Twisted covers and specializations

Pierre Dèbes and François Legrand

Abstract.

The central topic is this question: is a given k-étale algebra $\prod_l E_l/k$ the specialization of a given k-cover $f : X \to B$ at some unramified point $t_0 \in B(k)$? Our main tool is a *twisting lemma* that reduces the problem to finding k-rational points on a certain k-variety. Previous forms of this twisting lemma are generalized and unified. New applications are given: a Grunwald form of Hilbert's irreducibility theorem over number fields, a non-Galois variant of the Tchebotarev theorem for function fields over finite fields, some general specialization properties of covers over PAC or ample fields.

§1. Presentation

1.1. The central question

If $f : X \to B$ is an algebraic cover defined over a field k and t_0 a k-rational point on B, not in the branch locus of f, the specialization of f at t_0 is defined as a finite k-étale algebra of degree $n = \deg(f)$. For example, if $B = \mathbb{P}^1$ and f is given by some polynomial $P(T, Y) \in k[T, Y]$, it is the product of separable field extensions of k that correspond to the irreducible factors of $P(t_0, Y)$ (for all but finitely many $t_0 \in k$). Our central question is whether a given degree n k-étale algebra $\prod_l E_l/k$ is the specialization of a given degree n k-cover $f : X \to B$ at some unramified point $t_0 \in B(k)$. The classical Hilbert specialization property corresponds to the special case for which étale algebras are taken to be single degree n field extensions and the answer is positive for at least one of them.

Received Month Day, Year.

Revised Month Day, Year.

2000 *Mathematics Subject Classification.* Primary 11R58, 12E30, 12E25, 14G05, 14H30; Secondary 12Fxx, 14Gxx, 14H10.

Key words and phrases. Specialization, algebraic covers, twisting lemma, Hilbert's irreducibility theorem, PAC fields, finite fields, local fields, global fields.

The question has already been investigated in [DG11a] and [DG11b] for regular Galois covers and in [DL11] for covers with geometric monodromy group S_n (definitions recalled in §2.2). The aim of this paper is to handle the situation of arbitrary covers, to provide a unifying approach and to give further applications.

1.2. The twisting lemma

Our main tool is a *twisting lemma* that gives a general answer to the question: under certain hypotheses, *the answer is* Yes *if there exist unramified k-rational points on the covering space $\widetilde{X}$ of certain twisted covers $\widetilde{f} : \widetilde{X} \to B$*. This lemma has several variants. The first one, for regular Galois covers, was established in [Dèb99a] for covers of $\mathbb{P}^1$ and in [DG11a] for a general base space. It is used in [DL11] to obtain the second one, for covers with geometric monodromy group S_n. We will prove the two variants shown on the top row of the following diagram, which indicates that they generalize the two previous ones, shown on the bottom row.

$$\begin{array}{ccc} \text{Galois} & \Leftrightarrow & \text{general} \\ \Downarrow & & \Downarrow \\ \text{regular Galois} & \Rightarrow & \text{monodromy } S_n \end{array}$$

The *Galois* variant is for the situation $f : X \to B$ is a Galois cover, regular or not; it is proved in §3.1. The *general* variant is proved in §3.2 and concerns arbitrary covers, Galois or not, regular or not. Implication $\Rightarrow$ in the upper row means that the general variant will be obtained from the Galois variant. We will also be interested in the converse of the twisting lemma: the answer to the original question is Yes *if and only if* there exist unramified k-rational points on the twisted covers.

The twisting lemma is a geometric *avatar* of an argument of Tchebotarev known as the *Field Crossing Argument* and which notably appears in the proof of the Tchebotarev density theorems over global fields and in the theory of PAC fields (see [FJ04]). The twisting lemma formalizes the core of the argument and produces a geometric tool: the variety $\widetilde{X}$. This allows a unifying approach over an arbitrary base field: questions are reduced to finding rational points on $\widetilde{X}$. Letting the base field vary then yields previous results in various contexts and leads to new applications. The twisted cover $\widetilde{f} : \widetilde{X} \to B$, which appeared first in [Dèb99a] and [Dèb99b], could also be defined by using the language of torsors. Another related approach using an embedding problem presentation has also been recently proposed by Bary-Soroker [BS10].

1.3. Applications

As in previous papers, they are obtained over fields with good arithmetic properties: PAC fields, finite fields, number fields, ample fields. We present them below in connection with those from previous works.

1.3.1. *Over a PAC field k* (definition recalled in §4.1), the regular Galois variant was used in [Dèb99a] to prove that, given a group G and a subgroup $H \subset G$, any Galois extension E/k of group H is a specialization of any regular Galois k-cover $f : X \to \mathbb{P}^1$ of group G (thereby proving the so-called Beckmann-Black conjecture for PAC fields). A not necessarily Galois analog with an arbitrary degree n k-étale algebra $\prod_l E_l/k$ replacing E/k is proved in [DL11] under the assumption that f is a degree n k-cover of geometric monodromy group S_n. Corollary 4.1 is a refinement of the first result (the regularity assumption is relaxed) while corollary 4.2 is a variant of the second one (allowing more general monodromy groups). Similar applications have been obtained by Bary-Soroker [BS10].

The general spirit of these results is that over a PAC field there is no diophantine obstruction[1] to a given étale algebra being a specialization of some given cover; obstructions only come from Galois theory. This has some impact on the arithmetic of PAC fields. For example a by-product of [DL11] is that if k is a PAC field of characteristic 0 (for simplicity), every degree n extension E/k can be realized by some trinomial $Y^n - Y + b$ with $b \in k$.

1.3.2. *Over a finite field $k = \mathbb{F}_q$*, the twisting lemma can be combined with Lang-Weil to obtain an estimate for the number of points $t_0 \in \mathbb{F}_q$ at which a given degree n étale algebra $\prod_l E_l/\mathbb{F}_q$ is a specialization of a given degree n $\mathbb{F}_q$-cover $f : X \to \mathbb{P}^1$ of geometric monodromy group S_n (corollary 4.3). This type of result is known in the literature as *a Tchebotarev theorem for function fields over finite fields*. For example, if $\prod_l E_l/\mathbb{F}_q$ is the single degree n field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, the estimate is of the form $q/n + O(\sqrt{q})$. In the specific case where f is given by the trinomial $Y^n + Y - T$, it yields results of Cohen and Ree proving a conjecture of Chowla. See §4.2 for details and references.

For finite fields $\mathbb{F}_q$, the same general spirit as for PAC fields can be retained — no diophantine obstruction to the problem —, but provided that q be suitably large.

1.3.3. *The local-global situation* of a number field k given with some completions k_v was central in [DG11a]. The main result was a Hilbert-Grunwald theorem showing that every regular Galois k-cover $f : X \to \mathbb{P}^1$

[1] in the sense that existence of rational points on some variety, which is a condition of our twisting lemma in general, is automatic over a PAC field k.

of group G has specializations at points $t_0 \in k$ that are *Galois field extensions of group G* (Hilbert) with the extra property (Grunwald) that *they induce prescribed unramified extensions E^v/k_v of Galois group $H_v \subset G$* at each finite place v in a given finite set S, the only condition on the places being that the residue fields be suitably big and of order prime to $|G|$. An analog is given in [DL11] for not necessarily Galois covers: the Hilbert condition becomes that the specialization at t_0 is *a degree n field extension* and the Grunwald condition that *the local degrees* are imposed at each $v \in S$; this is proved under the assumption that f is a degree n k-cover of geometric monodromy group S_n.

§4.3 has a similar local-global flavor. The outcome is a generalization to general regular covers $f : X \to \mathbb{P}^1$ of the non-Galois analog above (corollary 4.5). On the way the following typical result of Fried is reproved (and generalized): if the Galois group $\overline{G} \subset S_n$ over $\overline{\mathbb{Q}}(T)$ of a degree n polynomial $P(T, Y) \in \mathbb{Q}(T)[Y]$ contains a n-cycle, then the associated Hilbert subset contains infinitely many arithmetic progressions with ratio a prime number. See §4.3 for details and references.

Here it is the relative flexibility of the local extensions obtained from global specializations that is the striking phenomenon. In the Galois situation, the very existence of global extensions with such local properties may sometimes even be questioned. Recall for example that results from [DG11a] lead to some obstruction to the Regular Inverse Galois Problem (yet unproved to be not vacuous) related to some analytic questions around the Tchebotarev density theorem.

Other local-global situations can be considered, for example that of a base field that is a function field $\kappa(x)$ with κ either a suitably large finite field or a PAC field with enough cyclic extensions. We refer to [DG11b] where these situations have been considered.

1.3.4. *Over ample fields* (definition recalled in §4.4), the twisting lemma leads to this general property of ample fields (corollary 4.6): if a k-cover $f : X \to B$ of curves specializes to some k-étale algebra $\prod_l E_l/k$ at some unramified point $t_0 \in B(k)$, then it specializes to the same k-étale algebra $\prod_l E_l/k$ at infinitely many unramified points $t \in B(k)$.

§2. Basics

In this section we set up the terminology and notation for the basic notions we will use. The reader who is familiar with étale algebras, covers and their specializations, Galois groups, fundamental groups and their representations can skip this section to get to the core of the paper and come back to it when needed.

Given a field k, we fix an algebraic closure $\overline{k}$ and denote the separable closure of k in $\overline{k}$ by k^{sep} and its absolute Galois group by G_k. If k' is an overfield of k, we use the notation $\otimes_k k'$ for the scalar extension from k to k': for example, if X is a k-curve, $X \otimes_k k'$ is the k'-curve obtained by scalar extension. For more on this section, we refer to [DD97, §2] or [Dèb09, chapitre 3].

2.1. Etale algebras and their Galois representations

Given a field k, a *k-étale algebra* is a product $\prod_{l=1}^{s} E_l/k$ of finite sub-field extensions $E_1/k, \ldots, E_s/k$ of k^{sep}/k. Set $m_l = [E_l : k]$, $l = 1, \ldots, s$ and $m = \sum_{l=1}^{s} m_l$. If N/k is a Galois extension containing the Galois closures of $E_1/k, \ldots, E_s/k$, the Galois group $\mathrm{Gal}(N/k)$ acts by left multiplication on the left cosets of $\mathrm{Gal}(N/k)$ modulo $\mathrm{Gal}(N/E_l)$ for each $l = 1, \ldots, s$. The resulting action $\mathrm{Gal}(N/k) \to S_m$ on the set of these m left cosets, which is well-defined up to equivalence (*i.e.* up to conjugation by an element of S_m), is called the *Galois representation of* $\prod_{l=1}^{s} E_l/k$ *relative to* N. Equivalently it can be defined as the action of $\mathrm{Gal}(N/k)$ on the set of all k-embeddings $E_l \hookrightarrow N$, $l = 1, \ldots, s$.

Conversely, an action $\mu : \mathrm{Gal}(N/k) \to S_m$ determines a k-étale algebra in the following way. For $i = 1, \ldots, m$, denote the fixed field in N of the subgroup of $\mathrm{Gal}(N/k)$ consisting of all τ such that $\mu(\tau)(i) = i$ by E_i. The product $\prod_l E_l/k$ for l ranging over a set of representatives of the orbits of the action μ is a k-étale algebra with $\sum_l [E_l : k] = m$. If two k-étale algebras $\prod_{l=1}^{s} E_l/k$ and $\prod_{l=1}^{s'} E'_l/k$ are obtained in this manner from two different choices of the set of representatives of the orbits of μ, then they are equivalent in the sense that $s = s'$ and there exist $\sigma_1, \ldots, \sigma_s \in \mathrm{Gal}(N/k)$ such that $\sigma_l(E_l) = E'_l$, $l = 1, \ldots, s$. Equivalently an equivalence class of k-étale algebras can be viewed as a product of k-isomorphism classes of finite sub-field extensions of k^{sep}/k.

G-*Galois variant*: if $\prod_{l=1}^{s} E_l/k$ is a *single Galois extension* E/k, the restriction $\mathrm{Gal}(N/k) \to \mathrm{Gal}(E/k)$ is called *the* G-*Galois representation of* E/k (relative to N). Any map $\varphi : \mathrm{Gal}(N/k) \to G$ obtained by composing $\mathrm{Gal}(N/k) \to \mathrm{Gal}(E/k)$ with a monomorphism $\mathrm{Gal}(E/k) \to G$ is called a G-Galois representation of E/k (relative to N). The extension E/k can be recovered from $\varphi : \mathrm{Gal}(N/k) \to G$ by taking the fixed field in N of $\ker(\varphi)$. One obtains the Galois representation $\mathrm{Gal}(N/k) \to S_n$ of E/k (relative to N) from a G-Galois representation $\varphi : \mathrm{Gal}(N/k) \to G$ (relative to N) by composing it with the left-regular representation of the image group $\varphi(\mathrm{Gal}(N/k))$; here $n = |\varphi(\mathrm{Gal}(N/k))|$.

2.2. Covers and function field extensions

Given a regular projective geometrically irreducible k-variety B, a *k-cover of B* is a finite and generically unramified morphism $f : X \to B$ defined over k with X a normal and irreducible variety. Through the function field functor k-covers $f : X \to B$ correspond to finite separable field extensions $k(X)/k(B)$. The k-cover $f : X \to B$ is said to be *Galois* if the field extension $k(X)/k(B)$ is; if in addition $f : X \to B$ is given together with an isomorphism $G \to \mathrm{Gal}(k(X)/k(B))$, it is called a k-G-Galois cover of group G.

A k-cover $f : X \to B$ is said to be *regular* if $k(X)$ is a regular extension of k, *i.e.* if $k(X) \cap \overline{k} = k$, or equivalently, if X is geometrically irreducible. In general, there is some *constant extension* in $f : X \to B$, which we denote by $\widehat{k}_f/k$ and is defined by $\widehat{k}_f = k(X) \cap k^{\mathrm{sep}}$ (the special case $\widehat{k}_f = k$ corresponds to the situation $f : X \to B$ is regular).

If $f : X \to B$ is a k-cover, its Galois closure over k is a Galois k-cover $g : Z \to B$, which *via* the cover-field extension dictionary, corresponds to the Galois closure of $k(X)/k(B)$. The Galois group $\mathrm{Gal}(k(Z)/k(B))$ is called the *monodromy group* of f. Denote next by $k^{\mathrm{sep}}(Z)$ the *compositum* of $k(Z)$ and k^{sep} (in a fixed separable closure of $k(B)$)[2]. The Galois group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ is called the *geometric monodromy group* of f; it is a normal subgroup of the monodromy group $\mathrm{Gal}(k(Z)/k(B))$. The *branch divisor* of the k-cover f is the formal sum of all hypersurfaces of $B \otimes_k k^{\mathrm{sep}}$ such that the associated discrete valuations are ramified in the field extension $k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B)$.

If $f : X \to B$ is regular, $f \otimes_k k^{\mathrm{sep}}$ is a k^{sep}-cover, the Galois closure of its function field extension is $k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B)$ and its branch divisor is the same as the branch divisor of f, and it is the formal sum of all hypersurfaces of $B \otimes_k k^{\mathrm{sep}}$ such that the associated discrete valuations are ramified in the field extension $k^{\mathrm{sep}}(X)/k^{\mathrm{sep}}(B)$. From Purity of the Branch Locus, f is étale above $B \setminus D$.

2.3. π_1-representations

Given a reduced effective divisor $D \subset B$, denote the *k-fundamental group* of $B \setminus D$ by $\pi_1(B \setminus D, t)_k$ where $t \in B(\overline{k}) \setminus D$ is a base point (which corresponds to the choice of an algebraic closure of $k(B)$). Conjoining the two dictionaries covers-function field extensions and field extensions-Galois representations, we obtain the following correspondences: k-covers of B of degree n (resp. k-G-Galois covers of B of

[2]Note that as $g : Z \to B$ is Galois, $k(Z)$ only depends on the $k(B)$-isomorphism class of $k(X)/k(B)$ (but not on $k(X)/k(B)$ itself).

group G) with branch divisor contained in D correspond to transitive morphisms[3] $\phi : \pi_1(B \setminus D, t)_k \to S_n$ (resp. to epimorphisms $\phi : \pi_1(B \setminus D, t)_k \to G$). The regularity property corresponds to the extra condition that the restriction of ϕ to $\pi_1(B \setminus D, t)_{k^{\rm sep}}$ remains transitive (resp. remains onto). These morphisms are called *fundamental group representations* (π_1-representations for short) of the corresponding k-covers and k-G-Galois covers.

2.4. Specializations

Each k-rational point $t_0 \in B(k) \setminus D$ provides a section $\mathsf{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ to the exact sequence

$$1 \to \pi_1(B \setminus D, t)_{k^{\rm sep}} \to \pi_1(B \setminus D, t)_k \to \mathrm{G}_k \to 1$$

which is uniquely defined up to conjugation by an element in the fundamental group $\pi_1(B \setminus D, t)_{k^{\rm sep}}$.

If $\phi : \pi_1(B \setminus D, t)_k \to G$ represents a k-G-Galois cover $f : X \to B$, the morphism $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to G$ is a G-Galois representation. The fixed field in $k^{\rm sep}$ of $\ker(\phi \circ \mathsf{s}_{t_0})$ is the residue field at some point above t_0 in the extension $k(X)/k(B)$ (in fact at any point above t_0 since the extension $k(X)/k(B)$ is Galois). We denote it by $k(X)_{t_0}$ and call $k(X)_{t_0}/k$ *the specialization* of the k-G-cover f at t_0.

If $\phi : \pi_1(B \setminus D, t)_k \to S_n$ represents a k-cover $f : X \to B$, the morphism $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to S_n$ is the *specialization representation* of f at t_0. The corresponding k-étale algebra is denoted by $\prod_{l=1}^{s} k(X)_{t_0,l}/k$ and called the *specialization algebra* of f at t_0. Each field $k(X)_{t_0,l}$ is a residue extension at some prime above t_0 in the extension $k(X)/k(B)$ and *vice-versa*; $k(X)_{t_0,l}$ is called *a specialization* of f at t_0. The *compositum* in $k^{\rm sep}$ of the Galois closures of all specializations at t_0 is *the* specialization at t_0 of the Galois closure of f (viewed as a k-G-Galois cover). If the k-cover f is regular, the fields $k(X)_{t_0,l}$ correspond to the definition fields of the points in the fiber $f^{-1}(t_0)$ and $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to S_n$ to the *action* of G_k on them.

§3. The twisting lemma

Given a field k, the question we address is whether a given k-cover specializes to a given k-étale algebra at some unramified k-rational point. We first consider the situation of Galois covers in §3.1 and then handle the non-Galois situation in §3.2 by "going to the Galois closure". The

[3] *i.e.* such that the image group is a transitive subgroup of S_n.

Galois situation was considered in [DG11a] in the special case of *regular* Galois covers. But the Galois closure of a k-cover is not regular in general, even if $f : X \to B$ is regular, and this special case needs to be extended. §3.1 is a generalization of the twisting lemma from [DG11a] to not necessarily regular Galois covers.

3.1. The twisting lemma for Galois covers

Fix the field k and a Galois k-cover $g : Z \to B$. Denote its branch divisor by D, the Galois group $\mathrm{Gal}(k(Z)/k(B))$ by G, the π_1-representation of the k-G-Galois cover $g : Z \to B$ by $\phi : \pi_1(B \setminus D, t)_k \to G$, the geometric monodromy group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ by $\overline{G}$ and the constant extension in $g : Z \to B$ by $\widehat{k}_g/k$.

3.1.1. *Twisting Galois covers* Let N/k be some Galois extension with Galois group H isomorphic to a subgroup of G. With no loss we may and will view H itself as a subgroup of G. The constant extension $\widehat{k}_g/k$ is characterized by this condition: $\widehat{k}_g(B)$ is the fixed field in $k(Z)$ of geometric monodromy group $\overline{G} \subset G$. We assume the following *compatibility condition* of N/k with the constant extension $\widehat{k}_g/k$:

(const/comp) *the fixed field* $N^{H\cap\overline{G}}$ *of* $H \cap \overline{G}$ *in* N *is the field* $\widehat{k}_g$.

This condition is trivially satisfied in the regular case as both fields $N^{H\cap\overline{G}}$ and $\widehat{k}_g$ equal k.

Consider the homomorphism $\Lambda : \mathrm{G}_k \to G/\overline{G}$ induced by ϕ on the quotient $\mathrm{G}_k = \pi_1(B \setminus D, t)_k/\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$. The map Λ is a G-Galois representation of the constant extension $\widehat{k}_g/k$ (relative to k^{sep}); it is called the *constant extension map* [DD97, §2.8]. As it is surjective, we have $\mathrm{Gal}(\widehat{k}_g/k) \simeq G/\overline{G}$ and so condition (const/comp) implies that $H\overline{G} = G$.

Let $\varphi : \mathrm{G}_k \to H$ be the G-Galois representation of the Galois extension N/k (relative to k^{sep}) and $\overline{\varphi} : \mathrm{G}_k \to G/\overline{G}$ be the composed map of φ with the canonical surjection $\overline{\cdot} : G \to G/\overline{G}$. Hypothesis (const/comp) rewrites as follows:

(const/comp) *There exists* $\overline{\chi} \in \mathrm{Aut}(G/\overline{G})$ *such that* $\Lambda = \overline{\chi} \circ \overline{\varphi}$.

(The equivalence follows from $\widehat{k}_g = (k^{\mathrm{sep}})^{\ker(\Lambda)}$ and

$$(k^{\mathrm{sep}})^{\ker(\overline{\varphi})} = \big((k^{\mathrm{sep}})^{\ker(\varphi)}\big)^{\ker(\overline{\varphi})/\ker(\varphi)} = N^{\varphi(\ker(\overline{\varphi}))} = N^{H\cap\overline{G}} \ .$$

Also note that as $\Lambda : \mathrm{G}_k \to G/\overline{G}$ is onto, an automorphism $\overline{\chi}$ satisfying (const/comp) is unique).

Assume there exists an isomorphism $\chi : H \to H'$ onto a subgroup $H' \subset G$ that induces $\overline{\chi}$ modulo $\overline{G}$. With $\mathrm{Per}(G)$ the permutation group of G, consider then the map

$$\widetilde{\phi}^{\chi\varphi} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(G)$$

defined by this formula, where r is the restriction $\pi_1(B \setminus D, t)_k \to \mathrm{G}_k$: for $\theta \in \pi_1(B \setminus D, t)_k$ and $x \in G$,

$$\widetilde{\phi}^{\chi\varphi}(\theta)(x) = \phi(\theta)\ x\ (\chi \circ \varphi \circ r)(\theta)^{-1}$$

It is easily checked that $\widetilde{\phi}^{\chi\varphi}$ is a group homomorphism. However the corresponding action of $\pi_1(B \setminus D, t)_k$ on G is not transitive in general. More precisely we have the following.

Lemma 3.1. *Under hypothesis* (const/comp)*, we have* $\widetilde{\phi}^{\chi\varphi}(\theta)(\overline{G}) \subset \overline{G}$ *for every* $\theta \in \pi_1(B \setminus D, t)_k$*.*

Proof. For all $\theta \in \pi_1(B \setminus D, t)_k$ and $x \in \overline{G}$, we have:

$$\overline{\widetilde{\phi}^{\chi\varphi}(\theta)(x)} \ = \ \overline{\phi(\theta)} \,.\, \overline{x} \,.\, \overline{(\chi \circ \varphi \circ r)(\theta)}^{-1} \ = \ \Lambda(r(\theta)) \,.\, \overline{\chi}(\varphi(r(\theta)))^{-1} \ = \ 1$$

Q.E.D.

Consider the morphism, denoted by $\widetilde{\phi}^{\chi\varphi}_{\overline{G}} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(\overline{G})$, that sends $\theta \in \pi_1(B \setminus D, t)_k$ to the restriction of $\widetilde{\phi}^{\chi\varphi}(\theta)$ on $\overline{G}$. Its restriction $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}} \to \mathrm{Per}(\overline{G})$ is given by

$$\widetilde{\phi}^{\chi\varphi}_{\overline{G}}(\theta)(x) = \phi(\theta)\ x \qquad (\theta \in \pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}, x \in \overline{G})$$

Thus this restriction is obtained by composing the original π_1-representation ϕ restricted to $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ with the left-regular representation $\overline{G} \to \mathrm{Per}(\overline{G})$ of $\overline{G}$. This shows that $\widetilde{\phi}^{\chi\varphi}_{\overline{G}} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(\overline{G})$ is the π_1-representation of some regular k-cover, which we denote by $\widetilde{g}^{\chi\varphi} : \widetilde{Z}^{\chi\varphi} \to B$ and call the *twisted cover* of g by $\chi\varphi$.

3.1.2. *Statement of the twisting lemma for Galois covers* The following statement gives the main property of the twisted cover.

Some notation is needed. Conjugation automorphisms in some group $\mathcal{G}$ are denoted by $\mathrm{conj}(\omega)$ for $\omega \in \mathcal{G}$: $\mathrm{conj}(\omega)(x) = \omega\, x\, \omega^{-1}$ $(x \in \mathcal{G})$. The set of all isomorphisms $\chi : H \to H'$ onto a subgroup $H' \subset G$ that induce $\overline{\chi}$ modulo $\overline{G}$ is denoted by $\mathrm{Isom}_{\overline{\chi}}(H, H')$.

Fix then a set $\{\chi_\gamma : H \to H_\gamma \mid \gamma \in \Gamma\}$ of representatives of all isomorphims $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ with H' ranging over all subgroups of G isomorphic to H, modulo the equivalence that identifies $\chi_1 \in \mathrm{Isom}_{\overline{\chi}}(H, H'_1)$ and $\chi_2 \in \mathrm{Isom}_{\overline{\chi}}(H, H'_2)$ if $H'_2 = \omega\, H'_1\, \omega^{-1}$ and $\chi_2 \chi_1^{-1} = \mathrm{conj}(\omega)$ for some $\omega \in \overline{G}$.

Twisting lemma 3.2 (Galois form)**.** *Under condition* (const/comp)*, we have the following conclusions* (a) *and* (b)*.*

(a) *For each subgroup $H' \subset G$ isomorphic to H, each $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ and each $t_0 \in B(k) \setminus D$, these conditions are equivalent:*

(i) *there exists a point $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ such that $\widetilde{g}^{\chi\varphi}(x_0) = t_0$,*

(ii) *there is $\omega \in \overline{G}$ such that $(\phi \circ \mathsf{s}_{t_0})(\tau) = \omega\,(\chi \circ \varphi)(\tau)\,\omega^{-1}$, $\tau \in \mathrm{G}_k$, (where $\mathsf{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ is the section associated with t_0).*

(b) *For each $t_0 \in B(k) \setminus D$, the following are equivalent:*

(iii) *the specialization $k(Z)_{t_0}/k$ of the k-G-Galois cover $g : Z \to B$ is the extension N/k,*

(iv) *there exists an isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ such that conditions* (i)-(ii) *hold for this χ,*

(v) *there exists $\gamma \in \Gamma$ such that conditions* (i)-(ii) *hold for $\chi = \chi_\gamma$.*

Furthermore an element $\gamma \in \Gamma$ as in (v) *is necessarily unique.*

A *single* twisted cover is involved in (a) while there are several in (b). In this respect the representation viewpoint used in (a) may look more natural than the field extension one in (b). The latter however is more useful in practice. Also note that conditions (iv)-(v), being equivalent to (iii), do not depend on the chosen π_1-representation $\phi : \pi_1(B \setminus D, t)_k \to G$ of $g : Z \to B$ modulo conjugation by elements of G.

Remark 3.3. (a) Existence of some subgroup $H' \subset G$ such that the set $\mathrm{Isom}_{\overline{\chi}}(H, H')$ is non-empty, which amounts to $\Gamma \neq \emptyset$, is not guaranteed; if $\Gamma = \emptyset$, conditions (iii)-(iv)-(v) fail. It is however guaranteed under each of the assumptions $\overline{\chi} = \mathrm{Id}_{G/\overline{G}}$ or $\mathrm{Out}(G/\overline{G}) = \{1\}$. Indeed if $\overline{\chi} = \mathrm{Id}_{G/\overline{G}}$, then $\mathrm{Id}_H \in \mathrm{Isom}_{\overline{\chi}}(H, H)$, and if $\mathrm{Out}(G/\overline{G}) = \{1\}$, the automorphism $\overline{\chi} \in \mathrm{Aut}(G/\overline{G})$ is inner, of the form $\mathrm{conj}(\overline{\omega})$ with $\overline{\omega} \in G/\overline{G}$, and, as $H\overline{G} = G$, lifts to some isomorphism $\mathrm{conj}(\omega) : H \to H$ with $\omega \in H$. Both assumptions include the regular case as then $G/\overline{G} = \{1\}$.

(b) Some uniqueness property can be added to (iv), as in (v). Indeed an isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ satisfying conditions (i)-(ii), as the one in (iv), is necessarily unique up to left composition by $\mathrm{conj}(\omega)$ with $\omega \in \mathrm{Nor}_{\overline{G}}(\phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$. The advantage of condition (v) is that the set $\bigcup_{\gamma\in\Gamma} \widetilde{Z}^{\chi_\gamma\varphi}(k)$ where unramified k-rational points should be found to conclude that (iii) holds does not depend on t_0 (although the element $\gamma \in \Gamma$ in (v) does). Moreover the uniqueness property in (v) makes it easier to count the points $t_0 \in B(k)$ for which (iii) holds.

(c) The proof of (i) $\Leftrightarrow$ (ii) below shows further that the number of k-rational points on $\widetilde{Z}^{\chi\varphi}$ above some given unramified point $t_0 \in B(k)$, if positive, is equal to the order of the group $\mathrm{Cen}_{\overline{G}}(\chi(H))$.

3.1.3. *Proof of the twisting lemma 3.2* (a) Fix a subgroup $H' \subset G$ isomorphic to H, an isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ and a point $t_0 \in B(k) \setminus D$. The map $\widetilde{\phi}^{\chi\varphi}_{\overline{G}} \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to \mathrm{Per}(\overline{G})$ is the action of G_k on the fiber $(\widetilde{g}^{\chi\varphi})^{-1}(t_0)$; it is given by

$$\widetilde{\phi}^{\chi\varphi}_{\overline{G}}(\mathsf{s}_{t_0}(\tau))(x) = \phi(\mathsf{s}_{t_0}(\tau))\ x\ (\chi\circ\varphi)(\tau)^{-1} \qquad (\tau \in \mathrm{G}_k, x \in \overline{G})$$

The elements $\widetilde{\phi}^{\chi\varphi}_{\overline{G}}(\mathsf{s}_{t_0}(\tau))$ have a common fixed point $\omega \in \overline{G}$ if and only if $\phi(\mathsf{s}_{t_0}(\tau)) = \omega\,(\chi\circ\varphi)(\tau)\,\omega^{-1}$ $(\tau \in \mathrm{G}_k)$. This yields (i) $\Leftrightarrow$ (ii). Furthermore, the set of all $\omega \in \overline{G}$ satisfying the preceding condition, if non empty, is a left coset $\omega_0\,\mathrm{Cen}_{\overline{G}}(\chi(H))$; this proves remark 3.3 (c).

(b) Fix $t_0 \in B(k) \setminus D$ and a representative of the section $\mathsf{s}_{t_0} : \mathrm{G}_k \to \pi_1(B\setminus D, t)_k$ (defined up to conjugation by an element in $\pi_1(B\setminus D, t)_{k^{\mathrm{sep}}}$).

Implication (iv) $\Rightarrow$ (iii) follows from the fact that if $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi\circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ satisfies (i)-(ii), then $\ker(\phi \circ \mathsf{s}_{t_0})$ and $\ker(\varphi)$ are equal, hence so are their fixed fields in k^{sep}. Conversely assume that the extensions $k(Z)_{t_0}/k$ and N/k are equal, *i.e.* $\ker(\phi\circ\mathsf{s}_{t_0})$ and $\ker(\varphi)$ are the same subgroup, say $\mathcal{K}$, of G_k. The two morphisms $\phi\circ\mathsf{s}_{t_0} : \mathrm{G}_k \to \phi\circ\mathsf{s}_{t_0}(\mathrm{G}_k) \subset G$ and $\varphi : \mathrm{G}_k \to H \subset G$ then differ from $\mathrm{G}_k \to \mathrm{G}_k/\mathcal{K}$ by some isomorphisms $\phi\circ\mathsf{s}_{t_0}(\mathrm{G}_k) \to \mathrm{G}_k/\mathcal{K}$ and $H \to \mathrm{G}_k/\mathcal{K}$, respectively. Thus they differ from one another by an isomorphism $\chi : H \to \phi\circ\mathsf{s}_{t_0}(\mathrm{G}_k)$: $\phi\circ\mathsf{s}_{t_0} = \chi\circ\varphi$. It follows from this and from uniqueness of $\overline{\chi}$ satisfying (const/comp) that χ automatically induces $\overline{\chi}$ modulo $\overline{G}$. Conclude that $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi\circ\mathsf{s}_{t_0}(\mathrm{G}_k))$ and conditions (i)-(ii) hold for this χ.

Assume (v) holds, *i.e.*, for some $\gamma \in \Gamma$, condition (i)-(ii) are satisfied for the isomorphism $\chi_\gamma : H \to H_\gamma$ and some $\omega \in \overline{G}$. It readily follows that $\chi = \mathrm{conj}(\omega)\circ\chi_\gamma$ also satisfies (ii) and is in $\mathrm{Isom}_{\overline{\chi}}(H, \phi\circ \mathsf{s}_{t_0}(\mathrm{G}_k))$. This establishes (iv). Conversely assume (iv) holds. Let $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi\circ\mathsf{s}_{t_0}(\mathrm{G}_k))$ be an isomorphism such that conditions (i)-(ii) hold, for some $\omega \in \overline{G}$. There exist $\gamma \in \Gamma$ and $\omega' \in \overline{G}$ such that $\chi = \mathrm{conj}(\omega')\circ\chi_\gamma$. It follows that condition (ii) holds for χ_γ as well (with conjugation factor $\omega\omega'$). Uniqueness of $\gamma \in \Gamma$ in condition (v) readily follows from condition (ii) and the definition of the set $\{\chi_\gamma \,|\, \gamma \in \Gamma\}$. Q.E.D.

3.2. The general form of the twisting lemma

We fix a degree n k-cover $f : X \to B$ and a degree n k-étale algebra $\prod_{l=1}^{s} E_l/k$ and the question we address is whether $\prod_{l=1}^{s} E_l/k$ *is (equivalent to) the specialization algebra* $\prod_l k(X)_{t_0,l}/k$ *of* f *at some unramified point* $t_0 \in B(k)$.

3.2.1. *Statement of the result* Denote the branch divisor of $f : X \to B$ by D, its Galois closure by $g : Z \to B$, the Galois group $\mathrm{Gal}(k(Z)/k(B))$ by G, the π_1-representation of the k-G-Galois cover $g : Z \to B$ by $\phi : \pi_1(B \setminus D, t)_k \to G$, the Galois representation of the field extension $k(X)/k(B)$ relative to $k(Z)$ by $\nu : G \to S_n$, the geometric monodromy group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ by $\overline{G}$ and the constant extension in $g : Z \to B$ by $\widehat{k}_g/k$.

Let N/k be the *compositum* inside k^{sep} of the Galois closures of the extensions E_l/k, $l = 1, \ldots, s$, and $H = \mathrm{Gal}(N/k)$. A necessary condition for a positive answer to the question is that N be the *compositum* inside k^{sep} of the Galois closures of the extensions $k(X)_{t_0,l}/k$. In particular, H should be isomorphic to some subgroup of G. From now on we will assume it. With no loss we may then and will view H as a subgroup of G. Finally let $\varphi : \mathrm{G}_k \to H$ be the G-Galois representation of N/k relative to k^{sep} and $\mu : H \to S_n$ be the Galois representation of $\prod_{l=1}^{s} E_l/k$ relative to N.

Some further notation from §3.1 is retained. The constant extension compatibility condition (const/comp) determines a unique automorphism $\overline{\chi}$ of $G/\overline{G}$ (§3.1.1). The twisted cover $\widetilde{g}^{\chi\varphi} : \widetilde{Z}^{\chi\varphi} \to B$ is defined for every isomorphism $\chi : H \to H'$ onto a subgroup $H' \subset G$ inducing $\overline{\chi}$ modulo $\overline{G}$ (§3.1.1). The set of all such isomorphisms $\chi : H \to H'$ is denoted by $\mathrm{Isom}_{\overline{\chi}}(H, H')$. The isomorphisms $\chi_\gamma : H \to H_\gamma$ ($\gamma \in \Gamma$) are defined in §3.1.2.

Twisting lemma 3.4 (general form)**.** *Let $f : X \to B$ be a k-cover and $\prod_{l=1}^{s} E_l/k$ be a k-étale algebra as above. Assume further that condition* (const/comp) *from §3.1.1 holds for the Galois closure $g : Z \to B$ of f. Then for each $t_0 \in B(k) \setminus D$, the following conditions are equivalent:*

(i) $\prod_l E_l/k$ *is the specialization algebra* $\prod_l k(X)_{t_0,l}/k$ *of* f *at* t_0.

(ii) *there is a subgroup $H' \subset G$ isomorphic to H and an isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ such that*

1. *there exists $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ with $\widetilde{g}^{\chi\varphi}(x_0) = t_0$, and*
2. *there exists $\sigma \in S_n$ that $\nu \circ \chi(h) = \sigma\, \mu(h)\, \sigma^{-1}$ for every $h \in H$.*

Furthermore if (ii) *holds, it holds for some isomorphism $\chi_\gamma : H \to H_\gamma$ for some $\gamma \in \Gamma$ and the element γ is then necessarily unique.*

3.2.2. *About condition* (ii-2) We focus on condition (ii-2) which is the group-theoretical part of condition (ii) (while condition (ii-1) is the diophantine part).

We first note for later use that if condition (ii-2) holds for $\chi = \chi_{\gamma_0}$ with $\gamma_0 \in \Gamma$, the number of $\gamma \in \Gamma$ for which condition (ii-2) holds for $\chi = \chi_\gamma$ is equal to the number of isomorphisms χ_γ ($\gamma \in \Gamma$) such that the actions $\nu \circ \chi_\gamma : H \to S_n$ and $\nu \circ \chi_{\gamma_0} : H \to S_n$ are conjugate in S_n.

Below we give three standard situations where condition (ii-2) holds.

(a) *geometric monodromy group* S_n: $G = \overline{G} = S_n$ as in [DL11]. Condition (const/comp) holds and $\nu : S_n \to S_n$ is the natural action: $\nu = \mathrm{Id}_{S_n}$. Condition $\nu \circ \chi_\gamma(h) = \sigma\, \mu(h)\, \sigma^{-1}$ ($h \in H$) is satisfied with χ_γ the representative of the isomorphism $\mu : H \to \mu(H) \subset S_n$ (and some $\sigma \in S_n$).

(b) *Galois situation*: $f : X \to B$ is a Galois k-cover, $\prod_l E_l/k$ is a Galois field extension E/k of group $H \subset G$ and $\Gamma \neq \emptyset$. Then ν is the left-regular representation $G \to \mathrm{Per}(G)$ and μ its restriction $H \to \mathrm{Per}(G)$. Note next that if $\gamma \in \Gamma$, the restriction $\nu|_H : H \to \mathrm{Per}(G)$ and $\nu \circ \chi_\gamma : H \to \mathrm{Per}(G)$ are conjugate actions. Condition (ii-2) follows.

In (c) below, the *type of a permutation* $\sigma \in S_n$ is the (multiplicative) divisor of all lengths of disjoint cycles involved in the cycle decomposition of σ (for example, an n-cycle is of type n^1).

(c) *cyclic specializations*: condition (const/comp) holds, H is a cyclic subgroup of G generated by an element ω such that $\nu(\omega)$ is of type equal to the divisor of all degrees $[E_l : k]$ of field extensions in the étale algebra $\prod_l E_l/k$.

Indeed for every integer $a \geq 1$ such that $(a, |H|) = 1$, let $\chi_a : H \to H$ be the morphism that maps ω to ω^a. As $H\overline{G} = G$, each map χ_a induces an automorphism of the cyclic group $G/\overline{G}$. Then there is necessarily an integer $a \geq 1$ such that χ_a induces $\overline{\chi}$ modulo $\overline{G}$ and $(a, |H|) = 1$ [4]. From the hypothesis, the types of $\nu(\omega)$ and $\mu(\omega)$ are the same. But so are the types of $\nu(\omega)$ and $\nu \circ \chi_a(\omega)$. Conclude that the actions $\nu \circ \chi_a$ and μ are conjugate.

3.2.3. *Comparizon with previous forms* We compare the general form (lemma 3.4) with the Galois form (lemma 3.2) and the geometric monodromy group S_n form [DL11, lemma 2.1] of the twisting lemmas.

---

[4] An exercise: this amounts to showing that if b is an integer prime to $\nu = |G/\overline{G}|$ and $|G| = \mu\nu$, then there exists an integer $a = b + k\nu$ that is prime to $\mu\nu$. Take for k the product of the prime divisors of μ that do not divide b.

Lemma 3.4 (general form) ⇒ lemma 3.2 (Galois form): Both forms have the assumption (const/comp). In the Galois situation from §3.1, the k-cover is *Galois* (and so $f = g$) and the k-étale algebra is a *Galois* field extension E/k with group $\mathrm{Gal}(E/k) = H$ (so $\prod_{l=1}^{s} E_l/k = E/k$ and $N = E$). Then statement (i) ⇔ (ii) in lemma 3.4 exactly corresponds to statement (iii) ⇔ (v) in lemma 3.2.

Indeed condition (ii) from lemma 3.4 reduces to its first part (ii-1) (see §3.2.2 (b)) and then coincides with condition (v) from lemma 3.2, and condition (i) from lemma 3.4 corresponds to condition (iii) from lemma 3.2 (note that the étale algebra $\prod_l E_l/k$ (resp. $\prod_l k(X)_{t_0,l}/k$) from condition (i) is a product of $|G|/|H|$ copies of the Galois field extension E/k (resp. $k(X)_{t_0}/k$)).

Lemma 3.4 (general form) ⇒ lemma 2.1 from [DL11]: In [DL11], the k-cover $f : X \to B$ is of degree n and geometric monodromy group S_n. Then $G = \overline{G} = S_n$, that is, we are in the standard situation (a) from §3.2.2. Thus condition (ii-2) holds. The twisted cover $\widetilde{g}^N : \widetilde{Z}^N \to B$ in [DL11, lemma 2.1] is the twisted cover $\widetilde{g}^{\mu\varphi} : \widetilde{Z}^{\mu\varphi} \to B$ in this paper. Conclude that (i) ⇒ (ii) in [DL11, lemma 2.1] exactly corresponds to (ii) ⇒ (i) in lemma 3.4.

3.2.4. *Proof of the twisting lemma 3.4* We will use the Galois form of the twisting lemma to establish the general form.

(i) ⇒ (ii): Assume (i) holds. Necessarily N is the compositum of the Galois closures of the extensions $k(X)_{t_0,l}/k$. From the twisting lemma 3.2 for Galois covers, there is a unique $\gamma \in \Gamma$ satisfying condition (ii-1) from lemma 3.4. And from lemma 3.2 (a), this last condition is equivalent to existence of some $\omega \in \overline{G}$ such that $(\phi \circ \mathsf{s}_{t_0})(\tau) = \omega\,(\chi_\gamma \circ \varphi)(\tau)\,\omega^{-1}$ for all $\tau \in \mathrm{G}_k$. Thus we obtain:

$$(\nu \circ \phi \circ \mathsf{s}_{t_0})(\tau) = \nu(\omega)\ (\nu \circ \chi_\gamma \circ \varphi)(\tau)\ \nu(\omega)^{-1} \qquad (\tau \in \mathrm{G}_k)$$

But condition (i) gives $\nu \circ \phi \circ \mathsf{s}_{t_0}(\tau) = \beta\,\mu \circ \varphi(\tau)\,\beta^{-1}$ $(\tau \in \mathrm{G}_k)$, for some $\beta \in S_n$. Conjoining these equalities yields condition (ii-2).

(ii) ⇒ (i): Assume (ii) holds. From lemma 3.2, existence of $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ such that $\widetilde{g}^{\chi\varphi}(x_0) = t_0$ implies that N is the compositum of the Galois closures of the $k(X)_{t_0,l}$, and so we have $(\phi \circ \mathsf{s}_{t_0})(\tau) = \omega\,(\chi \circ \varphi)(\tau)\,\omega^{-1}$ for some $\omega \in \overline{G}$ and all $\tau \in \mathrm{G}_k$.

Denote the orbits of $\mu : H \to S_n$, which correspond to the extensions $E_1, \dots E_s$, by $\mathcal{O}_1, \dots, \mathcal{O}_s$. Fix one of them, *i.e.* $l \in \{1, \dots, s\}$, and let $i \in \{1, \dots, n\}$ be some index such that E_l is the fixed field in k^{sep} of the

subgroup of G_k fixing i *via* the action $\mu \circ \varphi$. For $j = \nu(\omega)(\sigma(i))$ (with σ given by condition (ii-2)), we have

$$\begin{aligned}(\nu \circ \phi \circ \mathsf{s}_{t_0})(\tau)(j) &= \nu(\omega)\,(\nu \circ \chi \circ \varphi)(\tau)\,(\sigma(i)) \\ &= \nu(\omega)\,(\mathrm{conj}(\sigma) \circ \mu \circ \varphi)(\tau)\,(\sigma(i)) \\ &= \nu(\omega)\;\sigma\;(\mu \circ \varphi)(\tau)(i)\end{aligned}$$

and so j is fixed by $(\nu \circ \phi \circ \mathsf{s}_{t_0})(\tau)$ if and only if i is fixed by $(\mu \circ \varphi)(\tau)$. Conclude that the specialization $k(X)_{t_0,j}$ is the field E_l. Q.E.D.

§4. Applications

4.1. PAC fields

Recall that a field k is said to be PAC if every non-empty geometrically irreducible k-variety has a Zariski-dense set of k-rational points. If k is PAC, the twisting lemma leads to the following statements in the two standard situations (b) and (c) from §3.2.2 (the standard situation (a) corresponds to corollary 3.1 from [DL11]). Similar applications over PAC fields can also be found in Bary-Soroker's works [BS10] [BS09].

Corollary 4.1. *Let k be a PAC field, $f : X \to B$ be a k-G-Galois cover of group G and geometric monodromy group $\overline{G}$, and let E/k be a Galois extension of group $H \subset G$. Assume that condition* (const/comp) *from §3.1 holds and* $\mathrm{Out}(G/\overline{G}) = \{1\}$. *Then E/k is* the *specialization $k(X)_{t_0}/k$ of f at each point t_0 in a Zariski-dense[5] subset of $B(k) \setminus D$.*

The special case $G = \overline{G}$ corresponds to theorem 3.2 of [Dèb99a] (which proved the Beckmann-Black conjecture over PAC fields).

Proof. Assumption $\mathrm{Out}(G/\overline{G}) = \{1\}$ assures that $\Gamma \neq \emptyset$ (remark 3.3 (a)). Pick $\gamma \in \Gamma$. Since k is PAC, the variety $\widetilde{Z}^{\chi_\gamma \varphi}$ has a Zariski-dense set $\mathcal{Z}$ of k-rational points. From lemma 3.2, the Zariski-dense subset $\widetilde{g}^{\chi_\gamma \varphi}(\mathcal{Z}) \setminus D \subset B(k) \setminus D$ satisfies the announced conclusion. Q.E.D.

Corollary 4.2. *Let k be a PAC field, $f : X \to B$ be a degree n k-cover and let $1^{\beta_1} \cdots n^{\beta_n}$ be the type of some element of the monodromy group G in the Galois representation $\nu : G \to S_n$ of $k(X)/k(B)$. Let $\prod_l E_l/k$ be an étale algebra such that*
- the divisor of all degrees $[E_l : k]$ is $1^{\beta_1} \cdots n^{\beta_n}$,
- condition (const/comp) *holds,*
- the compositum N/k of the Galois closures of the extensions E_l/k is a cyclic extension of order $\mathrm{lcm}\{\, i \mid \beta_i \neq 0\}$.

[5] but not necessarily Zariski open.

Then $\prod_l E_l/k$ is the specialization algebra $\prod_l k(X)_{t_0,l}/k$ of f at each point t_0 in a Zariski-dense subset of $B(k) \setminus D$.

A useful special case is for $1^{\beta_1} \cdots n^{\beta_n} = n^1$: it can then be concluded that $f : X \to B$ specializes to some degree n field extension at each t_0 in a Zariski-dense subset of $B(k) \setminus D$ (*i.e.* the Hilbert irreducibility conclusion) under the assumptions that there is a n-cycle in $\nu(G)$ and k has a degree n cyclic extension satisfying condition (const/comp). This can be compared to [BS09, corollary 1.4] (and [DL11, corollary 3.1]) which has the same Hilbert conclusion under the assumptions that $G = \overline{G} = S_n$ and k has a degree n separable extension.

Proof. Let $\omega \in G$ with $\nu(\omega)$ of type $1^{\beta_1} \cdots n^{\beta_n}$. Identify the Galois group $H = \mathrm{Gal}(N/k)$ with the subgroup $\langle \omega \rangle \subset G$. We are in the standard situation (c) from §3.2.2 and so condition (ii-2) from lemma 3.4 holds for some isomorphism χ_γ ($\gamma \in \Gamma$). Since k is PAC, condition (ii-1) holds for all t_0 in a Zariski-dense subset of $B(k) \setminus D$. Therefore condition (i) from lemma 3.4 holds as well, thus ending the proof. Q.E.D.

4.2. Finite fields

If k is a suitably large finite field $\mathbb{F}_q$, the Lang-Weil estimates can be used to guarantee that the twisted covers have $\mathbb{F}_q$-rational points. More specifically we have the following result, where we take $B = \mathbb{P}^1$ for simplicity.

Corollary 4.3. *Let $f : X \to \mathbb{P}^1$ be a regular $\mathbb{F}_q$-cover of degree $n \geq 2$, with r branch points and with geometric monodromy group S_n. Let $m_1, \ldots, m_s$ be some positive integers (possibly repeated) such that $\sum_{l=1}^s m_l = n$. Then the number $\mathcal{N}(f, m_1, \ldots, m_s)$ of unramified points $t_0 \in \mathbb{F}_q$ such that $\prod_{l=1}^s \mathbb{F}_{q^{m_l}}/\mathbb{F}_q$ is the specialization algebra of f at t_0 can be evaluated as follows:*

$$\left| \mathcal{N}(f, m_1, \ldots, m_s) - \frac{(q+1)\,|m_1^1 \cdots m_s^1|}{n!} \right| \leq r\, n! \sqrt{q}$$

where $|m_1^1 \cdots m_s^1|$ is the number of elements in the conjugacy class in S_n corresponding to the type $m_1^1 \cdots m_s^1$.

This extends similar estimates that have appeared in the literature for Galois covers under the name of Tchebotarev theorems for function fields over finite fields. See [Wei48], [Fri74] [Eke90], [FJ04, §6], and also [DG11b, cor.3.5] where the Galois analog of corollary 4.3 is obtained as the outcome of our approach in standard situation §3.2.2 (b).

For the type $m_1^1 \cdots m_s^1 = n^1$ of n-cycles, we obtain that the number $\mathcal{N}(f, n)$ is asymptotic to q/n when $q \to +\infty$. For example if $f : X \to$

$\mathbb{P}^1$ over $\mathbb{F}_p$ is given by the trinomial $Y^n + Y - T$ (which satisfies the assumptions of corollary 4.3 if $p \not| n(n-1)$ [Ser92, §4.4]), the number of irreducible trinomials $Y^n+Y+a \in \mathbb{F}_p[Y]$ realizing the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is asymptotic to p/n as $p \to \infty$, a result due to Cohen [Coh70] and Ree [Ree71] proving a conjecture of Chowla [Cho66].

Proof. We are in the standard situation $G = \overline{G} = S_n$. Condition (const/comp) trivially holds. Furthermore, it follows from the beginning note of §3.2.2 that the number of $\gamma \in \Gamma$ for which condition (ii-2) holds is 1; denote by χ_0 the corresponding isomorphism. From lemma 3.4, the set of unramified $\mathbb{F}_q$-rational points on the twisted variety $\widetilde{Z}^{\chi_0\varphi}$ maps *via* the cover $\widetilde{g}^{\chi_0\varphi} : \widetilde{Z}^{\chi_0\varphi} \to \mathbb{P}^1$ to the set of points $t_0 \in \mathbb{P}^1(\mathbb{F}_q)$ satisfying the desired conclusion. Using remark 3.3 (c), we obtain

$$0 \leq \frac{|\widetilde{Z}^{\chi_0\varphi}(\mathbb{F}_q)|}{|\mathrm{Cen}_{S_n}(\chi_0(H))|} - \mathcal{N}(f, m_1, \ldots, m_s) \leq \frac{rn!/2}{|\mathrm{Cen}_{S_n}(\chi_0(H))|}$$

where $H = \mathrm{Gal}(\mathbb{F}_{q^M}/\mathbb{F}_q)$ with $M = \mathrm{lcm}(m_1, \ldots, m_s)$ and the term $rn!/2$ is an upper bound for the number of ramified points on $\widetilde{Z}^{\chi_0\varphi}$. Also note that $\widetilde{g}^{\chi_0\varphi}$ and g being isomorphic over k^{sep}, they have the same branch point number, which is the branch point number r of f, and that the curves $\widetilde{Z}^{\chi_0\varphi}$ and Z have the same genus, say g.

The cyclic subgroup $\chi_0(H) \subset S_n$ is generated by a permutation of type $m_1^1 \cdots m_s^1$ (condition (ii-2) from lemma 3.4). Hence we have $|\mathrm{Cen}_{S_n}(\chi_0(H))| = n!/|m_1^1 \cdots m_s^1|$. The Lang-Weil estimates give:

$$|\,|\widetilde{Z}^{\chi_0\varphi}(\mathbb{F}_q)| - (q+1)| \leq 2\mathrm{g}\sqrt{q}$$

The Riemann-Hurwitz formula yields $\mathrm{g} \leq (r-2)(n!-1)/2$. The announced estimate easily follows. (We use that the largest cardinality of a conjugacy class in S_n is $n(n-2)!$, *i.e.*, that of the class of $n-1$-cycles). Q.E.D.

4.3. Number fields

Over number fields, we will follow a local-global approach as in [DL11] and [DG11a]. We start with a local result at one prime. We give two versions: a *mere version* for a cover $f : X \to \mathbb{P}^1$ and a G-*version* for a G-Galois cover $g : Z \to \mathbb{P}^1$.

For the next two statements, let k be a number field, $f : X \to \mathbb{P}^1$ be a degree n regular k-cover, r be the branch point number, G (resp. $\overline{G}$) be the monodromy group (resp. the geometric monodromy group), $g : Z \to \mathbb{P}^1$ be the Galois closure of f, $\nu : G \to S_n$ be the Galois

representation of $k(X)/k(T)$ (relative to $k(Z)$) and $\widehat{k}_g/k$ be the constant extension in g. A prime number p is said to be *bad* if it is one from the finite list of primes for which the branch divisor is not étale or there is vertical ramification at p [DG11a], it is said to be *good* otherwise.

Corollary 4.4. *Suppose given*
(in the mere version): *the type* $1^{\beta_1}\cdots n^{\beta_n}$ *of an element of* $\nu(\overline{G})\subset S_n$,
(in the G-version): *an element* $\omega\in\overline{G}$.
Then for each prime $p\geq r^2|\overline{G}|^2$, *good and totally split in* $\widehat{k}_g/\mathbb{Q}$, *there exists an integer* $b_p\in\mathbb{Z}$ *such that for each integer* $t_0\equiv b_p \bmod p$,
(mere version) *the specialization algebra of* $f\otimes_k\mathbb{Q}_p$ *at* t_0 *is an étale algebra* $\prod_l E_l/\mathbb{Q}_p$ *with degree divisor* $\prod_l[E_l:\mathbb{Q}_p]^1=1^{\beta_1}\cdots n^{\beta_n}$,
(G-version) *the specialization of the* $\mathbb{Q}_p$-G-*Galois cover* $g\otimes_k\mathbb{Q}_p$ *at* t_0 *is the unramified extension* $N_p/\mathbb{Q}_p$ *of degree* $|\langle\omega\rangle|$.

The mere version generalizes theorem 4 from [Fri74]: if $\nu(\overline{G})$ contains an n-cycle, then, for $1^{\beta_1}\cdots n^{\beta_n}=n^1$, the conclusion, stated as in [Fri74] in the situation f is given by a polynomial $P(T,Y)$, is that $P(t_0,Y)$ is irreducible in $\mathbb{Q}_p[Y]$, and so in $k[Y]$ too.

Proof. Consider first the mere version. Let p be a totally split prime in the extension $\widehat{k}_g/\mathbb{Q}$ (infinitely many such primes exist from the Tchebotarev density theorem). In particular $\mathbb{Q}_p\widehat{k}_g=\mathbb{Q}_p$. For each $i=1,\dots,n$ with $\beta_i>0$, let $E^{p,i}/\mathbb{Q}_p$ be the unique unramified extension of $\mathbb{Q}_p$ of degree i. Here we use the twisting lemma 3.4 in the "cyclic specializations" standard situation (c) from §3.2.2; we apply it to the cover $f\otimes_k\mathbb{Q}_p$ and the $\mathbb{Q}_p$-étale algebra $\prod_i(E^{p,i}/\mathbb{Q}_p)^{\beta_i}$, where the exponent β_i indicates that the extension $E^{p,i}/\mathbb{Q}_p$ appears β_i times. Condition (const/comp) holds by definition of $\widehat{k}_g$ and condition (ii-2) from lemma 3.4 holds for some isomorphism χ_γ, $\gamma\in\Gamma$ (§3.2.2 (c)). If p is a good prime, the twisted curve $\widetilde{Z}^{\chi_\gamma\varphi}\otimes_k\mathbb{Q}_p$ has good reduction, and the Lang-Weil estimates then show that if $p\geq r^2|\overline{G}|^2$, the special fiber has at least one unramified $\mathbb{F}_p$-rational point; see [DL11, corollary 3.2] for more details. From Hensel's lemma, such a $\mathbb{F}_p$-rational point lifts to a $\mathbb{Q}_p$-rational point on $\widetilde{Z}^{\chi_\gamma\varphi}$. Conclude with lemma 3.4 that the étale algebra $\prod_i(E^{p,i}/\mathbb{Q}_p)^{\beta_i}$ is the specialization algebra of $f\otimes_k\mathbb{Q}_p$ at each point t_0 in a coset of $\mathbb{Z}_p$ modulo $p\mathbb{Z}_p$.

The G-version is very similar, but it is the Galois form of the twisting lemma (lemma 3.2) that should be applied, to the regular $\mathbb{Q}_p$-G-Galois cover $g\otimes_k\mathbb{Q}_p$ and the unramified extension of $\mathbb{Q}_p$ of degree $|\langle\omega\rangle|$. Q.E.D.

Corollary 4.4 can be used simultaneously for several types of elements in $\nu(\overline{G}) \subset S_n$ and for several elements of $\overline{G}$. The weak approximation property of $\mathbb{P}^1$ (the Artin-Whaples theorem) then provides arithmetic progressions $(am+b)_{m\in\mathbb{Z}} \subset \mathbb{Z}$ with ratio a the product of several corresponding primes. In particular by using all non-trivial elements of $\overline{G}$, it can be guaranteed that the specialization at $am+b$ (for every $m \in \mathbb{Z}$) of the $\widehat{k}_g$-G-Galois cover $g \otimes_k \widehat{k}_g$ be a Galois extension of group $\overline{G}$; this uses a standard argument (recalled in [DG11a, §3.4]) based on a lemma of Jordan. This implies that the specialization at $am+b$ of the k-G-Galois cover g is a Galois extension of group a subgroup of G containing $\overline{G}$. As the k-cover $f : X \to \mathbb{P}^1$ is assumed to be regular (and so $\nu(\overline{G})$ is a transitive subgroup of S_n), it follows that the specialization algebra at $am+b$ of the k-cover f is a single field extension of degree n, *i.e.* Hilbert's conclusion holds at $am+b$ (for every $m \in \mathbb{Z}$).

We obtain the following statement, which generalizes [DL11, corollary 4.1] to arbitrary regular covers.

The constants however are not as good as in the "$G = \overline{G} = S_n$" situation of [DL11] because of the preliminary condition on the primes p that uses the Tchebotarev theorem.

Corollary 4.5. *There exist integers $m_0, \beta > 0$ depending on f such that the following holds. Let $\mathcal{S}$ be a finite set of primes $p > m_0$, good and totally split in $\widehat{k}_g/\mathbb{Q}$, each given with positive integers $d_{p,1} \dots, d_{p,s_p}$ (possibly repeated) such that $d_{p,1}^1 \cdots d_{p,s_p}^1$ is the type of some element in $\nu(\overline{G})$. Then there exists an integer $b \in \mathbb{Z}$ such that*

(*) *for each integer $t_0 \equiv b \bmod (\beta \prod_{p\in\mathcal{S}} p)$, t_0 is not a branch point of f and the specialization algebra of f at t_0 is a single degree n field extension with residue degrees $d_{p,1} \dots, d_{p,s_p}$ at p for each $p \in \mathcal{S}$.*

Addendum 4.5 (on the constants) Denote the number of non-trivial conjugacy classes of $\overline{G}$ by $\mathrm{cc}(\overline{G})$. One can take m_0 such that the interval $[r^2|\overline{G}|^2, m_0]$ contains at least $\mathrm{cc}(\overline{G})$ primes, good and totally split in $\widehat{k}_g/\mathbb{Q}$, and β to be the product of $\mathrm{cc}(\overline{G})$ such primes.

Proof. We use corollary 4.4 simultaneaously for several primes: a first set of primes associated to all non-trivial elements of $\overline{G}$ as explained above, and the set of primes given in the statement with the associated types. We apply the G-version of corollary 4.4 to the former data and the mere version to the latter. This provides an arithmetic progression $(am+b)_{m\in\mathbb{Z}} \subset \mathbb{Z}$ with ratio $a = \beta \prod_{p\in\mathcal{S}} p$ where $\beta > 0$ is the product of the primes in the first set. The primes dividing β guarantee that the specialization algebra at $am+b$ of the k-cover f is a single field extension

E/k of degree n. And each of the primes $p \in \mathcal{S}$ gives that the $\mathbb{Q}_p$-étale algebra $E \otimes_k \mathbb{Q}_p$ has degree divisor $d^1_{p,1} \cdots d^1_{p,s_p}$. Q.E.D.

4.4. Ample fields

Recall that a field k is said to be *ample* if every smooth k-curve with a k-rational point has infinitely many k-rational points. Over an ample field, the twisting lemma 3.4 yields the following statement which generalizes §3.3.2 (***) from [Dèb99a].

Corollary 4.6. *Let k be an ample field and $f : X \to B$ be a degree n k-cover of curves. Let $t_0 \in B(k)$ not in the branch point set $\mathbf{t}$. There exist infinitely many $t \in B(k) \setminus \mathbf{t}$ such that the specialization algebras $\prod_l k(X)_{t,l}/k$ and $\prod_l k(X)_{t_0,l}/k$ at t and t_0 respectively are equal.*

Proof. Take the k-étale algebra $\prod_{l=1}^s E_l/k$ from lemma 3.4 to be the specialization algebra $\prod_{l=1}^s k(X)_{t_0,l}/k$ at t_0. With the notation from §3.1, we have $\varphi = \phi \circ \mathsf{s}_{t_0}$ and $\overline{\varphi} = \Lambda$. Hence condition (const/comp) holds with $\overline{\chi} = \mathrm{Id}_{G/\overline{G}}$, and $\Gamma \neq \emptyset$ (remark 3.3 (a)). From implication (i) $\Rightarrow$ (ii) in lemma 3.4, there exists $\gamma \in \Gamma$ such that conditions (ii-1) and (ii-2) are satisfied for t_0 with $\chi = \chi_\gamma$. Condition (ii-1) is that there exists $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ with $\widetilde{g}^{\chi\varphi}(x_0) = t_0$. As k is ample and $\widetilde{Z}^{\chi\varphi}$ is a smooth k-curve, there are infinitely many k-rational points x on $\widetilde{Z}^{\chi\varphi}$. The corresponding points $t = \widetilde{g}^{\chi\varphi}(x) \in B(k)$, excluding the branch points, satisfy conditions (ii-1) and (ii-2) from lemma 3.4. Implication (ii) $\Rightarrow$ (i) of this lemma finishes the proof. Q.E.D.

Remark 4.7. The proof and the result generalize to higher dimensional covers $f : X \to B$. It should be assumed however that the covering space Z^{sep} of the cover $Z^{\mathrm{sep}} \to B \otimes_k k^{\mathrm{sep}}$ corresponding to the field extension $k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B)$ is smooth (Z^{sep} is the normalization of B in the field $k^{\mathrm{sep}}(Z)$ (defined in §2.2) and so is *a priori* only normal). The ampleness of k then provides a Zariski-dense subset of k-rational points on $\widetilde{Z}^{\chi\varphi}$ and the conclusion becomes that there exists a Zariski-dense subset $\mathcal{B} \subset B(k) \setminus D$ such that the specialization algebra $\prod_l k(X)_{t,l}/k$ at each $t \in \mathcal{B}$ equals $\prod_l k(X)_{t_0,l}/k$.

References

[BS09] Lior Bary-Soroker. Dirichlet's theorem for polynomial rings. *Proc. Amer. Math. Soc.*, 137:73–83, 2009.

[BS10] Lior Bary-Soroker. Irreducible values of polynomials. *manuscript*, 2010.

[Cho66] Sarvadavan Chowla. A note on the construction of finite Galois fields $GF(p^n)$. *J. Math. Anal. Appl.*, 15:53–54, 1966.

[Coh70] Stephan D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.

[DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers: field of moduli versus field of definition. *Annales Sci. E.N.S.*, 30:303–338, 1997.

[Dèb99a] Pierre Dèbes. Galois covers with prescribed fibers: the Beckmann-Black problem. *Ann. Scuola Norm. Sup. Pisa,* Cl. Sci. (4), 28:273–286, 1999.

[Dèb99b] Pierre Dèbes. Some arithmetic properties of algebraic covers. In *Aspects of Galois Theory*, volume 256 of *London Math. Soc. Lecture Note Series*, pages 66–84. Cambridge University Press, 1999.

[Dèb09] Pierre Dèbes. Arithmétique des revêtements de la droite. 2009. at http://math.univ-lille1.fr/~pde/ens.html.

[DG11a] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *Ann. Inst. Fourier*, 61, 2011.

[DG11b] Pierre Dèbes and Nour Ghazi. Specializations of Galois covers of the line. In *Alexandru Myller Mathematical Seminar, Proceedings of the Centennial Conference*, volume 1329 of *American Institute of Physics*, pages 98–108. V. Barbu and O. Carja, Eds, 2011.

[DL] Pierre Dèbes and François Legrand. Specialization results in Galois theory. *Trans. A.M.S.* (to appear).

[Eke90] Torsten Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988/1989*, volume 91 of *Progress in Mathematics*, pages 241–248. Birkhäuser, 1990.

[FJ04] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2004. (first edition 1986).

[Fri74] Michael D. Fried. On Hilbert's irreducibility theorem. *J. Number Theory*, 6:211–231, 1974.

[Ree71] Rumhak Ree. Proof of a conjecture of S. Chowla. *J. Number Theory*, 3:210–212, 1971.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics. Jones and Bartlett Publishers, 1992.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés algébriques qui s'en déduisent*. Hermann, Paris, 1948.

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France
E-mail address: Pierre.Debes@math.univ-lille1.fr
E-mail address: Francois.Legrand@math.univ-lille1.fr