GALOIS GROUPS OVER RATIONAL FUNCTION FIELDS AND EXPLICIT HILBERT IRREDUCIBILITY

DAVID KRUMM AND NICOLE SUTHERLAND

Abstract. Let $P \in \mathbb{Q}[t,x]$ be a polynomial in two variables with rational coefficients, and let G be the Galois group of P over the field $\mathbb{Q}(t)$. It follows from Hilbert's Irreducibility Theorem that for most rational numbers c the specialized polynomial $P(c,x)$ has Galois group isomorphic to G and factors in the same way as P. In this paper we discuss methods for computing the group G and obtaining an explicit description of the exceptional numbers c, i.e., those for which $P(c,x)$ has Galois group different from G or factors differently from P. To illustrate the methods we determine the exceptional specializations of three sample polynomials. In addition, we apply our techniques to prove a new result in arithmetic dynamics.

1. Introduction

Let $P \in \mathbb{Q}[t,x]$ be nonconstant in the variable x, and let G be the Galois group of P over the function field $\mathbb{Q}(t)$. For any rational number c we may consider the polynomial $P_c = P(c,x) \in \mathbb{Q}[x]$ and its Galois group, which we denote by G_c. Hilbert's Irreducibility Theorem (henceforth abbreviated HIT) implies that as c varies in $\mathbb{Q}$, most specializations P_c have Galois group isomorphic to G and factor in the same way as P. However, there may exist rational numbers c such that G_c is not isomorphic to G or P_c factors differently from P; we will call the set of all such numbers the *exceptional set* of P, denoted $\mathcal{E}(P)$. The main purpose of this article is to develop a method for obtaining an explicit description of the set $\mathcal{E}(P)$.

A standard step in the proof of HIT is to show that there exist a finite set $D \subset \mathbb{Q}$ and algebraic curves $C_1, \dots, C_r$ having the following property: for $c \in \mathbb{Q} \smallsetminus D$, c belongs to the set $\mathcal{E}(P)$ if and only if c is a coordinate of a rational point on one of the curves C_i. Our method for explicitly describing the exceptional set of P is based on a constructive proof of this result, which we summarize in the following theorem.

Theorem (see 2.7)**.** *Let $\Delta(t)$ and $\ell(t)$ be the discriminant and leading coefficient of P, respectively. Let $M_1, \dots, M_r$ be representatives of all the conjugacy classes of maximal subgroups of G. For $i = 1, \dots, r$, let F_i be the fixed field of M_i and let $f_i(t,x)$ be a monic irreducible polynomial in $\mathbb{Q}[t][x]$ such*

2010 *Mathematics Subject Classification.* 11R32, 11R09.

Key words and phrases. Hilbert Irreducibility Theorem, Galois groups, Function fields.

that $F_i/\mathbb{Q}(t)$ is generated by a root of $f_i(t,x)$. Suppose that $c \in \mathbb{Q}$ satisfies

$$\Delta(c) \cdot \ell(c) \cdot \prod_{i=1}^{r} \operatorname{disc} f_i(c,x) \neq 0. \tag{1.1}$$

Then $c \in \mathcal{E}(P) \iff$ there is an index i such that $f_i(c,x)$ has a root in $\mathbb{Q}$.

It should be noted that versions of this theorem can be found in the literature; see, for instance, [5, §3.1]. However, we are not aware of any reference proving the result for reducible polynomials P, or explicitly identifying a finite set that needs to be excluded, as in (1.1).

It follows from the theorem that we may take D to be the set of all $c \in \mathbb{Q}$ for which (1.1) does not hold, and we may take C_i to be the plane curve defined by the equation $f_i(t,x) = 0$. The problem of explicitly describing the set $\mathcal{E}(P)$ can therefore be reduced to the following:

(1) Compute the polynomials f_i, and
(2) Determine all the rational points on the curves C_i.

At present there is no hope of an algorithmic solution to the problem of determining the set of rational points on an algebraic curve, though there are several techniques available for approaching the problem on an *ad hoc* basis. A survey of current methods may be found in [25]. We give in §4 a few relatively simple examples using some of these methods; more sophisticated examples can be found in the articles [21] and [9].

In contrast to step (2) above, all of the computational tools needed for the first step are currently available. To achieve step (1), one must begin by computing a permutation representation of the Galois group G; this can be done using methods of Fieker and Klüners [8]. Though these authors mainly discuss the case of irreducible polynomials over $\mathbb{Q}$, their methods can be extended to work more generally. For instance, Fieker [6] adapted the algorithm to compute Galois groups of irreducible polynomials over $\mathbb{Q}(t)$. In the present paper we discuss the modifications needed for Fieker's implementation and we further extend the method so that it applies to reducible polynomials over $\mathbb{Q}(t)$. This generalized algorithm for computing Galois groups over $\mathbb{Q}(t)$ has been implemented by the second author and is included in Magma V2.24 [3].

Once the group G has been computed, its maximal subgroups can be obtained using an algorithm of Cannon and Holt [4]. Finally, the fixed field of any subgroup of G can be computed using known methods; see [14, §3.3] and our discussion in §3.3. Hence, given the polynomial P it is possible to compute defining equations for the curves C_i. Functionality for this computation is available in Magma via the intrinsic `HilbertIrreducibilityCurves`.

In summary, by using currently available methods in computational group theory and Galois theory, and by applying techniques for determining rational points on curves, it is possible in many cases to obtain a complete characterization of the exceptional set of a given polynomial $P \in \mathbb{Q}[t,x]$.

This article is organized as follows. We devote §2 to the proof of the above theorem, and §3 to a discussion of the algorithms for computing Galois groups and fixed fields over $\mathbb{Q}(t)$. In order to illustrate the process described earlier, we include three examples in §4.

The first example concerns the polynomial $P(t,x) = x^6 + t^6 - 1$, which has a finite exceptional set. The case $n = 3$ of Fermat's Last Theorem implies that the only rational numbers c for which P_c has a rational root are 0 and ± 1. We prove that in fact 0 and ± 1 are the only rational numbers for which P_c is reducible.

In the second example we consider the polynomial $P(t,x) = x^6 - 4x^2 - t^2$, which is irreducible and has Galois group isomorphic to the symmetric group S_4. Our analysis will show that, in addition to the obvious reducible specialization P_0, there is an infinite family of reducible specializations. More precisely, we prove that for $c \neq 0$,

$$P_c \text{ is reducible if and only if } c = \frac{v^4 + 16}{8v} \text{ for some } v \in \mathbb{Q}.$$

Moreover, when c has the above form we show that P_c factors as a product of two irreducible cubic polynomials.

The third example relates to the polynomial $P(t,x) = 3x^4 - 4x^3 + 1 + 3t^2$, which is one polynomial in a family discussed by Serre [22, §4.5]. The Galois group of P is isomorphic to the alternating group A_4, so a typical specialization P_c will have Galois group $G_c \cong A_4$. However, there are infinitely many exceptions to this: we prove that

$$G_c \ncong A_4 \iff c = \frac{v^3 - 9v}{9(1 - v^2)} \text{ for some } v \in \mathbb{Q}.$$

Furthermore, for numbers c of the above form, we determine precisely which groups G_c arise as v varies. We show in particular that the groups $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ and $\mathbb{Z}/2\mathbb{Z}$ arise for infinitely many such numbers c.

In addition to these detailed examples with polynomials P of small degree, we briefly discuss two additional examples with polynomials of degrees 12 and 30.

In §5 we apply our methods to prove a new result in arithmetic dynamics. Let $\phi(z) \in \mathbb{Q}(z)$ be a rational function, and for $n \geq 1$ let ϕ^n denote the n-fold composition of ϕ with itself. We say that a rational number x is *periodic* for ϕ if there exists $n \geq 1$ such that $\phi^n(x) = x$; in that case, the least such n is called the *period* of x. An important open problem in arithmetic dynamics is a uniform boundedness conjecture of Morton and Silverman [18] which in particular would imply the following: there exists a constant M such that for every rational function $\phi(z)$ of degree 2 and every period $n > M$, ϕ has no rational point of period n. This conjecture has been refined in various special cases. For example, Poonen [21] studied the family of maps of the form $\phi(z) = z^2 + c$ and Manes [19] studied maps of the form $\phi(z) = kz + b/z$. Manes conjectures that no such map can have a rational point of period

$n > 4$, and shows that there exist at most finitely many such maps having a rational point of period 5. We prove the following stronger statement: for all but finitely many maps of the form $\phi(z) = kz + b/z$, there exists a positive proportion of prime numbers p such that $\phi(z)$ does not have a point of period 5 in the p-adic field $\mathbb{Q}_p$.

2. An explicit form of HIT

Let k be a field of characteristic 0 and let $P(t,x) \in k[t,x]$ be a polynomial of degree $n \geq 1$ in the variable x. We will henceforth regard P as an element of the ring $k(t)[x]$ and assume that P is separable. We define the *factorization type* of P, denoted $\mathcal{F}(P)$, to be the multiset consisting of the degrees of the irreducible factors of P.

Let $N/k(t)$ be a splitting field of P and let $G = \mathrm{Gal}(N/k(t))$ be the Galois group of P. We assume that G is nontrivial. For every element $c \in k$, let P_c denote the specialized polynomial $P(c,x) \in k[x]$. The Galois group and factorization type of P_c will be denoted by G_c and $\mathcal{F}(P_c)$, respectively.

It follows from HIT that there is a thin[1] subset of k outside of which we have $\mathcal{F}(P_c) = \mathcal{F}(P)$ and $G_c \cong G$. We define the *exceptional set* of P, denoted $\mathcal{E}(P)$, to be the set of all elements $c \in k$ for which either one of these conditions fails to hold:

$$\mathcal{E}(P) = \{c \in k \mid \mathcal{F}(P_c) \neq \mathcal{F}(P) \text{ or } G_c \not\cong G\}.$$

Our aim in this section is to prove a version of HIT from which one can deduce a method for explicitly describing the set $\mathcal{E}(P)$; our main result in this direction is Theorem 2.7 below.

It should be noted that the expert will be familiar with several of the results proved in this section. However, we have included complete proofs of most statements due to the lack of a reference treating this subject at the desired level of generality, in particular allowing the polynomial P to be reducible.

Let $\Delta(t)$ and $\ell(t)$ be the discriminant and leading coefficient of P, respectively, and let $A \subset k(t)$ be the ring

$$A = k[t]\left[\ell(t)^{-1}\right], \tag{2.1}$$

i.e., the localization of $k[t]$ by the multiplicative set generated by $\ell(t)$.

For every intermediate field F between $k(t)$ and N, let $\mathcal{O}_F$ denote the integral closure of A in F. Note that $\mathcal{O}_F/A$ is an extension of Dedekind domains with A being a PID. By a *prime* of F (or of $\mathcal{O}_F$) we mean a maximal ideal of $\mathcal{O}_F$. If $\mathfrak{p}$ is a prime of A and $\mathfrak{q}$ is a prime of $\mathcal{O}_F$, we denote by $\kappa(\mathfrak{q})$ and $\kappa(\mathfrak{p})$ the residue fields of $\mathfrak{q}$ and $\mathfrak{p}$, respectively. Thus,

$$\kappa(\mathfrak{q}) = \mathcal{O}_F/\mathfrak{q}, \quad \kappa(\mathfrak{p}) = A/\mathfrak{p}.$$

If $\mathfrak{q}$ divides $\mathfrak{p}\mathcal{O}_F$, we denote the ramification index and residual degree of $\mathfrak{q}$ over $\mathfrak{p}$ by $e(\mathfrak{q}/\mathfrak{p})$ and $f(\mathfrak{q}/\mathfrak{p})$, respectively.

[1]See [22, §3.1] for a definition of thin sets.

For every prime $\mathfrak{P}$ of N, let $G_{\mathfrak{P}}$ be the decomposition group of $\mathfrak{P}$ over $k(t)$ and let $Z_{\mathfrak{P}}$ be the decomposition field of $\mathfrak{P}$, i.e., the fixed field of $G_{\mathfrak{P}}$. We refer the reader to [20, Chap. I, §§8-9] for the standard material on decomposition groups and ramification used in this section.

If $c \in k$ is any element satisfying $\ell(c) \neq 0$, the evaluation homomorphism $k[t] \to k$ given by $a(t) \mapsto a(c)$ extends uniquely to a homomorphism $A \to k$. Let $\mathfrak{p}_c$ be the kernel of this map. We will henceforth identify the residue field $\kappa(\mathfrak{p}_c)$ with k via the map $a(t) \bmod \mathfrak{p}_c \mapsto a(c)$. Note that with this identification, if $f(t,x) \in A[x]$ is an arbitrary polynomial, then upon reducing the coefficients of f modulo $\mathfrak{p}_c$ we obtain the specialized polynomial $f(c,x) \in k[x]$.

It will be necessary for our purposes in this section to be able to determine how the prime $\mathfrak{p}_c$ factors in any intermediate field F between $k(t)$ and N. Recall that by a well-known theorem of Dedekind and Kummer, for all but finitely many primes $\mathfrak{p}$ of A, the factorization of $\mathfrak{p}$ in F can be determined by choosing an integral primitive element θ of $F/k(t)$ and factoring its minimal polynomial modulo $\mathfrak{p}$. The finite set of primes that need to be excluded are those that are not relatively prime to the conductor of the ring $A[\theta]$; see [20, p. 47, Prop. 8.3] for details. The following lemma provides sufficient conditions on $c \in k$ so that $\mathfrak{p}_c$ will be relatively prime to this conductor, and therefore the Dedekind–Kummer criterion can be applied to $\mathfrak{p}_c$.

Lemma 2.1. *Let F be an intermediate field between $k(t)$ and N with primitive element $\theta \in \mathcal{O}_F$ having minimal polynomial $f(t,x) \in A[x]$. Let*

$$\mathfrak{F} = \{\alpha \in \mathcal{O}_F \mid \alpha \cdot \mathcal{O}_F \subseteq A[\theta]\}$$

be the conductor of the ring $A[\theta]$. Suppose that $c \in k$ satisfies

$$\ell(c) \cdot \operatorname{disc} f(c,x) \neq 0.$$

Then $\mathfrak{p}_c\mathcal{O}_F$ is relatively prime to $\mathfrak{F}$. Furthermore, $\mathfrak{p}_c$ is unramified in F.

Proof. Let $\delta \in A$ be the discriminant of f. By a linear algebra argument (see Lemma 2.9 in [20, p. 12]) we have $\delta \cdot \mathcal{O}_F \subseteq A[\theta]$ and therefore $\delta \in \mathfrak{F}$. Suppose that $\mathfrak{q}$ is a prime of F dividing both $\mathfrak{F}$ and $\mathfrak{p}_c\mathcal{O}_F$. Since $\mathfrak{F} \subseteq \mathfrak{q}$ we have $\delta \in \mathfrak{q}$, so $\delta \in \mathfrak{q} \cap A = \mathfrak{p}_c$. By definition of $\mathfrak{p}_c$ this implies that $\operatorname{disc} f(c,x) = \delta(c) = 0$, which is a contradiction. Therefore $\mathfrak{p}_c$ must be relatively prime to $\mathfrak{F}$.

The Dedekind–Kummer theorem now allows us to relate the factorization of $\mathfrak{p}_c$ in F to the factorization of $f(c,x)$ in $k[x]$. In particular, the theorem implies that if $\mathfrak{p}_c$ is ramified in F, then $f(c,x)$ has a repeated irreducible factor, which contradicts our assumption that $\operatorname{disc} f(c,x) \neq 0$. Therefore $\mathfrak{p}_c$ must be unramified in F. □

Lemma 2.2. *Suppose that $c \in k$ satisfies $\Delta(c) \cdot \ell(c) \neq 0$. Then the prime $\mathfrak{p}_c$ is unramified in N.*

Proof. Since N is the compositum of the fields $k(t)(\theta)$ as θ ranges over all the roots of P in N, it suffices to show that $\mathfrak{p}_c$ is unramified in every such field. (See [17, p. 119, Cor. 8.7].) Thus, let $\theta \in \mathcal{O}_N$ be any root of P and

let $F = k(t)(\theta)$. Let $Q \in k[t][x]$ be an irreducible factor of P having θ as a root. Dividing Q by its leading coefficient we obtain a monic irreducible polynomial $f \in A[x]$ having θ as a root; it follows that f is the minimal polynomial of θ over $k(t)$. Let $\delta \in A$ be the discriminant of f. Since f divides P in $A[x]$, δ divides Δ in A. Hence, the hypothesis that $\Delta(c) \neq 0$ implies that $\delta(c) \neq 0$. By Lemma 2.1, $\mathfrak{p}_c$ is unramified in F. □

We recall the notion of an isomorphism of group actions. If $\mathcal{G}$ and $\mathcal{H}$ are groups acting on sets X and Y, respectively, then we say that there is an isomorphism of group actions between $\mathcal{G}$ and $\mathcal{H}$ if there exist an isomorphism $\phi : \mathcal{G} \to \mathcal{H}$ and a bijection $\sigma : X \to Y$ such that $\sigma(g \cdot x) = \phi(g) \cdot \sigma(x)$ for all $g \in \mathcal{G}$ and all $x \in X$.

Proposition 2.3. *Suppose that $c \in k$ satisfies $\Delta(c) \cdot \ell(c) \neq 0$, and let $\mathfrak{P}$ be a prime of N dividing $\mathfrak{p}_c$. Then there is an isomorphism of group actions $G_{\mathfrak{P}} \cong G_c$, where $G_{\mathfrak{P}}$ acts on the roots of P and G_c acts on the roots of P_c.*

Proof. For every element $a \in \mathcal{O}_N$ let $\bar{a}$ denote the image of a under the quotient map $\mathcal{O}_N \to \kappa(\mathfrak{P})$. Recall that the extension $\kappa(\mathfrak{P})/k$ is Galois and that there is a surjective homomorphism $G_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/k)$ given by $\sigma \mapsto \bar{\sigma}$, where $\bar{\sigma}(\bar{a}) = \overline{\sigma(a)}$ for every $a \in \mathcal{O}_N$. Furthermore, since $\mathfrak{p}_c$ is unramified in N by Lemma 2.2, this map is an isomorphism. We claim that $\kappa(\mathfrak{P})$ is a splitting field for P_c.

Note that if $\alpha \in \mathcal{O}_N$ is a root of P, then $\bar{\alpha} \in \kappa(\mathfrak{P})$ is a root of P_c. Moreover, if α and β are distinct roots of P, then $\bar{\alpha} \neq \bar{\beta}$; indeed, this follows from the fact that $\bar{\Delta} = \Delta(c) \neq 0$. Thus, reduction modulo $\mathfrak{P}$ is an injective map from the set of roots of P to the set of roots of P_c.

Let $x_1, \ldots, x_n \in \mathcal{O}_N$ be the roots of P in N, and let $S = k(\bar{x}_1, \ldots, \bar{x}_n)$. Clearly S is a splitting field for P_c, and $k \subseteq S \subseteq \kappa(\mathfrak{P})$. We will prove that $S = \kappa(\mathfrak{P})$ by showing that the group $\mathrm{Gal}(\kappa(\mathfrak{P})/S)$ is trivial. Let $\tau \in \mathrm{Gal}(\kappa(\mathfrak{P})/S)$ and let $\sigma \in G_{\mathfrak{P}}$ be the element such that $\bar{\sigma} = \tau$. Since τ is the identity map on S, we have $\tau(\bar{x}_i) = \bar{x}_i$ for every index i, and hence $\overline{\sigma(x_i)} = \bar{x}_i$ for all i. Since $\sigma(x_i)$ and x_i are roots of P, this implies that $\sigma(x_i) = x_i$. Thus, σ fixes every root of P, so σ is the identity element of $G_{\mathfrak{P}}$. Hence $\tau = \bar{\sigma}$ is the identity element of $\mathrm{Gal}(\kappa(\mathfrak{P})/S)$. This proves that $\mathrm{Gal}(\kappa(\mathfrak{P})/S)$ is trivial and therefore $\kappa(\mathfrak{P}) = S$ is a splitting field for P_c.

The map $\sigma \mapsto \bar{\sigma}$ is thus an isomorphism $G_{\mathfrak{P}} \to G_c$. Moreover, the fact that $\sigma(x_i) = x_j \iff \bar{\sigma}(\bar{x}_i) = \bar{x}_j$ implies that the actions of $G_{\mathfrak{P}}$ and G_c are isomorphic. □

Remark 2.4. In the case where the polynomial P is irreducible, Proposition 2.3 follows from Theorem 2.9 in [16, Chap. VII, §2].

Lemma 2.5. *Let $\mathfrak{p}$ be a prime of A and let $\mathfrak{P}$ be a prime of N dividing $\mathfrak{p}$. Then the following hold:*

(1) Setting $\mathfrak{Q} = \mathfrak{P} \cap Z_{\mathfrak{P}}$, we have $e(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{p}) = 1$.

(2) *Let F be an intermediate field between $k(t)$ and N, and let $\mathfrak{q} = \mathfrak{P} \cap F$. If $e(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}) = 1$, then $F \subseteq Z_{\mathfrak{P}}$.*

Proof. See [20, p. 55, Prop. 9.3] and [17, p. 118, Prop. 8.6]. □

Proposition 2.6. *Let F be an intermediate field between $k(t)$ and N. Let $\theta \in \mathcal{O}_F$ be a primitive element for $F/k(t)$ and let $f(t,x) \in A[x]$ be its minimal polynomial. Suppose that $c \in k$ satisfies*

$$\Delta(c) \cdot \ell(c) \cdot \operatorname{disc} f(c,x) \neq 0.$$

Then the following are equivalent:

(1) *The polynomial $f(c,x)$ has a root in k.*
(2) *There exists a prime $\mathfrak{q}$ of F dividing $\mathfrak{p}_c$ such that $f(\mathfrak{q}/\mathfrak{p}_c) = 1$.*
(3) *There exists a prime $\mathfrak{P}$ of N dividing $\mathfrak{p}_c$ such that $F \subseteq Z_{\mathfrak{P}}$.*
(4) *There exists a prime $\mathfrak{P}$ of N dividing $\mathfrak{p}_c$ such that $G_{\mathfrak{P}} \subseteq \operatorname{Gal}(N/F)$.*

Proof. By Lemma 2.1, $\mathfrak{p}_c$ is relatively prime to the conductor of $A[\theta]$. The Dedekind–Kummer theorem then implies that the degrees of the irreducible factors of $f(c,x)$ in $k[x]$ correspond to the residual degrees $f(\mathfrak{q}/\mathfrak{p}_c)$ for primes $\mathfrak{q}$ of F dividing $\mathfrak{p}_c$. The equivalence of (1) and (2) follows immediately.

We now show that (2) and (3) are equivalent. Suppose that (2) holds, and let $\mathfrak{P}$ be a prime of N dividing $\mathfrak{q}$. By Lemma 2.2, $\mathfrak{p}_c$ is unramified in N and therefore unramified in F. Hence, $e(\mathfrak{q}/\mathfrak{p}_c) = 1$. By Lemma 2.5, $F \subseteq Z_{\mathfrak{P}}$. Thus, (3) holds.

Conversely, suppose that (3) holds. Let $\mathfrak{P}$ be a prime of N dividing $\mathfrak{p}_c$ such that $F \subseteq Z_{\mathfrak{P}}$. Let $\mathfrak{Q} = \mathfrak{P} \cap Z_{\mathfrak{P}}$ and $\mathfrak{q} = \mathfrak{P} \cap F$. Since $f(\mathfrak{Q}/\mathfrak{p}_c) = 1$ and $f(\mathfrak{q}/\mathfrak{p}_c)$ divides $f(\mathfrak{Q}/\mathfrak{p}_c)$, we have $f(\mathfrak{q}/\mathfrak{p}_c) = 1$. Thus, (2) holds.

The equivalence of (3) and (4) is clear. □

We can now prove the main result for this section.

Theorem 2.7. *Let $M_1, \dots, M_r$ be representatives of all the conjugacy classes of maximal subgroups of G. For $i = 1, \dots, r$ let F_i be the fixed field of M_i, and let $f_i(t,x)$ be a monic irreducible polynomial in $k[t][x]$ such that $F_i/k(t)$ is generated by a root of $f_i(t,x)$. Suppose that $c \in k$ satisfies*

$$\Delta(c) \cdot \ell(c) \cdot \prod_{i=1}^{r} \operatorname{disc} f_i(c,x) \neq 0. \tag{2.2}$$

Then the following hold:

(1) *If $\mathcal{F}(P_c) \neq \mathcal{F}(P)$, then $G_c \not\cong G$.*
(2) *$G_c \not\cong G \iff$ there is an index i such that $f_i(c,x)$ has a root in k.*

Proof. We prove (1) by contradiction. Thus, suppose that $\mathcal{F}(P_c) \neq \mathcal{F}(P)$ and $G_c \cong G$. By Proposition 2.3, the latter condition implies that the group G acts on the roots of P in the same way that G_c acts on the corresponding roots of P_c. Since $\mathcal{F}(P_c) \neq \mathcal{F}(P)$, there must be an irreducible factor $f \in k[t,x]$ of P such that f_c is reducible. Note that G acts transitively on

the roots of f, but since f_c is reducible and separable, G_c does not act transitively on its roots. Thus we have a contradiction, proving (1).

For the proof of (2), suppose that $G_c \not\leq G$ and let $\mathfrak{P}$ be a prime of N dividing $\mathfrak{p}_c$. By Proposition 2.3, the group $G_{\mathfrak{P}}$ is a proper subgroup of G. Replacing $\mathfrak{P}$ by a conjugate ideal if necessary, we may therefore assume that $G_{\mathfrak{P}} \subseteq M_i$ for some index i. By Proposition 2.6 applied to the field F_i, this implies that $f_i(c,x)$ has a root in k. This proves one direction of (2). The converse follows by a similar argument. □

2.1. **Resolvent polynomial interpretation.** Instead of relying exclusively on the concepts and methods of algebraic number theory, it is also possible to prove a version of Theorem 2.7 by using only Proposition 2.3 together with the theory of resolvent polynomials, a standard tool in modern methods for computing Galois groups. We recall here the basic definitions and facts needed for our purposes; for further details on this topic as well as proofs of the statements made here, we refer the reader to the articles [23] and [12].

Let n be a positive integer and let G and H be subgroups of the symmetric group S_n with $H \leq G$. The group S_n acts on the polynomial ring

$$\mathcal{R} := \mathbb{Z}[y_1, \dots, y_n]$$

by permuting the variables; for $p \in \mathcal{R}$ and $\sigma \in S_n$ we will write p^σ to denote the polynomial $p(y_{\sigma(1)}, \dots, y_{\sigma(n)})$. A polynomial $J \in \mathcal{R}$ is called a *G-relative H-invariant* if H is the stabilizer of J in G. In that case one associates to the triple (G, H, J) the *resolvent polynomial* $Q = Q_{G,H,J} \in \mathcal{R}[y]$ given by the formula

$$Q(y_1, \dots, y_n, y) := \prod_{\sigma \in G//H} (y - J^\sigma(y_1, \dots, y_n)),$$

where $G//H$ denotes a set of representatives for the left cosets σH in G/H.

Lemma 2.8 (Stauduhar [23])**.** *With notation as above, let K be a field of characteristic 0 and let $f \in K[x]$ be a separable polynomial of degree n. Regard $\mathrm{Gal}(f)$ as a subgroup of S_n by fixing an ordering $\alpha_1, \dots, \alpha_n$ of the roots of $f(x)$ in $\bar{K}$, and suppose that $\mathrm{Gal}(f)$ is contained in G. If J is any G-relative H-invariant and Q is the corresponding resolvent, then the polynomial $q(x) := Q(\alpha_1, \dots, \alpha_n, x)$ has coefficients in K. Moreover, if $q(x)$ is separable, then the following are equivalent:*

(1) There exists $\sigma \in G$ such that $\mathrm{Gal}(f) \subseteq \sigma^{-1} H \sigma$.
(2) The polynomial $q(x)$ has a root in K.

Returning now to the context of Theorem 2.7 (2), fix an ordering $x_1, \dots, x_n$ of the roots of $P(t,x)$ and embed the group $G = \mathrm{Gal}(P)$ into S_n using this ordering. Let $M_1, \dots, M_r$ be the maximal subgroups defined in Theorem 2.7; let $Q_i \in \mathcal{R}[y]$ be a resolvent polynomial corresponding to a G-relative M_i-invariant; and let $q_i(t,x) = Q_i(x_1, \dots, x_n, x)$. By Lemma 2.8 applied with $K = k(t)$ and $f = P$, the polynomials $q_i(t,x)$ have coefficients in $k(t)$;

and since q_i also has coefficients in $\mathbb{Z}[x_1, \ldots, x_n] \subseteq \mathcal{O}_N$, then $q_i \in A[x]$, where A is the ring defined in (2.1).

Suppose now that $c \in k$ satisfies $\ell(c) \neq 0$, so that the specialized polynomials P_c and $q_i(c, x)$ are well defined, and suppose that

$$\Delta(c) \cdot \prod_{i=1}^{r} \operatorname{disc} q_i(c, x) \neq 0.$$

By Proposition 2.3 and its proof, the chosen ordering of the roots of P induces an ordering $\bar{x}_1, \ldots, \bar{x}_n$ of the roots of P_c, and moreover, as subgroups of S_n we have $G_c \leq G$. Note that $q_i(c, x) = Q_i(\bar{x}_1, \ldots, \bar{x}_n, x)$.

Applying Lemma 2.8 once again, but now with $K = k$ and $f = P_c$, we conclude that G_c is contained in a conjugate of M_i if and only if $q_i(c, x)$ has a root in k. We thus obtain a variant of Theorem 2.7 in which the polynomials f_i of the theorem are replaced with the q_i defined here.

3. Computation of Galois groups over $\mathbb{Q}(t)$

We restrict now to the case $k = \mathbb{Q}$. It is clear from Theorem 2.7 that in order to better understand the exceptional set of a given polynomial $P \in \mathbb{Q}[t][x]$ it is necessary to compute the Galois group G, the maximal subgroups of G, and their corresponding fixed fields. In this section we discuss a Galois group and fixed field algorithm over $\mathbb{Q}(t)$, the particulars of which have not been previously discussed elsewhere.

3.1. **Galois groups of irreducible polynomials over $\mathbb{Q}(t)$.** The article [8] describes an algorithm to compute Galois groups of irreducible polynomials over $\mathbb{Q}$. As noted in [8] Section 7.7, this algorithm can be adjusted to compute Galois groups of polynomials over fields other than the rational field. For example, [26,27] discusses this for polynomials over global rational and algebraic function fields. An algorithm for computing Galois groups of polynomials over $\mathbb{Q}(t)$ has been implemented in [6] and included in Magma V2.15.

After providing, for ease of reference, a brief summary of the algorithm given in [26,27] Algorithms 1 and 11, respectively, we describe here some of the adjustments to this algorithm that are necessary for these computations over $\mathbb{Q}(t)$. We address these adjustments using the same headings as [26,27]. Algorithm 3.1 is a description of the algorithm of [8] which uses the descent method of Stauduhar [23] and has no degree restrictions.

Algorithm 3.1 (Compute the Galois group of a polynomial ([26] Algorithm 1, [27] Algorithm 11))**.**
Input: A polynomial f of degree n over $\mathbb{Q}[t]$.
Output: The Galois group of f.

(1) Compute a splitting field S_f for f over a completion of F and roots of f in S_f.
(2) Find a group $G \subseteq S_n$ which contains $\mathrm{Gal}(f)$
(3) While G has maximal subgroups which could contain $\mathrm{Gal}(f)$:

(a) For each maximal subgroup H of G, compute a G-relative H-invariant polynomial for a representative maximal subgroup H.
(b) For a cheap maximal subgroup H of G (Stauduhar)
  (i) Compute the precision m needed in the roots of f and the roots of f in S_f to precision m.
  (ii) For the representatives $\tau \in G//H$ of the right cosets of H in G: evaluate I_H^τ at the roots of f. Decide whether this is the image of an element of F in S_f. If so $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$ and restart the loop (3) with $G = \tau H \tau^{-1}$.
(4) Return G.

We now discuss how some of the steps of the above algorithm can be carried out in the case where f is irreducible.

Choosing a good prime: (Step 1). A good prime is necessary for computing a completion of $\mathbb{Q}(t)$ and a splitting field over this completion. The image of f must be squarefree over the residue field at P. Instead of the completion being a p-adic field (completion of the rationals) or a series field over the field of constants (completion of a global rational function field) we complete in two directions and compute a completion as a series field over a p-adic field. For this we need two primes, an integer prime for computing a p-adic field and a polynomial prime to compute a series field over this p-adic field.

The choice of a good polynomial prime can be undertaken in the same way as for the global function fields; see [26] Section 3.1 or [27] Section 8.1. In contrast to the global case we consider only n primes. Let r_P be the degree of P, d_P the LCM of the degrees of the factors of the image of f mapped over $\mathbb{Q}[x]/P$, and let $l_{f,P}$ be the number of factors of the image of f mapped over $\mathbb{Q}[x]/P$. Similar to the global case we choose P with the smallest $r_P d_P l_{f,P}^{1.5} > n/4$ if such occurs for a prime we have considered; otherwise a prime we have considered with largest $r_P d_P l_{f,P}^{1.5} \le n/4$.

To choose a good integer prime for the p-adic part of the completion we construct the number field $K = \mathbb{Q}[x]/P(x)$, where P is the prime polynomial chosen. We map f to a polynomial f_K over K and compute a prime p which is good for the computation of the Galois group of f_K, a polynomial over a number field. Lemma 2.16 of [11] contains some necessary conditions such primes must satisfy. As discussed in [26,27] Section 3.1 and 8.1, respectively, we choose the prime p so that the extension of the p-adic field is not of too large degree to be expensive to work in nor of too small degree that computations will require excessive precision,

Computing roots: (Step 1) We construct the field $\mathbb{Q}_p(\alpha)((z))$ which will contain all the roots of the image of f. This splitting field is a combination of the extension $\mathbb{Q}_p(\alpha)$ of a p-adic field used when computing Galois groups of polynomials over $\mathbb{Q}$ or a number field and the extension $\mathbb{F}_{(q^{r_P})^{d_P}}((z))$ used when computing Galois groups of polynomials over $\mathbb{F}_q(t)$ or an extension

thereof. The local field $\mathbb{Q}_p(\alpha)$ contains the roots of f_K mapped over the completion of K at p.

We take z as the image of P in $K((z))$ and use the map $h : \mathbb{Q}(t) \to K((z))$ given by the completion mapping at P into $K((z))$, and then combine with the mappings $K \to K_p \to K_p(\beta) = \mathbb{Q}_p(\alpha)$. To compute the roots of f we first compute the roots of f_K in $\mathbb{Q}_p(\alpha)$ to the required p-adic precision and Hensel lift to the required P-adic precision.

A starting group: (Step 2) Section 3.3 of [26, 27] applies also for polynomials over $\mathbb{Q}(t)$. Subfields over $\mathbb{Q}(t)$ can be computing using [13].

Invariants: (Step 3a) The invariants and Tschirnhausen transformations presented in [8] are sufficient as all rings involved here have characteristic 0.

Mapping back to the function field: (Step 3(b)ii) Given a series $g \in \mathbb{Q}_p(\alpha)((z))$ we check whether the coefficients of g map back to elements of K. To the resulting series now in $K((z))$ we apply the homomorphism which maps z to P and the coefficients to polynomials over $\mathbb{Q}$ using a homomorphism mapping the generator of K to a root of P in $\mathbb{Q}(t)/P^r$, where r is the P-adic precision of g. Lastly we take the remainder of this resulting polynomial mod P^r.

Determining a descent: (Step 3(b)ii) Most of the discussion in [26] Section 3.8 and [27] Section 8.8 applies here, including bounding the degree of the evaluation of an invariant at the roots of f. However, just as we required two primes, we also require two bounds – one on the polynomial degree of an evaluation, and one on the size of the coefficients of that polynomial. The minimum infinite valuation, computed in the same way as for global fields, can be used to compute a precision for a series M over the integers (computed using complex roots) which is a bound for the complex size of the integral coefficients. This is used to compute a bound B on the T_2 norm as $\deg(P)$ times the square of a bound on the evaluation of the invariant at a transformed root of size $T(M)$, where T is a Tschirnhausen transformation. The absolute precision of B times $\deg(P)$ is used to bound the degree of the evaluation of an invariant mapped back to $\mathbb{Q}(t)$. The maximum coefficient of B is then used to bound the coefficients of this mapped evaluation.

Precision: Since we have two completions in our splitting field construction, we require both a p-adic precision and a series precision. These are computed from the bound computed above. The series precision is taken to be the absolute precision of the series bound and the p-adic precision is computed from the largest coefficient of the series bound using Proposition 3.12 in [1].

3.2. **Galois groups of reducible polynomials over $\mathbb{Q}(t)$.** Section 7.6 of [8] mentions that their algorithm can be used to compute Galois groups of reducible polynomials. Indeed it can be, but as with the different coefficient

rings some adjustments must be made. For reducible polynomials these adjustments are most specifically in the computation of a starting group and the handling of multiple roots and linear factors. These adjustments necessary to efficiently compute Galois groups of reducible polynomials over global rational and algebraic function fields are discussed in [26, 27] and included in Magma V2.18. Here we describe the similar necessary adjustments, included in Magma V2.23, to use the algorithm of [8] to efficiently compute Galois groups of reducible polynomials over $\mathbb{Q}(t)$. We use Algorithm 2 of [27] ([26] Algorithm 12) and address these adjustments using the same headings used there. This algorithm uses the product of some of the Galois groups of the factors of f to gain a smaller starting group in Step 2 of Algorithm 3.1, and also does some post processing with linear and multiple factors so that the descent steps are minimized.

Choosing a good prime: The same polynomial prime and same integer prime must be used to compute the Galois groups of each of the factors of f. Otherwise Section 4.1.1 of [26] (Section 9.2.1 of [27]) holds also for polynomials over $\mathbb{Q}(t)$.

Computing roots in the splitting field over the completion: The local field $\mathbb{Q}_p(\alpha)$ must be computed such that it contains the roots of $(f_i)_K$ over $\mathbb{Q}_p$ for all factors f_i of f. The field $\mathbb{Q}_p(\alpha)((z))$ can then be used as a splitting field.

Check disjointedness of splitting fields: By checking whether the splitting fields of the factors are disjoint we can reduce the size of the descent necessary by starting with a smaller group. Since [24] Theorem III.6.3 and Corollary III.5.8 hold when the constant field (in this case $\mathbb{Q}$) is a perfect field, the discussion of [26, §4.1.3] and [27, §9.2.3] holds when computing Galois groups of reducible polynomials over $\mathbb{Q}(t)$ as well as over $\mathbb{F}_q(t)$.

Invariants: The invariants presented in [8] are sufficient here as all the rings involved have characteristic zero.

Determination: The computation of the precision necessary is as in Section 3.1, using the minimum infinite valuation (negative of the maximum degree) of all scaled roots of f.

Multiple and linear factors: Section 4.1.6 of [26] (or Section 9.2.6 of [27]) holds also for polynomials over $\mathbb{Q}(t)$.

3.3. **Computing a fixed field of a subgroup of a Galois group.** The procedure needed for this computation, which was implemented in Magma by Fieker and Klüners, is independent of the coefficient ring of the polynomial. We summarize an algorithm below. Though the details differ between coefficient rings, the necessary adjustments are already addressed in the various descriptions of the Galois group algorithm given in [8, 26, 27] and above. This algorithm applies to both reducible and irreducible polynomials.

Algorithm 3.2 (Compute a fixed field of a subgroup of a Galois group)**.** Given a subgroup U of a Galois group G of a polynomial f of degree n, and given the data used to compute G from f, compute a defining polynomial for the fixed field of U.

(1) Compute a G-relative U-invariant polynomial I and the right transversal $G//U$.
(2) Compute a Tschirnhausen transformation T such that
$$\#\{I^\tau(T(r_1),\dots,T(r_n)) : \tau \in G//U\} = \#G//U.$$
using roots $\{r_i\}_{i=1}^n$ of f to some low precision in the splitting field used for the Galois group computation.
(3) Compute a bound B on the evaluation of the invariant I at the roots of f and the roots $\{r_i\}_{i=1}^n$ of f to a precision that allows the bound B to be used.
(4) Compute the monic polynomial g with roots
$$\{I^\tau(T(r_1),\dots,T(r_n)) : \tau \in G//U\}.$$
(5) Map the coefficients of g back to the coefficient ring of f, and return the resulting polynomial, which is a defining polynomial for the fixed field of U.

Remark 3.3. The polynomial returned by Algorithm 3.2 will be of degree $\#(G//U)$; this can cause difficulties in practice when $G//U$ is large. An example where this type of issue occurs is discussed in §4.5.

3.4. **Proof of Galois groups of polynomials over $\mathbb{Q}(t)$.** The correctness of Galois groups computed using lower precision than necessary, such as when $[G : H]$ is substituted with a smaller value in the precision computation, can be proved using absolute resolvents as in [11] Algorithm 5.1 and [8] Section 7.4. We consider here the adjustments to these algorithms needed over $\mathbb{Q}(t)$.

Suppose we know that $H \le \mathrm{Gal}(f) \le G$. Algorithm 5.1 of [11] determines whether $\mathrm{Gal}(f) \ne G$ or $\mathrm{Gal}(f) \ne H$ by computing a resultant polynomial R and two factors, f_1 and f_2, of R to precision 1 based on an H-orbit which is not a G-orbit. This factorization is lifted to F_1F_2 with precision k, where k is computed from a bound M on the coefficients of the factors of R as in the computation of the Galois group. If F_1 corresponds to a true factor of R, then $\mathrm{Gal}(f) \ne G$; otherwise $\mathrm{Gal}(f) \ne H$. Letting $\{\alpha_i\}$ be the roots of f, we use these bounds to bound the coefficients of
$$R(y) = \prod_\tau (y - I^\tau(\alpha_1,\dots,\alpha_n)),$$
where I is H-invariant, and its factors by the quantity
$$\max_{1\le i\le n}\left\{\binom{\deg(R)}{i}\right\} B^{\deg(R)},$$

where B is a bound on $I^\tau(\alpha_1, \dots, \alpha_n)$ obtained as in the "Determining a descent" step of Section 3.1.

4. Examples

Having developed the theoretical and algorithmic material that form the core of this article, we proceed to apply our results to study the exceptional sets of three sample polynomials. The following algorithm will be our main tool.

Algorithm 4.1.

Input: A separable polynomial $P \in \mathbb{Q}[t][x]$.
Output: A finite set $D \subset \mathbb{Q}$ and a finite set $S \subset \mathbb{Q}[t][x]$.

(1) Create empty sets D and S.
(2) Include in D all the rational roots of the discriminant of P.
(3) Include in D all the rational roots of the leading coefficient of P.
(4) Compute the group $G = \mathrm{Gal}(P)$. More precisely, find a permutation representation of G induced by a labeling of the roots of P.
(5) Find subgroups $M_1, \dots, M_r$ representing all the conjugacy classes of maximal subgroups of G.
(6) For $M \in \{M_1, \dots, M_r\}$:
    (a) Find a monic irreducible polynomial $f \in \mathbb{Q}[t][x]$ such that the fixed field of M is generated by a root of f.
    (b) Include f in the set S.
    (c) Include in D all the rational roots of the discriminant of f.
(7) Return the sets D and S.

For Step 4 we use Algorithm 3.1 when P is irreducible and the adjustments discussed in §3.2 when P is reducible. For Step 5 we use an algorithm of Cannon and Holt [4]. For Step 6(a) we use Algorithm 3.2 and adjust the polynomial returned so that it has coefficients in $\mathbb{Q}[t]$ and defines the same extension. All of our computations were done using Magma V2.23, which includes implementations of these algorithms. The intrinsic function `HilbertIrreducibilityCurves` in Magma V2.24 is an implementation of Algorithm 4.1.

For later reference we record the following consequence of Theorem 2.7.

Proposition 4.2. *Let $P \in \mathbb{Q}[t][x]$ be a separable polynomial with Galois group G, and let D and S form the output of Algorithm 4.1 with input P. Then for all $c \in \mathbb{Q} \smallsetminus D$ we have:*

(1) If $\mathcal{F}(P_c) \neq \mathcal{F}(P)$, then $G_c \not\subseteq G$.
(2) $G_c \not\subseteq G \iff$ there exists $f \in S$ such that $f(c, x)$ has a rational root.

4.1. **A finite exceptional set.** In our first example we consider the polynomial $P(t, x) = x^6 + t^6 - 1$. As follows from the case $n = 3$ of Fermat's Last Theorem, the specialized polynomial P_c has a rational root if and only if $c \in \{0, \pm 1\}$. We will prove the following stronger result.

Proposition 4.3. *Let $c \in \mathbb{Q}$. Then P_c is reducible if and only if $c \in \{0, \pm 1\}$.*

Proof. Suppose that P_c is reducible and that $c \notin \{0, \pm 1\}$. Applying Algorithm 4.1 to the polynomial P we obtain the set $\{-1, 1\}$ and the polynomials

$$\begin{aligned} F_1(t,x) &= x^2 - 2^8 \cdot 3^5 (t^6-1)^5, \\ F_2(t,x) &= x^2 + 64 \cdot 27 (t^6-1)^2, \\ F_3(t,x) &= x^2 + 6x + 9t^6, \\ F_4(t,x) &= x^3 + 12x^2 + 48x - 8t^6 + 72. \end{aligned}$$

By Proposition 4.2, at least one of the polynomials $F_i(c,x)$ must have a rational root; we accordingly divide the proof into four cases.

Case 1: There exists $r \in \mathbb{Q}$ such that $F_1(c,r) = 0$. Defining $u = c^2$ and

$$v = r / \left(2^4 \cdot 3^2 \cdot (c^6-1)^2\right),$$

the equation $F_1(c,r) = 0$ implies that $v^2 = 3(u^3 - 1)$. This equation defines the elliptic curve with Cremona label 36a3, which has rank 0, and its only affine rational point is $(1,0)$. It follows that $u = 1$ and thus $c = \pm 1$, which is a contradiction. Hence this case cannot occur.

Case 2: There exists $r \in \mathbb{Q}$ such that $F_2(c,r) = 0$. Letting $u = 8 \cdot 3 \cdot (c^6 - 1)$, we have $u \neq 0$ and $r^2 + 3u^2 = 0$, which is clearly impossible. Thus we have a contradiction.

Case 3: There exists $r \in \mathbb{Q}$ such that $F_3(c,r) = 0$. Letting $v = (r+3)/3$ and $u = -c^2$, the equation $F_3(c,r) = 0$ implies that $v^2 = u^3 + 1$. This equation defines the elliptic curve with Cremona label 36a1, which has rank 0 and a torsion subgroup of order 6; its only affine rational points are $(0, \pm 1)$, $(2, \pm 3)$, and $(-1, 0)$. Since $u < 0$, we must have $u = -1$ and therefore $c^2 = 1$, which is a contradiction.

Case 4: There exists $r \in \mathbb{Q}$ such that $F_4(c,r) = 0$. Letting $y = 2c^3$, the equation $F_4(c,r) = 0$ implies that $2y^2 = r^3 + 12r^2 + 48r + 72$. This equation defines the elliptic curve with Cremona label 36a1, the same curve that appeared in the previous case. Using the above model of the curve, the affine rational points are $(0, \pm 6)$, $(-4, \pm 2)$, and $(-6, 0)$. It follows that $y = \pm 6, \pm 2$, or 0, which implies that $c^3 = \pm 3$, $c = \pm 1$, or $c = 0$, all of which yield a contradiction.

Since every case has led to a contradiction, we conclude that $c \in \{0, \pm 1\}$. □

4.2. **An infinite family of exceptional factorizations.** Let $P(t,x) = x^6 - 4x^2 - t^2$, which is an irreducible polynomial with Galois group isomorphic to the symmetric group S_4. In this example we will determine precisely for which rational numbers c the specialization P_c is reducible, and how P_c factors in that case.

Proposition 4.4. *Let c be a nonzero rational number such that P_c is reducible. Then c has the form $c = (v^4 + 16)/(8v)$ for some $v \in \mathbb{Q}$.*

Proof. Applying Algorithm 4.1 to P we obtain the set $\{0\}$ and the polynomials

$$F_1(t,x) = x^4 - 8tx + 16,$$
$$F_2(t,x) = x^2 + 1728t^4 - 16384,$$
$$F_3(t,x) = x^3 + 24x^2 + 176x - 8t^2 + 384.$$

By Proposition 4.2, one of the polynomials $F_i(c,x)$ must have a rational root. We will show that i cannot be 2 or 3, from which the proposition follows easily.

Suppose that $F_2(c,x) = 0$ for some $x \in \mathbb{Q}$. Letting

$$X = \frac{x+128}{4c^2} \text{ and } Y = \frac{2x+256}{c^3}$$

we obtain $Y^2 = X^3 + 108X$. This equation defines an elliptic curve with exactly two rational points, namely the point at infinity and the point $(0,0)$. Hence we must have $X = Y = 0$, which implies that $x = -128$. However, the equation $F_2(c,-128) = 0$ implies that $c = 0$, which is a contradiction.

By a similar argument one can show that the only rational solutions to the equation $F_3(t,x) = 0$ are $(0,-4)$, $(0,-8)$, and $(0,-12)$; hence $F_3(c,x) = 0$ is impossible for $x \in \mathbb{Q}$ since $c \neq 0$. □

Lemma 4.5. *Let $\mathcal{C}$ and $\mathcal{D}$ be the curves in $\mathbb{A}^2 = \operatorname{Spec}\mathbb{Q}[v,x]$ defined by the equations $8vx^3 - 8v^2x^2 + 4v^3x - v^4 - 16 = 0$ and $8vx^3 + 8v^2x^2 + 4v^3x + v^4 + 16 = 0$, respectively. Then $\mathcal{C}(\mathbb{Q}) = \mathcal{D}(\mathbb{Q}) = \varnothing$.*

Proof. The curves $\mathcal{C}$ and $\mathcal{D}$ are both non-hyperelliptic curves of genus 3, but they admit a map to an elliptic curve of rank 0; this allows us to determine their rational points. We give the proof only for $\mathcal{C}$, since the argument is very similar for $\mathcal{D}$.

There is a map from $\mathcal{C}$ to the elliptic curve $E : Y^2 = X^3 + X^2 + X$ given by $(v,x) \mapsto \big((2x-v)/v, (-4)/v^2\big)$. The curve E has rank 0, and its only rational points are ∞ and $(0,0)$. Any rational point on $\mathcal{C}$ must necessarily have $v \neq 0$, and will therefore map to the point $(0,0)$ on E. However, this is impossible since $-4/v^2 \neq 0$. Hence $\mathcal{C}$ has no rational point. □

Proposition 4.6. *Suppose that c is of the form $c = (v^4+16)/(8v)$ for some rational number v. Then P_c factors as*

$$64v^2 \cdot P_c = (8vx^3 - 8v^2x^2 + 4v^3x - v^4 - 16)(8vx^3 + 8v^2x^2 + 4v^3x + v^4 + 16).$$

Moreover, both cubic factors of P_c are irreducible.

Proof. Substituting $c = (v^4+16)/(8v)$ in the polynomial $P(c,x)$ and factoring, we obtain the above factorization. Lemma 4.5 implies that neither factor of P_c can have a rational root, and therefore both factors are irreducible. □

4.3. **An infinite family of exceptional Galois groups.** In [22, §4.5] Serre shows that for even values of n, the polynomial

$$P_n(t,x) = (n-1)x^n - nx^{n-1} + 1 + (-1)^{n/2}(n-1)t^2$$

has the alternating group A_n as its Galois group. By HIT, most specializations $P_n(c,x)$ will have Galois group A_n as well. In the case $n = 4$ we obtain the polynomial

$$P(t,x) = 3x^4 - 4x^3 + 1 + 3t^2$$

with Galois group A_4. In this example we will determine precisely for which rational numbers c the Galois group G_c is different from A_4, and which groups G_c arise for such numbers c. Our main results are Propositions 4.9 and 4.12.

Lemma 4.7. *Let $F_1(t,x) = x^3 + 48x^2 + (336 - 1296t^2)x - 10368t^2 + 640$ and let $c \in \mathbb{Q}^*$. Then the polynomial $F_1(c,x)$ has a rational root if and only if c has the form*

$$c = \frac{v^3 - 9v}{9(1-v^2)} \tag{4.1}$$

for some rational number v.

Proof. Let C be the plane curve defined by the equation $F_1(t,x) = 0$. The curve C is parametrizable; indeed, the rational maps

$$\phi : C \dashrightarrow \mathbb{A}^1 = \operatorname{Spec}\mathbb{Q}[z] \text{ and } \psi : \mathbb{A}^1 \dashrightarrow C$$

given by

$$\psi(z) = \left(\frac{z^3 - 9z}{9(1-z^2)}, \frac{8(z^2-5)}{1-z^2}\right) \text{ and } \phi(t,x) = \frac{x^2 - 1296t^2 + 44x + 160}{144t}$$

are easily seen to be inverses.

Suppose that c is of the form (4.1). We may then define

$$r = \frac{8(v^2-5)}{1-v^2},$$

so that $\psi(v) = (c,r)$ is a rational point on C. Hence, the polynomial $F_1(c,x)$ has a rational root (namely r).

Conversely, suppose that $F_1(c,x)$ has a rational root, say r. Since $c \neq 0$, the map ϕ is defined at the point $(c,r) \in C(\mathbb{Q})$. Thus, we may define $v = \phi(c,r)$. We claim that $v \neq \pm 1$. A straightforward calculation shows that the rational points on the pullback of ± 1 under ϕ are $(0,-40)$ and $(0,-4)$. Since $c \neq 0$, the point (c,r) is different from these two points. Hence $v = \phi(c,r) \neq \pm 1$, as claimed. The map ψ is therefore defined at v, so $(c,r) = \psi(v)$. In particular, c is of the form (4.1). □

Lemma 4.8. *Let $F_2(t,x) = x^4 + 4x^3 + 81t^2 + 27$ and let $c \in \mathbb{Q}^*$. Then the polynomial $F_2(c,x)$ has no rational root.*

Proof. Suppose that $r \in \mathbb{Q}$ is such that $F_2(c,r) = 0$. Since $c \neq 0$, we must have $r \neq -3$. Defining $y = 9c/(r+3)$, the equation $F_2(c,r) = 0$ implies that

$$y^2 + (r-1)^2 + 2 = 0,$$

which is clearly impossible for $y, r \in \mathbb{Q}$. This contradiction proves the lemma. □

Proposition 4.9. *Let $c \in \mathbb{Q}$ and let G_c be the Galois group of P_c. Then*

$$G_c \not\subseteq A_4 \iff c = \frac{v^3 - 9v}{9(1-v^2)} \text{ for some } v \in \mathbb{Q}.$$

Proof. For $c = 0$ the proposition holds because both statements in the above equivalence are true. Indeed, we have

$$P_0 = 3x^4 - 4x^3 + 1 = (x-1)^2(3x^2 + 2x + 1),$$

so G_0 has order 2.

Suppose now that $c \neq 0$. Applying Algorithm 4.1 to the polynomial P we obtain the set $\{0\}$ and the polynomials

$$F_1(t,x) = x^3 + 48x^2 + (336 - 1296t^2)x - 10368t^2 + 640,$$
$$F_2(t,x) = x^4 + 4x^3 + 81t^2 + 27.$$

By Proposition 4.2 and Lemmas 4.7 and 4.8, we have the following:

$$\begin{aligned} G_c \not\subseteq A_4 &\iff F_1(c,x) \cdot F_2(c,x) \text{ has a rational root} \\ &\iff F_1(c,x) \text{ has a rational root} \\ &\iff c = \frac{v^3 - 9v}{9(1-v^2)} \text{ for some } v \in \mathbb{Q}. \end{aligned}$$ □

Continuing with this example, we turn now to the question of which subgroups of A_4 arise as groups G_c for some $c \in \mathbb{Q}$. Let N be a splitting field for P over $\mathbb{Q}(t)$. Let $G = \mathrm{Gal}(N/\mathbb{Q}(t))$ be the Galois group of P, and fix an isomorphism $G \cong A_4$. Since

$$\operatorname{disc} P = 2^8 \cdot 3^4 \cdot t^2(3t^2+1)^2,$$

Proposition 2.3 implies that for $c \neq 0$, the group G_c is isomorphic to a subgroup of A_4. The same holds true for $c = 0$ since G_0 has order 2 and A_4 has a subgroup of order 2. Proposition 4.9 thus leads naturally to the following question: when G_c is not isomorphic to A_4, which subgroup of A_4 is it isomorphic to? The methods of §§2-3 provide a way to answer this.

Up to conjugacy, A_4 has exactly three nontrivial proper subgroups:

$$A = \langle (1,2)(3,4), (1,3)(2,4) \rangle, \ B = \langle (1,2,3) \rangle, \text{ and } C = \langle (1,2)(3,4) \rangle.$$

We will henceforth identify A, B, and C with the subgroups of G that they correspond to under the isomorphism $G \cong A_4$.

Let F_A, F_B, and F_C be the fixed fields of A, B, and C, respectively. Using Magma we find that F_A and F_B are generated over $\mathbb{Q}(t)$ by the polynomials

$F_1(t,x)$ and $F_2(t,x)$ defined in Lemmas 4.7 and 4.8. For F_C we obtain the polynomial

$$F_3(t,x) = x^6 + 12x^5 + 48x^4 + 64x^3 \\ - (324t^2 + 108)x^2 - (1296t^2 + 432)x - 1296t^2 - 432.$$

Lemma 4.10. *Let $c \in \mathbb{Q}^*$, and let $\mathfrak{P}$ be a prime of N lying over the prime $(t-c) \subset \mathbb{Q}[t]$. Then $G_{\mathfrak{P}} \nsubseteq B$.*

Proof. Suppose, by contradiction, that $G_{\mathfrak{P}} \subseteq B$. We have

$$\operatorname{disc} F_2 = 2^8 \cdot 3^{10} \cdot t^2(3t^2+1)^2,$$

so $\operatorname{disc} F_2(c,x) \neq 0$. By Proposition 2.6 applied to the field F_B, the polynomial $F_2(c,x)$ has a rational root. However, this contradicts Lemma 4.8. □

It follows from the above lemma (and Proposition 2.3) that if $c \in \mathbb{Q}$ is such that $G_c \nsubseteq A_4$, then G_c must be isomorphic to either A or C. We now determine precisely when each case occurs.

Lemma 4.11. *Let $v \in \mathbb{Q} \setminus \{\pm 1\}$ and let $c = (v^3 - 9v)/(9(1-v^2))$. Then the polynomial $F_3(c,x)$ has a rational root if and only if v has one of the forms*

$$1 + 2w^2, \ -1 - 2w^2, \text{ or } \frac{2w}{1+w^2}$$

for some $w \in \mathbb{Q}$.

Proof. Substituting $c = (v^3 - 9v)/(9(1-v^2))$ in the polynomial $F_3(c,x)$ we find that there is a factorization

$$(v^2-1)^2 \cdot F_3(c,x) = f(v,x) \cdot g(v,x) \cdot h(v,x),$$

where $f, g, h \in \mathbb{Q}[t,x]$ are defined by

$$f(t,x) = (t-1)x^2 + (4t-4)x - 2t^2 - 6,$$
$$g(t,x) = (t+1)x^2 + (4t+4)x + 2t^2 + 6,$$
$$h(t,x) = (t^2-1)x^2 + (4t^2-4)x + 4t^2 + 12.$$

It follows that $F_3(c,x)$ has a rational root if and only if at least one of the discriminants of $f(v,x)$, $g(v,x)$, or $h(v,x)$ is a square. Now, it is a straightforward calculation to verify that

$$\operatorname{disc} f(v,x) = 8(v-1)(v+1)^2$$

is a square if and only if $v = 1 + 2w^2$ for some $w \in \mathbb{Q}$; that

$$\operatorname{disc} g(v,x) = -8(v+1)(v-1)^2$$

is a square if and only if $v = -1 - 2w^2$ for some $w \in \mathbb{Q}$; and that

$$\operatorname{disc} h(v,x) = -64(v^2-1)$$

is a square if and only if $v = (2w)/(1+w^2)$ for some $w \in \mathbb{Q}$. Therefore, $F_3(c,x)$ has a rational root if and only if v has one of these forms. □

We can now give a complete characterization of the groups G_c that are not isomorphic to A_4.

Proposition 4.12. *Suppose that $c \in \mathbb{Q}$ satisfies $G_c \not\cong A_4$, so that*

$$c = \frac{v^3 - 9v}{9(1 - v^2)} \text{ for some } v \in \mathbb{Q}.$$

If v has one of the forms

$$1 + 2w^2,\ -1 - 2w^2,\ \text{or } \frac{2w}{1 + w^2}, \tag{4.2}$$

then $G_c \cong C$. Otherwise $G_c \cong A$.

Proof. For $c = 0$ the result is easily verified; thus, we assume that $c \neq 0$. We then have $\operatorname{disc} F_3(c, x) = 2^{28} \cdot 3^{20} \cdot c^4(3c^2 + 1)^4 \neq 0$.

Suppose that v has one of the forms (4.2). By Lemma 4.11, the polynomial $F_3(c, x)$ has a rational root. By Proposition 2.6 this implies that there exists a prime $\mathfrak{P}$ of N lying over $(t - c)$ such that $G_{\mathfrak{P}} \subseteq C$. The group $G_{\mathfrak{P}}$ is nontrivial by Lemma 4.10, so $G_{\mathfrak{P}} = C$. Hence, by Proposition 2.3, G_c is isomorphic to C.

Suppose now that v cannot be written in any of the forms (4.2). By Lemma 4.11 and Lemma 4.7, the polynomial $F_3(c, x)$ does not have a rational root but $F_1(c, x)$ does. Hence, by Proposition 2.6, there exists a prime $\mathfrak{P}$ of N lying over $(t - c)$ such that $G_{\mathfrak{P}} \subseteq A$ but $G_{\mathfrak{P}} \not\subseteq C$. Hence $G_{\mathfrak{P}} = A$ and, by Proposition 2.3, $G_c \cong A$. □

4.4. **A reducible polynomial.** We end §4 by mentioning two sample computations with polynomials $P(t, x)$ of larger degrees. Let $\phi(x) = x^2 + t \in \mathbb{Q}(t)[x]$ and let n be a positive integer. The *n-th dynatomic polynomial* of ϕ is defined by the equation

$$\Phi_n(t, x) = \prod_{d \mid n} \left(\phi^d(x) - x\right)^{\mu(n/d)},$$

where μ is the Möbius function and ϕ^d denotes the d-fold composition of ϕ with itself. The significance of the polynomial Φ_n is that its roots are precisely the elements of $\overline{\mathbb{Q}(t)}$ having period n under iteration of $\phi(x)$. It is an important unsolved problem in the field of arithmetic dynamics to determine the exceptional set of Φ_n for every n.

Consider the problem of determining the exceptional set of the polynomial Φ_4, which has degree 12. Using Algorithm 4.1 we find that every rational number c of the form $c = (4 - 3v - v^3)/4v$ with $v \in \mathbb{Q}^*$ lies in $\mathcal{E}(\Phi_4)$. To determine what the Galois group of the specialized polynomial $\Phi_4(c, x)$ is when c has this form, we compute the Galois group, H, of the polynomial

$$P(v, x) := \Phi_4((4 - 3v - v^3)/4v, x) \in \mathbb{Q}(v)[x],$$

which is a product of a degree-8 and a degree-4 polynomial. An application of Algorithm 4.1 to $P(v, x)$ reveals that when v does not have the form

$v = (1 + 4s^3 - s^6)/(4s^2(s^2 - 1))$, the Galois group of $P(v, x)$ is equal to H, and when v does have this form, the Galois group is a proper subgroup of H. Note that these calculations require the ability to compute Galois groups of reducible polynomials over function fields.

4.5. **A polynomial of degree 30.** Consider now the polynomial $P = \Phi_5$. The Galois group G in this case is the wreath product $(\mathbb{Z}/5\mathbb{Z}) \wr S_6$, which has order 11,250,000. While the computation of G and its maximal subgroups did not present any problems, we were unable to fully carry out Algorithm 4.1 for this polynomial. The unique obstacle was the computation of the fixed field of one maximal subgroup of G that has index 3125. For the other maximal subgroups (all of which have index at most 15) we did successfully compute the corresponding fixed field.

5. An application to arithmetic dynamics

In [19] Manes studies the possible periods of rational numbers under iteration of maps of the form

$$\phi_{k,b}(z) = kz + b/z, \text{ where } k \in \mathbb{Q} \smallsetminus \{0, -1/2\} \text{ and } b \in \mathbb{Q}^*.$$

Manes conjectures that no such map can have a rational point of period greater than four, and proves the following finiteness result for points of period five: there exists a finite set $S \subset \mathbb{Q}$ such that if $k \notin S$ then, for any $b \in \mathbb{Q}^*$, the map $\phi_{k,b}$ has no point of period five in $\mathbb{Q}$. Our goal in this section is to prove a stronger statement.

Proposition 5.1. *There exists a finite set $S \subset \mathbb{Q}$ such that if $k \in \mathbb{Q} \smallsetminus S$, then the following holds for every $b \in \mathbb{Q}^*$: for at least one third of all prime numbers p (in the sense of Dirichlet density), the map $\phi_{k,b}$ has no point of period five in $\mathbb{Q}_p$.*

To prove the above proposition we will need to determine the exceptional set of polynomial $P \in \mathbb{Q}[t, x]$ given by

$$P(t, x) = t^4x^3 + a(t)x^2 + b(t)x + c(t),$$

where

$$\begin{aligned} a(t) &= 11t^6 + 11t^5 + 11t^4 + 7t^3 + 5t^2 + 2t + 1, \\ b(t) &= 19t^8 + 38t^7 + 57t^6 + 60t^5 + 55t^4 + 38t^3 + 24t^2 + 9t + 3, \\ c(t) &= (3t^3 + 3t^2 + 3t + 1)^2(t^4 + t^3 + t^2 + t + 1). \end{aligned}$$

The following lemma explains the precise relation between the polynomial P and points of period five for maps of the form $\phi_{k,b}$.

Lemma 5.2. *Let F be a field of characteristic 0, and let $k \in F \smallsetminus \{0, -1/2\}$ and $b \in F^*$. Suppose that the map $\phi_{k,b}(z)$ has a point of period five in F. Then the polynomial $P(k, x)$ has a root in F.*

Proof. This follows immediately from the proof of [19, p. 683, Prop. 3]. □

Lemma 5.3. *The exceptional set $\mathcal{E}(P)$ is finite.*

Proof. The polynomial P is irreducible and its Galois group G is isomorphic (as a group of permutations of the roots of P) to the symmetric group S_3. Up to conjugacy, G has exactly two maximal subgroups, namely the unique subgroup A of order 3 (which is isomorphic to the alternating group A_3), and a subgroup B of order 2. The fixed fields of these subgroups, F_A and F_B, are therefore extensions of $\mathbb{Q}(t)$ of degrees 2 and 3, respectively. Since P is an irreducible cubic polynomial over $\mathbb{Q}(t)$, it generates a cubic extension of $\mathbb{Q}(t)$; thus, by replacing B with a conjugate subgroup if necessary, we may assume that F_B is generated by P.

Using Magma to compute the group G and fixed field F_A, we find that the extension $F_A/\mathbb{Q}(t)$ is generated by a root of the polynomial $x^2 - f(t)$, where

$$f(t) = 256t^{12} + 256t^{11} + 576t^{10} + 384t^9 + 608t^8 + 336t^7 \\ + 432t^6 + 184t^5 + 193t^4 + 60t^3 + 50t^2 + 8t + 5.$$

By Theorem 2.7, in order to show that the exceptional set of P is finite it suffices to show that the curves defined by $P(t,x) = 0$ and $x^2 = f(t)$ have only finitely many rational points. The genera of these curves are 4 and 5, respectively, so the result is a consequence of Faltings's theorem. □

We can now prove our main result for this section.

Proof of Proposition 5.1. Let $S = \mathcal{E}(P) \cup \{0, -1/2\}$, which is a finite set by Lemma 5.3. Suppose that $k \in \mathbb{Q} \smallsetminus S$ and $b \in \mathbb{Q}^*$. Since $k \notin \mathcal{E}(P)$, the polynomial $P(k,x)$ is irreducible and its Galois group is isomorphic to $\mathrm{Gal}(P) \cong S_3$. By Proposition 2.3 this implies that the Galois group of $P(k,x)$ acts on the roots of this polynomial in the same way that S_3 acts on the set $\{1,2,3\}$.

Let $\mathcal{P}$ denote the set of primes p such that $P(k,x)$ has a root in $\mathbb{Q}_p$. For $i = 1,2,3$, let U_i be the stabilizer of i in S_3. The Chebotarev Density Theorem (see [2, Thm. 2] or [15, Thm. 2.1]) implies that the Dirichlet density of $\mathcal{P}$ is given by

$$\frac{|\bigcup_{i=1}^3 U_i|}{|S_3|} = \frac{2}{3}.$$

The complement of $\mathcal{P}$ therefore has density 1/3. Now, if p is a prime not in $\mathcal{P}$, then $P(k,x)$ does not have a root in $\mathbb{Q}_p$, and hence, by Lemma 5.2, the map $\phi_{k,b}(z)$ has no point of period five in $\mathbb{Q}_p$. This completes the proof of the proposition. □

Acknowledgements. The first author would like to thank Pierre Dèbes for several helpful discussions related to the material of §2. The second author would like to thank Claus Fieker and A.-Stephan Elsenhans for their help in working with the Galois group implementation of Fieker, which has been extended by Elsenhans.

References

[1] Karim Belabas, *A relative van Hoeij algorithm over number fields*, J. Symbolic Comput. **37** (2004), no. 5, 641–668.

[2] Daniel Berend and Yuri Bilu, *Polynomials with roots modulo every integer*, Proc. Amer. Math. Soc. **124** (1996), no. 6, 1663–1671.

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[4] John Cannon and Derek F. Holt, *Computing maximal subgroups of finite groups*, J. Symbolic Comput. **37** (2004), no. 5, 589–609.

[5] Pierre Dèbes and Yann Walkowiak, *Bounds for Hilbert's irreducibility theorem*, Pure Appl. Math. Q. **4** (2008), no. 4, 1059–1083.

[6] Claus Fieker, *Galois groups of polynomials over* $\mathbb{Q}(t)$ (2008). Magma implementation.

[7] Claus Fieker and Carsten Friedrichs, *On reconstruction of algebraic numbers*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 285–296.

[8] Claus Fieker and Jürgen Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math. **17** (2014), no. 1, 141–158.

[9] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J. **90** (1997), no. 3, 435–463.

[10] K. Geißler, *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*, Technische Universität Berlin, 2003.

[11] Katharina Geissler and Jürgen Klüners, *Galois group computation for rational polynomials*, J. Symbolic Comput. **30** (2000), no. 6, 653–674. Algorithmic methods in Galois theory.

[12] Alexander Hulpke, *Techniques for the computation of Galois groups*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 65–77.

[13] Jürgen Klüners, *Algorithms for function fields*, Experiment. Math. **11** (2002), no. 2, 171–181.

[14] Jürgen Klüners and Gunter Malle, *Explicit Galois realization of transitive groups of degree up to 15*, J. Symbolic Comput. **30** (2000), no. 6, 675–716. Algorithmic methods in Galois theory.

[15] David Krumm, *A local-global principle in the dynamics of quadratic polynomials*, Int. J. Number Theory **12** (2016), no. 8, 2265–2297.

[16] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[17] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996.

[18] Patrick Morton and Joseph H. Silverman, *Rational periodic points of rational functions*, Internat. Math. Res. Notices **2** (1994), 97–110.

[19] Michelle Manes, $\mathbb{Q}$*-rational cycles for degree-2 rational maps having an automorphism*, Proc. Lond. Math. Soc. **96** (2008), no. 3, 669–696.

[20] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999.

[21] Bjorn Poonen, *The classification of rational preperiodic points of quadratic polynomials over* $\mathbf{Q}$*: a refined conjecture*, Math. Z. **228** (1998), no. 1, 11–29.

[22] Jean-Pierre Serre, *Topics in Galois theory*, 2nd ed., Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008.

[23] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

[24] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[25] Michael Stoll, *Rational points on curves*, J. Théor. Nombres Bordeaux **23** (2011), no. 1, 257–277.
[26] Nicole Sutherland, *Computing Galois groups of polynomials (especially over function fields of prime characteristic)*, J. Symbolic Comput. **71** (2015), 73–97.
[27] ———, *Algorithms for Galois extensions of global function fields*, The University of Sydney, 2015.

Mathematics Department, Reed College
E-mail address: dkrumm@reed.edu
URL: http://maths.dk

Computational Algebra Group, School of Mathematics and Statistics, The University of Sydney
E-mail address: nicole.sutherland@sydney.edu.au