REGULAR LIFTING OF COVERS OVER AMPLE FIELDS

by

Dan Haran* and Moshe Jarden*

School of Mathematical Sciences, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: haran@math.tau.ac.il and jarden@math.tau.ac.il

Abstract

Let K be an ample field, G a finite group, and L a finite Galois extension of K such that $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of G. We prove that that $K(x)$ has a Galois extension F which is regular over L such that $\mathrm{Gal}(F/K(x)) \cong G$ and F has a K-place φ such that $\varphi(x) \in K$ and $\varphi(F) = L \cup \{\infty\}$.

5 November, 2007

* Partially supported by the Minkowski Center for Geometry at Tel Aviv University and the Mathematical Sciences Research Institute, Berkeley.

Introduction

Colliot-Thélène [CoT00] uses the technique of Kollár, Miyaoka, and Mori to prove the following result.

Theorem A: *Let K be an ample field of characteristic 0, x a transcendental element over K, and G a finite group. Then there is a Galois extension F of $K(x)$ with Galois group G, regular over K.*

Here K is said to be **ample** if every absolutely irreducible curve defined over K with a K-rational simple point has infinitely many K-rational simple points.

In fact, Colliot-Thélène proves a stronger version, still under the assumption that K is ample and $\mathrm{char}(K) = 0$:

Theorem B: *Given a Galois extension L/K with Galois group Γ which is a subgroup of G, there exist a Galois extension F of $K(x)$ with $\mathrm{Gal}(F/K(x)) \cong G$ and a place φ that fixes the elements of K and the residue field extension of $F/K(x)$ under φ is L/K.*

Case $\Gamma = G$ of Theorem B means that K has the arithmetic lifting property of Beckmann and Black [Bla99].

Since the results of Kollár, Miyaoka, and Mori are valid only in characteristic 0, Colliot-Thélène's proof works only in this case. Nonetheless, Theorem A holds in arbitrary characteristic ([Har87, Corollary 2.4] for complete fields, [Pop96, Main Theorem A]; see also [Liu95] and [HaV96]). Theorem B can be deduced for arbitrary characteristic from Théorème 1.1 of [MoB01]. The proof of that paper uses methods of formal patching.

Here we use algebraic patching to prove Theorem B for arbitrary characteristic. In fact, the main ingredient of the proof is almost contained in [HaJ98]. Therefore this note can be considered a sequel to [HaJ98]; a large portion of it recalls the situation and facts considered there.

The idea (displayed in our Lemma 2.1) to use the embedding problem $G \ltimes G \to G$ in order to obtain the arithmetic lifting property has been used in [Pop99]; we are grateful to F. Pop for making his note available to us.

1. Embedding problems and decomposition groups

Let K/K_0 be a finite Galois extension with Galois group Γ. Let x be a transcendental element over K. Put $E_0 = K_0(x)$. Suppose that Γ acts (from the right) on a finite group G; let $\Gamma \ltimes G$ be the corresponding semidirect product and $\pi\colon \Gamma \ltimes G \to \Gamma$ the canonical projection. We call

$$\pi\colon \Gamma \ltimes G \to \Gamma = \mathrm{Gal}(K/K_0) \tag{1}$$

a **finite constant split embedding problem**. A **solution** of (1) is a Galois extension F of E_0 such that $K \subseteq F$, $\mathrm{Gal}(F/E_0) = \Gamma \ltimes G$, and π is the restriction map $\mathrm{res}_K\colon \mathrm{Gal}(F/E_0) \to \mathrm{Gal}(K/K_0)$.

In [HaJ98, Theorem 6.4] we reprove the following result of F. Pop [Pop96]:

PROPOSITION 1.1: *Let K_0 be an ample field. Then each finite constant split embedding problem (1) has a solution F such that F has a K-rational place φ such that $\varphi(x) \in K_0 \cup \{\infty\}$ (in particular, F/K is regular).*

In this section we show that the proof of Proposition 1.1 in [HaJ98] yields a stronger assertion.

We denote the residue field of a place φ of a field F by $\bar{F}_\varphi$.

LEMMA 1.2: *Let F be a solution of (1). Put $F_0 = F^\Gamma$. Let $\varphi\colon F \to \widetilde{K_0} \cup \{\infty\}$ be a K-place with $\varphi(x) \in K_0 \cup \{\infty\}$. Assume that φ is unramified in F/E_0 and let D_φ be its decomposition group in F/E_0. Then $K \subseteq \bar{F}_\varphi$ and the following assertions are equivalent:*

(a) *$K = \bar{F}_\varphi$ and $\Gamma = D_\varphi$;*

(b) *$D_\varphi \subseteq \Gamma$;*

(c) *$K_0 = \bar{F}_{0,\varphi}$;*

(d) *$K = \bar{F}_\varphi$ and $\varphi(f^\gamma) = \varphi(f)^\gamma$ for each $\gamma \in \Gamma$ and $f \in F$ with $\varphi(f) \neq \infty$.*

Proof: Since $K \subseteq F$, we have $K = \bar{K}_\varphi \subset \bar{F}_\varphi$. Since the inertia group of φ in F/E_0 is trivial, we have an isomorphism $\theta\colon D_\varphi \to \mathrm{Gal}(\bar{F}_\varphi/K_0)$ given by

$$\varphi(f^\gamma) = \varphi(f)^{\theta(\gamma)}, \qquad \gamma \in D_\varphi,\ f \in F,\ \varphi(f) \neq \infty. \tag{2}$$

Hence, $|D_\varphi| = [\bar{F}_\varphi : K_0] \ge [K : K_0] = |\Gamma|$. This gives (a) $\Leftrightarrow$ (b).

Since φ is unramified over E_0, the decomposition field F^{D_φ} is the largest intermediate field of F/E_0 mapped by φ into $K_0 \cup \{\infty\}$, and hence (b) $\Leftrightarrow$ (c).

Clearly (d) $\Rightarrow$ (c). If $\bar{F}_\varphi = K$, then $f^\gamma = \varphi(f^\gamma) = \varphi(f)^{\theta(\gamma)} = f^{\theta(\gamma)}$ for all $f \in K$ and $\gamma \in D_\varphi$ (by (2)). Hence, $\theta(\gamma) = \gamma$ for all $\gamma \in D_\varphi$. Applying (2) once more, we have $\varphi(f^\gamma) = \varphi(f)^{\theta(\gamma)} = \varphi(f)^\gamma$ for each $f \in F$ with $\varphi(f) \ne \infty$ and $\gamma \in D_\varphi$. Consequently, (a) $\Rightarrow$ (d). ∎

Remark 1.3: Let K_0 be an ample field and F a solution of (1). Suppose F has a K-rational place φ unramified over E_0 such that $\varphi(x) \in K_0 \cup \{\infty\}$ and Γ is the decomposition group of φ in F/E_0. Then F has infinitely many such places.

Indeed, put $F_0 = F^\Gamma$. Recall that F_0 is regular over K_0. By Lemma 1.2,

(a) the assumption is that there is a K_0-place $\varphi: F_0 \to K_0$ unramified over $K_0(x)$, and

(b) we have to show that there are infinitely many such places.

But (a) $\Rightarrow$ (b) is a property of an ample field. ∎

PROPOSITION 1.4: *Let K_0 be an ample field. Then each finite constant split embedding problem (1) has a solution F with a K-rational place φ of F unramified over E_0 such that $\varphi(x) \in K_0 \cup \{\infty\}$ and Γ is the decomposition group of φ in F/E_0.*

Proof: Put $E = K(x) = KK_0(x)$.

PART A: As in the proof of [HaJ98, Theorem 6.4], we first assume that K_0 *is complete with respect to a non-trivial discrete ultrametric absolute value* $|\,|$, *with infinite residue field and K/K_0 is unramified.*

In this case [HaJ98, Proposition 5.2] proves Proposition 1.1. Claim C of that proof shows that, for every $b \in K_0$ with $|b| > 1$, $x \to b$ extends to a K-homomorphism $\varphi_b: R \to K$, where R is the principal ideal ring $K\{\frac{1}{x-c_i} \mid i \in I\}$ and the c_i's are properly chosen elements of K. From there it extends to a K-place $\varphi_b: Q \to K \cup \{\infty\}$ of the $Q = \mathrm{Quot}(R)$. Furthermore, [HaJ98, Lemma 1.3(b)] gives an E-embedding $\lambda: F \to Q$. The compositum $\varphi = \varphi_b \circ \lambda$ is a K-rational place of F. Excluding finitely many b's we may assume that φ is unramified over E_0. To verify that φ satisfies condition (d) of Lemma 1.2, we first recall the relevant facts from [HaJ98].

(a) [HaJ98, Proposition 5.2, Construction B] The group $\Gamma = \mathrm{Gal}(K/K_0)$ lifts isomorphically to $\mathrm{Gal}(E/E_0)$. By the choice of the c_i we have $\left(\frac{1}{x-c_i}\right)^\gamma = \frac{1}{x-c_i^\gamma}$, for each $\gamma \in \Gamma$. It follows that Γ continuously acts on R in the following way

$$\Big(a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}\big(\frac{1}{x-c_i}\big)^n\Big)^\gamma = a_0^\gamma + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}^\gamma\big(\frac{1}{x-c_i^\gamma}\big)^n.$$

This action induces an action of Γ on Q.

(b) [HaJ98, (7) on p. 334] The above mentioned action of Γ on Q defines an action of Γ on the Q-algebra

$$N = \mathrm{Ind}_1^G Q = \Big\{\sum_{\theta\in G} a_\theta\theta \mid a_\theta \in Q\Big\}$$

in the following way:

$$\Big(\sum_{\theta\in G} a_\theta\theta\Big)^\gamma = \sum_{\theta\in G} a_\theta^\gamma\theta^\gamma \qquad a_\theta \in Q,\ \gamma\in\Gamma.$$

Furthermore, the field F is a subring of N [HaJ98, p. 332] and Γ acts on it by restriction from N [HaJ98, Proof of Proposition 1.5, Part A].

(c) The embedding $\lambda\colon F \to Q$ is the restriction to F of the projection

$$\sum_{\theta\in G} a_\theta\theta \mapsto a_1$$

from $N = \mathrm{Ind}_1^G Q$ onto Q [HaV96, Proposition 3.4].

(d) The place $\varphi_b\colon Q \to K\cup\{\infty\}$ is induced from the evaluation homomorphism $\varphi_b\colon R \to K$ given by [HaJ98, Remark 3.5]

$$\varphi_b\Big(a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}\big(\frac{1}{x-c_i}\big)^n\Big) = a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}\big(\frac{1}{b-c_i}\big)^n.$$

In order to prove condition (d) of Lemma 1.2 it suffices to show that both λ and φ_b are Γ-equivariant.

Let $f = \sum_{\theta\in G} a_\theta\theta \in F \subseteq N$. Then, by (b) and (c),

$$\lambda(f^\gamma) = \lambda\Big(\sum_{\theta\in G} a_\theta^\gamma\theta^\gamma\Big) = a_1^\gamma = \Big(\lambda\Big(\sum_{\theta\in G} a_\theta\theta\Big)\Big)^\gamma = \lambda(f)^\gamma.$$

Furthermore, let $r = a_0 + \sum_{i\in I} \sum_{n=1}^{\infty} a_{in}\big(\frac{1}{x-c_i}\big)^n \in R$. By (a) and (d),

$$\varphi_b(r^\gamma) = \varphi_b\Big(a_0^\gamma + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}^\gamma\big(\frac{1}{x-c_i^\gamma}\big)^n\Big) = a_0^\gamma + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}^\gamma\big(\frac{1}{b-c_i^\gamma}\big)^n$$

$$= \Big(a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in}\big(\frac{1}{b-c_i}\big)^n\Big)^\gamma = \varphi_b(r)^\gamma.$$

Thus φ_b is Γ-equivariant.

PART B: *K_0 is an arbitrary ample field.* As in the proof of [HaJ98, Theorem 6.4] let $\hat{K}_0 = K_0((t))$ be the field of formal power series in t over K_0. Then $\hat{K} = K\hat{K}_0$ is an unramified extension of $\hat{K}_0$ with Galois group Γ and infinite residue field.

By Part A, $\hat{K}_0(x)$ has a Galois extension $\hat{F}$ which contains $\hat{K}(x)$, such that $\mathrm{Gal}(\hat{F}/\hat{K}_0(x)) = \Gamma \ltimes G$ and the restriction map $\mathrm{Gal}(\hat{F}/\hat{K}_0(x)) \to \mathrm{Gal}(K/K_0)$ is the projection $\pi\colon \Gamma \ltimes G \to \Gamma$. Furthermore, there is $b \in \hat{K}_0$ such that the place $x \to b$ of $\hat{K}_0(x)$ extends to an unramified $\hat{K}$-place $\hat{\varphi}\colon \hat{F} \to \hat{K} \cup \{\infty\}$ and $\hat{\varphi}(\hat{F}^\Gamma) = \hat{K}_0$. Put $m = |G|$.

Use the Weak Approximation to find $y \in \hat{F}^\Gamma$ mapped by the m distinct extensions of $x \to b$ to $\hat{F}^\Gamma$ into m distinct elements of the separable closure of $\hat{K}_0$; then $\hat{F}^\Gamma = \hat{K}_0(x, y)$.

Thus there exist polynomials $f \in \hat{K}_0[X, Z]$, $g \in \hat{K}_0[X, Y]$, elements $z \in \hat{F}$, $y \in \hat{F}^\Gamma$, and elements $b, c \in \hat{K}_0$, such that the following conditions hold:

(3a) $\hat{F} = \hat{K}_0(x, z)$, $f(x, Z) = \mathrm{irr}(z, \hat{K}_0(x))$; we identify $\mathrm{Gal}(f(x, Z), \hat{K}_0(x))$ with $\mathrm{Gal}(\hat{F}/\hat{K}_0(x))$;

(3b) $\hat{F}^\Gamma = \hat{K}_0(x, y)$, whence $\hat{F} = \hat{K}(x, y)$, and $g(x, Y) = \mathrm{irr}(y, \hat{K}_0(x))$; therefore $g(X, Y)$ is absolutely irreducible;

(3c) $\mathrm{discr}(g(b, Y)) \neq 0$ and $g(b, c) = 0$.

All of these objects depend on only finitely many parameters from $\hat{K}_0$. Hence, there are $u_1, \ldots, u_n \in \hat{K}_0$ such that the following conditions hold:

(4a) $F = K_0(\mathbf{u}, x, z)$ is a Galois over $K_0(\mathbf{u}, x)$, the coefficients of $f(X, Z)$ lie in $K_0[\mathbf{u}]$, $f(x, Z) = \mathrm{irr}(z, K_0(\mathbf{u}, x))$, and $\mathrm{Gal}(f(x, Z), K_0(\mathbf{u}, x)) = \mathrm{Gal}(f(x, Z), \hat{K}_0(x))$;

(4b) the coefficients of g lie in $K[\mathbf{u}]$; hence $g(x, Y) = \mathrm{irr}(y, K_0(\mathbf{u}, x))$; furthermore, $K_0(\mathbf{u}, x, y) = F^\Gamma$;

(4c) $b, c \in K_0[\mathbf{u}]$, $\mathrm{discr}(g(b, Y)) \neq 0$, and $g(b, c) = 0$.

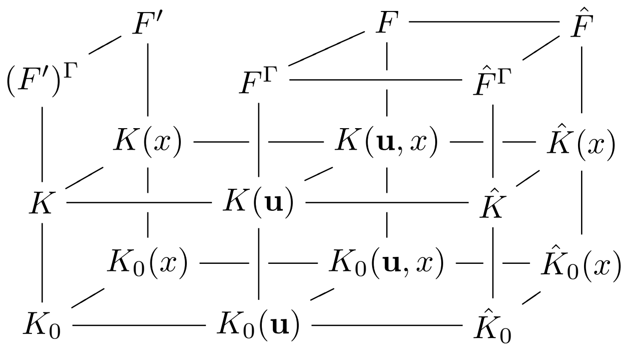
Since $\hat{K}_0$ has a K-rational place, namely, $x \to 0$, the field $\hat{K}_0$ and therefore also $K_0(\mathbf{u})$ are regular extensions of K_0. Thus, $\mathbf{u}$ generates an absolutely irreducible variety $U = \mathrm{Spec}(K_0[\mathbf{u}])$ defined over K_0. By Bertini-Noether [FrJ05, Proposition 9.4.3], the variety U has a nonempty Zariski open subset U' such that for each $\mathbf{u}' \in U'$ the K_0-specialization $\mathbf{u} \to \mathbf{u}'$ extends to a K-homomorphism $'$: $K[\mathbf{u}, x, z, y] \to K[\mathbf{u}', x, z', y']$ such that the following conditions hold:

(5a) $f'(x, z') = 0$, the discriminant of $f'(x, Z)$ is not zero, and $F' = K_0(\mathbf{u}', x, z')$ is the splitting field of $f'(x, Z)$ over $K_0(\mathbf{u}', x)$; in particular $F'/K_0(\mathbf{u}', x)$ is Galois;

(5b) $g'(X, Y)$ is absolutely irreducible and $g'(x, y') = 0$; so $g'(x, Y) = \mathrm{irr}(y', K(\mathbf{u}', x))$; furthermore, $K_0(\mathbf{u}', x, y') = (F')^\Gamma$;

(5c) $b', c' \in K_0[\mathbf{u}']$ and $\mathrm{discr}(g'(b', Y)) \neq 0$ and $g'(b', c') = 0$.

By assumption, K_0 is ample, so K_0 is existentially closed in $\hat{K}_0$ [Pop96, Prop. 1.1]. Since $\mathbf{u} \in U(\hat{K}_0)$, there is a $\mathbf{u}' \in U(K_0)$. Now repeat the end of the proof of [HaJ98, Lemma 6.2] (from "By (5a), the homomorphism…") to conclude that F' is a solution of (1).



Condition (5c) ensures that the place $x \to b'$ of $K_0(x)$ is unramified in $(F')^\Gamma$, hence in F', and extends to a K_0-rational place of $(F')^\Gamma$. This ends the proof by Lemma 1.2. ∎

2. Lifting property over ample fields

Consider a subgroup Γ of a finite group G, let Γ act on G by the conjugation in G

$$g^\gamma = \gamma^{-1} g \gamma.$$

and consider the semidirect product $\Gamma \ltimes G$. To fix notation, $\Gamma \ltimes G = \{(\gamma, g) \mid \gamma \in \Gamma, g \in G\}$ and the multiplication on $\Gamma \ltimes G$ is defined by

$$(\gamma_1, g_1)(\gamma_2, g_2) = (\gamma_1\gamma_2, g_1^{\gamma_2} g_2).$$

Notice the isomorphism $\Gamma \ltimes G \cong \Gamma \times G$ given by $(\gamma, g) \mapsto (\gamma, \gamma g)$ and the epimorphism $\rho\colon \Gamma \ltimes G \to G$ given by $(\gamma, g) \mapsto \gamma g$. Let $N = \mathrm{Ker}(\rho)$.

LEMMA 2.1: *Let K_0 be a field, K a Galois extension of K_0 with Galois group Γ, and x a transcendental element over K_0. Assume that (1) has a solution $\hat{F}$ with a K-rational place $\hat{\varphi}$ of $\hat{F}$ unramified over $K_0(x)$ such that $\hat{\varphi}(x) \in K_0 \cup \{\infty\}$ and Γ is the decomposition group of $\hat{\varphi}$ in $\hat{F}/K_0(x)$. Let $F = \hat{F}^N$ and let φ be the restriction of $\hat{\varphi}$ to F. Then*

(6a) *F is a Galois extension of $K_0(x)$ and $\mathrm{Gal}(F/K_0(x)) \cong G$;*

(6b) *F/K_0 is a regular extension;*

(6c) *φ represents a prime divisor $\mathfrak{p}$ of F/K_0 with decomposition group Γ in $F/K_0(x)$ and residue field K.*

Proof: By assumption, $\hat{F}$ is a Galois extension of $K_0(x)$ containing K, with Galois group $\Gamma \ltimes G$ such that the restriction $\mathrm{Gal}(\hat{F}/K_0(x)) \to \mathrm{Gal}(K/K_0)$ is the projection $\Gamma \ltimes G \to \Gamma$, and $\hat{F}/K$ is regular. Furthermore, $\hat{\varphi}\colon \hat{F} \to K$ is a K-place unramified over $K_0(x)$, with decomposition group $\Delta = \{(\gamma, 1) \mid \gamma \in \Gamma\} \cong \Gamma$ in $\hat{F}/K_0(x)$ and residue field extension K/K_0. In particular, $\hat{F}$ is regular over K.

From the definition of F we get (6a) and $\rho(\Delta) = \Gamma \le G$ is the decomposition group of the restriction $\varphi\colon F \to K$ of $\hat{\varphi}$ to F. Since $|\Delta| = [K : K_0]$, the residue field of φ is K. Since $\Gamma \ltimes G = NG$, the fields $F = \hat{F}^N$ and $K(x) = \hat{F}^G$ are linearly disjoint over $K_0(x)$. In addition, $FK = \hat{F}$ and $\hat{F}/K$ is regular. Therefore, F is regular over K_0. ∎

Lemma 2.1 together with Proposition 1.4 and Remark 1.3 yield the following result:

THEOREM 2.2: *Let K_0 be an ample field, G a finite group, Γ a subgroup, K a Galois extension of K_0 with Galois group Γ, and x a transcendental element over K_0. Then there is a field F that satisfies (6a), (6b) and*

(6d) *there are infinitely many prime divisors $\mathfrak{p}$ of F/K_0 with decomposition group Γ in $F/K_0(x)$ and residue field K.*

Remark 2.3: In case of $\Gamma = G$, Theorem 2.2 says that an ample field K_0 has the so-called **arithmetic lifting property** of Beckmann-Black [Bla99]. ∎

Remark 2.4: In the special case where K is a PAC field, it possible to refine Theorem 2.2. In this case if F is an arbitrary Galois extension of $K(x)$ regular over K and L/K is a Galois extension with Galois group isomorphic to a subgroup of $\mathrm{Gal}(F/K(x))$, there exists a place φ of F such that the residue field extension of $F/K(x)$ under φ is L [Deb99, Remark 3.3]. This stronger property of PAC fields does not hold for an arbitrary ample field K [CoT00, Appendix]. ∎

References

[BLa99] E.V. Black, *Deformations of dihedral 2-group extensions of fields,* Transactions of the AMS **351** (1999), 3229–3241.

[CoT00] J.-L. Colliot-Thélène, *Rational connectedness and Galois cover of the projective line,* Annals of Mathematics **151** (2000), 359-373.

[Deb99] P. Dèbes, *Galois Covers with Prescribed Fibers: The Beckmann-Black Problem,* Ann. Scuola Norm. Sup. Pisa **28** (1999), 273–286.

[FrJ05] M. D. Fried and M. Jarden, *Field Arithmetic, Second Edition, revised and enlarged by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2005.

[Har87] D. Harbater, *Galois coverings of the arithmetic line,* in: Lecture Notes in Mathematics **1240**, 165–195, Springer-Verlag 1987.

[HaJ98] D. Haran and M. Jarden, *Regular split embedding problems over complete valued fields,* Forum Mathematicum **10** (1998), 329–351 .

[HaV96] D. Haran and H. Völklein, *Galois groups over complete valued fields,* Israel Journal of Mathematics, **93** (1996), 9–27.

[Liu95] Q. Liu, *Tout groupe fini est un groupe de Galois sur* $\mathbb{Q}_p(T)$*, d'après Harbater,* Contemporary Mathematics **186** (1995), 261–265.

[MoB01] L. Moret-Bailly, *Construction de revêtements de courbes pointées,* Journal of Algebra **240** (2001), 505–534.

[Pop96] F. Pop, *Embedding problems over large fields,* Annals of Mathematics **144** (1996), 1–34.

[Pop99] F. Pop, *On the BB theory,* an unpublished note, 2 pages.