Dèbes, P. and Harbater, D.
Osaka J. Math.
58 (2021), 71–101

PRE-GALOIS THEORY

Pierre DÈBES and David HARBATER

(Received June 18, 2019, revised September 11, 2019)

Abstract

We introduce and study a class of field extensions that we call *pre-Galois*; viz. extensions that become Galois after some linearly disjoint Galois base change L/k. Among them are *geometrically Galois* extensions of $\kappa(T)$, with κ a field: extensions that become Galois and remain of the same degree over $\overline{\kappa}(T)$. We develop a pre-Galois theory that includes a Galois correspondence, and investigate the corresponding variants of the inverse Galois problem. We provide answers in situations where the classical analogs are not known. In particular, for every finite simple group G, some power G^n is a geometric Galois group over k, and is a pre-Galois group over k if k is Hilbertian. For every finite group G, the same conclusion holds for G itself ($n = 1$) if $k = \mathbb{Q}^{\mathrm{ab}}$ and G has a weakly rigid tuple of conjugacy classes; and then G is a regular Galois group over an extension of $\mathbb{Q}^{\mathrm{ab}}$ of degree dividing the order of $\mathrm{Out}(G)$. We also show that the inverse problem for pre-Galois extensions over a field k (that every finite group is a pre-Galois group over k) is equivalent to the *a priori* stronger inverse Galois problem over k, and similarly for the geometric vs. regular variants.

1. Introduction

Given a field k, the *inverse Galois problem* over k asks:

(IGP/k): Is every finite group a Galois group over k?

The answer is negative for many fields (e.g., algebraically closed fields, finite fields, and local fields), though the answer is believed to be affirmative for global fields, and more generally for Hilbertian fields. This remains open, however, for global fields, and in particular for $\mathbb{Q}$. The related *regular inverse Galois problem* over k asks:

(RIGP/k): Is every finite group a regular Galois group over k?

Recall that a "regular Galois group over k" is the Galois group of a Galois field extension F of $k(T)$ that is k-regular; i.e., in which k is algebraically closed.

The latter question is conjectured to have an affirmative answer for *all* fields; and if this is the case for a Hilbertian field k, then the question (IGP/k) also has an affirmative answer over k. In fact, most known realizations of simple groups as Galois groups over $\mathbb{Q}$ have been obtained by finding a regular realization of that group over $\mathbb{Q}$, typically by the method of rigidity. An affirmative answer to RIGP is known for fields that are algebraically closed ([21], Corollary 1.5), for complete discretely valued fields ([22], Theorem 2.3, Corollary 2.4), for the field of totally real algebraic numbers [8], its p-adic analogs [9], and more generally for the class of fields that Pop introduced and called "large" (see [26]; these fields

2020 Mathematics Subject Classification. Primary 12F10, 12F12 14H05; Secondary 14H25, 11G99.

The first author was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01). The second author was supported in part by NSF grants DMS-1463733 and DMS-1805439.

are also called “ample”). But in general the problem remains wide open.

In this paper we raise several related but more accessible questions, concerning extensions that become Galois after a base change.

We call a finite field extension $F/k(T)$ *geometrically Galois* if $F \otimes_k \overline{k}$ is a Galois field extension of $\overline{k}(T)$; and in that case we say that $\mathrm{Gal}(F \otimes_k \overline{k}/\overline{k}(T))$ is a *geometric Galois group* over k. Note that $F/k(T)$ is necessarily k-regular and separable. The *geometric inverse Galois problem* asks the following, which is weaker than RIGP/k:

(Geo-IGP/k): Is every finite group a geometric Galois group over k?

Observe that if $F/k(T)$ is geometrically Galois, then there is a finite Galois extension L/k such that $F \otimes_k L$ is an *L-regular* Galois field extension of $L(T)$. This suggests:

Question 1.1. If G is a geometric Galois group over k, for how small an extension L/k is G a regular Galois group over L?

More generally, a field extension E/k will be called *potentially Galois* with *Galois group* G if there is a finite field extension L/k such that

(∗) $E \otimes_k L$ is a Galois field extension of L with Galois group G.

If L can be chosen to be Galois over k, we call E/k *pre-Galois*. In the above situations, we say that G is a *potential Galois group* (resp. *pre-Galois group*) over k, and we also say that the extension E/k is potentially Galois (resp. pre-Galois) *over L*. For example the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is pre-Galois with group C_3, by taking $L = \mathbb{Q}(\zeta_3)$.

The following question, the *pre-inverse Galois problem* over k, naturally arises:

(Pre-IGP/k): Is every finite group a pre-Galois group over k?

Every geometrically Galois extension of $k(T)$ is pre-Galois over $k(T)$ (Proposition 3.1(a)). Also note that every pre-Galois extension of a field k is potentially Galois over k; and every potentially Galois extension of a field k is separable over k.

Our questions and answers concerning these notions are of three types.

1.1. Pre-inverse Galois problems. We give partial answers to the above problems, Geo-IGP and Pre-IGP. We first show that over a Hilbertian field, every finite group is a potential Galois group (Proposition 2.12). Regarding Geo-IGP, we show the following over an arbitrary field k (see Corollary 3.15):
(a) every finite group is the quotient of a geometric Galois group, and
(b) if G is a simple group then some power G^n is a geometric Galois group.
Using Proposition 3.5, if k is Hilbertian then one can deduce the corresponding assertions (a) and (b) for Pre-IGP; i.e., with “pre-Galois group” replacing “geometric Galois group” (see Corollary 3.15).

Under the assumption that the exact sequence $1 \to Z(G) \to G \to \mathrm{Inn}(G) \to 1$ is split, Corollary 2.10 shows that, over an arbitrary field, if G is a pre-Galois group, then it is a Galois group. Under this same assumption (or under the alternative hypothesis that $\mathrm{cd}(k) \leq 1$), Corollary 3.13(c) shows that, over a field k, if G is a geometric Galois group with $\mathrm{Out}(G)$ trivial, then it is a regular Galois group. Even without the above assumptions, Corollary 3.13(b, c) answers Question 1.1, by providing an explicit bound on $[L : k]$.

This has the following consequence, observed to us by J. König: if (Pre-IGP/k) holds (for all finite groups) then (IGP/k) holds (for all finite groups); thus the two problems (Pre-IGP/k) and (IGP/k) are equivalent (Corollary 2.11). Similarly, the two problems (Geo-IGP/k) and (RIGP/k) (for all finite groups) are equivalent (see Remark 3.14).

In the case that $k = \mathbb{Q}^{\mathrm{ab}}$, and G is a finite group with a weakly rigid tuple of conjugacy classes (see Section 3.5), we show in Corollary 3.17 that Geo-IGP and Pre-IGP have affirmative answers for G over k, along with a weak form of RIGP and IGP. A generalization appears at Theorem 3.22.

1.2. Pre-Galois theory. It is easily seen that pre-Galois extensions are not always Galois: e.g., $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is pre-Galois but not Galois. Similary $\mathbb{Q}(T^{1/n})/\mathbb{Q}(T)$ is geometrically Galois but not Galois. We consider these other questions, about how the new Galois properties compare to each other:

Question 1.2. Let k be any field.

(a) Is every finite separable field extension of k potentially Galois?
(b) Is every potentially Galois extension of k pre-Galois?
(c) If every k-regular pre-Galois extension of $k(T)$ geometrically Galois?

We show that the answers to parts (a), (b), and (c) of Question 1.2 are "no" in general, even for Hilbertian fields (see Propositions 2.14, 2.12(b) and 3.1(b)).

We also consider the following questions, which contribute to a "pre-Galois theory":

Question 1.3. Let E/k be any finite separable field extension.

(a) If E/k is pre-Galois, is the pre-Galois group unique?
(b) What are the minimal field extensions (resp. minimal Galois field extensions) L_0/k such that $E \otimes_k L_0$ is a Galois field extension of L_0? Does *every* field extension L/k satisfying condition $(*)$ contain a unique such minimal extension?
(c) If E/k is potentially Galois with group G, is there an analog of the usual Galois correspondence that relates the sub-extensions of E/k to subgroups of G?

We show that the answer to Question 1.3(a) is generally "no" (see Example 2.16). In fact, it is even possible for an extension to be pre-Galois with respect to one group and to be potentially Galois but not pre-Galois with respect to a different group (see Example 2.19); and for an extension of $k(T)$ to be geometrically Galois with respect to one group and to be pre-Galois but not geometrically Galois with respect to a different group (see Example 3.2). But we show that the answer to Question 1.3(a) is "yes", i.e. there is a unique pre-Galois group, if the extension has a pre-Galois group that is simple (see Proposition 2.18). Theorem 2.5 gives an explicit answer to Question 1.3(b). An answer to Question 1.3(c) is given in Proposition 2.21.

1.3. Lifting problems. An open question in Galois theory (called the arithmetic lifting problem or the Beckmann-Black problem) asks whether for every finite Galois extension E/k there is a regular Galois extension $F/k(T)$ such that E/k is obtained by specializing T to some element of k. This is known to hold in some cases (e.g., [1], [2]), and no counterexamples are known. It was shown in [12, Proposition 1.2] that if this conjecture holds for all k, then RIGP also holds over every field. A more accessible question is this:

Question 1.4. Given a finite group G and a Galois field extension E/k of group G, is there a geometrically Galois extension $F/k(T)$ that has group G and that specializes to E/k at some $t_0 \in k$?

An affirmative answer is known for k an ample (large) field such as $\mathbb{Q}_p$ and $k_0((t))$: see [12], [6], [25] (with the difference that in the last two references, it is the original form of the Beckmann-Black problem that is solved). Theorem 3.7 extends this affirmative answer under the weaker assumption that G is the Galois group of a k-regular extension $F/k(T)$ such that the corresponding cover $X \to \mathbb{P}^1$ has a k-rational point above an unbranched point $t_0 \in \mathbb{P}^1(k)$ (this assumption holds in particular if k is ample; see [10, Remark 4.3]). Theorem 3.7 shows further that there is a choice of the geometrically Galois extension $F/k(T)$ in Question 1.4 having the additional property that the constant extension in the Galois closure agrees with the given extension E/k. Remark 3.9(b) discusses the value of this additional conclusion.

Following this introduction, we devote Section 2 to discussing pre-Galois theory over a field k. Then in Section 3, we consider the case of function fields, and in particular extensions that are geometrically Galois.

We thank Joachim König for helpful comments about this manuscript, especially concerning the relationship between the usual inverse problems in Galois theory and the ones that we consider here. We also thank Bob Guralnick for providing several group-theoretical examples and counterexamples to us.

2. Pre-Galois extensions

Section 2.1 introduces and investigates the notions of potentially Galois and pre-Galois extensions. Some first questions from Section 1 are answered in this first subsection. More are answered in Section 2.2 which gives further examples and counterexamples. The analog for potentially Galois extensions of the classical Galois correspondence appears in Section 2.3. Finally Section 2.4 compares our pre-Galois theory with the previously introduced Hopf Galois theory.

2.1. Structure of pre-Galois extensions. Theorem 2.5 and Corollary 2.7 are the main structural conclusions of this subsection. Corollaries 2.9, 2.10, 2.11 provide general implications towards the pre-inverse Galois problem.

Let E/k be a finite extension of fields. Given an overfield L of k (not necessarily algebraic), and a finite group G, we say that E/k is *potentially Galois over L with group G* if $E \otimes_k L$ is a Galois field extension of L of Galois group G; and in this situation, if L/k is a (not necessarily finite) Galois field extension, we say that E/k is *pre-Galois over L with group G*. Note that if E/k is potentially Galois over L then E/k is necessarily separable, since the base change $E \otimes_k L$ is separable over L. So we will restrict attention to finite separable field extensions E/k. There is thus a Galois closure $\widehat{E}$ of E/k.

Given any overfield L/k, we may embed E into a separable closure L^{sep} of L as a k-algebra, and so we may take the compositum of fields EL in L^{sep}. The extension E/k is then potentially Galois over L with group G if and only if the field extension EL/L is Galois with group G (and so this does not depend on the choice of k-embedding $E \hookrightarrow L^{\mathrm{sep}}$).

Also, E/k is potentially Galois over L if and only if EL/L is Galois of degree equal to

$[E : k]$; this equality is equivalent to E and L being linearly disjoint over k. As another equivalent condition, E/k is potentially Galois over L if and only if the automorphism group $\mathrm{Aut}(EL/L)$ is of order equal to $[E : k]$.

Lemma 2.1. *Let E/k be a finite field extension, and let L be an overfield of k.*

(a) *If E/k is potentially Galois over L then the compositum EL contains the Galois closure $\widehat{E}$ of E over k.*

(b) *If E/k is pre-Galois over L then EL/k is Galois.*

Proof. For part (a), the extension E/k is separable and so has a primitive element y_1. Let $p(Y) = \prod_{i=1}^{m}(Y - y_i) \in k[Y]$ be the minimal polynomial of y_1 over k, where $y_i \in \widehat{E}$ and $m = [E : k]$. So $E = k(y_1)$ and $\widehat{E} = k(y_1, \dots, y_m)$. As EL/L is Galois of degree m, $p(Y)$ is irreducible over L and $L(y_1) = EL = L(y_1, \dots, y_d)$, whence $EL = \widehat{E}L$. Thus $EL \supset \widehat{E}$.

Part (b) then follows, using $EL = \widehat{E}L$, since the compositum of Galois extensions is Galois. □

Recall that a subgroup U is a *complement* of another subgroup V in a group Γ if every element $g \in \Gamma$ can be uniquely written as $g = uv$ with $u \in U$ and $v \in V$. If Γ is finite, this is equivalent to asserting that $|\Gamma| = |U| \cdot |V|$ and $U \cap V = \{1\}$. It is also equivalent to U acting freely and transitively on the set of left cosets of Γ modulo V, by left multiplication. The group Γ is then said to be the *Zappa-Szép product* (ZS-product for short) of U and V. If in addition U is normal in G, then the group Γ is the semi-direct product of U and V with V acting on U by conjugation.

Proposition 2.2. *Let E/k be a finite separable field extension. Let N/k be a Galois extension such that $E \subset N$, and let H be an arbitrary subgroup of* $\mathrm{Gal}(N/k)$. *Then the following conditions are equivalent:*

(i) *E/k is potentially Galois over the fixed field N^H of H in N and $N = EN^H$.*

(ii) $\mathrm{Gal}(N/k)$ *is the ZS-product of H and* $\mathrm{Gal}(N/E)$.

Proof. (i) ⇒ (ii): Assume that (i) holds. By $EN^H = N$, together with $E = N^{\mathrm{Gal}(N/E)}$, it follows that $H \cap \mathrm{Gal}(N/E) = \{1\}$. We have

$$|H| = [N : N^H] = [EN^H : N^H] = [E : k].$$

The equality $|\mathrm{Gal}(N/k)| = |\mathrm{Gal}(N/E)| \cdot |H|$ follows.

(ii) ⇒ (i): Assume that (ii) holds. We have in particular

$$|H| = |\mathrm{Gal}(N/k)|/|\mathrm{Gal}(N/E)| = [E : k].$$

Now $E = N^{\mathrm{Gal}(N/E)}$ and $\mathrm{Gal}(N/E) \cap H = \{1\}$; hence $N = EN^H$. Thus EN^H/N^H is Galois with group H, and its degree is equal to $[E : k]$. So E/k is potentially Galois over N^H. □

Proposition 2.3. *Let k, E, N be as in* Proposition 2.2*, and let L be an overfield of k such that $N \subset EL$. Then the restriction map* $\mathrm{res} : \mathrm{Aut}(EL/L) \to \mathrm{Gal}(N/k)$ *identifies the group* $\mathrm{Aut}(EL/L)$ *to a subgroup H of* $\mathrm{Gal}(N/k)$. *Moreover E/k is potentially Galois over L if and only if the equivalent conditions of* Proposition 2.2 *hold.*

Proof. The inclusions $E \subset N \subset EL$ imply that $NL = EL$, and so the restriction map $\mathrm{res} : \mathrm{Aut}(EL/L) \to \mathrm{Gal}(N/k)$ is injective. This proves the first assertion.

Assume that E/k is potentially Galois over L. Then EL/L is Galois and $H = r(\mathrm{Gal}(EL/L))$ is of order $[E : k]$. Set $L_0 = N^H$. The extensions L_0/k and E/k are linearly disjoint since L/k and E/k are linearly disjoint and since $L_0 = N^H \subset (EL)^{\mathrm{Gal}(EL/L)} = L$. Consequently $[EL_0 : L_0] = [E : k] = |H|$. But $EL_0 \subset N$ and $[N : L_0] = |H|$. Therefore $EL_0 = N$ and EL_0/L_0 is Galois (of group H). That is, condition (i) of Proposition 2.2 holds.

Conversely, assume that condition (i) of Proposition 2.2 holds. Then the group $\mathrm{Aut}(EL/L)$, being isomorphic to $H = \mathrm{Gal}(N/N^H) = \mathrm{Gal}(EN^H/N^H)$, has order $[EN^H : N^H] = [E : k]$. By the last equivalence stated prior to Lemma 2.1, it follows that E/k is potentially Galois over L. □

NOTATION 2.4. Let E/k be a finite separable extension, with Galois closure $\widehat{E}/k$. The sets $\mathscr{L}, \mathscr{G}$ and the maps $\mathbb{L}$, $\mathbb{G}$ that are defined below depend on the extension E/k. For simplicity we omit the reference to E/k in the notation.

Write $\mathscr{L}$ for the (possibly empty) set of all overfields L of k such that E/k is potentially Galois over L, and $\mathscr{G}$ for the (possibly empty) set of complements of $\mathrm{Gal}(\widehat{E}/E)$ in $\mathrm{Gal}(\widehat{E}/k)$. Note that if $G \in \mathscr{G}$, then $|G| = [E : k]$.

If $L \in \mathscr{L}$, then for $N = \widehat{E}$, both conditions $E \subset N$ of Proposition 2.2 and $N \subset EL$ of Proposition 2.3 are satisfied (via Lemma 2.1(b) for the latter). It follows from those propositions that the group $\mathbb{G}(L) := \mathrm{res}(\mathrm{Gal}(EL/L))$, with $\mathrm{res} : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(\widehat{E}/k)$ the restriction map, is a complement of $\mathrm{Gal}(\widehat{E}/E)$ in $\mathrm{Gal}(\widehat{E}/k)$; i.e. is in the set $\mathscr{G}$. We thus have a map $\mathbb{G} : \mathscr{L} \to \mathscr{G}$ given by

$$L \mapsto \mathbb{G}(L) = \mathrm{res}(\mathrm{Gal}(EL/L)) \subset \mathrm{Gal}(\widehat{E}/k).$$

By definition E/k is potentially Galois over L with group $\mathbb{G}(L)$.

Theorem 2.5. *Let E/k be a separable field extension of degree d, and let $\widehat{E}/k$ be its Galois closure. Let $\mathscr{L}_{\mathrm{m}} \subset \mathscr{L}$ be the subset of minimal fields L in $\mathscr{L}$.*

(a) *The restriction $\mathbb{G} : \mathscr{L}_{\mathrm{m}} \to \mathscr{G}$ of $\mathbb{G}$ to $\mathscr{L}_{\mathrm{m}}$ is a bijection whose inverse is the map $\mathbb{L} : \mathscr{G} \to \mathscr{L}_{\mathrm{m}}$ defined by $\mathbb{L}(G) = \widehat{E}^G$.*

(b) *For each $L \in \mathscr{L}_{\mathrm{m}}$, we have $L \subset \widehat{E}$, $EL = \widehat{E}$ and the extension E/k is potentially Galois over L with group $\mathbb{G}(L) = \mathrm{Gal}(\widehat{E}/L)$.*

(c) *For every $L \in \mathscr{L}$, there is a unique $L_0 \in \mathscr{L}_{\mathrm{m}}$ such that $L_0 \subset L$; and $L_0 = \mathbb{L}(\mathbb{G}(L))$. The extension EL/L is obtained from EL_0/L_0 by base change. Furthermore, $\mathbb{G}(L) = \mathbb{G}(L_0)$. Finally if L/k is Galois, so is L_0/k, and $\mathbb{G}(L)$ is normal in $\mathrm{Gal}(\widehat{E}/k)$.*

Proof. The proof proceeds in several steps.

First argument. Let $L \in \mathscr{L}$ and $G = \mathbb{G}(L)$. It follows from the definition of $\mathbb{G}(L)$ (Notation 2.4) that $L = (EL)^{\mathrm{Gal}(EL/L)} \supset \widehat{E}^G$. As $\widehat{E}L = EL$ (Lemma 2.1(b)), we obtain that

(*) the extension EL/L is obtained from $\widehat{E}/\widehat{E}^G$ by base change $L/\widehat{E}^G$.

Furthermore, by definition of $\mathscr{G}$, for every $G \in \mathscr{G}$, $\mathrm{Gal}(\widehat{E}/k)$ is the ZS-product of G and $\mathrm{Gal}(\widehat{E}/E)$. It follows from Proposition 2.2 ((ii) ⇒ (i), with $N = \widehat{E}$) that

(**) E/k is potentially Galois over $\widehat{E}^G$ and $\widehat{E} = E\widehat{E}^G$; in particular $\mathbb{G}(\widehat{E}^G) = G$.

Proof that $\mathbb{L}(\mathscr{G}) \subset \mathscr{L}_{\mathrm{m}}$ *and* $\mathscr{G} = \mathbb{G}(\mathscr{L}_{\mathrm{m}})$. Let $G \in \mathscr{G}$. Then $\widehat{E}^G \in \mathscr{L}$ (from (**) above). Now suppose that $L \in \mathscr{L}$ satisfies $L \subset \widehat{E}^G$. We have $EL \subset \widehat{E}$, and as we already know that $EL \supset \widehat{E}$, we obtain $EL = \widehat{E}$. It follows that $\mathbb{G}(L) = \mathrm{Gal}(\widehat{E}/L) \supset G$ and this containment is in fact an equality: $\mathbb{G}(L) = G$, as the groups have the same order d. The first argument then applies and gives $L \supset \widehat{E}^G$. Hence $L = \widehat{E}^G$ and $\widehat{E}^G \in \mathscr{L}_{\mathrm{m}}$. As this holds for every $G \in \mathscr{G}$, we have $\mathbb{L}(\mathscr{G}) \subset \mathscr{L}_{\mathrm{m}}$. Also $G = \mathbb{G}(\widehat{E}^G)$. So since $\widehat{E}^G \in \mathscr{L}_{\mathrm{m}}$ for every $G \in \mathscr{G}$, it follows that $\mathscr{G} \subset \mathbb{G}(\mathscr{L}_{\mathrm{m}})$. As $\mathbb{G}(\mathscr{L}_{\mathrm{m}}) \subset \mathbb{G}(\mathscr{L}) \subset \mathscr{G}$ (Notation 2.4), we obtain $\mathscr{G} = \mathbb{G}(\mathscr{L}_{\mathrm{m}})$.

Proof of (b) and of $\mathscr{L}_{\mathrm{m}} = \mathbb{L}(\mathscr{G})$. For every $L \in \mathscr{L}_{\mathrm{m}}$, the first argument shows that $L \supset \widehat{E}^G$ for some $G \in \mathscr{G}$, and so $L = \widehat{E}^G$ since L and $\widehat{E}^G$ are in $\mathscr{L}_{\mathrm{m}}$. Taking into account (**) above, statement (b) follows immediately. It also follows that $\mathscr{L}_{\mathrm{m}} \subset \mathbb{L}(\mathscr{G})$; but $\mathbb{L}(\mathscr{G}) \subset \mathscr{L}_{\mathrm{m}}$, and so $\mathscr{L}_{\mathrm{m}} = \mathbb{L}(\mathscr{G})$.

Proof of (a). We already know that the maps $\mathbb{L} : \mathscr{G} \to \mathscr{L}_{\mathrm{m}}$ and $\mathbb{G} : \mathscr{L}_{\mathrm{m}} \to \mathscr{G}$ are well-defined and surjective. For every $L \in \mathscr{L}_m$, the equality $\mathbb{G}(L) = \mathrm{Gal}(\widehat{E}/L)$ (proved in (b)) yields $\mathbb{L}(\mathbb{G}(L)) = L$. Finally we know from above that for every $G \in \mathscr{G}$, $\mathbb{L}(G) = \widehat{E}^G \in \mathscr{L}_{\mathrm{m}}$. Statement (b) then gives $\mathbb{G}(\mathbb{L}(G)) = \mathrm{Gal}(\widehat{E}/\mathbb{L}(G)) = G$, completing the proof of (a).

Proof of (c). Let $L \in \mathscr{L}$. The fact that the field $L_0 = \mathbb{L}(\mathbb{G}(L))$ satisfies $L_0 \in \mathscr{L}_{\mathrm{m}}$ and $L_0 \subset L$ was already proved. Assume that there is another $L_0' \in \mathscr{L}_{\mathrm{m}}$ such that $L_0' \subset L$. Write $L_0' = \mathbb{L}(G')$ with $G' \in \mathscr{G}$. It follows from $L_0 = \widehat{E}^{\mathbb{G}(L)} \subset L$ and $L_0' = \widehat{E}^{G'} \subset L$ that

$$\mathbb{G}(L) = \mathrm{res}(\mathrm{Gal}(EL/L)) \subset \mathrm{Gal}(\widehat{E}/\widehat{E}^{\mathbb{G}(L)}) \cap \mathrm{Gal}(\widehat{E}/\widehat{E}^{G'}) = \mathbb{G}(L) \cap G'.$$

As the groups $\mathbb{G}(L)$ and G' have the same order, namely $d = [E : k]$, we have necessarily $\mathbb{G}(L) = G'$ and so $L_0 = L_0'$. The second sentence of statement (c) corresponds to (*) in the first argument. The equality $\mathbb{G}(L_0) = \mathbb{G}(L)$ follows from $\mathbb{G} \circ \mathbb{L} = \mathrm{Id}_{\mathscr{G}}$. Finally, assume that L/k is a Galois extension. Then the field $EL = \widehat{E}L$ is a Galois extension of k; and $L_0 = \mathbb{L}(\mathbb{G}(L))$ is the fixed field in $\widehat{E}L$ of the subgroup $\Gamma \subset \mathrm{Gal}(\widehat{E}L/k)$ that is generated by $\mathrm{Gal}(\widehat{E}L/L)$ and $\mathrm{Gal}(\widehat{E}L/\widehat{E})$. As the extensions $\widehat{E}/k$ and L/k are Galois, both these subgroups are normal in $\mathrm{Gal}(\widehat{E}L/k)$. Therefore so is Γ and hence L_0/k is Galois; equivalently, $\mathbb{G}(L)$ is normal in $\mathrm{Gal}(\widehat{E}/k)$. □

Remark 2.6. We will sometimes use the following facts, contained in Theorem 2.5:

(a) An overfield L of k is in $\mathscr{L}_{\mathrm{m}}$ if and only if it is of the form $L = \mathbb{L}(G)$ for some unique $G \in \mathscr{G}$ (Theorem 2.5(a)), and then $\mathbb{L}(G) \subset \widehat{E}$, $E\mathbb{L}(G) = \widehat{E}$ and the extension E/k is potentially Galois over $\mathbb{L}(G)$ with group $\mathbb{G}(\mathbb{L}(G)) = G$ (Theorem 2.5(b)).

(b) If an extension E/k is potentially or pre-Galois, then by Theorem 2.5(b) it is so over some extension L/k that is contained in the Galois closure $\widehat{E}/k$, with $EL = \widehat{E}$: e.g. any L/k with $L \in \mathscr{L}_{\mathrm{m}}$. (There is in fact no other choice: if $L \in \mathscr{L}$ and $L \subset \widehat{E}$, then $L \in \mathscr{L}_{\mathrm{m}}$. Indeed, from Theorem 2.5(c), if $L \in \mathscr{L}$, then L contains some $L_0 \in \mathscr{L}_{\mathrm{m}}$, which satisfies $EL_0 = \widehat{E}$ (Theorem 2.5(b)); and if $L \subset \widehat{E}$, then $EL = \widehat{E}$. This, combined with $[EL : L] = [EL_0 : L_0]$, gives $L = L_0$).

Corollary 2.7. *Let E/k be a degree d separable extension and $\widehat{E}/k$ be its Galois closure.*

(a) *E/k is potentially Galois (resp. pre-Galois) if and only if* $\mathrm{Gal}(\widehat{E}/k)$ *is the ZS-product of some order d subgroup G and of* $\mathrm{Gal}(\widehat{E}/E)$ *(resp. the semi-direct product of some* *order d normal subgroup G and* $\mathrm{Gal}(\widehat{E}/E)$*); and then E/k is potentially Galois (resp. pre-Galois) of group G.*

(b) *The potential Galois groups (resp. the pre-Galois groups) of E/k are exactly the complements (resp. the normal complements) of* $\mathrm{Gal}(\widehat{E}/E)$ *in* $\mathrm{Gal}(\widehat{E}/k)$*.*

(c) *An extension E/k is pre-Galois if and only it is potentially Galois and one of the minimal extensions $\mathbb{L}(G)/k$ ($G \in \mathscr{G}$) is Galois.*

Proof. (a) With our notation, E/k is potentially Galois if and only if $\mathscr{L} \neq \emptyset$, which, from Theorem 2.5(c), is equivalent to $\mathscr{L}_{\mathrm{m}} \neq \emptyset$, which in turn is equivalent to $\mathscr{G} \neq \emptyset$ by Theorem 2.5(a). This proves the "potentially Galois" part of statement (a). The "pre-Galois" part is proved similarly using the final part of Theorem 2.5(c).

(b) A group G being a potential Galois group (resp. pre-Galois group) means that there is an extension E/k that is potentially Galois (resp. pre-Galois) over L and G is isomorphic to $\mathbb{G}(L)$. Thus (b) straightforwardly follows from (a).

(c) The direct part is straightforward from Theorem 2.5(c). The reverse part is clear. □

Remark 2.8. (a) By Theorem 2.5(a), if $L \in \mathscr{L}_{\mathrm{m}}$, then $L = \mathbb{L}(\mathbb{G}(L))$. If E/k is pre-Galois over L (of group $\mathbb{G}(L)$), the action of $\mathrm{Gal}(L/k)$ on $\mathbb{G}(L)$ is faithful. To see this, note that EL/k is Galois (by Lemma 2.1(b)), and $\mathrm{Gal}(EL/k)$ is a semi-direct product of the normal subgroup $\mathbb{G}(L)$ with the quotient group $\mathrm{Gal}(L/k) = \mathrm{Gal}(EL/E)$. If the action of $\mathrm{Gal}(L/k)$ on $\mathbb{G}(L)$ were not faithful, we could take the invariant subfield in L of the kernel of the action, and that would be a smaller (Galois) extension of k whose pullback makes E/k Galois.

(b) By Theorem 2.5(c), if $L \in \mathscr{L}$ and L/k is Galois (i.e., E/k pre-Galois over L), then the same is true for the corresponding minimal field $L_0 = \mathbb{L}(\mathbb{G}(L)) \in \mathscr{L}_{\mathrm{m}}$. We note however that "Galois" cannot be weakened to "pre-Galois" in this statement; viz., it may happen that L/k is pre-Galois but L_0/k is not. We provide an example in Section 3.3 (see Example 3.10).

Corollary 2.9. *A finite group G is a pre-Galois group over k if and only if there exists a group action $A \to$* $\mathrm{Aut}(G)$ *such that the semi-direct product $G \rtimes A$ is a Galois group over k.*

Proof. ($\Rightarrow$) If G is a pre-Galois group over k, then G is a normal complement of $\mathrm{Gal}(\widehat{E}/E)$ in $\mathrm{Gal}(\widehat{E}/k)$, by Corollary 2.7(b). Thus, with $A := \mathrm{Gal}(\widehat{E}/E)$, we have $\mathrm{Gal}(\widehat{E}/k) = G \rtimes A$, where A acts on G by conjugation in $\mathrm{Gal}(\widehat{E}/k)$.

($\Leftarrow$) Assume $G \rtimes A$ is the group of some Galois extension N/k. For $E = N^A$, the extension E/k satisfies condition (ii) from Proposition 2.2 with $H = G$. Therefore we have condition (i) of that result; in particular E/k is potentially Galois over $L = N^G$. As G is normal in $\mathrm{Gal}(N/k)$, the extension L/k is Galois and E/k is pre-Galois over L, of group G. □

Joachim König observed the following consequences of Corollary 2.9.

Corollary 2.10. *Let G be a finite group such that* $\mathrm{Out}(G)$ *is trivial, and such that the exact sequence* $1 \to Z(G) \to G \to \mathrm{Inn}(G) \to 1$ *is split. If G is a pre-Galois group over a field k, then G is a Galois group over k.*

Proof. By Corollary 2.9, it suffices to show that every semi-direct product $G \rtimes A$ is isomorphic to $G \times A$, since then G is a quotient of the Galois group $G \times A$ and hence itself a Galois group.

Given a semi-direct product $G \rtimes A$, let $\alpha : A \to \mathrm{Aut}(G)$ be the associated action. Since $\mathrm{Out}(G)$ is trivial, $\mathrm{Aut}(G) = \mathrm{Inn}(G)$. Composing the resulting map $A \to \mathrm{Inn}(G)$ with the given section $\mathrm{Inn}(G) \to G$ of $G \to \mathrm{Inn}(G)$, we obtain a homomorphism $\sigma : A \to G$ such that $\alpha(a)(g) = \sigma(a)g\sigma(a)^{-1}$ for $a \in A$ and $g \in G$.

Let $A^* = \{(\sigma(a), a^{-1}) \in G \rtimes A \,|\, a \in A\}$. One checks directly that the map $A \to A^*$ given by $a \mapsto (\sigma(a), a^{-1})$ is an isomorphism; that the subgroups $G \times 1$ and A^* of $G \rtimes A$ commute; that they intersect trivially; and that they generate $G \rtimes A$. Hence $G \rtimes A \cong (G \times 1) \times A^* \cong G \times A$. □

Recall that a group G is said to be *complete* if both $Z(G)$ and $\mathrm{Out}(G)$ are trivial. Symmetric groups S_n with $n \notin \{2, 6\}$ and all automorphism groups of non-abelian simple groups are examples of complete groups [27, Section 13.5.10].

Corollary 2.11. *Let k be an arbitrary field. The following statements are equivalent:*

(i) *Every finite group is a Galois group over k.*

(ii) *Every finite group is a pre-Galois group over k.*

(iii) *Every finite group is a normal subgroup of a Galois group over k.*

(iv) *Every complete finite group is a normal subgroup of a Galois group over k.*

Proof. The implication (i)⇒(ii) is obvious; (ii)⇒(iii) follows from Corollary 2.9; and (iii)⇒(iv) is obvious. We are left with proving (iv)⇒(i).

Let G be a finite group. By [23, Theorem 1], G is a quotient of some complete group $\widetilde{G}$. By (iv), $\widetilde{G}$ is a normal subgroup of some group Γ that is a Galois group over k. Since $\widetilde{G}$ is complete, the exact sequence

$$1 \to \widetilde{G} \to \Gamma \to \Gamma/\widetilde{G} \to 1$$

splits [27, Section 13.5.8] and Γ is isomorphic to a semidirect product $\widetilde{G} \rtimes A$ with $A = \Gamma/\widetilde{G}$. From Corollary 2.9, $\widetilde{G}$ is a pre-Galois group over k. But since $\widetilde{G}$ is complete, this implies that $\widetilde{G}$ is a Galois group over k (Corollary 2.10). It follows that G itself is a Galois group over k. □

2.2. Examples and counterexamples. This section presents in particular our answers to Question 1.2(a)-(b) about the connections between the notions, and to Question 1.3(a) about the uniqueness of the pre-Galois group.

Concerning Pre-IGP, a pre-Galois group G over a field k must satisfy these conditions:
- G is a potential Galois group over k,
- G is a Galois group $\mathrm{Gal}(N/L)$ with L/k a Galois extension.

As parts (a) and (c) of Proposition 2.12 below show, both of these conditions hold for *all* finite groups G, provided that k is a global field, or more generally any Hilbertian field.

We adhere to the definition of a Hilbertian field given in [18, Section 12.1]. Given integers $r, m \geq 1$ and polynomials $f_1(T_1, \ldots, T_r, Y), \ldots, f_m(T_1, \ldots, T_r, Y)$ that are irreducible in $k(T_1, \ldots, T_r)[Y]$ and separable in Y, the set of all $(t_1, \ldots, t_r) \in k^r$ such that $f_i(t_1, \ldots, t_r, Y)$ is irreducible in $k[Y]$, $i = 1, \dots, r$, is called a *separable Hilbert subset* of k^r, and the field k is said to be *Hilbertian* if for every $r \geq 1$, every separable Hilbert subset of k^r is Zariski-dense in k^r. Classical Hilbertian fields include the field $\mathbb{Q}$, the rational function fields $\mathbb{F}_q(u)$ (with u some indeterminate) and all of their finitely generated extensions [18, Theorem 13.4.2].

Recall that S_d is a Galois group over every Hilbertian field. This follows from the fact that S_d is a Galois group over a purely transcendental extension of any field k (viz., the Galois group of $k(x_1, \dots, x_d)/k(\sigma_1, \dots, \sigma_d)$, where σ_i is the i-th elementary symmetric polynomial in $x_1, \dots, x_d$).

Proposition 2.12. *Let k be a Hilbertian field and let G be any finite group.*

(a) *Then G is a potential Galois group over k, and, every extension E/k of degree $d = |G|$ and with Galois closure of group S_d is potentially Galois of group G.*

(b) *If $d \geq 5$, there is a potentially Galois extension of k of degree d, which is not pre-Galois.*

(c) *There is a finite Galois extension L/k such that G is the Galois group of some finite Galois field extension N/L.*

Proof. Let $d \geq 1$ be an integer and N/k a Galois extension of group S_d; this exists by the paragraph before the proposition. Let $M \subset S_d$ be the subgroup fixing one letter; thus M has index d and is isomorphic to S_{d-1}.

(a) Assume N/k is the Galois closure $\widehat{E}/k$ of a given degree d extension E/k. Then E is the fixed field of M in N (for some letter). Let G be any group of order d. Embed it in S_d via the regular representation. The group G is then a complement of M in S_d. By Corollary 2.7(a), the extension E/k is potentially Galois of group G.

(b) Assume $d \geq 5$. Let E be the fixed field of M in the extension N/k. Any complement of M in S_d has order d; but no such subgroup is normal in S_d. Hence E/k is not pre-Galois, by Corollary 2.7(b). But the group M has a (non-normal) complement in S_d, e.g. the group generated by a d-cycle in S_d; and so E/k is potentially Galois, again by Corollary 2.7(b).

(c) With k^{sep} the separable closure of k, the group G is a Galois group over $k^{\text{sep}}(T)$, by the RIGP over separably closed fields (a special case of RIGP over large fields). Hence there is a finite separable extension L/k and a Galois field extension $F/L(T)$ with group G, such that L is algebraically closed in F. After replacing L by its Galois closure over k, we may assume that L/k is Galois. Since k is Hilbertian, it follows that some specialization E/L of $F/L(T)$ is a Galois field extension of L of group G. □

Remark 2.13. As the proof of Proposition 2.12 shows, parts (a) and (b) hold more generally for any field k over which S_d is a Galois group, even if k is not assumed Hilbertian.

Proposition 2.12(a) solves the "potential inverse Galois problem" over a Hilbertian field, and, with Proposition 2.12(c), provides evidence for an affirmative answer to Pre-IGP in that situation. Note that in the case of $k = \mathbb{Q}$, part (c) was shown at [22, Proposition 1.4].

Proposition 2.12(b) shows that Question 1.2(b) has a negative answer.

Concerning Question 1.2(a), every separable extension of degree 2 is Galois and so pre-Galois. Separable extensions of degree 3 either are Galois or have a Galois closure of group S_3, so they are pre-Galois too (Proposition 2.12(a)). Moreover, every separable extension of degree 4 is pre-Galois, by [20, Theorem 4.6] (where it is shown that degree 4 separable extensions are "almost classically Galois"; see Section 2.4 below). Nevertheless, extensions exist that are not potentially Galois, and so the answer to Question 1.2(a) is in general negative, even for Hilbertian fields k:

Proposition 2.14. *Let $d \geq 2$ be an integer such that some simple group of order $2d$ is a Galois group over k. Then there is a degree d separable field extension E/k that is not potentially Galois.*

Proof. Let N/k be a Galois extension of degree $2d$ whose Galois group Γ is simple, and let $\sigma \in \Gamma$ be an element of order 2. As Γ is simple, the extension $E = N^\sigma$ of k is not Galois and its Galois closure is N/k. The group $\mathrm{Gal}(N/E)$ has no complement in Γ (for it would be of index 2). From Corollary 2.7(b), E/k is not potentially Galois. □

So for example, over any Hilbertian field k, there is a separable extension of degree 30 that is not potentially Galois over k, because A_5 is a Galois group over k (every alternating group A_n is classically known to be a regular Galois group over $\mathbb{Q}$ (see [28, Section 4.5]), and so a Galois group over any Hilbertian field of characteristic 0; see [3] for the positive characteristic case).

Remark 2.15. More generally, let E/k be a non-Galois degree d field extension, with Galois closure $\widehat{E}/k$. Suppose that no order d subgroup of $\mathrm{Gal}(\widehat{E}/k)$ has a complement in $\mathrm{Gal}(\widehat{E}/k)$. Then E/k is not potentially Galois over k. In particular, let Γ be a group with a non-trivial subgroup M, and assume that M has no complement in Γ and that no nontrivial subgroup of M is normal in Γ. If Γ is the Galois group of some extension N/k, the extension N^M/k is not potentially Galois. For example, we may take $\Gamma = A_4$, with M of order 2.

Question 1.3(a) also has a negative answer, since a subgroup U of a Galois group $\Gamma = \mathrm{Gal}(E/k)$ can have more than one normal complement up to isomorphism:

Example 2.16. This example was provided to us by R. Guralnick. Let Γ be the dihedral group of order 8, with generators a and b of orders 4 and 2. Let U be the 2-cyclic subgroup generated by b. Let V be the cyclic subgroup generated by a, and let V' be the Klein four subgroup generated by a^2 and ab. The groups V and V' are each complements to U and are normal in Γ, and V is not isomorphic to V'.

Since every finite group Γ is a Galois group over some number field k, one can therefore obtain examples of pre-Galois extensions of k with more than one pre-Galois group.

However, Proposition 2.18 below does provide a uniqueness assertion in a special case. First we need a group-theoretic lemma.

Lemma 2.17. *Suppose G, G' are each normal complements of a subgroup U in a group Γ.*

(a) *For every $g \in G$, there is a unique element $\gamma \in U$ such that $g\gamma \in G'$.*
(b) *Every element of $G/(G \cap G')$ commutes with every element of $G'/(G \cap G')$ (inside the group $\Gamma/(G \cap G')$),*
(c) *The map $\phi : G \to G'$ that sends g to $g\gamma$ is a bijection which satisfies:*
    (i) $\phi(g_1 g_2) = \phi(g_2)^{g_1} \phi(g_1)$ $(g_1, g_2 \in G)$,

(ii) *ϕ is the identity on $G \cap G'$,*

(iii) *ϕ induces an anti-isomorphism $G/(G \cap G') \to G'/(G \cap G')$.*

Proof. (a) Every element $g \in \Gamma$ is uniquely of the form $g = uv$ with $u \in G'$, $v \in U$. Applying this to every $g \in G \subset \Gamma$ gives the assertion.

(b) Let $g \in G$ and $g' \in G'$. As both G and G' are normal in Γ, the commutator $gg'g^{-1}(g')^{-1}$ is in $G \cap G'$, whence the assertion.

(c) If $g_i \in G$ and $\gamma_i \in U$ with $g_i\gamma_i \in G'$ for $i = 1, 2$, then $g_1^{-1}g_2 = \gamma_1\gamma_2^{-1} \in G \cap U = \{1\}$, using that G, U are complements. This shows that ϕ is injective. Hence ϕ is bijective as $|G| = |G'|$. It remains to show assertions (i) – (iii) of (c).

(c)(i) Write $\phi(g_1) = g_1\gamma_1$ and $\phi(g_2) = g_2\gamma_2$. Then we have

$$\phi(g_2)^{g_1}\phi(g_1) = g_1(g_2\gamma_2)g_1^{-1}(g_1\gamma_1) = (g_1g_2)(\gamma_2\gamma_1).$$

As G' is normal in Γ, $\phi(g_2)^{g_1} \in G'$. As $\gamma_2\gamma_1 \in U$, we obtain

$$\phi(g_2)^{g_1}\phi(g_1) = \phi(g_1g_2).$$

(c)(ii) is clear.

(c)(iii) By (c)(i) and (b), it follows that the map $\overline{\phi} : G \to G'/(G \cap G')$ that sends every element $g \in G$ to the coset $\phi(g)(G \cap G')$ satisfies $\overline{\phi}(g_1g_2) = \overline{\phi}(g_2)\overline{\phi}(g_1)$, *i.e.* is an anti-morphism. From (c)(ii), $G \cap G' \subset \ker(\overline{\phi})$. The other containment $G \cap G' \supset \ker(\overline{\phi})$ is clear: if $\phi(g) \in G \cap G'$, there exists $\gamma \in U$ such that $g\gamma \in G \cap G'$; but then $\gamma \in G \cap U$ so $\gamma = 1$ and $g \in G \cap G'$. Therefore $\overline{\phi}$ induces an injective anti-morphism $G/(G \cap G') \to G'/(G \cap G')$, which is bijective as $|G| = |G'|$. □

Proposition 2.18. *Let G be a finite simple group.*

(a) *If G is a normal complement to a subgroup U in a group Γ, then every normal complement of U in Γ is isomorphic to G.*

(b) *Hence if E/k is a pre-Galois extension for which the simple group G is a pre-Galois group, then every pre-Galois group of E/k is isomorphic to G.*

Proof. The second assertion is immediate from the first assertion and Corollary 2.7(b). For the first assertion, let G' be another normal complement of U in Γ. As $G \cap G'$ is normal in G, it follows that $G \cap G' = \{1\}$. Thus there is an anti-isomorphism $\phi : G \to G'$ by Lemma 2.17; and hence the map $\phi^* : G \to G'$ sending each $g \in G$ to $\phi(g)^{-1}$ is an isomorphism. □

As the following example shows, it is possible for a field extension to be pre-Galois with respect to one group, and to be potentially Galois but *not* pre-Galois with respect to a different group. In particular, among the minimal field extensions $\mathbb{L}(G)$ ($G \in \mathscr{G}$), it is possible that one of them is Galois over k and another is not.

Example 2.19. Let $\Gamma = S_4$ and let M be the subgroup of permutations fixing 4; thus M is isomorphic to S_3. The Klein four subgroup G of S_4, generated by the transpositions (1 2) and (3 4), is a normal complement of M. But the cyclic group G' generated by (1 2 3 4) is a non-normal complement of M, and G' is not isomorphic to G. Now let $\widehat{E}/k$ be a Galois field extension of group Γ and let E be the fixed field of M, so that $[E : k] = 4$ and $\widehat{E}$ is the Galois closure of E/k. Let L, L' be the fixed fields in $\widehat{E}$ of G, G', respectively. Then $E \otimes_k L = E \otimes_k L' = \widehat{E}$ is Galois over L with group G, and is Galois over L' with group G'. So E/k is potentially Galois of group G, and of group G'. Furthermore L/k is Galois (as G is normal in Γ), so E/k is pre-Galois of group G. On the other hand, Γ has no normal cyclic subgroup of order 4; in particular, M has no normal cyclic complement (of order 4). So, from Corollary 2.7(a), E/k is not pre-Galois with respect to the cyclic group of order 4. Summarizing, E/k is pre-Galois with respect to the Klein four group, whereas it is potentially Galois but not pre-Galois with respect to the cyclic group of order four.

Given a field k and two finite field extensions E and L of k, if E is Galois over k then the compositum EL is Galois over L. But the corresponding property does not in general hold for potentially Galois extensions, as the next example shows.

Example 2.20. Consider a Galois extension N/k of group S_6. Let H be the subgroup generated by the 6-cycle (1 2 3 4 5 6) and let $E = N^H$ be the fixed field of H in N. The Galois closure of E/k is N/k, and H has a complement in S_6, e.g. the copy of $S_5 \subset S_6$ fixing 6. Hence E/k is potentially Galois, of group S_5.

Next, let $L = N^{A_6}$ be the fixed field of $A_6 \subset S_6$ in N. Then

- $NL = N$ (as $L \subset N$),
- $EL = N^H N^{A_6} = N^{H \cap A_6}$,
- N/EL is Galois, and its Galois group is the order 3 subgroup $H \cap A_6$ generated by the square of (1 2 3 4 5 6).

Thus N/L is the Galois closure of EL/L, and Gal(N/EL) has no complement in the group Gal(N/L) = A_6 (as such a complement would be of order 120 and A_6 has no subgroup of order 120). Therefore EL/L is not potentially Galois, even though E/k is potentially Galois.

2.3. Potential Galois correspondence. As we discuss next, there is an analog of the Galois correspondence for potentially Galois extensions (see Question 1.3(c)).

Let E/k be a degree d potentially Galois extension and L/k be an extension with EL/L Galois of degree d. Let $\widehat{E}$ be the Galois closure of E over k. We produce below a 1-1 correspondence between the set of sub-extensions of E/k and a certain subset of subgroups of the potential Galois group $\mathbb{G}(L) = \mathrm{res}(\mathrm{Gal}(EL/L))$, where res is as before the restriction map $\mathrm{Gal}(EL/L) \to \mathrm{Gal}(\widehat{E}/k)$.

Set $\Gamma = \mathrm{Gal}(\widehat{E}/k)$ and $\Gamma_E = \mathrm{Gal}(\widehat{E}/E)$. Let $\mathrm{Subgp}_\Gamma(\mathbb{G}(L))$ be the set of subgroups $H \subset \mathbb{G}(L)$ such that the product set $H\Gamma_E := \{hg \mid h \in H, g \in \Gamma_E\}$ is a subgroup of Γ (or equivalently, such that $H\Gamma_E = \Gamma_E H$). Let $\mathrm{Subfld}_k(E)$ be the set of subfields of E that contain k. We then define maps between these sets as follows:

- $\varepsilon_L : \mathrm{Subgp}_\Gamma(\mathbb{G}(L)) \to \mathrm{Subfld}_k(E)$, $\varepsilon_L(H) = E^H := E \cap \widehat{E}^H$.
- $\eta_L : \mathrm{Subfld}_k(E) \to \mathrm{Subgp}_\Gamma(\mathbb{G}(L))$, $\eta_L(E'/k) = \mathrm{res}(\mathrm{Gal}(EL/E'L))$. Note that for every sub-extension E'/k of E/k, the extension $EL/E'L$ is Galois of degree $[E : E']$ because E/k is potentially Galois over L; so E/E' is potentially Galois over L.

Proposition 2.21. *Let E/k be a finite field extension that is potentially Galois over L. Let $\widehat{E}$ be the Galois closure of E over k, and set* $\Gamma = \mathrm{Gal}(\widehat{E}/k)$ *and* $\Gamma_E = \mathrm{Gal}(\widehat{E}/E)$. *Then the maps ε_L and η_L as above define a bijective "potential Galois correspondence" between the set of subgroups* $\mathrm{Subgp}_\Gamma(\mathbb{G}(L))$ *and the set of subfields* $\mathrm{Subfld}_k(E)$.

More precisely, for every subfield $E' \in \mathrm{Subfld}_k(E)$ and every subgroup $H \in \mathrm{Subgp}_\Gamma(\mathbb{G}(L))$,

- *$\varepsilon_L(H) = E^H/k$ is a sub-extension of E/k of subdegree equal to $|H|$ (i.e. $[E : E^H] = |H|$),*
- *$\eta_L(E'/k) = \mathrm{res}(\mathrm{Gal}(EL/E'L))$ is a subgroup of $\mathbb{G}(L)$ such that $\eta_L(E'/k)\Gamma_E$ is a subgroup of Γ and is of order $[E : E']$,*
- *$\varepsilon_L \circ \eta_L(E'/k) = E'/k$ and $\eta_L \circ \varepsilon_L(H) = H$.*

Furthermore, if L/k is Galois and H is a characteristic subgroup of $\mathbb{G}(L)$, then $H\Gamma_E$ is a subgroup of Γ and the extension $\varepsilon_L(H) = E^H/k$ is pre-Galois over L, of group $\mathbb{G}(L)/H$.

The proof of Proposition 2.21 starts with this pure group-theoretical lemma.

Lemma 2.22. *Let $\Gamma = GA$ be the ZS-product of two subgroups G and A. There is an index preserving 1-1 correspondence ε between the collection $\mathcal{F}_G(A)$ of subgroups $H \subset G$ such that HA is a subgroup of Γ and the collection $\mathcal{N}_\Gamma(A)$ of the subgroups of Γ that contain A.*

More precisely, this 1-1 correspondence is given by the maps

$$\begin{array}{rccc} \varepsilon : & \mathcal{F}_G(A) & \to & \mathcal{N}_\Gamma(A) \\ & H & \mapsto & HA \end{array} \quad \textit{and} \quad \begin{array}{rccc} \varepsilon^{-1} : & \mathcal{N}_\Gamma(A) & \to & \mathcal{F}_G(A) \\ & H' & \mapsto & G \cap H' \end{array}$$

Proof. For $H \in \mathcal{F}_G(A)$ and $H' \in \mathcal{N}_\Gamma(A)$, we have

$$|\Gamma|/|\varepsilon(H)| = |\Gamma|/|HA| = |G||A|/|H||A| = |G|/|H|$$

and

$$|G|/|\varepsilon^{-1}(H')| = |G|/|G \cap H'| = |GH'|/|H'| = |\Gamma|/|H'|$$

(as $GH' \supset GA = \Gamma$). Thus the maps ε and ε^{-1} preserve the indices.

Now the containment $(G \cap H')A \subset H'$ is clear; and using the above we obtain

$$[\Gamma : H'] = [G : (G \cap H')] = [GA : (G \cap H')A] = [\Gamma : (G \cap H')A].$$

Hence $(G \cap H')A = H'$ and so $\varepsilon^{-1}(H') \in \mathcal{F}_G(A)$.

It is then easily checked that the map $\varepsilon : \mathcal{F}_G(A) \to \mathcal{N}_\Gamma(A)$ and $\varepsilon^{-1} : \mathcal{N}_\Gamma(A) \to \mathcal{F}_G(A)$ are inverse to each other. Namely $\varepsilon \circ \varepsilon^{-1} = \mathrm{Id}$ means that $(G \cap H')A = H'$ for every $H' \in \mathcal{N}_\Gamma(A)$, which has just been checked. And we have $\varepsilon^{-1} \circ \varepsilon = \mathrm{Id}$: if $H \in \mathcal{F}_G(A)$, then $(HA) \cap G = H$; the containment $\supset$ is clear and the converse one easily follows from $G \cap A = \{1\}$. □

Proof of Proposition 2.21. Let $A = \Gamma_E = \mathrm{Gal}(\widehat{E}/E)$. In the notation of Lemma 2.22, $\mathrm{Subgp}_\Gamma(\mathbb{G}(L)) = \mathcal{F}_{\mathbb{G}(L)}(A)$. Note that the group $\Gamma = \mathrm{Gal}(\widehat{E}/k)$ is the ZS-product of $\mathbb{G}(L)$ with A. So Lemma 2.22 applies, and we obtain a bijection $\varepsilon : \mathrm{Subgp}_\Gamma(\mathbb{G}(L)) \to \mathcal{N}_\Gamma(A)$. We will show that the "potential Galois correspondence" of Proposition 2.21 is obtained by composing this bijection with the classical Galois correspondence $\gamma : \mathcal{N}_\Gamma(A) \to \mathrm{Subfld}_k(E)$.

First, for $H \in \mathrm{Subgp}_\Gamma(\mathbb{G}(L))$, we have $\gamma \circ \varepsilon(H) = \widehat{E}^{HA}/k = E^H/k = \varepsilon_L(H)$. Second, to check that $\varepsilon^{-1} \circ \gamma^{-1} = \eta_L$, we introduce the unique $L_0 \in \mathscr{L}$ such that $L_0 \subset L$ (see Theorem 2.5); recall that $\mathbb{G}(L) = \mathbb{G}(L_0)$. For $E'/k \in \mathrm{Subfld}_k(E)$, we have:

$$\varepsilon^{-1} \circ \gamma^{-1}(E'/k) = \varepsilon^{-1}(\mathrm{Gal}(\widehat{E}/E'))$$

$$
\begin{aligned}
&= \mathbb{G}(L) \cap \mathrm{Gal}(\widehat{E}/E') \\
&= \mathbb{G}(L_0) \cap \mathrm{Gal}(\widehat{E}/E') \\
&= \mathrm{Gal}(\widehat{E}/L_0) \cap \mathrm{Gal}(\widehat{E}/E') \\
&= \mathrm{Gal}(\widehat{E}/E'L_0) \\
&= \mathrm{Gal}(EL_0/E'L_0) \\
&= \mathrm{res}(\mathrm{Gal}(EL/E'L)) = \eta_L(E'/k).
\end{aligned}
$$

For the final part of of Proposition 2.21, assume that L/k is Galois. Then the extension E/k is pre-Galois and $\widehat{E}/k$ is Galois of group a semi-direct product $\mathbb{G}(L) \rtimes \Gamma_E$. Being a characteristic subgroup of $\mathbb{G}(L)$ implies for the subgroup H that it is a normal subgroup of $\mathbb{G}(L) \rtimes \Gamma_E$. In particular, $H\Gamma_E$ is a subgroup of Γ. By the above, $\varepsilon_L(H) = E^H/k$ is potentially Galois over L, and so pre-Galois over L (as L/k is Galois), and $E^H L/L$ is Galois of group $\mathbb{G}(L)/H$. □

Corollary 2.23. *Let E/k be a finite field extension that is potentially Galois over L. As above, set $\Gamma = \mathrm{Gal}(\widehat{E}/k)$ and $\Gamma_E = \mathrm{Gal}(\widehat{E}/E)$.*

(a) *The base change correspondence $E'/k \mapsto E'L/L$ yields a 1-1 correspondence between the set* $\mathrm{Subfld}_k(E)$ *and the set of sub-extensions F/L of EL/L such that the product set* $\mathrm{Gal}(EL/F)\,\Gamma_E$ *is a subgroup of* Γ.

(b) *If $L, L' \in \mathscr{L}$, the map $\eta_{L'} \circ \varepsilon_L$ yields a 1-1 correspondence between the two sets* $\mathrm{Subgp}_\Gamma(\mathbb{G}(L))$ *and* $\mathrm{Subgp}_\Gamma(\mathbb{G}(L'))$.

Proof. By the usual Galois correspondence the latter set in (a) is in bijection with the set $\mathrm{Subgp}_\Gamma(\mathbb{G}(L))$. So (a) follows from the 1-1 correspondence between $\mathrm{Subfld}_k(E)$ and $\mathrm{Subgp}_\Gamma(\mathbb{G}(L))$ proved in Proposition 2.21. Part (b) is clear since $\eta_{L'}$ and ε_L are bijective, by Proposition 2.21. (Part (b) can also be deduced from a pure group-theoretical observation: with the notation of Lemma 2.22, if $\Gamma = GA = G'A$ is the ZS-product of G and A, and also of G' and A, then the correspondence $H \mapsto HA \cap G'$ yields a 1-1 correspondence $\mathcal{F}_G(A) \to \mathcal{F}_{G'}(A)$. We leave the details to the reader.) □

2.4. Related conditions. A notion of "Hopf Galois theory" was introduced in [4] and studied further in [20]. That latter paper also considered conditions on field extensions that were more general than being Galois. Given a finite separable field extension E/k and a finite k-Hopf algebra H, they defined a notion of E/k being "H-Galois" (pages 239-240 in [20]), and a more restrictive notion of E/k being "almost classically Galois" (pages 252-253 in [20]).

These two notions can each be formulated in terms of the left multiplication action of $\mathrm{Gal}(\widehat{E}/k)$ on the group $\mathrm{Perm}(\mathcal{S})$ of permutations of the set $\mathcal{S}$ of left cosets of $\mathrm{Gal}(\widehat{E}/k)$ modulo $\mathrm{Gal}(\widehat{E}/E)$. (As before, $\widehat{E}$ denotes the Galois closure of E over k.) Namely, according to [20, Theorem 2.1], E/k is H-Galois for some k-Hopf algebra H if and only if there is a subgroup $G \subset \mathrm{Perm}(\mathcal{S})$ acting freely and transitively on $\mathcal{S}$ and which is normalized by the subgroup $\mathrm{Gal}(\widehat{E}/k) \subset \mathrm{Perm}(\mathcal{S})$ (where the containment is via μ). By [20, Proposition 4.1], E/k is almost classically Galois if and only if the above condition holds for some $G \subset \mathrm{Gal}(\widehat{E}/k)$. The latter condition is strictly stronger than the former, by [20, Corollary 4.4]. For these notions, partial analogs of the usual Galois correspondence were shown (with versions in [4, Theorem 7.6], [20, Section 5], and [7, Section 2]), though they do not include an analog of the usual bijection between normal subgroups and intermediate Galois extensions.

Meanwhile, from our Corollary 2.7(a), E/k is potentially Galois if and only if there is a subgroup $G \subset \mathrm{Gal}(\widehat{E}/k)$ that acts freely and transitively on $\mathcal{S}$ via μ, since this is equivalent to G being a complement to $\mathrm{Gal}(\widehat{E}/E)$ in $\mathrm{Gal}(\widehat{E}/k)$. Thus the condition of being almost classically Galois is a strengthening both of being H-Galois for some H and also of being potentially Galois. Moreover, given a finite separable extension E/k, with Galois closure $\widehat{E}/k$, one of the equivalent conditions for E/k to be almost classically Galois is that $\mathrm{Gal}(\widehat{E}/E)$ has a normal complement G in $\mathrm{Gal}(\widehat{E}/k)$ (see [20, Proposition 4.1]). So by Corollary 2.7(a) above, E/k is almost classically Galois if and only if it is pre-Galois with group G.

By [20, Introduction, Remark 3], it follows that E/k is H-Galois if and only $\mathrm{Spec}(E)$ is a μ-torsor over k, where the finite group scheme μ is $\mathrm{Spec}(H^*)$, and where H^* is the dual Hopf algebra to H. In particular, if E/k is a Galois field extension of group G, then $\mathrm{Spec}(E)$ is a G-torsor, and E/k is H-Galois with H being the group ring kG; moreover, E/k is almost classically Galois. Thus every pre-Galois extension K/k with group G has the property that $\mathrm{Spec}(K)$ is a μ-torsor over k for some twisted form μ of G; but not conversely. Also, every pre-Galois extension is potentially Galois, but not conversely (see Proposition 2.12(b)). Thus

$$E/k \text{ pre-Galois} \Rightarrow E/k \text{ potentially Galois} + \mathrm{Spec}(E) \text{ a torsor},$$

and one can ask whether the converse holds:

Question 2.24. Let E/k be a finite separable field extension and let G be a finite group. If E/k is potentially Galois with group G, and if $\mathrm{Spec}(E)$ is a μ-torsor over k where μ is a twisted form of G, must E/k be pre-Galois with group G?

Example 2.25. Concerning the two hypotheses in Question 2.24 (being potentially Galois, and the spectrum being a torsor), we show by example that neither implies the other. Note that otherwise, Question 2.24 could not have an affirmative answer, given the above comments about the separate converses not holding.

(a) Let $k = \mathbb{Q}$ and let $E = k(\zeta_8) = k(\sqrt[4]{-1})$. Then $\mathrm{Spec}(E)$ is μ_4-torsor, and μ_4 is a twisted form of $\mathbb{Z}/4\mathbb{Z}$. But E/k is a Galois extension with group $(\mathbb{Z}/2\mathbb{Z})^2$; and so for any field extension L/k such that $LE = L \otimes_k E$ is a field, LE/L is also Galois with group $(\mathbb{Z}/2\mathbb{Z})^2$. Hence LE/L is not Galois with group $\mathbb{Z}/4\mathbb{Z}$, and thus E/k is not potentially Galois with group $\mathbb{Z}/4\mathbb{Z}$, even though $\mathrm{Spec}(E)$ is μ_4-torsor.

(b) Let E/k be a potentially Galois extension of degree 5 that is not pre-Galois, as in Proposition 2.12(b). Thus its group is $\mathbb{Z}/5\mathbb{Z}$. If $\mathrm{Spec}(E)$ is a μ-torsor for some form μ of $\mathbb{Z}/5\mathbb{Z}$, then μ is given by an action of the absolute Galois group $\mathrm{Gal}(k)$ of k on $\mathbb{Z}/5\mathbb{Z}$; i.e., by a homomorphism $\mathrm{Gal}(k) \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$. The kernel of that action has index $1, 2$, or 4; and so μ becomes isomorphic to $\mathbb{Z}/5\mathbb{Z}$ over a Galois extension k'/k of degree $1, 2$, or 4. Since k'/k is Galois of degree 5, it follows that k' and E are linearly disjoint over k. So their compositum $k'E/k'$ has degree 5, and is isomorphic to $k' \otimes_k E$. Thus $\mathrm{Spec}(k'E)$ is a $\mu_{k'}$-torsor over k'. But $\mu_{k'}$ is just the constant group $\mathbb{Z}/5\mathbb{Z}$, and so $k'E/k'$ is a $\mathbb{Z}/5\mathbb{Z}$-Galois field extension. That says that E/k is pre-Galois, and that is a contradiction. Hence $\mathrm{Spec}(E)$ is not a μ-torsor over

k for any form μ of $\mathbb{Z}/5\mathbb{Z}$, even though E/k is potentially Galois with group $\mathbb{Z}/5\mathbb{Z}$. (If $\mathrm{Gal}(\widehat{E}/k) = S_5$ or A_5, then one can also see that $\mathrm{Spec}(E)$ is not a μ-torsor over k, or equivalently that E/k is not H-Galois, by [20, Corollary 4.8].)

3. Function field extensions

We now investigate the pre-Galois notion in the context of finite extensions of function fields. Fix an arbitrary field k and a regular projective geometrically irreducible k-variety B of positive dimension, e.g. $B = \mathbb{P}^1_{\mathbb{Q}}$. We indicate the separable closure of k by k^{sep} and its absolute Galois group by $\mathrm{Gal}(k)$.

3.1. Geometrically Galois extensions. Let $F/k(B)$ be a finite separable extension. It is called *k-regular* if $F \cap \overline{k} = k$; and in this case, F is the function field of a geometrically irreducible branched k-cover $X \to B$.

We sometimes view finite k-regular extensions $F/k(B)$ as fundamental group representations $\phi : \pi_1(B \smallsetminus D, t)_k \to S_d$. Here D denotes the branch divisor of the extension $F\overline{k}/\overline{k}(B)$, $t \in B\smallsetminus D$ a fixed *base point*, $\pi_1(B\smallsetminus D, t)_k$ the k-fundamental group of $B\smallsetminus D$ and $d = [F : k(B)]$. We refer to [11] or [16] for more on the correspondence.

Let $\widehat{F}/k(B)$ be the Galois closure of $F/k(B)$. It is easily checked that, for any overfield k' of k, the Galois closure of the extension $Fk'/k'(B)$ is the extension $\widehat{F}k'/k'(B)$ (where the field compositum of $\widehat{F}$ and k' is taken in an algebraic closure of $k'(B)$).

The Galois closure $\widehat{F}/k(B)$ is not k-regular in general. Its constant extension $\widehat{F}\cap\overline{k}$ is called the *constant extension in the Galois closure* of $F/k(B)$ and denoted by $\widehat{k_F}$. By definition, $\widehat{F}/\widehat{k_F}(B)$ is $\widehat{k_F}$-regular; hence $[\widehat{F} : \widehat{k_F}(B)] = [\widehat{F}k' : k'(B)]$ for every overfield k' of $\widehat{k_F}$. Consequently the Galois groups $\mathrm{Gal}(\widehat{F}k'/k'(B))$ with $k' \supset \widehat{k_F}$ are all equal to the same group, called the *monodromy group* of the extension $F/k(B)$ and denoted by G.

Note that $\widehat{k_F} \subset k^{\mathrm{sep}}$, hence $\widehat{k_F} = \widehat{F} \cap k^{\mathrm{sep}}$. Furthermore the extension $\widehat{k_F}/k$ is Galois and $\mathrm{Gal}(\widehat{k_F}/k) \subset \mathrm{Nor}_{S_d}(G)/G$, where $d = [F : k(B)]$ and G is viewed as a subgroup of S_d via the *monodromy action* $G \hookrightarrow S_d$ of G on the $k(B)$-embeddings $F \hookrightarrow \widehat{F}$ [11, Proposition 2.3].

We say that a finite k-regular extension $F/k(B)$ is *geometrically Galois* if the field extension $F\overline{k}/\overline{k}(B)$ is Galois. This generalizes the definition given in the introduction for $B = \mathbb{P}^1_k$. Also note that the condition is equivalent to $Fk^{\mathrm{sep}}/k^{\mathrm{sep}}(B)$ being Galois. Indeed, if $F\overline{k}/\overline{k}(B)$ is Galois, then $\widehat{F}\overline{k} = F\overline{k}$, and it follows from the equalities

$$[\widehat{F}k^{\mathrm{sep}} : k^{\mathrm{sep}}(B)] = [\widehat{F}\overline{k} : \overline{k}(B)] = [F\overline{k} : \overline{k}(B)] = [Fk^{\mathrm{sep}} : k^{\mathrm{sep}}(B)]$$

that $\widehat{F}k^{\mathrm{sep}} = Fk^{\mathrm{sep}}$, and so that $Fk^{\mathrm{sep}}/k^{\mathrm{sep}}(B)$ is Galois. The converse is clear; i.e., if $Fk^{\mathrm{sep}}/k^{\mathrm{sep}}(B)$ is Galois then $F\overline{k}/\overline{k}(B)$ is Galois.

If $F/k(B)$ is geometrically Galois, then the Galois group $\mathrm{Gal}(F\overline{k}/\overline{k}(B))$ is the monodromy group G of $F/k(B)$, of order $d = [F : k(B)]$. For every field $k' \supset \widehat{k_F}$, since $[Fk' : k'(B)] = d$ and $[\widehat{F}k' : k'(B)] = |G|$, it follows that $\widehat{F}k' = Fk'$ and hence $Fk'/k'(B)$ is Galois. Note that if $F/k(B)$ is not itself Galois, then the field extension $\widehat{k_F}/k$ must therefore be non-trivial, and $\widehat{F}/k(B)$ then cannot be k-regular. (See also Remark 3.9(b).) Furthermore, $\mathrm{Gal}(\widehat{k_F}/k) \subset \mathrm{Aut}(G)$; viz., the monodromy action $G \hookrightarrow S_d$ is the regular representation, and $\mathrm{Nor}_{S_d}(G)/G$ is isomorphic to $\mathrm{Aut}(G)$. (See the proof of [11, Proposition 3.1]; see also [24, Theorem 3.2].)

Proposition 3.1. *Let k be a field.*

(a) *Every geometrically Galois extension $F/k(T)$ is pre-Galois: more precisely, for every Galois extension k'/k with $k' \supset \widehat{k_F}$, the extension $F/k(T)$ is pre-Galois over $k'(T)$, and the corresponding pre-Galois group is the monodromy group* $\mathrm{Gal}(F\overline{k}/\overline{k}(T))$.

(b) *The converse of the first assertion in (a) does not hold: there are k-regular pre-Galois extensions of $k(T)$ that are not geometrically Galois.*

(c) *The following partial converse of (a) holds: Consider a k-regular field extension $F/k(T)$ such that there exists a Galois extension $L/k(T)$ such that FL/L is Galois and the extensions $F\overline{k}/\overline{k}(T)$ and $L\overline{k}/\overline{k}(T)$ have no common branch point (and so $F\overline{k}/\overline{k}(T)$ and $L\overline{k}/\overline{k}(T)$ are linearly disjoint). Then the extension $F/k(T)$ is geometrically Galois.*

Part (b) of this result shows that the answer to Question 1.2(c) is in general "no".

Proof. Part (a) follows from the above observation that if $k' \supset \widehat{k_F}$ then $Fk'/k'(T)$ is Galois.

For part (b), take a Galois extension $N/\mathbb{C}(T)$ of group $\mathcal{G} = G \rtimes H$ with H not normal in $\mathcal{G}$ acting on G (such an extension exists as the Inverse Galois Problem is solved over $\mathbb{C}(T)$). For $F = N^H$, $F/\mathbb{C}(T)$ is not Galois and not geometrically Galois either ($\mathbb{C}$ is algebraically closed) but is pre-Galois (Corollary 2.7(a)).

For part (c), by Remark 2.6(b), one may take $L/k(T)$ so that $FL = \widehat{F}$. But then each branch point of $L\overline{k}/\overline{k}(T)$ is a branch point of $\widehat{F\overline{k}}/\overline{k}(T)$ and so is a branch point of $F\overline{k}/\overline{k}(T)$. Therefore $L\overline{k}/\overline{k}(T)$ is unramified everywhere, which gives $L\overline{k} = \overline{k}(T)$ hence $L \subset \overline{k}(T)$. Finally we have $[F\overline{k} : \overline{k}(T)] = [F : k(T)]$ since $F/k(T)$ is k-regular, and $F\overline{k}/\overline{k}(T)$ is Galois since FL/L is already Galois, so $F/k(T)$ is indeed geometrically Galois. □

Although a geometrically Galois extension of $k(T)$ has a unique geometric Galois group (by definition), it can have more than one group when viewed as a pre-Galois extension of $k(T)$, as the following geometric analog of Example 2.16 shows.

Example 3.2. Let $k = \mathbb{Q}$ and $F = \mathbb{Q}(T^{1/4})$. The extension $F/\mathbb{Q}(T)$ is geometrically Galois with group $\mathbb{Z}/4\mathbb{Z}$, since $F/\mathbb{Q}(T)$ becomes Galois with group $\mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}(i)(T)$; and hence it is also pre-Galois with group $\mathbb{Z}/4\mathbb{Z}$. The Galois group Γ of its Galois closure $\widehat{F}/\mathbb{Q}(T)$ is isomorphic to D_8, the dihedral group of order 8. The 4-cyclic subgroup $G = \mathrm{Gal}(F(i)/\mathbb{Q}(i)(T)) \subset \Gamma$ is a normal complement to the 2-cyclic subgroup $\mathrm{Gal}(\widehat{F}/F)$; but the latter group also has a normal complement $G' \cong (\mathbb{Z}/2\mathbb{Z})^2$ in Γ (see Example 2.16). Thus $F/k(T)$ is also pre-Galois over $L = \widehat{F}^{G'}$, with group $(\mathbb{Z}/2\mathbb{Z})^2$. Note that L cannot be of the form $k'(T)$: otherwise $G' = \mathrm{Gal}(Fk'/k'(T))$ would be G, as it contains $\mathrm{Gal}(F\overline{k}/\overline{k}(T)) = G$ and has the same order. (This can also be seen explicitly.)

Remark 3.3. The geometric analog of the situation considered in Section 2.4 is simpler than the one there: An extension of $k(T)$ is geometrically Galois if and only if it is a torsor and it is regular. For the former implication, every geometrically Galois extension is pre-Galois (by Proposition 3.1(a)) and hence a torsor (by the comments in Section 2.4); and it was noted in the Introduction that it is regular. Conversely, suppose that an extension of $F/k(T)$ is a μ-torsor for some finite group scheme μ, and that it is regular. Then F is linearly disjoint from $\overline{k}$ over $k(T)$, and so $F \otimes_k \overline{k}$ is a field and a $\mu_{\overline{k}}$-torsor over $\overline{k}(T)$. But since $\overline{k}$ is algebraically closed, $\mu_{\overline{k}}$ is a constant finite group G. Thus $F \otimes_k \overline{k}$ is a Galois field extension of $\overline{k}(T)$ having group G; and so $F/k(T)$ is geometrically Galois.

3.2. Specialization. In this subsection, we extend classical results about specializing Galois function field extension to our pre-Galois context. In particular, we prove Proposition 3.5 over Hilbertian fields. As in Section 3.1, k is an arbitrary field and B is a regular projective geometrically irreducible k-variety B of positive dimension.

Given a finite k-regular extension $F/k(B)$ and a point $t_0 \in B(k)$ not in the branch divisor D, the specialization F_{t_0}/k of $F/k(B)$ at t_0 is defined as follows: if $\mathrm{Spec}(V)$ is an affine neighborhood (for the Zariski topology) of t_0, which corresponds to some maximal ideal $\mathfrak{p}_{t_0}$ such that $V/\mathfrak{p}_{t_0} = k$ and U is the integral closure of V in F, then F_{t_0} is the k-étale algebra $U \otimes_V V/\mathfrak{p}_{t_0}$ (it does not depend on the affine subset $\mathrm{Spec}(V)$ and is defined up to $k(B)$-isomorphism). If $F/k(B)$ corresponds to the fundamental group representation $\phi : \pi_1(B \setminus D, t)_k \to S_d$ and $s_{t_0} : \mathrm{Gal}(k) \to \pi_1(B \setminus D, t)_k$ is the section associated to t_0, F_{t_0}/k is the étale algebra associated with the map $\phi \circ s_{t_0} : \mathrm{Gal}(k) \to S_d$. The k-algebra F_{t_0} is a field if and only if $\phi \circ s_{t_0}(\mathrm{Gal}(k))$ is a transitive subgroup of S_d.

Proposition 3.4. *Let B be a regular projective geometrically irreducible variety of positive dimension over a field k. Let $F/k(B)$ be a separable degree d extension and $\widehat{F}/k(B)$ be its Galois closure.*

(a) *Assume $F/k(B)$ is potentially Galois of group G. For every point t_0 in $B(k) \setminus D$ such that $[(\widehat{F})_{t_0} : k] = [\widehat{F} : k(B)]$, the extension F_{t_0}/k is a degree d field extension that is potentially Galois of group G. Furthermore F_{t_0}/k is pre-Galois if $F/k(T)$ is.*

(b) *Assume $F/k(B)$ is geometrically Galois of group G and let $\widehat{k}_F/k$ be the constant extension in the Galois closure $\widehat{F}/k(B)$ of $F/k(B)$. For every point $t_0 \in B(k) \setminus D$ such that F_{t_0} is a field and $[F_{t_0}\widehat{k}_F : \widehat{k}_F] = d$, we have the following, where $\widehat{F_{t_0}}/k$ is the Galois closure of F_{t_0}/k:*

  (i) $\widehat{F_{t_0}} = F_{t_0}\widehat{k}_F = (\widehat{F})_{t_0}$.

  (ii) *the extension F_{t_0}/k is pre-Galois over $\widehat{k}_F$ of group G.*

Proof. (a) By Theorem 2.5, there is a sub-extension $L/k(B)$ of $\widehat{F}/k(B)$ such that $\widehat{F} = FL$ and FL/L is Galois with group G; and the Galois group $\mathrm{Gal}(\widehat{F}/k(B))$ is the ZS-product of G and $\mathrm{Gal}(\widehat{F}/F)$.

Let $t_0 \in B \setminus D$ such that $[(\widehat{F})_{t_0} : k] = [\widehat{F} : k(B)]$. Then

- $(\widehat{F})_{t_0}/k$ is a Galois field extension of group $\mathrm{Gal}(\widehat{F}/k(B))$,
- F_{t_0}/k is an extension of degree d,
- $(\widehat{F})_{t_0}/F_{t_0}$ is a Galois field extension of group $\mathrm{Gal}(\widehat{F}/F)$.

It follows that $(\widehat{F})_{t_0}/k$ is a Galois field extension containing F_{t_0}/k and its Galois group is the ZS-product of G and $\mathrm{Gal}((\widehat{F})_{t_0}/F_{t_0})$. By Proposition 2.2, F_{t_0}/k is potentially Galois over the fixed field $((\widehat{F})_{t_0})^G$. If $F/k(B)$ is further assumed to be pre-Galois, the original extension $L/k(B)$ may be assumed to be Galois and then G is normal in $\mathrm{Gal}(\widehat{F}/k(B))$. Hence the extension $((\widehat{F})_{t_0})^G/k$ is Galois as well and F_{t_0}/k is pre-Galois of group G.

(b) It follows from $F\widehat{k}_F = \widehat{F}$ that $F_{t_0}\widehat{k}_F \subset (\widehat{F})_{t_0}$. As $[F_{t_0}\widehat{k}_F : \widehat{k}_F] = d$ and $\mathrm{Gal}((\widehat{F})_{t_0}/\widehat{k}_F) \subset \mathrm{Gal}(\widehat{F}/\widehat{k}_F(T)) = G$, we have $F_{t_0}\widehat{k}_F = (\widehat{F})_{t_0}$ and $F_{t_0}\widehat{k}_F/\widehat{k}_F$ is Galois of group G, *i.e.* assertion (b)(ii) holds. It remains to prove $\widehat{F_{t_0}} = (\widehat{F})_{t_0}$, which we do below.

It follows from $F_{t_0} \subset (\widehat{F})_{t_0}$ that $\widehat{F_{t_0}} \subset (\widehat{F})_{t_0}$. For the other containment $(\widehat{F})_{t_0} \subset \widehat{F_{t_0}}$, since $(\widehat{F})_{t_0} = F_{t_0}\widehat{k}_F$, we have to prove that $\widehat{k}_F \subset \widehat{F_{t_0}}$. Denote by $\phi : \pi_1(B \smallsetminus D, t)_k \to S_d$ the fundamental group representation of $F/k(T)$ and by $s_{t_0} : \mathrm{Gal}(k) \to \pi_1(B \smallsetminus D, t)_k$ the section associated to t_0. Proving $\widehat{k}_F \subset \widehat{F_{t_0}}$ amounts to showing that $\ker(\phi \circ s_{t_0}) \subset \mathrm{Gal}(\widehat{k}_F)$. Let $\tau \in \ker(\phi \circ s_{t_0})$, *i.e.* $s_{t_0}(\tau) \in \ker(\phi)$. Thus $s_{t_0}(\tau)$ fixes $\widehat{F} = F\widehat{k}_F$ and in particular fixes $\widehat{k}_F$. Hence $\tau \in \mathrm{Gal}(\widehat{k}_F)$, which finishes the proof. □

Along the lines of the implication (Regular IGP/k) ⇒ (IGP/k), we have the following result for any Hilbertian field (e.g., a number field), via specialization:

Proposition 3.5. *Let k be a Hilbertian field and let G be a finite group. If G is a pre-Galois group over $k(T)$, then G is a pre-Galois group over k.*

Proof. By hypothesis, there exists a pre-Galois extension $F/k(T)$ of group G. For $B = \mathbb{P}^1$, the set of $t_0 \in k$ such that $[(\widehat{F})_{t_0} : k] = [\widehat{F} : k(B)]$ contains a separable Hilbert subset of k, which is infinite since k is Hilbertian. Using Proposition 3.4(a), we obtain that G is a pre-Galois group over k, namely the pre-Galois group of some specialization F_{t_0}/k of $F/k(T)$. □

Combining Proposition 3.5 with Proposition 3.1(a), we have implications

$$\text{(Geometric IGP}/k) \Rightarrow (\text{Pre-IGP}/k(T)) \Rightarrow (\text{Pre-IGP}/k)$$

for k Hilbertian. These problems offer a natural graduation of inverse Galois theory. Note that the implication (Geometric IGP/k) ⇒ (Pre-IGP/k) can also be seen directly in this situation by using Proposition 3.4(b). Namely, consider the set of $t_0 \in k$ such that F_{t_0} is a field and $[F_{t_0}\widehat{k}_F : \widehat{k}_F] = d$. This set contains a separable Hilbert subset of k, which is necessarily infinite if k is Hilbertian.

3.3. Lifting Problems. We turn to Question 1.4, which is a weakening of the arithmetic lifting problem (or Beckmann-Black problem), in which we ask for a geometrically Galois extension, rather than a regular Galois extension, that lifts a given Galois extension of the field. Theorem 3.7 and Corollary 3.8 provide some answers.

Recall that B is a regular projective geometrically irreducible k-variety.

The definition of the twisted extension $\widetilde{F}^E/k(B)$ appearing in the statement below is recalled in the proof, together with its main properties. For more on twisting, we refer to [16] or in [12] (where a form of Proposition 3.6(c) already appears).

Proposition 3.6. *Let G be a group with trivial center and $F/k(B)$ be a k-regular Galois extension of group G such that the corresponding cover of B has a k-rational point above some point $t_0 \in B(k)$ not in the branch divisor. Let E/k be a Galois extension of group H isomorphic to a subgroup of G. Consider the extension $\widetilde{F}^E/k(B)$ obtained by twisting $F/k(B)$ by E/k.*

(a) *Then the extension $\widetilde{F}^E/k(B)$ is geometrically Galois of group G. Its Galois closure is the extension $FE/k(B)$, which has Galois group $G \times H$.*
(b) *The constant extension in the Galois closure of $\widetilde{F}^E/k(B)$ is E/k.*
(c) *The specialization of $\widetilde{F}^E/k(B)$ at t_0 is the k-étale algebra corresponding to $(G : H)$*

copies of E/k.

Proof. One may assume $H \subset G$. Let $\phi : \pi_1(B \smallsetminus D, t)_k \to G$ be the fundamental group representation of $F/k(B)$ and $\varphi : \mathrm{Gal}(k) \to G$ be a Galois representation of E/k. Write $\mathrm{Perm}(G)$ for the group of permutations of the set G. The twisted extension $\widetilde{F}^E/k(B)$ corresponds to the fundamental group representation $\widetilde{\phi}^E : \pi_1(B \smallsetminus D, t)_k \to \mathrm{Perm}(G)$ given as follows: for each element of $\pi_1(B \smallsetminus D, t)_k$ uniquely written $x\, s_{t_0}(\tau)$ (with $x \in \pi_1(B \smallsetminus D, t)_{k^{\mathrm{sep}}}$, $\tau \in \mathrm{Gal}(k)$ and $s_{t_0} : \mathrm{Gal}(k) \to \pi_1(B \smallsetminus D, t)_k$ the section associated to t_0), we have, for every $g \in G$,

$$\widetilde{\phi}^E(x\, s_{t_0}(\tau))(g) = \phi(x\, s_{t_0}(\tau))\, g\, \varphi(\tau)^{-1} = \phi(x)\, g\, \varphi(\tau)^{-1}$$

(we have $\phi(s_{t_0}(\tau)) = 1$ as there is a k-rational point above t_0).

The extension $\widetilde{F}^E/k(B)$ becomes isomorphic to $F/k(B)$ after scalar extension to k^{sep} (as ϕ and $\widetilde{\phi}^E$ have the same restriction on $\pi_1(\mathbb{P}^1 \smallsetminus \mathbf{t})_{k^{\mathrm{sep}}}$). The same is true *a fortiori* over $\overline{k}$, hence $\widetilde{F}^E/k(B)$ is geometrically Galois of group G. Furthermore, using that $Z(G) = \{1\}$, one easily checks that

$$\ker(\widetilde{\phi}^E) = \ker(\phi) \cap \ker(\varphi),$$

which indeed shows that the Galois closure of $\widetilde{F}^E/k(B)$ is the extension $FE/k(T)$. This proves (a).

The constant extension in the Galois closure of $\widetilde{F}^E/k(B)$ is given by the map $\mathrm{Gal}(k) \to \mathrm{Nor}_{\mathrm{Perm}(G)}(G)/G$ induced on $\mathrm{Gal}(k)$ by $\widetilde{\phi}^E$ (this is detailed in [11, Section 2.8]). Here $G \hookrightarrow \mathrm{Perm}(G)$ is the left-regular representation of G. Then $\mathrm{Nor}_{\mathrm{Perm}(G)}(G)/G$ is the image of G via the right-regular representation of G. Taking into account that $Z(G) = \{1\}$, the map $\mathrm{Gal}(k) \to \mathrm{Nor}_{\mathrm{Perm}(G)}(G)/G$ can be identified to the one sending each $\tau \in \mathrm{Gal}(k)$ to the right multiplication map $g \mapsto g \cdot \varphi(\tau)^{-1}$. Its kernel is the same as the initial representation $\varphi : \mathrm{Gal}(k) \to G$. This proves (b).

Statement (c) follows as well as the specialization of $\widetilde{F}^E/k(B)$ at t_0 corresponds to the map $\widetilde{\phi}^E \circ s_{t_0} : \mathrm{Gal}(k) \to \mathrm{Nor}_{\mathrm{Perm}(G)}(G)$ which also sends each $\tau \in \mathrm{Gal}(k)$ to the right multiplication $g \mapsto g \cdot \varphi(\tau)^{-1}$. The stabilizer of a given $g \in G$ is $\ker(\varphi)$ and the corresponding fixed field is E. □

In particular, we obtain an affirmative answer to Question 1.4 in the above situation:

Theorem 3.7. *Let G be a finite group with trivial center, and let k be a field. Suppose there is a k-regular Galois extension $F/k(T)$ with Galois group G, whose corresponding cover $\pi : X \to \mathbb{P}^1_k$ has an unramified k-point P. Then given a Galois field extension E/k of group $H \subset G$, there exists a geometrically Galois extension $\mathcal{E}/k(T)$, with group G, that specializes to $E^{(G:H)}/k$ at $\pi(P) \in \mathbb{P}^1(k)$, and whose constant extension in the Galois closure is E.*

Proof. This is a special case of Proposition 3.6, with $B = \mathbb{P}^1_k$, and where we let $\mathcal{E} = \widetilde{F}^E$, using that E/K is Galois with group H. □

Even more is known in the case of fields k that are *ample* (*large*). Recall that these are the fields k with the property that every geometrically irreducible k-variety with a smooth k-point has infinitely many such points; they include in particular henselian fields, PAC fields, and totally real and totally p-adic closures of number fields. Namely, for such fields k, given a finite group G and a Galois extension E/k with group $H \subset G$, there is a regular Galois extension $\mathcal{E}/k(T)$ with group G, having specified fiber $E^{(G:H)}/k$ ([6], [25]); in particular, there is an affirmative answer to the arithmetic lifting problem in that situation. Over such fields, concerning Question 1.4, the hypothesis of Theorem 3.7 is satisfied and hence also the conclusion, including the assertion about the constant extension in the Galois closure:

Corollary 3.8. *Let k be an ample (large) field, and let G be a finite group with trivial center. Given a Galois extension E/k of group $H \subset G$, there is a geometrically Galois extension $F/k(T)$ of group G with constant extension E/k in its Galois closure, which specializes to $E^{(G:H)}/k$ at some unbranched point $t_0 \in \mathbb{P}^1(k)$, and such that the corresponding cover has an unramified k-point.*

Proof. By [26] and [10, Remark 4.3], the hypothesis on k implies that there is a k-regular Galois extension $N/k(T)$ of group G (in fact, of any specified Galois group) with a k-rational point above some unbranched point $t_0 \in k$. Thus the result follows from Theorem 3.7. □

Of course the key case above is with $H = G$, where we realize any given Galois extension of k with group G as a fiber of a geometrically Galois extension of $k(T)$.

Remark 3.9. (a) Assume that k is ample (large) and also Hilbertian; e.g., $k = \mathbb{Q}^{\mathrm{tr}}(i)$ with $\mathbb{Q}^{\mathrm{tr}}$ the field of totally real algebraic numbers. Let H be a subgroup of a finite group G with trivial center. Then there exists a geometrically Galois extension $F/k(T)$ of group G with constant extension $\widehat{k_F}/k$ of group H, and whose corresponding cover has an unramified k-point. Indeed consider $N/k(T)$ as in the proof of Corollary 3.8, and similarly take a k-regular Galois extension of group $H \subset G$. Since k is Hilbertian, this latter extension can be specialized to provide a Galois extension E/k of group $H \subset G$. Corollary 3.8 then provides an extension $F/k(T)$ as desired.

(b) In general, given an extension of a field $k(T)$, the extension of constants in the Galois closure is not well understood; and this poses an obstacle for assertions such as the Regular Inverse Galois Problem. The above results give some control over that extension of constants in special cases. It would be desirable to obtain a more general understanding of the field extension $\widehat{k_F}/k$ and its Galois group.

Example 3.10. The following example completes Remark 2.8(b). The extension E/K constructed below is potentially Galois, of group G, over some extension L/K that is pre-Galois, but the corresponding minimal extension $L_0 = \mathbb{L}(G)$ is not pre-Galois over K.

Take $K = k(T)$ with k a field that, as in Remark 3.9(a) above, is ample and Hilbertian. Fix a non-abelian simple group G of order $d \geq 5$ and a nontrivial subgroup $H \subset G$, e.g. $G = A_5$ and $H = \langle(1\,2\,3\,4\,5)\rangle$. The assumptions on k guarantee the existence of a k-regular Galois extension $N/k(T)$ of group S_d whose corresponding cover has an unramified k-rational point, as well as the existence of a Galois extension ε/k of group H (see Remark 3.9(a)).

Let $M \subset S_d$ be the subgroup fixing one letter and let E be the fixed field in N of M; so $E/k(T)$ is of degree d and its Galois closure is $N/k(T)$. By Proposition 2.12(a), $E/k(T)$ is potentially Galois of group G (embedded in S_d via the regular representation). By Theorem 2.5(b), $E/k(T)$ is in fact potentially Galois over $L_0 = \mathbb{L}(G)$. Furthermore we have $L_0 = N^G$ and $N = \widehat{E} = EL_0$. By Corollary 2.7(b) (see also the proof of Proposition 2.12(b)), the extension $E/k(T)$ is not pre-Galois. In particular, $L_0/k(T)$ is not Galois. The next argument shows that $L_0/k(T)$ is not even pre-Galois.

First note that $N/k(T)$ is also the Galois closure of $L_0/k(T)$ (since $L_0 \subset N$; $N/k(T)$ is Galois; and no nontrivial subgroup of G is normal in S_d). By Corollary 2.7(a), if $L_0/k(T)$ were pre-Galois, then G would have a normal complement in $\mathrm{Gal}(N/k(T)) = S_d$. But this is not the case, and so indeed $L_0/k(T)$ is not pre-Galois.

As $L_0 \subset N$, the extension $L_0/k(T)$ is k-regular and the corresponding cover has an unramified k-rational point. One can write $L_0 = k(B)$, with B a smooth projective curve. The extension $N/k(B)$ is k-regular and is Galois of group G; and the corresponding cover has an unramified k-rational point. Thus one may apply Proposition 3.6.

Let $L/k(B)$ be the extension obtained by twisting $N/k(B)$ by ε/k (in the notation of Proposition 3.6, we have $L = \widetilde{N}^{\varepsilon}$). Since G is simple, it follows that $N \cap L = k(B) = L_0$ and so $N/k(B)$ and $L/k(B)$ are linearly disjoint. By construction, $E/k(T)$ and $k(B)/k(T)$ are also linearly disjoint. Therefore $E/k(T)$ and $L/k(T)$ are linearly disjoint, and so $E/k(T)$ remains potentially Galois over L. Recall that, from Theorem 2.5(c), both groups $\mathbb{G}(L) = \mathrm{Gal}(EL/L)$ and $\mathbb{G}(L_0) = \mathrm{Gal}(EL_0/L_0)$ coincide and are equal to G. Note further that the extension $L/k(T)$ is not Galois for otherwise $L_0/k(T)$ would be Galois, again by Theorem 2.5(c).

Finally we show that $L/k(T)$ is pre-Galois. More precisely, we verify below that it is pre-Galois over $\varepsilon(T)$. Note first that, as ε/k is Galois, $\varepsilon(T)/k(T)$ is Galois too. Then, from Proposition 3.6, we have $L\varepsilon(T) = L\varepsilon = N\varepsilon$. This field is a Galois extension of $k(T)$ (hence a Galois extension of $\varepsilon(T)$), as it is the compositum of the two Galois extensions $N/k(T)$ and $\varepsilon(T)/k(T)$. Finally $L/k(T)$ and $\varepsilon(T)/k(T)$ are linearly disjoint since $L \cap \overline{k} = k$ (as a consequence of the k-regularity of $L/k(B)$). Thus $L/k(T)$ is pre-Galois, as asserted.

3.4. A descent result. In this subsection we address Question 1.1 in Corollary 3.13, which we deduce from a more general version, Theorem 3.11. We also prove Corollary 3.15, which concerns the geometric inverse Galois problem discussed in the introduction.

Recall the following useful terminology. Let $\mathcal{F}/k^{\mathrm{sep}}(B)$ be a finite k^{sep}-regular extension.

(a) We say that $\mathcal{F}/k^{\mathrm{sep}}(B)$ *descends to k as a field extension* if there exists a k-regular extension $F/k(B)$ such that $\mathcal{F} = Fk^{\mathrm{sep}}$. If $\mathcal{F}/k^{\mathrm{sep}}(B)$ is Galois, then the extension $F/k(B)$ is geometrically Galois, of group $\mathrm{Gal}(\mathcal{F}/k^{\mathrm{sep}}(B)) = \mathrm{Gal}(\mathcal{F}\overline{k}/\overline{k}(B))$. If in addition $F/k(B)$ is Galois, we say that $\mathcal{F}/k^{\mathrm{sep}}(B)$ *descends to k as a Galois extension*.

(b) Consider the subgroup $M_{\mathrm{m}}(\mathcal{F}/k^{\mathrm{sep}}(B))$ of the absolute Galois group $\mathrm{Gal}(k)$, consisting of all τ such that for every prolongation (equivalently for some prolongation) of τ to a $k(B)$-automorphism $\widetilde{\tau}$ of $k(B)^{\mathrm{sep}}$, there is a $k^{\mathrm{sep}}(B)$-isomorphism $\chi_\tau : \mathcal{F} \to \mathcal{F}^{\tilde{\tau}}$. The fixed field in k^{sep} of the subgroup $M_{\mathrm{m}}(\mathcal{F}/k^{\mathrm{sep}}(B))$ is called *the field of moduli of $\mathcal{F}/k^{\mathrm{sep}}(B)$ as a field extension* (relative to k^{sep}/k) and is denoted by $k_{\mathrm{m}}(\mathcal{F}/k^{\mathrm{sep}}(B))$, or k_{m} for short.

If $\mathcal{F}/k^{\mathrm{sep}}(B)$ is Galois, consider the subgroup $M_G(\mathcal{F}/k^{\mathrm{sep}}(B)) \subset \mathrm{Gal}(k)$, consisting of all $\tau \in \mathrm{Gal}(k)$ such that for every prolongation (equivalently for some prolongation) of τ to a $k(B)$-automorphism $\widetilde{\tau}$ of $k(B)^{\mathrm{sep}}$, there exists a $k^{\mathrm{sep}}(B)$-isomorphism $\chi_\tau : \mathcal{F} \to \mathcal{F}^{\tilde{\tau}}$ such that $\tau\sigma\tau^{-1} = \chi_\tau\sigma\chi_\tau^{-1}$ for every $\sigma \in \mathrm{Gal}(\mathcal{F}/k^{\mathrm{sep}}(B))$. The fixed field in k^{sep} of the subgroup $M_{\mathrm{m}}(\mathcal{F}/k^{\mathrm{sep}}(B))$ is called *the field of moduli of $\mathcal{F}/k^{\mathrm{sep}}(B)$*

as a Galois extension (relative to k^{sep}/k) and is denoted by $k_G(\mathcal{F}/k^{\text{sep}}(B))$, or k_G for short.

If $\mathcal{F}/k^{\text{sep}}(B)$ descends to k in either sense, we have $k_{\text{m}} = k$ and $k_G = k$ respectively. (For more on fields of definition and fields of moduli, see [17], [5], [11], and [14].)

Theorem 3.11. *Assume that the set $B(k)$ of k-rational points of the k-variety B is Zariski-dense. Let $\mathcal{F}/k^{\text{sep}}(B)$ be a k^{sep}-regular extension of degree d and with field of moduli k, $N/k^{\text{sep}}(B)$ its Galois closure, $G = \text{Gal}(N/k^{\text{sep}}(B))$ its monodromy group (also equal to $\text{Gal}(N\overline{k}/\overline{k}(B))$), and $G \hookrightarrow S_d$ the monodromy action associated with $\mathcal{F}/k^{\text{sep}}(B)$.*

(a) *Then $N/k^{\text{sep}}(B)$ descends to k as a field extension, and to k' as a Galois extension, for some Galois extension k' of k whose Galois group is contained in* $\text{Aut}(G)$*.*

(b) *Let k_G be the field of moduli of $N/k^{\text{sep}}(B))$ as a Galois extension. Then k_G/k is Galois, and its Galois group* $\text{Gal}(k_G/k)$ *is a subgroup of* $\text{Nor}_{S_d}(G)/(G\text{Cen}_{S_d}(G))$*. In particular, if $\mathcal{F}/k^{\text{sep}}(B)$ is Galois, then k_G is its field of moduli as a Galois extension, and* $\text{Gal}(k_G/k)$ *is a subgroup of* $\text{Out}(G)$*.*

(c) *Assume further that the exact sequence $1 \to Z(G) \to G \to \text{Inn}(G) \to 1$ is split or that* $\text{cd}(k) \leq 1$*. Then $N/k^{\text{sep}}(B)$ descends to its field of moduli k_G as a Galois extension.*

The fields $\mathbb{Q}^{\text{ab}}$ and $\overline{k}(T)$ are typical examples for which $\text{cd}(k) \leq 1$.

Proof. We begin with part (a). As N is the compositum of all the $k^{\text{sep}}(B)$-conjugates of $\mathcal{F}$, it follows from the field of moduli of $\mathcal{F}/k^{\text{sep}}(T)$ being k that $N^{\tilde{\tau}} = N$ for every prolongation $\tilde{\tau}$ to N of every $\tau \in \text{Gal}(k)$. This means that the field of moduli of $N/k^{\text{sep}}(B)$ as a field extension is k. The first conclusion of (a) follows then from [5, Proposition 2.5], which says that this extension descends to its field of moduli k. (The cited result was originally stated with $B = \mathbb{P}^1_{\mathbb{Q}}$, where $\overline{k}(B) = \overline{\mathbb{Q}}(T)$. But the proof extends to more general fields k and varieties B such that B has a k-point where the cover corresponding to N is not branched; see [11, Section 2.9 and Corollary 3.4].)

As to the second conclusion of (a), it rests on the standard fact (recalled at the beginning of Section 3.1) that if a k-regular extension $N_0/k(B)$ induces $N/k^{\text{sep}}(B)$, then $N_0/k(B)$ becomes Galois after extending scalars from k to $\widehat{k}_{N_0}$ and that $\text{Gal}(\widehat{k}_{N_0}/k) \subset \text{Aut}(G)$.

For (b), we view k-regular extensions of $k(B)$ as fundamental group representations. Recall that we have the *fundamental group exact sequence*

$$(*) \qquad 1 \to \pi_1(B \smallsetminus D, t)_{k^{\text{sep}}} \to \pi_1(B \smallsetminus D, t)_k \to \text{Gal}(k) \to 1$$

and each point $t_0 \in B(k) \smallsetminus D$ provides a section $\mathsf{s}_{t_0} : \text{Gal}(k) \to \pi_1(B \smallsetminus D, t)_k$.

The extension $\mathcal{F}/k^{\text{sep}}(B)$ corresponds to a transitive homomorphism $\phi_{k^{\text{sep}}} : \pi_1(B \smallsetminus D, t)_{k^{\text{sep}}} \to S_d$ with $d = [\mathcal{F} : k^{\text{sep}}(B)]$. Furthermore the Galois closure $N/k^{\text{sep}}(B)$ corresponds to the epimorphism $\phi_{k^{\text{sep}}} : \pi_1(B \smallsetminus D, t)_{k^{\text{sep}}} \to G$ and we have $G = \phi_{k^{\text{sep}}}(\pi_1(B \smallsetminus D, t)_{k^{\text{sep}}})$.

Fix a point $t_0 \in B(k) \smallsetminus D$. Since k is the field of moduli of $\mathcal{F}/k^{\text{sep}}(B)$, there is a natural map

$$\overline{\varphi} : \pi_1(B \smallsetminus D, t)_k \to \text{Nor}_{S_d}(G)/\text{Cen}_{S_d}(G)$$

such that for each $\tau \in \text{Gal}(k)$,

$$\phi_{k^{\text{sep}}}(x^{\mathsf{s}_{t_0}(\tau)}) = \phi_{k^{\text{sep}}}(x)^{(\overline{\varphi} \circ \mathsf{s}_{t_0})(\tau)} \text{ for all } x \in \pi_1(B \smallsetminus D, t)_{k^{\text{sep}}}.$$

(See [11, Section 2.7]; there this map is called the "representation of $\pi_1(B \setminus D, t)_k$ modulo $\mathrm{Cen}_{S_d}(G)$ given by the field of moduli condition".) Consider the subgroup

$$H = (\overline{\varphi} \circ \mathsf{s}_{t_0})^{-1}(G\mathrm{Cen}_{S_d}(G)/\mathrm{Cen}_{S_d}(G)) \subset \mathrm{Gal}(k).$$

Its fixed field in k^{sep} is the field of moduli k_G of $N/\overline{k}(B)$ as a Galois extension (see [11, Section 2.7]).

As H is normal in $\mathrm{Gal}(k)$, the extension k_G/k is Galois. More precisely, H is the kernel of the map $\overline{\varphi} \circ \mathsf{s}_{t_0}$ composed with the canonical surjection $\mathrm{Nor}_{S_d}(G)/\mathrm{Cen}_{S_d}(G) \to \mathrm{Nor}_{S_d}(G)/(G\mathrm{Cen}_{S_d}(G))$. This yields the desired embedding of $\mathrm{Gal}(k_G/k) \simeq \mathrm{Gal}(k)/H$ into $\mathrm{Nor}_{S_d}(G)/G\mathrm{Cen}_{S_d}(G)$. In the special case that $\mathcal{F}/k^{\mathrm{sep}}(B)$ is Galois, the monodromy action $G \to S_d$ is the regular representation, and the group $\mathrm{Nor}_{S_d}(G)/(G\mathrm{Cen}_{S_d}(G))$ from the general case is simply $\mathrm{Out}(G)$ (e.g., see the proof of [11, Proposition 3.1]).

We next turn to part (c). The assumption in this part implies that the field of moduli k_G of $N/k^{\mathrm{sep}}(B)$ is a field of definition as a Galois extension, by Corollary 3.2 and Corollary 3.4 (or Main Theorem III(b)) of [11]. □

Remark 3.12. (a) Note that [11, Corollary 3.4] (used above) assumed that the fundamental group exact sequence (∗) splits; a condition called (Seq/Split) there. That assumption is satisfied here, as a consequence of our assumption that $B(k)$ is Zariski-dense; so [11, Corollary 3.4] does apply. Our assumption on $B(k)$ also guarantees that for every branched cover of B there are k-points of B outside the branch locus; and so we can use [5, Proposition 2.5]. But to be able to cite [11, Corollary 3.4], the density assumption may be replaced by the weaker condition (Seq/Split).

(b) A weaker form of Theorem 3.11(b) appeared in a paper of H. Hasson, saying that $\mathrm{Gal}(k_G/k)$ is a subquotient of $\mathrm{Aut}(G)$; see [24, Corollary 3.8].

(c) The proof of Theorem 3.11(b) used that $\mathrm{Nor}_{S_d}(G)/(G\mathrm{Cen}_{S_d}(G)) = \mathrm{Out}(G)$ if $G \hookrightarrow S_d$ is the regular representation. More generally, for any embedding $G \hookrightarrow S_d$, there is a natural monomorphism $\mathrm{Nor}_{S_d}(G)/G\mathrm{Cen}_{S_d}(G) \hookrightarrow \mathrm{Out}(G)$; so $|\mathrm{Nor}_{S_d}(G)/G\mathrm{Cen}_{S_d}(G)|$ divides $|\mathrm{Out}(G)|$. This is not an equality in general: e.g., if $G = A_6$ and $G \hookrightarrow S_6$ is given by the containment $A_6 \subset S_6$, then $\mathrm{Nor}_{S_6}(G) = S_6$ and $\mathrm{Cen}_{S_6}(G) = \{1\}$; so $|\mathrm{Nor}_{S_6}(G)/G\mathrm{Cen}_{S_6}(G)| = 2$ whereas $|\mathrm{Out}(G)| = 4$.

Corollary 3.13. *Let G be a finite group and k an arbitrary field.*

(a) *Then G is a geometric Galois group over k if and only if G is the monodromy group of a k^{sep}-regular extension $\mathcal{F}/k^{\mathrm{sep}}(T)$ that has field of moduli k (as a field extension).*

(b) *If G is a geometric Galois group over k, then G is a regular Galois group over some Galois extension of k of degree dividing* $|\mathrm{Aut}(G)|$.

(c) *Let G be a geometric Galois group over k, and suppose that the exact sequence* $1 \to Z(G) \to G \to \mathrm{Inn}(G) \to 1$ *is split or that* $\mathrm{cd}(k) \leq 1$. *Then G is a regular Galois group over some Galois extension of k of degree dividing* $|\mathrm{Out}(G)|$. *Consequently, if in addition* $\mathrm{Out}(G)$ *is trivial, then G is a regular Galois group over k.*

Proof. The condition that the group G is a geometric Galois group over k means that there is a k-regular extension $F/k(T)$ such that $F\overline{k}/\overline{k}(T)$ is Galois of group G; or equivalently, as remarked in Section 3.1, such that $Fk^{\mathrm{sep}}/k^{\mathrm{sep}}(T)$ is Galois of group G.

For the forward implication in part (a), the asserted conclusion holds with $\mathcal{F} = Fk^{\mathrm{sep}}$. The reverse implication in part (a) and the assertion in part (b) follow from Theorem 3.11(a). We obtain part (c) from Theorem 3.11(b,c). □

Remark 3.14. (a) Corollary 3.13 has the following consequence, which can be compared to Corollary 2.11: given a field k, the statements that all finite groups are geometric Galois groups over k and that all finite groups are regular Galois groups over k are equivalent. Namely, let G be a finite group. By [23, Theorem 1], G is a quotient of some complete group $\widetilde{G}$. If all finite groups are geometric Galois groups over k, then $\widetilde{G}$ is. By Corollary 3.13, $\widetilde{G}$ is a regular Galois group over k. It follows that G is a regular Galois group over k as well.

(b) Remark (a) above suggests a possible strategy for attacking the RIGP. Given a finite group G and an integer $r \geq 1$, there is a moduli space in characteristic zero for the Galois branched covers of $\mathbb{P}^1$ with r branch points whose Galois group is isomorphic to G. (E.g., see [5, Section 1], where this *Hurwitz space* is denoted by $\widetilde{\mathcal{P}}$; and [19, Section 1.2], where it is denoted by $\mathcal{H}_r^{\mathrm{ab}}(G)$.) For k an extension of $\mathbb{Q}$, a k-rational point on this space corresponds to a Galois extension of $\overline{k}(T)$ with group G whose field of moduli as a field extension is contained in k; or equivalently (by Theorem 3.11(a)) to a geometrically Galois extension of $k(T)$ with group G. If for *every* finite group G there is a k-point on $\mathcal{H}_r^{\mathrm{ab}}(G)$ for some r depending on G, then Remark (a) implies that every finite group is a regular Galois group over k. (Compare this with [19, Theorem 1], which considers a related Hurwitz space $\mathcal{H}_r^{\mathrm{in}}(G)$, parametrizing pairs consisting of a cover as above together with an isomorphism of its Galois group with G. It shows that a point on $\mathcal{H}_r^{\mathrm{in}}(G)$ corresponds to a Galois extension of $\overline{k}(T)$ with group G whose field of moduli as a Galois extension contains k; and hence to a Galois extension of $k(T)$ with group G if G has trivial center.)

Corollary 3.15. *Let k be a field and G be a finite group.*

(a) *Then G is a quotient of some geometric Galois group over k. Hence if k is Hilbertian, G is also a quotient of a pre-Galois group over k.*

(b) *If G is a simple group, then some power G^n is a geometric Galois group over k. Hence if k is Hilbertian, G^n is a pre-Galois group over k.*

Proof. The RIGP property holds over the field k^{sep} by [26], since that field is ample (large); if k is perfect it also follows from [21, Corollary 1.5] since then $k^{\mathrm{sep}} = \overline{k}$. Thus there exists a k^{sep}-regular Galois extension $F/k^{\mathrm{sep}}(T)$ of group G. Consider the algebraic extension $F/k(T)$ and denote its Galois closure by $\mathcal{F}/k(T)$. The extension $\mathcal{F}/k^{\mathrm{sep}}(T)$ is finite and Galois, say of group $\mathcal{G}$. As $F/k^{\mathrm{sep}}(T)$ is Galois, G is a quotient of $\mathcal{G}$. Furthermore, as $\mathcal{F}/k(T)$ is Galois, the field of moduli of $\mathcal{F}/k^{\mathrm{sep}}(T)$ as a field extension is k.

For the first assertion of part (a), note that Theorem 3.11(a) yields that $\mathcal{F}/k^{\mathrm{sep}}(T)$ descends to a field extension $\mathcal{F}_0/k(T)$ defined over k. By construction $\mathcal{F}_0/k(T)$ is geometrically Galois of group $\mathcal{G}$ and G is a quotient of $\mathcal{G}$.

For the first assertion of (b), assume that G is simple. We may assume that G is nonabelian, since every cyclic group of prime order is the Galois group of a k-regular Galois extension of $k(T)$.

Since F is defined over E for some finite extension E/k, there are finitely many distinct conjugate fields F^σ of F over $k(T)$, as σ ranges over $\mathrm{Gal}(k)$. The field $\mathcal{F}$ is the compositum of these fields F^σ in $\overline{k(T)}$.

We claim that $\mathcal{G} = \mathrm{Gal}(\mathcal{F}/k^{\mathrm{sep}}(T))$ is of the form G^n. This follows by induction from the following elementary assertion: If L_1, L_2 are Galois field extensions of a field K with Galois groups G_1, G_2 such that G_1 is simple, and if L_1 is not contained in L_2, then $\mathrm{Gal}(L_1L_2/K) = G_1 \times G_2$. (This last assertion holds because the simplicity of G_1 implies that $L_1 \cap L_2 = K$).

By Corollary 3.13(a), it then follows that G^n is a geometric Galois group over k.

The last assertions in parts (a) and (b), for k Hilbertian, follow by Proposition 3.5. □

3.5. Extensions $\mathcal{F}/\bar{k}(T)$ with field of moduli k. The notion of rigidity has been used to realize many finite groups as Galois groups over $\mathbb{Q}$, or over small extensions of $\mathbb{Q}$. In this subsection we generalize that notion and apply Theorem 3.11 in order to obtain sharper results along those lines, and to obtain results about geometric Galois groups and pre-Galois groups, in Theorem 3.22. Here we work over subfields k of $\mathbb{C}$, so that we can rely on the correspondence between branched covers and tuples of elements, given by Riemann's Existence Theorem.

Definition 3.16. Let $\mathbf{C} = (C_1, \dots, C_r)$ be a tuple of conjugacy classes of a finite group G. We say that $\mathbf{C}$ is *weakly rigid with respect to an embedding $G \hookrightarrow S_d$* if

(a) there are generators $g_1, \dots, g_r$ of G with $g_1 \cdots g_r = 1$ and $g_i \in C_i$, $i = 1, \dots, r$, and

(b) if $g_1', \dots, g_r'$ are generators of G with the same properties, there exists $\omega \in S_d$ such that $g_i' = \omega g_i \omega^{-1}$, $i = 1, \dots, r$.

In the special case where $G \hookrightarrow S_d$ is the regular representation, this is equivalent to the traditional notion of being *weakly rigid*, in which the conclusion of part (b) is replaced by the condition that for each choice of $g_1', \dots, g_r'$ there exists $\sigma \in \mathrm{Aut}(G)$ such that each $\sigma(g_i)$ equals g_i'. (See [29, Def. 2.15]. If in addition σ is an inner automorphism of G, i.e. if ω is in the image of G, then the tuple is *rigid*.) When that narrower condition of weak rigidity is satisfied, Theorem 3.11 has the following consequence:

Corollary 3.17. *Let G be a finite group with a weakly rigid tuple of conjugacy classes. Then*

(a) *G is a geometric Galois group over $\mathbb{Q}^{\mathrm{ab}}$ and a regular Galois group over some Galois extension of $\mathbb{Q}^{\mathrm{ab}}$ of degree dividing* $|\mathrm{Out}(G)|$.

(b) *G is a pre-Galois group over $\mathbb{Q}^{\mathrm{ab}}$ and is a Galois group over some Galois extension of $\mathbb{Q}^{\mathrm{ab}}$ of degree dividing* $|\mathrm{Out}(G)|$.

Proof. Since the given tuple of conjugacy classes $\mathbf{C} = (C_1, \dots, C_r)$ is weakly rigid, [29, Theorem 2.17] applies. That is, up to isomorphism of field extensions, there is a unique finite extension $L/\mathbb{C}(T)$ that is Galois with group G and that corresponds to a branched cover $X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$, with given rational branch points, and having branch cycle description $(g_1, \dots, g_r)$ for some $g_i \in C_i$. Since the branch points are rational, this branched cover descends to $\overline{\mathbb{Q}}(T)$. Moreover the field of moduli (relative to $\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}$) of the corresponding field extension of $\overline{\mathbb{Q}}(T)$ is equal to $\mathbb{Q}^{\mathrm{ab}}$, since $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}})$ acts on branch cycle descriptions by preserving conjugacy classes (cf. [29, Lemma 2.8]).

The first assertion in part (a) of the corollary now follows from Theorem 3.11(a). The second assertion in part (a) follows from Theorem 3.11(b, c), using that $\mathrm{cd}(\mathbb{Q}^{\mathrm{ab}}) = 1$. Part (b) of the corollary follows from part (a) by specialization in the Hilbertian field $\mathbb{Q}^{\mathrm{ab}}$ (see Proposition 3.5) in combination with Proposition 3.1(a). □

In Theorem 3.22 below, we prove a more general result using the broader notion given in Definition 3.16. First we extend the usual notion of *rationality* (see [29, Definition 3.7]) to that more general setting.

Definition 3.18. The r-tuple $\mathbf{C}$ is *weakly rational with respect to an embedding $G \hookrightarrow S_d$* if for each $m \in (\mathbb{Z}/d\mathbb{Z})^\times$, $C_1^m, \ldots, C_r^m$ is a permutation of $C_1, \ldots, C_r$, up to conjugation by an element $\omega \in \mathrm{Nor}_{S_d}(G)$. Given a subfield $k \subset \mathbb{C}$, $\mathbf{C}$ is *weakly k-rational with respect to $G \hookrightarrow S_d$* if the condition holds for values m of the cyclotomic character $\chi_k : \mathrm{Gal}(k) \to (\mathbb{Z}/d\mathbb{Z})^\times$.

For short, we just say *weakly rigid*, *weakly rational* and *weakly k-rational* if $G \hookrightarrow S_d$ is the regular representation of G; in this case, conjugating by some element $\omega \in \mathrm{Nor}_{S_d}(G)$ is equivalent to acting by some automorphism $\gamma \in \mathrm{Aut}(G)$. The conditions are then weaker than with any other embedding $G \hookrightarrow S_d$. The classical rational and k-rational notions correspond to the special situation where one can take $\omega \in S_d$ to be in (the image of) G, in the definition above.

Recall the classical action of $\mathrm{Gal}(k)$ on the conjugacy classes C of G: for each $\tau \in \mathrm{Gal}(k)$, C is mapped to $C^{1/\chi_k(\tau)}$ where $\chi_k : \mathrm{Gal}(k) \to (\mathbb{Z}/d\mathbb{Z})^\times$ is the cyclotomic character modulo d: that is $\zeta_d^\tau = \zeta_d^{\chi_k(\tau)}$ where $\zeta_d = e^{2i\pi/d}$.

We use the notation $\mathbf{C}$ for a r-tuple $(C_1, \ldots, C_r)$ of conjugacy classes of G and $\mathbf{t}$ for a r-tuple $(t_1, \ldots, t_r)$ of distinct points in $\mathbb{P}^1(\overline{k})$. We always assume that the sets $\{C_1, \ldots, C_r\}$ and $\{t_1, \ldots, t_r\}$ are invariant under the action of $\mathrm{Gal}(k)$. For $\tau \in \mathrm{Gal}(k)$ and $i = 1, \ldots, r$, denote by $\tau(i)$ the index such that $t_i^\tau = t_{\tau(i)}$.

Definition 3.19. A triple $[G \hookrightarrow S_d, \mathbf{C}, \mathbf{t}]$ is *weakly k-rational* if for each $\tau \in \mathrm{Gal}(k)$, there exists some element $\omega_\tau \in \mathrm{Nor}_{S_d}(G)$ such that

$$C_{\tau(i)}^{\chi_k(\tau)} = C_i^{\omega_\tau}, \quad i = 1, \ldots, r.$$

It is *k-rational* if one can take $\omega_\tau = 1$ ($\tau \in \mathrm{Gal}(k)$).

Definition 3.19 generalizes definitions from [29] of *(weakly) k-rational type* for which $G \hookrightarrow S_d$ is the regular representation: see Definition 3.7 and Remark 3.9(b) there.

If $[G \hookrightarrow S_d, \mathbf{C}, \mathbf{t}]$ is weakly k-rational (resp. is k-rational), then in particular the r-tuple $\mathbf{C}$ is weakly k-rational (resp. is k-rational) with respect to the embedding $G \hookrightarrow S_d$. The former condition is stronger in that the permutation of $C_1, ..., C_r$ involved in Definition 3.19 should be the permutation induced by the action of τ on the branch points, for any $\tau \in \mathrm{Gal}(k)$.

Triples $[G \hookrightarrow S_d, \mathbf{C}, \mathbf{t}]$ are used to represent the *ramification invariants* of an extension $\mathcal{F}/\overline{k}(T)$: G is the monodromy group, $G \hookrightarrow S_d$ the monodromy action, $\mathbf{t}$ the branch point tuple and $\mathbf{C}$ the tuple of inertia canonical classes (in the Galois closure), with $\mathbf{t}$ and $\mathbf{C}$ ordered in such a way that C_i corresponds to t_i, $i = 1, \ldots, r$.

The following lemmas adjust classical rigidity statements to the non-Galois situation.

Lemma 3.20. *Let $\mathcal{F}/\overline{k}(T)$ be an extension such that its ramification invariant $[G \hookrightarrow S_d, \mathbf{C}, \mathbf{t}]$ is weakly k-rational and* $\mathbf{C}$ *is weakly rigid w.r.t. $G \hookrightarrow S_d$. Then $\mathcal{F}/\overline{k}(T)$ has field of moduli k as a field extension.*

Proof. In the case $G \hookrightarrow S_d$ is the regular representation, a proof is given in Theorem 3.8 and Remark 3.9(b)-(c) in [29]. We consider a more general embedding $G \hookrightarrow S_d$.

Every $\tau \in \mathrm{Gal}(k)$ maps the extension $\mathcal{F}/\overline{k}(T)$ to some conjugate extension $\mathcal{F}^\tau/\overline{k}(T)$, which is of ramification invariant

$$[\,G \hookrightarrow S_d,\ (C_1^{1/\chi_k(\tau)}, \dots, C_r^{1/\chi_k(\tau)}),\ (t_1^\tau, \dots, t_r^\tau)\,];$$

or, after reordering $(t_1^\tau, \dots, t_r^\tau)$ as $(t_1, \dots, t_r)$,

$$[\,G \hookrightarrow S_d,\ (C_{\tau(1)}^{\chi_k(\tau)}, \dots, C_{\tau(r)}^{\chi_k(\tau)}),\ (t_1, \dots, t_r)\,].$$

Due to the weak k-rationality assumption, this triple is $[G \hookrightarrow S_d, \mathbf{C}^{\omega_\tau}, \mathbf{t}]$ for some $\omega_\tau \in \mathrm{Nor}_{S_d}(G)$. By the weak rigidity assumption, there is a unique isomorphism class of extensions of $\overline{k}(T)$ with this ramification invariant. Therefore $\mathcal{F}^\tau/\overline{k}(T)$ is $\overline{k}(T)$-conjugate to $\mathcal{F}/\overline{k}(T)$. As this holds for every $\tau \in \mathrm{Gal}(k)$, the field of moduli of $\mathcal{F}/\overline{k}(T)$ is k. □

Lemma 3.21. *Let* $\mathbf{C}$ *be an r-tuple of conjugacy classes of G. If* $\mathbf{C}$ *is weakly k-rational w.r.t. an embedding $G \hookrightarrow S_d$, then there exists an r-tuple* $\mathbf{t} \subset \mathbb{P}^1(\overline{k})$ *such that the triple $[G \hookrightarrow S_d, \mathbf{C}, \mathbf{t}]$ is weakly k-rational.*

Proof. The construction is explained in Lemma 3.16 of [29] in the case $G \hookrightarrow S_d$ is the regular representation and easily generalizes to our situation: the only change is that the conjugacy classes should be regarded modulo the action of $\mathrm{Nor}_{S_d}(G)$. □

Theorem 3.22. *Let G be a finite group and k be a subfield of* $\mathbb{C}$.

(a) *Assume G has a weakly rigid tuple* $\mathbf{C}$ *that is also weakly k-rational. Then G is a geometric Galois group over k, and is a regular Galois group over for some Galois extension $\widehat{k}$ of k of degree $[\widehat{k} : k]$ dividing* $|\mathrm{Aut}(G)|$.

(b) *Assume G has a tuple* $\mathbf{C}$ *that is weakly rigid with respect to some transitive embedding $G \hookrightarrow S_d$ and is weakly k-rational for some field k with respect to the same embedding. Suppose that the exact sequence* $1 \to Z(G) \to G \to \mathrm{Inn}(G) \to 1$ *is split or that k is of cohomological dimension* $\mathrm{cd}(k) \leq 1$. *Then G is a regular Galois group over some Galois extension k_G of k of degree dividing* $|\mathrm{Nor}_{S_d}(G)/G\,\mathrm{Cen}_{S_d}(G)|$ *and hence* $|\mathrm{Out}(G)|$.

Proof. We will show that the assumptions guarantee that there is an extension $\mathcal{F}/\overline{k}(T)$ with field of moduli k and then apply Theorem 3.11. Fix a finite group G, a transitive embedding $G \hookrightarrow S_d$, an integer $r \geq 2$ and a subfield $k \subset \mathbb{C}$.

Assume as in part (b) that G is given with an r-tuple $\mathbf{C}$ of conjugacy classes that is weakly k-rational and weakly rigid with respect to an embedding $G \hookrightarrow S_d$. By Lemma 3.21, there is an r-tuple $\mathbf{t} \subset \mathbb{P}^1(\overline{k})$ such that $[G \hookrightarrow S_d, \mathbf{C}, \mathbf{t}]$ is weakly k-rational. Consider next an extension $\mathcal{F}/\overline{k}(T)$ of degree d, of monodromy group $G \hookrightarrow S_d$, of branch point set $\mathbf{t}$, and corresponding canonical inertia invariant $\mathbf{C}$; the existence of such an extension is guaranteed by the Riemann Existence Theorem. It follows from Lemma 3.20 that $\mathcal{F}/\overline{k}(T)$

has field of moduli k as a field extension. By Theorem 3.11(c), if $N/\overline{k}(T)$ is the Galois closure of $\mathcal{F}/\overline{k}(T)$, then $N/\overline{k}(T)$ descends to its field of moduli k_G as a Galois extension; this is a regular realization of G, as asserted in part (b). The assertion about the degree then follows from Theorem 3.11(b) and Remark 3.12(c).

For part (a), we simply note that "weakly rigid and weakly k-rational" is the same as "weakly rigid and weakly k-rational with respect to the regular representation $G \hookrightarrow S_{|G|}$". We can then proceed as above but use Theorem 3.11(a) instead of Theorem 3.11(b,c). □

Note that Corollary 3.17(a) is the special case of Theorem 3.22 for which $k = \mathbb{Q}^{\mathrm{ab}}$ and the embedding $G \hookrightarrow S_d$ in (b) is given by the regular representation. Again this uses that $\mathrm{cd}(\mathbb{Q}^{\mathrm{ab}}) = 1$, along with the fact that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}})$ acts on branch cycle descriptions by preserving conjugacy classes (i.e., $\mathbf{C}$ is $\mathbb{Q}^{\mathrm{ab}}$-rational).

References

[1] S. Beckmann: *On extensions of number fields obtained by specializing branched coverings*, J. Reine Angew. Math., **419** (1991), 27–53.

[2] E.V. Black: *On semidirect products and the arithmetic lifting property*, J. London Math. Soc. (2) **60** (1999), 677–688.

[3] D. Brink: *On alternating and symmetric groups as Galois groups*, Israel J. Math. **142** (2004), 47–60.

[4] S.U. Chase and M.E. Sweedler: Hopf algebras and Galois theory, Lecture Notes in Mathematics **97**, Springer-Verlag, Berlin-New York, 1969.

[5] K. Coombes and D. Harbater: *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), 821–839.

[6] J.-L. Colliot-Thélène: *Rational connectedness and Galois covers of the projective line*, Ann. of Math. (2) **151** (2000), 359–373.

[7] T. Crespo, A. Rio and M. Vela: *On the Galois correspondence theorem in separable Hopf Galois theory*, Publ. Mat. **60** (2016), 221–234.

[8] P. Dèbes and M.D. Fried: *Nonrigid constructions in Galois theory*, Pacific J. Math. **163** (1994), 81–122.

[9] P. Dèbes: *Covers of $\boldsymbol{P}^1$ over the p-adics*: in Recent developments in the inverse Galois problem (Seattle, WA, 1993), 217–223, Contemp. Math. **186**, 1995.

[10] P. Dèbes and B. Deschamps: *The regular inverse Galois problem over large fields*; in Geometric Galois Action, London Math. Soc. Lecture Note Ser. **243**, 119–138, Cambridge University Press, Cambridge, 1997.

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

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

[13] P. Dèbes: *Some arithmetic properties of algebraic covers*; in Aspects of Galois Theory, London Math. Soc. Lecture Note Ser. **256**, 66–84, Cambridge University Press, 1999.

[14] P. Dèbes: *Descent theory for algebraic covers*; in Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 3–25, Proc. Sympos, Pure Math. **70**, 3–25. Cambridge University Press, 1999.

[15] P. Dèbes and N. Ghazi: *Galois covers and the Hilbert-Grunwald property*, Ann. Inst. Fourier, **62** (2012), 989–1013.

[16] P. Dèbes and F. Legrand: *Twisted covers and specializations*; in Galois-Teichmüller theory and Arithmetic Geometry, 141–162, Adv. Stud. Pure Math. **63**, Math. Soc. Japan, Tokyo, 2012.

[17] M.D. Fried: *Fields of definition of function fields and Hurwitz families – groups as Galois groups*, Comm. Algebra **5** (1977), 17–82.

[18] M.D. Fried and M. Jarden: Field arithmetic, second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete **11**, Springer-Verlag, Berlin, 2004.

[19] M.D. Fried and H. Völklein: *The Inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), 771–800.

[20] C. Greither and B. Pareigis: *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), 239–258.

[21] D. Harbater: *Mock covers and Galois extensions*, J. Algebra, **91** (1984), 281–293.

[22] D. Harbater: *Galois coverings of the arithmetic line*; in Number Theory (New York, 1984–85), Lecture Notes in Mathematics **1240**, Springer-Verlag, Berlin, 1987, 165–195.

[23] B. Hartley and D.J.S. Robinson: *On finite complete groups*, Arch. Math. (Basel) **35** (1980), 67–74.

[24] H. Hasson: *Minimal fields of definition for Galois action*, arXiv 1310.4287.

[25] L. Moret-Bailly: *Construction de revêtements de courbes pointées*, J. Algebra, **240** (2001), 505–534.

[26] F. Pop: *Embedding problems over large fields*, Annals of Math. **144** (1996), 1–35.

[27] D.J.S. Robinson: A Course in the Theory of Groups, Graduate Texts in Mathematics **80**, Springer-Verlag, Berlin, New York, 1996.

[28] J.-P. Serre: Topics in Galois theory, Lecture notes prepared by Henri Damon [Henri Darmon], Research Notes in Mathematics, Jones and Bartlett Publishers, Boston, MA, 1992.

[29] H. Völklein: Groups as Galois Groups, Cambridge Studies in Advanced Mathematics **53**, Cambridge University Press, Cambridge, 1996.

Pierre Dèbes
Laboratoire Paul Painlevé
Mathématiques, Université de Lille
59655 Villeneuve d'Ascq Cedex
France
e-mail: Pierre.Debes@univ-lille.fr

David Harbater
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104–6395
USA
e-mail: harbater@math.upenn.edu