Journal of Pure and Applied Algebra 225 (2021) 106717

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

On parametric and generic polynomials with one parameter

Pierre Dèbes [a], Joachim König [b], François Legrand [c,*], Danny Neftin [d]

[a] *Laboratoire de Mathématiques Paul Painlevé, Université de Lille, 59655 Villeneuve d'Ascq Cedex, France*
[b] *Department of Mathematics Education, Korea National University of Education, 28173 Cheongju, South Korea*
[c] *Institut für Algebra, Fachrichtung Mathematik, TU Dresden, 01062 Dresden, Germany*
[d] *Department of Mathematics, Technion, Israel Institute of Technology, Haifa 32000, Israel*

ARTICLE INFO

Article history:
Received 10 August 2020
Received in revised form 26 October 2020
Available online 15 February 2021
Communicated by V. Suresh

MSC:
12F12; 11R58; 11G05; 12E30

ABSTRACT

Given fields $k \subseteq L$, our results concern one parameter L-*parametric* polynomials over k, and their relation to generic polynomials. The former are polynomials $P(T,Y) \in k[T][Y]$ of group G which parametrize all Galois extensions of L of group G via specialization of T in L, and the latter are those which are L-parametric for every field $L \supseteq k$. We show, for example, that being L-parametric with L taken to be the single field $\mathbb{C}((V))(U)$ is in fact sufficient for a polynomial $P(T,Y) \in \mathbb{C}[T][Y]$ to be generic. As a corollary, we obtain a complete list of one parameter generic polynomials over a given field of characteristic 0, complementing the classical literature on the topic. Our approach also applies to an old problem of Schinzel: subject to the Birch and Swinnerton-Dyer conjecture, we provide one parameter families of affine curves over number fields, all with a rational point, but with no rational generic point.

1. Introduction

Understanding the set $\mathsf{R}_G(k)$ of all finite Galois extensions of a given number field k with given Galois group G is a central objective in algebraic number theory. A first natural question in this area, which goes back to Hilbert and Noether, is the so-called *inverse Galois problem*: is $\mathsf{R}_G(k) \neq \emptyset$ for every number field k and every finite group G? A more applicable goal is an explicit description of the sets $\mathsf{R}_G(k)$, such as a parametrization. A classical landmark in this context is the following definition (see the book [15]):

Definition 1.1. Let k be a (number) field, G a finite group, $n \geq 1$, and $P(T_1, \ldots, T_n, Y) \in k[T_1, \ldots, T_n][Y]$ a monic separable polynomial of group G over $k(T_1, \ldots, T_n)$.

* Corresponding author.
E-mail addresses: pierre.debes@univ-lille.fr (P. Dèbes), jkoenig@knue.ac.kr (J. König), francois.legrand@tu-dresden.de (F. Legrand), dneftin@technion.ac.il (D. Neftin).

https://doi.org/10.1016/j.jpaa.2021.106717
0022-4049/

(1) Given an overfield $L \supseteq k$, say that $P(T_1, \dots, T_n, Y)$ is *L-parametric* if, for every extension $E/L \in \mathsf{R}_G(L)$, there exists $(t_1, \dots, t_n) \in L^n$ such that E is the splitting field over L of $P(t_1, \dots, t_n, Y)$.
(2) Say that $P(T_1, \dots, T_n, Y)$ is *generic* if it is L-parametric for every overfield $L \supseteq k$.

For example, the polynomial $Y^2 - T$ is generic for the group $G = \mathbb{Z}/2\mathbb{Z}$ over any number field k. On the other hand, some number fields k and finite groups G are known not to have a generic polynomial with coefficients in k, e.g., $k = \mathbb{Q}$ and $G = \mathbb{Z}/8\mathbb{Z}$ (see [15, §2.6]). However, if k is a given number field and G is a given finite group, it is in general unknown whether there is a generic polynomial of group G with coefficients in k; existence of such polynomial implies $\mathsf{R}_G(k) \neq \emptyset$, which is already open in general. Even for groups like $G = A_d$, for which $\mathsf{R}_G(k) \neq \emptyset$ is known, the question is open (for $d \geq 6$ and $k = \mathbb{Q}$; see [15, §8.5]).

The case $n = 1$ is better understood. If k is any field of characteristic zero, finite groups G with a generic polynomial $P(T, Y) \in k[T][Y]$ are precisely known (see §2.3). In the case $k = \mathbb{Q}$, those groups are exactly the subgroups of S_3. If k is arbitrary, only cyclic groups and dihedral groups of order $2m$ with $m \geq 3$ odd can have a generic polynomial $P(T, Y) \in k[T][Y]$.

Here are the main stages of the classification.
- If $G \not\subset \mathrm{PGL}_2(k)$ and if $P(T, Y) \in k[T][Y]$ is of group G, then $P(T, Y)$ is not generic; indeed, the Noether invariant extension $k(\mathbf{T})/k(\mathbf{T})^G$, with $\mathbf{T} = (T_1, \dots, T_{|G|})$, cannot be reached by specializing $P(T, Y)$ at some $T = t_0 \in k(\mathbf{T})^G$ (see [15, Proposition 8.1.4]).
- If G ($\subset \mathrm{PGL}_2(k)$ and) has a non-cyclic abelian subgroup, then the *essential dimension* theory of Buhler–Reichstein (see [1,15]) shows that there is no generic polynomial $P(T, Y) \in k[T][Y]$ of group G.
- The remaining finite subgroups of $\mathrm{PGL}_2(k)$ have a generic polynomial $P(T, Y) \in k[T][Y]$, except $\mathbb{Z}/n\mathbb{Z}$ when n is even and k contains $\zeta_n + \zeta_n^{-1}$ but not ζ_n (ζ_n a primitive n-th root of unity).

We present a new approach, which allows more precise non-parametricity conclusions, over some specific fields, and leads to improvements on the above results. Theorem 1.2 is a new general result on one parameter non-generic polynomials. Corollary 1.3 shows the concrete gain for the classification discussed above.

Theorem 1.2. *Let k be a field of characteristic zero, $P(T, Y) \in k[T][Y]$ a monic separable polynomial, and U, V two indeterminates. Suppose $P(T, Y)$ is not generic. Then either $P(T, Y)$ is not $\overline{k}((V))(U)$-parametric or $P(T, Y)$ is not $k(U)$-parametric.*

Thus Theorem 1.2 gives explicit base changes L/k such that any non-generic polynomial $P(T, Y) \in k[T][Y]$ is not L-parametric. Compared to the previous approach, our base changes are purely transcendental, of transcendence degree 1, and do not depend on the Galois group G of $P(T, Y)$ over $k(T)$, unlike the base change $k(\mathbf{T})^G/k$ of the first stage above.

We refer to Corollary 3.5 for a more general version of Theorem 1.2, which also presents some variants. For example, we prove that, if G is neither cyclic nor dihedral of order $2n$ with $n \geq 3$ odd (in particular, $P(T, Y)$ is not generic), then $P(T, Y)$ is not $\overline{k}((V))(U)$-parametric.

The proof of Theorem 1.2 uses a variety of tools, including the arithmetic specialization methods of [19], patching methods from [12], and the geometric specialization methods of [8].

Using Theorem 1.2, we obtain an explicit list of all the one parameter generic polynomials over any field k of characteristic 0 (and not only the groups with such a polynomial). For simplicity, we give the list for $k = \mathbb{Q}$ (see Corollary 3.6 for the general case).

Corollary 1.3. *Let G be a non-trivial finite group and $P(T, Y) \in \mathbb{Q}[T][Y]$ a monic separable polynomial of group G and splitting field F over $\mathbb{Q}(T)$. Then $P(T, Y)$ is generic if and only if one of these conditions holds (up to a Möbius transformation on T):*
(1) *$G = \mathbb{Z}/2\mathbb{Z}$ and F is the splitting field over $\mathbb{Q}(T)$ of $Y^2 - T$,*

(2) $G = \mathbb{Z}/3\mathbb{Z}$ *and* F *is the splitting field over* $\mathbb{Q}(T)$ *of* $Y^3 - TY^2 + (T-3)Y + 1$,
(3) $G = S_3$ *and* F *is the splitting field over* $\mathbb{Q}(T)$ *of* $Y^3 + TY + T$.

Note that the list is essentially known to experts, and the given polynomials are also known to be generic. The list complements the literature by showing that these indeed are the only one parameter generic polynomials (over $\mathbb{Q}$).

Our second type of results gives non-parametricity conclusions over k itself (i.e., no base change L/k is allowed). Such conclusions depend more on the arithmetic of k. For example, if k is PAC, i.e., if every non-empty geometrically irreducible k-variety has a Zariski-dense set of k-rational points (see [10]), *every* polynomial $P(T,Y) \in k[T][Y]$ (whose splitting field F over $k(T)$ fulfills $F \cap \overline{k} = k$) is k-parametric (see [5]).[1]

However, if k is a number field, it is expected that, as in the generic situation, most finite groups fail to have a k-parametric polynomial $P(T,Y) \in k[T][Y]$. Yet, no such group was known before [18,19], which provide many examples. But the question remains of the classification of all the finite groups G with a k-parametric polynomial $P(T,Y) \in k[T][Y]$, and of the associated polynomials. Could it be the same as in the generic situation? For $n \geq 2$, this is not the case: $\mathbb{Z}/8\mathbb{Z}$ has a $\mathbb{Q}$-parametric polynomial $P(T_1, \dots, T_n, Y) \in \mathbb{Q}[T_1, \dots, T_n][Y]$ for some $n \geq 2$ (see [32]) but no generic polynomial over $\mathbb{Q}$. For $n = 1$, the question is subtler. We show that, for polynomials $P(T,Y) \in k[T][Y]$, "k-parametric" is still strictly weaker than "generic", and even weaker than "$k(U)$-parametric", but only under the Birch and Swinnerton-Dyer conjecture.

This comparison between the various notions relates to the following old problem of Schinzel (see [33, Chapter 5, §5.1]):

Question 1.4. *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 $k(U)^2$?*

We combine previous works producing "lawful evil" elliptic curves (see, e.g., [4,24]) and a result of [6] on the branch point number of rational pullbacks of Galois covers of $\mathbb{P}^1$ to obtain infinitely many (conditional) counter-examples to Question 1.4. For example, we have the following (see Theorem 4.3 for a more general result):

Theorem 1.5. *Let $Q(T) \in \mathbb{Q}[T]$ be a degree 3 separable polynomial such that the elliptic curve given by $Y^2 = Q(T)$ has complex multiplication by $\mathbb{Q}(\sqrt{-m})$ for some $m \in \{11, 19, 43, 67, 163\}$. Set $P(U,T,Y) = Y^2 - UQ(T)$. Under the Birch and Swinnerton-Dyer conjecture, there exist infinitely many quadratic number fields k such that*
(1) *the answer to Question 1.4 is negative for k and P, and*
(2) *the polynomial $P(1,T,Y)$ and the field k form a counter-example to this implication:*
$(*)$ *k-parametric $\Rightarrow$ $k(U)$-parametric.*

A concrete situation where Theorem 1.5 applies is $Q(T) = T^3 - T^2 - 7T + 41/4$, $m = 11$, and $k = \mathbb{Q}(\sqrt{-d})$, where $d > 0$ is squarefree and fulfills $(\frac{d}{11}) = 1$ (see Remark 4.4).

All counter-examples to Question 1.4 known to us are in genus 1, i.e., when the $\mathbb{C}(U)$-curve $P(U,T,Y) = 0$ is of genus 1.[2] This suggests that the genus 1 case is exceptional. It remains plausible that the answer to

[1] There are PAC fields k with $\mathsf{R}_G(k) \neq \emptyset$ for every finite group G, and so for which the k-parametricity property is not trivial as it is for algebraically closed fields. A concrete example (due to Pop) is $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$.
[2] For an earlier counter-example, subject to a conjecture of Selmer, see [33, pp. 318-319].

Question 1.4 is "Yes" in genus ≥ 2.[3] The same could be true of Implication $(*)$. Indeed, by [6], a positive answer to (a close variant) of Question 1.4 implies (a close variant of) Implication $(*)$. See §4 for more details.

Our results are stated in terms of polynomials $P(T,Y)$. They translate immediately in terms of field extensions $F/k(T)$. The latter viewpoint is the one that we will prefer in the sequel. We refer to Lemma 2.3 for the exact connection between the two viewpoints.

Acknowledgments. We thank Danny Krashen and the referee for helpful comments. 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.

2. Preliminaries

§2.1 and §2.2 are devoted to terminology and notation. In §2.3, we review the classification of all the finite groups with a one parameter generic polynomial with coefficients in a given field of characteristic zero (see Theorem 2.5). As said in §1, Corollary 3.6 will more precisely give the list of corresponding polynomials. Finally, in §2.4, we briefly discuss étale algebras, which will be used to prove Theorem 1.2 and its generalizations.

2.1. Basic terminology

Let k be a field of characteristic zero and $F/k(T)$ a finite Galois extension. Say that $F/k(T)$ is *k-regular* if $F\cap\overline{k}=k$. By the *branch point set* of $F/k(T)$, we mean the finite set $\mathbf{t}$ of points $t\in\mathbb{P}^1(\overline{k})$ such that the associated discrete valuations are ramified in $F\overline{k}/\overline{k}(T)$. As k has characteristic 0, we have the *inertia canonical invariant* $\mathbf{C}$ of $F/k(T)$: if $\mathbf{t}=\{t_1,\dots,t_r\}$, then $\mathbf{C}$ is an r-tuple $(C_1,\dots,C_r)$ of conjugacy classes of $\mathrm{Gal}(F\overline{k}/\overline{k}(T))$, and C_i is the conjugacy class of the distinguished generators of the inertia groups $I_{\mathfrak{P}}$ above t_i in $F\overline{k}/\overline{k}(T)$ (i.e., these generators correspond to $e^{2i\pi/e_i}$ in the canonical isomorphism $I_{\mathfrak{P}}\to\mu_{e_i}=\langle e^{2i\pi/e_i}\rangle$). We also use the notation $\mathbf{e}=(e_1,\dots,e_r)$ for the r-tuple whose i-th entry is the ramification index $e_i=|I_{\mathfrak{P}}|$ of primes above t_i; e_i is also the order of elements of C_i. By the *genus* of $F/k(T)$, we mean the genus of $F\overline{k}$.

The *specialization* F_{t_0}/k of $F/k(T)$ at $t_0\in\mathbb{P}^1(k)$ is defined as follows. For $t_0\in k$ (resp., $t_0=\infty$), the field F_{t_0} is the residue field of the integral closure of $k[T]$ (resp., of $k[1/T]$) in F at any prime ideal $\mathfrak{P}$ containing $T-t_0$ (resp., $1/T$). The extension F_{t_0}/k is Galois and, if $t_0\notin\mathbf{t}$, its Galois group is the decomposition group of $F/k(T)$ at $\mathfrak{P}$. If F is the splitting field over $k(T)$ of a monic separable polynomial $P(T,Y)\in k[T][Y]$, then, for $t_0\in k$ with $P(t_0,Y)$ separable, $t_0\notin\mathbf{t}$ and F_{t_0} is the splitting field over k of $P(t_0,Y)$.

Lemma 2.1. *We have $(FL)_{t_0}=F_{t_0}L$ for every overfield $L\supseteq k$ and every $t_0\in\mathbb{P}^1(k)$.*

Proof. Without loss, we may assume $t_0\neq\infty$. Denote the integral closure of $k[T]$ in F by B_k. Pick $s\geq 1$ and $b_1,\dots,b_s$ in B_k with $B_k=k[T]b_1+\cdots+k[T]b_s$. As k has characteristic zero, L/k is separable (in the sense of non-necessarily algebraic extensions; see, e.g., [22, Chapter VIII, §4]). Then, by, e.g., [10, Proposition 3.4.2], the integral closure B_L of $L[T]$ in FL equals $L[T]b_1+\cdots+L[T]b_s$. Let $\mathfrak{P}_L$ be a prime ideal of B_L containing $T-t_0$. Then the restriction $\mathfrak{P}_k=\mathfrak{P}_L\cap B_k$ of $\mathfrak{P}_L$ to B_k also contains $T-t_0$. We then have $(FL)_{t_0}=B_L/\mathfrak{P}_L=L(\overline{b_1},\dots,\overline{b_s})$, where $\overline{b_1},\dots,\overline{b_s}$ denote the reductions modulo $\mathfrak{P}_L$ of $b_1,\dots,b_s$, respectively. But these reductions modulo $\mathfrak{P}_L$ are the reductions $\underline{b_1},\dots,\underline{b_s}$ modulo $\mathfrak{P}_k$ of $b_1,\dots,b_s$, respectively. Hence, $(FL)_{t_0}=k(\underline{b_1},\dots,\underline{b_s})L=F_{t_0}L$. □

[3] In genus 0, the answer to Question 1.4 is "Yes" (see [9, Theorem 2] and [31, Theorem 38]).

2.2. Generic and parametric extensions

Given a finite group G and a field k (of characteristic zero), we will use the following notation.
- $\mathsf{R}_G(k)$: set of all Galois extensions E/k of group G.
- $\mathsf{R}_{\leq G}(k)$: set of all Galois extensions E/k of group contained in G.
- For a finite Galois extension $F/k(T)$ of branch point set $\mathbf{t}$, we define

$$\mathsf{SP}(F/k(T)) = \{F_{t_0}/k \mid t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}\} \quad (\mathsf{SP} \text{ for "SPecialization"}).$$

Definition 2.2. Let k be of characteristic 0 and $F/k(T)$ a Galois extension of group G.
(1) Given an overfield $L \supseteq k$, the extension $F/k(T)$ is *L-parametric* (resp., *strongly L-parametric*) if $\mathsf{SP}(FL/L(T)) \supseteq \mathsf{R}_G(L)$ (resp., if $\mathsf{SP}(FL/L(T)) = \mathsf{R}_{\leq G}(L)$).
(2) The extension $F/k(T)$ is *generic* if it is L-parametric for every overfield $L \supseteq k$.

The field extension viewpoint used in Definition 2.2 is of course equivalent to the polynomial one used in §1. The next two lemmas, which will be used on several occasions in the sequel, provide the precise arguments to pass from one viewpoint to the other.

Lemma 2.3. *Let k be a field of characteristic zero, G a finite group, $F/k(T)$ a Galois extension of group G, and $P(T,Y) \in k[T][Y]$ a monic separable polynomial of splitting field F over $k(T)$. Let $L \supseteq k$ be any overfield.*
(1) *Let $E/L \in \mathsf{R}_G(L)$. If E is the splitting field over L of $P(t_0,Y)$ for some $t_0 \in L$, then $E/L \in \mathsf{SP}(FL/L(T))$.*
(2) *Let $E/L \in \mathsf{R}_{\leq G}(L)$. If there exist infinitely many $t_0 \in \mathbb{P}^1(L)$ such that $E/L = (FL)_{t_0}/L$, then E is the splitting field over L of $P(t_0,Y)$ for infinitely many $t_0 \in L$.*

Proof. (1) Assume there is $t_0 \in L$ such that E is the splitting field over L of $P(t_0,Y)$. It is always true that the splitting field of $P(t_0,Y)$ is contained in the field $(FL)_{t_0}$. As, in our situation, the former is of degree $|G|$ over L, both fields coincide and we get $E = (FL)_{t_0}$. To conclude, note that t_0 is not a branch point of $F/k(T)$, since $\mathrm{Gal}((FL)_{t_0}/L) = G$.
(2) By the assumption, there are infinitely many $t_0 \in \mathbb{P}^1(L)$ with $E = (FL)_{t_0}$. For such a t_0 with $t_0 \neq \infty$ and $P(t_0,Y)$ separable, the splitting field of $P(t_0,Y)$ over L equals $(FL)_{t_0}$ (as recalled in §2.1), i.e., equals E. □

Our second lemma adjusts [15, Proposition 5.1.8] to our situation:

Lemma 2.4. *Let k be a field of characteristic zero and $F/k(T)$ a generic extension. Then there exists a generic polynomial $P(T,Y) \in k[T][Y]$ of splitting field F over $k(T)$.*

Proof. First, denote the integral closure of $k[T]$ in F by B_k. Pick a positive integer s and an s-tuple $(b_1,\dots,b_s)$ of elements of B_k with $B_k = k[T]b_1 + \cdots + k[T]b_s$. Up to reordering, we may assume there exists $s' \leq s$ satisfying these two conditions:
- for $1 \leq i \neq j \leq s'$, b_i and b_j are not conjugate over $k(T)$,
- for $i > s'$, there exists $1 \leq j \leq s'$ such that b_i and b_j are conjugate over $k(T)$.

For each $i \in \{1,\dots,s'\}$, denote the minimal polynomial of b_i over $k(T)$ by $m_i(T,Y)$. Set $P_1(T,Y) = \prod_{i=1}^{s'} m_i(T,Y)$. Then $P_1(T,Y)$ is a monic separable polynomial with coefficients in $k[T]$, and its splitting field over $k(T)$ is equal to F.

Now, let $L \supseteq k$ and $E/L \in \mathsf{R}_{\leq G}(L)$ (with $G = \mathrm{Gal}(F/k(T))$). Assume $E/L = (FL)_{t_0}/L$ for some $t_0 \in L$. Let $\mathfrak{P}_L$ be a maximal ideal of the integral closure B_L of $L[T]$ in FL containing $T - t_0$. As in the proof of

Lemma 2.1, we have $B_L = L[T]b_1 + \cdots + L[T]b_s$. Hence, with $\overline{b_1}, \ldots, \overline{b_s}$ the respective reductions modulo $\mathfrak{P}_L$ of $b_1, \ldots, b_s$, we have $(FL)_{t_0} = B_L/\mathfrak{P}_L = L(\overline{b_1}, \ldots, \overline{b_s})$. Thus, E is the splitting field over L of $P_1(t_0, Y)$.

Next, if we replace T by $1/T$, the same arguments yield a monic separable polynomial $P_2(T, Y) \in k[T][Y]$ of splitting field F over $k(T)$ which fulfills this: for all $L \supseteq k$ and $E/L \in \mathsf{R}_{\leq G}(L)$, if $E = (FL)_\infty$, then E is the splitting field over L of $P_2(0, Y)$.

Finally, since $F/k(T)$ is assumed to be generic, we get the following: for every overfield $L \supseteq k$ and every extension $E/L \in \mathsf{R}_G(L)$, there are $i \in \{1, 2\}$ and $t_0 \in L$ such that E is the splitting field over L of $P_i(t_0, Y)$. It then remains to use [15, Corollary 1.1.6] to get that either $P_1(T, Y)$ or $P_2(T, Y)$ is generic. □

2.3. Finite groups with a one parameter generic polynomial/extension

We give the classification of these groups over any given field of characteristic zero:

Theorem 2.5. *Let k be a field of characteristic 0 and G a finite group. Then the following three conditions are equivalent:*

(1) *there exists a generic extension $F/k(T)$ of group G,*
(2) *there exists a generic polynomial $P(T, Y) \in k[T][Y]$ of group G,*
(3) *one of the following three conditions holds:*
   (a) *G is cyclic of even order n and $e^{2i\pi/n} \in k$,*
   (b) *G is cyclic of odd order n and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$,*
   (c) *G is dihedral of order $2n$ with $n \geq 3$ odd and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$.*

Proof. Implication (2) ⇒ (1) is an immediate consequence of Lemma 2.3(1) while Lemma 2.4 yields Implication (1) ⇒ (2). It then remains to show (2) ⇔ (3). This equivalence is known to experts but does not seem to appear explicitly in the literature. For the convenience of the reader, we recall the main ingredients.

First, assume there is a generic polynomial $P(T, Y) \in k[T][Y]$ of group G. By [15, Proposition 8.2.4], the *essential dimension* of G over $\overline{k}$ is 1. Over fields of characteristic 0 containing all roots of unity, such groups are exactly cyclic groups and dihedral groups of order $2n$ with $n \geq 3$ odd (see [1, Theorem 6.2]). Hence, G is cyclic or dihedral of order $2n$ with $n \geq 3$ odd.

Now, suppose $G = \mathbb{Z}/n\mathbb{Z}$ ($n \geq 2$). Using again [15, Proposition 8.2.4], if there is a generic polynomial $P(T, Y) \in k[T][Y]$ of group G, the essential dimension of G over k is 1. Theorem 1.3 of [3] then yields $e^{2i\pi/n} + e^{-2i\pi/n} \in k$ if n is odd, and $e^{2i\pi/n} \in k$ if n is even. Conversely, assume either n is even and $e^{2i\pi/n} \in k$, or n is odd and $e^{2i\pi/n} + e^{-2i\pi/n} \in k$. In the even case, $Y^n - T$ has Galois group G over $k(T)$ and is generic (by the Kummer theory). Now, in the odd case, there is a generic polynomial $P(T, Y) \in k[T][Y]$ of group G, by [15, §2.1 and Exercise 5.13].

Finally, given $n \geq 3$ odd, suppose G is dihedral of order $2n$. If there is a generic polynomial $P(T, Y) \in k[T][Y]$ of group G, then, by [15, Proposition 8.2.4] and [3, Theorem 1.4], we have $e^{2i\pi/n} + e^{-2i\pi/n} \in k$. Conversely, if $e^{2i\pi/n} + e^{-2i\pi/n} \in k$, then, by a classical construction of Hashimoto and Miyake (see [15, Theorem 5.5.4]), there is a generic polynomial $P(T, Y) \in k[T][Y]$ of group G. □

Remark 2.6. Groups with essential dimension 1 over a given field k (of any characteristic) are classified in [3]. It might then be possible to derive the list of all groups with a one parameter generic polynomial/extension over k, as done above in characteristic 0.

2.4. Étale algebras

Let k be a field of characteristic 0. A general reference for this section is [15, §4.3]. Every G-Galois extension L/k of étale algebras is an *induced* from a Galois field extension L'/k whose Galois group $H =$

$\mathrm{Gal}(L'/k)$ is a subgroup of G. In particular, $L = \bigoplus_{\sigma H \in G/H} \sigma(L')$. The Galois group of the field extension L'/k is then its stabilizer under the action of G. The *underlying field* L' is determined up to choosing a direct summand of L. When picking a conjugate copy $\sigma(L')$, the resulting stabilizer is the conjugate subgroup $\sigma H \sigma^{-1}$.

Remark 2.7. Given an overfield $M \supseteq k$, the tensor product $(L \otimes_k M)/M$ is well-known to be a G-Galois extension of étale algebras, whose underlying field is a compositum $L \cdot M$ via some embedding of $\overline{k}$ into $\overline{M}$.

The induced G-Galois extension $k^{|G|}$ from the trivial extension k/k is called the *split* G-Galois extension.

3. Parametricity and genericity

§3.1 states the main results of this section. These results are proved in §3.2–§3.5. Finally, in §3.6, we explain how Theorem 1.2 and Corollary 1.3 are derived.

3.1. Main results

Let G be a non-trivial finite group, k a field of characteristic 0, and U, V two indeterminates. Let $F/k(T)$ be a 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 denoted by $\mathbf{e}$.

The main topic of this section is this question:
$(*)$ *Given an overfield $L \supseteq k$, is $F/k(T)$ L-parametric?*
In the next result, we give three explicit base changes 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 $(*)$ is negative in general, if L is taken among the fields L_1, L_2, and L_3.

Recall that a field K is *ample* (or *large*) if every smooth K-curve has 0 or infinitely many K-rational points. Ample fields include algebraically closed fields, the complete valued fields $\mathbb{Q}_p$, $\mathbb{R}$, $\kappa((Y))$, the field $\mathbb{Q}^{\mathrm{tr}}$ of totally real numbers (algebraic numbers such that all conjugates are real). See [14,2,29] for more details.

Theorem 3.1. (1) *Let $K \supseteq k$ be an ample overfield and $L_1 = K(U)$. Assume $g \geq 1$. Then $\mathsf{R}_G(L_1) \setminus \mathsf{SP}(FL_1/L_1(T))$ contains infinitely many K-regular extensions.*
(2) *Let $K \supseteq k$ be an algebraically closed overfield and $L_2 = K((V))(U)$. Assume G has a non-cyclic abelian subgroup. Then $\mathsf{R}_G(L_2) \setminus \mathsf{SP}(FL_2/L_2(T))$ contains infinitely many $K((V))$-regular extensions.*
(3) *Let $L_3 = k(U)$. Assume either one of the following two conditions holds:*
(a) *G is cyclic of even order, $r = 2$, and $\mathbf{t} \not\subset \mathbb{P}^1(k)$,*
(b) *G is dihedral of order $2n$ with $n \geq 3$ odd, $r = 3$, and $\mathbf{t} \not\subset \mathbb{P}^1(k)$.*
Then $\mathsf{R}_G(L_3) \setminus \mathsf{SP}(FL_3/L_3(T))$ contains infinitely many k-regular extensions.

The extensions for which none of the statements of Theorem 3.1 applies are of genus 0 (by (1)). Recall that, if $F \cap \overline{k} = k$, the case $g = 0$ can occur only in the next situations:
- 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 $\mathbf{e} = (2, 3, 5)$.

Hence, taking now (2) and (3) into account, we obtain that, if $F \cap \overline{k} = k$, the only cases for which none of the statements of Theorem 3.1 applies are the following ones:

(a) G is cyclic of even order, $r = 2$, and $\mathbf{t} \subset \mathbb{P}^1(k)$,
(b) G is cyclic of odd order and $r = 2$,
(c) G is dihedral of order $2n$ with $n \geq 3$ odd, $r = 3$, and $\mathbf{t} \subset \mathbb{P}^1(k)$.

Proposition 3.2. *Assume $F \cap \overline{k} = k$ and that* (a) *or* (b) *or* (c) *holds. Then, for every field $L \supseteq k$ and every E/L in $\mathsf{R}_{\leq G}(L)$, we have $E = (FL)_{t_0}$ for infinitely many $t_0 \in \mathbb{P}^1(L)$.*

3.2. Proof of Theorem 3.1(1)

As K is ample, $\mathsf{R}_G(L_1)$ contains infinitely many pairwise linearly disjoint K-regular extensions (see [28, Main Theorem A]). If $F \cap \overline{k} \neq k$, at most one of these is in $\mathsf{SP}(FL_1/L_1(T))$. Hence, assume $F \cap \overline{k} = k$. Then, as $g \geq 1$ and K is ample, [8, Theorem 3.10(a-1)] and its proof yield infinitely many K-regular extensions $E/L_1 \in \mathsf{R}_G(L_1)$ each of which satisfies $E \neq (FL_1)_{t_0}$ for any $t_0 \in L_1 \setminus K$. Pick such an E/L_1 and assume $E = (FL_1)_{t_0}$ for some $t_0 \in \mathbb{P}^1(L_1)$. Then $t_0 \in \mathbb{P}^1(K)$ and Lemma 2.1 gives $E = (FK)_{t_0}L_1$. As $E \cap \overline{K} = K$, we get $(FK)_{t_0} = K$ and so $E = L_1$, a contradiction.

3.3. Proof of Theorem 3.1(2)

Set $M = K((V))$ (so $L_2 = M(U) = K((V))(U)$). For each $u \in M$, denote by $\mathfrak{P}_u$ the prime ideal of $M[U]$ generated by $U - u$.

We will need the following two lemmas. The first one is a function field analog of [19, Proposition 6.3] (which is stated over number fields):

Lemma 3.3. *Assume $F \cap \overline{k} = k$. For each $t_0 \in \mathbb{P}^1(L_2)$ and all but finitely many $u \in M$ (not depending on t_0), the Galois group of the completion at $\mathfrak{P}_u$ of $(FL_2)_{t_0}/L_2$ is cyclic.*

Proof. The proof is similar to that in the number field case, and relies on [19, Theorem 4.1] (the main result of that paper). For the convenience of the reader, we offer a proof, with the needed adjustments. Let $u \in M$ and $t_0 \in \mathbb{P}^1(L_2)$. If $(FL_2)_{t_0}/L_2$ is unramified at $\mathfrak{P}_u$, then the Galois group of its completion at $\mathfrak{P}_u$ is cyclic (as $M = K((V))$ with K algebraically closed of characteristic 0). We may then suppose $(FL_2)_{t_0}/L_2$ is ramified at $\mathfrak{P}_u$. In particular, $t_0 \notin \mathbf{t}$. Indeed, if $t_0 \in \mathbf{t}$, then $t_0 \in \mathbb{P}^1(\overline{k})$. By Lemma 2.1, we would have $(FL_2)_{t_0} = (F\overline{k})_{t_0}L_2 = L_2$, which cannot happen as $(FL_2)_{t_0}/L_2$ ramifies at $\mathfrak{P}_u$. Up to dropping finitely many values of u (depending only on $FL_2/L_2(T)$), we may use the Specialization Inertia Theorem of [23, §2.2] to get that t_0 meets some branch point of $F/k(T)$, say t, modulo $\mathfrak{P}_u$ (see [23, Definition 2.2]). As above, $(FL_2)_t = L_2$. Let I_t be the inertia group of $Fk(t)/k(t)(T)$ at $\langle T - t \rangle$. Up to dropping finitely many values of u (depending only on $FL_2/L_2(T)$), [19, Theorem 4.1] yields that the Galois group of the completion at $\mathfrak{P}_u$ of $(FL_2)_{t_0}/L_2$ embeds into I_t. As I_t is cyclic, we are done. □

Lemma 3.4. *For every $u \in M$, there exists an M-regular extension $E/L_2 \in \mathsf{R}_G(L_2)$ whose completion at $\mathfrak{P}_u$ has a non-cyclic abelian Galois group.*

Proof. By a linear change of the variable U, we may without loss of generality assume that $\mathfrak{P}_u = \langle U \rangle$. To prove the lemma, we follow the construction and patching methods of [12, §4], and adjust these to our setup. Let $X = \mathbb{P}^1_K$ be the closed fibre of $\hat{X} = \mathbb{P}^1_{K[[V]]}$. Our prime $\mathfrak{P}_u$ corresponds to a maximal ideal $\langle V, U \rangle \lhd K[[V]][U]$ whose image in $K[U]$ is $\langle U \rangle$, the prime corresponding to the point $0 \in \mathbb{P}^1_K$ of the closed fibre.

Let $\mathcal{C}$ be the set of cyclic subgroups of G, and $S \subseteq \mathbb{A}^1_K \subseteq X$ a finite set of points[4] consisting of $u_0 = 0 \in \mathbb{A}^1_K$ and distinct non-zero points $u_c \in \mathbb{A}^1_K$, $c \in \mathcal{C}$. For $u_c \in S$, let $F_c = K((V, U - u_c))$ denote the fraction field of the complete local ring $\hat{R}_c = K[[V, U - u_c]]$ at u_c. For the (open) complement $O = X \setminus S$, consider the V-adic completion of the subring of functions on $\hat{X}$ that are regular on O, and let F_O be its fraction field. For $u_c \in S$, also consider the localization of $\hat{R}_c$ at the prime $\langle V \rangle$ (corresponding to a branch in [12]), and let $F_{\wp(c)} = K((U - u_c))((V))$ be the fraction field of its V-adic completion.

Consider the inverse system I whose objects are the above fields F_O and F_c, $F_{\wp(c)}$ for $u_c \in S$, and whose morphisms are the natural inclusions $F_c \subseteq F_{\wp(c)}$ and $F_O \subseteq F_{\wp(c)}$ for $u_c \in S$. A collection of G-Galois extensions E_ξ/F_ξ, $\xi \in I$ of étale algebras, together with isomorphisms $E_O \otimes_{F_O} F_{\wp(c)} \to E_{\wp(c)}$, $E_c \otimes_{F_c} F_{\wp(c)} \to E_{\wp(c)}$ for all $u_c \in S$, is called a *patching data* (of G-Galois étale algebras).

We construct the fields E_ξ, $\xi \in I$ following the proof of [12, Proposition 4.4]. Let $E_O = F_O^{|G|}$ and $E_{\wp(c)} = F_{\wp(c)}^{|G|}$, $u_c \in S$ be split G-Galois extensions. It now remains to define the G-Galois extensions E_c/F_c whose underlying field E'_c is contained in $F_{\wp(c)}$, and hence $E_c \otimes_{F_c} F_{\wp(c)} \cong F_{\wp(c)}^{|G|} = E_{\wp(c)}$, giving the desired isomorphisms.

Put $f_c = U - u_c \in \hat{R}_c$ and set

$$a_c = \frac{f_c}{f_c - V} \text{ for } u_c \in S, \text{ and } b_0 = \frac{U - V^2}{U - V - V^2}.$$

For $c \in \mathcal{C}$, let $E'_c = F_c(\sqrt[m]{a_c})$ for $m = |c|$. As a_c is not a d-th power for any $d > 1$, Kummer theory yields $\mathrm{Gal}(E'_c/F_c) = c$. Moreover, since $E_{\wp(c)}$ is complete with respect to $\langle V \rangle$, the element a_c is an m-th power in $F_{\wp(c)}$ by Hensel's lemma, and hence $E'_c \subseteq F_{\wp(c)}$. Then let E_c/F_c be the G-Galois extension induced from the c-Galois field extension E'_c/F_c.

Finally, let $H \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ be a non-cyclic abelian subgroup of G for a prime q, and $E'_0 = F_0(\sqrt[q]{a_0}, \sqrt[q]{b_0})$. Using Kummer theory as before, $F_0(\sqrt[q]{a_0})/F_0$ and $F_0(\sqrt[q]{b_0})/F_0$ both have Galois group $\mathbb{Z}/q\mathbb{Z}$. The extension $F_0(\sqrt[q]{a_0})/F_0$ is ramified at the prime $\langle U \rangle \lhd \hat{R}_0$ while $F_0(\sqrt[q]{b_0})/F_0$ is unramified there. Hence, $F_0(\sqrt[q]{a_0})$ and $F_0(\sqrt[q]{b_0})$ are linearly disjoint over F_0, and E'_0/F_0 is a Galois extension of fields with Galois group H. Applying Hensel's lemma as before, one has $E'_0 \subseteq F_{\wp(0)}$. Then let E_0/F_0 be the extension induced from E'_0/F_0. As $E'_c \subseteq F_{\wp(c)}$, $u_c \in S$, we conclude that E_ξ, $\xi \in I$ is a patching data.

By [12, Theorem 4.1], there exists a G-Galois extension E/F of étale algebras such that $E \otimes_{L_2} F_c$ is isomorphic to E_c for every $u_c \in S$. Moreover, identifying the two via this isomorphism, E_c is generated by E and F_c, and the subalgebra $E' \otimes_{L_2} F_c \subseteq E_c$, generated by F_c and the underlying field E' of E, contains a conjugate copy of E'_c, for every $u_c \in S$. We claim that E/L_2 is an M-regular field extension. Put $G' = \mathrm{Gal}(E'/L_2)$. For every $c \in \mathcal{C}$, the subgroup c of G is the stabilizer of E'_c under the action of G. As $E' \otimes_{L_2} F_c$ contains a conjugate copy of E'_c and is stabilized by G', we get that G' contains a conjugate of c. As G' contains a conjugate of every cyclic subgroup c of G, Jordan's theorem (see [16]) implies that $G' = G$, and hence $E' = E$ is a field. To show that E is M-regular, let $\overline{G} \trianglelefteq G$ be the subgroup fixing the constant field $E \cap \overline{M}$. As E'_c is a compositum of E' and F_c by Remark 2.7 and E'_c/F_c is M-regular, we get that $\overline{G}$ contains a conjugate of c. As $\overline{G}$ is normal, $c \leq \overline{G}$ for every $c \in \mathcal{C}$, and hence $\overline{G} = G$, as claimed.

Finally, since the completion of E at $\mathfrak{P}_u$ is the field underlying $E \otimes_{L_2} M((U))$, and since the field E'_0 is a compositum of E and F_0, the completion of E at $\langle U \rangle$ is isomorphic to the underlying field $M((U))(\sqrt[q]{a_0}, \sqrt[q]{b_0})$ of $E'_0 \otimes_{F_0} M((U))$. Now, $M((U))(\sqrt[q]{a_0})/M((U))$ has Galois group $\mathbb{Z}/q\mathbb{Z}$ and is totally ramified. On the other hand, $M((U))(\sqrt[q]{b_0})/M((U))$ is unramified and hence linearly disjoint from $M((U))(\sqrt[q]{a_0})/M((U))$. We claim that $\mathrm{Gal}(M((U))(\sqrt[q]{b_0})/M((U))) = \mathbb{Z}/q\mathbb{Z}$. Given the claim, the above shows that the extension $M((U))(\sqrt[q]{a_0}, \sqrt[q]{b_0})/M((U))$ is of group H, which is non-cyclic abelian, as desired.

[4] Note that, although in [12] the set S is chosen specifically, [13, Proposition 3.4] shows that the set S can be chosen to be an arbitrary finite set.

To prove the claim, observe that $b_0 \equiv V/(V+1)$ modulo U, and put $\overline{b_0} = V/(V+1)$. As $M(\sqrt[q]{\overline{b_0}})/M$ is totally ramified at $\langle V\rangle$, we deduce that $\mathrm{Gal}(M(\sqrt[q]{\overline{b_0}})/M) = \mathbb{Z}/q\mathbb{Z}$. Hensel's lemma then implies that $M((U))(\sqrt[q]{\overline{b_0}})/M((U))$ also has Galois group $\mathbb{Z}/q\mathbb{Z}$. □

Proof of Theorem 3.1(2). If $F \cap \overline{k} \neq k$, then $\mathrm{Gal}(FL_2/L_2(T)) \neq G$. Hence, $\mathsf{R}_G(L_2) \cap \mathsf{SP}(FL_2/L_2(T)) = \emptyset$. But, as K is algebraically closed of characteristic 0, Riemann's existence theorem yields $\mathsf{R}_G(K(U)) \neq \emptyset$ and so $\mathsf{R}_G(L_2)$ contains infinitely many M-regular extensions. Hence, we may assume $F \cap \overline{k} = k$. Lemmas 3.3 and 3.4 then yield that $\mathsf{R}_G(L_2) \setminus \mathsf{SP}(FL_2/L_2(T))$ contains infinitely many M-regular extensions, as needed. □

3.4. Proof of Theorem 3.1(3)

First, recall that, if a finite group G is a regular Galois group over an infinite field k, i.e., if there is a k-regular Galois extension of $k(U)$ of group G, then applying suitable Möbius transformations on U leads to infinitely many k-regular Galois extensions of $k(U)$ of group G such that the branch point sets of any two such extensions are disjoint. The Riemann–Hurwitz formula then shows that these k-regular Galois extensions of $k(U)$ are pairwise linearly disjoint. In the present situation, G is cyclic or dihedral of order $2n$ with $n \geq 3$ odd, and k is of characteristic 0. Since abelian groups and dihedral groups are regular Galois groups over all fields, we get that $\mathsf{R}_G(L_3)$ contains infinitely many pairwise linearly disjoint k-regular extensions. If $F/k(T)$ is not k-regular, at most one of these can be in $\mathsf{SP}(F(U)/L_3(T))$. Hence, assume $F \cap \overline{k} = k$.

Now, assume $G = \mathbb{Z}/n\mathbb{Z}$ for some even $n \geq 2$ and $r = 2$. As n is even, there is an L_3-regular Galois extension of $L_3(T)$ of group G with a branch point in $\mathbb{P}^1(L_3)$, and with another branch point of ramification index n. Then, by [23, Corollary 3.4], there is a prime $\mathfrak{Q}$ of $k[U]$ such that, for all but finitely many u in k, there is $E_u/L_3 \in \mathsf{R}_G(L_3)$ which ramifies at $\mathfrak{P}_u = \langle U - u\rangle$, and whose ramification index at $\mathfrak{Q}$ is n. In particular, E_u/L_3 is k-regular (by the last condition). Suppose $E_u/L_3 \in \mathsf{SP}(F(U)/L_3(T))$ for infinitely many $u \in k$. Without loss, we may assume $\infty \notin \mathbf{t}$. For $i \in \{1,2\}$, denote the minimal polynomial of t_i over k by $m_i(T)$. Then, by [23, Corollary 2.12 and Remark 3.11], the reduction modulo $\mathfrak{P}_u$ of $m_1(T)m_2(T) \in k[U][T]$ has a root in the residue field $k[U]/\mathfrak{P}_u$ for some $u \in k$. As this residue field is k, $m_1(T)m_2(T)$ has a root in k. Hence, by the Branch Cycle Lemma (see [11] and [36, Lemma 2.8]), t_1 and t_2 are in $\mathbb{P}^1(k)$.

Finally, assume G is dihedral of order $2n$ 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 [10, §16.2 and Proposition 16.4.4], every k-regular extension in $\mathsf{R}_{\mathbb{Z}/2\mathbb{Z}}(L_3)$ embeds into a k-regular extension in $\mathsf{R}_G(L_3)$. Hence, if all but finitely many k-regular extensions in $\mathsf{R}_G(L_3)$ are in $\mathsf{SP}(F(U)/L_3(T))$, then, as G has a unique subgroup of index 2, all but finitely many k-regular extensions in $\mathsf{R}_{\mathbb{Z}/2\mathbb{Z}}(L_3)$ are specializations of the quadratic subextension of $F(U)/L_3(T)$. As the latter has only two branch points (namely, t_1 and t_2), a similar argument as in the cyclic case yields that these branch points have to be in $\mathbb{P}^1(k)$.

3.5. Proof of Proposition 3.2

Assume $F \cap \overline{k} = k$ and one of the following holds:
(a) G is cyclic of even order, $r = 2$, and $\mathbf{t} \subset \mathbb{P}^1(k)$,
(b) G is cyclic of odd order and $r = 2$,
(c) G is dihedral of order $2n$ with $n \geq 3$ odd, $r = 3$, and $\mathbf{t} \subset \mathbb{P}^1(k)$.
Let $L \supseteq k$ and $E/L \in \mathsf{R}_{\leq G}(L)$. By the twisting lemma (see [5]), there is a k-regular extension $(FL)_E/L(T)$ such that $(FL)_E\overline{L} = F\overline{L}$ and such that, 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 $E/L = (FL)_{t_0}/L$. In each case, the genus of F is 0 (if (c) holds,

this follows from **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 (a) holds, then the unique prime ideal lying over $\langle T-t_1\rangle$ in $(FL)_E/L(T)$ has residue degree 1. If (b) holds, the desired conclusion follows from G being of odd order and the genus being 0; see, e.g., end of Page 1 of [34]. Finally, assume (c) 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 that 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 $L(\sqrt{dT})$. 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 is $y_0\in L$ such that the specialization of $(FL)_E/L(Y)$ at y_0 is L/L. Hence, there is a prime ideal lying over $\langle T-(y_0)^2/d\rangle$ in $(FL)_E/L(T)$ with residue degree 1.

3.6. Proofs of Theorem 1.2 and Corollary 1.3

We conclude this section by explaining how Theorem 1.2 and Corollary 1.3 follow from Theorem 3.1 and Proposition 3.2.

We start with the following consequence, of which Conclusion (1) is Theorem 1.2 and Conclusion (2) is mentioned in the abstract:

Corollary 3.5. *Let k be of characteristic 0, let U,V be indeterminates, and let $P(T,Y)\in k[T][Y]$ be a monic separable polynomial of group G and splitting field F over $k(T)$.*
(1) *Assume $P(T,Y)$ is not generic. Then either $P(T,Y)$ is not $k(U)$-parametric or $P(T,Y)$ is not $K((V))(U)$-parametric for any algebraically closed overfield $K\supseteq k$.*
(2) *Assume $P(T,Y)$ is not generic and k is algebraically closed. Then $P(T,Y)$ is not $K((V))(U)$-parametric for any algebraically closed overfield $K\supseteq k$.*
(3) *Assume G is neither cyclic nor dihedral of order $2n$ with $n\geq 3$ odd. Then $P(T,Y)$ is not $K((V))(U)$-parametric for any algebraically closed overfield $K\supseteq k$.*
(4) *If $G\not\subset \mathrm{PGL}_2(\mathbb{C})$, then $P(T,Y)$ is $K(U)$-parametric for no ample overfield $K\supseteq k$.*

Proof. (1) Assume $P(T,Y)$ is $k(U)$-parametric and $K((V))(U)$-parametric for some algebraically closed overfield $K\supseteq k$. Then, by Lemma 2.3(1), the same holds for $F/k(T)$. As in the proof of Theorem 3.1(2) (see the end of §3.3), $F/k(T)$ being $K((V))(U)$-parametric implies that $F/k(T)$ is k-regular. Moreover, by Theorem 3.1, one of the three conditions stated before Proposition 3.2 holds. Hence, by that proposition, we have that, for every overfield $L\supseteq k$ and every $E/L\in \mathsf{R}_G(L)$, there exist infinitely many $t_0\in\mathbb{P}^1(L)$ such that $E=(FL)_{t_0}$. It then remains to use Lemma 2.3(2) to conclude that $P(T,Y)$ is generic.
(2) The proof is similar to that of (1), except that we have to use that neither Condition (a) nor Condition (b) of Theorem 3.1(3) can happen (since k is algebraically closed).
(3) If $P(T,Y)$ is $K((V))(U)$-parametric for some algebraically closed overfield $K\supseteq k$, then, as in (1), $F/k(T)$ is $K((V))(U)$-parametric and k-regular. Moreover, Theorem 3.1(1) and Theorem 3.1(2) yield that we are in the situation of Theorem 3.1(3) or in that of Proposition 3.2. In both cases, G is cyclic or dihedral of order $2n$ with $n\geq 3$ odd.
(4) Assume $P(T,Y)$ is $K(U)$-parametric for some ample overfield $K\supseteq k$. As in the proof of (1), $F/k(T)$ is $K(U)$-parametric. As already recalled in §3.2, $\mathsf{R}_G(K(U))$ contains infinitely many pairwise linearly disjoint extensions. Hence, $F/k(T)$ is k-regular. Finally, Theorem 3.1(1) gives that $F/k(T)$ is of genus 0, and so $G\subset\mathrm{PGL}_2(\mathbb{C})$. □

We finally get to the classification of all the one parameter generic polynomial/extensions over a given field of characteristic zero:

Corollary 3.6. *Let k be of characteristic 0 and $P(T,Y) \in k[T][Y]$ a monic separable polynomial of group G and splitting field F over $k(T)$. Denote the branch point number (resp., branch point set) of $F/k(T)$ by r (resp., by $\mathbf{t}$). The following three conditions are equivalent:*
(1) *$F/k(T)$ is generic,*
(2) *$P(T,Y)$ is generic,*
(3) *$F \cap \overline{k} = k$ and one of the following three conditions holds:*
  (a) *G is cyclic of even order n such that $e^{2i\pi/n} \in k$, $r = 2$, and $\mathbf{t} \subset \mathbb{P}^1(k)$,*
  (b) *G is cyclic of odd order n such that $e^{2i\pi/n} + e^{-2i\pi/n} \in k$ and $r = 2$,*
  (c) *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 $\mathbf{t} \subset \mathbb{P}^1(k)$.*

We need the next lemma, which is classical in inverse Galois theory. The "only if" part is an immediate consequence of the Branch Cycle Lemma (see [11] and [36, Lemma 2.8]) and the "if" part is due to the rigidity method (see, e.g., [36, Chapter 3]).

Lemma 3.7. *Let k be a field of characteristic zero.*
(1) *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 if and only if $e^{2i\pi/n} + e^{-2i\pi/n} \in k$; both branch points can be chosen in $\mathbb{P}^1(k)$ if and only if $e^{2i\pi/n} \in k$.*
(2) *Given $n \geq 3$ odd, there is a k-regular Galois extension of $k(T)$ with dihedral Galois group of order $2n$, with three branch points, and all branch points in $\mathbb{P}^1(k)$ if and only if $e^{2i\pi/n} + e^{-2i\pi/n} \in k$.*

Proof of Corollary 3.6. First, (2) $\Rightarrow$ (1) follows from Lemma 2.3(1). Now, assume (1) holds. Then, as already seen, $F/k(T)$ is k-regular. Moreover, by Theorem 3.1, one of the conditions stated before Proposition 3.2 holds. Then, by Lemma 3.7, (3) holds. Finally, if (3) holds, then $P(T,Y)$ is generic, by Lemma 2.3(2) and Proposition 3.2. □

Remark 3.8. (1) Corollary 3.6 and Lemma 3.7 give another proof of Theorem 2.5.
(2) In the spirit of Definition 2.2, say that $F/k(T)$ is *strongly generic* if it is strongly L-parametric for every overfield $L \supseteq k$. Clearly, we have $F/k(T)$ strongly generic $\Rightarrow$ $F/k(T)$ generic. The converse holds by combining Proposition 3.2 and Corollary 3.6.
(3) Definition 1.1 is the definition of generic polynomials of [15]. Variants could have been used. For example, a strong one, used by Kemper (see [17]), requires extensions in $\mathsf{R}_{\leq G}(L)$ to be parametrized. In [7], DeMeyer even requires every extension in $\mathsf{R}_{\leq G}(L)$ to be realized by a *separable* specialized polynomial. Lemma 2.3(2), Proposition 3.2, and Corollary 3.6 show that, for one parameter polynomials over fields of characteristic 0, the three definitions are equivalent. In particular, we retrieve [17, Theorem 1] in this case (Kemper's result asserts, more generally, that the first two definitions are equivalent over infinite fields, for polynomials with an arbitrary number of parameters).

Proof of Corollary 1.3. Let G be finite non-trivial and $P(T,Y) \in \mathbb{Q}[T][Y]$ be monic separable of group G and splitting field F over $\mathbb{Q}(T)$. By (2) $\Leftrightarrow$ (3) in Corollary 3.6 (with $k = \mathbb{Q}$), $P(T,Y)$ is generic if and only if $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$ and one of these conditions holds:
- $G = \mathbb{Z}/2\mathbb{Z}$ and $F/\mathbb{Q}(T)$ has two branch points, which are $\mathbb{Q}$-rational,
- $G = \mathbb{Z}/3\mathbb{Z}$ and $F/\mathbb{Q}(T)$ has two branch points,
- $G = S_3$ and $F/\mathbb{Q}(T)$ has three branch points, which are $\mathbb{Q}$-rational.

In the first case, observe next that any $\mathbb{Q}$-regular quadratic extension of $\mathbb{Q}(T)$ with two branch points, which are $\mathbb{Q}$-rational, equals $\mathbb{Q}(\sqrt{d(T-a)(T-b)})/\mathbb{Q}(T)$ or $\mathbb{Q}(\sqrt{d(T-a)})/\mathbb{Q}(T)$ for some $d \in \mathbb{Z}$ and $a, b \in \mathbb{Q}$. All of these are derived from $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$, by applying a suitable Möbius transformation on T. Hence, if $G = \mathbb{Z}/2\mathbb{Z}$, the polynomial $P(T,Y)$ is generic if and only if $F = \mathbb{Q}(\sqrt{T})$, up to some Möbius transformation on T.

In the second case, let $F_1/\mathbb{Q}(T)$ and $F_2/\mathbb{Q}(T)$ be $\mathbb{Q}$-regular Galois extensions of group $\mathbb{Z}/3\mathbb{Z}$ with two branch points. Fix $j \in \{1,2\}$. By the Branch Cycle Lemma, the branch points of $F_j/\mathbb{Q}(T)$ are $\mathbb{Q}$-conjugate and generate $\mathbb{Q}(e^{2i\pi/3})$ over $\mathbb{Q}$. Moreover, $(F_j)_{t_j} = \mathbb{Q}$ for some $t_j \in \mathbb{P}^1(\mathbb{Q})$. Up to applying $T \mapsto 1/(T-t_j)$, we may assume $t_j = \infty$. Then, up to applying $T \mapsto (T-a)/b$ for some $a, b \in \mathbb{Q}$ with $b \neq 0$, which fixes ∞, we may also assume the branch point set of $F_j/\mathbb{Q}(T)$ is $\{e^{2i\pi/3}, e^{4i\pi/3}\}$. Then $F_1\overline{\mathbb{Q}} = F_2\overline{\mathbb{Q}}$. Indeed, we would have otherwise that $F_1F_2\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ has Galois group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and so has at least three branch points, which cannot happen. Hence, $[F_1F_2\overline{\mathbb{Q}} : \overline{\mathbb{Q}}(T)] = 3$. If $F_1 \neq F_2$, then $[F_1F_2 : \mathbb{Q}(T)] = 9$ and $F_1F_2/\mathbb{Q}(T)$ has a degree 3 constant subextension. But the latter cannot happen as $(F_1F_2)_\infty = (F_1)_\infty(F_2)_\infty = \mathbb{Q}$ (see [10, Lemma 2.4.8] for the first equality). We then have $F_1 = F_2$. Hence, a $\mathbb{Q}$-regular Galois extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/3\mathbb{Z}$ with two branch points is unique, up to Möbius transformations on T. Let F' be the splitting field of $Y^3 - TY^2 + (T-3)Y + 1$ over $\mathbb{Q}(T)$. As $F'/\mathbb{Q}(T)$ is $\mathbb{Q}$-regular of group $\mathbb{Z}/3\mathbb{Z}$, and has two branch points, we are done in the case $G = \mathbb{Z}/3\mathbb{Z}$.

Finally, consider the case $G = S_3$. The inertia canonical invariant of a $\mathbb{Q}$-regular Galois extension of $\mathbb{Q}(T)$ of group S_3 with 3 branch points is (C_2, C_2, C_3), with C_n the conjugacy class of the n-cycles. As (C_2, C_2, C_3) is a rigid triple of rational conjugacy classes of the centerless group S_3, there is only one $\mathbb{Q}$-regular Galois extension of $\mathbb{Q}(T)$ of group S_3 with three $\mathbb{Q}$-rational branch points, up to Möbius transformation on T (see [34, Chapters 7 and 8]). Then we are done as, if F' is the splitting field of $Y^3 + TY + T$ over $\mathbb{Q}(T)$, then $F'/\mathbb{Q}(T)$ is $\mathbb{Q}$-regular, of group S_3, and of branch point set $\{0, \infty, -27/4\}$. □

4. On Schinzel's problem and its variants

We investigate the connections between k-parametricity and $k(U)$-parametricity, in relation with Schinzel's problem (Question 1.4).

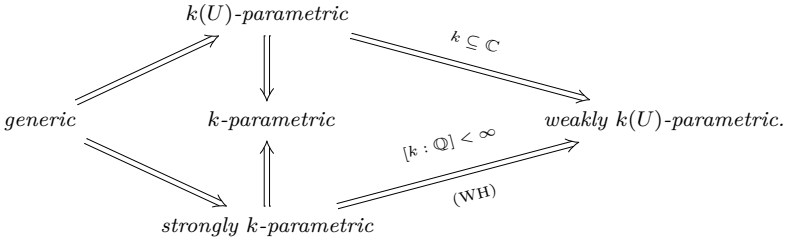
In §1, we mentioned a close variant of Question 1.4. It corresponds to the following diophantine working hypothesis, which is introduced in [6, §2.4.2]:

(WH) *Let k be a number field, and let $f_i : X_i \to \mathbb{P}^1_{k(U)}$, $i = 1, \dots, N$, be $k(U)$-regular covers. Assume that no curve X_i has a $\mathbb{C}(U)$-rational point that is unramified w.r.t. the cover f_i, $i = 1, \dots, N$. Then, for infinitely many $u_0 \in k$, the covers $f_1, \dots, f_N$ have good reduction at $U = u_0$ and no reduced curve $X_i|_{u_0}$ has a k-rational point that is unramified w.r.t. the cover $f_i|_{u_0} : X_i|_{u_0} \to \mathbb{P}^1_k$, $i = 1, \dots, N$.*

Proposition 4.2 below summarizes some of the connections between our notions of parametricity and genericity. As already said, if k is a number field, a close variant of the implication "k-parametric $\Rightarrow$ $k(U)$-parametric" holds under (WH). It is given by the implication "strongly k-parametric $\Rightarrow$ weakly $k(U)$-parametric" below.

Definition 4.1. Let G be a finite group, k a subfield of $\mathbb{C}$, and $F/k(T)$ a k-regular extension in $\mathsf{R}_G(k(T))$. We say that $F/k(T)$ is *weakly $k(U)$-parametric* if every k-regular extension $E/k(U) \in \mathsf{R}_G(k(U))$ is a specialization of $F(U)/k(U)(T)$, after base change $\mathbb{C}/k$.

Proposition 4.2. *For a field k of characteristic zero and a finite k-regular Galois extension of $k(T)$, we have*



Proof. The implications "generic $\Rightarrow$ $k(U)$-parametric" and "strongly k-parametric $\Rightarrow$ k-parametric" are clear, while "generic $\Rightarrow$ strongly k-parametric" follows from Remark 3.8(2). Next, [6, Remark 2.3] proves "strongly $k(U)$-parametric $\Rightarrow$ strongly k-parametric". With the same arguments as there, we get "$k(U)$-parametric $\Rightarrow$ k-parametric". Now, if $k \subseteq \mathbb{C}$, the implication "$k(U)$-parametric $\Rightarrow$ weakly $k(U)$-parametric" follows from Lemma 2.1. Finally, if k is a number field and (WH) holds, then the implication "strongly k-parametric $\Rightarrow$ weakly $k(U)$-parametric" is [6, Proposition 2.17(b)]. □

The implication "strongly k-parametric $\Rightarrow$ weakly $k(U)$-parametric", which holds under (WH) and if k is a number field, was used in [6] to produce (conditionally) examples of finite groups with no strongly k-parametric extension $F/k(T)$, by first providing examples of finite groups with no weakly $k(U)$-parametric extension $F/k(T)$. The following theorem suggests, however, that this approach fails in general.

To word it, we denote by $W(C/k) \in \{\pm 1\}$ the root number of an elliptic curve C over a number field k. We refer to, e.g., [35,30] for the definition and, more generally, for more on the terminology of elliptic curves that is used below.

Theorem 4.3. *Let k be a number field and $Q(T) \in k[T]$ an irreducible degree 3 polynomial such that the elliptic curve $C : Y^2 = Q(T)$ fulfills $W(C/k) = -1$, but $W(C/L) = +1$ for every quadratic extension L/k. Set $F/\mathbb{Q}(T) = \mathbb{Q}(T)(\sqrt{Q(T)})/\mathbb{Q}(T)$ and $P(U,T,Y) = Y^2 - UQ(T)$. Then, under the Birch and Swinnerton-Dyer conjecture, we have:*
(1) *$F/\mathbb{Q}(T)$ is strongly k-parametric but neither weakly $k(U)$-parametric nor $k(U)$-parametric,*
(2) *$Y^2 - Q(T)$ is strongly k-parametric but not $k(U)$-parametric,*
(3) *the answer to Question 1.4 is negative for the field k and the polynomial $P(U,T,Y)$,*
(4) *the above hypothesis* (WH) *fails for the number field k and the sole $k(U)$-regular Galois cover $X \to \mathbb{P}^1_{k(U)}$ given by the polynomial $P(U,T,Y)$.*

Proof of Theorem 4.3. Under the Birch and Swinnerton-Dyer conjecture, and by our assumption on $W(C/k)$, the elliptic curve C has odd rank over k, and so infinitely many k-rational points. Similarly, for every non-square $u_0 \in k$, the twisted elliptic curve $C_{u_0} : Y^2 = u_0 Q(T)$ has positive rank, and so infinitely many k-rational points. See [4] for more details. Hence, the next two statements (which are equivalent) hold:
(a) *for each $u_0 \in k^*$, the polynomial $P(u_0,T,Y)$ has a zero (t,y) in k^2 such that $y \neq 0$,*
(b) *every trivial or quadratic extension of k is the splitting field over k of some separable polynomial $Y^2 - Q(t_0)$ with $t_0 \in k$.*

Now, we have:
(c) *given a field L of characteristic zero, $L(\sqrt{U})/L(U) \notin \mathsf{SP}(FL(U)/L(U)(T))$.*
Indeed, let L be a field of characteristic 0. Since $F/\mathbb{Q}(T)$ has 4 branch points while $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$ has only 2, [6, Theorem 2.1] yields $L(\sqrt{U}) \neq (FL(U))_{t_0}$ for every $t_0 \in L(U) \setminus L$. Then use Lemma 2.1 as in §3.2 to rule out the constant specializations at points $t_0 \in \mathbb{P}^1(L)$.

Next, (c) is equivalent to the following:
(d) *for L of characteristic zero, $P(U,T,Y)$ has no zero $(t,y) \in L(U)^2$ such that $y \neq 0$.*
In particular, we have:
(e) *the polynomial $P(U,T,Y)$ has no zero in $k(U)^2$.*
Indeed, suppose $P(U,T,Y)$ has such a zero (t,y). As $Q(T)$ is assumed irreducible over k, we have that t is not a root of $Q(T)$. Hence, $y \neq 0$, which cannot happen by (d).

Finally, by (b) and (c), $F/\mathbb{Q}(T)$ is strongly k-parametric but not weakly $k(U)$-parametric. The (weaker) conclusion that it is not $k(U)$-parametric then follows from Proposition 4.2. Now, (2) follows from (b), (1), and Lemma 2.3(1). Next, (3) follows from (a) and (e). As to (4), it basically follows from (1) and Proposition 4.2 (in fact, from (a) and (d)). □

We now explain how Theorem 1.5 follows from Theorem 4.3:

Proof of Theorem 1.5. Let $Q(T) \in \mathbb{Q}[T]$ be a degree 3 separable polynomial such that the elliptic curve $C/\mathbb{Q}$ given by $Y^2 = Q(T)$ has complex multiplication by $k_0 = \mathbb{Q}(\sqrt{-m})$ for some $m \in \{11, 19, 43, 67, 163\}$. As $k_0 \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$, we may apply [24, Corollary 4.10] to get that there exist infinitely many quadratic number fields k such that $W(C/k) = -1$ and $W(C/L) = +1$ for every quadratic extension L of k. Moreover, since $C/\mathbb{Q}$ has complex multiplication by $k_0 = \mathbb{Q}(\sqrt{-m})$ for some $m \in \{11, 19, 43, 67, 163\}$, the elliptic curve $C/\mathbb{Q}$ has trivial $\mathbb{Q}$-torsion (see the table in [26]). In particular, the triviality of the rational 2-torsion subgroup is equivalent to the irreducibility of $Q(T)$ over $\mathbb{Q}$, and so over every quadratic number field. Consequently, there exist infinitely many quadratic number fields k such that the elliptic curve C/k fulfills the assumptions of Theorem 4.3, thus yielding the assertion. □

Remark 4.4. (1) First explicit examples of elliptic curves C and number fields k as in Theorem 4.3 were given in [4], where they are called "lawful evil" elliptic curves. See [24, Theorem 4.9] for an even more general construction of such curves C and fields k. The explicit example given right after the statement of Theorem 1.5 is taken from [24, Example 4.12(ii)].
(2) In the context of Theorem 4.3, the polynomial $Q(T)$ is separable of degree 3. Hence, the $\mathbb{C}(U)$-curve $P(U, T, Y) = 0$ is of genus 1. It remains plausible that (WH) holds if $f_1, \dots, f_N$ are all of genus ≥ 2, which would yield that any given finite k-regular Galois extension $F/k(T)$ of genus ≥ 2 which is not weakly $k(U)$-parametric is actually not strongly k-parametric. Similarly, it is plausible that the answer to Question 1.4 is affirmative for $\mathbb{C}(U)$-curves $P(U, T, Y) = 0$ of genus at least 2.

As recalled in Proposition 4.2, if a k-regular Galois extension of $k(T)$ is $k(U)$-parametric, then it is k-parametric. Theorem 4.3(1) shows that the converse fails (conditionally) over number fields. Here is another counter-example, unconditional, over Laurent series fields:

Proposition 4.5. *Let k be algebraically closed of characteristic zero and G a finite group.*
(1) *There exists $F/k(T) \in \mathsf{R}_G(k(T))$ fulfilling the following. Let $K \supseteq k$ be algebraically closed and $L = K((V))$. Then $F/k(T)$ is strongly L-parametric. More precisely, given $E/L \in \mathsf{R}_{\leq G}(L)$, we have $E = (FL)_{t_0}$ for infinitely many $t_0 \in \mathbb{P}^1(L)$.*
(2) *If G is neither cyclic nor dihedral of order $2n$ with $n \geq 3$ odd, then, for $L = K((V))$ where K is any algebraically closed field containing k, the extension $F/k(T)$ is not $L(U)$-parametric.*

Lemma 4.6. *Let k be of characteristic zero, $K \supseteq k$ an algebraically closed overfield, G a finite group, and $L = K((V))$. Then a given k-regular extension $F/k(T) \in \mathsf{R}_G(k(T))$ with inertia canonical invariant $(C_1, \dots, C_r)$ is strongly L-parametric if and only if*
$(*)$ 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. Moreover, if $(*)$ holds, then, given $E/L \in \mathsf{R}_{\leq G}(L)$, there exist infinitely many $t_0 \in \mathbb{P}^1(L)$ such that $E = (FL)_{t_0}$.

Proof. The set $\mathsf{R}_{\leq G}(L)$ precisely consists of all the extensions of the form $L(\sqrt[n]{V})/L$, where n is any element order in G. As 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 extension $F/k(T) \in \mathsf{R}_G(k(T))$ is strongly L-parametric if and only if $FL/L(T)$ has a specialization at some $t_0 \in \mathbb{P}^1(L)$, which is not a branch point of $F/k(T)$, of ramification index n at $\mathfrak{P}$, for each element order n in G.

Firstly, assume $(*)$ 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 [23, Theorem 3.1], there are infinitely many $t_0 \in L$ such that the inertia group at $\mathfrak{P}$ of $(FL)_{t_0}/L$ is generated by an element of C_i^m. In particular, the ramification index at $\mathfrak{P}$ of such a specialization is n. Hence, $F/k(T)$ is strongly L-parametric. Conversely, assume $F/k(T)$ is strongly L-parametric. Let n be an element order in G. By the above characterization,

$FL/L(T)$ has a specialization of ramification index n at $\mathfrak{P}$. Then, by the Specialization Inertia Theorem, the inertia canonical invariant of $F/k(T)$ contains the conjugacy class of an element of G of order divisible by n. Hence, $(*)$ holds. □

Proof of Proposition 4.5. By Riemann's existence theorem, there is $F/k(T) \in \mathsf{R}_G(k(T))$ whose inertia canonical invariant contains the conjugacy class of every element of $G \setminus \{1\}$. In particular, $F/k(T)$ fulfills Condition $(*)$ of Lemma 4.6. Hence, $F/k(T)$ is strongly L-parametric, for $K \supseteq k$ algebraically closed and $L = K((V))$, and, given $E/L \in \mathsf{R}_{\leq G}(L)$, there are infinitely many $t_0 \in \mathbb{P}^1(L)$ with $E = (FL)_{t_0}$. Finally, if G is neither cyclic nor dihedral of order $2n$ with $n \geq 3$ odd, $F/k(T)$ is not $L(U)$-parametric by Theorem 3.1 and the subsequent paragraph. □

Remark 4.7. Using Lemma 2.3 yields this polynomial analog of Proposition 4.5:
Let k be algebraically closed of characteristic 0 and G a finite group. There is a monic separable polynomial $P(T,Y) \in k[T][Y]$ of group G such that, for $K \supseteq k$ algebraically closed and $L = K((V))$, the polynomial $P(T,Y)$ is strongly L-parametric. Furthermore, if G is neither cyclic nor dihedral of order $2n$ with $n \geq 3$ odd, then $P(T,Y)$ is not $L(U)$-parametric.

5. Polynomials with more variables

We conclude with several remarks on polynomials with more than one variable. The first one compares a single parametric polynomial with a finite "parametric set".

Remark 5.1. As already used in the proof of Lemma 2.4, it is well-known that, over infinite fields, using more than one polynomial is redundant in the setup of generic polynomials. Namely, suppose $P_1(T_1,\dots,T_n,Y),\dots,\ P_r(T_1,\dots,T_n,Y) \in k[T_1,\dots,T_n][Y]$ are finitely many monic separable polynomials of group G over $k(T_1,\dots,T_n)$ fulfilling this: for every overfield $L \supseteq k$ and every $E/L \in \mathsf{R}_G(L)$, there are $i \in \{1,\dots,r\}$ and $(t_1,\dots,t_n) \in L^n$ such that E is the splitting field over L of $P_i(t_1,\dots,t_n,Y)$. By [15, Corollary 1.1.6], it follows that at least one of the polynomials $P_i(T_1,\dots,T_n,Y)$ has to be generic itself.

On the other hand, the analogous property for parametric polynomials fails in general, e.g., for $G = \mathbb{Z}/8\mathbb{Z}$ and $k = \mathbb{Q}(\sqrt{17})$. Namely, there exist $n \geq 1$ and finitely many monic separable polynomials $P_1(T_1,\dots,T_n,Y),\dots,P_r(T_1,\dots,T_n,Y) \in k[T_1,\dots,T_n][Y]$ of group G over $k(T_1,\dots,T_n)$ fulfilling this: for every $E/k \in \mathsf{R}_G(k)$, there are $i \in \{1,\dots,r\}$ and $(t_1,\dots,t_n) \in k^n$ such that E is the splitting field over k of $P_i(t_1,\dots,t_n,Y)$ (see [25, Theorems 3.3 and 4.2]).[5] Such a set is called a *finite k-parametric set of polynomials for G*. However, there exists no k-parametric polynomial $P(T_1,\dots,T_n,Y) \in k[T_1,\dots,T_n][Y]$ of group G over $k(T_1,\dots,T_n)$, for any number of variables n (see [20, Remark A.2]).

Our second remark suggests a notion of "parametric dimension" measuring the complexity of all the Galois extensions of a given field with any given finite Galois group.

Remark 5.2. Recall that the *generic dimension* of a finite group G over a field k, denoted by $\mathrm{gd}_k G$, is either the smallest $n \geq 1$ such that there is a generic polynomial $P(T_1,\dots,T_n,Y) \in k[T_1,\dots,T_n][Y]$ of group G, or ∞ if there is no generic polynomial of group G with coefficients in k (see [15, §8.5]). In view of Remark 5.1, for the analogous notion of parametric dimension, we allow finite k-parametric sets of polynomials. Define the *(generalized) parametric dimension* of G over k, denoted by $\mathrm{pd}_k G$, to be either the smallest $n \geq 1$ for

[5] By the proof of [25, Theorem 4.2], one can actually take $n = 5$.

which there exists a finite k-parametric set of polynomials in $k[T_1,\dots,T_n][Y]$ for G, or ∞ if there is no such set.[6]

Clearly, $\mathrm{pd}_k G \le \mathrm{gd}_k G$, and it may happen that equality does not hold. For example, if k is PAC (the definition is recalled in §1), we always have $\mathrm{pd}_k G = 1$ (while $\mathrm{gd}_k G \ge 2$ for many groups G; see [15, Proposition 8.2.4] and [3]), by [5] and the fact that the answer to the regular inverse Galois problem over PAC fields is positive (see [28, Main Theorem A]). A family of non-PAC examples is given by Remark 4.7: if k is algebraically closed of characteristic 0, then we always have $\mathrm{pd}_{k((V))} G = 1$.

Finally, let us recall the following definition (see [1,15]):

Definition 5.3. Let k be a field.
(1) Let M/L be a finite separable field extension with $k \subseteq L$. If, for an intermediate field $k \subseteq L' \subseteq L$, there is a field extension M' of L' contained in M, and with $[M' : L'] = [M : L]$ and $M = M'L$, we say that M/L is *defined* over L'. Moreover, the *essential dimension* of M/L over k is the minimum of the transcendence degree of L'/k, when L' runs through all intermediate fields over which M/L is defined.
(2) Let G be a finite group, acting regularly on a set $\mathbf{T} = \{T_1,\dots,T_{|G|}\}$ of indeterminates. Then the *essential dimension* $\mathrm{ed}_k G$ of G over k is the essential dimension of $k(\mathbf{T})/k(\mathbf{T})^G$ over k.

Note that $\mathrm{ed}_k G \le \mathrm{gd}_k G$ and, when $\mathrm{gd}_k G$ is finite, it is conjectured that $\mathrm{ed}_k G = \mathrm{gd}_k G$ (see [15, §8.5]). However, the following known example (see [27, Theorem 3.4]) shows that $\mathrm{pd}_k G$ may be strictly smaller even than $\mathrm{ed}_k G$ (with k a number field).

Example 5.4. Let $k = \mathbb{Q}(\sqrt{-1})$, $G = (\mathbb{Z}/2\mathbb{Z})^5$, and consider the three polynomials $P_i(T_1,T_2,T_3,T_4,Y) = (Y^2 - T_1 - \dots - T_i)\prod_{i=1}^4 (Y^2 - T_i)$, $i = 2,3,4$, over $k(T_1,T_2,T_3,T_4)$. We claim that $\{P_2,P_3,P_4\}$ is a finite k-parametric set for G, and hence $\mathrm{pd}_k G \le 4 < 5 = \mathrm{ed}_k G$ (see, e.g., [15, Theorem 8.2.11] for the last equality).

To show the claim, note that any Galois extension E of k of group G is of the form $E = k(\sqrt{t_1},\dots,\sqrt{t_5})$ for some $t_i \in k^\times$, $i = 1,\dots,5$. Then, by the Hasse–Minkowski theorem (see [21, Chapter VI, Corollary 3.5]), and as k is totally imaginary, there is $(a_1,\dots,a_4) \in k^4$ such that $t_5 = \sum_{j=1}^4 t_j a_j^2$ (up to reordering the t_i's). Rearrange the values of t_j, so that $a_j \ne 0$ for $j \le i$, and $a_j = 0$ for $j > i$, for some $2 \le i \le 4$ (note that $i = 1$ is impossible as $[k(\sqrt{t_1},\sqrt{t_5}) : k] = 4$). The splitting field of $P_i(s_1,\dots,s_4,Y)$ over k, where $s_j = t_j a_j^2$ for $j \le i$ and $s_j = t_j$ for $j > i$, is then E, as desired.

Ongoing research will investigate further the connection between generic, essential, and parametric dimensions.

References

[1] Joe P. Buhler, Zinovy Reichstein, On the essential dimension of a finite group, Compos. Math. 106 (2) (1997) 159–179.
[2] Lior Bary-Soroker, Arno Fehm, Open problems in the theory of ample fields, in: Geometric and Differential Galois Theories, in: Sémin. Congr., vol. 27, Soc. Math. France, Paris, 2013, pp. 1–11.
[3] Huah Chu, Shou-Jen Hu, Ming-Chang Kang, Jiping Zhang, Groups with essential dimension one, Asian J. Math. 12 (2) (2008) 177–191.
[4] Tim Dokchitser, Vladimir Dokchitser, Elliptic curves with all quadratic twists of positive rank, Acta Arith. 137 (2) (2009) 193–197.
[5] Pierre Dèbes, Galois covers with prescribed fibers: the Beckmann–Black problem, Ann. Sc. Norm. Super. Pisa, Cl. Sci. (4) 28 (2) (1999) 273–286.
[6] Pierre Dèbes, Groups with no parametric Galois realizations, Ann. Sci. Éc. Norm. Supér. (4) 51 (1) (2018) 143–179.
[7] Frank R. DeMeyer, Generic polynomials, J. Algebra 84 (2) (1983) 441–448.

[6] Note that the splitting fields of the given polynomials have Galois group G over the rational function field $k(T_1,\dots,T_n)$, as opposed to the definition of "essential parametric dimension" in [20], which allows extensions of arbitrary function fields.

[8] Pierre Dèbes, Joachim König, François Legrand, Danny Neftin, Rational pullbacks of Galois covers, to appear in Mathematische Zeitschrift, arXiv:1807.01937v3.
[9] Harold Davenport, Donald John Lewis, Andrzej Schinzel, Quadratic Diophantine equations with a parameter, Acta Arith. 11 (1965/1966) 353–358.
[10] Michael D. Fried, Moshe Jarden, Field Arithmetic, third edition, 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), vol. 11, Springer-Verlag, Berlin, 2008, xxiv+792 pp. Revised by Jarden.
[11] Michael D. Fried, Fields of definition of function fields and Hurwitz families-groups as Galois groups, Commun. Algebra 5 (1) (1977) 17–82.
[12] David Harbater, Julia Hartmann, Daniel Krashen, Patching subfields of division algebras, Trans. Am. Math. Soc. 363 (6) (2011) 3335–3349.
[13] David Harbater, Julia Hartmann, Danny Krashen, Weierstrass preparation and algebraic invariants, Math. Ann. 356 (4) (2013) 1405–1424.
[14] Moshe Jarden, Algebraic Patching, Springer Monographs in Mathematics, Springer, Heidelberg, 2011, xxiv+290 pp.
[15] Christian U. Jensen, Arne Ledet, Noriko Yui, Generic Polynomials. Constructive Aspects of the Inverse Galois Problem, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, 2002, x+258 pp.
[16] Camille Jordan, Recherches sur les substitutions, J. Liouville 17 (1872) 351–367.
[17] Gregor Kemper, Generic polynomials are descent-generic, Manuscr. Math. 105 (1) (2001) 139–141.
[18] Joachim König, François Legrand, Non-parametric sets of regular realizations over number fields, J. Algebra 497 (2018) 302–336.
[19] Joachim König, François Legrand, Danny Neftin, On the local behavior of specializations of function field extensions, Int. Math. Res. Not. 2019 (9) (2019) 2951–2980.
[20] Joachim König, Danny Neftin, The local dimension of a finite group over a number field, Manuscript, 2020, arXiv: 2007.05383.
[21] Tsit Yuen Lam, Introduction to Quadratic Forms over Fields, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005, xxii+550 pp.
[22] Serge Lang, Algebra, revised third edition, Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002, xvi+914 pp.
[23] François Legrand, Specialization results and ramification conditions, Isr. J. Math. 214 (2) (2016) 621–650.
[24] Wan Lee, Myungjun Yu, On elliptic curves with complex multiplication and root numbers, to appear in Int. J. Number Theory, https://doi.org/10.1142/S179304212150010X.
[25] Dominique Martinais, Leila Schneps, A complete parametrization of cyclic field extensions of 2-power degree, Manuscr. Math. 80 (2) (1993) 181–197.
[26] Loren D. Olson, Points of finite order on elliptic curves with complex multiplication, Manuscr. Math. 14 (1974) 195–205.
[27] Catherine O'Neil, Sampling spaces and arithmetic dimension, in: Number Theory, Analysis and Geometry, Springer, New York, 2012, pp. 499–518.
[28] Florian Pop, Embedding problems over large fields, Ann. Math. (2) 144 (1) (1996) 1–34.
[29] Florian Pop, Little survey on large fields - old & new, in: Valuation Theory in Interaction, in: EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2014, pp. 432–463.
[30] Cristian Popescu, Karl Rubin, Alice Silverberg (Eds.), Arithmetic of L-Functions. Lectures from the Graduate Summer, School Held in Park City, UT, June 29–July 17, 2009, IAS/Park City Mathematics Series, vol. 18, American Mathematical Society/Institute for Advanced Study (IAS), Providence, RI/Princeton, NJ, 2011, xiv+499 pp.
[31] Andrzej Schinzel, Selected Topics on Polynomials, University of Michigan Press, Ann Arbor, Mich., 1982, xxi+250 pp.
[32] Leila Schneps, On cyclic field extensions of degree 8, Math. Scand. 71 (1) (1992) 24–30.
[33] Andrzej Schinzel, Polynomials with Special Regard to Reducibility, Encyclopedia of Mathematics and Its Applications, vol. 77, Cambridge University Press, Cambridge, 2000, x+558 pp. With an appendix by Umberto Zannier.
[34] Jean-Pierre Serre, Topics in Galois Theory, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, xvi+117 pp. Lecture notes prepared by Henri Darmon. With a foreword by Darmon and the author.
[35] Joseph H. Silverman, The Arithmetic of Elliptic Curves, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, xx+513 pp.
[36] Helmut Völklein, Groups as Galois Groups. An Introduction, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, xviii+248 pp.