Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 347 (2009) 385–388
COMPTES RENDUS MATHEMATIQUE

Algebraic Geometry

A twisted theorem of Chebotarev

Ivan Tomašić

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

Received 8 April 2008; accepted after revision 4 February 2009

Available online 5 March 2009

Presented by Jean-Pierre Serre

Abstract

The classical function field version of Chebotarev's Theorem follows from the Lang–Weil estimate and an 'untwisting' trick. We obtain an analogue in the framework of difference schemes, using Hrushovski's twisted Lang–Weil estimate. ***To cite this article: I. Tomašić, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Résumé

Un théorème de Chebotarev tordu. La version classique du Théorème de Chebotarev pour les corps de fonctions se déduit de l'estimation de Lang–Weil et un astuce de « détordage ». On obtient un analogue dans le cadre des schémas aux différences, en utilisant l'estimation de Lang–Weil tordue de Hrushovski. ***Pour citer cet article : I. Tomašić, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

1. Introduction

Intuitively speaking, a *difference scheme* is a scheme with a distinguished endomorphism. Classical algebraic geometry is well suited for studying schemes and morphisms of finite type. Difference schemes usually being of infinite type as algebraic schemes, but of *finite transformal type*, thus fall just beyond the reach of classical tools and methodology.

Our goal is to develop *difference algebraic geometry* up to the level where it reveals the fine number-theoretic information regarding numbers of points of difference schemes over fields with powers of Frobenius. The present note establishes a difference analogue of Chebotarev's Theorem for function fields, using the twisted Lang–Weil estimate of Hrushovski from [1]. We chose to present the main result in a form of a trace formula, in order to give the reader a taste of the forthcoming developments.

Among others, our result should be of interest to model-theorists, because it allows counting points on definable sets uniformly over fields with powers of Frobenius as expounded in Remark 2.

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

1631-073X/$ – see front matter
doi:10.1016/j.crma.2009.02.015

2. Difference schemes

A *difference scheme* is a pair (X, σ), where X is an affine scheme and $\sigma : X \to X$ is a morphism. We consider the fixed set of σ (Hrushovski glues these into more general difference schemes),

$$X^\sigma = \{x \in X\colon \sigma(x) = x\}.$$

This X^σ inherits Zariski topology from X, and we let the structure sheaf on X^σ be the restriction $\mathcal{O}_{X^\sigma} = \mathcal{O}_X \restriction X^\sigma$. The restriction of $\sigma^\# : \mathcal{O}_X \to \sigma_*\mathcal{O}_X$ to $\mathcal{O}_{X^\sigma}$ gives an endomorphism $\sigma^\# : \mathcal{O}_{X^\sigma} \to \mathcal{O}_{X^\sigma}$. A *morphism* of difference schemes $f : (X, \sigma) \to (Y, \tau)$ is a morphism $f : X \to Y$ such that $f \circ \sigma = \tau \circ f$. Clearly, $f(X^\sigma) \subseteq Y^\tau$.

A difference scheme is of *finite σ-type,* if its ambient affine scheme is the spectrum of a difference algebra (R, σ) over a difference field which is generated by σ-iterates of finitely many elements. It is *well-mixed*, if $fg = 0$ in R implies $f\sigma g = 0$. All our difference schemes will be well-mixed of finite σ-type, and all morphisms will respect the relevant structure morphisms to the ground difference field.

Let (K, φ) be a difference field. The set of (K, φ)-rational points of a difference variety (X, σ) is the set

$$(X, \sigma)(K, \varphi) := \mathrm{Hom}\big(\mathrm{Spec}(K, \varphi), (X, \sigma)\big).$$

Let $k = \mathbb{F}_q$ be a finite field, $\bar{k}$ its algebraic closure and let φ_k be the power of the Frobenius automorphism of $\bar{k}$ which generates $\mathrm{Gal}(\bar{k}/k)$. Given a suitable (in the technical sense of Section 4) difference scheme (X, σ), we are interested in the number of $(\bar{k}, \varphi_k)$-rational points of (X, σ),

$$N_q = \big|(X, \sigma)(\bar{k}, \varphi_k)\big|.$$

Theorem 2.1 *(Hrushovski).* (i) *N_q is finite for all q if and only if the* σ-dimension *of X^σ is* 0 *if and only if the* total dimension *of X^σ is finite* (*cf.* [1] *for definitions of these dimensions*).

(ii) *There exist $C > 0$ and $\mu \in \mathbb{Q}$ (mostly $\mathbb{Z}$) such that, writing d for the total dimension of X,*

$$\big|N_q - \mu q^d\big| < C q^{d-1/2}.$$

Corollary 2.2 *(Macintyre, independently of 2.1). For large q, $N_q \neq 0$.*

Example 1. (i) The coordinate ring of the 'long transformal line' is $k[x_i\colon i \in \mathbb{N}_0]$, where $\sigma : x_i \mapsto x_{i+1}$. It is of finite σ-type (σ-generated by x_0), its σ-dimension is 1 and its total dimension is infinite.

(ii) The difference variety associated with the ring $\mathbb{Z}[x_i, y_i\colon i \in \mathbb{N}_0]/\langle x_{i+1}^2 + x_i + y_i^3, x_i^3 + y_{i+2} + 1\colon i \in \mathbb{N}_0\rangle$ in which $\sigma : x_i \mapsto x_{i+1}$, $y_i \mapsto y_{i+1}$ is of finite σ-type of σ-dimension 0 and of total dimension 3. Reducing mod p and substituting the Frobenius $\varphi_{\mathbb{F}_q}$ for σ we see that $N_q \approx 2q^3$ so in this case $\mu = 2$.

3. Twisted Galois coverings

Let $\pi : (X, \sigma) \to (Y, \tau)$ be a morphism of inversive difference schemes (where σ and τ are invertible) which is locally of finite type. We call it a *Galois covering* with group $(G, ()^\sigma)$ (where $()^\sigma$ is a group automorphism), if the map $\pi : X \to Y$ is a Galois (étale) covering with finite group G such that for all $g \in G$ and $x \in X$,

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

It is convenient to consider the group $\tilde{G} = G \rtimes \langle\sigma\rangle$ 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 $\mathrm{Gal}(\bar{k}/k)$. 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 $\varphi_{k,x} \in G$ 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

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

Thus, $\varphi_{k,x}$ and $\varphi_{k,x'}$ are $()^\sigma$-*conjugate* in G 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 $\pi(x) = y$.

Clearly, a $()^\sigma$-central function $\alpha : G \to \mathbb{C}$ (constant on $()^\sigma$-conjugacy classes), can be obtained from a central function $\tilde{\alpha} : \tilde{G} \to \mathbb{C}$ by the rule $\alpha(g) = \tilde{\alpha}(g\sigma)$, and such an $\tilde{\alpha}$ will be a linear combination of characters of finite-dimensional representations of $\tilde{G}$. For such functions, the expressions $\alpha(\varphi_{k,y})$ and $\tilde{\alpha}(\tilde{\varphi}_{k,y})$ are well-defined and equal.

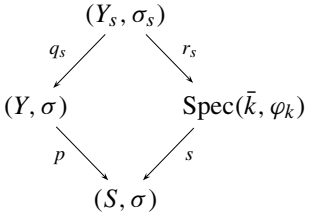
When a map $\tilde{p} : \tilde{G} = G \rtimes \langle\sigma\rangle \to \tilde{H} = H \rtimes \langle\tau\rangle$ is *level-preserving* in the sense that $\tilde{p}(\sigma) \in H\tau$, given finite-dimensional representations ρ of $\tilde{G}$ and θ of $\tilde{H}$, the generalised induced and restricted representations $\tilde{p}_*\rho$ and $\tilde{p}^*\theta = \theta \circ \tilde{p}$ are again finite-dimensional, and we have the expected Frobenius reciprocity law.

In the particular case where $\tilde{p}$ is onto with $K = \ker(\tilde{p} \restriction G)$, if $\tilde{\alpha} : \tilde{G} \to \mathbb{C}$ is central,

$$\tilde{p}_*\tilde{\alpha}\big(\tilde{p}(g)\big) = \frac{1}{|K|}\sum_{k\in K}\tilde{\alpha}(kg). \tag{1}$$

4. Main theorem

Let (S,σ) be a difference scheme of finite σ-type over $\mathbb{Z}$ and let $(X,\sigma) \to (Y,\sigma)$ be a Galois covering of (S,σ)-difference schemes of finite σ-type and finite total dimension with group $(G,()^\sigma)$ and the associated group $\tilde{G} = G \rtimes \langle\sigma\rangle$. Given a finite field k and a $(\bar{k},\varphi_k)$-valued point s in (S,σ), let $(Y_s,\sigma_s) = (Y,\sigma) \times_{(S,\sigma)} \mathrm{Spec}(\bar{k},\varphi_k)$ be the fibre over s, as depicted in the following diagram:



Given a σ-central function $\alpha : G \to \mathbb{C}$, we are interested in the behaviour of sums

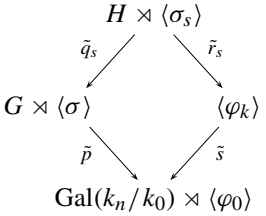
$$\sum_{y\in(Y_s,\sigma_s)(\bar{k},\varphi_k)} \alpha(\varphi_{k,q_s(y)}) = \sum_{y\in(Y_s,\sigma_s)(\bar{k},\varphi_k)} q_s^*\alpha(\varphi_{k,y}),$$

as k and s vary, where $q_s^*\alpha$ is the inverse image of α, to be defined below in a special case. In an effort to keep the present paper short and self-contained, we shall only state and prove our main theorem in the case where $(S,\sigma) = \mathrm{Spec}(k_0,\varphi_0)$ with k_0 a finite field and φ_0 a power of the Frobenius on k_0. A paper with the general case (also covering more general difference schemes in the sense of Hrushovski) will follow shortly.

Let us assume for simplicity that X is geometrically integral over k_n, the relative algebraic closure of k_0 in $\mathbf{k}(X)$. Then the Galois cover $X \to Y$ factors as $X \to Y \times_{k_0} k_n \to Y$, where the first group is some $H \leqslant G$ and the second $\mathrm{Gal}(k_n/k_0) \simeq \mathbb{Z}/n\mathbb{Z}$. We have the following short exact sequence of groups (where $\tilde{p}$ is level-preserving):

$$1 \longrightarrow H \longrightarrow G \rtimes \langle\sigma\rangle \xrightarrow{\tilde{p}} \mathrm{Gal}(k_n/k_0) \rtimes \langle\varphi_0\rangle \longrightarrow 1.$$

Here is the diagram of relevant Galois groups (maps are level-preserving and defined up to conjugacy):



Theorem 4.1. *With the above notation, there is a constant $C > 0$ and a localisation (S', σ) of (S, σ) such that for every σ-central function $\alpha : G \to \mathbb{C}$ (and the associated central function $\tilde{\alpha} : \tilde{G} \to \mathbb{C}$), for every finite field k, and every point $s \in (S', \sigma)(\bar{k}, \varphi_k)$,*

$$\left| \sum_{y \in (Y_s, \sigma_s)(\bar{k}, \varphi_k)} \tilde{q}_s^* \tilde{\alpha}(\tilde{\varphi}_{k,y}) - \tilde{p}_* \tilde{\alpha}(\tilde{\varphi}_{k,s}) \big| (Y_s, \sigma_s)(\bar{k}, \varphi_k) \big| \right| < C|k|^{d-1/2}.$$

We sketch the main steps in the proof. By a direct calculation of the difference scheme invariants that figure in the μ-term from Hrushovski's estimate 2.1, we see that for each $h \in H$, up to $\mathrm{O}(|k|^{d-1/2})$,

$$\big|(X_s, h\sigma_s)(\bar{k}, \varphi_k)\big| \approx \big|(Y_s, \sigma_s)(\bar{k}, \varphi_k)\big|. \tag{2}$$

Moreover, for the above diagram of Galois groups one easily verifies a 'baby base change theorem':

$$\tilde{r}_{s*} \tilde{q}_s^* \tilde{\alpha}(\varphi_k) = \tilde{s}^* \tilde{p}_* \tilde{\alpha}(\varphi_k). \tag{3}$$

Finally,

$$\begin{aligned}
\sum_{y \in (Y_s, \sigma_s)(\bar{k}, \varphi_k)} \tilde{\alpha}(\tilde{\varphi}_{k, q_s(y)}) &= \sum_{y \in (Y_s, \sigma_s)(\bar{k}, \varphi_k)} \tilde{q}_s^* \tilde{\alpha}(\tilde{\varphi}_{k,y}) = \frac{1}{|H|} \sum_{\substack{x \in X_s(\bar{k}) \\ \pi(x) \in (Y_s, \sigma_s)}} \tilde{q}_s^* \tilde{\alpha}(\tilde{\varphi}_{k,x}) \\
&= \frac{1}{|H|} \sum_{h \in H} \tilde{q}_s^* \tilde{\alpha}(h\sigma_s) \big|(X_s, h\sigma_s)(\bar{k}, \varphi_k)\big| \overset{(2)}{\approx} \frac{1}{|H|} \sum_{h \in H} \tilde{q}_s^* \tilde{\alpha}(h\sigma_s) \big|(Y_s, \sigma_s)(\bar{k}, \varphi_k)\big| \\
&\overset{(1)}{=} \tilde{r}_{s*} \tilde{q}_s^* \tilde{\alpha}(\tilde{\varphi}_k) \big|(Y_s, \sigma_s)(\bar{k}, \varphi_k)\big| \overset{(3)}{=} \tilde{s}^* \tilde{p}_* \tilde{\alpha}(\varphi_k) \big|(Y_s, \sigma_s)(\bar{k}, \varphi_k)\big| \\
&= \tilde{p}_* \tilde{\alpha}(\tilde{\varphi}_{k,s}) \big|(Y_s, \sigma_s)(\bar{k}, \varphi_k)\big|.
\end{aligned}$$

Corollary 4.2. *In the* geometric *case where X is already geometrically integral over k_0, if C is a $()^\sigma$-conjugacy class in G,*

$$\big|\big\{y \in (Y_s, \sigma_s)(\bar{k}, \varphi_k) \colon \varphi_{k,y} = C\big\}\big| \approx |C|/|G| \big|(Y_s, \sigma_s)(\bar{k}, \varphi_k)\big|.$$

Remark 1. In the special case $\sigma = 1$, the above specialises to the classical theorem of Chebotarev for function fields. Its proof exactly fits the above template, with step (2) replaced by the following well-known untwisting trick. The number of $(\bar{k}, \varphi_k)$-points on a difference scheme (X_s, h) with h of finite order is shown equal to that of an algebraic variety and then estimated using the classical Lang–Weil estimate.

Remark 2. It can be shown that definable sets over fields with powers of Frobenius (or ACFA) can be stratified into sets of form $\{y \in Y^\sigma \colon \varphi_y = C\}$, where $(X, \sigma)/(Y, \sigma)$ is a twisted Galois covering with group $(G,)^\sigma)$, and C is a $()^\sigma$-conjugacy class in G. Thus we can use 4.1 to count the number of points on such definable sets.

References

[1] E. Hrushovski, The elementary theory of the Frobenius automorphism, preprint, 2004.