

## ARITHMETIC DESCENT OF SPECIALIZATIONS OF GALOIS COVERS

RYAN EBERHART, HILAF HASSON

**Abstract:** Given a  $G$ -Galois branched cover of the projective line over a number field  $K$ , we study whether there exists a closed point of  $\mathbb{P}_K^1$  with a connected fiber such that the  $G$ -Galois field extension induced by specialization “arithmetically descends” to  $\mathbb{Q}$  (i.e., there exists a  $G$ -Galois field extension of  $\mathbb{Q}$  whose compositum with the residue field of the point is equal to the specialization). We prove that the answer is frequently positive (whenever  $G$  is regularly realizable over  $\mathbb{Q}$ ) if one first allows a base change to a finite extension of  $K$ . If one does not allow base change, we prove that the answer is positive when  $G$  is cyclic. Furthermore, we provide an explicit example of a Galois branched cover of  $\mathbb{P}_K^1$  with no  $K$ -rational points of arithmetic descent.

**Keywords:** Galois covers, Galois groups, curves, arithmetic descent, specializations, Inverse Galois Problem.

### 1. Introduction

In this paper we introduce and study the notion of *arithmetic descent* (see definition 2.3) of specializations of  $G$ -Galois branched covers (see definition 2.1). Arithmetic descent is closely related to the Inverse Galois Problem (IGP), which asks whether for every finite group  $G$  there exists a  $G$ -Galois field extension of  $\mathbb{Q}$ .

Using Riemann’s Existence Theorem, one can show (see for example [Har03, Corollary 3.3.5]) that for every finite group  $G$  there exists a  $G$ -Galois branched cover of  $\mathbb{P}_{\mathbb{Q}}^1$ . By descent, this implies that there is a  $G$ -Galois branched cover over *some* number field  $K$ . By Hilbert’s Irreducibility Theorem ([FJ05, Theorem 13.4.2]) there exist infinitely many  $G$ -Galois field extensions of  $K$  arising from specializations of this cover at  $K$ -rational points. Most efforts to solve the IGP over  $\mathbb{Q}$  have been aimed at producing a  $G$ -Galois branched cover of  $\mathbb{P}_{\mathbb{Q}}^1$  that descends to  $\mathbb{Q}$  and then specializing. (Especially important is the technique of *rigidity*, developed by Belyi, Feit, Fried, Shih, Thompson, Matzat and others; see [Völ96], [Ser08], and [MM99] for details. There has also been research aimed at understanding how the

*field of moduli* depends on the group, as well as on topological data; see for example [Bec89], [Flo04], [Wew03], [Obu12], [Obu13], and [Has13].) In this paper we study an alternative method of attack.

By the above, for every finite group  $G$  there exists a  $G$ -Galois branched cover of  $\mathbb{P}_K^1$  for some number field  $K$ . We now ask whether a point on  $\mathbb{P}_K^1$  can be chosen cleverly so that the  $G$ -Galois field extension coming from specialization descends to  $\mathbb{Q}$ , even if the cover itself does not. For example, consider the cyclic  $C_4$ -Galois cover  $\mathbb{P}_{\mathbb{Q}(i)}^1 \rightarrow \mathbb{P}_{\mathbb{Q}(i)}^1$  given by  $y^4 = x$ . This cover does *not* descend (together with its Galois action) to  $\mathbb{Q}$ . However, by specializing at  $x = i$  we get the  $C_4$ -Galois extension  $\mathbb{Q}(\zeta_{16})/\mathbb{Q}(i)$  (where  $\zeta_{16}$  is a primitive 16<sup>th</sup> root of unity), which *does* arithmetically descend to the  $C_4$ -Galois extension  $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})/\mathbb{Q}$  (i.e., the compositum  $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})\mathbb{Q}(i)$  is equal to  $\mathbb{Q}(\zeta_{16})$ ).

There are several natural questions concerning arithmetic descent, which we now discuss. Let  $G$  be a finite group, let  $L/K$  be a finite extension of Hilbertian fields (examples of Hilbertian fields include number fields and function fields; see definition 2.6), and let  $X \rightarrow \mathbb{P}_L^1$  be a  $G$ -Galois branched cover. In this situation, we ask the following questions:

### Questions 1.1.

1. Does there exist an  $L$ -rational point  $P$  of  $\mathbb{P}_L^1$  such that the specialization at  $P$  arithmetically descends to  $K$ ?
2. Does there exist a *closed point*  $P$  of  $\mathbb{P}_L^1$ , not necessarily  $L$ -rational, such that the specialization at  $P$  arithmetically descends to  $K$ ?
3. Does Question (1) hold after finite base change? In other words, does there exist a finite field extension  $E/L$  and an  $E$ -rational point  $P$  of  $\mathbb{P}_E^1$  such that the specialization at  $P$  in  $X_E \rightarrow \mathbb{P}_E^1$  arithmetically descends to  $K$ ?

Note that a positive answer to Question 1.1.1 implies a positive answer to Question 1.1.2, which implies a positive answer to Question 1.1.3. To illustrate the difference between Question 1.1.2 and Question 1.1.3, consider the following example. Let  $\mathbb{P}_{\mathbb{Q}}^1 \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  be the  $C_2$ -Galois cover given by  $y^2 = x$ . The specialization at  $x = (1 + i)$  does not arithmetically descend to  $\mathbb{Q}$ . However, after base changing to  $E = \mathbb{Q}(i, \sqrt{2 + 2i})$ , specialization at the ( $E$ -rational) point  $x = (1 + i)$  does arithmetically descend to  $\mathbb{Q}$ , since  $E(\sqrt{1 + i})/E$  is isomorphic to  $E(\sqrt{2})/E$ .

In the remainder of this paper, we attack all three questions. In Section 2 we introduce the definitions we require. In Section 3 (theorem 3.1) we show that the answer to Question 1.1.3 is frequently positive—whenever  $G$  is regularly realizable over  $K$ . While this motivates further investigation, the proof of theorem 3.1 does not lend itself to generalization. In Section 4 (theorem 4.1) we answer Question 1.1.2 positively for cyclic groups of order coprime to  $\text{char}(K)$ . In Section 5 (theorem 5.1) we exhibit an explicit cover for which the answer to Question 1.1.1 is negative. Thus, our results seem to suggest that while Question 1.1.3 is the most likely to have a positive answer, Question 1.1.2 is the most geometrically interesting of the above questions.

## 2. Definitions

**Definition 2.1.** Let  $G$  be a finite group, let  $K$  be a field, and let  $X$  and  $Y$  be geometrically irreducible varieties over  $K$ . A map  $X \rightarrow Y$  of  $K$ -varieties is called a *branched cover* (sometimes shortened to *cover*) if it is finite and generically étale. A branched cover  $f : X \rightarrow Y$  is *Galois* if  $\text{Aut}(X/Y)$ , the group of  $K$ -automorphisms of  $X$  commuting with  $f$ , has order equal to the degree of  $f$ . A Galois branched cover is called  *$G$ -Galois* if  $\text{Aut}(X/Y)$  is isomorphic to  $G$ .

**Definition 2.2.** Let  $f : X \rightarrow Y$  be a branched cover of curves and  $P$  a closed point of  $Y$ . The *specialization* of  $f$  at  $P$  is the restriction of  $f$  to the fiber above  $P$ . More precisely, it is the map

$$\text{Spec} \left( \prod_{Q \in f^{-1}(P)} \mathcal{O}_{X,Q}/\mathfrak{m}_Q \right) \rightarrow \text{Spec} (\mathcal{O}_{Y,P}/\mathfrak{m}_P),$$

where  $\mathcal{O}_{X,Q}$  (resp.  $\mathcal{O}_{Y,P}$ ) is the local ring at the closed point  $Q$  (resp.  $P$ ), with maximal ideal  $\mathfrak{m}_Q$  (resp.  $\mathfrak{m}_P$ ). We say the specialization of  $f$  at  $P$  is *connected* if the domain of this restriction is connected. Note that if  $f$  is Galois, and  $P$  is an unramified point of  $f$  whose specialization is connected, then this specialization is a  $G$ -Galois extension of residue fields.

**Definition 2.3.** Let  $G$  be a finite group,  $L/K$  a field extension, and  $E/L$  a  $G$ -Galois extension of fields. We say that  $E/L$  *arithmetically descends to  $K$*  if there exists a  $G$ -Galois field extension  $F/K$  such that  $F \otimes_K L \cong E$  as  $L$ -algebras.

If  $f : X \rightarrow Y$  is a branched cover of curves over  $L$  then we say that a closed point  $P$  of  $Y$  *arithmetically descends to  $K$*  if the specialization of  $f$  at  $P$  is connected and the residue field extension arithmetically descends to  $K$ .

**Definition 2.4.** Let  $V$  be an irreducible variety over a field  $K$ . Following [Ser08], a subset  $A$  of  $V(K)$  is of *type  $C_1$*  if there is a closed proper subset  $W \subseteq V$  such that  $A \subseteq W(K)$ . A subset  $A$  of  $V(K)$  is of *type  $C_2$*  if there is a geometrically irreducible variety  $V'$  of the same dimension as  $V$ , and a generically surjective morphism  $\pi : V' \rightarrow V$  of degree greater than one, such that  $A \subseteq \pi(V'(K))$ .

A subset  $A$  of  $V(K)$  is called *thin* if it is contained in a finite union of sets of type  $C_1$  and  $C_2$ . The variety  $V$  is of *Hilbert type* if  $V(K)$  is non-thin.

**Remark 2.5.** The definition of sets of type  $C_2$  in [Ser08] requires that  $V'$  is only irreducible, rather than geometrically irreducible. However, by the remark after Definition 3.1.3 in [Ser08], the two definitions are equivalent.

While we are primarily interested in number fields, most of our results apply to a more general type of field called Hilbertian fields. (See [FJ05, Chapters 12 and 13] for a detailed discussion.)

**Definition 2.6.** A field  $K$  is called *Hilbertian* if  $\mathbb{P}_K^1$  is of Hilbert type.

**Definition 2.7.** Let  $L/K$  be a field extension and  $X$  a  $K$ -scheme. The notation  $X_L$  will be used for the base change  $X \times_K L$  of  $X$  to  $L$ . Let  $\pi : X_L \rightarrow X$  be the morphism induced by this base change. For the sake of brevity,  $X_L(K)$  will refer to the set  $\pi^{-1}(X(K))$  of  $L$ -points of  $X_L$  coming from  $K$ -points of  $X$ .

The notation  $C_n$  will be used for a cyclic group of order  $n$ , and the notation  $\zeta_n$  will refer to a coherent choice of a primitive  $n^{\text{th}}$  root of unity in a fixed separable closure of the field in question.

### 3. Arithmetic descent after finite base change

The following shows that the answer to Question 1.1.3 is often affirmative:

**Theorem 3.1.** *In the situation of Questions 1.1, assume that  $G$  is regularly realizable over  $K$ . Then the answer to Question 1.1.3 is positive for any  $L/K$  and any  $G$ -Galois branched cover  $X \rightarrow \mathbb{P}_L^1$ . In particular, the Regular Inverse Galois Problem (RIGP) over  $K$  implies an affirmative answer to Question 1.1.3 for any  $L/K$  and any  $G$ -Galois branched cover of  $\mathbb{P}_L^1$ .*

**Proof.** Let  $P$  be an  $L$ -rational point of  $\mathbb{P}_L^1$  whose fiber in  $X$  is connected, and let  $F/L$  be the resulting  $G$ -Galois field extension. By assumption, there exists a  $G$ -Galois branched cover  $Y \rightarrow \mathbb{P}_K^1$ . Consider the base change of this cover to  $F$ . The set  $\mathbb{P}_F^1(K)$  is non-thin by [Ser08, Proposition 3.2.1], while the subset of  $\mathbb{P}_F^1(F)$  of points whose fiber in  $Y_F \rightarrow \mathbb{P}_F^1$  is connected is the complement of a thin set by [Ser08, Proposition 3.3.1]. The intersection of these two sets is non-empty, since otherwise we would have a non-thin set contained in a thin set. This implies that there is a point  $Q \in \mathbb{P}_F^1(K)$  whose fiber in  $Y_F$  is connected. By specializing at the corresponding  $K$ -point of  $\mathbb{P}_K^1$  in  $Y \rightarrow \mathbb{P}_K^1$ , the resulting  $G$ -Galois field extension  $E/K$  is linearly disjoint with  $F$  over  $K$ .

Note that  $(E \otimes_K F)/L$  is a Galois extension of fields with group  $G \times G$ . Let  $\Delta$  denote the subgroup  $\{(g, g) | g \in G\}$  of  $G \times G$  and let  $L'$  be the subfield of  $E \otimes_K F$  fixed by  $\Delta$ . Let  $P_{L'}$  be the unique  $L'$ -point of  $\mathbb{P}_{L'}^1$ , lying above  $P$ . Then  $P_{L'}$  is a point of arithmetic descent for  $X_{L'} \rightarrow \mathbb{P}_{L'}^1$ . Indeed, the specialization is the field extension  $F \otimes_L L'$  of  $L'$ , which is isomorphic as an  $L'$ -algebra to  $E \otimes_K F$ , which, in turn, is isomorphic to  $E \otimes_K L'$  since  $\Delta \cap (G \times 1) = \Delta \cap (1 \times G) = 1$ . ■

### 4. Closed points of arithmetic descent for cyclic groups

In this section, our objective is to establish the following answer to Question 1.1.2.

**Theorem 4.1.** *Question 1.1.2 has a positive answer for any  $G$ -Galois branched cover  $X \rightarrow \mathbb{P}_L^1$ , where  $G$  is a cyclic group of order coprime to  $\text{char}(K)$ . In fact, one can replace  $\mathbb{P}_L^1$  with any smooth curve over  $L$ .*

Roughly, our method of proof will be to show (theorem 4.2) that the set of points of arithmetic descent for a particularly simple  $C_n$ -Galois cover is non-thin. After employing a suitable Cartesian diagram and dealing with issues arising from the potential lack of a primitive  $n^{\text{th}}$  root of unity in  $L$ , the result will follow for a general  $C_n$ -Galois cover.

**Theorem 4.2.** *Let  $K$  be a Hilbertian field,  $n$  a positive integer coprime to  $\text{char}(K)$ , and  $L = K(\zeta_n)$ . Let  $\mathbb{P}_L^1 \rightarrow \mathbb{P}_L^1$  be the  $C_n$ -Galois cover defined by  $y^n = x$ . Then the set of  $L$ -rational points which arithmetically descend to  $K$  for this cover is non-thin.*

**Proof.** We first remark that there are infinitely many non-isomorphic  $C_n$ -Galois field extensions of  $L$  which arithmetically descend to  $K$ . Indeed, assume by contradiction that all such extensions of  $L$  are contained in a finite extension  $E/L$ . By [FJ05, Lemma 16.3.4] there exists a  $C_n$ -Galois branched cover  $Z \rightarrow \mathbb{P}_K^1$ . The subset  $\mathbb{P}_E^1(K)$  of  $\mathbb{P}_E^1(E)$  is non-thin ([Ser08, Proposition 3.2.1]), and the set of  $E$ -rational points whose fiber in  $Z_E \rightarrow \mathbb{P}_E^1$  is connected is the complement of a thin set ([Ser08, Proposition 3.3.1]). Since the intersection of a non-thin set and the complement of a thin set is non-empty, it follows that there is a  $C_n$ -Galois extension of  $E$  which arithmetically descends to  $K$ . In particular there is a  $C_n$ -Galois extension of  $L$  that arithmetically descends to  $K$  which is not contained in  $E$ , a contradiction.

By the above, let  $\{L_i\}_{i \in I}$  be an infinite set of non-isomorphic  $C_n$ -Galois field extensions of  $L$ , each of which arithmetically descends to  $K$ . For each  $i$  in  $I$  there exists an  $a_i$  in  $L$  such that  $L_i = L(\sqrt[n]{a_i})$ . Let  $f_i : \mathbb{P}_L^1 \rightarrow \mathbb{P}_L^1$  be given by  $x \mapsto a_i x^n$ . Note that by Kummer theory  $f_i(\mathbb{P}_L^1(L) \setminus \{0, \infty\})$  is the set of  $L$ -rational points whose specialization in the cover  $\mathbb{P}_L^1 \rightarrow \mathbb{P}_L^1$  given by  $y^n = x$  is isomorphic to  $L(\sqrt[n]{a_i})/L$ . Therefore it suffices to show that  $S = \bigcup f_i(\mathbb{P}_L^1(L))$  is non-thin.

Suppose that  $S$  is thin. By [FJ05, p. 245 Claim B(f)] any set of type  $C_1$  is contained in a set of type  $C_2$ , so we have that

$$S \subseteq \bigcup_{j=1}^n g_j(Y_j(L))$$

where each  $Y_j$  is a geometrically irreducible curve over  $L$  and each  $g_j : Y_j \rightarrow \mathbb{P}_L^1$  has degree greater than one. Let  $Y$  denote the disjoint union of the curves  $Y_j$  and  $g : Y \rightarrow \mathbb{P}_L^1$  the map induced from the  $g_j$ 's.

Fix an index  $i$ . After taking the reduced structure if necessary, let  $W$  denote the fiber product in the following diagram

$$\begin{array}{ccc} W := Y \times_{\mathbb{P}_L^1} \mathbb{P}_L^1 & \xrightarrow{\pi} & \mathbb{P}_L^1 \\ \downarrow & & \downarrow f_i \\ Y & \xrightarrow{g} & \mathbb{P}_L^1 . \end{array}$$

Since  $f_i(\mathbb{P}_L^1(L)) \subseteq g(Y(L))$ , we have that  $\mathbb{P}_L^1(L) \subseteq \pi(W(L))$  and thus  $\pi(W(L))$  is non-thin. Finiteness is base change invariant, so  $\pi$  is finite, which implies that  $W$  consists of finitely many irreducible components of dimension no greater than one. These facts collectively imply that there exists an irreducible component  $W'$  of  $W$  such that the restriction of  $\pi$  to  $W'$  has a section on an open subvariety  $U$  of  $\mathbb{P}_L^1$ . Thus for every index  $i$  we have that  $x \mapsto a_i x^n$  factors birationally through one of finitely many maps  $g_j : Y_j \rightarrow \mathbb{P}_L^1$ . However, this is impossible since  $f_i(\mathbb{P}_L^1(L)) \cap f_{i'}(\mathbb{P}_L^1(L)) = \{0, \infty\}$  for  $i \neq i'$ . ■

Before proving theorem 4.1, we require one last lemma.

**Lemma 4.3.** *Let  $L'/L$  be a finite extension of Hilbertian fields, and let  $S \subseteq \mathbb{P}_{L'}^1(L')$  be a non-thin set. Suppose that  $S = \bigcup_{i \in I} S_i$  where each  $S_i$  is equal to  $f_i(\mathbb{P}_{L'}^1(L'))$  for a cover  $f_i : \mathbb{P}_{L'}^1 \rightarrow \mathbb{P}_{L'}^1$ . If  $R$  is a thin set, then there exists an index  $i \in I$  such that  $S_i \setminus R$  is infinite.*

**Proof.** By [FJ05, p. 245 Claim B(f)] any set of type  $C_1$  is contained in a set of type  $C_2$ , so we have that

$$R \subseteq \bigcup_{j=1}^n g_j(Z_j(L'))$$

where each  $Z_j$  is a geometrically irreducible curve over  $L'$  and each  $g_j : Z_j \rightarrow \mathbb{P}_{L'}^1$  has degree greater than one. Let  $Y_j$  be the smooth projective model of  $Z_j$ . The map  $g_j$ , considered as a map on the smooth locus of  $Z_j$ , can be extended to a map  $\tilde{g}_j : Y_j \rightarrow \mathbb{P}_{L'}^1$ . Let  $R'$  be the union  $\bigcup \tilde{g}_j(Y_j(L'))$ .

Assume that  $S_i \setminus R'$  is finite. We claim that  $S_i$  is then contained in  $R'$ . To this end, let  $U$  be the open subscheme of  $\mathbb{P}_{L'}^1$ , obtained by removing  $f_i^{-1}(S_i \setminus R')$ . Let  $Y$  be the disjoint union of the curves  $Y_j$  and  $g : Y \rightarrow \mathbb{P}_{L'}^1$ , the map induced by the  $\tilde{g}_j$ 's. Since  $f_i(U \cap \mathbb{P}_{L'}^1(L'))$  is contained in  $g(Y(L'))$ , and since  $U \cap \mathbb{P}_{L'}^1(L)$  is a non-thin set, a similar argument to the one in the proof of theorem 4.2 shows that there exists a rational map  $h$  such that the following commutes:

$$\begin{array}{ccc} & & U \\ & \swarrow h & \downarrow f_i \\ Y & \longrightarrow & \mathbb{P}_{L'}^1 \end{array}$$

Since  $Y$  is proper,  $h$  can be extended to a map defined on all of  $\mathbb{P}_{L'}^1$ , and the claim follows.

Since  $S$  is non-thin, there must exist an  $i \in I$  such that  $S_i$  is not contained in  $R'$ . By the above,  $S_i \setminus R'$  is then infinite. Because  $R'$  contains all but finitely elements of  $R$ ,  $S_i \setminus R$  is infinite as well. ■

With the above results, we are now ready to prove theorem 4.1.

**Proof of theorem 4.1.** Let  $f : X \rightarrow Y$  be a  $C_n$ -Galois branched cover of curves over  $L$ . Let  $L' = L(\zeta_n)$  and let  $f_{L'} : X_{L'} \rightarrow Y_{L'}$  be the base change of  $f$  to  $L'$ . By Kummer theory  $f_{L'}$  is given by  $t^n = g$ , where  $g \in \kappa(Y_{L'})$ . Observe the Cartesian diagram

$$\begin{array}{ccc} X_{L'} & \longrightarrow & \mathbb{P}_{L'}^1 \\ f_{L'} \downarrow & & \downarrow \\ Y_{L'} & \xrightarrow{g} & \mathbb{P}_{L'}^1, \end{array}$$

where the bottom horizontal map is induced by  $g$ , the vertical right map is  $y^n = x$ , and the vertical left map is  $f_{L'}$ .

Since  $L'$  is Hilbertian, the set  $D$  of  $L'$ -points of  $\mathbb{P}_{L'}^1$ , whose fiber in the map  $g \circ f_{L'} : X_{L'} \rightarrow \mathbb{P}_{L'}^1$ , is disconnected is a thin set. Indeed, let  $L^{\text{sep}}$  be a separable closure of  $L'$ , let  $\bar{X} \rightarrow \mathbb{P}_{L^{\text{sep}}}^1$  be the base change of  $X_{L'} \rightarrow \mathbb{P}_{L'}^1$  to  $L^{\text{sep}}$ , let  $\bar{Z} \rightarrow \mathbb{P}_{L^{\text{sep}}}^1$  be its Galois closure, and let  $Z \rightarrow \mathbb{P}_E^1$  be a model of this Galois closure over some finite field extension  $E$  of  $L'$ . Then by [Ser08, Proposition 3.3.1], the set of  $E$ -points in  $\mathbb{P}_E^1$  whose fiber in  $Z$  is disconnected is thin. This implies, using [Ser08, Proposition 3.2.1], that the subset of points of  $\mathbb{P}_{L'}^1(L')$  whose fiber in  $Z$  is disconnected is thin. In particular, the subset of points in  $\mathbb{P}_{L'}^1(L')$  whose fiber in  $X_{L'}$  is disconnected is thin.

Let  $A \subseteq \mathbb{P}_{K(\zeta_n)}^1(K(\zeta_n))$  be the set of points of arithmetic descent for the cover  $y^n = x$ . By theorem 4.2,  $A$  is non-thin. By [Ser08, Proposition 3.2.1]  $A$ , considered as a subset of  $\mathbb{P}_{L'}^1(L')$ , remains non-thin. Moreover,  $A \setminus D$ , with  $D$  defined as in the previous paragraph, is non-thin. For any  $a \in A \setminus D$ , let  $b$  be the unique preimage of  $a$  under  $g : Y_{L'} \rightarrow \mathbb{P}_{L'}^1$ . By our choice of  $a$ , the  $C_n$ -Galois field extension  $L'(\sqrt[n]{a})/L'$  arithmetically descends to  $K$ . The specialization of  $f_{L'}$  at  $b$  is then  $(L'(\sqrt[n]{a}) \otimes_{L'} \kappa(b))/\kappa(b)$ , where  $\kappa(b)$  is the residue field of  $b$ . This specialization is a field extension since the fiber of  $g \circ f_{L'}$  over  $b$  is connected. Therefore,  $b$  is a point of arithmetic descent to  $K$  for the cover  $f_{L'}$ .

Note that if  $L'$  is equal to  $L$  (i.e., if  $L$  already contains a primitive  $n^{\text{th}}$  root of unity), then this concludes the proof. We may therefore assume that  $L'$  is a non-trivial extension of  $L$ . Let  $\pi : Y_{L'} \rightarrow Y_L$  be the base change map. Let

$$B = \{a \in A \mid \zeta_n \notin \kappa(\pi(z)) \text{ for every } z \text{ such that } g(z) = a\}.$$

It suffices to show that  $A \setminus (B \cup D)$  is non-empty. Indeed, for any  $a$  in  $A \setminus (B \cup D)$ , the closed point  $\pi(g^{-1}(a))$  is then a point of arithmetic descent.

Define an equivalence relation on  $A$  by  $a_1 \sim a_2$  if and only if  $a_1/a_2$  is an  $n^{\text{th}}$  power in  $L$ . We proceed to show that only finitely many elements in each equivalence class of  $A$  are contained in  $B$ . Indeed, let  $a$  be an element of  $A$ , and let  $c$  be an element of  $L$  such that  $c^n a$  is in  $B$ . Then by the definition of  $B$  there is a  $z \in Y_{L'}$  such that  $g(z) = c^n a$  and the residue field  $\kappa(\pi(z))$  of  $\pi(z)$  does not contain  $L'$ . After fixing an  $L$ -embedding of  $\kappa(\pi(z))$  into  $L^{\text{sep}}$ , this implies that

$\kappa(\pi(z)) \cap L'$  is a proper subextension  $F$  of  $L'/L$ . Note that this subextension is independent of the embedding, because every subextension of  $L'/L$  is Galois over  $L$ . It suffices to show that only finitely many such  $z$  can produce the same  $F$ .

To this end, we first show that  $g$  cannot be of the form  $g = c \cdot h$  where  $c$  is in  $L'$  and  $h$  is in  $\kappa(Y_F)$ . Indeed, let  $y^n = h$  define a cover  $X' \rightarrow Y_F$  of curves over  $F$ . Since this map is a model over  $F$  of the cover  $X_{L^{\text{sep}}} \rightarrow Y_{L^{\text{sep}}}$  given by  $y^n = g$ , by [Has14, Lemma 4.16]  $X' \rightarrow Y_F$  is a “twist” (in the sense defined in [Has14]) of  $X_F \rightarrow Y_F$ . Furthermore, since  $C_n$  is abelian  $X' \rightarrow Y_F$  must be Galois by [Has14, Lemma 4.18]. However,  $y^n = h$  cannot be Galois over  $F$  since  $F$  does not contain a primitive  $n^{\text{th}}$  root of unity. (Note that since we have assumed that  $X$  is geometrically irreducible, it follows that  $g$  is not an  $n^{\text{th}}$  power in  $\kappa(Y_{L^{\text{sep}}})$ , and so  $h$  is not an  $n^{\text{th}}$  power in  $\kappa(Y_F)$ .)

Let  $k$  be the degree of  $L'/F$ , and write  $g = \sum_{i=0}^{k-1} g_i \zeta_n^i$  and  $a = \sum_{i=0}^{k-1} a_i \zeta_n^i$ , where each  $g_i$  is in  $\kappa(Y_F)$  and each  $a_i$  is in  $F$ . Since  $g$  is not an  $L'$ -multiple of an element in  $\kappa(Y_F)$ , there are indices  $i$  and  $j$  such that  $g_i/g_j$  is a non-constant function. By assumption  $\kappa(\pi(z)) \cap L' = F$ , and so we have that  $g_i(z) = c^n a_i$  and  $g_j(z) = c^n a_j$ . Since only finitely many points map via  $g_i/g_j$  to  $a_i/a_j$ , only finitely many  $z$ 's satisfy that  $\kappa(\pi(z)) \cap L'$  is equal to  $F$ , as claimed.

Let  $a$  be an element of  $A$ . Note that the equivalence class of  $a$  in  $A$  is precisely the image of  $\mathbb{P}_{L'}^1(L)$  for the map  $\mathbb{P}_{L'}^1 \rightarrow \mathbb{P}_{L'}^1$  defined by  $x \mapsto ax^n$ . Therefore, lemma 4.3 (with  $A$  in the role of  $S$ , the equivalence classes of  $A$  in the role of the  $S_i$ 's, and  $D$  in the role of  $R$ ) implies that there is an equivalence class of  $A$  which has infinitely many points not in  $D$ . Since each such equivalence class of  $A$  has only finitely many points in  $B$ , the set  $A \setminus (B \cup D)$  is non-empty, as we wanted to prove. ■

### 5. A cover with no rational points of arithmetic descent

The objective of this section is to provide an example of a cover for which the answer to Question 1.1.1 is negative. To be precise, in this section we prove the following.

**Theorem 5.1.** *Let  $z$  be a parameter for  $\mathbb{P}_{\mathbb{Q}(\zeta_3)}^1$ . Then the  $C_3$ -Galois cover of  $\mathbb{P}_{\mathbb{Q}(\zeta_3)}^1$  defined by  $t^3 = 3(z^3 + 2)$  has no  $\mathbb{Q}(\zeta_3)$ -rational points that arithmetically descend to  $\mathbb{Q}$ .*

In order to prove this theorem, we first give a complete characterization of the points of arithmetic descent of a particularly simple  $C_3$ -Galois cover.

**Proposition 5.2.** *Let  $T$  be the set of  $\mathbb{Q}(\zeta_3)$ -rational points which arithmetically descend to  $\mathbb{Q}$  for the  $C_3$ -Galois cover  $\mathbb{P}_{\mathbb{Q}(\zeta_3)}^1 \rightarrow \mathbb{P}_{\mathbb{Q}(\zeta_3)}^1$  given by  $t^3 = z$ . Let  $C$  be the set of cubes in  $\mathbb{Q}(\zeta_3)$ . Then  $T = \{(x + \zeta_3 y)^2(x + \zeta_3^2 y) \mid x, y \in \mathbb{Q}\} \setminus C$ .*

**Proof.** Let  $a = (x + \zeta_3 y)^2(x + \zeta_3^2 y)$  where  $x, y \in \mathbb{Q}$ , and let  $\sqrt[3]{a}$  be a third root of  $a$  in the specialization at  $z = a$ . Note that the specialization at  $z = a$  is disconnected precisely when  $a \in C$ . Let  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{a})/\mathbb{Q}(\zeta_3))$  be such that  $\sigma(\sqrt[3]{a}) = \zeta_3 \sqrt[3]{a}$ ,

and let  $\tau$  be the generator of  $\text{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ . Note that  $\frac{\sqrt[3]{a^2}}{x+\zeta_3y}$  is a third root of  $\tau(a)$ . Indeed,

$$\left(\frac{\sqrt[3]{a^2}}{x+\zeta_3y}\right)^3 = \frac{a^2}{(x+\zeta_3y)^3} = (x+\zeta_3^2y)^2(x+\zeta_3y) = \tau(a).$$

Therefore,  $\tau$  extends to an element in  $\text{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{a})/\mathbb{Q})$  by taking  $\sqrt[3]{a}$  to  $\frac{\sqrt[3]{a^2}}{x+\zeta_3y}$ . In order to show that  $z = a$  is a point of arithmetic descent, we wish to show that  $\sigma$  and  $\tau$  commute. It suffices to check this on  $\sqrt[3]{a}$ :

$$\sigma(\tau(\sqrt[3]{a})) = \sigma\left(\frac{\sqrt[3]{a^2}}{x+\zeta_3y}\right) = \zeta_3^2 \frac{\sqrt[3]{a^2}}{x+\zeta_3y} = \tau(\zeta_3) \frac{\sqrt[3]{a^2}}{x+\zeta_3y} = \tau(\zeta_3 \sqrt[3]{a}) = \tau(\sigma(\sqrt[3]{a})).$$

We now show the reverse direction. Let  $a$  be in  $T$ , and let  $\sqrt[3]{a}$  be a third root of  $a$  in the specialization at  $z = a$ . As before, let  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{a})/\mathbb{Q}(\zeta_3))$  be such that  $\sigma(\sqrt[3]{a}) = \zeta_3 \sqrt[3]{a}$ , and let  $\tau$  be the generator of  $\text{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ . Since  $z = a$  is a point of arithmetic descent, the automorphism  $\tau$  extends to an element in  $\text{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{a})/\mathbb{Q})$  that commutes with  $\sigma$ . Therefore,

$$\sigma(\tau(\sqrt[3]{a})) = \tau(\sigma(\sqrt[3]{a})) = \tau(\zeta_3 \sqrt[3]{a}) = \zeta_3^2 \tau(\sqrt[3]{a}).$$

Since  $\sigma(\sqrt[3]{a^2}) = \zeta_3^2 \sqrt[3]{a^2}$ , it follows that  $\sigma(\frac{\tau(\sqrt[3]{a^2})}{\sqrt[3]{a^2}}) = \frac{\tau(\sqrt[3]{a^2})}{\sqrt[3]{a^2}}$ . Therefore  $\frac{\tau(\sqrt[3]{a^2})}{\sqrt[3]{a^2}}$  is equal to an element  $b$  in  $\mathbb{Q}(\zeta_3)$ . Since  $\tau$  is an involution, it follows that

$$\sqrt[3]{a} = \tau^2(\sqrt[3]{a}) = \tau(b\sqrt[3]{a}) = \tau(b)\tau(\sqrt[3]{a^2}) = \tau(b)b^2\sqrt[3]{a^4} = \tau(b)b^2a\sqrt[3]{a}.$$

Therefore  $a = \frac{1}{\tau(b)b^2} = \tau(\frac{1}{b})(\frac{1}{b})^2$ . Taking  $x, y \in \mathbb{Q}$  so that  $\frac{1}{b} = x + \zeta_3y$ , we see that  $a = (x + \zeta_3y)^2(x + \zeta_3^2y)$ . ■

**Remark 5.3.** That every point in  $T$  is a point of arithmetic descent is a rephrasing of an observation in [Alb37], which, together with its generalization in [Mik78], applies to every power of an odd prime. Those results, together with an analogous result for powers of 2 (first appearing in [Sue81]), are summarized neatly in Section 2 of [Sal82] (and in particular Theorems 2.3 and 2.4).

The reverse direction does not appear in these papers, but is most closely related to Theorem 2.3.b in [Sal82]. Indeed, following the proof one sees that Saltman proves a slightly stronger statement than Theorem 2.3.b. Namely, in his notation, he proves that  $a^k$  is in the image of  $M_\tau$ . In the situation of Theorem 2.3, if  $q = 3$  then it's possible to choose  $m = 2$ , in which case  $k = 1$ , and the proposition above follows.

Throughout this section, we let  $g(x, y) = (x + \zeta_3y)^2(x + \zeta_3^2y)$ . By proposition 5.2, if  $g(x, y) = 3(z^3 + 2)$  has no solution where  $x, y \in \mathbb{Q}$  and  $z \in \mathbb{Q}(\zeta_3)$ , then the cover  $t^3 = 3(z^3 + 2)$  has no  $\mathbb{Q}(\zeta_3)$ -rational point of arithmetic descent, except possibly at infinity. We shall prove that this is the case by showing that this equation has no solution in the completion at the unique prime  $(\pi)$  above  $(3)$  in  $\mathbb{Q}(\zeta_3)$ , where  $\pi = 1 + 2\zeta_3$ .

We first collect the requisite technical lemmas.

**Lemma 5.4.** *Let  $x$  and  $y$  be elements in  $\mathbb{Z}$  such that  $\pi$  divides  $g(x, y) = (x + \zeta_3 y)^2(x + \zeta_3^2 y)$ . Then  $\pi$  divides both  $(x + \zeta_3 y)$  and  $(x + \zeta_3^2 y)$ . Moreover, there exist  $x', y' \in \mathbb{Z}$  such that  $g(x', y') = g(x, y)/\pi^3$ .*

**Proof.** The first part of the lemma follows easily from the fact that  $\mathbb{Z}[\zeta_3]$  is a PID, and that  $x + \zeta_3^2 y$  is the Galois conjugate of  $x + \zeta_3 y$ .

Let  $N : \mathbb{Q}(\zeta_3) \rightarrow \mathbb{Q}$  denote the field norm. For any  $a, b \in \mathbb{Z}$ , we have that  $g(a, b) = (a + \zeta_3 b)N(a + \zeta_3 b)$ . Since  $\pi$  divides  $g(x, y)$ , by the first part of this lemma  $\pi$  divides  $(x + \zeta_3 y)$ . Therefore, there exist  $x', y' \in \mathbb{Z}$  such that  $(x' + \zeta_3 y') = -(x + \zeta_3 y)/\pi$ . We have that

$$\begin{aligned} g(x', y') &= (x' + \zeta_3 y')N(x' + \zeta_3 y') = \frac{-(x + \zeta_3 y)}{\pi} \cdot \frac{N(-1)N(x + \zeta_3 y)}{N(\pi)} \\ &= \frac{-(x + \zeta_3 y)N(x + \zeta_3 y)}{-\pi^3} = \frac{g(x, y)}{\pi^3}, \end{aligned}$$

proving the second part of the lemma. ■

A key step in the proof of theorem 5.1 is reducing the question of finding solutions to  $g(x, y) = 3(z^3 + 2)$  to finding solutions in the finite ring  $\mathbb{Z}[\zeta_3]/(81)$ . After this reduction, we shall make use of the following two lemmas.

**Lemma 5.5.** *Consider  $g(x, y)$  as a polynomial in  $(\mathbb{Z}[\zeta_3]/(81))[x, y]$  and fix  $c \in \mathbb{Z}[\zeta_3]/(81)$ . Then the set  $\{c^3 \cdot g(x, y) \mid x, y \in \mathbb{Z}/(81)\}$  is contained in  $\{g(x, y) \mid x, y \in \mathbb{Z}/(81)\}$ .*

**Proof.** This is a finite checking problem. We implemented an algorithm in SAGE [S<sup>+</sup>14] which verifies this result. The interested reader may consult [EH14] for the code. ■

**Lemma 5.6.** *The equation  $g(x, y) = 3(z^3 + 2)$  has no solution with  $x, y \in \mathbb{Z}/(81)$  and  $z \in \mathbb{Z}[\zeta_3]/(81)$ .*

**Proof.** This is also a finite checking problem, which we again verify using SAGE [S<sup>+</sup>14]. The interested reader may consult [EH14] for the code. ■

We remark that we reduce modulo 81 since it is the first power of 3 for which lemma 5.6 holds. Equipped with the above lemmas, we can now prove the main result of this section.

**Proof of theorem 5.1.** By the discussion at the beginning of this section, we need to show that there is no solution to  $g(x, y) = 3(z^3 + 2)$  where  $x, y \in \mathbb{Q}$  and  $z \in \mathbb{Q}(\zeta_3)$ , and in addition we need to show that the point at infinity does not arithmetically descend to  $\mathbb{Q}$ .

Assume by contradiction that we have such a solution to  $g(x, y) = 3(z^3 + 2)$ . Let  $x = x_0/x_1, y = y_0/y_1$ , and  $z = z_0/z_1$ , where  $x_i, y_i \in \mathbb{Z}$  and  $z_i \in \mathbb{Z}[\zeta_3]$ . Clearing denominators, we have that  $(z_1)^3 g(x_0 y_1, y_0 x_1) = 3((z_0 x_1 y_1)^3 + 2(x_1 y_1 z_1)^3)$ . Therefore it suffices to show that there is no solution to the equation

$$a^3 g(x, y) = 3(z^3 + 2c^3) \tag{5.1}$$

with  $x, y \in \mathbb{Z}, z \in \mathbb{Z}[\zeta_3]$ , and non-zero  $a, c \in \mathbb{Z}[\zeta_3]$ .

Case 1:  $\pi$  does not divide  $c$ . Reduce eq. (5.1) modulo  $(81) = (\pi)^8$ . We denote the reduction by the use of bars over the elements. Since  $\pi$  does not divide  $c$ ,  $\bar{c}^3$  is a unit in  $\mathbb{Z}/(81)$  and so we may divide by it. Letting  $z' = \bar{z}/\bar{c}$ , the resulting equation may be written as  $(\bar{a}/\bar{c})^3 g(\bar{x}, \bar{y}) = 3((z')^3 + 2)$ . Since  $(\bar{a}/\bar{c})^3$  is a cube, there are  $x', y' \in \mathbb{Z}/(81)$  such that  $g(x', y') = (\bar{a}/\bar{c})^3 g(\bar{x}, \bar{y})$  by lemma 5.5. Therefore  $g(x', y') = 3((z')^3 + 2)$ , in contradiction to lemma 5.6.

Case 2:  $\pi$  divides  $c$ . From this solution we shall produce a solution where  $\pi$  does not divide  $c$ , which we have shown is impossible in Case 1 of the proof. Since  $\pi$  divides the right hand side of eq. (5.1) (because  $\pi$  divides 3), it must divide either  $a$  or  $g(x, y)$ . Due to lemma 5.4, it follows that  $\pi^3$  must divide the left hand side of eq. (5.1). Since  $\pi^3$  does not divide 3,  $\pi$  must divide  $z^3 + 2c^3$ . Since  $\pi$  divides  $z^3 + 2c^3$  and  $c$ , it must also divide  $z^3$ , and therefore  $z$ .

As mentioned,  $\pi$  divides either  $a$  or  $g(x, y)$ . Assume first that  $\pi$  divides  $a$ . In this case, we may divide eq. (5.1) by  $\pi^3$  and get  $(a/\pi)^3 g(x, y) = 3((z/\pi)^3 + 2(c/\pi)^3)$ . Iterating this process yields a solution where either  $\pi$  does not divide  $c$  (in which case we are done by Case 1 of the proof), or  $\pi$  divides  $c$  but not  $a$ .

Therefore, we are left with the case where  $\pi$  divides  $g(x, y)$  but not  $a$ . By lemma 5.4, there are then  $x', y' \in \mathbb{Z}$  such that  $g(x', y') = g(x, y)/\pi^3$ . Dividing both sides of eq. (5.1) by  $\pi^3$  yields the equation  $a^3 g(x', y') = 3((z/\pi)^3 + (c/\pi)^3)$ . By iterating this process, we reduce to the case where  $\pi$  does not divide  $c$ , as desired.

It remains to check that infinity does not arithmetically descend to  $\mathbb{Q}$ . Homogenizing  $t^3 = 3(z^3 + 2)$  with respect to  $w$  gives us  $t^3 = 3(z^3 + 2w^3)$ . This equation defines a smooth curve in  $\mathbb{P}_{\mathbb{Q}(\zeta_3)}^2$ , giving a projective model for the cover. Above infinity (when  $w = 0$ ), the fiber is connected with residue field extension  $\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q}(\zeta_3)$ . If the equation  $g(x, y) = 3$  has no solution where  $x, y \in \mathbb{Q}$ , this field extension does not arithmetically descend to  $\mathbb{Q}$  by proposition 5.2. One checks that  $g(x, y) \in \mathbb{Q}$  precisely when  $y = 0$ . Since  $g(x, 0) = x^3$ , there is no solution to  $g(x, y) = 3$  because 3 is not a cube in  $\mathbb{Q}$ . ■

**Remark 5.7.** theorem 4.1 states that, although this cover has no  $\mathbb{Q}(\zeta_3)$ -rational points of arithmetic descent, there are infinitely many *closed* points which arithmetically descend to  $\mathbb{Q}$ .

**Acknowledgements.** The authors would like to thank Akshay Venkatesh for helpful discussions.

## References

- [Alb37] A.A. Albert, *Modern Higher Algebra*, University of Chicago Press, 1937.
- [Bec89] S. Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, J. Algebra **125** (1989), no. 1, 236–255.
- [EH14] R. Eberhart and H. Hasson, *Sage algorithms*, 2014, <http://www.personal.psu.edu/rde3/arithmeticedescent.html>.
- [FJ05] M. Fried and M. Jarden, *Field arithmetic*, second ed., Ergebnisse Math. series, vol. 11, Springer-Verlag, 2005.
- [Flo04] S. Flon, *Ramification dans le corps des modules*, Ann. Inst. Fourier (Grenoble) **54** (2004), no. 2, 253–293.
- [Har03] D. Harbater, *Patching and Galois theory*, Galois Groups and Fundamental Groups (Leila Schneps, ed.) **41** (2003), 313–424.
- [Has13] H. Hasson, *The prime-to- $p$  part of étale fundamental groups of curves*, arXiv:1209.3693[math.AG] (2013).
- [Has14] H. Hasson, *Minimal fields of definition for Galois action*, arXiv:1310.4287[math.AG] (2014).
- [Mik78] H. Miki, *On Grunwald-Hasse-Wang’s theorem*, J. Math. Soc. Japan **30** (1978), no. 2, 313–325.
- [MM99] G. Malle and B.H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.
- [Obu12] A. Obus, *Fields of moduli of three-point  $G$ -covers with cyclic  $p$ -Sylow, I*, Algebra Number Theory **6** (2012), no. 5, 833–883.
- [Obu13] A. Obus, *Fields of moduli of three-point  $G$ -covers with cyclic  $p$ -Sylow, II*, J. Théor. Nombres Bordeaux **25** (2013), no. 3, 579–633.
- [S<sup>+</sup>14] W.A. Stein et al., *Sage Mathematics Software (Version 6.2.0)*, The Sage Development Team, 2014, <http://www.sagemath.org>.
- [Sal82] D. Saltman, *Generic Galois extensions and problems in field theory*, Adv. in Math. **43** (1982), no. 3, 250–283.
- [Ser08] J.-P. Serre, *Topics in Galois theory*, with notes by Henri Darmon, second ed., Res. Notes Math., vol. 1, A.K. Peters, 2008.
- [Sue81] Y. Sueyoshi, *A note on Miki’s generalization of the Grunwald-Hasse-Wang theorem*, Mem. Fac. Sci. Kyushu Univ. Ser. A **35** (1981), no. 2, 229–234.
- [Völ96] H. Völklein, *Groups as Galois Groups – an introduction*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, 1996.
- [Wew03] S. Wewers, *Three point covers with bad reduction*, J. Amer. Math. Soc. **16** (2003), no. 4, 991–1032 (electronic).

**Addresses:** Ryan Eberhart: Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA;  
 Hilaf Hasson: Department of Mathematics, Stanford University, Palo Alto, CA 94305, USA.

**E-mail:** rde3@psu.edu, hilaf@math.umd.edu

**Received:** 17 February 2015; **revised:** 26 July 2016