RATIONAL PULLBACKS OF GALOIS COVERS

PIERRE DÈBES, JOACHIM KÖNIG, FRANÇOIS LEGRAND, AND DANNY NEFTIN

ABSTRACT. The finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ are shown to be the only finite groups G with the following property: for some bound r_0, all Galois covers $X \to \mathbb{P}^1_{\mathbb{C}}$ of group G can be obtained by pulling back those with at most r_0 branch points along all non-constant rational maps $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. For $G \subset \mathrm{PGL}_2(\mathbb{C})$, it is in fact enough to pull back one well-chosen cover with at most 3 branch points. A worthwhile consequence of the converse for inverse Galois theory is that, for $G \not\subset \mathrm{PGL}_2(\mathbb{C})$, letting the branch point number grow always provides truly new realizations $F/\mathbb{C}(T)$ of G. Our approach also leads to some improvements of results of Buhler-Reichstein about generic polynomials with one parameter. For example, if G is neither cyclic nor odd dihedral, no polynomial $P \in \mathbb{C}[T, Y]$ of Galois group G can parametrize, via specialization of T, all Galois extensions E/k of group G; here k is some specific base field, not depending on G, viz. $k = \mathbb{C}((V))(U)$. A final application, related to an old problem of Schinzel, provides, subject to the Birch & Swinnerton-Dyer conjecture, a 1-parameter family of affine curves over some number field, all with a rational point, but with no rational generic point.

1. INTRODUCTION

Specialization of field extensions $F/k(T)$ at points $T = t_0 \in k$ is a central tool in Galois theory, going back to Hilbert[1]. Rational pullback is another one, in fact a variant.

Given a finite connected cover[2] $f : X \to \mathbb{P}^1_k$ (over some field k), by a *rational pullback* of f we mean a cover $f_{T_0} : X_{T_0} \to \mathbb{P}^1_k$ obtained by pulling back f along some non-constant rational map $T_0 : \mathbb{P}^1_k \to \mathbb{P}^1_k$. If f is given by a polynomial equation $P(t, y) = 0$ (with f corresponding to the t-coordinate projection) and T_0 is viewed as a rational function $T_0(U) \in k(U)$, then an equation for the pullback f_{T_0} is merely $P(T_0(u), y) = 0$.

As we recall below (§2.1), for "many" T_0, the cover f_{T_0} remains connected; hence if f is Galois of group G, then so is f_{T_0}, which in addition remains defined over k.

Rational pullback is thus a natural tool to create Galois covers of group G over some field k if one is known. Finding covers g that are *not* rational pullbacks of some given covers f may be even more important for inverse Galois theory: if none of these f are defined over k, those covers g, rather than the pullbacks f_{T_0}, are the best chance to find some and so to realize G as a regular Galois group over k [3]. Theorems 1.1 and 1.2, presented in §1.1 below, fit in this theme.

Another question relating rational pullbacks and specializations arises. The set of k-specializations of f (essentially the splitting fields of polynomials $P(t_0, Y)$, $t_0 \in k$) clearly contains that of f_{T_0} (same but with polynomials $P(T_0(u_0), Y)$, $u_0 \in k$). The challenge is

Date: July 5, 2018.

2010 *Mathematics Subject Classification.* Primary 12F12, 11R58, 14E20; Sec. 14E22, 12E30, 11Gxx.

Key words and phrases. Galois extensions, covers, specialization, rational pullback, inverse Galois theory, parametric and generic extensions.

Acknowledgment. This work was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01) and ISF grants No. 577/15 and No. 696/13.

[1]The notion of "specialization" or "specialized extension" is precisely recalled in §2.1.

[2]For pullback, we rather use the cover viewpoint rather than the function field equivalent one.

[3]i.e., as the automorphism group of a k-Galois cover $X \to \mathbb{P}^1$ with X geometrically irreducible.

the converse: are rational pullbacks f_{T_0} of f the only covers with this property, in which case, being a rational pullback could be read off from the specialization set containment? Our contribution to this question is described at the end of §1.2.

A related theme, presented in §1.2, focuses on the set of L-specializations of f – same as above but for the polynomials $P(t_0, Y)$ with t_0 ranging here over a given overfield L of k. Can this set contain every Galois extension of L of group G? With $L = k(U)$, the question takes us back to the rational pullback territory. With L varying over all overfields of k, it refers to the notion of *generic extension* (with one parameter). Theorems 1.4 and 1.5 improve on results of Buhler-Reichstein [BR97] in this context.

1.1. **Regular parametricity.** Assume first that $k = \mathbb{C}$. Consider the situation that all Galois covers $X \to \mathbb{P}^1$ of given group G can be obtained from a proper subset of them by rational pullback; say then that the subset is *regularly parametric*[4]. For some groups, a single cover f may suffice: for example, the degree 2 cover $\mathbb{P}^1 \to \mathbb{P}^1$ sending z to z^2 *is* regularly parametric. Such situations are however exceptional: for "general" groups, an opposite conclusion holds.

Theorem 1.1. *The finite subgroups G of $\mathrm{PGL}_2(\mathbb{C})$: $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$, D_n for $n \geq 2$, S_4, A_4, A_5, are exactly those finite groups which have a regularly parametric cover $f : X \to \mathbb{P}^1_{\mathbb{C}}$. Furthermore, if $G \not\subset \mathrm{PGL}_2(\mathbb{C})$, not only one cover f is not enough but even the set of all Galois covers $X \to \mathbb{P}^1_{\mathbb{C}}$ of group G and with at most r_0 branch points is not regularly parametric, for any $r_0 \geq 0$.*

Hence, for $G \not\subset \mathrm{PGL}_2(\mathbb{C})$, letting the branch point number grow provides an endless source of "new" Galois covers of group G, i.e., not mere rational pullbacks of some with a bounded branch point number, and so truly new candidates to be defined over $\mathbb{Q}$.

Covers are understood here as algebraic branched covers, but Theorem 1.1 and the following Theorem 1.2 may already be of interest at the topological level.

Both directions in the first statement of Theorem 1.1 are non-trivial. The one showing that finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ have a regularly parametric cover over $\mathbb{C}$ (with at most 3 branch points) was proved in [Dèb18, Corollary 2.5] as a consequence of the twisting lemma and Tsen's theorem. The part about "general" groups, those not contained in $\mathrm{PGL}_2(\mathbb{C})$, is a new result of this paper. It solves in particular Problem 2.14 from [Dèb18].

Here is a more precise version. Given an integer $r \geq 0$ and an r-tuple $\mathbf{C}$ of non-trivial conjugacy classes of G, denote the stack of all Galois covers of group G with r branch points by $\mathbf{H}_{G,r}$ and the stack of those with ramification type $(r, \mathbf{C})$ by $\mathbf{H}_{G,r}(\mathbf{C})$ (see §2.2); these are the so-called *Hurwitz stacks*. From Theorem 1.1, if $G \not\subset \mathrm{PGL}_2(\mathbb{C})$,

$$\mathbf{H}_{G,\leq r_0} = \bigcup_{r \leq r_0} \mathbf{H}_{G,r}$$

is never *regularly parametric* ($r_0 \geq 1$). More precisely, we have the following.

Theorem 1.1 (continued)**.** *Let k be an algebraically closed field of characteristic 0 and let G be a finite group.*

(a) *Assume $G \not\subset \mathrm{PGL}_2(\mathbb{C})$. Given an integer $r_0 \geq 0$, if R is suitably large (depending on r_0) and $(R, \mathbf{C})$ is a ramification type of G such that $\mathbf{H}_{G,R}(\mathbf{C}) \neq \emptyset$, then not all k-covers in $\mathbf{H}_{G,R}(\mathbf{C})$ are rational pullbacks of k-covers in $\mathbf{H}_{G,\leq r_0}$.*

(b) *Assume G has at least 5 maximal non-conjugate cyclic subgroups* (in particular, $G \not\subset \mathrm{PGL}_2(\mathbb{C})$). *Given $r_0 \geq 0$, for every suitably large even integer R, there is a non-empty*

[4]The term "regularly" will be fully justified with the general definition of "k-regular parametricity" for which the base field k is not necessarily algebraically closed (see Definition 2.2). We also mean to distinguish "regular parametricity" from the arithmetic notion of "parametricity" (recalled later).

Hurwitz stack $\mathbf{H}_{G,R}(\mathbf{C})$ *such that no* k*-cover in* $\mathbf{H}_{G,R}(\mathbf{C})$ *is a rational pullback of some* k*-cover in* $\mathbf{H}_{G,\leq r_0}$.

Subgroups of $\mathrm{PGL}_2(\mathbb{C})$ have at most 3 maximal non-conjugate cyclic subgroups. Other groups have exactly 3: the quaternion group $\mathbb{H}_8$ or more generally dicyclic groups DC_n of order $4n$ ($n \geq 2$) (which include generalized quaternion groups $\mathrm{DC}_{2^{k-1}}$ $k \geq 2$), groups $G = \mathrm{SL}_2(\mathbb{F}_q)$ with q a prime power, etc. For these groups, conclusion from (a) holds but that from (b) is unclear. Replacing 5 by 4 in Theorem 1.1(b) seems feasible in light of the techniques of §4, but hard and technical; for the sake of brevity, we avoid this slight improvement. Groups with 4 maximal non-conjugate cyclic subgroups (for which conclusion from (b) might also hold) include $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, A_6, etc.

The assumption in Theorem 1.1 that k is algebraically closed can be weakened to only assume that k is ample, or even arbitrary (of characteristic 0) in some situations; see Theorem 3.7. Recall that a field k is *ample* if for every smooth k-curve C, either $C(k) = \emptyset$ or $C(k)$ is infinite. Ample fields include separably closed fields, Henselian fields, fields $\mathbb{Q}^{\mathrm{tot}\mathbb{R}}$, $\mathbb{Q}^{\mathrm{tot}p}$ of totally real, totally p-adic algebraic numbers and their variants.

If instead of the sets $\mathbf{H}_{G,\leq r}$, one considers the smaller subsets $\mathbf{H}_{G,r}(\mathbf{C})$, one obtains even more striking conclusions.

Theorem 1.2. *Let* G *be a finite group not contained in* $\mathrm{PGL}_2(\mathbb{C})$ *and let* $(R, \mathbf{C})$ *be a ramification type for* G*. Then there exists a ramification type* $(R+1, \mathbf{D})$ *for* G *such that* $\mathbf{H}_{G,R+1}(\mathbf{D}) \neq \emptyset$ *and no cover in* $\mathbf{H}_{G,R+1}(\mathbf{D})$ *is a pullback from* $\mathbf{H}_{G,R}(\mathbf{C})$.

These results have the following consequence. To ease notation, denote the set of all Galois covers $X \to \mathbb{P}^1$ of group G by $\mathbf{H}_G$ (over the algebraically closed field k). Say that a finite group G has the *Beckmann-Black regular lifting property* if for any two Galois covers $g_1, g_2 \in \mathbf{H}_G$, there is a Galois cover $f : X \to \mathbb{P}^1 \in \mathbf{H}_G$ and two non-constant rational maps $T_{01}, T_{02} : \mathbb{P}^1 \to \mathbb{P}^1$ such that $g_i = f_{T_{0i}}$ $(i = 1, 2)$.

Corollary 1.3. *The finite subgroups of* $\mathrm{PGL}_2(\mathbb{C})$ *are exactly those finite groups for which the Beckmann-Black regular lifting property holds.*

The proof combines Theorem 1.1 above with Theorem 2.1 from [Dèb18]. It is given in §2.3.2 where the latter is recalled.

Our lifting property is a geometric variant of the *Beckmann-Black arithmetic* lifting property for which k is a number field and the k-Galois cover $f : X \to \mathbb{P}^1 \in \mathbf{H}_G$ is requested to specialize to some given Galois extensions E_i/k, $i = 1, \ldots, N$ of group G at some points $t_{0i} \in \mathbb{P}^1(k)$. This property is already interesting with $N = 1$ as it supports Hilbert's strategy to solve the Inverse Galois problem by first realizing a k-Galois cover $f : X \to \mathbb{P}^1$ of given group. It is only known to hold for some groups: abelian, odd dihedral[5], S_n, A_n and a few others, and has no known counterexample. Our geometric variant is obvious for $N = 1$ (as $f_{T_0} = f$ for $T_0(U) = U$) and Corollary 1.3 shows that it fails for $N \geq 2$ if $G \not\subset \mathrm{PGL}_2(\mathbb{C})$.

1.2. **Regular parametricity and genericity.** Before regular parametricity, a notion of mere *parametricity* was pre-existing: given a field k of characteristic zero and an overfield $L \supset k$, a Galois extension $F/k(T)$ of group G that is k-regular[6] is L*-parametric* if

(∗) *every Galois extension* E/L *of group* G *is a specialization of the extension* $FL/L(T)$ *at some point* $t_0 \in \mathbb{P}^1(L)$.

[5] i.e., a dihedral group of order $2n$ with $n > 1$ odd.

[6] that is, such that k is algebraically closed in F.

A rational pullback $f_{T_0} : X_{T_0} \to \mathbb{P}^1_k$ can in fact be seen as a specialization and regular parametricity as some variant of parametricity. Namely, view $f : X \to \mathbb{P}^1_k$ as its function field extension $k(X)/k(T)$ and $T_0 : \mathbb{P}^1_k \to \mathbb{P}^1_k$ as an element $T_0(U)$ of $k(U)$ (with U some new indeterminate). Then, if f_{T_0} is connected, the function field extension $k(X_{T_0})/k(U)$ of the pullback $f_{T_0} : X_{T_0} \to \mathbb{P}^1_k$ is the specialization at $T = T_0(U) \in k(U)$ of the function field extension $k(U)(X)/k(U)(T)$ of $f \otimes_k k(U)$. Hence, the extension $k(X)/k(T)$ being $k(U)$-parametric implies that the cover $f : X \to \mathbb{P}^1_k$ is k-regularly parametric[7].

In general, the L-parametricity property (condition $(*)$) is not preserved by base change over bigger fields. A classical property – the *genericity* property – in fact requests that the L-parametricity property holds for *every* base change L/k. This property is much stronger. Finite groups $G \not\subset \mathrm{PGL}_2(k)$ are automatically ruled out: they do not have any generic extension $F/k(T)$ since the *Noether invariant extension* (of group G)

$$E/L = k(\mathbf{T})/k(\mathbf{T})^G, \text{ with } \mathbf{T} = (T_1, \dots, T_{|G|}),$$

can be a specialization of $FL/L(T)$ only if F is of genus 0, and so $G \subset \mathrm{PGL}_2(k)$ (a Lüroth like consequence of $k(\mathbf{T})$ being purely transcendental; see [JLY02, Proposition 8.1.4]).

The Noether extension can no longer be used to disprove the weaker $\overline{k}(U)$-parametricity property of a given k-regular Galois extension $F/k(T)$ of group G as it is then a Galois extension E of $L = \overline{k}(U)$ (instead of $L = k(\mathbf{T})^G$) of group G, not being a specialization of $FL/L(T)$, that should be produced. This is what Theorem 1.1 does for finite groups $G \not\subset \mathrm{PGL}_2(\mathbb{C})$: they have no regularly parametric cover $f : X \to \mathbb{P}^1_{\overline{k}}$, *a fortiori* no $\overline{k}(U)$-parametric extension $F/k(T)$.

Our approach also clarifies the question for finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$. Theorem 1.4 below recapitulates the whole situation, over a non-necessarily algebraically closed field:

Theorem 1.4. *Let G be a finite group, k a field of characteristic zero, $F/k(T)$ a k-regular Galois extension of group G, and U, V two indeterminates.*
(a) *If $G \not\subset \mathrm{PGL}_2(\mathbb{C})$, then, $F/k(T)$ is neither $\overline{k}(U)$-parametric nor $\overline{k}((V))(U)$-parametric.*
(b) *If G is neither cyclic nor odd dihedral, then, $F/k(T)$ is not $\overline{k}((V))(U)$-parametric.*

We refer to Theorem 5.1 for a more general version which also covers most of the k-regular Galois extensions of $k(T)$ with either cyclic or odd dihedral Galois group.

Statement (b) applies in particular to these finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$: S_4, A_4, A_5, and even dihedral groups. Theorem 1.4 implies that these groups, and, more generally, all neither cyclic nor odd dihedral finite groups, do not have any generic extension $F/k(T)$. This was known from the *essential dimension theory* of Buhler-Reichstein [BR97]; see also [JLY02][8]. Our alternate approach provides stronger conclusions:

(a) It explicitly produces a base change L/k over which the L-parametricity property fails: one can take $L = \overline{k}(U)$ or $L = \overline{k}((V))(U)$. In comparison, the base change $k(\mathbf{T})^G/k$ (coming from the Noether extension) is not purely transcendental in general, is of high transcendence degree, and depends on G.

(b) Regarding generic extensions $F/k(T)$, our approach not only gives the exact list of groups having one (as [BR97] did), but also the list of corresponding extensions.

Namely, we have the following result, in which we take $k = \mathbb{Q}$ for simplicity:

[7]The equivalence does not hold *a priori* as $f : X \to \mathbb{P}^1_k$ being k-regularly parametric only implies that the Galois extensions $E/k(U)$ (with the corresponding Galois group) that are k-regular be specializations of $k(U)(X)/k(U)(T)$ (see Remark 2.3).

[8]More precisely, it was already known that these groups have no *one parameter generic polynomial* over k (a polynomial version of the notion of generic extension $F/k(T)$). We refer to Proposition B.2 for a clarifying result about the equivalence between these two notions.

Theorem 1.5. *Let G be a non-trivial finite group and $F/\mathbb{Q}(T)$ a $\mathbb{Q}$-regular Galois extension of group G. The following three conditions are equivalent:*
(a) *$F/\mathbb{Q}(T)$ is generic,*
(b) *$F/\mathbb{Q}(T)$ is $\overline{\mathbb{Q}}((V))(U)$-parametric and $\mathbb{Q}(U)$-parametric,*
(c) *one of the following three conditions holds:*
  (i) *$G = \mathbb{Z}/2\mathbb{Z}$ and $F/\mathbb{Q}(T)$ has two branch points, which are $\mathbb{Q}$-rational,*
  (ii) *$G = \mathbb{Z}/3\mathbb{Z}$ and $F/\mathbb{Q}(T)$ has two branch points,*
  (iii) *$G = S_3$ and $F/\mathbb{Q}(T)$ has three branch points, which are $\mathbb{Q}$-rational.*

We refer to Corollary 5.4 for the case of an arbitrary field of characteristic zero.

A final application relates to the following old problem of Schinzel, presented in [Sch00, Chapter 5, §5.1, Problem 1]:

Question 1.6. *Let k be a number field and $P \in \mathbb{C}[U,T,Y]$ a polynomial such that, for all but finitely many $u_0 \in \mathbb{Z}$, the polynomial $P(u_0,T,Y)$ has a zero in k^2. Does P, viewed as a polynomial in T and Y, have a zero in $k(U)^2$?*

While the answer is "Yes" when $k = \mathbb{Q}$ and P is of degree at most 2 in (T,Y) (see [DLS66, Theorem 2]), the answer seems to be negative in general. However, only conjectural counter-examples, subject to a conjecture of Selmer, are known. We refer to [Sch00, pp. 318-319] for more details and references.

In [Dèb18], a close variant of Question 1.6, called (WH), is introduced and used as a Working Hypothesis; it is explicitly recalled in §5.4. By [Dèb18, Proposition 2.17(a)], under (WH), we have a full positive answer to one of our motivating questions:

Question 1.7. *Let k be a number field and let $f_1 : X_1 \to \mathbb{P}^1_k$ and $f_2 : X_2 \to \mathbb{P}^1_k$ be two k-regular Galois covers with the same Galois group such that the set of specializations of f_2 is contained in that of f_1. Is f_2 a rational pullback of f_1, after base change $\mathbb{C}/k$?*

Here, subject to the Birch and Swinnerton-Dyer conjecture, we provide a counterexample of genus 1 over $k = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{11})$ both to Question 1.6 and Question 1.7, and so to (WH) too; see Theorem 5.8. This counterexample gives evidence that the genus 1 case is exceptional. It is plausible that the answer to Question 1.7 is positive for covers of genus at least 2.

The paper is organized as follows. §2 is a preliminary section providing the basic notation and terminology together with some general prerequisites. §3 and §4 are concerned with our regular parametricity results, while §5 is devoted to those around the connection between regular parametricity and genericity. In particular, Theorem 1.1 is proved in §3, Theorem 1.2 in §4, and Theorems 1.4 and 1.5 in §5.

2. Notation, terminology, and prerequisites

2.1. **Basic terminology** (for more details, see [DD97b] and [DL13])**.** The base field k is always assumed to be of characteristic 0. We also fix a big algebraically closed field containing the complex field $\mathbb{C}$ and the indeterminates that will be used, and in which every field compositum should be understood.

Given a field k, a finite extension $F/k(T)$ is said to be ***k-regular*** if $F \cap \overline{k} = k$. We make no distinction between a k-regular extension $F/k(T)$ and the associated *k-regular* cover $f : X \to \mathbb{P}^1_k$: f is the normalization of $\mathbb{P}^1_k$ in F and F is the function field $k(X)$ of X. In particular, we make no distinction between rational maps $T_0 : \mathbb{P}^1_k \to \mathbb{P}^1_k$ and the rational functions $T_0 \in k(U)$.

We also use ***affine equations***: we mean the irreducible polynomial $P \in k[T,Y]$ of a primitive element of $F/k(T)$, integral over $k[T]$. We say ***defining equation*** if the primitive element is not necessarily integral over $k[T]$; then, $P \in k(T)[Y]$.

By ***group*** and ***branch point set*** of a k-regular extension $F/k(T)$, we mean those of the extension $F\overline{k}/\overline{k}(T)$: the group of $F\overline{k}/\overline{k}(T)$ is the Galois group of its Galois closure and the branch point set of $F\overline{k}/\overline{k}(T)$ is the (finite) set of points $t \in \mathbb{P}^1(\overline{k})$ such that the associated discrete valuations are ramified in $F\overline{k}/\overline{k}(T)$.

The field k being of characteristic 0, we also have the ***inertia canonical invariant*** $\mathbf{C}$ of the k-regular extension $F/k(T)$, defined as follows. If $\mathbf{t} = \{t_1, \dots, t_r\}$ is the branch point set of f, then, $\mathbf{C}$ is an r-tuple $(C_1, \dots, C_r)$ of conjugacy classes of the group G of $F/k(T)$: for $i = 1, \dots, r$, the class C_i is the conjugacy class of the distinguished[9] generators of the inertia groups $I_{\mathfrak{P}}$ above t_i in the Galois closure $\widehat{F}/k(T)$ of $F/k(T)$. The couple $(r, \mathbf{C})$ is called the ***ramification type*** of $F/k(T)$. More generally, given a finite group G, we say that a couple $(r, \mathbf{C})$ is ***a ramification type*** for G over k if it is the ramification type of at least one k-regular Galois extension $F/k(T)$.

We also use the notation $\mathbf{e} = (e_1, \dots, e_r)$ for the r-tuple with ith entry the ramification index $e_i = |I_{\mathfrak{P}}|$ of primes above t_i; e_i is also the order of elements of C_i, $i = 1, \dots, r$.

We say that two k-regular extensions $F/k(T)$ and $L/k(T)$ are ***isomorphic*** if there is a field isomorphism $F \to L$ that restricts to an automorphism $\chi : k(T) \to k(T)$ equal to the identity on k, and that they are ***$k(T)$-isomorphic*** if, in addition, χ is the identity on $k(T)$.

Given a Galois extension $F/k(T)$ and $t_0 \in \mathbb{P}^1(k)$, the ***specialized extension*** F_{t_0}/k ***of*** $F/k(T)$ ***at*** t_0 is the Galois extension defined as follows. For $t_0 \in \mathbb{A}^1(k)$, consider the integral closure B of $A = k[T]$ in F. Then, F_{t_0}/k is the residue extension of an arbitrary prime ideal of B above the ideal $\langle T - t_0 \rangle$. For $t_0 = \infty$, do the same but with $A = k[1/T]$ replacing $A = k[T]$ and $\langle 1/T \rangle$ replacing $\langle T - t_0 \rangle$.

If $P \in k[T,Y]$ is an affine equation of $F/k(T)$ and $\Delta_P \in k[T]$ is its discriminant w.r.t. Y, then, for every $t_0 \in k$ such that $\Delta_P(t_0) \neq 0$, t_0 is not a branch point of $F/k(T)$ and the specialized field F_{t_0} is the splitting field over k of $P(t_0, Y)$.

The following easy lemma will be used on several occasions in the sequel:

Lemma 2.1. *Let $L \supset k$ be an overfield and $t_0 \in \mathbb{P}^1(k)$. Then, one has $(FL)_{t_0} = F_{t_0}L$.*

Proof. Without loss of generality, we may assume $t_0 \neq \infty$. Denote the integral closure of $k[T]$ in F by B_k. Pick $b_1, \dots, b_{|G|}$ in B_k such that

$$B_k = k[T]b_1 \oplus \cdots \oplus k[T]b_{|G|}.$$

As k has characteristic zero, the extension L/k is separable (in the sense of non-necessarily algebraic extensions; see, e.g., [Lan02, Chapter VIII, §4]). Then, by, e.g., [FJ08, Proposition 3.4.2], the integral closure B_L of $L[T]$ in FL satisfies

$$B_L = L[T]b_1 \oplus \cdots \oplus L[T]b_{|G|}.$$

Let $\mathfrak{P}_L$ be a prime ideal of B_L lying over that of $L[T]$ generated by $T - t_0$. Then, the restriction $\mathfrak{P}_k = \mathfrak{P}_L \cap B_k$ of $\mathfrak{P}_L$ to B_k lies over the prime ideal of $k[T]$ generated by $T - t_0$. One then has

$$(FL)_{t_0} = B_L/\mathfrak{P}_L = L(\overline{b_1}, \dots, \overline{b_{|G|}}),$$

[9] "distinguished" means that these generators correspond to the e_ith root $e^{2i\pi/e_i}$ of 1 in the canonical isomorphism $I_{\mathfrak{P}} \to \mu_{e_i} = \langle e^{2i\pi/e_i} \rangle$.

where $\overline{b_1}, \dots, \overline{b_{|G|}}$ denote the reductions modulo $\mathfrak{P}_L$ of $b_1, \dots, b_{|G|}$, respectively. But these reductions modulo $\mathfrak{P}_L$ are the reductions $\underline{b_1}, \dots, \underline{b_{|G|}}$ modulo $\mathfrak{P}_k$ of $b_1, \dots, b_{|G|}$, respectively. Hence, one has

$$(FL)_{t_0} = k(\underline{b_1}, \dots, \underline{b_{|G|}})L = F_{t_0}L,$$

as needed for the lemma. □

If $f : X \to \mathbb{P}^1_k$ is a k-regular Galois cover of group G and $T_0 \in k(U) \setminus k$, the ***pullback*** f_{T_0} ***of*** f ***along*** T_0 is the k-cover $f_{T_0} : X_{T_0} \to \mathbb{P}^1_k$ obtained by *pulling back* f along the rational map $T_0 : \mathbb{P}^1_k \to \mathbb{P}^1_k$. If X_{T_0} is connected, then, the pullback f_{T_0} can be viewed as a specialization:

$$k(X_{T_0})/k(U) = (k(U)(X))_{T_0}/k(U).$$

In this case, if $P \in k[T, Y]$ is an affine equation of f, then, $\Delta_P(T_0) \neq 0$ and so $P(T_0(U), Y)$ is a defining equation of the pullback f_{T_0}.

The subset $H_{P,k(U)}$ of $k(U)$ of all T_0 such that $P(T_0(U), Y)$ is irreducible in $k(U)[Y]$ is a Hilbert subset of the field $k(U)$. For $T_0 \in H_{P,k(U)}$, the cover f_{T_0} is connected, hence Galois of group G. The field $k(U)$ being Hilbertian, the subset $H_{P,k(U)}$ is "big" in various senses: it is infinite, it is dense for the Strong Approximation Topology, etc.

2.2. **More specific notation and terminology.** Given a finite group G, an integer $r \geq 1$, an r-tuple $\mathbf{C}$ of non-trivial conjugacy classes of G, and a field k (of characteristic zero), we use the following notation:

- $\mathbf{R}_G(k)$: set of all Galois extensions E/k of group G,

- $\mathbf{H}_G(k)$: set of all k-regular Galois extensions $F/k(T)$ of group G or, equivalently, of all k-regular Galois covers $f : X \to \mathbb{P}^1_k$ of group G,

- $\mathbf{H}_{G,r}(k)$: subset of $\mathbf{H}_G(k)$ defined by the extra condition that the branch point number is r,

- $\mathbf{H}_{G,r}(\mathbf{C})(k)$: subset of $\mathbf{H}_{G,r}(k)$ defined by the extra condition that the inertia canonical invariant is $\mathbf{C}$.

One can more generally define $\mathbf{H}_{G,r}$ and $\mathbf{H}_{G,r}(\mathbf{C})$ as stacks; $\mathbf{H}_{G,r}(k)$ and $\mathbf{H}_{G,r}(\mathbf{C})(k)$ can then be viewed as the set of k-rational points on these stacks.

- For $\mathbf{H} \subset \mathbf{H}_G(k)$, we define

$$\mathrm{SP}(\mathbf{H}) = \left\{ F_{t_0}/k \;\middle|\; \begin{array}{l} F/k(T) \in \mathbf{H} \\ t_0 \in \mathbb{P}^1(k) \end{array} \right\}$$

and

$$\mathrm{PB}(\mathbf{H}) = \left\{ f_{T_0} \;\middle|\; \begin{array}{l} f \in \mathbf{H} \\ T_0 \in k(U) \setminus k \end{array} \right\}.$$

Definition 2.2. Let $\mathbf{H}$ be a subset of $\mathbf{H}_G(k)$.

(a) $\mathbf{H}$ is said to be *k-parametric* if $\mathrm{SP}(\mathbf{H}) \supset \mathbf{R}_G(k)$.

(b) More generally, given a field extension L/k, $\mathbf{H}$ is said to be *L-parametric* if the set $\mathbf{H}_L = \{FL/L(T) \mid F/k(T) \in \mathbf{H}\}$ is L-parametric.

(c) $\mathbf{H}$ is said to be *generic* if $\mathbf{H}$ is *L-parametric* for every field extension L/k.

(d) $\mathbf{H}$ is said to be *k-regularly parametric* if $\mathrm{PB}(\mathbf{H}) \supset \mathbf{H}_G(k)$.

(e) An extension $F/k(T) \in \mathbf{H}_G(k)$ is said to be *L-parametric* for a given extension L/k (resp., is said to be *generic*) if $\mathbf{H} = \{F/k(T)\}$ is L-parametric (resp., is generic).

Remark 2.3. Given a subset $\mathbf{H}$ of $\mathbf{H}_G(k)$, we have the following implications:

$$\mathbf{H} \text{ generic} \Rightarrow \mathbf{H}\ k(U)\text{-parametric} \Rightarrow \mathbf{H}\ k\text{-regularly parametric.}$$

Indeed, only the latter requires explanations. Let $E/k(U)$ be a k-regular Galois extension of group G and assume without loss that G is not trivial. If $\mathbf{H}$ is $k(U)$-parametric, there are $F/k(T) \in \mathbf{H}$ and $T_0 \in \mathbb{P}^1(k(U))$ such that $E = (Fk(U))_{T_0}$. If T_0 is in $\mathbb{P}^1(k)$, then, by Lemma 2.1, we get $E = F_{T_0}k(U)$. Hence, as $E/k(U)$ is k-regular, the field F_{T_0} is equal to k, that is, $E = k(U)$, which cannot happen. Consequently, T_0 is not constant and $E/k(U)$ is the pullback of $F/k(T)$ along T_0, thus showing that $\mathbf{H}$ is k-regularly parametric.

Compared to the right-hand side condition, the middle one also requires that the Galois extensions of $k(U)$ of group G which are not k-regular are parametrized (in particular, the constant extensions $E(U)/k(U)$ with $E/k \in \mathbf{R}_G(k)$). However, these two conditions are equivalent if k is algebraically closed.

2.3. **Prerequisites.** The field k is here algebraically closed and of characteristic 0.

2.3.1. *Riemann Existence Theorem.* This fundamental tool of the theory of covers of $\mathbb{P}^1$ allows turning questions about covers into combinatorics and group theory considerations.

Riemann Existence Theorem (RET). *Given a finite group G, an integer $r \geq 2$, a subset $\mathbf{t}$ of $\mathbb{P}^1(k)$ of r points, and an r-tuple $\mathbf{C} = (C_1, \dots, C_r)$ of non-trivial conjugacy classes of G, there is a Galois extension $F/k(T)$ of group G, branch point set $\mathbf{t}$, and inertia canonical invariant $\mathbf{C}$ iff there exists $(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r$ such that $g_1 \cdots g_r = 1$ and $\langle g_1, \dots, g_r \rangle = G$. Furthermore, the number of such extensions $F/k(T)$ (in a fixed algebraic closure of $k(T)$) equals the number of r-tuples $(g_1, \dots, g_r)$ as above, counted modulo componentwise conjugation by an element of G.*

The RET shows that a couple $(r, \mathbf{C})$ is a ramification type for G over k if the set, traditionally called the ***Nielsen class***, of all $(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r$ such that $g_1 \cdots g_r = 1$ and $\langle g_1, \dots, g_r \rangle = G$ is non-empty. We shall use the RET to construct Galois extensions of given group G and with some special ramification type.

2.3.2. *Bounds for the branch point number and the genus of pulled-back covers.*

Theorem 2.4. *Let $f : X \to \mathbb{P}^1$ be in $\mathbf{H}_G(k)$ and $T_0 : \mathbb{P}^1 \to \mathbb{P}^1$ a non-constant rational map. Assume the pullback $f_{T_0} : X_{T_0} \to \mathbb{P}^1$ is connected. Denote the branch point number of f and the genus of X (resp., the branch point number of f_{T_0} and the genus of X_{T_0}) by r and g (resp., by r_{T_0} and g_{T_0}). We have:*

(a) *$r \leq r_{T_0}$ and $g \leq g_{T_0}$,*

(b) *if $g > 1$ and T_0 is not an isomorphism, then, $g < g_{T_0}$.*

Comments on proof. Regarding branch point numbers, it is a main result from [Dèb18]; see Theorem 2.1. Regarding genera, one may assume $g \neq 0$ and T_0 is not an isomorphism. The claim then follows from applying the Riemann-Hurwitz formula to the cover $X_{T_0} \to X$. Namely, we obtain $2g_{T_0} - 2 \geq N(2g-2)$ with $N = \deg(f)$, whence $g_{T_0} \geq 2(g-1)+1 \geq g$ if $g \geq 1$, with equality only if $g = 1$. □

We can now explain how Corollary 1.3 is deduced from Theorem 1.1.

Proof of Corollary 1.3 assuming Theorem 1.1. First, assume G satisfies the Beckmann-Black regular lifting property. Pick a Galois cover $g_1 \in \mathbf{H}_G$ (such a cover exists from the Riemann Existence Theorem). Let r_1 be the branch point number of g_1. Then, for any $g_2 \in \mathbf{H}_G$, there exists $f \in \mathbf{H}_G$ such that $g_i = f_{T_{0i}}$ $(i = 1, 2)$. From Theorem 2.4, it follows

from $g_1 = f_{T_{01}}$ that the branch point number of f is $\leq r_1$. This shows that $\mathbf{H}_{G,\leq r_1}$ is regularly parametric. From Theorem 1.1, $G \subset \mathrm{PGL}_2(\mathbb{C})$.

Conversely, if $G \subset \mathrm{PGL}_2(\mathbb{C})$, then, G has a regularly parametric cover $f : X \to \mathbb{P}^1$ [Dèb18, Corollary 2.5], *a fortiori* the Beckmann-Black regular lifting property holds. □

2.3.3. *On varieties and their dimension.* In the following, the term variety (over k) should always be understood to mean "irreducible quasi-projective variety". We recall some well-known facts from algebraic geometry about the structure and dimension of images and preimages under algebraic morphisms.

It is elementary that the image of an n-dimensional variety under an algebraic morphism is always of dimension $\leq n$. A bound in the opposite direction is given via the dimension of a fiber, cf., e.g., [Mum99, §1.8, Theorems 2 and 3]:

Theorem 2.5. *Let $f : X \to Y$ be a dominant morphism between varieties X and Y. Then,*

$$\dim(Y) \leq \dim(X) \leq \dim(Y) + \dim(f^{-1}(p)),$$

where p is any point in $f(X)$.

Theorem 2.6 (Chevalley)**.** *Let $f : X \to Y$ be a morphism between varieties X and Y. Then, the image of any constructible subset of X is constructible*[10]*.*

In particular, the image of any subvariety X_0 of X is a finite union of varieties $Y_i \subset Y$, each of dimension at most $\dim(X_0)$.

For short, we shall say that a subset S of a variety X is *of dimension $\leq d$*, if it is contained in a finite union of subvarieties of dimension $\leq d$.

2.3.4. *Defining equations for Galois covers and their pullbacks.* To prove Theorem 1.1(a), we shall use affine equations $P(T, Y) = 0$ to define Galois covers of $\mathbb{P}^1_k$.

Lemma 2.7. *Let G be a finite group and $r_0 \in \mathbb{N}$. Then, every Galois cover in $\mathbf{H}_{G,\leq r_0}(k)$ can be defined by an affine equation $P(T, Y) = 0$, where P is irreducible, monic, and integral in Y, of bounded T-degree depending only on r_0 and G, and of degree $|G|$ in Y.*

Proof. This follows from [Sad99, Section 2.2], where it is shown that a Galois cover of $\mathbb{P}^1_k$ with group G and of prescribed genus g can always be defined by an affine equation of degree $\leq (2g+1)|G|\log|G|/\log(2)$ in T (and with the remaining assertions as in the statement above). See also [Dèb17, Lemma 4.1]. It then suffices to note that the genus g of a Galois cover of $\mathbb{P}^1$ with r_0 branch points is bounded from above only in terms of G; indeed, the Riemann-Hurwitz formula gives $2g \leq 2 - 2|G| + r_0(|G| \cdot (1 - 1/e_{\max}))$, where $e_{\max}$ is the maximal element order in G. □

Definition 2.8. Let $d, e \in \mathbb{N}$. We denote by $\mathcal{P}_{d,e}$ the space of polynomials $P(T, Y) \in k[T, Y]$ in two variables, of degree exactly d in T and exactly e in Y, viewed up to multiplicative constants. Furthermore, denote by $\mathcal{R}_d$ the set of rational functions over k in one indeterminate U of degree exactly d.

Of course, $\mathcal{P}_{d,e}$ is a variety in a natural way, via identifying a polynomial $P(T, Y) = \sum_{i=0}^{d}\sum_{j=0}^{e}\alpha_{i,j}T^iY^j$ with the coordinate tuple $(\alpha_{i,j})_{i,j}$. In the same way, $\mathcal{R}_d$ is a variety, by identifying a rational function $T_0 = T_0(U) = (\sum_{i=0}^{d}\beta_iU^i)/(\sum_{j=0}^{d}\gamma_jU^j)$ with the coordinate tuple $(\beta_0 : \cdots : \beta_d : \gamma_0 : \cdots : \gamma_d) \in \mathbb{P}^{2d+1}$. Note that this identification is well-defined since either the numerator or the denominator of $T_0(U)$ are of degree d.

We can now define pullback maps on the level of the above spaces of polynomials and rational functions.

[10]Here, a subset of a topological space is called *constructible* if it is a finite union of locally closed sets.

Lemma 2.9. *Let d_1, d_2, and d_3 be positive integers. Then, the map*

$$\mathrm{PB} : \mathcal{P}_{d_1,d_2} \times \mathcal{R}_{d_3} \to \mathcal{P}_{d_1 \cdot d_3, d_2},$$

defined by $(P(T,Y), T_0(U)) \mapsto$ "numerator of $P(T_0(U), Y)$" is a morphism of algebraic varieties.

Proof. Let $P(T,Y) = \sum_{i=0}^{d_1} \sum_{j=0}^{d_2} \alpha_{i,j} T^i Y^j$ and $T_0 = (\sum_{k=0}^{d_3} \beta_k U^k)/(\sum_{k=0}^{d_3} \gamma_k U^k)$. Then,

$$\mathrm{PB}(f, T_0) = \textstyle\sum_{i,j} \alpha_{i,j} (\sum_k \beta_k U^k)^i (\sum_k \gamma_k U^k)^{d_1 - i} Y^j \quad ,$$

and identification with the spaces of coordinate tuples shows that PB is given by a polynomial map. This shows the assertion. □

3. Regular Parametricity - Part One

This section and the following §4 articulate around our results on regular parametricity: §§3.1, 3.2, §4 respectively correspond to Theorems 1.1(a), 1.1(b), 1.2 from §1.

Throughout this section, except in §3.3, the field k is algebraically closed of characteristic 0. To simplify the notation, we then generally omit the reference to the rationality field: for example, we write $\mathbf{H}_G$ for $\mathbf{H}_G(k)$.

Our proofs make use of the fact that k is algebraically closed but certain parts carry over to more general fields. We collect such considerations in §3.3.

3.1. **Proof of Theorem 1.1(a).** In this section, apart from the sets $\mathbf{H}_{G,r}(\mathbf{C})$ of covers with ramification type $(r, \mathbf{C})$, we also use *(inner) Hurwitz spaces*. These are moduli spaces of equivalence classes of covers. We will denote them by $\mathcal{H}^{in}_{G,r}(\mathbf{C})$, and the equivalence class of $f \in \mathbf{H}_{G,r}(\mathbf{C})$ by $[f]$. For a precise definition, cf., e.g., [FV91]. We will use only the following well-known facts here:
Firstly, for any ramification type $(r, \mathbf{C})$, the set $\mathcal{H}^{in}_{G,r}(\mathbf{C})$ is equipped with an algebraic structure which makes it a finite union of quasi-projective varieties of dimension r. Secondly, if $Z(G) = \{1\}$, then $f \in \mathbf{H}_{G,r}(\mathbf{C})$ is defined over a field K if and only if $[f]$ is a K-rational point of $\mathcal{H}^{in}_{G,r}(\mathbf{C})$.

3.1.1. *Reduction to Theorem 3.1 and Lemma 3.2.* The most challenging part in the proof of Theorem 1.1(a) is the following result about covers of genus at least 2.

Theorem 3.1. *Let G be a finite group, let $r_0 \in \mathbb{N}$, and let*

$$\mathbf{H}_{G,\le r_0, g\ge 2}(k) := \mathbf{H}_{G,\le r_0}(k) \setminus \{\textit{genus} \le 1 \textit{ covers}\}$$

be the set of all k-Galois covers $f : X \to \mathbb{P}^1$ of genus at least 2 with Galois group G and at most r_0 branch points. Then there exists $R_0 \in \mathbb{N}$ such that for every ramification type $(R, \mathbf{C})$ for G with $R \ge R_0$, one has

$$\mathbf{H}_{G,R}(\mathbf{C})(k) \not\subset \mathrm{PB}(\mathbf{H}_{G,\le r_0, g\ge 2}(k)).$$

In particular, $\mathbf{H}_{G,\le r_0, g\ge 2}(k)$ is not k-regularly parametric.

Theorem 3.1 is proved in §3.1.2-4 below. The following lemma shows non-parametricity for sets of Galois covers of genus 1.

Lemma 3.2. *Let $\mathbf{H}_{G,g=1}(k)$ be the set of Galois covers $f : X \to \mathbb{P}^1$ of genus 1 with Galois group G. Then there exists a ramification type $(r, \mathbf{C})$ for G such that no cover in $\mathbf{H}_{G,r}(\mathbf{C})(k)$ is a pullback from $\mathbf{H}_{G,g=1}(k)$. In particular, $\mathbf{H}_{G,g=1}(k)$ is not k-regularly parametric.*

Proof. Let $f : X \to \mathbb{P}^1$ be an element of $\mathbf{H}_{G,g=1}$. As an immediate consequence of the Riemann-Hurwitz formula, the tuple of element orders in the inertia canonical invariant of f is one of $(2,2,2,2)$, $(3,3,3)$, $(2,4,4)$, or $(2,3,6)$. Furthermore, in each case G has a normal subgroup N with cyclic quotient group G/N of order 2, 3, 4 and 6 respectively; and such that $X \to X^N$ is an unramified cover of genus-1 curves over k. Assume first that $|N| = 1$. Then G is cyclic[11] and therefore possesses coverings of genus zero. In particular, no set of coverings of genus ≥ 1 can have those as pullbacks, by Theorem 2.4.

Assume therefore that $|N| > 1$. Let $x \in N \setminus \{1\}$, and let $(r, \mathbf{C})$ be any ramification type for G involving the conjugacy class of x. Since $X \to X^N$ is unramified, any rational pullback of it must also be unramified. But of course for any cover $\widetilde{X} \to \mathbb{P}^1$ with inertia canonical invariant $\mathbf{C}$, the subcover $\widetilde{X} \to \widetilde{X}^N$ is ramified by definition. Therefore no cover of inertia canonical invariant $\mathbf{C}$ can be a pullback of f. □

Remark 3.3. In the case that G is non-cyclic, the above proof in fact shows immediately that, for $(r, \mathbf{C})$ a ramification type of genus 1 with group G ($r \in \{3,4\}$), and for each $s \geq r+1$, there exists a ramification type $(s, \mathbf{D})$ for G such that no cover in $\mathbf{H}_{G,s}(\mathbf{D})$ is a pullback from $\mathbf{H}_{G,r}(\mathbf{C})$. Indeed, for the only critical case $s = r+1$, it suffices to replace $(x_1, \ldots, x_n) \in \mathbf{C}$, where $x_1 \notin N$ without loss, by $(x_0, x_0^{-1}x_1, \ldots, x_n)$ with $x_0 \in N \setminus \{1\}$.

Assuming Theorem 3.1 and Lemma 3.2, we can now derive Theorem 1.1(a).

Proof of Theorem 1.1(a). By assumption, G does not possess any Galois covers of genus zero. Let $\mathbf{C} := (C_1, \ldots, C_R)$ be a ramification type for G. From Theorem 3.1, we know that not all covers of inertia canonical invariant $\mathbf{C}$ can be rational pullbacks of some element of $\mathbf{H}_{G,\leq r_0}$ of genus ≥ 2, as soon as the length R of $\mathbf{C}$ is sufficiently large (depending on r_0). From Lemma 3.2 and its proof, we know that no cover of inertia canonical invariant $\mathbf{C}$ can be a rational pullback of an element of $\mathbf{H}_{G,\leq r_0}$ of genus 1, as soon as $\mathbf{C}$ contains certain conjugacy classes. Altogether, if $\mathbf{C}$ contains all classes of G sufficiently often, then certainly not all covers of inertia canonical invariant $\mathbf{C}$ can be reached via rational pullback from $\mathbf{H}_{G,\leq r_0}$. □

3.1.2. *Proof of Theorem 3.1: Some dimension estimates.* To prepare the proof of Theorem 3.1, we investigate the behaviour of rational pullbacks of Galois covers.

Recall that we have introduced two different ways of associating algebraic varieties to certain sets of Galois covers: the Hurwitz spaces, and the spaces of defining equations. In Lemma 3.4 below, we relate the two concepts via a dimension estimate, stating in particular that in order to obtain defining equations for all covers in an r-dimensional Hurwitz space, we require at least r-dimensional subvarieties in the space of defining equations.

To state the lemma, denote by $\mathcal{P}^{\mathrm{sep}}_{d,e}$ the subset of separable (in Y) polynomials in $\mathcal{P}_{d,e}$. Note that this is a dense open subset of $\mathcal{P}_{d,e}$. Due to Lemma 2.7, when looking for defining equations for covers in some $\mathbf{H}_{G,\leq r_0}$, we can restrict without loss to a suitable finite union of $\mathcal{P}^{\mathrm{sep}}_{d,e}$ (for d smaller than some bound depending only on G and r_0, and in fact always with $e := |G|$).

Lemma 3.4. *Let $r, s, d, e \in \mathbb{N}$. Let $V \subset \mathcal{P}^{\mathrm{sep}}_{d,e}$ be a subvariety of dimension s. Let G be a finite group and let $(r, \mathbf{C})$ be a ramification type for G. Then the set of equivalence classes of covers $[f] \in \mathcal{H}^{in}_{G,r}(\mathbf{C})$ such that f has a defining equation in V is of dimension*

[11] In fact, $|G| = \{2,3,4,6\}$, since G is then a group of automorphisms of some elliptic curve. Cf. [Sil09, Chapter III, Theorem 10.1]

$\leq s$.[12] *In particular, if $s < r$, then there are infinitely many covers in $\mathbf{H}_{G,r}(\mathbf{C})$ which do not have a defining equation in V.*

Proof. The discriminant map $\Delta : P(T,Y) \mapsto \Delta(P) \in k[T]$ (where P is viewed as a polynomial in Y) induces an algebraic morphism from $\mathcal{P}_{d,e}$ into some space $\mathcal{P}_{\leq c}$ of polynomials in T of degree $\leq c$, viewed up to constant factors. Here we use the definition of polynomial discriminant $\Delta(\sum_{i=0}^{e} a_i Y^i) := a_e^{2e-2} \prod_{i<j}(r_i - r_j)$, where the r_i are the roots of $\sum_{i=0}^{e} a_i Y^i$, counted with multiplicities.

The fact that the degree of $\Delta(P)$ is bounded only in terms of d and e follows easily from the fact that the discriminant is a polynomial expression in the coefficients, viewed as transcendentals.

In particular, the image of V inside $\mathcal{P}_{\leq c}$ is of dimension at most $\dim(V) = s$. Note also that this image does not contain the zero polynomial, since rational pullbacks of separable polynomials remain separable.

Next, for any $r \leq t \leq c$ and any r-subset R of $\{1, \ldots, t\}$, consider the morphisms $u : (\mathbb{A}^1)^t \to \mathcal{P}_{\leq c}$ given by $(a_1, \ldots, a_t) \mapsto \prod_{i=1}^{t}(T - a_i)$ and $v : (\mathbb{A}^1)^t \to (\mathbb{A}^1)^r$ the projection on the coordinates in R. For each of these finitely many possible maps u, v, the map u is finite and so $v(u^{-1}(W))$ is of dimension $\leq s$, where $W := \Delta(V)$. But since any branch point (assumed to be finite without loss) of a cover is necessarily a root of the discriminant of a defining equation, a cover can only have a defining equation in V if its branch point set is in $v(u^{-1}(W))$ for some u, v as above. Now let $\mathcal{U}^r$ and $\mathcal{U}_r$ denote the spaces of ordered, resp., of unordered r-sets in $\mathbb{P}^1$. There is a well-defined finite morphism from $\mathcal{H}^{in}_{G,r}(\mathbf{C})$ to $\mathcal{U}_r$: the branch point reference map. Now let $\mathcal{H}' := \mathcal{H}^{in}_{G,r}(\mathbf{C}) \times_{\mathcal{U}_\mathbf{r}} \mathcal{U}^\mathbf{r}$ be the "ordered branch point set version" of the Hurwitz space $\mathcal{H}^{in}_{G,r}(\mathbf{C})$. Then the branch point reference map induces a finite morphism $\psi : \mathcal{H}' \to \mathcal{U}^r (\subset (\mathbb{P}^1)^r)$. Furthermore, $\mathcal{H}'$ has a natural finite morphism π to $\mathcal{H}^{in}_{G,r}(\mathbf{C})$ by definition. In particular, each set $\pi(\psi^{-1}(v(u^{-1}(W))))$, and thus finally also the set of $[f] \in \mathcal{H}^{in}_{G,r}(\mathbf{C})$ such that f has (only finite branch points and) a defining equation in V, is of dimension $\leq s$. The additional assertion in the case $s < r$ follows immediately, since $\psi(\mathcal{H}') \cap (\mathbb{A}^1)^r$ is of dimension r, and in fact equal to the set of all ordered r-sets in $\mathbb{A}^1$, by the Riemann Existence theorem. This concludes the proof. □

In the proof of Theorem 3.1, we will show as an intermediate result that a rational function pulling a prescribed Galois cover f back into a prescribed $\mathbf{H}_{G,R}(\mathbf{C})$ can only have a certain maximal number of branch points outside of the branch point set of f. We then require the following auxiliary result stating that varieties of rational functions with such partially prescribed branch point sets cannot be too large.

Lemma 3.5. *Let $d, m, n, s \in \mathbb{N}$, and let W be a subvariety of $\mathcal{P}^{sep}_{m,n}$. Then the subset $W' \subset W \times \mathcal{R}_d$ of all $(P, T_0) \in W \times \mathcal{R}_d$ such that at most s branch points of T_0 are not roots of $\Delta(P)$, is of dimension at most $\dim W + s + 3$.*

Proof. Denote the discriminant map on $\mathcal{P}^{\text{sep}}_{m,n}$ by Δ_1 and the one on $\mathcal{R}_d$ by Δ_2. Here we define the discriminant of a rational function $T_0(U) := T_{0,1}(U)/T_{0,2}(U)$ as the discriminant of the polynomial $T_{0,1}(U) - T \cdot T_{0,2}(U)$ with respect to U. Note that in the special case of rational functions, every root of the discriminant is in fact a branch point; see e.g. [Mül02, Lemma 3.1] for a stronger version of this statement. This means that, with $u : (a_1, \ldots, a_t) \mapsto \prod_{i=1}^{t}(T - a_i)$ as before, an element of $u^{-1}(\Delta_2(T_0))$ is already the exact branch point set of T_0, up to multiplicities.

[12] Note here that equivalent covers have the same defining equations by definition.

Consider now the following chain of maps

$$W' \subset W \times \mathcal{R}_d \xrightarrow{\mathrm{id}\times\Delta_2} W \times \mathcal{P}_{\leq t} \xleftarrow{\mathrm{id}\times u} W \times (\mathbb{A}^1)^t \xleftarrow{\alpha} W \times (\mathbb{A}^1)^t,$$

where α is defined by $\alpha(P,(a_1,\ldots,a_t)) := (P,(\Delta_1(P)(a_1),\ldots,\Delta_1(P)(a_t)))$. Clearly, all maps in this chain are morphisms, and except for the first map $\mathrm{id}\times\Delta_2$, they are all finite. Therefore $(\mathrm{id}\times\Delta_2)(W')$ is of the same dimension as $\alpha(\mathrm{id}\times(u^{-1}\circ\Delta_2))(W')$, and by definition of W', the latter is contained in one of finitely many varieties isomorphic to $W\times(\mathbb{A}^1)^s$; indeed, up to repetitions, all except for at most s roots of $\Delta_2(T_0)$ are mapped to 0 under $\Delta_1(P)$, for $(P,T_0)\in W'$. Thus, $(\mathrm{id}\times\Delta_2)(W')$ is of dimension at most $\dim(W)+s$. Theorem 2.5 then yields that W' is of dimension at most $\dim(W)+s+\dim(\Delta_2^{-1}(p))$ for any p equal to the discriminant of a rational function T_0 as above.

It remains to show that $\Delta_2^{-1}(p)$ is of dimension ≤ 3. Now the set of genus zero covers $\mathbb{P}^1\to\mathbb{P}^1$ (viewed up to equivalence) of degree d with prescribed branch point set is finite, and each such cover is given by a degree-d rational function, unique up to $\mathrm{PGL}_2(k)$-equivalence. Since $\dim(\mathrm{PGL}_2(k))=3$, the claim follows, completing the proof. □

3.1.3. *Proof of Theorem 3.1: reduction to Lemma 3.6.*

Lemma 3.6. *Let G be a finite group and $f: X\to\mathbb{P}^1$ a Galois cover with group G and genus ≥ 2. Then for every $j\in\mathbb{N}$, there exists a constant $R_0\in\mathbb{N}$, depending only on j and the branch point number of f, such that for every class-R-tuple $\mathbf{C}$ of G ($R\geq R_0$) and for every rational function $T_0:\mathbb{P}^1_k\to\mathbb{P}^1_k$ with more than $R-j$ branch points outside the branch point set of f, the pullback of f by T_0 is not in $\mathbf{H}_{G,R}(\mathbf{C})$.*

Proof of Theorem 3.1 assuming Lemma 3.6. Let $f: X\to\mathbb{P}^1\in\mathbf{H}_{G,\leq r_0,g\geq 2}$. Let g be the genus of X. Let $F:=F(T,Y)$ be a separable defining equation for f, of minimal degree in T. Using the pullback map PB as in Lemma 2.9, denote by $\mathrm{PB}(f)$ the set of all pullbacks of F by rational functions of arbitrary degree, i.e., $\mathrm{PB}(f):=\cup_{d\in\mathbb{N}}\mathrm{PB}(\{F\}\times\mathcal{R}_d)$. Then $\mathrm{PB}(f)$ contains defining equations for all rational pullbacks of the cover f.

Let $(R,\mathbf{C})$ be a ramification type for G. By the Riemann-Hurwitz formula, the genus of a Galois cover with group G arising as a degree-d pullback of f is at least $d(g-1)+1$. Since $g\geq 2$, this shows immediately that there exists $d_0\in\mathbb{N}$, depending only on $\mathbf{C}$, such that for all $d>d_0$, a degree-d pullback of f cannot have inertia canonical invariant $\mathbf{C}$ (since the genus is the same for all covers with invariant $\mathbf{C}$). In other words, to investigate the set of polynomials in $\mathrm{PB}(f)$ which are defining equations for covers in $\mathbf{H}_{G,R}(\mathbf{C})$, it suffices to restrict to pullback functions $T_0\in\mathcal{R}_d$, $d\leq d_0$, with some bound $d_0\in\mathbb{N}$ depending only on $\mathbf{C}$.

Let $D\in\mathbb{N}$ be such that every $f\in\mathbf{H}_{G,\leq r_0}$ has a separable defining equation in some space $\mathcal{P}_{d_1,|G|}$ with $d_1\leq D$. Such D exists by Lemma 2.7. Let δ be the dimension of $\mathcal{P}(D,|G|)$ (to be explicit, $\delta=(D+1)(|G|+1)-1$).

Fix an integer $j>\delta+3$, choose R_0 sufficiently large[13] and $R\geq R_0$, and denote by $\mathcal{S}_f$ the set of all rational functions T_0 which pull a given $f\in\mathbf{H}_{G,\leq r_0,g\geq 2}$ back to a connected R-branch-point cover. As seen above, the degree of such T_0 is absolutely bounded from above (in terms of the genus, and thus the branch point number of f), and by Lemma 3.6, all $T_0\in\mathcal{S}_f$ have at most $R-j$ branch points outside the branch point set of f. *A fortiori*, they are contained in the set $\mathcal{S}'_F$ of rational functions (of bounded degree as before and) with at most $R-j$ finite branch points outside the set of roots of the discriminant of $F(T,Y)$, for a defining equation $F(T,Y)=0$. The latter sets $\mathcal{S}'_F$ can be defined for all $F\in\mathcal{P}^{\mathrm{sep}}_{d_1,d_2}$ (not just for those defining Galois covers).

[13]See e.g. the proof of Lemma 3.6 for an explicit bound on R_0.

Now consider the set $\mathcal{S} := \cup_{d_1 \le D} \cup \{F\} \times \mathcal{S}'_F$, where the inner union is over all $F \in \mathcal{P}^{\mathrm{sep}}_{d_1,|G|}$. From Lemma 3.5 (with $W := \mathcal{P}^{\mathrm{sep}}_{d_1,|G|}$) it follows that $\mathcal{S}$ is contained in a a finite union of varieties, of dimension at most $\dim(\mathcal{P}_{D,|G|}) + R - j + 3 \le \delta + R - j + 3 < R$.

Therefore the image of $\mathcal{S}$ under PB is of dimension strictly smaller than R as well. On the other hand, Lemma 3.4 shows that no finite union of varieties of dimension $< R$ can contain defining equations for all elements of $\mathbf{H}_{G,R}(\mathbf{C})$. Hence $\mathbf{H}_{G,\le r_0, g\ge 2}$ is not k-regularly parametric. This proves the assertion. □

3.1.4. *Proof of Lemma 3.6.*

First step: Explicit choice of R_0.

Let $t_1, \dots, t_s$ be the branch points of f and let $e_1, \dots, e_s$ be the corresponding orders of inertia groups of f. By the Riemann-Hurwitz formula, the genus g of f fulfills

$$g - 1 = \frac{1}{2}|G|(s - 2 - \sum_{i=1}^{s} \frac{1}{e_i}),$$

and since $g \ge 2$, Hurwitz's automorphism theorem yields $|G| \le 84(g-1)$, yielding in total that

$$s - 2 - \sum_{i=1}^{s} \frac{1}{e_i} \ge 1/42. \tag{1}$$

We may assume without loss that $j > 3$, and we pick $R_0 \in \mathbb{N}$ such that $R_0 > 42s(j-3)$.

Let $R \ge R_0$, and let $(R, \mathbf{C})$ be a ramification type for G. Let $T_0 : \mathbb{P}^1_k \to \mathbb{P}^1_k$ be a rational function such that the pullback of f by T_0 defines a Galois cover with inertia canonical invariant $\mathbf{C}$, and let $\mathcal{T}$ (resp., d) be the ramification type (resp., the degree) of T_0.

Note that, since the branch point number of a degree-d rational pullback of f is trivially bounded from above by sd, our choice $R_0 > 42s(j-3)$ implies $d > 42(j-3)$, and thus, using (1), we obtain

$$d\sum_{i=1}^{s} 1/e_i \le d(s - 2 - 1/42) < d(s-2) - (j-3). \tag{2}$$

Second step: Translation into a combinatorial statement.

Let $\sigma_1, \dots, \sigma_s \in S_d$ be the inertia group generators of T_0 at $t_1, \dots, t_s$, and $\sigma_{s+1}, \dots, \sigma_{s+m}$ the non-trivial inertia group generators at further points. For $\sigma \in S_d$, denote by $o(\sigma)$ the number of orbits of $\langle\sigma\rangle$, and set $\mathrm{ind}(\sigma) = d - o(\sigma)$. We claim that, assuming choice of R_0 as above, the following holds:

Claim:

$$\sum_{i=1}^{s} \mathrm{ind}(\sigma_i) \ge 2d - 2 - R + j,$$

or equivalently:

$$\sum_{i=1}^{s} o(\sigma_i) \le d(s-2) - j + 2 + R. \tag{3}$$

The assertion then follows from (3), since T_0 defines a genus-zero cover, whence the Riemann-Hurwitz genus formula yields $\sum_{i=1}^{s+m} \mathrm{ind}(\sigma_i) = 2d - 2$. Together with the claim, this enforces $m \le R - j$.

Third step: Transformation of cycle structures.

To prove the claim, consider the cycle structures of σ_i $(i = 1, \dots, s)$. We will manipulate the cycle structures of the σ_i in a controlled way, to make it easier to estimate the total

number of orbits of all σ_i $(i = 1, \dots, s)$.
By the definition of T_0 and by Abhyankar's lemma, the cycle lengths of the σ_i are multiples of e_i, for $i = 1, \dots, s$, with a total of exactly R exceptions over all $i \in \{1, \dots, s\}$.

Let $n_i \in \mathbb{N}$ be such that $n_i \cdot e_i$ is the sum of all "non-exceptional" cycle lengths (i.e., of those which are multiples of e_i) in σ_i. Now for each $i \in \{1, \dots, s\}$, let τ_i be a permutation of cycle structure $[e_i^{n_i}, r_i]$, where r_i is the sum of all exceptional cycle lengths in σ_i. We then have $o(\tau_i) \leq \lfloor d/e_i \rfloor + 1$ for all $i = 1, \dots, s$, with strict inequality if $r_i = 0$ or $r_i \geq e_i$. Let $t \in \mathbb{N}$ be the number of i with $1 \leq r_i < e_i$. It follows that $\sum_{i=1}^s o(\tau_i) \leq \sum_{i=1}^s \lfloor d/e_i \rfloor + t \leq (d \sum_{i=1}^s 1/e_i) + t$. Using (2), this implies

$$\sum_{i=1}^{s} o(\tau_i) \leq (d(s-2) - (j-3) + t) - 1 = d(s-2) - j + 2 + t.$$

Furthermore, it follows from the definition of the τ_i that

$$\sum_{i=1}^{s} o(\tau_i) \geq \sum_{i=1}^{s} o(\sigma_i) - (R - t),$$

since a total of R cycles of length not divisible by e_i in the σ_i gets replaced by a total of $\geq t$ cycles in the τ_i, and the number of non-exceptional cycles in τ_i is at least as large as in σ_i. In total, $\sum_{i=1}^s o(\sigma_i) \leq d(s-2) - j + 2 + R$, showing the claim. This completes the proof.

3.2. **Proof of Theorem 1.1(b).** We continue with proving the (b) part of Theorem 1.1, for which the assumption on G is stronger than not being a subgroup of $\mathrm{PGL}_2(\mathbb{C})$.

Fix a finite group G with at least 5 non-conjugate maximal cyclic subgroups. At first assume that not all maximal conjugacy classes are of order 2. Let $\gamma_1, \dots, \gamma_5$ be generators of 5 non conjugate maximal cyclic subgroups of G and let $\mathcal{C}_1, \dots, \mathcal{C}_5$ be their conjugacy classes. Denote the order of γ_i by e_i, $i = 1, \dots, 5$ and without loss of generality assume $e_1 > 2$. Consider then a tuple $(\mathcal{C}_1, \dots, \mathcal{C}_5, \mathcal{C}_6, \dots, \mathcal{C}_s)$ of conjugacy classes of G, not necessarily distinct, and satisfying the following:

(A) all the non-trivial conjugacy classes of G, but the powers $\mathcal{C}_i^j$, $i = 1, \dots, 4$, $j = 1, \dots, e_i - 1$, appear in the set $\{\mathcal{C}_5, \dots, \mathcal{C}_s\}$.

Consider the $(2s)$-tuple $\underline{\mathcal{C}} = (\mathcal{C}_1, \mathcal{C}_1^{-1}, \dots, \mathcal{C}_s, \mathcal{C}_s^{-1})$. Note that the integer s can be taken to be any suitably large integer, for example by repeating the conjugacy class $\mathcal{C}_5$. Picking an element $g_i \in \mathcal{C}_i$, we form the tuple $\underline{g} = (g_1, g_1^{-1}, \dots, g_s, g_s^{-1})$.

Since the elements of $\underline{g}$ and their powers contain at least one element from each conjugacy class, a classical lemma of Jordan implies that $\underline{g}$ forms a generating set of G. By construction the product in $\underline{g}$ is 1. From the Riemann Existence Theorem, the set $\mathbf{H}_{G,2s}(\underline{\mathcal{C}})$ of Galois covers $X \to \mathbb{P}^1$ with group G, $2s$ branch points and inertia canonical invariant $\underline{\mathcal{C}}$, is nonempty.

Let h be a cover in the set $\mathbf{H}_{G,2s}(\underline{\mathcal{C}})$. Assume there exist $r_0 \in \mathbb{N}$, a Galois cover $f \in \mathbf{H}_{G,\leq r_0}$ and $T_0 \in \mathbb{C}(U) \setminus \mathbb{C}$ of degree N, such that h and f_{T_0} are isomorphic. Denote the branch point number of f by r $(r \leq r_0)$ and its inertia canonical invariant by $\mathbf{C} = (C_{f,1}, \dots, C_{f,r})$. By [Dèb18, §3.1], the inertia canonical invariant of f_{T_0} is a tuple $\mathbf{C}_{f,T_0}$ obtained by concatenating tuples of the form $\mathbf{C}_{f,T_0,j} = (C_{f,j}^{e_{j1}}, \dots, C_{f,j}^{e_{jr_j}})$, $j = 1, \dots, r$, where $r_j, e_{j,\ell}$ are integers with $r_j \geq 0$ and $e_{j,\ell} \geq 1$ for all $\ell = 1, \dots, r_j$, and $j = 1, \dots, r$. Note that some of the classes in $\mathbf{C}_{f,T_0}$ might be trivial.

Denote by p_j (resp., q_j) the number of $e_{j,\ell}$'s, $\ell = 1, \dots, r_j$, equal to 1 (resp., > 1), for $j = 1, \dots, r$. For $j = 1$, denote further by u_j (resp., v_j) the number of $e_{1,\ell}$'s, $\ell = 1, \dots, r_1$,

equal to 2 (resp., > 2). Recall further from [Dèb18, §3.1] that since $e_{j1}, \ldots, e_{jr_j}$ are the ramification indices of T_0 over some point, we have $\sum_{\ell=1}^{r_j} e_{j,\ell} = N$, for $j = 1, \ldots, r$. Hence, $p_j + 2q_j \leq N$, and $p_1 + 2u_1 + 3v_1 \leq N$, or equivalently:

$$q_j \leq \frac{N - p_j}{2} \leq \frac{N}{2} \text{ for } j = 2, \ldots, r \text{ and } v_1 \leq \frac{N - p_1 - 2u_1}{3} \leq \frac{N}{3}. \tag{4}$$

By the Riemann–Hurwitz formula for T_0, we also have

$$2N - 2 \geq \sum_{\ell=1}^{r_1}(e_{1,\ell} - 1) + \sum_{j=2}^{r}\sum_{\ell=1}^{r_j}(e_{j,\ell} - 1) = N - p_1 - u_1 - v_1 + \sum_{j=2}^{r}(N - p_j - q_j). \tag{5}$$

As f_{T_0} and h are isomorphic, the tuples $\mathbf{C}_{f,T_0}$ and $\underline{\mathcal{C}}$ are equal, up to order. Without loss of generality we may assume $\mathcal{C}_1 \in \mathbf{C}_{f,T_0,1}$. For each index $i = 1, \ldots, 4$, if $j_i \in \{1, \ldots, r\}$ is an index such that $\mathcal{C}_i \in \mathbf{C}_{f,T_0,j_i}$ [14], then, as $\langle \gamma_i \rangle$ is a maximal cyclic subgroup of G, one has $\mathcal{C}_i = C_{f,j_i}^{w_i}$ for some integer w_i relatively prime to e_i. This together with the assumption that $\mathcal{C}_1, \ldots, \mathcal{C}_4$ are not powers of each other, implies that the correspondence $i \mapsto j_i$ is injective. Thus (5) and (4) give

$$2N - 2 \geq N - p_1 - u_1 - v_1 + \sum_{i=2}^{4}(N - p_{j_i} - q_{j_i}) > \frac{13}{6}N - (p_1 + u_1) - \sum_{i=2}^{4} p_{j_i},$$

and hence

$$N < 6(p_1 + u_1 + \sum_{i=2}^{4} p_{j_i}). \tag{6}$$

Since each $\mathcal{C}_i$, $i = 1, \ldots, 4$, appears at most twice in $\mathbf{C}_{f,T_0}$ by (A), it follows that $p_{j_i} \leq 2$ for $i = 1, \ldots, 4$. Furthermore, since the powers of $\mathcal{C}_1$ appear at most twice and $e_1 > 2$, we also have $p_1 + u_1 \leq 2$. Thus (6) gives $N < 48$. However, by a priori choosing s to be large, the degree N of T_0 is forced to be at least 48, contradiction.

It remains to consider the case where all maximal conjugacy classes are of order 2. In this case G is an elementary abelian 2-group of rank at least 3. It follows that the number of maximal conjugacy classes of cyclic groups is at least 7. Repeating the above argument with seven classes $\mathcal{C}_1, \ldots, \mathcal{C}_7$, replacing the previous $\mathcal{C}_1, \ldots, \mathcal{C}_5$, (5) and (4) take the form:

$$2N - 2 \geq \sum_{j=1}^{r}(N - p_j - q_j) \text{ and } q_{j_i} \leq \frac{N - p_{j_i}}{2} \leq \frac{N}{2} \text{ for } i = 1, \ldots, 6.$$

Thus, their combination gives:

$$2N - 2 \geq \sum_{i=1}^{6}(N - p_{j_i} - q_{j_i}) > 3N - \sum_{i=1}^{6} p_{j_i},$$

and hence $N < \sum_{i=1}^{6} p_{j_i}$. Once again choosing s and hence N large enough we obtain a contradiction.

[14] There may be *a priori* two different indices $j_i \in \{1, \ldots, r\}$ such that $\mathcal{C}_i \in \mathbf{C}_{f,T_0,j}$.

3.3. **Extension to more general fields.** We assume that the field k is algebraically closed in our proof of Theorem 1.1 because we use the Riemann Existence Theorem. However, as we explain below, this assumption can be relaxed in some situations.

Theorem 3.7. *Let G be a finite group and let k be a field of characteristic* 0.
(a) *Theorem 1.1*(a) *holds in each of these situations:*
  (a-1) *k is ample*[15]*,*
  (a-2) *G is abelian of even order,*
  (a-3) *G is the direct product $A \times H$ of an abelian group A of even order and of a non-solvable group H occuring as a regular Galois group over k* [16]*,*
  (a-4) *$G = S_5$.*
(b) *Theorem 1.1*(b) *holds if either k is ample or G is abelian.*

In particular, the full Theorem 1.1 holds if k is ample.

3.3.1. *Proof of Theorem 3.7*(b). In the proof of Theorem 1.1(b) (§3.2), the assumption $k = \overline{k}$ was only used to guarantee that there is at least one k-cover in the Hurwitz stack $\mathbf{H}_{G,2s}(\underline{\mathcal{C}})$. When k is no longer algebraically closed, we first slightly modify the tuple $\underline{\mathcal{C}}$ to make it *k-rational*, i.e., such that the action of $\mathrm{Gal}(\overline{k}/k)$ on $\underline{\mathcal{C}}$ (taking the power of the classes by the cyclotomic character) preserves $\underline{\mathcal{C}}$, up to the order. This can be done by replacing, for each index $i = 1, \dots, 4$,

$$\text{each pair } (\mathcal{C}_i, \mathcal{C}_i^{-1}) \text{ by the tuple } (\mathcal{C}_i, \mathcal{C}_i^{-1}, , \dots, \mathcal{C}_i^{e_i-1}, \mathcal{C}_i^{-(e_i-1)}).$$

The modified tuple is indeed k-rational and the proof of Theorem 1.1(b) still holds after some slight adjustments: inequalities $p_{j_i} \leq 2$ become $p_{j_i} \leq 2(e_i - 1)$, $i = 1, \dots, 4$, which only changes the constants in the final estimates.

With the tuple $\underline{\mathcal{C}}$ now k-rational, it is still true that the Hurwitz stack $\mathbf{H}_{G,2s}(\underline{\mathcal{C}})$ has a k-cover, and so that Theorem 1.1(b) holds, in the following situations:
- G abelian and k arbitrary (as a consequence of the classical rigidity theory, see e.g., [MM99, Chapter I, §4] or [Völ96, §3.2]), and
- k ample and G arbitrary. Namely, recall that over a complete discretely valued field k, the so-called 1/2-Riemann Existence Theorem of Pop [Pop96] can be used to ensure that $\mathbf{H}_{G,2s}(\underline{\mathcal{C}})(k)$ is non-empty. Furthermore this last conclusion extends to ample fields, via some classical specialization argument [Pop96, Proposition 1.1] [DD97a, §4.2].

3.3.2. *Proof of Theorem 3.7*(a). We will deduce Theorem 3.7(a) from Theorem 3.9 below. Start with an arbitrary field k and consider the following condition, for a finite group G.

Condition 3.8. (a) *There exist a constant $m \geq 0$, infinitely many integers R, and for each R a ramification type $(R, \mathbf{C})$ for G such that the set of all equivalence classes $[f] \in \mathcal{H}^{in}_{G,R}(\mathbf{C})$ such that f is a k-Galois cover cannot be covered by finitely many varieties of dimension $< R - m$ (in $\mathcal{H}^{in}_{G,R}(\mathbf{C})(\overline{k})$).*
(b) *Each $\mathbf{C}$ in* (a) *contains every conjugacy class of G at least once.*

We then have the following analog of Theorem 3.1 and Lemma 3.2:

Theorem 3.9. *Assume that G fulfills Condition 3.8(a) (resp., Condition 3.8(a) and (b)) over k. Let $r_0 \in \mathbb{N}$, and let $\mathbf{H} := \mathbf{H}_{G,\leq r_0, g\geq 2}(k)$ (resp., $\mathbf{H} := \mathbf{H}_{G,\leq r_0, g\geq 1}(k)$) be the set of k-Galois covers with group G, branch point number $\leq r_0$ and genus ≥ 2 (resp., ≥ 1). Then there are infinitely ramification types $(R, \mathbf{C})$ for G over k such that $\mathbf{H}_{G,R}(\mathbf{C})(k) \not\subset \mathrm{PB}(\mathbf{H})$. In particular, $\mathbf{H}$ is not k-regularly parametric.*

[15] Definition of "ample field" is recalled in §1.1.

[16] In fact, the assumption on H to be non-solvable can be removed with a bit of extra effort.

Proof. Observe that the crucial Lemma 3.6 in the proof of Theorem 3.1 (§3.1.3) guarantees the following: there exists $R_0 \in \mathbb{N}$, such that for every ramification type $(R, \mathbf{C})$ for G ($R \geq R_0$), the set of (defining equations of) G-covers with inertia canonical invariant $\mathbf{C}$ which arise as rational pullbacks of some cover with $\leq r_0$ branch points is contained in a union of finitely many varieties of dimension at most $R-(m+1)$. Then, with R sufficiently large and $(R, \mathbf{C})$ as in Condition 3.8, it follows as in Lemma 3.4 that these varieties are not sufficient to yield defining equations for every cover in $\mathbf{H}_{G,R}(\mathbf{C})(\overline{k})$ which is defined over k. Furthermore, the additional Condition 3.8(b) is sufficient for the proof of Lemma 3.2 over k, if G is non-cyclic. For cyclic $G = \mathbb{Z}/n\mathbb{Z}$, Lemma 3.2 holds as soon as the genus-0 extension $k(\sqrt[n]{T})/k(T)$ is k-regular, i.e., as soon as $e^{2ipi/n} \in k$. On the other hand, Galois groups of genus-1 cyclic covers are only $\mathbb{Z}/n\mathbb{Z}$ for $n \in \{2,3,4,6\}$, and it is easy to verify that for $e^{2ipi/n} \notin k$, these genus-1 covers cannot be defined over k either, as a special case of Branch Cycle Lemma (see [Fri77] and [Völ96, Lemma 2.8]). □

Proof of Theorem 3.7(a-1). Let k be an ample field of characteristic zero. Equivalently to the definition of "ample", every absolutely irreducible variety over k with a simple k-rational point has a Zariski-dense set of k-rational points, see [Jar11, Lemma 5.3.1]. On the other hand, the 1/2-Riemann Existence Theorem yields plenty of class r-tuples $\mathbf{C}$ of G such that $\mathbf{H}_{G,r}(\mathbf{C})(k)$ is non-empty. For example, all $\mathbf{C}$ corresponding to an arbitary long repetition of the tuple $(x_1, x_1^{-1}, \ldots, x_n, x_n^{-1})$, where x_i runs through all non-identity elements of G, are fine. For $Z(G) = \{1\}$, this then implies the existence of a k-rational point on $\mathcal{H}^{in}_{G,r}(\mathbf{C})$, and therefore in fact of a Zariski-dense set of k-rational points. Since these k-rational points are exactly the equivalence classes of covers f defined over k, Condition 3.8 holds, even with $m = 0$, and therefore the assertion of Theorem 3.9 holds over k. Finally, by an easy and classical argument, the case of arbitrary G can be reduced to the above assumption $Z(G) = \{1\}$ upon embedding G as a quotient into a group with trivial center. □

Proof of Theorem 3.7(a-2). As a first example, let G be an elementary abelian 2-group. Since G is abelian, every tuple $(C_1, \ldots, C_R)$ of conjugacy classes in G with non-empty Nielsen class is a rigid tuple. Furthermore, since all non-identity elements of G are of order 2, every conjugacy class is trivially *rational* (i.e., unchanged if taken to a power relatively prime to the order of its elements). It then follows from the rigidity method that for every choice $(t_1, \ldots, t_R)$ of R distinct points in $\mathbb{P}^1(k)$, there exists a Galois cover of $\mathbb{P}^1$, defined over k, with inertia canonical invariant $(C_1, \ldots, C_R)$ and branch points $(t_1, \ldots, t_R)$. In particular, the set of all these covers cannot be obtained by a set of defining equations of dimension $< R$. Hence G fulfills Condition 3.8 over k. The assertion of Theorem 3.9 therefore holds for G over an arbitrary field of characteristic zero.

As a next step, let G be an arbitrary abelian group of even order. As before, all class tuples with non-empty Nielsen class are rigid. Let $(C_1, \ldots, C_R)$ be a class tuple of G containing each element of order ≥ 3 exactly once, and each element of order 2 an arbitrary even number of times. This then yields a product-1 tuple generating G, and if the branch points for each set of generators of a cyclic subgroup $\mathbb{Z}/e\mathbb{Z}$ are chosen appropriately to form a full set of conjugates (under the action of $\mathrm{Gal}(\mathbb{Q}(e^{2ipi/e})/\mathbb{Q})$) in $k(e^{2ipi/e})$, then the associated ramification type is a rational ramification type, implying that there is again a k-Galois cover with inertia canonical invariant $(C_1, \ldots, C_R)$ and with the prescribed branch point set. Note that the branch points for elements of order 2 are still allowed to be chosen freely in k. Since there are less than $|G|$ other branch points, it follows as above that the set of Galois covers with these ramification data

cannot be obtained by a set of defining equations of dimension $\leq R - |G|$. Therefore again, Condition 3.8 is fulfilled. □

Proof of Theorem 3.7(a-3). Now, let $G = A \times H$, where A is an abelian group of even order and H is any non-solvable group which occurs as a regular Galois group over k. We use the non-solvability assumption only to obtain that there are then no Galois covers of genus ≤ 1 with group H, and a fortiori none with group G. Take a tuple $(C_1, \ldots, C_R)$ of classes of $A \leq G$ as in the previous case, and prolong it by a fixed tuple $(C_{R+1}, \ldots, C_S)$ of classes which occurs as some ramification type for H over k. With the appropriate choice of branch point set for the H-cover, we obtain a Galois cover with group $A \times H$, where once again the branch points with involution inertia in A can be chosen freely (outside of the fixed branch points of the H-cover). Increasing R as above (whilst fixing $(C_{R+1}, \ldots, C_S)$), we again obtain that Condition 3.8(a) is fulfilled, and so the assertion of Theorem 3.9 holds over k for Galois covers of genus ≥ 2. Since G has no Galois covers of genus ≤ 1, Theorem 1.1(a) holds for G over all fields of characteristic 0. □

Proof of Theorem 3.7(a-4). Let $H_{g,d}$ denote the moduli space of simply branched covers (i.e., all non-trivial inertia groups are generated by transpositions) of degree d and genus g. It is known ([AC81]) that $H_{g,5}$ is unirational for all $g \geq 6$, and in fact, this holds even over the smallest field of definition $\mathbb{Q}$ (and therefore over all fields of characteristic zero).

Note that $H_{g,5}$ parameterizes S_5-covers with inertia canonical invariant $(C_1, \ldots, C_{8+2g})$, where each C_i is the class of transpositions. This space is of dimension $8 + 2g$, and unirationality (over k) implies that its function field is of finite index in some $k(T_1, \ldots, T_{8+2g})$ with independent transcendentals T_i. But of course, every k-rational value of $(T_1, \ldots, T_{8+2g})$ then leads to a k-rational point on $H_{g,5}$ (and thus, a cover defined over k), and the set of such k-rational points on a unirational variety is always Zariski-dense.

This implies that Condition 3.8(a) is fulfilled, and since S_5 does not possess Galois covers of genus ≤ 1, Theorem 1.1(a) holds for S_5 over all fields of characteristic 0, thus concluding the proof. It would be interesting to find out if something similar can be obtained for larger S_n. □

4. Regular Parametricity - Part Two, Proof of Theorem 1.2

Throughout the section fix an algebraically closed field k of characteristic 0 and a Galois cover $f : X \to \mathbb{P}^1$ with group G and ramification type $(r, \mathbf{C})$. Assume G is not a subgroup of $PGL_2(\mathbb{C})$. We treat here the case $r \geq 4$. The case $r = 3$ is more technical and is treated with similar tools in Appendix A. Let $\mathbf{t} = \{t_1, \ldots, t_r\}$ be the branch point set of f. Let $e_f(t_0)$ denote the ramification index of $t_0 \in \mathbb{P}^1$ under f, and set $e_i = e_f(t_i)$ for $i = 1, \ldots, r$. Given $T_0 \in k(U) \setminus \mathbb{P}^1$ and $t_0 \in k$, let $e(q|t_0)$ denote the ramification index under T_0 of $q \in T_0^{-1}(t_0)$. The proof is based on the following estimate on the number of branch points of a pullback, which strengthens the bounds in [Dèb18, Theorem 3.1(b-2)].

Lemma 4.1. *Let $T_0 \in k(U) \setminus k$ be of degree n such that the pullback f_{T_0} is connected. Let a_i be the number of preimages $q \in T_0^{-1}(t_i)$ with $e_i \mid e(q|t_i)$ for $i = 1, \ldots, r$, and let $U_{T_0,f}$ be the set of points $q \in \mathbb{P}^1$ such that $e(q|t_0) \neq e_f(t_0)$ for $t_0 = T_0(q)$. Then the number r_{T_0} of branch points of f_{T_0} is at least*

$$r_{T_0} \geq (r-4)n + 4 + \sum_{i=1}^{r}(e_i - 2)a_i + \sum_{q \in U_{T_0,f}} \big(e(q|t_0) - 1\big).$$

Moreover, equality holds if and only if T_0 is unramified away from $\mathbf{t}$ and its ramification indices over t_i are either e_i or not divisible by e_i, for $i = 1, \ldots, r$.

Proof. Let b_i denote the number of preimages q in $T_0^{-1}(t_i)$ such that $e(q|t_i)$ is not divisible by e_i, for $i = 1, \ldots, r$. Note that since f_{T_0} is connected, Abhyankar's lemma implies that

$$r_{T_0} = \sum_{i=1}^{r} b_i. \tag{7}$$

By the Riemann–Hurwitz formula for T_0 one has:

$$2n-2 = \sum_{t_0 \in \mathbb{P}^1} \sum_{q \in T_0^{-1}(t_0)} (e(q|t_0)-1) \geq \sum_{q \in U_{T_0,f}} \big(e(q|t_0)-1\big) + \sum_{i=1}^{r} (e_i - 1)a_i, \tag{8}$$

with equality if and only if $e(q|t_i)$ is either e_i or non-divisible by e_i, for all points $q \in T_0^{-1}(t_i), i = 1, \ldots, r$. The same Riemann–Hurwitz formula also implies

$$2n-2 \geq \sum_{i=1}^{r} (n - a_i - b_i) = rn - \sum_{i=1}^{r} (a_i + b_i),$$

with equality if and only if T_0 is unramified away from $\mathbf{t}$. Combined with (8) this gives:

$$\begin{aligned} 2n-2 &\geq rn - \sum_{i=1}^{r} (a_i + b_i) \\ &\geq rn + \sum_{i=1}^{r} (e_i - 2)a_i + \sum_{q \in U_{T_0,f}} \big(e(q|t_0)-1\big) - (2n-2) - \sum_{i=1}^{r} b_i. \end{aligned}$$

Combined with (7) this gives

$$r_{T_0} = \sum_{i=1}^{r} b_i \geq (r-4)n + 4 + \sum_{i=1}^{r} (e_i - 2)a_i + \sum_{q \in U_{T_0,f}} \big(e(q|t_0)-1\big), \tag{9}$$

with equality if and only if T_0 is unramified away from $\mathbf{t}$ and every ramification index $e(q|t_i)$ for $q \in T_0^{-1}(t_i)$, $i = 1, \ldots, r$ which is divisible by e_i, is equal to e_i. □

Let E denote the multiset $\{e_1, \ldots, e_r\}$.

Proof of Theorem 1.2 when $r \geq 4$ and $E \neq \{2,2,2,3\}, \{2,2,2,4\}$. The case where f is of genus 1 follows from Remark 3.3, so henceforth we shall assume that the genus of X is at least 2. Let $(g_1, \ldots, g_r)$ be a tuple in the Nielsen class of $\mathbf{C}$, corresponding to f. As any permutation of the tuple $\mathbf{C} = (C_1, \ldots, C_r)$ has a non-empty Nielsen class, without loss of generality we may assume that g_i is a branch cycle over t_i and the orders $e_1, \ldots, e_r$ of $g_1, \ldots, g_r$ are ordered in decreasing order. This tuple can be modified to a tuple (P_y) $y, y^{-1}g_1, \ldots, g_r$ for any $y \neq g_1$. Such a tuple generates G and has product 1, giving a non-empty Nielsen class corresponding to a ramification type which we denote by $(r+1, \mathbf{D}_y)$. We will show that for a suitable choice of $y \in G$, no connected pullback f_{T_0}, along $T_0 \in k(U) \setminus k$ of degree $n > 1$, has ramification type $(r+1, \mathbf{D}_y)$. Since a cover with ramification type $(r+1, \mathbf{D}_y)$ is a pullback of f only if y is a power of some element in $C_1, \ldots, C_r$, by varying y, we may assume that every conjugacy class in G is a power of one of $C_1, \ldots, C_r$.

As in Lemma 4.1, let a_i (resp. b_i) denote the number of preimages q in $T_0^{-1}(t_i)$ such that the ramification index $e(q|t_i)$ is divisible by e_i (resp. is not divisible by e_i) for $i = 1, \ldots, r$. For $r \geq 6$, as $n \geq 2$, the lower bound on r_{T_0} from Lemma 4.1 is at least $r+2$, as desired.[17]

[17] We note that for $r \geq 6$, this claim also follows for any choice of y from [Dèb18, Theorem 3.1.(b-2)], since the latter implies that every pullback of $\mathbf{C}$ has at least $r+2$ branch points, and hence is not in $\mathbf{H}_{G,r}(\mathbf{D}_y)$.

The case $r = 5$**:** We may assume $r_{T_0} = 6$. By Lemma 4.1

$$n \leq 2 - \sum_{i=1}^{r}(e_i - 2)a_i - \sum_{q \in U_{T_0,f}} \big(e(q|t_0) - 1\big).$$

As $n > 1$, this forces $n = 2$, $e(q|t_0) = 1$ for all $q \in U_{T_0,f}$, and $\sum_{i=1}^{r}(e_i - 2)a_i = 0$. Thus, every ramification index of T_0 over t_i is either e_i or 1, and T_0 is unramified away from $\mathbf{t}$. Since T_0 is of degree 2, it ramifies over exactly two branch points with ramification index 2. Hence without loss of generality we may assume $e_4 = e_5 = 2$, so that the inertia canonical invariant of f_{T_0} is $\mathbf{C}_{T_0} = (C_1, C_1, C_2, C_2, C_3, C_3)$. If $e_1 > 2$, by picking y to be an involution, then every cover with ramification type $(r + 1, \mathbf{D}_y)$ is not a pullback of f, as $\mathbf{D}_y$ has more conjugacy classes of involutions than $\mathbf{C}_{T_0}$ does. Similarly, if $e_1 = 2$ and G contains an element y of order > 2, then every cover whose ramification type coincides with $(r + 1, \mathbf{D}_y)$ is not a pullback of f, as its Nielsen class has a conjugacy class of non-involutions. If $e_1 = 2$ and all elements of G are of order 2, then G is an elementary abelian 2-group generated by three conjugacy classes (C_1, C_2, C_3). As G is not a subgroup of $\mathrm{PGL}_2(\mathbb{C})$, this forces $G \cong (\mathbb{Z}/2\mathbb{Z})^3$. In the latter case, we may choose y to be an involution whose conjugacy class is different from C_1, C_2, C_3, C_4, C_5, so that every cover with ramification type $(r + 1, \mathbf{D}_y)$ is not a pullback of f.

The case $r = 4$**:** Assume $r_{T_0} = 5$. By Lemma 4.1

$$\sum_{i=1}^{r}(e_i - 2)a_i + \sum_{q \in U_{T_0,f}} \big(e(q|t_0) - 1\big) \leq 1. \tag{10}$$

Let $\mathbf{t}_2$ (resp. $\mathbf{t}_{>2}$) denote the set of t_i with $e_i = 2$ (resp. $e_i > 2$). Since every point $q \in T_0^{-1}(t_i)$, $t_i \in \mathbf{t}_2$, with ramification index $e(q|t_0) > 2$ contributes at least 2 to (10), we deduce that $e(q|t_i) = 1$ or 2 for all $q \in T_0^{-1}(t_i)$, $t_i \in \mathbf{t}_2$. On the other hand for $t_i \in \mathbf{t}_{>2}$, (10) gives $a_i = 0$ with the possible exception of a single t_ι for which $a_{t_\iota} = 1$ and $e_\iota = 3$. Moreover, if such ι exists, then the contribution of the sum over $U_{T_0,f}$ in (10) is 0, and hence

$$\begin{aligned} &e(q|t_i) = 1 \text{ for all points } q \in T_0^{-1}(t_i),\ t_i \in \mathbf{t}_{>2}, \text{ with the possible} \\ &\text{exception of a single } q_\iota \in T_0^{-1}(t_\iota) \text{ where } e_\iota = e(q_\iota|t_\iota) = 3. \end{aligned} \tag{11}$$

Otherwise $a_i = 0$ for all $t_i \in \mathbf{t}_{>2}$, in which case (10) shows that

$$\begin{aligned} &e(q|t_i) = 1 \text{ for all points } q \in T_0^{-1}(t_i),\ t_i \in \mathbf{t}_{>2}, \text{ with the possible} \\ &\text{exception of a single } q_\eta \in T_0^{-1}(t_\eta) \text{ where } e(q_\eta|t_\eta) = 2 \neq e_\eta. \end{aligned} \tag{12}$$

If G is of odd order, (11) and (12) force T_0 to have at most one ramification point, which by the Riemann–Hurwitz formula forces a contradiction to $n > 1$. Henceforth assume G is of even order.

Let $a = \#\mathbf{t}_{>2}$. Since the genus of X is more than 1 and $r = 4$, the Riemann–Hurwitz formula for f implies that $a \geq 1$. Assume first that $a > 1$. In this case we let $y \in G$ be an involution. The number of elements of order > 2 in (P_y) is a or $a - 1$. In case there exists ι as above, (11) forces every point $t_i \in \mathbf{t}_{>2} \setminus \{t_\iota\}$ to have at least three unramified preimages and hence forces f_{T_0} to have at least $3(a - 1)$ branch points with ramification index > 2. As $3(a-1) > a$ for $a > 1$, f_{T_0} does not not have ramification type $(r+1, \mathbf{D}_y)$. The same argument applies if (12) holds and $n \geq 3$. If $n = 2$ and (12) holds, then f_{T_0} has at least $2(a-1)+1$ branch points with ramification index > 2. Similarly $2(a-1)+1 > a$ and hence f_{T_0} does not have ramification $(r + 1, \mathbf{D}_y)$.

Henceforth assume $a = 1$, that is $E = \{e, 2, 2, 2\}$. Note that $e > 4$ by assumption. Condition (11) does not hold since $e > 3$, and hence (12) does. The latter implies that

the inertia canonical conjugacy classes of f_{T_0} over points in $T_0^{-1}(t_1)$ are either C_1 or C_1^2, hence of order e or $e/2$. Thus if we pick y to be of order different from e and $e/2$, then the only element of (P_y) that can appear in such conjugacy class is yx_1. Thus, (12) implies that

(13) $T_0^{-1}(t_1)$ consists of a single point q_η with ramification $e(q_\eta|t_1) = 2$ such that the inertia canonical invariant of f_{T_0} over q_η is the conjugacy class of yx_1.

The latter then has to be of order $\tilde{e} = e/2$ or e.

At first consider the case where the conjugacy classes C_2, C_3, C_4 do not coincide. Without loss of generality we may then assume that C_2 is different from C_3 and C_4. Picking $y = x_3$, (13) implies that $n = 2$, and $(r+1, \mathbf{D}_y)$ is a ramification type consisting of conjugacy classes of orders $2, \tilde{e}, 2, 2, 2$, with $\tilde{e} = e$ or $e/2$. In particular, $\tilde{e} > 2$ and C_2 appears at most once in $\mathbf{D}_y$. Since $n = 2$ and f_{T_0} is assumed to have 5 branch points, T_0 has to ramify over exactly one of the places t_2, t_3, t_4, say t_k. If $k = 2$, then C_2 does not appear in the ramification type of f_{T_0}, contradicting its appearance in $\mathbf{D}_y$. If $k = 3$ or 4, then t_2 is unramified under T_0 and hence C_2 appears at least twice in the ramification type of f_{T_0}, but only once in $\mathbf{D}_y$, contradiction.

Now consider the case $C_2 = C_3 = C_4$. Note that since G is non-cyclic, C_2 is not a power of C_1. Assume next that e is even. We may then pick y to be an involution which is a power of x_1. As y is not of order e or $e/2$, we get that $y \notin C_1 \cup C_1^2 \cup C_2$, contradicting that those are the only conjugacy classes that may appear in the ramification type of f_{T_0}. Next assume e is odd, and pick a prime p dividing e. If $p = e$, then G is solvable by Burnside's theorem. Letting N be a minimal normal subgroup of G, it follows that N contains exactly one of C_1 and C_2. The product 1 relation then gives a contradiction in G/N. Thus, we may assume p is a proper divisor of e. In this case, if we pick y to be a power of x_1 of order p, then (13) implies that the only conjugacy classes appearing in the ramification type of f_{T_0} are C_1, C_1^2 or C_2, neither of which contains y, contradiction. □

Remark 4.2. In the following we shall use Magma for computations with small order groups. More specifically, we use the command ExtensionsOfElementaryAbelianGroup to run over extensions of a given group by an elementary abelian group.

Finally, we show that if E is $\{3,2,2,2\}$ or $\{4,2,2,2\}$, then either $G \subseteq \mathrm{PGL}_2(\mathbb{C})$ or there is no group G whose maximal conjugacy classes are the classes of a product 1 tuple $x_1, \ldots, x_4$ with orders in E. Since in both cases $\#G$ is divisible by at most two primes, G is solvable by Burnside's theorem. Let N be a minimal normal subgroup of G, so that $N \cong (\mathbb{Z}/2\mathbb{Z})^u$ or $(\mathbb{Z}/3\mathbb{Z})^u$, for $u \geq 1$.

Case {3,2,2,2}: If $N \cong (\mathbb{Z}/3\mathbb{Z})^u$, the images of x_2, x_3, x_4 in G/N remain of order 2 and hence $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$. Since moreover G/N acts transitively on the $\mathbb{Z}/3\mathbb{Z}$ subgroups of N, it follows that $u = 1$ or 2. A check using Magma (Remark 4.2) shows that all such group extensions G contain an element of order 6.

In the case $N \cong (\mathbb{Z}/2\mathbb{Z})^u$, N contains exactly one of the conjugacy classes C_2, C_3, C_4 since otherwise we get a contradiction to the product 1 relation in G/N. Since G/N is generated by three elements of orders $3, 2$ and 2 with product 1, it is isomorphic to S_3. As G/N acts transitively on the $\mathbb{Z}/2\mathbb{Z}$ copies in N, we have $u = 1$ or 2. Once again a Magma check shows that all such group extensions G contain an element of order 4 or 6, contradicting that C_i, $i = 1, \ldots, 4$ are the only maximal ones.

Case {4,2,2,2}: In this case G is a 2-group, and $N \cong (\mathbb{Z}/2\mathbb{Z})^u$. The conjugacy classes of involutions in G are C_1^2, C_2, C_3, and C_4. If N does not contain C_1^2, then the product one relation in G/N implies that N contains exactly one of the conjugacy classes C_2, C_3, C_4. In this case G/N is dihedral of order 8, acting transitively on the $\mathbb{Z}/2\mathbb{Z}$ copies in N.

Hence $u = 1$ or 2. A Magma check shows that such a G either contains an element of order 8, or has more than four conjugacy classes of involutions, or has more than two conjugacy classes of elements of order 4 (in which case there is more than one conjugacy class of cyclic subgroups of order 4).

If N contains C_1^2, then all elements of G/N are involutions, and hence G/N is an elementary abelian 2-group. Since we may assume N is a proper subgroup of G, the product 1 relation in G/N implies that N one or two of the conjugacy classes C_2, C_3, C_4. In the former case, G/N is a 2-group acting transitively on involutions in N, forcing $u = 1$. In this case, a Magma check shows that for such group extensions either the number of conjugacy classes of involutions is more than 4 or the number of conjugacy classes of order 4 elements is more than 2. If N contains two of C_2, C_3, C_4, then $G/N \cong \mathbb{Z}/2\mathbb{Z}$. Thus by minimality of N, we get that $u \leq 2$ and hence that G is isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{C})$.

5. Regular Parametricity and Genericity

For this section, let k be an arbitrary field of characteristic zero and (T, U, V) a triple of indeterminates. Given a non-trivial finite group G, let $F/k(T)$ be a k-regular Galois extension of group G and branch point set $\mathbf{t} = \{t_1, \dots, t_r\}$. We also denote the genus of F by g and the ramification indices of $t_1, \dots, t_r$ by $e_1, \dots, e_r$, respectively. The unordered r-tuple $(e_1, \dots, e_r)$ is finally denoted by $\mathbf{e}$. The main topic of the present section is the following question: *given a field extension L/k, is the extension $F/k(T)$ L-parametric?*

5.1. **Main results.** In Theorem 5.1 below, which generalizes and complements Theorem 1.4 from §1, we give three explicit field extensions L_1/k, L_2/k, and L_3/k, independent of either the extension $F/k(T)$ or the group G, such that the answer to the above question is in general negative if L is taken among the fields L_1, L_2, and L_3.

Theorem 5.1. (a) *Assume $g \geq 1$. Then, $F/k(T)$ is not L_1-parametric, where $L_1 = K(U)$ and $K \supset k$ is any overfield which is ample. More precisely, infinitely many K-regular Galois extensions of L_1 of group G are not specializations of $FL_1/L_1(T)$.*

(b) *Assume one of the following three conditions holds:*

(i) *$G = S_n$ ($n \geq 4$),*

(ii) *$G = A_n$ ($n \geq 4$),*

(iii) *$G = D_n$ ($n \geq 2$ even).*

Then, $F/k(T)$ is not L_2-parametric, where $L_2 = K((V))(U)$ and $K \supset k$ is any overfield which is algebraically closed. More precisely, infinitely many $K((V))$-regular Galois extensions of L_2 of group G are not specializations of $FL_2/L_2(T)$.

(c) *Assume either one of the following two conditions holds:*

(i) *G is cyclic of even order, $r = 2$, and $\mathbf{t} \not\subset \mathbb{P}^1(k)$,*

(ii) *G is odd dihedral, $r = 3$, and $\mathbf{t} \not\subset \mathbb{P}^1(k)$.*

Then, $F/k(T)$ is not L_3-parametric, where $L_3 = k(U)$. More precisely, infinitely many k-regular Galois extensions of L_3 of group G are not specializations of $FL_3/L_3(T)$.

Remark 5.2. Given a field K, the field $K((V))$ is ample. Hence, (b) is a special case of (a) under the extra assumption $g \geq 1$ (e.g., if $G = S_n$ with $n \geq 5$, see below). However, as we shall see in §5.2.2, we shall use a different approach, which works regardless of the value of g, to prove (b).

Since the case $g = 0$ can occur only in the following five cases:

- G is cyclic and $\mathbf{e} = (|G|, |G|)$,

- G is dihedral and $\mathbf{e} = (2, 2, |G|/2)$,
- $G = A_4$ and $\mathbf{e} = (2, 3, 3)$,
- $G = S_4$ and $\mathbf{e} = (2, 3, 4)$,
- $G = A_5$ and $\mathbf{e} = (2, 3, 5)$,

the following three cases are the only ones which are not covered by Theorem 5.1:
(1) G is cyclic of even order, $r = 2$, and $\mathbf{t} \subset \mathbb{P}^1(k)$,
(2) G is cyclic of odd order and $r = 2$,
(3) G is odd dihedral, $r = 3$, and $\mathbf{t} \subset \mathbb{P}^1(k)$.
We handle them in Proposition 5.3 below:

Proposition 5.3. *Assume one of the conditions* (1), (2), *and* (3) *holds. Then, $F/k(T)$ is generic. More precisely, for every field extension L/k and every Galois extension E/L of group contained in G, one has $E = (FL)_{t_0}$ for infinitely many points $t_0 \in \mathbb{P}^1(L)$.*

Theorem 5.1 and Proposition 5.3 are proved in §5.2 and §5.3, respectively.

A first consequence of Theorem 5.1 and Proposition 5.3 is the following: to prove that the extension $F/k(T)$ is generic, it suffices to check the L-parametricity property for each of the three explicit extensions L_1/k, L_2/k, and L_3/k given in Theorem 5.1. They actually provide a full description of all k-regular Galois extensions of $k(T)$ that are generic. Specifically, we have this corollary which generalizes Theorem 1.5 from §1:

Corollary 5.4. *The following three conditions are equivalent:*
(a) *the extension $F/k(T)$ is generic,*
(b) *the extension $F/k(T)$ is $\overline{k}((V))(U)$-parametric and $k(U)$-parametric,*
(c) *one of the following three conditions holds:*
  (i) *G is cyclic of even order n such that $e^{2i\pi/n} \in k$, $r = 2$, and $\mathbf{t} \subset \mathbb{P}^1(k)$,*
  (ii) *G is cyclic of odd order n such that $e^{2i\pi/n} + e^{-2i\pi/n} \in k$ and $r = 2$,*
  (iii) *G is dihedral of order $2n$ with $n \geq 3$ odd and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$, $r = 3$, and $\mathbf{t} \subset \mathbb{P}^1(k)$.*

In particular, G occurs as the group of a k-regular Galois extension of $k(T)$ that is generic iff one of the following three conditions holds:
- *G is cyclic of even order n and $e^{2i\pi/n} \in k$,*
- *G is cyclic of odd order n and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$,*
- *G is dihedral of order $2n$ with $n \geq 3$ odd and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$.*

Proof. The corollary is a combination of Theorem 5.1, Proposition 5.3, and the following two statements on regular realizations of cyclic and odd dihedral groups, which are consequences of the rigidity method and the Branch Cycle Lemma:
- given $n \geq 2$, there is a k-regular Galois extension of $k(T)$ of group $\mathbb{Z}/n\mathbb{Z}$ and with two branch points iff $e^{2i\pi/n} + e^{-2i\pi/n} \in k$; both branch points can be chosen to be in $\mathbb{P}^1(k)$ iff $e^{2i\pi/n} \in k$,
- given $n \geq 3$ odd, there is a k-regular Galois extension of $k(T)$ of group D_n, with three branch points, and all branch points in $\mathbb{P}^1(k)$ iff $e^{2i\pi/n} + e^{-2i\pi/n} \in k$. □

Remark 5.5. If k is algebraically closed, then, the assumptions of Theorem 5.1(c) cannot happen. In particular, condition (b) above can then be replaced by
(b)' *the extension $F/k(T)$ is $k((V))(U)$-parametric.*

5.2. **Proof of Theorem 5.1.** We break the proof into three parts, corresponding to the three statements (a), (b), and (c) of Theorem 5.1.

5.2.1. *Proof of* (a). Assume $g \geq 1$ and let $K \supset k$ be an overfield as in (a). As shown in the proof of Theorem 3.7(a-1), Condition 3.8 holds for every finite group and every ample

field of characteristic zero. Hence, by Theorem 3.9, there are infinitely many K-regular Galois extensions $E/K(U)$ of group G each of which satisfies $E \neq (FK(U))_{t_0}$ for each $t_0 \in K(U) \setminus K$. Pick such an extension $E/K(U)$ and suppose there is $t_0 \in \mathbb{P}^1(K(U))$ such that $E = (FK(U))_{t_0}$. One then has $t_0 \in \mathbb{P}^1(K)$ by the previous property. Lemma 2.1 then yields $E = (FK)_{t_0}K(U)$. As $E/K(U)$ is K-regular, one has $(FK)_{t_0} = K$ and then $E = K(U)$, which cannot happen. Hence, (a) holds.

5.2.2. *Proof of* (b). Let K be an algebraically closed field containing k, set $M = K((V))$, and, for each $u \in M$, denote by $\mathfrak{P}_u$ the prime ideal of $M[U]$ generated by $U - u$. Below, we show that there are infinitely many M-regular Galois extensions of $M(U)$ of group G which are not specializations of $FM(U)/M(U)(T)$, provided one of the following three conditions holds:
(i) $G = S_n$ $(n \geq 4)$,
(ii) $G = A_n$ $(n \geq 4)$,
(iii) $G = D_n$ $(n \geq 2$ even).

First, we need the following lemma, which is a function field analog of [KLN17, Proposition 6.3] (which is stated over number fields):

Lemma 5.6. *For all but finitely many $u \in M$, the Galois group of the completion at $\mathfrak{P}_u$ of every specialization of $FM(U)/M(U)(T)$ is cyclic.*

Proof. The proof is similar to that in the number field case and relies on [KLN17, Theorem 4.1], which is the main result of that paper. For the convenience of the reader, we offer a full proof below, with the necessary adjustments.

Let t_0 be in $\mathbb{P}^1(M(U))$ and u in M. If $(FM(U))_{t_0}/M(U)$ is unramified at $\mathfrak{P}_u$, then, the Galois group of its completion at $\mathfrak{P}_u$ clearly is cyclic. We may then assume the extension $(FM(U))_{t_0}/M(U)$ is ramified at $\mathfrak{P}_u$. In particular, t_0 is not a branch point of $F/k(T)$. Indeed, if it was, then, it would be in $\mathbb{P}^1(\overline{k})$. By Lemma 2.1, one would have

$$(FM(U))_{t_0} = (F\overline{k})_{t_0}M(U) = M(U),$$

which cannot happen as $(FM(U))_{t_0}/M(U)$ ramifies at $\mathfrak{P}_u$. Up to dropping finitely many values of u (depending only on $FM(U)/M(U)(T)$), one may use the Specialization Inertia Theorem of [Leg16, §2.2] to get that t_0 meets some branch point of $F/k(T)$, say t, modulo $\mathfrak{P}_u$[18]. As above, one has $(FM(U))_t = M(U)$. Denote the inertia group of $Fk(t)/k(t)(T)$ at the prime ideal $\langle T - t\rangle$ by I_t. Up to dropping finitely many values of u (depending only on $FM(U)/M(U)(T)$), [KLN17, Theorem 4.1] then shows that the Galois group of the completion at $\mathfrak{P}_u$ of $(FM(U))_{t_0}/M(U)$ embeds into I_t. As I_t is cyclic, we are done. □

Then, to prove (b), it suffices, by Lemma 5.6, to show that the following holds:
(∗) *for each $u \in M$, there is a M-regular Galois extension of $M(U)$ of group G and whose completion at $\mathfrak{P}_u$ has non-cyclic Galois group.*

First, assume condition (i) holds. Given $u \in M$, consider the Galois extension

$$E_1/M(U) = M(U)(\sqrt{U-u}, \sqrt{V})/M(U).$$

Pick distinct elements $\alpha_1, \ldots, \alpha_{n-4}$ of $M[U]$ and set

$$P_1(Y) = (Y^2 - (U-u))(Y^2 - V)(Y - \alpha_1)\cdots(Y - \alpha_{n-4}).$$

Then, denote the trivial extension $M(U)/M(U)$ by $E_2/M(U)$. Pick distinct elements $\beta_1, \ldots, \beta_n$ of $M[U]$ and set

$$P_2(Y) = (Y - \beta_1)\cdots(Y - \beta_n).$$

[18]We refer to [Leg16, Definition 2.2] for more details about the terminology.

Finally, let $E_3/M(U)$ be a Galois extension of group S_n. Pick $\gamma_0, \dots, \gamma_{n-1} \in M[U]$ such that

$$P_3(Y) = Y^n + \gamma_{n-1}Y^{n-1} + \cdots + \gamma_1 Y + \gamma_0$$

is separable and E_3 is the splitting field of $P_3(Y)$ over $M(U)$. By polynomial interpolation, there are polynomials $a_0(T), \dots, a_{n-1}(T) \in M[U][T]$ such that

$$Y^n + a_{n-1}(i)Y^{n-1} + \cdots + a_1(i)Y + a_0(i) = P_i(Y)$$

for each $i \in \{1, 2, 3\}$. Let $\mathcal{F}$ be the splitting field over $M(U)(T)$ of

$$Y^n + a_{n-1}(T)Y^{n-1} + \cdots + a_1(T)Y + a_0(T).$$

By the above and since $P_1(Y)$, $P_2(Y)$, and $P_3(Y)$ are separable, the points 1, 2, and 3 are not branch points of $\mathcal{F}/M(U)(T)$ and the corresponding specialized extensions are $E_1/M(U)$, $E_2/M(U)$, and $E_3/M(U)$, respectively. In particular, $\mathcal{F}/M(U)(T)$ is $M(U)$-regular (since $E_2/M(U)$ is trivial) and it has Galois group S_n (since this is true for $E_3/M(U)$). By the compatibility between the Hilbert specialization property and the weak approximation property of $\mathbb{P}^1$, there are infinitely many points t_0 in $M(U)$ such that $\mathcal{F}_{t_0}/M(U)$ has Galois group S_n and its completion at $\mathfrak{P}_u$ is the completion of $E_1/M(U)$ at $\mathfrak{P}_u$, that is, the extension

$$M((U-u))(\sqrt{U-u}, \sqrt{V})/M((U-u)),$$

which has Galois group $(\mathbb{Z}/2\mathbb{Z})^2$. Moreover, given $u' \in M \setminus \{u\}$, for infinitely many such points t_0, one may require that the completion of $\mathcal{F}_{t_0}/M(U)$ at $\mathfrak{P}_{u'}$ is the completion at $\mathfrak{P}_{u'}$ of $E_2/M(U)$, that is, the extension

$$M((U-u'))/M((U-u')).$$

Consequently, $\mathcal{F}_{t_0}/M(U)$ is M-regular for such a t_0. Hence, condition $(*)$ holds.

Now, assume condition (ii) holds. Given $u \in M$, set $u' = u - V^2$ and consider the Galois extension

$$E/M(U) = M(U)(\sqrt{(U-u')V}, \sqrt{(U-u)(U-u')})/M(U),$$

which is of group $(\mathbb{Z}/2\mathbb{Z})^2$. Clearly, the completion of $E/M(U)$ at $\mathfrak{P}_u$ has Galois group $(\mathbb{Z}/2\mathbb{Z})^2$ and that at $\mathfrak{P}_{u'}$ is totally ramified of degree 2. By a classical result of Mestre (see [Mes90] and [KM01, Theorem 3]), the extension $E/M(U)$ occurs as a specialization of some $M(U)$-regular Galois extension $\mathcal{F}/M(U)(T)$ of group A_n. As under condition (i), there are infinitely many points t_0 in $M(U)$ such that $\mathcal{F}_{t_0}/M(U)$ has Galois group A_n and its completion at $\mathfrak{P}_u$ (resp., at $\mathfrak{P}_{u'}$) is the completion of $E/M(U)$ at $\mathfrak{P}_u$ (resp., at $\mathfrak{P}_{u'}$), which is not cyclic (resp., which is totally ramified). In particular, by the last condition, $\mathcal{F}_{t_0}/M(U)$ is M-regular, thus proving condition $(*)$.

Finally, assume condition (iii) holds. Set

$$P(U, Y) = Y^{2n} - UY^n + V^n \in M[U, Y]$$

and let $y \in \overline{M(U)}$ be a root of $P(U, Y)$. Clearly, y^n is equal to $(U \pm \sqrt{U^2 - 4V^n})/2$, thus showing that the fields $M(U)(y^n)$ and $M(U)(\sqrt{U^2 - 4V^n})$ coincide. Moreover, y^n is of valuation w.r.t. ∞ equal to ± 1. Then, by the Capelli lemma (see, e.g., [Lan02, Chapter VI, §9, Theorem 9.1]), the polynomial $Y^n - y^n$ is irreducible over $\overline{M}(U)(\sqrt{U^2 - 4V^n})$. As a consequence, the polynomial $P(U, Y)$ is irreducible over $\overline{M}(U)$; denote the field $M(U)(y)$ by E. Clearly, $e^{2i\pi/n}y$ is a root of $P(U, Y)$ and it is easily checked that the same holds for V/y. Consequently, the distinct elements $e^{2i\pi m/n}y$, $m \in \{0, \dots, n-1\}$, and $V/(e^{2i\pi m/n}y)$, $m \in \{0, \dots, n-1\}$, of $\overline{M(U)}$ are the distinct roots of $P(U, Y)$, which are in E. Hence, the M-regular extension $E/M(U)$ is Galois. Moreover, there are σ and

τ in $\mathrm{Gal}(E/M(U))$ such that $\sigma(y) = e^{2i\pi/n}y$ and $\tau(y) = V/y$. Since $\langle \sigma, \tau \rangle = D_n$, the group $\mathrm{Gal}(E/M(U))$ is then equal to D_n. Now, set $u = 2V^{n/2} \in M$ (as n is even). Then, the completion of $E/M(U)$ at $\mathfrak{P}_u$ contains

$$M((U-u))(\sqrt{U^2 - 4V^n}) = M((U-u))(\sqrt{(U-u)(U+u)})$$

(which is the completion at $\mathfrak{P}_u$ of the quadratic subfield of $E/M(U)$) and

$$M((U-u))(\sqrt{V})$$

(as $\sqrt{V}$ is a root of the specialized polynomial $P(u, Y)$). As the former (resp., the latter) is (totally) ramified (resp., unramified) of degree 2 over $M((U-u))$, the group $(\mathbb{Z}/2\mathbb{Z})^2$ is a quotient of the Galois group of the completion of $E/M(U)$ at $\mathfrak{P}_u$, which cannot be cyclic. Hence, up to applying suitable changes of variable, condition $(*)$ holds.

Remark 5.7. (a) Under condition (i) or condition (iii), shorter proofs of condition $(*)$ could have been given, by using that the involved groups have a *generic polynomial* over K, and a classical result of Saltman (see [Sal82, Theorem 5.9]) asserting that, under the existence of such a polynomial, *Grunwald problems* (that is, approximation of finitely many local extensions by a global one of given group) can be solved. However, as we intend to apply our approach to generic polynomials (see Appendix B), we have deliberately avoided such tools above.

(b) A property shared by all groups in Theorem 5.1(b) that we have used in our local approach is that they have a non-cyclic abelian subgroup. Under the sole condition that G has a non-cyclic abelian subgroup, the same tools show that there are infinitely many M-regular Galois extensions of $M(U)$ of group *contained in* G which are not specializations of $FM(U)/M(U)(T)$ [19].

Indeed, G then contains $(\mathbb{Z}/p\mathbb{Z})^2$ for some prime number p. By Lemma 5.6, it suffices to show that, for each $u \in M$, there is a M-regular Galois extension of $M(U)$ of group $(\mathbb{Z}/p\mathbb{Z})^2$ and whose completion at $\mathfrak{P}_u$ has Galois group $(\mathbb{Z}/p\mathbb{Z})^2$. Fix $u \in M$ and set

$$E_u = M(U)(\sqrt[p]{U-u}, \sqrt[p]{V+U-u}).$$

Then, the group of the Galois extension $E_u/M(U)$ is $(\mathbb{Z}/p\mathbb{Z})^2$ since the subextension $M(U)(\sqrt[p]{U-u})/M(U)$ (resp., $M(U)(\sqrt[p]{V+U-u})/M(U)$) is totally ramified at $\mathfrak{P}_u$ (resp., unramified at $\mathfrak{P}_u$) of degree p. The same argument shows that the completion of $E_u/M(U)$ at $\mathfrak{P}_u$ is also of Galois group $(\mathbb{Z}/p\mathbb{Z})^2$. Finally, we claim that $E_u/M(U)$ is M-regular. Indeed, if it was not, then, one would have

$$E_u = M(U)(\sqrt[p]{V}, \sqrt[p]{U-u}).$$

But this last equality cannot happen as the branch point sets of the extensions $E_u/M(U)$ and $M(U)(\sqrt[p]{V}, \sqrt[p]{U-u})/M(U)$ are $\{u, u-V, \infty\}$ and $\{u, \infty\}$, respectively.

5.2.3. *Proof of* (c). First, assume $G = \mathbb{Z}/n\mathbb{Z}$ for some even $n \geq 2$ and $r = 2$. As n is even, there is a $k(U)$-regular Galois extension of $k(U)(T)$ of group G, with a branch point in $\mathbb{P}^1(k(U))$, and with another branch point of ramification index n. Then, by [Leg16, Corollary 3.4], there is a prime $\mathfrak{P}$ of $k[U]$ such that, for all but finitely many u in k, there is a Galois extension $E_u/k(U)$ of group G, which ramifies at $\mathfrak{P}_u = \langle U-u \rangle$, and whose ramification index at $\mathfrak{P}$ is n. In particular, $E_u/k(U)$ is k-regular (by the last condition). Suppose $E_u/k(U)$ is a specialization of $Fk(U)/k(U)(T)$ for infinitely many $u \in k$. Without loss, we may assume $\infty \notin \mathbf{t}$. For $i \in \{1, 2\}$, denote the minimal

[19] In particular, the extension $F/k(T)$ is not *strongly* $M(U)$*-parametric* in the sense of the upcoming Definition 5.9.

polynomial of t_i over k by $m_i(T)$. Then, by [Leg16, Corollary 2.12 and Remark 3.11], the reduction modulo $\mathfrak{P}_u$ of $m_1(T)m_2(T)$ (viewed as a polynomial in $k[U][T]$) has a root in the residue field $k[U]/\mathfrak{P}_u$ for some $u \in k$. As this residue field is k, the polynomial $m_1(T)m_2(T)$ has a root in k. Hence, by the Branch Cycle Lemma, t_1 and t_2 are in $\mathbb{P}^1(k)$.

Now, assume $G = D_n$ for some odd $n \geq 3$ and $r = 3$. As n is odd, the ramification indices e_1, e_2, and e_3 are 2, 2, and n, respectively (up to reordering). In particular, by the Branch Cycle Lemma (and as $n \neq 2$), t_3 is in $\mathbb{P}^1(k)$. By [FJ08, §16.2 and Proposition 16.4.4], every k-regular quadratic extension of $k(U)$ embeds into a k-regular Galois extension of $k(U)$ of group G. Hence, if all but finitely many k-regular Galois extensions of $k(U)$ of group G are specializations of $Fk(U)/k(U)(T)$, then, as G has a unique subgroup of index 2, all but finitely many k-regular quadratic extensions of $k(U)$ have to occur as specializations of the quadratic subextension of $Fk(U)/k(U)(T)$. As this quadratic subextension has only two branch points (namely, t_1 and t_2), one may use a similar argument as in the cyclic case to get that these branch points have to be in $\mathbb{P}^1(k)$.

5.3. **Proof of Proposition 5.3.** Assume one of the following three conditions holds:
(1) G is cyclic of even order, $r = 2$, and $\mathbf{t} \subset \mathbb{P}^1(k)$,
(2) G is cyclic of odd order and $r = 2$,
(3) G is odd dihedral, $r = 3$, and $\mathbf{t} \subset \mathbb{P}^1(k)$.
Let L/k be a field extension and E/L a Galois extension of group contained in G. Below, we show that the extension E/L occurs as the specialized extension of the extension $FL/L(T)$ at t_0 for infinitely many points $t_0 \in \mathbb{P}^1(L)$.

By the twisting lemma [Dèb99], there is a k-regular extension $(FL)_E/L(T)$ such that $(FL)_E\overline{L} = F\overline{L}$ and, given $t_0 \in \mathbb{P}^1(L) \setminus \mathbf{t}$, if there is a prime ideal lying over $\langle T - t_0\rangle$ in $(FL)_E/L(T)$ with residue degree 1, then, E/L is the specialized extension of $FL/L(T)$ at t_0. In each case, the genus of F is 0 (if (3) holds, this follows from $\mathbf{e}$ being $(2, 2, |G|/2)$). Hence, $(FL)_E$ has genus 0 as well. It then suffices to find $t \in \mathbb{P}^1(L)$ for which there is a prime ideal lying over $\langle T - t\rangle$ in $(FL)_E/L(T)$ with residue degree 1.

If (1) holds, then, the unique prime ideal lying over $\langle T-t_1\rangle$ in $(FL)_E/L(T)$ has residue degree 1. If (2) holds, the desired conclusion follows from G being of odd order and the genus being equal to 0; see, e.g., [Ser92, §1.1] for more details. Finally, assume (3) holds. As already seen, the ramification indices e_1, e_2, and e_3 are 2, 2, and n, where $|G| = 2n$, respectively (up to reordering). As $\{t_1, t_2\} \subset \mathbb{P}^1(k)$, we may assume the quadratic subfield of F is $k(\sqrt{T})$ (up to applying a suitable change of variable). Hence, there is $d \in L \setminus \{0\}$ such that $(FL)_E$ contains the quadratic field $L(\sqrt{dT})$. Set $Y = \sqrt{dT}$. The extension $(FL)_E/L(Y)$ is of degree n and it has only two branch points; it is then Galois of group $\mathbb{Z}/n\mathbb{Z}$ and of genus 0. As n is odd, there exists $y_0 \in L$ such that the specialized extension of $(FL)_E/L(Y)$ at y_0 is L/L. Consequently, there is a prime ideal lying over $\langle T-(y_0)^2/d\rangle$ in $(FL)_E/L(T)$ with residue degree 1, thus concluding the proof of Proposition 5.3.

5.4. **On Schinzel's problem and its variants.** In this subsection, we explain how to obtain a conjectural counter-example to the problem of Schinzel recalled as Question 1.6, Question 1.7, and the Working Hypothesis of [Dèb18].

To do this, consider the polynomial $P(T) = T^3 + (5/4)T^2 - 2T - 7 \in \mathbb{Q}[T]$ and the number field $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{11})$. Let $f_1 : X_1 \to \mathbb{P}^1_{\mathbb{Q}}$ and $f_2 : X_2 \to \mathbb{P}^1_{\mathbb{Q}}$ be the $\mathbb{Q}$-Galois covers given by the affine equations $Y^2 - P(T)$ and $Y^2 - T$, respectively.

First, consider the elliptic curve $C : Y^2 = P(T)$. Subject to the Birch and Swinnerton-Dyer conjecture, for every non-square $u_0 \in K$, the twisted elliptic curve $C_{u_0} : Y^2 = u_0P(T)$ has positive rank, and then infinitely many K-rational points; see [DD09] for

more details. Moreover, as C has rank 2 over $\mathbb{Q}(\sqrt{-3})$ (checked with Magma), C has infinitely many K-rational points. Hence, the following equivalent two conditions hold:

(i) *the containment* $\mathbf{SP}(f_2 \otimes_{\mathbb{Q}} K) \subseteq \mathbf{SP}(f_1 \otimes_{\mathbb{Q}} K)$ *holds*,

(ii) *for each* $u_0 \in K^*$, *the polynomial* $Y^2 - u_0 P(T)$ *has a zero* (y,t) *in* K^2 *such that* $y \neq 0$.

Now, the cover f_1 has four branch points while f_2 has only two. In particular, by Theorem 2.4, the following condition holds:

(iii) *given a field* L *of characteristic zero,* $f_2 \otimes_{\mathbb{Q}} L$ *is not a rational pullback of* $f_1 \otimes_{\mathbb{Q}} L$.

By using Lemma 2.1, one sees that (iii) is equivalent to

(iv) *given a field* L *of characteristic zero,* $L(\sqrt{U})/L(U)$ *does not occur as a specialization of* $L(U)(T)(\sqrt{P(T)})/L(U)(T)$.

Finally, this shows that the following condition holds:

(v) *the polynomial* $Y^2 - UP(T)$ *has no zero in* $K(U)^2$.

Indeed, suppose $Y^2 - UP(T)$ has a zero $(Y(U), T(U))$ in $K(U)^2$. As $P(T)$ is irreducible over K (checked with Magma), $T(U)$ is not a root of $P(T)$. Hence, $K(\sqrt{U})/K(U)$ is the specialization of $K(U)(T)(\sqrt{P(T)})/K(U)(T)$ at $T(U)$, which cannot happen by (iv).

By using (i)-(v), one then obtains the following theorem:

Theorem 5.8. *Subject to the Birch and Swinnerton-Dyer conjecture,*

(a) *the answer to Question 1.6 is negative for the number field* K *and the polynomial* $Y^2 - UP(T)$,

(b) *the answer to Question 1.7 is negative for the number field* K *and the covers* $f_1 \otimes_{\mathbb{Q}} K$ *and* $f_2 \otimes_{\mathbb{Q}} K$,

(c) *the following Working Hypothesis fails for the number field* K *and the sole* $K(U)$*-Galois cover* $X \to \mathbb{P}^1_{K(U)}$ *given by the affine equation* $Y^2 - UP(T)$*:*

(WH) *Let* L *be a number field and* $f_i : X_i \to \mathbb{P}^1_{L(U)}$, $i = 1, \dots, N$, *be* $L(U)$*-covers. Assume none of the* $L(U)$*-curves* $X_1, \dots, X_N$ *has an unramified*[20] $\mathbb{C}(U)$*-rational point. Then, for infinitely many* $u_0 \in L$, *the covers* $f_1, \dots, f_N$ *have good reduction at* $U = u_0$ *and none of the reduced curves* $X_1|_{u_0}, \dots, X_N|_{u_0}$ *has an unramified* L*-rational point.*

5.5. **L-parametricity versus $L(U)$-parametricity.** Let us now introduce the following strong variant of Definition 2.2(e):

Definition 5.9. Given an overfield $L \supset k$, say that $F/k(T)$ is *strongly L-parametric* if every Galois extension E/L of group contained in G is a specialization of $FL/L(T)$.

Remark 5.10. Similarly, one could say that the extension $F/k(T)$ is *strongly generic* if $F/k(T)$ is strongly L-parametric for every field extension L/k. Clearly, one would have

$$F/k(T) \text{ strongly generic} \Rightarrow F/k(T) \text{ generic.}$$

However, Theorem 5.1 and Proposition 5.3 show that the converse holds.

To conclude this paper, we discuss connections between the $L(U)$-parametricity (resp., the strongly $L(U)$-parametricity) and the L-parametricity (resp., the strongly L-parametricity) properties for overfields $L \supset k$.

Recall that, by [Dèb18, Remark 2.3], any k-regular Galois extension of $k(T)$ is strongly k-parametric if it is strongly $k(U)$-parametric[21]. However, there is no general converse:

[20] by "unramified on X_i" we mean w.r.t. the cover $f_i : X_i \to \mathbb{P}^1_{L(U)}$; similarly below "unramified on $X_i|_{u_0}$" means w.r.t. the cover $f_i|_{u_0} : X_i|_{u_0} \to \mathbb{P}^1_L$, $i = 1, \dots, N$.

[21] The argument given there shows that this implication also holds if "strongly" is removed twice.

• if k is PAC[22], then, by [Dèb99], every k-regular Galois extension of $k(T)$ is strongly k-parametric but, as noted in [Leg15, Remark 7.2], some of them are not $k(U)$-parametric,

• if $k = \mathbb{C}$, then, by [Dèb18, Corollary 2.5] and Theorem 1.1(a) (see also Remark 2.3), the following three conditions are equivalent:

(a) G is the group of a Galois extension of $k(T)$ that is strongly $k(U)$-parametric,

(b) G is the group of a Galois extension of $k(T)$ that is $k(U)$-parametric,

(c) $G \subset \mathrm{PGL}_2(\mathbb{C})$.

Below, we provide two new situations for which there is no general converse. The first one relies on Theorem 5.8:

Subject to the Birch and Swinnerton-Dyer conjecture, the $\mathbb{Q}$-regular quadratic extension $\mathbb{Q}(T)(\sqrt{P(T)})/\mathbb{Q}(T)$ is strongly K-parametric but not $K(U)$-parametric, where $P(T) = T^3 + (5/4)T^2 - 2T - 7$ and $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{11})$.

Our second example is devoted to Laurent series fields:

Proposition 5.11. *Assume k is algebraically closed. Then, there is a Galois extension of $k(T)$ of group G that is strongly L-parametric, where $L = K((V))$ and $K \supset k$ is any overfield which is algebraically closed.*

In contrast, by Theorem 5.1(a) and Theorem 5.1(b), no Galois extension of $k(T)$ of group G is $L(U)$-parametric, provided G is neither cyclic nor odd dihedral[23].

Proposition 5.11 is a straightforward combination of the RET and the following lemma, which does not use the assumption that k is algebraically closed:

Lemma 5.12. *Let $K \supset k$ be an algebraically closed overfield and set $L = K((V))$. Then, a given k-regular Galois extension of $k(T)$ of group G and inertia canonical invariant $(C_1, \dots, C_r)$ is strongly L-parametric iff the following condition is satisfied:*
$(**)$ for each element order n in G, there is $i \in \{1, \dots, r\}$ such that elements of C_i have order divisible by n.

Proof. Galois extensions of L of group contained in G are exactly extensions $L(\sqrt[n]{V})/L$, where n runs over the set of all element orders in G. Since such an extension $L(\sqrt[n]{V})/L$ is (totally) ramified of index n at the unique maximal ideal $\mathfrak{P}$ of $K[[V]]$, a given k-regular Galois extension $\mathcal{F}/k(T)$ of group G is strongly L-parametric iff, for each element order n in G, the extension $\mathcal{F}L/L(T)$ has a specialization of ramification index n at $\mathfrak{P}$.

First, assume condition $(**)$ holds. Let n be an element order in G. Pick $i \in \{1, \dots, r\}$ such that the order e of every element of C_i is a multiple of n, and set $e = nm$. By [Leg16, Theorem 3.1], there are infinitely many points $t_0 \in L$ such that the inertia group at $\mathfrak{P}$ of $(\mathcal{F}L)_{t_0}/L$ is generated by an element of C_i^m. In particular, the ramification index at $\mathfrak{P}$ of such a specialization is n. Hence, $\mathcal{F}/k(T)$ is strongly L-parametric. Conversely, assume $\mathcal{F}/k(T)$ is strongly L-parametric. Let n be an element order in G. By the above characterization, $\mathcal{F}L/L(T)$ has a specialization of ramification index n at $\mathfrak{P}$. Then, by the Specialization Inertia Theorem, the inertia canonical invariant of $\mathcal{F}/k(T)$ contains the conjugacy class of an element of G of order divisible by n. Hence, condition $(**)$ holds. □

[22]Recall that a field κ is *Pseudo Algebraically Closed* (PAC) if every non-empty geometrically irreducible κ-variety has a Zariski-dense set of κ-rational points. See, e.g., [FJ08] for more on PAC fields.

[23]The assumption that k is algebraically closed is not needed here.

Appendix A. Proof of Theorem 1.2 for $r = 3$

Let k be a fixed algebraically closed field of characteristic 0. We start with the case where the multiset of ramification indices $E := \{e_1, e_2, e_3\}$ of our cover is different from

$$\{2,4,5\}, \{2,4,6\}, \{2,3,7\}, \{2,3,8\}, \{3,3,4\}, \{3,3,5\}. \tag{14}$$

In this case we shall use the following estimate:

Lemma A.1. *Let $f : X \to \mathbb{P}^1$ be a cover corresponding to a product 1 tuple $x_1x_2x_3 = 1$ with x_i of order e_i, $i = 1,2,3$. If f_{T_0} is a pullback of f along $T_0 \in k(U) \setminus k$ with corresponding tuple $x_1x_1^{-1}x_2x_2^{-1} = 1$ and degree $n := \deg T_0$, then*

$$\frac{1}{2e_3} \geq \left(\frac{1}{2} - \frac{1}{n}\right)\left(1 - \frac{1}{e_1} - \frac{1}{e_2}\right).$$

Proof. Denote by $e_{i,j}$, $j = 1, \dots, b_i$, the ramification indices of T_0 over t_i which are not multiples of e_i, and by $e(q|t_i)$ the ramification index of $q \in T_0^{-1}(t_i)$ under T_0, for $i = 1,2,3$. The Riemann–Hurwitz formula for T_0 then gives

$$\begin{aligned} 2n - 2 \geq \sum_{i=1}^{3} \sum_{q \in T_0^{-1}(t_i)} (e(q|t_i) - 1) &\geq \sum_{i=1}^{3} \left(\frac{n - \sum_{j=1}^{b_i} e_{i,j}}{e_i}(e_i - 1) + \sum_{j=1}^{b_i}(e_{i,j} - 1) \right) \\ &= \sum_{i=1}^{3} \left(n\frac{e_i - 1}{e_i} - b_i + \frac{1}{e_i}\sum_{j=1}^{b_i} e_{i,j} \right). \end{aligned}$$

Since f_{T_0} has four branch points, by Abhyankar's lemma $b_1 + b_2 + b_3 = 4$. Thus the previous estimate gives:

$$2 \geq n\left(1 - \sum_{i=1}^{3} \frac{1}{e_i}\right) + \sum_{i=1}^{3}\sum_{j=1}^{b_i} \frac{e_{i,j}}{e_i}. \tag{15}$$

Moreover, since f_{T_0} has four branch points with ramification indices e_1, e_1, e_2, e_2, Abhyankar's lemma implies that $e_i / \gcd(e_{i,j}, e_i) = e_1$ or e_2, where each of the values is obtained for exactly two of the $e_{i,j}$'s. In particular, $e_{i,j}/e_i$ is at least $1/e_1$ for two of the $e_{i,j}$'s and at least $1/e_2$ for the other two. Thus (15) gives

$$2 \geq n\left(1 - \sum_{i=1}^{r} \frac{1}{e_i}\right) + \frac{2}{e_1} + \frac{2}{e_2},$$

which is equivalent to the desired assertion. □

Remark A.2. We shall also repeatedly use Burnside's theorem: If G is a group of order $p^a q^b$ for some primes p, q and integers a, b, then G is solvable. If moreover, $p = q$ and G has only two maximal conjugacy classes of cyclic groups, and hence $G/[G,G]$ has at most 2 maximal conjugacy classes, then $G/[G,G]$ is cyclic. By Burnside's basis theorem this implies that G is cyclic.

Proof of Theorem 1.2 when $r = 3$ and E is not in (14). Suppose $f : X \to \mathbb{P}^1$ is a G-cover and $x_1x_2x_3 = 1$ is a product 1 tuple corresponding to f. As oppose to the case $r \geq 4$, we assume the orders e_1, e_2, e_3 of x_1, x_2, x_3 are ordered increasingly. Since the genus of X is non-zero as $G \not\leq \mathrm{PGL}_2(\mathbb{C})$, and since the case where X is of genus 1 follows from Remark 3.3, we shall assume that the genus of X is at least 2. This implies by the

Riemann–Hurwitz formula for f that

$$\sum_{i=1}^{3} 1/e_i < 1. \tag{RH$_f$}$$

Let C_i be the conjugacy class of x_i, for $i = 1, 2, 3$. If every ramification type with four branch points occurs as the ramification type of a pullback of f, then every conjugacy class in G is a power of one of C_1, C_2, C_3. Hence, we divide the proof into cases according to maximality of conjugacy classes.

Case 1: Assume next that G has at least three maximal conjugacy classes of cyclic subgroups. We show that no pullback f_{T_0} has a product 1 tuple (R_1) $x_1, x_1^{-1}, x_2, x_2^{-1}$. Denote by n the degree of $T_0 \in k(U) \setminus k$. Since each conjugacy class is a power of a conjugacy class in $\mathbf{C}$, there are exactly three maximal conjugacy classes of cyclic groups. In particular, the cyclic subgroup generated by C_1 (resp. by C_2) is not a power of C_3. Hence, $b_3 = 0$, that is, all ramification indices of T_0 over t_3 are divisible by e_3. In particular, e_3 divides n. The only tuples (e_1, e_2, e_3) satisfying the latter, (RH$_f$), and the assertion of Lemma A.1, are[24] either in (14) or $(3, 4, 4)$ with $n = 4$, or $(4, 4, 4)$ with $n = 4$, or $(2, 5, 5)$ with $n = 5$. A direct inspection shows that in the latter three cases, no pullback along a function T_0 of that degree gives the tuple (R_1).

Since a finite group G is never the union of conjugates of a proper subgroup $H \leq G$, the group G has a unique maximal conjugacy class of cyclic groups if and only if G is cyclic. We can therefore assume from now that G has two maximal conjugacy classes of cyclic groups and one of the classes in $\mathbf{C}$ is not maximal. As $e_3 \geq e_i$ for $i = 1, 2$, the (unique) non-maximal conjugacy class of cyclic groups among C_1, C_2, C_3 is either C_1 or C_2.

Case 2: Assume C_2 is the only non-maximal conjugacy class. In this case, since C_2 has to be a power of C_3, we have $e_2 \mid e_3$. Moreover as all ramification indices of T_0 over t_3 are multiples of e_3/e_2, we have $(e_3/e_2) \mid n$. The only tuples (e_1, e_2, e_3) and values of n which satisfy $e_2 \mid e_3$, $(e_3/e_2) \mid n$, (RH$_f$), and the assertion of Lemma A.1 are either in (14) or of the form $(e_1, e_2, 2e_2)$ when $n = 2$, or of the form (e_1, e_2, e_2) with $n \leq 6$, or one of $(2, 3, 9)$ with $n = 3, 6$, $(2, 3, 12)$ and $(2, 4, 8)$ with $n = 4$, $(2, 4, 12)$ with $n = 3$, or $(3, 3, 9)$ with $n = 3$.

The cases of the form (e_1, e_2, e_2) contradict the assumption that C_2 is non-maximal, and hence do not appear in this case.

The cases $(e_1, e_2, 2e_2)$ where $e_2 > 3$ satisfy the above constraints only with $n = 2$, and the map T_0 is ramified only over t_2 and t_3. In particular, one obtains the desired ramification type only if e_2 is odd. In these cases, consider the product 1 tuple (R_2) $x_1, x_1^{-1}, x_3, x_3^{-1}$. For such a cover to be a pullback f_{T_0} for some T_0, we must have all ramification indices over t_2 divisible by e_2, and hence in particular for such T_0, the degree $n = \deg T_0$ is divisible by e_2. Applying Lemma A.1 to a function T_0 such that f_{T_0} corresponds to a tuple $x_1 x_1^{-1} x_3 x_3^{-1} = 1$, we get:

$$\frac{1}{2e_2} \geq \left(\frac{1}{2} - \frac{1}{n}\right)\left(1 - \frac{1}{e_1} - \frac{1}{2e_2}\right). \tag{16}$$

[24]We carry out such numeric calculations using Magma as follows. First note that the inequality in Lemma A.1 for $e_3 \geq e_2 \geq e_1 \geq 4$ and $e_3 \mid n$, implies $e_1 = e_2 = e_3 = n = 4$. The inequality for $e_1 = 3$, $e_3 \geq e_2 \geq 4$, and $e_3 \mid n$ implies $e_2 = e_3 = n = 4$. The inequality for $e_3 \geq 5$, $e_2 = e_1 = 3$, and $e_3 \mid n$ implies $e_3 = n = 5$. For $e_1 = 2$, $e_2 \geq 4$, $e_3 \geq 6$ and $e_3 \mid n$, it implies $e_2 = 4$, $e_3 = n = 6$. For $e_1 = 2$, $e_2 = 3$, $e_3 \geq 8$ and $e_3 \mid n$, it implies $e_3 = n = 8$. If $e_1 = e_2 = 2$, then G is generated by two involutions and hence dihedral. The remaining list of possibilities is finite, and is computed using Magma. In similar sequel inequalities, similar computations are carried out.

The only tuple $(e_1, e_2, 2e_2)$ satisfying (16), with $e_2 \mid n$, and e_2 odd, and (RH_f) is $(3,3,6)$, treated at the end of this case.

A direct inspection shows that for $(2,4,12)$ there is no T_0 of degree 3 for which f_{T_0} has four branch points with ramification indices $2,2,4,4$. In the cases $(2,4,8)$ and $(3,3,9)$, the group is a non-cyclic p-group, and hence by Remark A.2 has at least 3 maximal conjugacy classes of cyclic groups.

In the cases $(2,3,9)$, and $(2,3,12)$, we claim there is no product 1 tuple with only two maximal conjugacy classes C_1 and C_3. Indeed, G is solvable by Remark A.2. Let N be a minimal normal subgroup of G. Since G is solvable N is isomorphic either to $(\mathbb{Z}/2\mathbb{Z})^t$ or to $(\mathbb{Z}/3\mathbb{Z})^t$ for some $t \geq 1$. In the case $(2,3,9)$ (resp. $(2,3,12)$): if $N \cong (\mathbb{Z}/2\mathbb{Z})^t$ then the images of x_2 and x_3^{-1} in G/N are equal contradicting that their orders remain 3 and 9 (resp. 3 and (6 or 12)). If $N \cong (\mathbb{Z}/3\mathbb{Z})^t$ then N must contain C_2: Indeed, as C_2 is non-maximal it coincides with a power of C_3^3 (resp. C_3^4), and hence generates the unique conjugacy class of cyclic subgroups of order 3. Hence the images of x_1 and x_3^{-1} coincide in G/N, contradicting that their orders are 2 and 3 (resp. 2 and 4).

In the case $(3,3,6)$, we may split x_3 as a product $x_3^4 \cdot x_3^3$. Since C_3^2 is a coprime to 3 power of C_2, we obtain a product 1 tuple in the Nielsen class C_1, C_2, C_2^u, C_3^3, where u is coprime to 3. It is straightforward to show that a cover with this ramification type is a pullback f_{T_0} for some T_0 only if $T_0^{-1}(t_1)$ and $T_0^{-1}(t_2)$ each have a single preimage with ramification index coprime to 3, and $T_0^{-1}(t_3)$ has a single preimage with ramification index divisible by 3 but not by 6, and a single one which is even but not divisible by 6. The Riemann–Hurwitz formula shows that this is possible only when $n = \deg T_0 \leq 3$, and hence there is no such possible ramification type for T_0.

Case 3: Finally, assume that C_1 is the only non-maximal conjugacy class. We separate here again into two cases. If C_1 is not a power of C_3, then as in Case 1, one has $e_3 \mid n = \deg T_0$, and the same analysis as in Case 1 applies. Henceforth we assume that C_1 is a power of C_3 and that e_3 does not divide n. Here, we separate into two cases:

Case 3a: Assume C_1 is a power of C_2. In this case e_1 properly divides e_2 and e_3. Moreover, if f_{T_0} corresponds to the tuple (R_1) $x_1, x_1^{-1}, x_2, x_2^{-1}$, then e_3/e_1 divides n. The only tuples satisfying these constraints, the assertion of Lemma A.1, and (RH_f), are $(e_1,e_2,e_3) = (2,4,6)$ which appears in (14), $(e, 2e, 2e)$ with $n = 2$ and $e \geq 3$, $(2,6,6)$ with $n = 3$, and $(2,4,8)$. In the latter case, by Remark A.2 there are more than two maximal conjugacy classes of cyclic groups. A direct inspection shows that in the cases $(e, 2e, 2e)$ (resp. $(2,6,6)$), there is no T_0 of degree 2 (resp. 3) for which f_{T_0} is of ramification $C_1, C_1^{-1}, C_2, C_2^{-1}$.

Case 3b: Assume C_1 is not a power of C_2. In this case, we consider the product 1 tuple (R_2) corresponding to the ramification $C_1, C_1^{-1}, C_3, C_3^{-1}$ and hence we can assume $e_2 \mid n = \deg T_0$. The only tuples satisfying this constraint, (16) and (RH_f) are $(3,4,6)$, $(3,3,3\ell)$ for $\ell \geq 2$, $(2,5,6)$, $(2,4,2\ell)$ for $\ell \geq 3$, and $(2,3,2\ell)$ for $\ell \geq 4$. In the case $(3,3,3\ell)$ Lemma A.1 shows that f_{T_0} can have ramification $C_1, C_1^{-1}, C_2, C_2^{-1}$ (corresponding to the tuple (R_1)) only if $\ell = 2$ or 3. The case $(3,3,9)$ was already ruled out. The case $(3,3,6)$ is ruled out as in the end of Case 2 (by simply switching the roles of C_1 and C_2). In the cases $(2,4,2\ell)$, Lemma A.1 shows that there is a pullback f_{T_0} with ramification $C_1, C_1^{-1}, C_2, C_2^{-1}$ only if $\ell \leq 4$. Case $(2,4,6)$ appears in (14) and $(2,4,8)$ has more than 2 maximal conjugacy classes by Remark A.2.

In the cases $(2,3,2\ell)$, Lemma A.1 and a direct inspection show that f_{T_0} can have ramification $C_1, C_1^{-1}, C_2, C_2^{-1}$ only if $\ell \leq 4$. Case $(2,3,8)$ appears in (14). Finally, Lemma A.1 shows that in the case $(3,4,6)$ (resp. $(2,5,6)$), there is a pullback f_{T_0} with ramification

$C_1, C_1^{-1}, C_2, C_2^{-1}$ only when $\deg T_0 \leq 3$ (resp. $\deg T_0 \leq 4$), however there is no such T_0 in these degrees. □

The remaining cases. Finally, we show that if E is in (14), then either the group G has more than three maximal conjugacy classes of cyclic groups or it does not contain a product 1 tuple $x_i \in C_i$, $i = 1, 2, 3$ that generates G. From now on let N be a minimal normal subgroup of G. As before assume $e_1 \leq e_2 \leq e_3$.

Lemma A.3. *Suppose that every maximal conjugacy class of G is a power of one of C_1, C_2, C_3 and $x_i \in C_i$, $i = 1, 2, 3$ are elements with product 1.*

(1) *If $N \lhd G$ is a proper subgroup, then it contains at most one of the conjugacy classes C_1, C_2, C_3.*
(2) *If N contains C_i for some $i \in \{1, 2, 3\}$, then, for the distinct j, ℓ in $\{1, 2, 3\} \setminus \{i\}$, there exist integers d_j, d_ℓ such that $e_j/d_j = e_\ell/d_\ell$, and d_j divides e_i and e_j, and d_ℓ divides e_i and e_ℓ.*

Proof. Note that since N is proper it cannot contain all maximal conjugacy classes of G, and note that if N contains an element from C_i and C_j for distinct $i, j \in \{1, 2, 3\}$, then it contains x_i and x_j and hence by the product 1 relation all x_i's. Thus N may contain at most one of the conjugacy classes C_1, C_2, C_3. Moreover if it contains C_i, then modulo N, the product one relation gives $x_j N = x_\ell^{-1} N$ and hence these are elements of the same order $e_j/d_j = e_\ell/d_\ell$ for some integer d_j (resp. d_ℓ) dividing e_j (resp. e_ℓ) and e_i, for the distinct j, ℓ in $\{1, 2, 3\} \setminus \{i\}$. □

Case (2,3,7): Since every conjugacy class is minimal, N contains at least one of C_1, C_2, C_3. If $N = 1$ then G is simple, contradicting the fact that there is no simple group with these element orders [Dea89]. Lemma A.3(1) shows that N contains exactly one of the conjugacy classes in $\mathbf{C}$. Since $2, 3, 7$ are distinct primes, there are no divisors d_j and d_ℓ as in Lemma A.3(2).

In the rest of the cases note that there are only two primes dividing the order of G and hence by Burnside's theorem G is solvable. Since G is solvable and N is minimal, N is elementary abelian.

Case (2,3,8): In this case $N \cong (\mathbb{Z}/2\mathbb{Z})^\ell$ or $(\mathbb{Z}/3\mathbb{Z})^\ell$ for some $\ell \geq 1$. Moreover, by Lemma A.3(2), the group N is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^\ell$, it contains C_3^4 but not C_1. It follows that the elements $x_i N$, $i = 1, 2, 3$, are of order $2, 3, 4$, respectively, and hence $G/N \cong S_4$. Since N contains only one conjugacy class of $\mathbb{Z}/2\mathbb{Z}$ subgroups, this forces $\ell = 1$ or 2. A Magma check via Remark 4.2 shows that every such extension G contains an element of order 6 or a maximal conjugacy class of order 4, contradicting that the powers of C_1, C_2, C_3 are the only maximal conjugacy classes.

Case (2,4,5): In this case $N \cong (\mathbb{Z}/2\mathbb{Z})^\ell$ or $(\mathbb{Z}/5\mathbb{Z})^\ell$ for some $\ell \geq 1$. Furthermore by Lemma A.3(2), $N \cong (\mathbb{Z}/2\mathbb{Z})^\ell$, the group N contains C_2^2 but not C_1. It follows that the orders of $x_i N$, $i = 1, 2, 3$ in G/N are $2, 2$, and 5, respectively. That is, G/N is either cyclic or dihedral of order 10. Moreover, since N contains only one conjugacy class of elements of order 2, the group G/N acts transitively on the $\mathbb{Z}/2\mathbb{Z}$ subgroups in N, so that N has either $1, 2, 5$ or 10 such groups. Since $N \cong (\mathbb{Z}/2\mathbb{Z})^\ell$ this forces $\ell = 1$. However any such extension of G/N by $\mathbb{Z}/2\mathbb{Z}$ contains an element of order 10, contradicting the maximality of C_3.

Case (3,3,5): In this case $N \cong (\mathbb{Z}/3\mathbb{Z})^\ell$ or $(\mathbb{Z}/5\mathbb{Z})^\ell$ for some $\ell \geq 1$. Furthermore neither of these is possible in view of Lemma A.3(2).

Case (3,3,4): In this case $N \cong (\mathbb{Z}/2\mathbb{Z})^\ell$ or $(\mathbb{Z}/3\mathbb{Z})^\ell$ for some $\ell \geq 1$. Furthermore by Lemma A.3(2), N is $(\mathbb{Z}/2\mathbb{Z})^\ell$ and contains C_3^2. Thus the images of x_1, x_2, x_3 in G/N are

of order $3, 3, 2$, and hence $G/N \cong S_3$ or $\mathbb{Z}/6\mathbb{Z}$. Since G/N acts transitively on the $\mathbb{Z}/2\mathbb{Z}$ subgroups of N, we have $\ell = 1$ or 2. A check using Magma, via Remark 4.2, shows that the only extension of S_3 by $(\mathbb{Z}/2\mathbb{Z})^\ell$ for $\ell \in \{1, 2\}$ which does not contain an element of order divisible by 6 is S_4. However, transpositions form a maximal conjugacy class in S_4 which is different from the C_i's.

Case (2,4,6): $N \cong (\mathbb{Z}/2\mathbb{Z})^\ell$ or $(\mathbb{Z}/3\mathbb{Z})^\ell$ for some $\ell \geq 1$. In the latter case, N contains C_3^2 and hence the images of x_1, x_2, x_3 in G/N are of order $2, 4, 2$, respectively, and hence G/N is dihedral of order 8. Since G/N acts transitively on the $\mathbb{Z}/3\mathbb{Z}$ subgroups of N, it follows that $\ell = 1$ or 2. In this case a computation using Magma shows that the orders of the maximal conjugacy classes are not contained in the multiset $\{2, 4, 6\}$.

In the case $N \cong (\mathbb{Z}/2\mathbb{Z})^\ell$, the subgroup N contains C_2^2 or C_3^3 but does not contain C_1 by Lemma A.3(2). Thus the images of x_1, x_2, x_3 in G/N are of orders (A) $2, 2, 3$ or (B) $2, 2, 6$ or (C) $2, 4, 3$, respectively. Moreover, in cases (B) and (C), N contains a unique conjugacy class of involutions. In cases (B) and (C), G/N is dihedral of order 12 and S_4 respectively. As it acts transitively on the $\mathbb{Z}/2\mathbb{Z}$ subgroup of N, this forces $\ell = 1$ or 2. A check using Magma shows that in both cases, every such group extension G contains a conjugacy class of order different from $2, 4$, and 6.

In case (A), G/N is S_3 and has one or two orbits on $\mathbb{Z}/2\mathbb{Z}$ subgroups of N, forcing $\ell \leq 3$. A check using Magma shows that for all such group extensions G, the orders of maximal conjugacy classes of cyclic groups is not contained in the multiset $\{2, 4, 6\}$.

Appendix B. Generic extensions versus generic polynomials

Let k be a field of characteristic zero, T an indeterminate, and G a non-trivial finite group. Before generic extensions of $k(T)$, a notion of (one parameter) generic polynomial over k was pre-existing:

Definition B.1. Let $P(T, Y) \in k[T, Y]$ be a monic separable polynomial (in Y) of group G over $k(T)$. Say that $P(T, Y)$ is *generic* if, for every field extension L/k and every Galois extension E/L of group G, the field E is the splitting field over L of the polynomial $P(t_0, Y)$ for some $t_0 \in L$.

The following proposition unifies both notions:

Proposition B.2. *Let $P(T, Y) \in k[T, Y]$ be a monic separable polynomial (in Y) of Galois group G and splitting field F over $k(T)$. Then, $P(T, Y)$ is generic if and only if $F/k(T)$ is generic.*

Proof. First, assume $P(T, Y)$ is generic. Let L/k be a field extension and E/L a Galois extension of group G. As $P(T, Y)$ is generic, there is $t_0 \in L$ such that E is the splitting field over L of $P(t_0, Y)$. In particular, $P(t_0, Y)$ has Galois group G over L. Since $(FL)_{t_0}$ contains the splitting field over L of $P(t_0, Y)$ and has degree at most $|G|$, one sees that $(FL)_{t_0}$ and this splitting field coincide. Hence, $E/L = (FL)_{t_0}/L$.

Note that, by using Theorem 5.1 and Proposition 5.3, one can actually show that, if L/k is a field extension and E/L is Galois of group *contained in* G, then, there are *infinitely many* points $t_0 \in L$ such that $E/L = (FL)_{t_0}/L$. Indeed, assume first $G \not\subset \mathrm{PGL}_2(\mathbb{C})$. By Theorem 5.1(a), there are infinitely many Galois extensions of $\overline{k}(U)$ of group G which are not specializations of $F\overline{k}(U)/\overline{k}(U)(T)$. But, for each $t_0 \in \overline{k}(U)$ such that $P(t_0, Y)$ is separable, the splitting field of $P(t_0, Y)$ over $\overline{k}(U)$ and $(F\overline{k}(U))_{t_0}$ coincide. Hence, there are infinitely many Galois extensions $E/\overline{k}(U)$ of group G such that E is the splitting field over $\overline{k}(U)$ of $P(t_0, Y)$ for no $t_0 \in \overline{k}(U)$, which cannot happen as $P(T, Y)$ is generic. Now,

if $G \subset \mathrm{PGL}_2(\mathbb{C})$, then, by Theorem 5.1, one sees that one of the conditions (1), (2), and (3) stated before Proposition 5.3 holds. In particular, our stronger conclusion holds.

Now, assume $F/k(T)$ is generic. By either (the proof of) [JLY02, Proposition 8.1.4] or Theorem 3.1 and Lemma 3.2, the genus g of F is 0. Let L/k be a field extension and E/L a Galois extension of group G. As $F/k(T)$ is generic, there is $t_0 \in \mathbb{P}^1(L)$ such that $E = (FL)_{t_0}$ and, as $\mathrm{Gal}(E/L) = G$, t_0 is not a branch point of $F/k(T)$. Then, by the twisting lemma and as $g = 0$, there exist infinitely many such points t_0. Hence, E is the splitting field over L of $P(t_0, Y)$ for infinitely many points $t_0 \in L$.

As before, a stronger conclusion can be obtained by using Theorem 5.1 and Proposition 5.3. Namely, let L/k be a field extension and E/L a Galois extension of group *contained in* G. As $F/k(T)$ is generic, Theorem 5.1 and Proposition 5.3 show that there are infinitely many points $t_0 \in \mathbb{P}^1(L)$ such that $E = (FL)_{t_0}$. Hence, E is the splitting field over L of $P(t_0, Y)$ for infinitely many points $t_0 \in L$. □

We then obtain this analog of Corollary 5.4 for one parameter generic polynomials:

Corollary B.3. *Let $P(T, Y) \in k[T, Y]$ be a monic separable polynomial (in Y) of Galois group G and splitting field F over $k(T)$. Denote the branch point set of $F/k(T)$ by $\mathbf{t}$. Then, the following two conditions are equivalent:*

(a) *$P(T, Y)$ is generic,*

(b) *one of the following three conditions holds:*

(i) *G is cyclic of even order n such that $e^{2i\pi/n} \in k$, $r = 2$, and $\mathbf{t} \subset \mathbb{P}^1(k)$,*

(ii) *G is cyclic of odd order n such that $e^{2i\pi/n} + e^{-2i\pi/n} \in k$ and $r = 2$,*

(iii) *G is dihedral of order $2n$ with $n \geq 3$ odd and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$, $r = 3$, and $\mathbf{t} \subset \mathbb{P}^1(k)$.*

In particular, G has a one parameter generic polynomial over k iff one of the following three conditions holds:

- *G is cyclic of even order n and $e^{2i\pi/n} \in k$,*
- *G is cyclic of odd order n and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$,*
- *G is dihedral of order $2n$ with $n \geq 3$ odd and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$.*

Remark B.4. (a) Definition B.1 is the definition of (one parameter) generic polynomial that is used in the classical book [JLY02]. Several other choices could have been possible. For example, a strong variant, used by Kemper (see [Kem01]), requires Galois extensions E/L of group *contained in* G to be parametrized. In [DeM83], DeMeyer even requires every Galois extension E/L of group contained in G to be realized by a *separable* specialized polynomial. However, the proof of Proposition B.2 shows that, for one parameter polynomials over fields of characteristic zero, these three definitions are actually equivalent. In particular, one retrieves [Kem01, Theorem 1] in this situation[25].

(b) In the case k contains all roots of unity, the last part of Corollary B.3[26] was known from the essential theory of Buhler-Reichstein; see [BR97] and [JLY02]. The general case, though feasible with the same tools, does not seem to appear explicitly in the literature.

References

[AC81] Enrico Arbarello and Maurizio Cornalba. Footnotes to a paper of Beniamino Segre: "On the modules of polygonal curves and on a complement to the Riemann existence theorem" (Italian) [Math. Ann. **100** (1928), 537–551; Jbuch **54**, 685]. The number of g^1_d's on a general d-gonal

[25] This result asserts more generally that the first two definitions are equivalent over infinite fields (for polynomials with an arbitrary number of parameters).

[26] That is, G has a one parameter generic polynomial over k iff G is either cyclic or odd dihedral.

curve, and the unirationality of the Hurwitz spaces of 4-gonal and 5-gonal curves. *Math. Ann.*, 256(3):341–362, 1981.

[BR97] J. Buhler and Z. Reichstein. On the essential dimension of a finite group. *Compositio Math.*, 106(2):159–179, 1997.

[DD97a] Pierre Dèbes and Bruno Deschamps. The regular inverse Galois problem over large fields. In *Geometric Galois actions, 2*, volume 243 of *London Math. Soc. Lecture Note Ser.,* (L. Schneps and P. Lochak ed), pages 119–138. Cambridge Univ. Press, Cambridge, 1997.

[DD97b] Pierre Dèbes and Jean-Claude Douai. Algebraic covers: field of moduli versus field of definition. *Ann. Sci. École Norm. Sup. (4)*, 30(3):303–338, 1997.

[DD09] Tim Dokchitser and Vladimir Dokchitser. Elliptic curves with all quadratic twists of positive rank. *Acta Arith.*, 137(2):193–197, 2009.

[Dea89] Marian Deaconescu. Classification of finite groups with all elements of prime order. *Proc. Amer. Math. Soc.*, 106(3):625–629, 1989.

[Dèb99] Pierre Dèbes. Galois covers with prescribed fibers: the Beckmann-Black problem. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 28(2):273–286, 1999.

[Dèb17] Pierre Dèbes. On the Malle conjecture and the self-twisted cover. *Israel J. Math.*, 218(1):101–131, 2017.

[Dèb18] Pierre Dèbes. Groups with no parametric Galois realizations. *Ann. Sci. Éc. Norm. Supér. (4)*, 51(1):143–179, 2018.

[DeM83] Frank R. DeMeyer. Generic polynomials. *J. Algebra*, 84(2):441–448, 1983.

[DL13] Pierre Dèbes and François Legrand. Specialization results in Galois theory. *Trans. Amer. Math. Soc.*, 365(10):5259–5275, 2013.

[DLS66] H. Davenport, D. J. Lewis, and A. Schinzel. Quadratic Diophantine equations with a parameter. *Acta Arith.*, 11:353–358, 1965/1966.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden. xxiv+792 pp.

[Fri77] Michael D. Fried. Fields of definition of function fields and Hurwitz families-groups as Galois groups. *Comm. Algebra*, 5(1):17–82, 1977.

[FV91] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4):771–800, 1991.

[Jar11] Moshe Jarden. *Algebraic patching*. Springer Monographs in Mathematics. Springer, Heidelberg, 2011. xxiv+290 pp.

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials. Constructive Aspects of the Inverse Galois Problem*. Cambridge University Press, 2002.

[Kem01] Gregor Kemper. Generic polynomials are descent-generic. *Manuscripta Math.*, 105(1):139–141, 2001.

[KLN17] Joachim König, François Legrand, and Danny Neftin. On the local behaviour of specializations of function field extensions. *International Mathematics Research Notices*, 2017. To appear; doi: 10.1093/imrn/rny016.

[KM01] Jürgen Klüners and Gunter Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196, 2001.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, revised third edition, 2002.

[Leg15] François Legrand. Parametric Galois extensions. *J. Algebra*, 422:187–222, 2015.

[Leg16] François Legrand. Specialization results and ramification conditions. *Israel J. Math.*, 214(2):621–650, 2016.

[Mes90] Jean-François Mestre. Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$. (French). *J. Algebra*, 131(2):483–495, 1990.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[Mül02] Peter Müller. Finiteness results for Hilbert's irreducibility theorem. *Ann. Inst. Fourier (Grenoble)*, 52(4):983–1015, 2002.

[Mum99] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Second, expanded edition, 1999. Includes the Michigan

lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello. x+306 pp.
[Pop96] Florian Pop. Embedding problems over large fields. *Ann. of Math. (2)*, 144(1):1–34, 1996.
[Sad99] Bounab Sadi. *Descente effective du corps de définition des revêtements*. Thèse Univ. Lille 1, 1999.
[Sal82] David J. Saltman. Generic Galois extensions and problems in field theory. *Adv. in Math.*, 43(3):250–283, 1982.
[Sch00] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier. x+558 pp.
[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics. Jones and Bartlett Publishers, 1992.
[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. xx+513 pp.
[Völ96] Helmut Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. An introduction. xviii+248 pp.

E-mail address: Pierre.Debes@math.univ-lille1.fr

E-mail address: jkoenig@kaist.ac.kr

E-mail address: francois.legrand@tu-dresden.de

E-mail address: dneftin@technion.ac.il

Laboratoire de Mathématiques Paul Painlevé, Université de Lille, 59655 Villeneuve d'Ascq Cedex, France

Department of Mathematical Sciences, KAIST, 291 Daehak-ro Yuseong-gu Daejeon 34141, South Korea

Institut für Algebra, Fachrichtung Mathematik, TU Dresden, 01062 Dresden, Germany

Department of Mathematics, Technion, Israel Institute of Technology, Haifa 32000, Israel