C. R. Acad. Sci. Paris, Ser. I 349 (2011) 827–830

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Logic/Algebraic Geometry

Twisted Galois stratification

La stratification galoisienne tordue

Ivan Tomašić

School of Mathematics, Queen Mary University of London, Mile End Road, London E1 4NS, UK

ARTICLE INFO

Article history:
Received 28 March 2011
Accepted after revision 18 July 2011
Available online 15 August 2011

Presented by Christophe Soulé

ABSTRACT

We give an algebraic description of definable sets over fields with Frobenius in terms of twisted Galois formulae.

© 2011 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

RÉSUMÉ

On donne une description algébrique des ensembles définissables au dessus des corps avec Frobenius en termes de formules galoisiennes tordues.

© 2011 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

1. Introduction

Galois stratification, originally developed through work of Fried, Haran, Jarden and Sacerdote [2], provides an explicit arithmetic–geometric description of definable sets over finite fields in terms of Galois formulae associated to Galois coverings of algebraic varieties. Benefits were numerous, but possibly the most impressive application was in the work of Denef and Loeser on arithmetic motivic integration. They assign a Chow motive to a Galois formula, thus extending the consideration of algebraic–geometric invariants of varieties to arbitrary first-order formulae.

We develop the theory of *twisted Galois stratification* in order to describe first-order definable sets in the language of *difference rings* over fields equipped with powers of the Frobenius automorphism. To this end, we use techniques previously unknown in difference algebraic geometry, and treat several genuinely new difference phenomena which do not arise in the algebraic case. The crucial ingredients for this work include Babbitt's decomposition theorem in difference algebra and the present author's Chebotarev lemma from [4]. Our main result is that a definable set over fields with Frobenius can be described by a *twisted Galois formula* associated with *finite* Galois covers of difference varieties.

2. Difference schemes

An *affine difference scheme* is the set of fixed points $X^\sigma = \{x \in X\colon\ \sigma(x) = x\}$ in an ambient space (X, σ), where X is an affine scheme and $\sigma : X \to X$ is a morphism, together with Zariski topology and the structure sheaf inherited from X. For our purposes, a *morphism* of difference schemes is given by a morphism of ambient spaces $f : (X, \sigma) \to (Y, \tau)$, i.e., a morphism $f : X \to Y$ such that $f \circ \sigma = \tau \circ f$ (this is more restrictive than the general notion from [3]). With these assumptions, $f(X^\sigma) \subseteq Y^\tau$.

A difference scheme is of *finite σ-type* over a difference field (k, φ) if its ambient affine scheme is the spectrum of a difference algebra (R, σ) over k which is generated by σ-iterates of finitely many elements, i.e., there is a finite tuple $a \in R$

E-mail address: i.tomasic@qmul.ac.uk.

1631-073X/$ – see front matter © 2011 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.
doi:10.1016/j.crma.2011.07.018

such that, writing $R_i = k[a, \sigma a, \dots, \sigma^i a]$, $R = \varinjlim R_i$. Then each $X_i = \operatorname{Spec}(R_i)$ is a scheme of finite type, and we have the tower of 'prolongations' $\pi_{i+1,i} : X_{i+1} \to X_i$ with maps $\sigma_i : X_{i+1} \to X_i$ such that (X, σ) identifies with the projective limit of X_i and σ_i.

If P is a property of morphisms of algebraic varieties, we shall say that a difference scheme morphism $(X, \sigma) \to (Y, \tau)$ is σ–P, provided there is a morphism of some prolongation sequences of X and Y such that each $X_i \to Y_i$ has the property P.

All our difference schemes and morphisms will be affine of finite σ-type, and we will assume that our difference schemes can be dominated by *inversive* difference schemes in which σ is an automorphism.

Let $(K, \varphi)/(k, \varphi)$ be a difference field extension. The set of (K, φ)-*rational points* of a difference scheme (X, σ) over (k, φ) is the set $(X, \sigma)(K, \varphi) := \operatorname{Hom}_{(k,\varphi)}(\operatorname{Spec}(K, \varphi), (X, \sigma))$. We shall primarily be interested in rational points over *fields with powers of Frobenius* $(\bar{k}, \varphi_k)$, where $k = \mathbb{F}_q$ is a finite field, $\bar{k}$ its algebraic closure and φ_k is the power of the Frobenius automorphism of $\bar{k}$ which generates $\mathrm{G}(\bar{k}/k)$.

A morphism $(X, \sigma) \to (Y, \sigma)$ of finite σ-type is called *benign* if there exists a quasi-finite $X_0 \to Y$, such that, writing $X_{i+1} \simeq X_i \times_Y Y$ for $i \geqslant 0$ (where the morphism $Y \to Y$ is σ), (X, σ) is the (limit) fibre product of X_i and the canonical projections $\sigma_i : X_{i+1} \to X_i$ over Y. In the *benign Galois* case, X_0 is a finite Galois covering of Y with group G_0 and the Galois group $\mathrm{G}(X/Y) = (G, ()^\sigma)$ is isomorphic to the direct product of $G_i = \mathrm{G}(X_i/Y)$ and $()^\sigma$ 'shifts' from G_i to G_{i+1}. In view of such a specific form of G, for any $h, h' \in G$ there is a $g \in G$ such that $h' = g^{-1} h g^\sigma$, i.e. h and h' are $()^\sigma$-*conjugate*, and we get:

Lemma 2.1. *For any $y \in Y^\sigma$, any algebraically closed difference field (K, φ) extending $(\mathbf{k}(y), \sigma)$, any $\bar{y} \in (Y, \sigma)(K, \varphi)$ and any $g \in G$, there exists an $\bar{x} \in (X, g\sigma)(K, \varphi)$ lifting $\bar{y}$.*

Babbitt's theorem on algebraic extensions of difference fields [1] has the following easy consequence in our terminology, providing a deep structure theorem:

Theorem 2.2 *(Babbit's decomposition). Any σ-Galois (σ-étale) morphism $(X, \sigma) \to (Y, \sigma)$ of normal (inversive) affine difference schemes factorises as*

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

where $(X_0, \sigma) \to (Y, \sigma)$ is finite Galois and for $i \geqslant 0$, $(X_{i+1}, \sigma) \to (X_i, \sigma)$ is benign Galois.

3. Twisted Galois formulae

We briefly recall the notion of a twisted Galois cover from [4]. Let $\pi : (X, \sigma) \to (Y, \tau)$ be a morphism of inversive difference schemes which is σ-finite. We call it a *Galois covering* with group $(G, ()^\sigma)$ (where $()^\sigma$ is a group automorphism), if the morphism $\pi : X \to Y$ is a Galois (étale) covering with finite group $G = \mathrm{G}(X/Y)$ such that for all $g \in G$ and $x \in X$,

$$\sigma(g.x) = g^\sigma.\sigma(x).$$

It is convenient to consider the group $\tilde{G} = G \rtimes \langle\sigma\rangle = \tilde{\mathrm{G}}(X/Y)$ naturally associated with the above situation, as well as its action on X.

Let k be a finite field and let φ_k be the power of Frobenius generating $\mathrm{G}(\bar{k}/k)$. Let $y \in (Y, \tau)(\bar{k}, \varphi_k)$, meaning that $\tau y = y\varphi_k$. Pick any $x \in X(\bar{k})$ with $\pi(x) = y$. The *local Frobenius substitution at x* is the element $\varphi_{k,x} = \varphi_{k,x}^{X/Y} \in G$ such that

$$\varphi_{k,x}\sigma x = x\varphi_k.$$

We denote by $\tilde{\varphi}_{k,x}$ the element $\varphi_{k,x}\sigma \in \tilde{G}$. If $\pi(x) = \pi(x') = y$, there is a $g \in G$ with $x' = gx$ and

$$\varphi_{k,x}\sigma x = x\varphi_k = g^{-1}x'\varphi_k = g^{-1}\varphi_{k,x'}\sigma x' = g^{-1}\varphi_{k,x'}\sigma g x = g^{-1}\varphi_{k,x'} g^\sigma \sigma x.$$

Thus, $\varphi_{k,x}$ and $\varphi_{k,x'}$ are $()^\sigma$-*conjugate* in G, $\varphi_{k,x} \sim^\sigma \varphi_{k,x'}$, and we let $\varphi_{k,y}$ be the $()^\sigma$-conjugacy class of any $\varphi_{k,x}$ in G where $\pi(x) = y$. Equivalently, $\tilde{\varphi}_{k,x}$ and $\tilde{\varphi}_{k,x'}$ are conjugate in $\tilde{G}$, and we let $\tilde{\varphi}_{k,y}$ be the conjugacy class of any $\tilde{\varphi}_{k,x}$ in $\tilde{G}$ where $\pi(x) = y$.

Let (S, σ) be a difference scheme of finite σ-type over $\mathbb{Z}$ 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 integral normal σ-locally closed difference (S, σ)-subvarieties (X_i, σ) of (X, σ), each equipped with a twisted Galois covering $(Z_i, \sigma)/(X_i, \sigma)$ with group $(G_i, ()^\sigma)$, and C_i is a $()^\sigma$-conjugacy domain, i.e., a union of $()^\sigma$-conjugacy classes in G_i.

We define the *twisted Galois formula* over (S,σ) associated with the above stratification $\mathcal{A}$ through its realisations. Given a finite field k and a $(\bar{k},\varphi_k)$-valued point s in (S,σ),

$$\mathcal{A}_s(\bar{k},\varphi_k)=\bigcup_i\bigl\{x\in X_{i,s}(\bar{k},\varphi_k)\bigm|\varphi_{k,x}^{Z_i/X_i}\in C_i\bigr\}.$$

The following corollary of the *twisted theorem of Chebotarev* established in [4] by the present author provides an important stepping stone in the study of twisted Galois formulae:

Theorem 3.1. *Let $(Z,\sigma)\to(X,\sigma)$ be a twisted Galois covering over (S,σ) with group $\tilde{G}$. There exists a σ-localisation S' of S such that for every large enough finite field k, for every $s\in S'(\bar{k},\varphi_k)$, and every conjugacy class C in $\tilde{G}$ which restricts to φ_k, there exists a point $x\in X_s(\bar{k},\varphi_k)$ with $\tilde{\varphi}_{k,x}=C$.*

4. Direct images

Let (S,σ) be a difference scheme of finite σ-type over $\mathbb{Z}$ and let $\pi:(X,\sigma)\to(Y,\sigma)$ be a morphism of integral (S,σ)-difference schemes of finite σ-type.

Theorem 4.1. *For every twisted Galois stratification $\mathcal{A}$ of X, there exists a twisted Galois stratification $\mathcal{B}$ of Y such that for each sufficiently large finite field k, for each $s\in S(\bar{k},\varphi_k)$,*

$$\pi_s\bigl(\mathcal{A}_s(\bar{k},\varphi_k)\bigr)=\mathcal{B}_s(\bar{k},\varphi_k).$$

Proof. The case when π is totally unramified is easily resolved. Thus, by generic σ-smoothness, after a possible refinement of $\mathcal{A}$, we may assume that the scheme-theoretic image $Y_i:=\pi(X_i)$ is integral, normal locally closed (S,σ)-subscheme of (Y,σ) and that $\pi_i:=\pi\restriction_{X_i}:(X_i,\sigma)\to(Y_i,\sigma)$ is σ-smooth.

By considering the normalisation $\tilde{Y}_i$ in the relative algebraic closure of $\mathbf{k}(Y_i)$ inside $\mathbf{k}(X_i)$, we obtain a baby Stein factorisation $(X_i,\sigma)\to(\tilde{Y}_i,\sigma)\to(Y_i,\sigma)$, where the first map has geometrically connected fibres, and the second is σ-finite so we can split our considerations into two cases.

We disregard the index i and write $\pi:(X,\sigma)\to(Y,\sigma)$ in place of π_i. Let $(Z,\sigma)/(X,\sigma)$ be the given Galois cover with group $(G,()^{\sigma})$ and let C be the σ-conjugacy domain in G stipulated by $\mathcal{A}$.

Case 1. π has geometrically connected fibres. Let W be the normalisation of Y in the algebraic closure of $\mathbf{k}(Y)$ in $\mathbf{k}(Z)$. Then W is a Galois cover of Y with group $(H,()^{\sigma})$ and we obtain an exact sequence

$$1\to\mathrm{G}(Z/X\times_Y W)\to\mathrm{G}(Z/X)\to\mathrm{G}(W/Y)\to 1. \tag{1}$$

Let D be the image of C in H and we claim that for large enough k, and $s\in S(\bar{k},\varphi_k)$,

$$\bigl\{y\in Y_s(\bar{k},\varphi_k)\bigm|\exists x\in X_s(\bar{k},\varphi_k),\ \varphi_{k,x}\in C,\ \pi_s(x)=y\bigr\}=\bigl\{y\in Y_s(\bar{k},\varphi_k)\bigm|\varphi_{k,y}\in D\bigr\}. \tag{2}$$

A routine verification of the left to right inclusion needs no assumptions on the size of k.

Conversely, let $y\in Y_s(\bar{k},\varphi_k)$, $\varphi_{k,y}\sim^{\sigma}d\in D$. Pick some y' in the fibre of W/Y above y with $\varphi_{k,y'}\sim^{\sigma}d$ and consider $X_{y'}=X\times_Y y'$ and $Z_{y'}=Z\times_{X\times_Y W}X_{y'}=Z\times_W y'$. By construction, $Z\to W$ has geometrically connected fibres so we conclude that $Z_{y'}$ is geometrically connected and $\mathrm{G}(Z_{y'}/X_{y'})\cong\mathrm{G}(Z/X\times_Y W)$. We obtain the following diagram with exact rows, where the left vertical arrow is an isomorphism.

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{G}(Z/X\times_Y W) \arrow[r] & \tilde{\mathrm{G}}(Z/X) \arrow[r] & \tilde{\mathrm{G}}(W/Y) \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{G}(Z_{y'}/X_{y'}) \arrow[r] \arrow[u] & \tilde{\mathrm{G}}(Z_{y'}/X_y) \arrow[r] \arrow[u] & \tilde{\mathrm{G}}(y'/y) \arrow[r] \arrow[u] & 1
\end{tikzcd}$$

Since d maps to φ_k in $\tilde{\mathrm{G}}(y'/y)$, the diagram shows that there exists a $c'\in\tilde{\mathrm{G}}(Z_{y'}/X_y)$ that maps into $\tilde{C}$ and then to d on one side, and onto φ_k on the other. It suffices to find an $x\in X_y(\bar{k},\varphi_k)$ with $\tilde{\varphi}_{k,x}\sim^{\sigma}c'$ with respect to the cover $Z_{y'}/X_y$, and this is possible for large enough k by Twisted Chebotarev 3.1.

Case 2. π is σ-étale. Some care is required to pass to the Galois closure of X over Y in order to benefit from Babbitt's decomposition, but eventually we reduce to two subcases as follows.

Case 2(a). π is finite Galois. It is straightforward to check (2) if we take $W=Z$, and we let D be the image of C under the inclusion in the exact sequence

$$1 \to \mathrm{G}(Z/X) \to \mathrm{G}(Z/Y) \to \mathrm{G}(X/Y) \to 1.$$

Case 2(b). π is benign Galois. Babbitt's decomposition applied to Z/Y yields a sequence

$$Z = Z_n \to \cdots \to Z_1 \to Z_0 = W \to Y$$

where W/Y is finite Galois with group H 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 (1) again. Let D be the image of C in H, and we claim that (2) holds for any k and $s \in S(\bar{k}, \varphi_k)$. To see the non-trivial inclusion, let y be an element of the right-hand side and let $z_0 \in W = Z_0$ such that $z_0 \mapsto y$ and $\varphi_{k,z_0} \in D$. Using the property 2.1 repeatedly, we can lift z_0 through the 'stack' of benign extensions Z_{i+1}/Z_i to a point $z \in (Z_s, c\sigma)$ with $c \in C$, and then the image x of z in X_s has the properties $\varphi_{k,x} \in C$ and $\pi(x) = y$. □

The above theorem shows that the class of twisted Galois formulae is closed under direct images, which is equivalent to saying that it admits elimination of (a block of) existential quantifiers. It is folklore to deduce that all quantifiers can be eliminated and we obtain the following algebraic characterisation of definable sets over fields with powers of Frobenius.

Corollary 4.2. *Let $\psi_z(x) = \psi(x; z)$ be a first order formula in the language of difference rings in variables $x = x_1, \ldots, x_n$ with parameters z from (S, σ). There exists a σ-localisation S' of S and a twisted Galois stratification $\mathcal{A}$ of the difference affine n-space over S' such that for large enough k, for every $s \in S'(\bar{k}, \varphi_k)$,*

$$\psi_s(\bar{k}, \varphi_k) = \mathcal{A}_s(\bar{k}, \varphi_k).$$

There is an analogous result over models of ACFA.

References

[1] A.E. Babbitt, Finitely generated pathological extensions of difference fields, Trans. AMS 102 (1962).

[2] M.D. Fried, M. Jarden, Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 11, Springer-Verlag, Berlin, 1986.

[3] E. Hrushovski, The elementary theory of the Frobenius automorphisms, preprint, 2004.

[4] I. Tomašić, A twisted theorem of Chebotarev, C. R. Acad. Sci. Paris, Ser. I 347 (2009) 385–388.