homomorphisms $()^{\pi_i}:G_{i+1}\to G_i$, $()^{\sigma_i}:G_{i+1}\to G_i$ satisfying

$$\pi_i g^{\pi_i}=g\pi_i,\quad\text{and}\quad\sigma_i g^{\sigma_i}=g\sigma_i,\quad\text{for } g\in G_{i+1};$$

(3) we have

$$(G, ()^\sigma) = \varprojlim \langle G_i, ()^{\sigma_i}; ()^{\pi_i} \rangle.$$

Let $A = C^G = \varinjlim A_i$, for $A_i = C_i^{G_i}$. From the property

$$\sigma g^\sigma = g\sigma,$$

it follows that $\sigma(A) \subseteq A$, so that (A, σ) is a difference ring of invariants. For every i, let Σ_i denote the set of homomorphisms $C_i \to C_{i+1}$ lifting $\sigma_i : A_i \to A_{i+1}$ and assume that $\Sigma_i = \sigma_i G_i$. Let $(C, \Sigma) = (\varinjlim C_i, \varprojlim \Sigma_i)$, i.e.,

$$\Sigma = \sigma G,$$

with the continuous action of G by (C, Σ)-automorphisms, where $()^g : \Sigma \to \Sigma$ is

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

Under these conditions, we say that

$$(A, \sigma) \to (C, \Sigma)$$

is a *Galois* extension with *Galois group* $(G, \tilde{\Sigma})$, where $\tilde{\Sigma} = \{()^\tau : \tau \in \Sigma\}$.

Remark 3.2. Examples of Galois extension abound. Let (A, σ) be a normal transformal domain of finite σ-type over (k, σ) and let (L, Σ) be a an extension of $(\mathbf{k}(A), \sigma)$ of finite transformal type with $L/\mathbf{k}(A)$ Galois, and Σ is the set of all lifts of σ to L. Let (C, Σ) be the integral closure of (A, σ) in (L, Σ). Then $(A, \sigma) \to (C, \Sigma)$ is a Galois extension with group $G = \mathrm{Gal}(L/\mathbf{k}(A))$. Indeed, from[3, V, §2.3, Corollaire 1 to Proposition 6], it follows immediately that, for any $\tau \in \Sigma$, we have

$$\Sigma = \tau G$$

and that we have a continuous homomorphism $()^\tau : G \to G$ such that, for every $g \in G$,

$$g\tau = \tau g^\tau.$$

Thus $(G, \tilde{\Sigma})$, where $\tilde{\Sigma} = \{()^\tau : \tau \in \Sigma\}$ acts by generalised difference automorphisms on (C, Σ), where $()^g : \Sigma \to \Sigma$ is given by $\tau^g = g^{-1}\tau g = \tau(g^{-1})^\tau g \in \Sigma$. The continuity of the action is clear, and moreover $C^G = C \cap \mathbf{k}(C)^G = C \cap \mathbf{k}(A) = A$ since A is integrally closed.

The most important case of *finite* G conforms to a more general treatment in [19, Section 3]. The following is a weaker infinitary variant of [19, Proposition 3.1].

Proposition 3.3. *Suppose that $(A, \tau) \to (C, \Sigma)$ is a Galois extension of difference rings of finite transformal type with group $(G, \tilde{\Sigma})$. Let $X = \mathrm{Spec}^\Sigma(C)$, $Y = \mathrm{Spec}^\tau(A)$ and let $p : (X, \Sigma) \to (Y, \tau)$ be the canonical (G-invariant) morphism. Then the following holds.*

(1) C is integral over A.

(2) The morphism p is surjective and its fibres are G-orbits.

(3) Let $x \in X$, $y = p(x)$, let G_x be the stabiliser of x and let $\Sigma_x = \{\sigma \in \Sigma : \sigma(x) = x\} = \{\sigma \in \Sigma : x \in X^\sigma\}$. 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.

(4) (Y,σ) *is a geometric quotient of* (X,Σ) *by* $(G,\tilde{\Sigma})$*, i.e., for an algebraically closed difference field* (F,φ)*,*

$$(A,\sigma)(F,\varphi) \simeq (C,\Sigma)(F,\varphi)/G.$$

Proof. The statement (1) is obvious, since every C_i is integral over A_i.
(2) Recall that p is the morphism associated to the inclusion $(A,\tau) \hookrightarrow (C,\Sigma)$. Let us denote $\tilde{p} : \tilde{X} \to \tilde{Y}$ the morphism of ambient affine schemes $\tilde{X} = \mathrm{Spec}(C)$ and $\tilde{Y} = \mathrm{Spec}(A)$ induced by $A \hookrightarrow C$, so that $p = \tilde{p} \restriction X$. The statement of (2) for $\tilde{p}$ follows by continuity and the classically known statement for each $\mathrm{Spec}(C_i) \to \mathrm{Spec}(A_i)$. Thus, it suffices to prove that $\tilde{p}^{-1}(Y) = X$. Pick an $y \in Y$. Then, for any $\sigma \in \Sigma$ we have $\tilde{p} \circ {}^a\sigma = {}^a\tau \circ \tilde{p}$ on $\tilde{X}$, so given any $x \in \tilde{X}$ such that $\tilde{p}(x) = y$,

$$\tilde{p}({}^a\sigma x) = {}^a\tau(\tilde{p}x) = {}^a\tau(y) = y = \tilde{p}(x),$$

so there exists a $g \in G$ with ${}^a\sigma x = gx$. By assumption, ${}^aG\,{}^a\Sigma \subseteq {}^a\Sigma$, so $x \in X^{g^{-1}\sigma} \subseteq X$.
(3) The fact that the natural homomorphism $G_x \to \mathrm{Gal}(\mathbf{k}(x)/\mathbf{k}(y))$ is surjective is known (loc. cit), and the difference superstructure is a bookkeeping exercise.
(4) This statement is immediate from item (2). □

Definition 3.4. Let $(A,\sigma) \to (C,\Sigma)$ be a morphism of normal transformal domains of finite transformal type over a difference field such that $\mathbf{k}(C)$ is a separable algebraic extension of $\mathbf{k}(A)$. Let $\tilde{L}$ be the (algebraic) Galois closure of $\mathbf{k}(C)$ over $\mathbf{k}(A)$, and let $\tilde{\Sigma}$ be the set of all lifts of σ from $\mathbf{k}(A)$ to $\tilde{L}$, and $\mathring{\Sigma} \subseteq \tilde{\Sigma}$ is the set of all lifts of Σ from $\mathbf{k}(C)$ to $\tilde{L}$. Let $\tilde{C}$ be the normalisation of C in $\tilde{L}$. The diagram

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

is called the *Galois closure* of (C,Σ) over (A,σ).

Fact 3.5 ([17, 3.15])**.** *Let* (A,σ) *be a transformal domain of finite* σ*-type over* (R,σ) *and let* $(A,\sigma) \to (C,\Sigma)$ *be a finite Galois extension over* (R,σ)*. If the generic fibres of* $(R,\sigma) \to (A,\sigma)$ *and* $(R,\sigma) \to (C,\Sigma)$ *are geometrically transformally integral, by* σ*-localising* R*,* A*,* C*, we can achieve that the fibres* A_s *and* C_s *are geometrically directly transformally integral and that*

$$\mathrm{Gal}(C_s/A_s) = \mathrm{Gal}(C/A),$$

for all $s \in (R,\sigma)(F,\varphi)$*.*

Definition 3.6. We shall say that a Galois extension $(A,\sigma) \to (C,\Sigma)$ is *étale*, if for every geometric point $c \in (C,\Sigma)(F,\varphi)$, the stabiliser of c in G is trivial, or, equivalently, if for all $x \in \mathrm{Spec}^{\Sigma}(C)$, the canonical map from 3.3(3) is bijective (i.e., the *inertia* group at x is trivial).

Remark 3.7. In the case of a finite group action, the term 'étale' can be fully justified by combining [19, Section 3.2] and [17, 3.41].

In the infinite case, it is clear that a Galois extension which is σ-pro-étale in the sense of 2.12 (namely, where all $A_i \to C_i$ are (algebraically) étale), is étale in

the above sense. This observation is important since it allows us to conclude that étaleness can be achieved modulo a σ-localisation via 2.13.

Example 3.8 (A finite étale Galois extension)**.** Consider the difference algebra

$$C = k[x_i : i \in \mathbb{N}]/\langle x_{i+1}^3 x_i^7 - 1 : i \in \mathbb{N}\rangle$$

over a difference field k containing the primitive fourth root of unity ξ, with the operator σ induced by the rule $x_i \mapsto x_{i+1}$. Let $g : C \to C$ be the algebra automorphism extending the rule $gx_0 = \xi x_0$, and write $G = \langle g\rangle$ for the group generated by g, isomorphic to the group μ_4 of fourth roots of unity. Let $\pi : (C, \sigma) \to (C, \sigma)$ be the difference algebra endomorphism defined by $\pi(x_0) = x_0^4$. Then $A = C^G = \pi(C)$, and we have a finite étale Galois extension $(A, \sigma) \to (C, \Sigma)$, where $\Sigma = \sigma G$.

An easy calculation shows that $()^\sigma : G \to G$ swaps g and g^3 and fixes 1 and g^2, and that the $()^\sigma$-conjugacy classes in G are $\{1, g^2\}$ and $\{g, g^3\}$. Consequently, the G-conjugacy classes in Σ are $\{\sigma, \sigma g^2\}$ and $\{\sigma g, \sigma g^3\}$.

Example 3.9 (A benign Galois extension)**.** Let $C = k[x_i : i \in \mathbb{N}]$ with $\sigma : x_i \mapsto x_{i+1}$ be the difference polynomial ring in one variable, and let $A = k[x_i^2 : i \in \mathbb{N}] \subseteq C$. It is clear that $(C, \sigma) = [\sigma]_A A[x_0]$, i.e., C is an infinite tensor product of $A[x_i]$ over A, so this is a benign extension. Let $G = \prod_i \mu_2$ be the infinite product of groups $\mu_2 = \{1, -1\}$ acting in the obvious way on C over A so that $A = C^G$. The homomorphism $()^\sigma : G \to G$ is given by $(g_0, g_1, g_2, \ldots)^\sigma = (g_1, g_2, \ldots)$. To conclude, $(A, \sigma) \to (C, \sigma G)$ is a Galois extension with group $(G, \tilde{\Sigma})$, for $\Sigma = \sigma G$. We invite the reader to verify that all the elements of G are $()^\sigma$-conjugate, which illustrates the general principle 2.21 (and [17, 5.19]).

By a discussion analogous to that in [19, Section 3.2], the following definition is meaningful.

Definition 3.10. Let $(A, \sigma) \to (C, \Sigma)$ be an étale Galois extension, and let (F, φ) be an algebraically closed difference field.

(1) For $c \in (C, \Sigma)(F, \varphi)$, the *local φ-substitution at c* is the unique element $\varphi_c \in \Sigma$ satisfying
$$c\varphi_c = \varphi c.$$
(2) If $a \in (A, \sigma)(F, \varphi)$ is the restriction of $c, c' \in (C, \Sigma)(F, \varphi)$ to A, there exists a $g \in G$ with $c' = cg$ and
$$c\varphi_c = \varphi c = \varphi c' g^{-1} = c'\varphi_{c'} g^{-1} = cg\varphi_{c'} g^{-1},$$
so we conclude that φ_c and $\varphi_{c'}$ are G-conjugate, or, equivalently, Σ-conjugate. Thus we define the *local φ-substitution at a* to be the G-conjugacy class φ_a of any φ_c with c restricting to a.

Definition 3.11. Let (C, Σ) be a (generalised) difference ring and let (X, σ) be a difference scheme. We say that $(C, \Sigma)/(X, \sigma)$ is a *difference ring/scheme Galois cover* if there exists an étale Galois extension $(A, \sigma) \to (C, \Sigma)$ such that (X, σ) is isomorphic to $\mathrm{Spec}^\sigma(A)$.

Clearly, if $x \in X(F, \varphi)$ is a point with values in an algebraically closed difference field (F, φ) corresponding to a morphism $a : (A, \sigma) \to (F, \varphi)$, we can define the *local φ-substitution at x* as
$$\varphi_x = \varphi_x^{C/X} = \varphi_a.$$

3.2. **Galois stratifications and Galois formulae.**

Definition 3.12. Let (X,σ) be a (k,σ)-difference scheme. Its *realisation functor* $\tilde{X}$ assigns to each difference field (F,φ) extending (k,σ) the set

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

A (k,σ)-*subassignment* of X is any subfunctor $\mathcal{F}$ of $\tilde{X}$. Namely, for any (F,φ) extending (k,σ),

$$\mathcal{F}(F,\varphi) \subseteq X(F,\varphi),$$

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

Definition 3.13. Let (k,σ) be a difference field and let (X,σ) be a difference scheme over (k,σ). A *normal (twisted) Galois stratification*

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

of (X,σ) over (k,σ) is a partition of (X,σ) into a finite set of of integral normal σ-locally closed difference (k,σ)-subvarieties (X_i,σ) of (X,σ), each equipped with a *finite* difference ring/scheme Galois cover $(C_i,\Sigma_i)/(X_i,\sigma)$ over (k,σ) (with a finite group $(G_i,\tilde{\Sigma}_i)$ and a finite structure Σ_i), and Γ_i is a 'conjugacy domain' in Σ_i.

We reserve the possibility to consider *infinitary* stratifications $\langle X, C_i/X_i, \Gamma_i \,|\, i \in I\rangle$ with arbitrary Galois ring/scheme covers C_i/X_i, but these will only occur in proofs as auxiliary objects.

Definition 3.14. We define the *(twisted) Galois formula* over (k,σ) associated with the above stratification $\mathcal{A}$ to be its realisation subassignment $\tilde{\mathcal{A}}$ of X. Given an algebraically closed difference field (F,φ) extending (k,σ),

$$\tilde{\mathcal{A}}(F,\varphi) = \bigcup_i \{x \in X_i(F,\varphi) \mid \varphi_x^{C_i/X_i} \subseteq \Gamma_i\}.$$

The same definition applies to infinitary stratifications.

Definition 3.15. Let $\mathcal{A} = \langle X, C_i/X_i, \Gamma_i\rangle$ be a (k,σ)-Galois stratification on a difference scheme (X,σ).

(1) Suppose that for each i we have a difference ring/scheme (k,σ)-covering $(C_i',\Sigma_i')/(X_i,\sigma)$ which dominates $(C_i/\Sigma_i)/(X_i,\sigma)$. Let $\pi_i : \Sigma_i' \to \Sigma_i$ denote the associated *Diff*-morphism. The *inflation* of $\mathcal{A}$ is defined as

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

and has the property that for every algebraically closed (F,φ) extending (k,σ),

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

(2) Suppose that we have a further stratification of X_i into finitely many integral normal locally closed (k,σ)-difference subschemes X_{ij}. For each i,j, let $\mathfrak{p}_{ij} \in \mathrm{Spec}^\sigma(A)$ be the ideal corresponding to the generic point of X_{ij} and let $\mathfrak{q}_{ij}$ be an element of $\mathrm{Spec}^\Sigma(C_i)$ extending $\mathfrak{p}_{ij}$. Let G_{ij} be the stabiliser of $\mathfrak{q}_{ij}$ in G, let $\Sigma_{ij} = \{\sigma \in \Sigma_i : \sigma^{-1}(\mathfrak{q}_{ij}) = \mathfrak{q}_{ij}\}$, and write $\iota_{ij} : \Sigma_{ij} \hookrightarrow \Sigma_i$, $C_{ij} = C_i/\mathfrak{q}_{ij}$. Then each $(C_{ij},\Sigma_{ij})/(X_{ij},\sigma)$ is a ring/scheme covering with group $(G_{ij},\tilde{\Sigma}_{ij})$. The *refinement* of $\mathcal{A}$ is defined as

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

and has the property that for every algebraically closed (F,φ) extending (k,σ),

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

Definition 3.16. Let $(X,\sigma) = \mathrm{Spec}^\sigma(A)$ be a (k,σ)-difference scheme. The class of (k,σ)-Galois formulae on X has a *Boolean algebra* structure as follows.

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

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

(2) $\mathcal{A}\wedge\mathcal{B} = \langle X, C_i/X_i, \Gamma_i\cap\Delta_i\rangle$.
(3) $\mathcal{A}\vee\mathcal{B} = \langle X, C_i/X_i, \Gamma_i\cup\Delta_i\rangle$.
(4) $\neg\mathcal{A} = \langle X, C_i/X_i, \Sigma_i\setminus\Gamma_i\rangle$.

Example 3.17. With notation from 3.8, let $X = \mathrm{Spec}^\sigma(A)$ and consider the Galois stratifications $\mathcal{A} = \langle X, C/X, \{\sigma, \sigma g^2\}\rangle$ and $\mathcal{A}' = \neg\mathcal{A} = \langle X, C/X, \{\sigma g, \sigma g^3\}\rangle$ associated with the difference ring/scheme cover $(C,\Sigma)/(X,\sigma)$. Intuitively speaking, X is the difference scheme defined by the equation $x^7\sigma x^3 = 1$. Let X' be the difference scheme defined by $x^7\sigma x^3 = \xi$ and let $\pi' : X' \to X$ be the morphism $\pi'(x) = x^4$. Then, for every algebraically closed difference field (F,φ) extending (k,σ),

$$\mathcal{A}(F,\varphi) = \{y \in X(F,\varphi) : \exists x \in X(F,\varphi), x^4 = y\} = \pi(X(F,\varphi)),$$
$$\mathcal{A}'(F,\varphi) = \{y \in X(F,\varphi) : \exists x \in X'(F,\varphi), x^4 = y\} = \pi'(X'(F,\varphi)),$$

illustrating the general principle that Galois formulae correspond to first-order formulae, proved in 3.26.

3.3. **Direct Image Theorems.** The following result can be considered as a difference version of Chevalley's theorem from algebraic geometry stating that a direct image of a constructible set by a scheme morphism of finite presentation is again constructible. It follows promptly from [17, 7.7] and 2.29.

Proposition 3.18. *Let $(A,\sigma) \to (C,\Sigma)$ be a generic weak cover extension over (k,σ) of finite transformal type, let $(Y,\sigma) = \mathrm{Spec}^\sigma(A)$ and denote by*

$$f : (C,\Sigma)(F,\varphi) \to Y(F,\varphi)$$

the corresponding map of points in an existentially closed difference field (F,φ) extending (k,σ). Then the image of f contains a dense open subset of Y.

An important way of reading this result is the following. Images of (dominant) morphisms of ordinary difference schemes rarely contain an open subset, as we shall see in the sequel. However, by a finite 'fattening' of the difference structure of the domain, one can achieve that the range contains an open subset of the codomain. A variant of this idea appears in [20], where the author considers an enrichment by higher powers of σ.

Definition 3.19. Let (X,σ) be a difference scheme over a difference field (k,σ). Let $\mathcal{F}$ and $\mathcal{F}'$ be (k,σ)-subassignments of X. We shall say that $\mathcal{F}$ and $\mathcal{F}'$ are *equivalent modulo* ACFA_k and write

$$\mathcal{F} \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \mathcal{F}',$$

if for every existentially closed difference field (F,φ) extending (k,σ),

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

If the above happens already for all algebraically closed difference fields (F,φ), extending (k,σ), we shall write

$$\mathcal{F} \equiv_{(k,\sigma)} \mathcal{F}',$$

or, even more nonchalantly, we may write $\mathcal{F} \equiv \mathcal{F}'$ when (k,σ) is understood.

Definition 3.20. Let $f : (X,\sigma) \to (Y,\sigma)$ be a morphism of (k,σ)-difference schemes and let $\mathcal{A}$ be Galois stratification on X. For an algebraically closed difference field (F,φ) extending (k,σ), we define a subassignment $f_\exists\mathcal{A}$ of Y by the rule

$$f_\exists\mathcal{A}(F,\varphi) = f(\mathcal{A}(F,\varphi)) \subseteq Y(F,\varphi).$$

Lemma 3.21. *Suppose $(C,\Sigma_0)/(X,\sigma)$, $(C,\Sigma)/(Y,\sigma)$ are difference ring/scheme covers and let $f : (X,\sigma) \to (Y,\sigma)$ be a morphism compatible with the covers, inducing an inclusion $\mathrm{Gal}((C,\Sigma_0)/(X,\sigma)) \hookrightarrow \mathrm{Gal}((C,\Sigma)/(Y,\sigma))$. Then, writing $\iota : \Sigma_0 \hookrightarrow \Sigma$, for any $\mathrm{Gal}(C/X)$-conjugacy domain $\Gamma_0 \subseteq \Sigma_0$ we have*

$$f_\exists\langle (C,\Sigma_0)/(X,\sigma), \Gamma_0\rangle \equiv \langle (C,\Sigma)/(Y,\sigma), \iota_*\Gamma_0\rangle,$$

where $\iota_*\Gamma_0$ is the $\mathrm{Gal}(C/Y)$-conjugacy domain induced by Γ_0 in Σ.

Proof. Let us check the non-trivial right-to-left inclusion. Let (F,φ) be an algebraically closed difference field. Let $y \in Y(F,\sigma)$ with $\varphi_y \in \iota_*\Gamma_0$. There exists a $c \in (C,\Sigma)(F,\varphi)$ with $\varphi_c \in \iota_*\Gamma_0$, say $\varphi_c \in \Gamma_0^g$ for some $g \in \mathrm{Gal}((C,\Sigma)/(Y,\sigma))$. Then $\varphi_{g^{-1}c} \in \Gamma_0$, so the point $x \in X(F,\varphi)$ corresponding to the image of $g^{-1}c$ has the properties $\varphi_x \subseteq \Gamma_0$ and $f(x) = y$. □

The following is a direct consequence of 2.23.

Lemma 3.22. *Suppose we have the Babbitt's decomposition of a Galois covering*

$$(\tilde{C},\tilde{\Sigma})/(C,\Sigma)/(Y,\sigma),$$

i.e., $(\tilde{C},\tilde{\Sigma})/(Y,\sigma)$ and $(C,\Sigma)/(Y,\sigma)$ are ring/scheme covers, the extension of difference rings $(C,\Sigma) \to (\tilde{C},\tilde{\Sigma})$ is a tower of benign extensions, and $(\mathbf{k}(C),\Sigma)$ is the core of $(\mathbf{k}(Y),\sigma)$ in $(\mathbf{k}(\tilde{C}),\tilde{\Sigma})$. Writing $\pi : \tilde{\Sigma} \to \Sigma$ for the relevant Diff-surjection, for any conjugacy domain Γ in $\tilde{\Sigma}$,

$$\langle (\tilde{C},\tilde{\Sigma})/(Y,\sigma), \Gamma\rangle \equiv \langle (C,\Sigma)/(Y,\sigma), \pi_*\Gamma\rangle,$$

where $\pi_*\Gamma$ is the image of Γ by π.

The main result of this paper, Theorem 1.1, states that the class of Galois formulae over fields with Frobenii is closed under taking images by $f_\exists$. More precisely, we have the following.

Theorem 3.23. *Let $f : (X,\sigma) \to (Y,\sigma)$ be a morphism of difference schemes of finite σ-type over a difference field (k,σ). For every Galois formula $\mathcal{A}$ on X there exists a Galois formula $\mathcal{B}$ on Y such that*

$$f_\exists\mathcal{A} \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \mathcal{B}.$$

More explicitly, for each existentially closed difference field (F,φ) extending (k,σ),

$$(f_\exists\mathcal{A})(F,\varphi) = f(\mathcal{A}(F,\varphi)) = \mathcal{B}(F,\varphi).$$

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

By decomposing the situation into components, we reduce to the case where X and Y are transformally integral. Moreover, the case when f is purely inseparable or purely σ-inseparable is easily resolved.

Thus, using 3.18, after a possible refinement of $\mathcal{A}$, we obtain stratifications X_i and Y_j into transformally integral normal locally closed (k,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 dominant and generically σ-smooth (i.e., we can achieve that $\mathbf{k}(Y_j) \to \mathbf{k}(X_i)$ is separable and σ-separable) and that on each X_i, $\mathcal{A}$ is basic (i.e., given by a single Galois cover).

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 in view of 2.5, we may assume that f is obtained as a spectrum of a morphism $(B,\sigma) \to (A,\sigma)$ and we may further assume that $\mathcal{A}$ on X is basic, $\mathcal{A} = \langle C/X, \Gamma\rangle$, given by étale Galois extension of transformal domains $(A,\sigma) \to (C,\Sigma)$ with group $(G,\tilde{\Sigma}_C)$ and a conjugacy domain $\Gamma \subseteq \Sigma_C$.

Let L be the relative algebraic closure of $\mathbf{k}(Y)$ in $\mathbf{k}(X)$, and let $\tilde{Y}$ be the normalisation of Y in L. We obtain a baby Stein factorisation $(X,\sigma) \to (\tilde{Y},\sigma) \to (Y,\sigma)$, where the generic fibre of the first morphism is geometrically transformally integral (since $\mathbf{k}(\tilde{Y}) \to \mathbf{k}(X)$ is regular), and the second is generically σ-étale (since $\mathbf{k}(Y) \to \mathbf{k}(\tilde{Y})$ is separable algebraic, as well as σ-separable).

It is enough to show that the direct image of a Galois formula by both morphisms is (equivalent to) a Galois formula. Therefore, we can reduce our consideration to two cases.

Case 1: The generic fibre of f is geometrically transformally integral.

Let (D,Σ_D) be the integral closure of (B,σ) in the relative algebraic closure of $\mathbf{k}(B)$ in $(\mathbf{k}(C),\Sigma_C)$. Then (D,Σ_D) is a Galois cover of (Y,σ). Writing $(E,\Sigma_E) = (A,\sigma) \otimes_{(B,\sigma)} (D,\Sigma_D)$, we obtain an exact sequence

$$1 \to \mathrm{Gal}(C/E) \to \mathrm{Gal}(C/X) \to \mathrm{Gal}(D/Y) \to 1.$$

Note that $\mathbf{k}(D) \to \mathbf{k}(C)$ is regular, so by a σ-localisation and 2.15, 3.5, we may assume that:

(1) $(D,\Sigma_D)/(Y,\sigma)$ is finite étale Galois;
(2) both $B \to A$ (i.e. f) and $D \to C$ have geometrically directly transformally integral fibres (consequently $D \to E$ has the same property by base change);
(3) for all $d \in D$, $\mathrm{Gal}(C_d/E_d) = \mathrm{Gal}(C/E)$.

Let $\Delta = \pi_*(\Gamma)$ be the image of Γ in Σ_D by the *Diff*-quotient morphism

$$\pi : \Sigma_C \to \Sigma_C/\mathrm{Gal}(C/E) = \Sigma_D.$$

We claim that

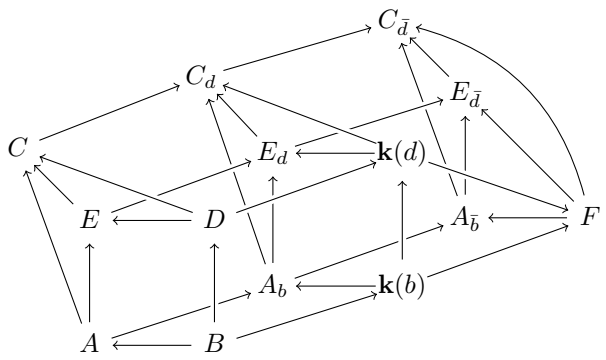
$$f_\exists\langle C/X,\Gamma\rangle \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \widetilde{\langle D/Y,\Delta\rangle},$$

i.e., for all existentially closed (F,φ) extending (k,σ),

$$\{y \in Y(F,\varphi) \mid \exists x \in X(F,\varphi), \varphi_x \in \Gamma, f(x) = y\} \\ = \{y \in Y(F,\varphi) \mid \varphi_y \in \Delta\}.$$

A verification of the left to right inclusion can be done even for F algebraically closed, without the assumption of existential closedness.

Conversely, let $\bar{y} \in Y(F,\varphi)$, corresponding to some $\bar{b} \in (B,\sigma)(F,\varphi)$ with $\varphi_{\bar{b}} = \Delta_0 \subseteq \Delta$. Pick some $\bar{d}$ in the 'fibre' of D/B above $\bar{b}$ with $\varphi_{\bar{d}} \in D_0$. Let us denote by $b \in \mathrm{Spec}^{\sigma}(B)$ and $d \in \mathrm{Spec}^{\Sigma_D}(D)$ the loci of $\bar{b}$ and $\bar{d}$, and consider the diagram



where

(1) $(A_b,\sigma_b) = (A,\sigma) \otimes_{(B,\sigma)} (\mathbf{k}(b),\sigma^b)$ corresponds to the fibre of X above y,
(2) $(A_{\bar{b}},\sigma_{\bar{b}}) = (A,\sigma) \otimes_{(B,\sigma)} (F,\varphi)$ corresponds to the fibre of X above $\bar{y}$,
(3) $(E_d,\Sigma_d) = (E,\Sigma_E) \otimes_{(D,\Sigma_D)} (\mathbf{k}(d),\Sigma^d)$ corresponds to the 'fibre' of E above d,
(4) $(E_{\bar{d}},\Sigma_{\bar{d}}) = (E,\Sigma_E) \otimes_{(D,\Sigma_D)} (F,\varphi)$ is the fibre of E above $\bar{d}$, where the choice of $\bar{d}$ determines a geometric component $E_{\bar{d}}$ of the fibre of E over $\bar{b}$,
(5) $(C_d,\Sigma_d) = (C,\Sigma_C) \otimes_{(E,\Sigma_E)} (A_d,\Sigma_d) = (C,\Sigma_C) \otimes_{(D,\Sigma_D)} (\mathbf{k}(d),\Sigma^d)$ is the fibre of C above d,
(6) $(C_{\bar{d}},\Sigma_{\bar{d}}) = (C,\Sigma_C) \otimes_{(D,\Sigma_D)} (F,\varphi)$ is the fibre of C above $\bar{d}$.

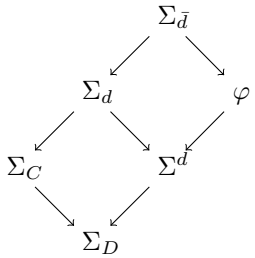
By construction, $X \to Y$ has geometrically directly transformally integral fibres, so A_b and $A_{\bar{b}}$ are directly transformally integral. Moreover, by construction, C_d (and $C_{\bar{d}}$) are directly transformally integral and $\mathrm{Gal}(C_d/E_d) \cong \mathrm{Gal}(C/E)$. In the diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(C_d/E_d) & \longrightarrow & \mathrm{Gal}(C_d/A_b) & \longrightarrow & \mathrm{Gal}(\mathbf{k}(d)/\mathbf{k}(b)) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Gal}(C/E) & \longrightarrow & \mathrm{Gal}(C/A) & \longrightarrow & \mathrm{Gal}(D/B) & \longrightarrow & 1 \end{array}$$

the left vertical arrow is an isomorphism so we infer that

$$\mathrm{Gal}(C_d/A_b) = \mathrm{Gal}(C/A) \times_{\mathrm{Gal}(D/B)} \mathrm{Gal}(\mathbf{k}(d)/\mathbf{k}(b))$$

and we get a diagram of difference structures in which both squares are Cartesian:



Since φ maps to $\varphi_{\bar{d}} \in \Delta$ in Σ_D, there will be a $\tau \in \Sigma_{\bar{d}}$ which maps both onto $\varphi_{\bar{d}}$ and into $\Gamma \subseteq \Sigma_C$. It suffices to find a point in $(C_{\bar{d}}, \tau)(F, \varphi)$, and this is possible by 2.29 since $(C_{\bar{d}}, \tau)$ is directly transformally integral over an existentially closed (F, φ).

Case 2: f is generically σ-étale. Using 2.13, we can assume that f is in fact σ-étale. Thus, $f : (X, \sigma) \to (Y, \sigma)$ is obtained as a spectrum of a morphism $(B, \sigma) \to (A, \sigma)$ which is σ-étale and we are given a Galois extension $(A, \sigma) \to (C, \Sigma)$ with C a domain and a conjugacy domain $\Gamma \subseteq \Sigma$.

We let $(\tilde{C}, \tilde{\Sigma})$ and $\iota : \mathring{\Sigma} \hookrightarrow \tilde{\Sigma}$ be the data associated with the Galois closure (3.4) of (C, Σ) over (B, σ). Moreover, let (D, Σ_D) be the integral closure of (B, σ) in the core of $(\mathbf{k}(\tilde{C}), \tilde{\Sigma})$ over $(\mathbf{k}(B), \sigma)$, and denote the associated *Diff*-morphisms by $\pi : \tilde{\Sigma} \to \Sigma_D$. Modulo a σ-localisation (to make it finite étale Galois), we can assume that $(D, \Sigma_D)/(Y, \sigma)$ is a difference ring/scheme cover. Needless to say, $(\tilde{C}, \tilde{\Sigma})/(Y, \sigma)$ and $(\tilde{C}, \mathring{\Sigma})/(X, \sigma)$ are in general infinite Galois covers. We obtain an exact sequence

$$1 \to \mathrm{Gal}(\tilde{C}/D) \to \mathrm{Gal}(\tilde{C}/B) \to \mathrm{Gal}(D/B) \to 1.$$

We inflate Γ in $(C, \Sigma)/(X, \sigma)$ to $\tilde{\Gamma}$ in $(\tilde{C}, \mathring{\Sigma})/(X, \sigma)$, and let us consider the conjugacy domain $\Delta = \pi_* \iota_* \tilde{\Gamma}$ in $(D, \Sigma_D)/(Y, \sigma)$, i.e., the 'deflation' of the the conjugacy class $\iota_* \tilde{\Gamma}$ generated by $\tilde{\Gamma}$ in $\tilde{C}/Y$. We claim that

$$f_\exists \langle (C, \Sigma)/(X, \sigma), \Gamma \rangle \equiv_{(k,\sigma)} \langle (D, \Sigma_D)/(Y, \sigma), \Delta \rangle.$$

In other words, for every algebraically closed difference field (F, φ) extending (k, σ),

$$f(\{x \in X(F, \varphi) : \varphi_x \in \Gamma\}) = \{y \in Y(F, \varphi) : \varphi_y \in \Delta\}.$$

Indeed, by inflation 3.15,

$$\langle (C, \Sigma)/(X, \sigma), \Gamma \rangle \equiv \langle (\tilde{C}, \mathring{\Sigma})/(X, \sigma), \tilde{\Gamma} \rangle$$

and thus

$$f_\exists \langle (\tilde{C}, \mathring{\Sigma})/(X, \sigma), \tilde{\Gamma} \rangle \overset{3.21}{\equiv} \langle (\tilde{C}, \tilde{\Sigma})/(Y, \sigma), \iota_* \tilde{\Gamma} \rangle \overset{3.22}{\equiv} \langle (D, \Sigma_D)/(Y, \sigma), \Delta \rangle.$$

□

Corollary 3.24. *With assumptions of 3.23, we can define a subassignment*

$$f_\forall \mathcal{A} \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \neg f_\exists (\neg \mathcal{A}),$$

and it is again a Galois formula on Y.

3.4. **Quantifier elimination for Galois formulae.** Let (k,σ) be a difference field.

Definition 3.25. (1) By a *first-order formula over* (k,σ) we will mean a first-order formula $\theta(x_1,\dots,x_n;\alpha_1,\dots,\alpha_m)$ in the language of difference rings with free variables $x_1,\dots,x_n$ with parameters $\alpha_1,\dots,\alpha_m$ from k.

(2) A (k,σ)-formula $\theta(x_1,\dots,x_n;\alpha_1,\dots,\alpha_m)$ gives rise to a subassignment $\tilde{\theta}$ of $\mathbb{A}^n_{(k,\sigma)}$ by the following procedure. For any difference field (F,φ) extending (k,σ), we take its set of realisations to be the value

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

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

Theorem 3.26 (Fine quantifier elimination for ACFA_k)**.** *Let (k,σ) be a difference field. The class of definable (k,σ)-subassignments is equal to the class of (k,σ)-Galois formulae modulo the relation $\equiv^{\mathrm{ACFA}}_{(k,\sigma)}$, i.e., modulo* ACFA_k.

More precisely, let $\theta(x) = \theta(x;s)$ be a first order formula in the language of difference rings in variables $x = x_1,\dots,x_n$ with parameters s from k. There exists a Galois stratification $\mathcal{A}$ of the difference affine n-space over k such that

$$\tilde{\theta} \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \tilde{\mathcal{A}}.$$

Conversely, every Galois formula over (k,σ) is $\equiv_{(k,\sigma)}$-equivalent to a first-order formula.

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

(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 $\mathbb{A}^n_{(k,\sigma)}$. 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 $X_i = \mathrm{Spec}^\sigma(A_i)$, we choose a trivial ring/scheme covering $(A_i,\sigma)/(X_i,\sigma)$, and we let $\Gamma_i = \{\sigma\}$ when $X_i \subseteq Z$, and $\Gamma_i = \emptyset$ otherwise. Then $\mathcal{A} = \langle \mathbb{A}^n_{(k,\sigma)}, A_i/X_i, \Gamma_i\rangle$ has the property that

$$\tilde{\theta} = \tilde{\mathcal{A}}.$$

(2) Suppose $\theta(\bar{x}) \equiv \theta_1(\bar{x}) \wedge \theta_2(\bar{x})$. By induction hypothesis, we can find Galois formulae $\mathcal{A}_i$ on $\mathbb{A}^n$ such that $\theta_i \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \mathcal{A}_i$. Then, using 3.16,

$$\theta \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \mathcal{A}_1 \wedge \mathcal{A}_2.$$

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

(4) If $\theta \equiv \neg\theta'$, and $\theta' \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \mathcal{A}$, then using 3.16,

$$\theta \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \neg\mathcal{A}.$$

(5) If $\theta(x_1,\dots,x_n) = \exists x_{n+1}\theta'(x_1,x_2,\dots,x_n,x_{n+1})$, and $\theta' \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \mathcal{A}$ on $\mathbb{A}^{n+1}$, writing x_{n+1} for the projection $\mathbb{A}^{n+1} \to \mathbb{A}^n$ to the variables $x_1,\dots,x_n$, we have that

$$\theta \equiv_{(k,\sigma)} \exists x_{n+1}\theta' \equiv^{\mathrm{ACFA}}_{(k,\sigma)} x_{n+1\exists}\mathcal{A},$$

which is Galois by 3.23.

(6) If $\theta = \forall x_{n+1}\theta'$, and $\theta' \equiv^{\mathrm{ACFA}}_{(k,\sigma)} \mathcal{A}$, then

$$\theta \equiv_{(k,\sigma)} \forall x_{n+1}\theta' \equiv^{\mathrm{ACFA}}_{(k,\sigma)} x_{n+1\forall}\mathcal{A},$$

which is Galois by 3.24.

We have checked all cases so the induction is complete. Note that working with existentially closed difference fields is only crucial in steps 5 and 6.

Conversely, suppose we have a Galois stratification $\mathcal{A} = \langle \mathbb{A}^n_{(k,\sigma)}, Z_i/X_i, C_i\rangle$. By refining it further, we may assume that each Galois covering $(Z_i, \Sigma_i) \to (X_i, \sigma)$ with group $(G, \tilde{\Sigma})$ is embedded in some affine space, in the sense that Z_i is embedded in some $\mathbb{A}^m_k$, and all automorphisms corresponding to elements of G are restrictions of difference rational endomorphisms of $\mathbb{A}^m_k$ to Z_i, and the canonical projection $Z_i \to X_i$ is a restriction of difference rational morphism $\mathbb{A}^m_k \to \mathbb{A}^n_k$. Then, if Γ_i is the conjugacy class of some element $\sigma_i \in \Sigma$, the set

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

can be expressed in a first-order way using an existential formula in the language of difference rings, provided we work over algebraically closed difference fields. When Γ_i is a union of conjugacy classes, we take the disjunction of the corresponding difference ring formulae. □

4. 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 ACFA *effective* in a sense 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 [15], [4], [12], where it was shown that the decision procedure is recursive. We indeed manage to prove in [18] that the logic quantifier elimination is primitive recursive, and the trick there is to reduce the considerations to *directly presented* difference schemes and their *direct* Galois covers, which essentially means that we reduce everything to operations with algebraic correspondences and algebraic varieties, and we can benefit from the known methods of constructive/effective algebraic geometry.

However, the *fine quantifier elimination* of the present paper requires intrinsic tools of difference algebra and geometry, and, in spite of a recent surge of interest in algorithms for operations with difference and differential polynomial ideals, the study of algorithmic difference algebra is only in its infancy at the time of the completion of this paper. In particular, very few basic constructions with difference polynomial ideals are known to be primitive recursive. Thus, all we can do at the moment is to show that our Galois stratification procedure is primitive recursive reducible to a number of basic operations in difference algebra.

We hope that these basic operations will be shown to be primitive recursive in the future. Should this happen, our Galois stratification, as well as the decision procedure for ACFA_k would be consequently shown to be primitive recursive. However, regardless of these future developments, our algorithm is presented as an implementable algorithm modulo the operations of difference algebra, which does not involve crude indefinite searches which would be needed if one were to use the model-theoretic quantifier elimination relying on the compactness theorem.

Definition 4.1. (1) A difference field (k, σ) is *primitive recursive*, if (modulo some Gödel numbering), k is a primitive recursive set and the operations of addition, multiplication, multiplicative inverse, as well as the difference operator σ are primitive recursive functions.

(2) A ring (R, σ) is said to be *effectively presented* over a primitive recursive field (k, σ) if it has a finite σ-presentation over k, with its generators and relations explicitly given.

(3) A normal Galois stratification $\mathcal{A} = \langle X, C_i/X_i, \Gamma_i \mid i \in I \rangle$ is *effectively given* over k, if all the rings C_i, A_i (with $X_i = \mathrm{Spec}^\sigma(A_i)$) are effectively presented over k.

Example 4.2. (1) For any prime p, and a power q of p, the algebraic closure $(\bar{\mathbb{F}}_p, \varphi_q)$ of $\mathbb{F}_p$ equipped with a power of the Frobenius automorphism is a primitive recursive difference field.

(2) Any difference field of finite σ-type over $\mathbb{Q}$ is primitive recursive.

The following is a list of elementary oracle operations needed for the proof of the Direct Image Theorem 3.23 over a given primitive recursive difference field (k, σ).

- $\dagger_1(k)$ Given a difference ideal I in a difference polynomial ring over k, find its minimal associated σ-primes, i.e., find an irredundant decomposition $\{I\}_\sigma = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ (as in [19, 2.45]).
- $\dagger_2(k)$ Given an extension $(K, \sigma) \to (L, \sigma)$ of difference fields effectively presented over k, compute the relative algebraic closure of K in L.
- $\dagger_3(k)$ Given a σ-separable Galois extension $(K, \sigma) \to (L, \sigma)$ of effectively presented difference fields over k, compute its Babbitt's decomposition (as in 2.25).
- $\dagger_4(k)$ For an effectively presented integrally closed domain (R, σ) over k with fraction field (K, σ), and an extension (L, σ) of (K, σ) which is also effectively presented over k, find the effective presentation over k of the integral closure (S, σ) of R in L, and compute the σ-localisation (R', σ) of R so that the corresponding S' is of finite σ-type over R' (cf. [19, 2.56]).
- $\dagger_5(k)$ Given an effectively presented morphism $f : (R, \sigma) \to (S, \sigma)$ of effectively presented difference rings over k and a suitable property P of scheme morphisms, if f is generically σ-pro-P, compute the σ-localisations 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 2.13 and 2.15).
- $\dagger_6(k)$ Given an algebraic extension $(K, \sigma) \to (L, \sigma)$ of effectively presented difference fields over k, compute the effective presentation over k of the quasi-Galois closure of L over K.
- $\dagger_7(k)$ For a finite Galois extension $(K, \sigma) \to (L, \Sigma)$ of effectively presented difference fields over k, establish an effective correspondence between the intermediate field extensions and subgroups of the Galois group.

Definition 4.3. Let (k, σ) be a primitive recursive difference field. We define $\dagger(k)$-*primitive recursive functions* as functions primitive recursive reducible to basic operations in Difference Algebraic Geometry over (k, σ) as follows.
Basic $\dagger(k)$-primitive recursive functions are:

(1) *Constant* functions, *Successor* function S, coordinate *Projections*;

(2) Elementary operations in *difference algebraic geometry* $\dagger_1(k)$–$\dagger_7(k)$.

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

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

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

Remark 4.4. The operations $\dagger_5(k)$–$\dagger_7(k)$ are primitive recursive, since they are based on classical algebraic-geometric operations on the algebraic schemes in the 'prolongation' sequences associated with the given difference schemes.

Remark 4.5. The fine quantifier elimination from 3.26 for ACFA over a given primitive recursive difference field (k, σ) is $\dagger(k)$-primitive recursive.

Proof. Clearly, it suffices to show that the proof of the Direct Image Theorem 3.23 is $\dagger(k)$-primitive recursive, i.e., that a $\dagger(k)$-primitive recursive procedure can compute a direct image of an effectively given Galois stratification $\mathcal{A}$. Since we covered all the basic steps in difference algebra and geometry by our choice of $\dagger(k)$-oracles, it suffices to argue that the noetherian induction architecture of the proof can be rewritten in terms of bounded loops.

This, however, follows from the fact that the noetherian induction is controlled in the following sense. In each step, we compute the direct image on an open dense subset and we identify the proper closed complement, the lower-dimensional 'bad locus', for which we have to reiterate the procedure. Now, the bad locus can be explicitly computed as the locus of various singularities and ramification that can be traced through the proof, and its complexity is bounded in terms of the existing data. Thus, while the number of components (and their complexities) of the bad locus can become extremely large, the $\dagger(k)$-oracles will be able to compute the relevant bounds. □

Corollary 4.6. *The theory* ACFA_k *of existentially closed difference fields extending a primitive recursive difference field* (k, σ) *is* $\dagger(k)$*-primitive recursively decidable.*

In view of the recent developments, 4.6 is superseded by the findings of [18], where we prove that ACFA_k, over a primitive recursive inversive difference field (k, σ) with a splitting algorithm, is primitive recursive decidable.

References

[1] James Ax. The elementary theory of finite fields. *Ann. of Math. (2)*, 88:239–271, 1968.
[2] Albert E. Babbitt, Jr. Finitely generated pathological extensions of difference fields. *Trans. Amer. Math. Soc.*, 102:63–81, 1962.
[3] N. Bourbaki. *Éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations*. Actualités Scientifiques et Industrielles, No. 1308. Hermann, Paris, 1964.
[4] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.
[5] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.

[6] Jan Denef and François Loeser. Definable sets, motives and p-adic integrals. *J. Amer. Math. Soc.*, 14(2):429–469 (electronic), 2001.
[7] 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):203–233, 1976.
[8] Michael D. Fried. Variables separated equations: Strikingly different roles for the Branch Cycle Lemma and the Finite Simple Group Classification. `arXiv:1012.5297v5`.
[9] Michael D. Fried, Dan Haran, and Moshe Jarden. Effective counting of the points of definable sets over finite fields. *Israel J. Math.*, 85(1-3):103–133, 1994.
[10] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.
[11] Gabriel Giabicani. Théorie de l'intersection en géométrie aux différences. PhD Thesis, 2011.
[12] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms. `arXiv:math/0406514`, 2004. The most recent version of the paper (2012) is available at `http://www.ma.huji.ac.il/~ehud/FROB.pdf`.
[13] Catarina Kiefe. Sets definable over finite fields: their zeta-functions. *Trans. Amer. Math. Soc.*, 223:45–59, 1976.
[14] Yves Laszlo. Notes informelles sur la géométrie aux différences. `http://www.math.polytechnique.fr/~laszlo/gdt/speachhrusch.pdf`, 2005. Preprint.
[15] Angus Macintyre. Generic automorphisms of fields. *Ann. Pure Appl. Logic*, 88(2-3):165–180, 1997. Joint AILA-KGS Model Theory Meeting (Florence, 1995).
[16] Johannes Nicaise. Relative motives and the theory of pseudo-finite fields. *Int. Math. Res. Pap. IMRP*, (1):Art. ID rpm001, 70, 2007.
[17] Ivan Tomašić. Twisted Galois stratification. `arXiv:1112.0802`, 2012. Submitted.
[18] Ivan Tomašić. Direct twisted Galois stratification. `arXiv:1412.8066`, 2014. Submitted.
[19] Ivan Tomašić. A twisted theorem of Chebotarev. *Proc. Lond. Math. Soc. (3)*, 108(2):291–326, 2014.
[20] Michael Wibmer. A Chevalley theorem for difference equations. *Math. Ann.*, 354(4):1369–1396, 2012.

Ivan Tomašić, School of Mathematical Sciences, Queen Mary University of London, London, E1 4NS, United Kingdom
E-mail address: `i.tomasic@qmul.ac.uk`