PIERRE DÈBES

Galois covers with prescribed fibers : the Beckmann-Black problem

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 28, nº 2 (1999), p. 273-286.

<http://www.numdam.org/item?id=ASNSP_1999_4_28_2_273_0>

Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)
Vol. XXVIII (1999), pp. 273-286

Galois Covers with Prescribed Fibers: the Beckmann-Black Problem

PIERRE DÈBES

Abstract. The Beckmann-Black problem asks whether every Galois extension E/K is the specialization of a Galois branched cover of $\mathbb{P}^1$ defined over K with the same Galois group. E. Black conjectures this is indeed always possible. We give three results about this conjecture. The first one is that it implies the Regular Inverse Galois Problem. The second one considers a "mere" form of the problem which requires that the realizing Galois cover be defined over K only as mere cover (i.e., without the Galois action). This mere form is shown to hold if K contains an ample field, e.g. K contains a complete valued field. Our last result is a proof of the original Beckmann-Black condition in the case K is a PAC field.

Mathematics Subject Classification (1991): 12F12 (primary), 12E25, 14H30, 11Gxx (secondary).

Introduction

This paper is devoted to the problem of realizing groups as Galois groups over $K(T)$ with the extra constraint that the specialization at some point is given in advance. A typical result is the following.

THEOREM (Theorem 3.1). *Let K be a field containing a complete valued field (e.g. $K \supset \mathbb{Q}_p$, $K \supset \kappa((x))$). Then given a finite group G and a Galois extension E/K of group G, there exists an absolutely irreducible polynomial $P(T, Y) \in K[T, Y]$ such that*

(i) *the field $\overline{K}(T)[Y]/(P(T, Y))$ is a Galois extension of $\overline{K}(T)$ of group G, and*
(ii) *the splitting field over K of the polynomial $P(0, Y)$ is the extension E/K.*

The proof uses previous arithmetic structure results of ours on the set of models of a given cover of the line [De3]; the main idea consists in twisting covers (Section 2). Theorem 3.1 is actually proved in the more general case K contains an *ample* field k. Recall a field k is called ample if every smooth k-curve has infinitely many k-rational points provided there is at least one

Pervenuto alla Redazione il 15 maggio 1998 e in forma definitiva il 8 febbraio 1999.

(e.g. [DeDes]). Complete valued fields are ample. From results of Pop [Po; Appendix I] (who also introduced the notion of ample fields), the fields $\mathbb{Q}^{\mathrm{tr}}$ and $\mathbb{Q}^{\mathrm{tp}}$ of all totally real, and respectively totally p-adic algebraic numbers are other typical ample fields. P(seudo) A(lgebraically) C(losed) fields are ample too: by definition, over a PAC field, every curve has at least one (in fact infinitely many) K-rational points [FrJa; Chapt. 10]. Thus the conclusion of Theorem 3.1 also holds for PAC fields. In fact, a stronger conclusion holds for PAC fields (Theorem 3.2): one may require that (i) holds over K itself (and not only over $\overline{K}$), that is, that the field $K(T)[Y]/(P(T,Y))$ is a Galois extension of $K(T)$ of group G. We note (Remark 3.3) that an argument for the PAC case is more or less implicit in the proof of a related result from [FrVo].

This solves the so-called Beckmann-Black problem for PAC fields. In more geometric terms, the question, originally stated by S. Beckmann [Be] (over $K=\mathbb{Q}$), is whether, given a field K and a group G, the following arithmetic lifting property holds: every finite Galois extension E/K of group G is the specialization of a G-cover of $\mathbb{P}^1$ defined over K (the prefix "G" in "G-cover" indicates that the Galois action is part of the data; see [DeDo] for a precise definition). S. Beckmann proved the lifting property when G is an abelian group or a symmetric group (over number fields). The problem has also been investigated by E. Black who introduced a cohomological method. She obtained that over a hilbertian field K, a semi-direct product of a finite cyclic group A with a group H having the lifting property also has the lifting property if $(|H|,|A|)=1$ and (char(K), $|A|)=1$ [Bl3]. That includes the case of abelian groups and provides new examples of groups with the lifting property over arbitrary fields, e.g.the dihedral groups D_n of order $2n$ when n is odd ([Bl1], see also [Bl3] for a detailed account of the problem). She conjectures that the lifting property holds unconditionally, i.e., for every group G and over every field K [Bl3]. Our initial statements rephrase as follows. Theorem 3.2 shows the Black conjecture holds over PAC fields, i.e., that over these fields, the arithmetic lifting property holds for all groups G[(1)]. Theorem 3.1 is that over fields containing an ample field, a slightly weaker form of the lifting property, called the *mere* form, holds. Namely, this mere form requires that the realizing cover be defined over K only as *mere* cover (that is, without the Galois action) and be Galois over $\overline{K}$.

E. Black also established some connections between the arithmetic lifting property and other classical Galois realization properties of groups. For example she showed that if a group G has a generic extension over K (e.g. if G satisfies the classical Noether's problem [Sa]), then G has the lifting property over K [Bl2]. In Section 1 we show one further connection, namely that the arithmetic lifting property for all groups and fields (i.e., the Black conjecture) implies the Regular Inverse Galois Problem (Proposition 1.2) (we note this

[(1)]Note that unlike algebraically closed fields which have no non-trivial algebraic extensions (and so for which the Beckmann-Black problem is trivial), PAC fields may have many fields extensions: in fact, each finite group is a Galois group over PAC hilbertian fields K (like the field $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$); more precisely, the absolute Galois group $G(K)$ of such fields is pro-free of infinite rank.

was observed independently by A. Tamagawa). This suggests that the whole Black conjecture, though plausible, is probably out of reach at the moment. The Regular Inverse Galois Problem is known to hold over ample fields (and so over PAC fields too). Solving the original Beckmann-Black problem over ample fields (and not the just the mere form as here) would be quite interesting.

ACKNOWLEDGEMENTS. The author wishes to thank E. Black, M. Emsalem and F. Pop for mathematical discussions and valuable comments.

1. – Beckmann-Black and the regular inverse Galois problem

1.1. – The conjectures

Throughout the paper the Galois group of a Galois extension E/k is denoted by $\mathrm{G}(E/k)$. Given a field K, we denote by K_s [resp. by $\overline{K}$] a separable [resp. algebraic] closure of K and by $\mathrm{G}(K)$ the absolute Galois group $\mathrm{G}(K) = \mathrm{G}(K_s/K)$ of K. Recall a field extension E/K is *regular* if E/K is separable and $E \cap \overline{K} = K$. As usual, we sometimes shorten the phrase "Galois extension $E/K(T)$ with E/K regular" to just say "regular Galois extension $E/K(T)$"; for such extensions, we have $\mathrm{G}(E/K(T)) = \mathrm{G}(E\overline{K}/\overline{K}(T))$ (which is in fact equivalent to the regularity condition). By cover of $\mathbb{P}^1$ we always mean a smooth projective model (of the associated function field extension). We use the phrase "G-cover" for Galois covers given with their automorphisms; non-necessarily Galois covers given without their automorphisms are referred to as *mere* covers.

Given a degree d mere cover $f_K : X_K \to \mathbb{P}^1$ defined over K and an unramified K-rational point $t_0 \in \mathbb{P}^1(K)$, denote the compositum of all fields of definition over K of points in the fiber $f_K^{-1}(t_0)$ by K_{f_K,t_0}; equivalently, K_{f_K,t_0} is the compositum of all residue fields at t_0 of the Galois closure of the extension $K(X_K)/K(T)$. We call the field K_{f_K,t_0} the *splitting field* or the *specialization* of f_K at t_0. With this notation, the Beckmann-Black arithmetic lifting condition can be reformulated as follows. We distinguish a G-form (the original one) and a mere form. The former, which is conjectured to hold for all fields K and groups G by E. Black, implies the latter.

BECKMANN-BLACK ARITHMETIC LIFTING CONDITION. Let K be a field, G be a finite group and E/K be a Galois extension of group G.

G-form (*G*-**BB**): There exists a G-cover $f : X_K \to \mathbb{P}^1$ of group G defined over K and some unramified point $t_0 \in \mathbb{P}^1(K)$ such that the splitting field extension $K_{f_K,t_0}/K$ of f_K at t_0 is K-isomorphic to E/K.

Mere form (*mere* **BB**): There exists a mere cover $f_K : X \to \mathbb{P}^1$ over K, Galois of group G over $\overline{K}$, and some unramified point $t_0 \in \mathbb{P}^1(K)$ such that the splitting field extension $K_{f_K,t_0}/K$ of f_K at t_0 is K-isomorphic to E/K.

The following conjecture is the central problem of Inverse Galois Theory.

Regular Inverse Galois Problem (**RIGP**). Given a field K and a finite group G, there exists a Galois extension $E/K(T)$ with E/K regular such that $\mathrm{G}(E/K(T)) = G$; or, equivalently, there exists a G-cover $f : X \to \mathbb{P}^1$ of group G defined over K.

Remark 1.1. (a) A G-form and a mere form of the **RIGP** could also be distinguished. The mere form would be: given a field K, each finite group G is the Galois group of a Galois cover defined over K as mere cover (but not necessarily Galois over K). To my knowledge, this mere form is not known to hold over more fields than the classical form (which would be the G-form of the **RIGP**).

(b) Given a field K and a group G, G-**BB** for G and $K(x)$ (with x transcendental over K) implies G-**BB** for G and K: this follows from Bertini's theorem. The converse is unclear. So are the analogous questions for algebraic extensions.

1.2. – G-BB implies RIGP

Proposition 1.2. *The Beckmann-Black lifting condition implies the Regular Inverse Galois Problem. More precisely, given a group G and a field K, G-***BB** *for G and over every regular extension of K implies* **RIGP** *over K. In particular, G-***BB** *for G and over every field of characteristic* 0 *implies* **RIGP** *over* $\mathbb{Q}$.

Proof. Suppose given a group G and a field K and assume that G-**BB** holds for G over every regular extension of K. Regard G, *via* its regular representation, as a subgroup of the symmetric group S_d (with $d = |G|$). Set $E = K(\mathbf{T})$ where $\mathbf{T} = \{T_1, \dots, T_d\}$ and let G act on E *via* its action on $\{T_1, \dots, T_d\}$. The fixed field E^G is a regular extension of K, hence the function field $K(B)$ of a d-dimensional K-variety B, which by construction is unirational.

We will now use the G-**BB** lifting property to construct a Galois extension $E'/K(B)$ of group G with E'/K regular and such that the extensions $\overline{K}E'/\overline{K}(B)$ and $\overline{K}E/\overline{K}(B)$ are linearly disjoint. The following diagram summarizes the argument.

$$\begin{tikzcd}
E \arrow[d, dash, "G"'] & E_T \arrow[l, "T=0"'] \arrow[r, dash] \arrow[d, dash, "G"'] & \overline{K}E_T \arrow[r, "T=t"] \arrow[d, dash, "G"'] & \overline{K}E_t \arrow[d, dash, "G"'] & \text{lin. disj.} \\
K(B) & K(B)(T) \arrow[r, dash] & \overline{K}(B)(T) & \overline{K}(B) \arrow[r, dash, "G"] & \overline{K}E
\end{tikzcd}$$

More specifically, from G-**BB**, there exists a Galois extension $E_T/K(B)(T)$ of group G with $E_T/K(B)$ regular which specializes to $E/K(B)$ at $T = 0$. Apply then the hilbertian property to the hilbertian field $\overline{K}(B)$ ($\dim(B) > 0$)): there exists $t \in K(B)^{(2)}$ such that the specialized extension $\overline{K}E_t/\overline{K}(B)$ is Galois of group G and is linearly disjoint from the extension $\overline{K}E/\overline{K}(B)$. Set $E' = E_t$; the extension $E'/K(B)$ has the required properties: in particular, the regularity of the extension E'/K follows from

$$G = \mathrm{G}\big(E_T/K(B)(T)\big) \supset \mathrm{G}\big(E_t/K(B)\big) \supset \mathrm{G}\big(\overline{K}E_t/\overline{K}(B)\big) = G\,.$$

The following lemma shows that $E'E$ is a Galois extension of $E = K(\mathbf{T})$ of group G and is regular over K. To complete the proof, we note that regular realization over $K(\mathbf{T})$ is equivalent to regular realization over $K(T)$. □

LEMMA 1.3. *Let $E/K(B)$ and $E'/K(B)$ be two finite extensions with both E/K and E'/K regular. Assume that $E'/K(B)$ is Galois of group G. Assume further that the extensions $\overline{K}E'/\overline{K}(B)$ and $\overline{K}E/\overline{K}(B)$ are linearly disjoint over $\overline{K}(B)$. Then $E'E/E$ is a Galois extension of group G and is regular over K.*

PROOF. Consider the diagrams

$$\begin{tikzcd}[arrows=dash]
E \arrow[r] \arrow[d] & E'E \arrow[d] \\
K(B) \arrow[r, "G"'] & E'
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
\overline{K}E \arrow[r] \arrow[d] & \overline{K}E'E \arrow[d] \\
\overline{K}(B) \arrow[r] & \overline{K}E'
\end{tikzcd}$$

We have *a priori* $G = \mathrm{G}(E'/K(B)) \supset \mathrm{G}(E'E/E) \supset \mathrm{G}(\overline{K}E'E/\overline{K}E)$. But it follows from the linear disjointness assumption over $\overline{K}$ and the regularity of the extension E'/K that $\mathrm{G}(\overline{K}E'E/\overline{K}E) = \mathrm{G}(\overline{K}E'/\overline{K}(B)) = \mathrm{G}(E'/K(B)) = G$. Conclude that $\mathrm{G}(E'E/E) = \mathrm{G}(\overline{K}E'E/\overline{K}E) = G$. □

1.3. – The linear disjoint realization condition

The G-**BB** condition was used in the proof of Proposition 1.2 to show that the unirational K-variety B has the following Linear Disjoint Realization property:

(**LDR**) Given a Galois extension $E/K(B)$ of group G with E/K regular, there exists a Galois extension $E'/K(B)$ of group G with E'/K regular and such that the extensions $\overline{K}E'/\overline{K}(B)$ and $\overline{K}E/\overline{K}(B)$ are linearly disjoint.

Lemma 1.3 actually shows that **LDR** (for all K-varieties B of dimension > 0) implies **RIGP**. Thus showing **LDR** can actually be an alternate way of using Noether's original idea to prove the inverse Galois problem. What is to be shown is that every G-cover can be somehow "deformed" into a G-cover (of the same base and with the same group) that is linearly disjoint (over $\overline{K}$). Note that if B is a rational variety (over K), then the **LDR** condition holds (use the

(2) That t can be picked in $K(B)$ follows for example from Theorem 2.2 of [De2].

argument in the proof below). Furthermore, unlike Noether's original program, this approach would yield the *regular* form of the inverse Galois problem. In fact, as we now show, for infinite fields, **LDR** (for all K-varieties) is equivalent to **RIGP**.

PROPOSITION 1.4. *Let K be an infinite field and assume the* **RIGP** *holds over K. Then every K-variety B (of dimension > 0) satisfies condition* **LDR**.

PROOF. Fix a K-variety B of dimension > 0 and a finite extension $E/K(B)$ with E/K regular. Let $\mathbf{T} = \{T_1, \dots, T_r\}$ be a transcendence basis of $K(B)$ over K. It follows from the **RIGP** over K that there exists a Galois extension $E^*/K(\mathbf{T})$ of group G with E^*/K regular: namely realize G over $K(T)$ regularly and extend $K(T)$ to $K(\mathbf{T})$. Denote the support of the ramification divisor of the extension $\overline{K}E/\overline{K}(\mathbf{T})$ [resp. the extension $\overline{K}E^*/\overline{K}(\mathbf{T})$] by $\mathrm{ram}(E)$ [resp. $\mathrm{ram}(E^*)$]. Then pick an automorphism χ of $K(\mathbf{T})$ such that the intersection $\chi^{-1}(\mathrm{ram}(E)) \cap \mathrm{ram}(E^*)$ consists only of components of codimension > 1 (this is possible since K is infinite; χ can be picked in $\mathrm{GL}_r(K)$). Denote the pull-back of the extension $E^*/K(\mathbf{T})$ along the automorphism χ by $E^*_\chi/K(\mathbf{T})$. The situation is summarized by the diagram at the end of the proof.

It follows from the construction and the purity theorem that the intersection $\overline{K}E \cap \overline{K}E^*_\chi$ is not ramified above $\overline{K}(\mathbf{T})$. Therefore $\overline{K}E \cap \overline{K}E^*_\chi = \overline{K}(\mathbf{T})$. Indeed, otherwise, $\overline{K}E \cap \overline{K}E^*_\chi$ would be a proper unramified extension of $\overline{K}(\mathbf{T})$, which canonically corresponds to a proper étale cover of $\mathbb{P}^r$. The contradiction follows since the fundamental group of $\mathbb{P}^r$ is trivial.

Conclude that the extensions $\overline{K}E^*_\chi/\overline{K}(\mathbf{T})$ and $\overline{K}E/\overline{K}(\mathbf{T})$ are linearly disjoint (the former is Galois). Set $E' = K(B)E^*_\chi$. It follows [La; Proposition 1 p. 262] that the extensions $\overline{K}E'/\overline{K}(B)$ and $\overline{K}E/\overline{K}(B)$ are linearly disjoint. The extension $E'/K(B)$ has the required properties.

$$
\begin{tikzcd}
E \arrow[d, dash] & & & \overline{K}E \arrow[d, dash] & \\
K(B) \arrow[r, dash, "G"] \arrow[d, dash] & E' = K(B)E^*_\chi \arrow[d, dash] & & \overline{K}(B) \arrow[r, dash, "G"] \arrow[d, dash] & \overline{K}E' \arrow[d, dash] \\
K(\mathbf{T}) \arrow[r, dash, "G"] \arrow[d, dash, "\chi"'] & E^*_\chi \arrow[d, dash] & & \overline{K}(\mathbf{T}) \arrow[r, dash, "G"] \arrow[d, dash, "\chi"'] & \overline{K}E^*_\chi \arrow[d, dash] \\
K(\mathbf{T}) \arrow[r, dash, "G"] & E^* & & \overline{K}(\mathbf{T}) \arrow[r, dash, "G"] & \overline{K}E^*
\end{tikzcd}
$$

□

2. – Twisting covers

This section is the technical core of the paper. In particular we explain how to twist a G-cover $f_K : X \to \mathbb{P}^1$ defined over K of group G by an homomorphism $\varphi : \mathrm{G}(K) \to G$. In order to do so we will view covers of $\mathbb{P}^1$ as representations of K-arithmetic fundamental groups; we refer to [DeDo] for more details on the dictionary between these two categories.

Denote the affine subset $\mathbb{P}^1$ with the reduced ramification divisor of f_K removed by $(\mathbb{P}^1)^*$ and the K-arithmetic fundamendal group of $(\mathbb{P}^1)^*$ by Π_K. Let $\phi_K : \Pi_K \to G$ be the representation corresponding to the G-cover f_K. The representation corresponding to the mere cover associated with f_K (by dropping the Galois action) is obtained by composing ϕ_K with the left-regular representation $\gamma : G \hookrightarrow S_d$ of G (where $d = |G|$). Identify G and $\gamma(G)$. The representation corresponding to the mere cover $f = f_K \otimes_K K_s$ is the restriction $\phi_{K_s} : \Pi_{K_s} \to G \subset S_d$ of the previous one to the K_s-fundamental group Π_{K_s} of $(\mathbb{P}^1)^*$. Each unramified K-rational point $t_0 \in (\mathbb{P}^1)^*$ provides a section $\mathrm{s}_{t_0} : \mathrm{G}(K) \to \Pi_K$ of the canonical surjection $\Pi_K \to \mathrm{G}(K)$. Recall this result from [De1].

Proposition 2.1 [De1; Proposition 2.1]. *For each $\tau \in \mathrm{G}(K)$, the element $(\phi_K \mathrm{s}_{t_0})(\tau)$ is conjugate in S_d to the action of τ on the fiber $f_K^{-1}(t_0)$. Consequently, the splitting field K_{f_K,t_0} of f_K at t_0 corresponds via Galois theory to the homomorphism $\phi_K \mathrm{s}_{t_0} : \mathrm{G}(K) \to G$; that is, it is the fixed field in K_s of* $\ker(\phi_K \mathrm{s}_{t_0})$ *and the Galois group of the extension $K_{f_K,t_0}/K$ is the image group of $\phi_K \mathrm{s}_{t_0}$. The homomorphism $\phi_K \mathrm{s}_{t_0}$ is called the arithmetic action of* $\mathrm{G}(K)$ *on the fiber $f_K^{-1}(t_0)$.*

Fix an unramified rational point $t_0 \in \mathbb{P}^1(K)$. Denote the map $\phi_K \mathrm{s}_{t_0} : \mathrm{G}(K) \to G$ by φ_0. Denote the right-regular representation of G by $\delta : G \to S_d$. Define $\varphi^* : \mathrm{G}(K) \to G$ by $\varphi^*(g) = \varphi(g)^{-1}$. Consider then the map $\tilde{\phi}_K^\varphi : \Pi_K \to S_d$ defined by

$$\begin{aligned}\tilde{\phi}_K^\varphi\big(x\mathrm{s}_{t_0}(\tau)\big) &= \phi_K\big(x\mathrm{s}_{t_0}(\tau)\big)\delta\varphi^*(\tau) \qquad \big(x \in \Pi_{K_s}, \tau \in \mathrm{G}(K)\big)\\ &= \phi_{K_s}(x)\varphi_0(\tau)\delta\varphi^*(\tau)\end{aligned}$$

The homomorphism $\delta\varphi^* \in \mathrm{Hom}(\mathrm{G}(K), \mathrm{Cen}_{S_d} G)$[3] can be viewed as a 1-cochain in $Z^1(K, \mathrm{Cen}_{S_d} G)$ (with trivial action). It follows from Proposition 2.3 of [De3] that the map $\tilde{\phi}_K^\varphi : \Pi_K \to S_d$ induces a representation of Π_K and that the associated mere cover, denoted by $\tilde{f}_K^\varphi : \tilde{X}^\varphi \to \mathbb{P}^1$, is a K-model of the mere cover f. The mere cover $\tilde{f}_K^\varphi$ is by definition the *twisted cover* of f_K by the homomorphism φ. The following statement contains the properties of the twisted cover that we will use. In the case of PAC fields, conclusion (b) corresponds to the "field crossing argument" from [FrVo; Lemma 1].

[3] Note that $\delta\varphi^*$ is an actual homomorphism because δ and φ^* are both anti-isomorphisms.

PROPOSITION 2.2. *The twisted cover* $\tilde{f}_K^{\varphi} : \tilde{X}^{\varphi} \to \mathbb{P}^1$ *has the following properties:*

(a) *The arithmetic action of* $\mathrm{G}(K)$ *on the fiber* $(\tilde{f}_K^{\varphi})^{-1}(t_0)$ *is the map* $\varphi_0 \cdot \delta\varphi^* : \mathrm{G}(K) \twoheadrightarrow G\mathrm{Cen}_{S_d} G$ *(by "*$\varphi_0 \cdot \delta\varphi^*$*" we mean the product map of* φ_0 *and* $\delta\varphi^*$*).*

(b) *Let* $x_1 \in \tilde{X}^{\varphi}(K)$ *be an unramified* K*-rational point. Set* $t_1 = \tilde{f}_K^{\varphi}(x_1)$*. Then the arithmetic action of* $\mathrm{G}(K)$ *on the fiber* $f_K^{-1}(t_1)$ *in the original cover* f_K *is conjugate in* G *to* $\varphi : \mathrm{G}(K) \to G$*.*

(c) *Let* $t_1 \in \mathbf{P}^1(K)$ *not a branch point. Denote the map* $\phi_K \, \mathrm{s}_{t_1} : \mathrm{G}(K) \to G$ *by* φ_1 *(the arithmetic action of* $\mathrm{G}(K)$ *on the fiber* $f_K^{-1}(t_1)$*). Then there is a* K*-rational point on the twisted cover* $\tilde{f}_K^{\varphi_1} : \tilde{X}^{\varphi_1} \to \mathbb{P}^1$ *above* t_1*.*

PROOF. (a) immediately follows from the definition of $\tilde{f}_K^{\varphi}$.

(b) Consider the sections s_{t_0} and s_{t_1} (from $\mathrm{G}(K)$ to Π_K). From Proposition 2.1, for each $\tau \in \mathrm{G}(K)$, the action of τ on the fiber $(\tilde{f}_K^{\varphi})^{-1}(t_1)$ is given by

$$\tilde{\phi}_K^{\varphi}\left(\mathrm{s}_{t_1}(\tau)\right) = \phi_K\left(\mathrm{s}_{t_1}(\tau)\right) \delta\varphi^*(\tau)$$

In S_d the element $\phi_K(\mathrm{s}_{t_1}(\tau)) \in G$ should really be viewed as the multiplication on the left by $\phi_K(\mathrm{s}_{t_1}(\tau))$ in G while the element $\delta\varphi^*(\tau)$ is the multiplication on the right by $\varphi(\tau)^{-1}$. By assumption, the elements $\tilde{\phi}_K^{\varphi}(\mathrm{s}_{t_1}(\tau))$ ($\tau \in \mathrm{G}(K)$) have a common fixed point, say $\omega \in G$. It follows that

$$\phi_K\left(\mathrm{s}_{t_1}(\tau)\right) = \omega\varphi(\tau)\omega^{-1}$$

(c) By definition, we have $\tilde{\phi}_K^{\varphi_1}(xs_{t_0}(\tau)) = \phi_K(xs_{t_0}(\tau))\,\delta\varphi_1^*(\tau)$ where $\varphi_1^*(\tau) = \varphi_1(\tau)^{-1}$. Whence

$$\begin{aligned}\tilde{\phi}_K^{\varphi_1}\left(s_{t_1}(\tau)\right) &= \phi_K\left(s_{t_1}(\tau)\right) \delta\varphi_1^*(\tau)\\ &= \varphi_1(\tau)\delta\varphi_1^*(\tau)\end{aligned}$$

That is, for each $\tau \in \mathrm{G}(K)$, $\tilde{\phi}_K^{\varphi_1}(s_{t_1}(\tau))$ is the conjugation by $\varphi_1(\tau)$ and so fixes 1. The corresponding point above t_1 is K-rational. □

3. – The Beckmann-Black problem over large fields

3.1. – The mere Beckmann-Black problem over ample fields

The following result is the goal of this section. A special case is the theorem stated in the introduction.

THEOREM 3.1. *The mere form of the Beckmann-Black lifting property (mere* **BB***) holds if* K *contains an ample field. That is, given a group* G*, each Galois extension* E/K *is the splitting field extension at some unramified point* $t_0 \in \mathbb{P}^1(K)$ *of some mere cover* $Y \to \mathbb{P}^1$ *defined over* K *and Galois over* $\overline{K}$ *of group* G*.*

PROOF. Let k be an ample field contained in K. The first stage uses the Regular Inverse Galois Problem over k. More specifically there exists a G-cover $f_k : X \to \mathbb{P}^1$ of group G defined over k; furthermore, the cover f_k can be required to have a totally k-rational fiber above some unramified point $t_0 \in \mathbb{P}^1(k)$ (that is, the fiber $f_k^{-1}(t_0)$ consists only of k-rational points on X). This result over ample fields is due to F. Pop [Po] in its final form. It had first been proved in the case k is a complete valued field by D. Harbater [Har], and in other various special cases (e.g. [DeFr], [De1]; see [DeDes] for a complete bibliography). The condition that the realizing cover has a totally k-rational unramified fiber is not explicitly stated in [Har] and [Po] but can be deduced from the proofs. For more details concerning this point see [De1] and [Li] for the complete valued field case and [DeDes; Section 4.2] for the general case of an ample field.

Consider then the G-cover f_K obtained from f_k by extension of scalars from k to K. Properties of f_k carry over to f_K over K, that is, f_K is a G-cover of group G defined over K and has a totally K-rational fiber above t_0.

The last stage uses Proposition 2.2. Let $\varphi : \mathrm{G}(K) \to G$ be a surjective homomorphism that corresponds to the given extension E/K (i.e., $\overline{K}^{\ker(\varphi)} = E$). By construction, the arithmetic action on the fiber above t_0 in the cover f_K is trivial. Consider the mere cover $\tilde{f}_K^{\varphi} : \tilde{X}^{\varphi} \to \mathbb{P}^1$ obtained from f_K by twisting by φ. From Proposition 2.2 (a), the arithmetic action of $\mathrm{G}(K)$ on the fiber $(\tilde{f}_K^{\varphi})^{-1}(t_0)$ is the map $\delta\varphi^* : \mathrm{G}(K) \twoheadrightarrow G\mathrm{Cen}_{S_d}G$. This map has the same kernel as φ. Conclude that the splitting field extension $K_{\tilde{f}_K,t_0}$ of $\tilde{f}_K^{\varphi}$ at t_0 is K-isomorphic to the extension E/K; the cover $\tilde{f}_K^{\varphi} : \tilde{X}^{\varphi} \to \mathbb{P}^1$ is the desired cover $Y \to \mathbb{P}^1$ of the statement. □

3.2. – Related comments

3.2.1. – Pointed RIGP

The proof shows more generally that the mere form of the Beckmann-Black lifting property holds over every field K for which a certain "pointed" form of the Regular Inverse Galois Problem holds. This pointed form requires that each group G be realized as the automorphism group of a G-cover $f : X \to \mathbb{P}^1$ of group G defined over K and with the additional property that there is an unramified totally K-rational fiber, or equivalently, that X has an unramified K-rational point. To my knowledge, no field is known for which the **RIGP** is known to hold but not the pointed **RIGP**. In fact no field is known for which the **RIGP** is known to hold and which does not contain an ample field (in which case the pointed **RIGP** holds). Producing examples of such fields seems to be a difficult question, firstly, because, such fields may not exist (if the **RIGP** only held over fields containing ample fields), secondly, because, it happens to be difficult to produce non-ample fields at all (at least inside $\overline{\mathbb{Q}}$ and apart from number fields). There is a natural candidate for that question though: the field $\mathbb{Q}^{ab}$; but that the **RIGP** holds over $\mathbb{Q}^{ab}$ and that $\mathbb{Q}^{ab}$ is not ample are both still open conjectures.

Incidentally we note that, even for number fields, the existing arguments that they are not ample are not elementary: one uses Faltings's theorem and another uses Merel's result on rational points on modular curves [Me]. In fact a natural way to prove that no number field is ample is to find a curve C defined over $\mathbb{Q}$ such that $C(K)$ is finite for all number fields K (and $C(\mathbb{Q}) \neq \emptyset$). That is, to prove Mordell's conjecture for one curve over all number fields. However some works of Szpiro and Moret-Bailly [Mo] show that, for some effective version of it, the Mordell conjecture for a single curve implies the *abc* conjecture and therefore, by a result of Elkies [El], the Mordell conjecture for all curves. We finally mention that an example of an infinite algebraic extension of $\mathbb{Q}$ that is not ample was communicated to us by P. Corvaja; his construction is not elementary either since it uses the Lang conjecture about rational points on subvarieties of abelian varieties, also proved by Faltings (and which implies the Mordell conjecture). It is unclear whether the **RIGP** holds over this field.

3.2.2. – G-BB for abelian extensions

The strategy of Theorem 3.1 can also be used to prove the G-form of the **BB** lifting property for abelian groups G over an arbitrary field K. This shows in particular that the G-form of the **BB** condition holds if K is a finite field. The argument was already developed in [De3]. We give below a brief sketch of the proof.

The first step is to realize the given abelian group G as the Galois group of a G-cover $f_K^o : X \to \mathbb{P}^1$ over K with at least one unramified point $t_0 \in \mathbb{P}^1(K)$. Then, just as above, it is possible to "twist" the G-cover f_K^o by any element of $\mathrm{Hom}(\mathrm{G}(K), \mathrm{Cen}_{S_d}(G))$, which, since G is abelian, equals $\mathrm{Hom}(\mathrm{G}(K), G)$. The resulting cover is still defined over K as G-cover and the splitting field extension at t_0 can be any Galois extension of group G given in advance. The G-**BB** lifting property clearly follows. As to the required preliminary regular realization of G, it is a classical result except possibly for the existence of at least one unramified point $t_0 \in \mathbb{P}^1(K)$. Obviously this is a difficulty only when K is a finite field, and more particularly, when the characteristic divides the order of G. For this technical point we refer to [De4].

3.3. – The case of PAC fields

3.3.1. – The Beckmann-Black problem over PAC fields

Over PAC fields, the original Beckmann-Black problem can be solved.

THEOREM 3.2. *The G-form of the Beckmann-Black lifting property* (*G*-**BB**) *holds if K is a PAC field. That is, given a group G, each Galois extension E/K of group G is the splitting field extension at some unramified point $t_0 \in \mathbb{P}^1(K)$ of some G-cover $Y \to \mathbb{P}^1$ of group G defined over K.*

PROOF. PAC fields are ample. So as in the proof of Theorem 3.1, we can realize G as the automorphism group of G-cover $f_K : X \to \mathbb{P}^1$ of group G defined over K. The extra condition about the existence of a totally K-rational fiber will not be needed here. Also we fix an unramified K-rational point t_0, we let $\varphi : \mathrm{G}(K) \to G$ be a surjective homomorphism that corresponds to the given extension E/K and consider the mere cover $\tilde{f}_K^{\varphi} : \tilde{X}^{\varphi} \to \mathbb{P}^1$ obtained from f by twisting by φ. Since the field K is PAC, the curve $\tilde{X}^{\varphi}$ has infinitely many K-rational points. Let x_1 be one of them that is unramified and set $t_1 = \tilde{f}_K^{\varphi}(x_1)$. From Proposition 2.2 (b), the arithmetic action of $\mathrm{G}(K)$ on the fiber $f_K^{-1}(t_1)$ in the original cover f_K is conjugate in G to $\varphi : \mathrm{G}(K) \to G$. Consequently, the specialization of f_K at t_0 is the field extension E/K. □

REMARK 3.3. The proof shows more generally that if K is PAC

(*) *any given G-cover $f_K : X \to \mathbb{P}^1$ of group G defined over K has the property that every Galois extension E/K of group G is the specialization of f_K at infinitely many unramified points $t \in \mathbb{P}^1(K)$.*

This specialization property actually implicitly appears in the proof of Theorem B of [FrVo] as a consequence of the field crossing argument, which, as we said earlier, corresponds to Proposition 2.2 (b) in the context of PAC fields. Fried and Völklein work over fields of characteristic 0 but this part of their argument remains valid in arbitrary characteristic. Thus [FrVo] implicitly contains a solution to the Beckmann-Black problem for PAC fields.

3.3.2. – Some specialization properties

The specialization property (*) is used in [FrVo] to show that, given a PAC field K, the following assertions are equivalent:

(i) Each group is a Galois group over K,

(ii) Each G-cover $f_K : X \to \mathbb{P}^1$ defined over K can be specialized to a Galois extension E/K with the same Galois group.

Fried and Völklein call *RG-hilbertian* a field satisfying condition (ii). They also produce an example of a non-hilbertian RG-hilbertian field; other examples are given in [DeHa].

Using Proposition 2.2 (b) (instead of the field crossing argument) leads to the following characterization of RG-hilbertian fields. Let K be an arbitrary field, i.e., we drop the assumption "K PAC" of [FrVo]. Given a group G and a G-cover $f_K : X \to \mathbb{P}^1$ defined over K of group G, consider the collection of all twisted covers $\tilde{f}_K^{\varphi} : \tilde{X}^{\varphi} \to \mathbb{P}^1$ where φ is any surjective homomorphism $\mathrm{G}_K \to G$. Denote then the disjoint union of all curves $\tilde{X}^{\varphi}$ by $\mathcal{X}_{f_K}$.

PROPOSITION 3.4. *The field K is RG-hilbertian if*

(**) *for each G-cover $f_K : X \to \mathbb{P}^1$ defined over K, the set $\mathcal{X}_{f_K}$ contains infinitely many K-rational points.*

Furthermore, if the **RIGP** *is known to hold over K, then the converse holds as well.*

Note that condition (i) above — each group is a Galois group over K — is implicitly contained in (**) since it assures that $\mathcal{X}_{f_K}$ is not the empty set. Thus there are two aspects in the characterization of RG-hilbertian fields given in Proposition 3.4: condition (i) is the Galois-theoretic part and the rest of condition (**) is a pure diophantine condition (in that it only consists in solving polynomial equations). Proposition 3.4 follows straightforwardly from Propostion 2.2 (b) and (c): these indeed assert that K-rational points on some twisted curve $\tilde{X}^{\varphi}$ exactly correspond to specializations of the cover f_K of Galois group G.

Condition (*), which is satisfied by PAC fields, is stronger than condition (**) since then *each* of the twisted curves $\tilde{X}^{\varphi}$ contains infinitely many rational points. We end this paper by some further observations on these two conditions. We note in particular (Section 3.3.3 and Section 3.3.4) that the stronger condition (*) does not hold in general over ample fields and so the proof of the Beckmann-Black lifting property for PAC fields does not carry over, as it stands, to the more general case of ample fields. Ample fields however satisfy the following specialization property, which readily follows from Proposition 2.2 and the definition of ample fields. This was first observed by M. Fried in the special case $K = \mathbb{Q}^{\mathrm{tr}}$.

(***) *any G-cover $f_K : X \to \mathbb{P}^1$ of group G defined over K has the property that if a Galois extension E/K of group G is the specialization of f_K at some unramified point $t \in \mathbb{P}^1(K)$, then it is the specialization of f_K at infinitely many unramified points $t \in \mathbb{P}^1(K)$.*

3.3.3. – The local field case

Take $K = \mathbb{R}$ and consider the G-cover $f_{\mathbb{R}}$ of group $\mathbb{Z}/2$ associated with the extension $\mathbb{R}(T, \sqrt{1+T^2})/\mathbb{R}(T)$. Clearly the extension $\mathbb{C}/\mathbb{R}$ is not a specialization of $f_{\mathbb{R}}$. There are similar examples over $\mathbb{Q}_p$. Consider the G-cover $f_{\mathbb{Q}_p}$ of group $\mathbb{Z}/2$ associated with the extension $\mathbb{R}(T, y)/\mathbb{R}(T)$ where $y^2 - y - \frac{pT}{T^2-p} = 0$. It is straightforwardly checked that for each $t \in \mathbb{Q}_p$, $t/(t^2 - p) \in \mathbb{Z}_p$; hence the polynomial $Y^2 - Y - \frac{pt}{t^2-p}$ reduces modulo p to $Y^2 - Y$. Conclude from Hensel's lemma that for each $t \in \mathbb{Q}_p$, $Y^2 - Y - \frac{pt}{t^2-p}$ is totally split over $\mathbb{Q}_p$. Thus no degree 2 extension of $\mathbb{Q}_p$ is a specialization of $f_{\mathbb{Q}_p}$.

3.3.4. – Using an argument of Saltman [Sa; Section 5]

Denote the cyclic group of order 8 by C_8. This example shows that the unique unramified extension $L_2/\mathbb{Q}_2$ of group C_8 is the specialization of no G-cover $f_{\mathbb{Q}_2} : X \to \mathbb{P}^1$ over $\mathbb{Q}_2$ with group C_8 and that is definable over $\mathbb{Q}$. Indeed let $f_{\mathbb{Q}}$ be a G-cover defined over $\mathbb{Q}$ of group C_8 and let $f_{\mathbb{Q}_2} = f_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_2$. Assume that $L_2/\mathbb{Q}_2$ is the specialization of $f_{\mathbb{Q}_2}$ at some unramified point $t \in \mathbb{P}^1(\mathbb{Q}_2)$. From Krasner's lemma, there exists $t_1 \in \mathbb{P}^1(\mathbb{Q})$ with the same property. But then the specialization of $f_{\mathbb{Q}}$ at t_1 is a Galois extension of $\mathbb{Q}$ of group C_8 and it remains Galois of group C_8 after extension of scalars to $\mathbb{Q}_2$. This contradicts Wang's counter-example to the Grunwald theorem. Equivalently, this example shows that there is no $\mathbb{Q}_2$-rational point on any of the covers $\tilde{f}^{\varphi}_{\mathbb{Q}_2} : \tilde{X} \to \mathbb{P}^1$ obtained by twisting $f_{\mathbb{Q}_2}$ by a surjective homomorphism $\varphi : \mathrm{G}(\mathbb{Q}_2) \to C_8$ of kernel $\mathrm{G}(L_2)$.

3.3.5. – The number field case

Assume K is a number field and that the G-cover f_K (of group G) is of genus ≥ 2. Then from Faltings's theorem, a given Galois extension F/K of group G is the specialization of f_K at at most finitely many points $t \in \mathbb{P}^1(K)$. Furthermore, there may be no points at all. For example take the cover $f_{\mathbb{Q}}$ associated with the extension $\mathbb{Q}(T, \sqrt{1+T^2})/\mathbb{Q}(T)$. The specializations of $f_{\mathbb{Q}}$ are only ramified at primes $p \equiv 1$ modulo 4. Therefore an extension $E/\mathbb{Q}$ ramified for example at 7 cannot be a specialization of $f_{\mathbb{Q}}$.

REFERENCES

[Be] S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering?*, J. Algebra **164** (1994), 430-451.

[Bl1] E. Black, *Arithmetic lifting of dihedral extensions*, J. Algebra **203** (1998), 12-29.

[Bl2] E. Black, *Deformation of dihedral 2-group extensions of fields*, Trans. Amer. Math. Soc. (to appear).

[Bl3] E. Black, *On semidirect products and arithmetic lifting property*, J. London Math. Soc. (to appear).

[De1] P. Dèbes, *Covers of $\mathbb{P}^1$ over the p-adics*, Contemporary Math. **186** (1995), 217-238.

[De2] P. Dèbes, *Density results for Hilbert subsets*, Indian J. Pure Appl. Math. (to appear).

[De3] P. Dèbes, *Some arithmetic properties of algebraic covers*, In: "Aspects of Galois Theory", Cambridge University Press, (to appear).

[De4] P. Dèbes, *Regular realization of abelian groups with controlled ramification*, Contemporary Math., Volume of the Finite Field conference in Seattle, Summer 1997 (to appear).

[DeDes] P. Dèbes – B. Deschamps, *The inverse Galois problem over large fields*, In "Geometric Galois Action", London Math. Soc. Lecture Note Series, Cambridge University Press, (1997), 119-138.

[DeDo] P. Dèbes – J-C. Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. **30** (1997), 303-338.

[DeFr] P. Dèbes – M. Fried, *Non rigid situations in constructive Galois Theory*, Pacific J. Math. **163** (1994), 81-122.

[DeHa] P. Dèbes – D. Haran, *Almost hilbertian fields*, Acta Arithmetica (to appear).

[El] N. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices **7** (1991), 99-109.

[FrJa] M. Fried – M. Jarden, "Field Arithmetic", Springer-Verlag, 1986.

[FrVo] M. FRIED – H. VÖLKLEIN, *The embedding problem over a Hilbertian PAC-field*, Ann. Math. **135** (1992), 469-481.

[Har] D. HARBATER, "Galois covering of the arithmetic line", Lecture Notes in Math. 1240 (1987), 165-195.

[La] S. LANG, "Algebra", Addison-Wesley, 1965.

[Li] Q. LIU, *Tout groupe fini est groupe de Galois sur* $\mathbb{Q}_p(T)$, Contemporary Math. **186** (1995), 261-265.

[Me] L. MEREL, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Inv. Math. **124** (1996), 437-449.

[Mo] L. MORET-BAILLY, *Hauteur et classes de Chern sur les surfaces arithmétiques*. Astérisque **183** (1990), 37-58.

[Po] F. POP, *Embedding problems over large fields*, Ann. Math. **144** (1996), 1-35.

[Sa] D. J. SALTMAN, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250-283.

Université Lille
Mathématiques
59655 Villeneuve d'Ascq Cedex, France
pde@ccr.jussieu.fr