Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Odoni's conjecture for number fields

Robert L. Benedetto and Jamie Juul

Abstract

Let K be a number field, and let $d \geq 2$. A conjecture of Odoni (stated more generally for characteristic zero Hilbertian fields K) posits that there is a monic polynomial $f \in K[x]$ of degree d, and a point $x_0 \in K$, such that for every $n \geq 0$, the so-called arboreal Galois group $\mathrm{Gal}(K(f^{-n}(x_0))/K)$ is an n-fold wreath product of the symmetric group S_d. In this paper, we prove Odoni's conjecture when d is even and K is an arbitrary number field, and also when both d and $[K : \mathbb{Q}]$ are odd.

1. *Introduction*

Let F be a field, let $f(x) \in F[x]$ be a polynomial of degree $d \geq 2$, and let $x_0 \in F$. For each $n \geq 0$, denote by f^n the n-iterate $f \circ f \circ \cdots \circ f$ of f, and consider the set

$$f^{-n}(x_0) = \{\alpha \in \bar{F} \mid f^n(\alpha) = x_0\}$$

of n-th preimages of x_0. If $f^n - x_0$ is separable for all n, then $f^{-n}(x_0)$ has exactly d^n elements for each n, and $F(f^{-n}(x_0))$ is a Galois extension of F.

In [**9**], Odoni showed that $\mathrm{Gal}(F(f^{-n}(x_0))/F)$ is isomorphic to a subgroup of $[S_d]^n$, the n-fold wreath product of the symmetric group S_d with itself. He also showed that if $\mathrm{char}\, F = 0$ and $E = F(s_{d-1}, \ldots, s_0)$, then the generic monic polynomial $G(x) = x^d + s_{d-1}x^{d-1} + \cdots + s_0 \in E[x]$ defined over the function field E satisfies $\mathrm{Gal}(E(G^{-n}(0))/E) \cong [S_d]^n$. In [**6**], the second author showed that this result also holds for fields of characteristic p, except in the case $p = d = 2$. It follows from Hilbert's Irreducibility Theorem that if $F = \mathbb{Q}$, or more generally if F is any Hilbertian field, then for any fixed $n \geq 0$, there are infinitely many polynomials $f(x) \in F(x)$ for which $\mathrm{Gal}(F(f^{-n}(x_0))/F) \cong [S_d]^n$. However, it does not follow immediately that there are any polynomials $f(x) \in F[x]$ for which this isomorphism holds for *all* $n \geq 0$. Based on his results, Odoni proposed the following conjecture.

Conjecture 1 (Odoni, Conjecture 7.5 [**9**]). For any Hilbertian field F of characteristic 0 and any $d \geq 2$, there is a monic polynomial $f(x) \in F[x]$ of degree d such that $\mathrm{Gal}(F(f^{-n}(0))/F) \cong [S_d]^n$ for all $n \geq 0$.

For any point $x_0 \in F$, if we set $g(x) = f(x + x_0) - x_0 \in F[x]$, then the fields $F(f^{-n}(x_0))$ and $F(g^{-n}(0))$ coincide. Thus, it is equivalent to phrase Odoni's conjecture in terms of the preimages $f^{-n}(x_0)$ of an arbitrary F-rational point x_0 instead of 0.

The Galois groups $\mathrm{Gal}(F(f^{-n}(x_0)/F)$ can be better understood through the framework of arboreal Galois representations [**2**]. It is not hard to see that $[S_d]^n \cong \mathrm{Aut}(T_{d,n})$ where $T_{d,n}$ is a d-ary rooted tree with n levels. We define an embedding $\mathrm{Gal}(F(f^{-n}(x_0))/F) \to \mathrm{Aut}(T_{d,n})$ by assigning each element of $\bigsqcup_{i=1}^{n} f^{-i}(x_0)$ to a vertex of the tree as follows: x_0 is the root of

---

2000 *Mathematics Subject Classification* 37P05 (primary), 11R32, 14G25 (secondary).

The first author gratefully acknowledges the support of NSF grant DMS-1501766.

the tree, and the points of $f^{-i}(x_0)$ are the vertices at the i-th level of the tree, with an edge connecting $\alpha \in f^{-i}(x_0)$ to $\beta \in f^{-i-1}(x_0)$ if $f(\beta) = \alpha$.

Jones [**5**] stated a version Odoni's Conjecture in the case that $F = \mathbb{Q}$ by further specifying that f should have coefficients in $\mathbb{Z}$. In this paper, however, we consider the original version of Conjecture 1, where f is allowed to have non-integral coefficients.

Conjecture 1 has already been proven in many cases. Odoni himself proved that $\mathrm{Gal}(\mathbb{Q}(f^{-n}(0))/\mathbb{Q}) \cong [S_2]^n$ for all $n \geq 0$ when $f(x) = x^2 - x + 1$, proving the conjecture for $F = \mathbb{Q}$ and $d = 2$ [**10**]. Stoll [**12**] produced infinitely many such polynomials for $F = \mathbb{Q}$ and $d = 2$. In 2017, Looper showed that Odoni's conjecture holds for $F = \mathbb{Q}$ and $d = p$ a prime [**8**].

In this paper, we prove Odoni's conjecture for even $d \geq 2$ over any number field, as well as for odd $d \geq 3$ over any number field K not containing $\mathbb{Q}(\sqrt{d}, \sqrt{d-2})$. (In particular, we prove the conjecture when d and $[K : \mathbb{Q}]$ are both odd.)

Theorem 1.1. *Let $d \geq 2$, and let K be a number field. Suppose either that d is even or that d and $d-2$ are not both squares in K. Then there is a monic polynomial $f(x) \in K[x]$ of degree d and a rational point $x_0 \in K$ such that for all $n \geq 0$,*

$$\mathrm{Gal}\left(K\big(f^{-n}(x_0)\big)/K\right) \cong [S_d]^n.$$

The proof, which builds on Looper's techniques, proceeds by induction on n, and involves studying the primes ramifying in $K(f^{-n}(x_0))$. In particular, to help generate the full group S_d when d is not necessarily prime, we introduce a positive integer $m < d$ and an auxiliary prime K that ramifies to degree m^n in $K(\alpha)$, for any $\alpha \in f^{-n}(x_0)$.

Recently, Borys Kadets [**7**] and Joel Specter [**11**] have announced proofs of similar theorems, and using similar extensions of Looper's techniques. Kadets proves Odoni's conjecture over $\mathbb{Q}$ for polynomials of even degree $d \geq 20$. Specter proves Odoni's conjecture for algebraic extensions of $\mathbb{Q}$ which are unramified outside of infinitely many primes. Our work, which we announced at the 2018 Joint Math Meetings in San Diego (see `https://rlbenedetto.people.amherst.edu/talks/sandiego18.pdf`), was done simultaneously and independently from these projects.

The outline of the paper is as follows. In Section 2 we give preliminary results on discriminant formulas and ramification, as well as a useful group theory lemma, Lemma 2.4. In Section 3 we prove sufficient conditions for $\mathrm{Gal}(K(f^{-n}(x_0))/K)$ to be isomorphic to $[S_d]^n$. Finaly, we prove Theorem 1.1 for even $d \geq 2$ in Section 4, and for odd $d \geq 3$ in Section 5.

2. *Ramification and the discriminant*

We begin with the following result on the discriminant of a field generated by a root of a trinomial.

Lemma 2.1. *Let K be a number field with ring of integers $\mathcal{O}_K$, let $d > m \geq 1$ with $(m, d) = 1$, let $A, B, C \in K$ with $A \neq 0$, and let S be a finite set of primes of $\mathcal{O}_K$ including all archimedean primes and all primes at which any of A, B, C have negative valuation.*

Suppose that $g(x) = Ax^d + Bx^m + C \in \mathcal{O}_{K,S}[x]$ is irreducible over K. Let $L = K(\theta)$, where θ is a root of $g(x)$. Then the discriminant $\Delta(\mathcal{O}_{L,S}/\mathcal{O}_{K,S})$ satisfies $\Delta(g) = k^2 \Delta(\mathcal{O}_{L,S}/\mathcal{O}_{K,S})$, where $k \in \mathcal{O}_{K,S}$, and

$$\Delta(g) = (-1)^{d(d-1)/2} A^{d-m-1} C^{m-1} \left[(-1)^{d-1} m^m (d-m)^{d-m} B^d + d^d A^m C^{d-m}\right]$$

is the discriminant of the polynomial g.

We will also make use of the following discriminant formula:

$$\Delta(f^{n+1}(x)-t)=\tilde{A}^{d^n}[\Delta(f^n(x)-t)]^d\prod_{f'(r)=0}(f^{n+1}(r)-t)^{m_r}, \tag{1}$$

where f is a polynomial of degree d and lead coefficient A, where $\tilde{A}=(-1)^{d(d-1)/2}d^dA^{d-1}$, and where m_r is the multiplicity of r as a root of $f'(x)$. See [**1**, Proposition 3.2].

Proof of Lemma 2.1 (Sketch). This is a standard result, using the fact that any prime $\mathfrak{p}\nmid A$ of $\mathcal{O}_{K,S}$ ramifying in $\mathcal{O}_{L,S}$ divides $\Delta(\mathcal{O}_{L,S}/\mathcal{O}_{K,S})$. See, for example, Lemma 7.2, Theorem 7.3, and Theorem 7.6 of [**4**].

To prove the formula for $\Delta(g)$, we apply formula (1) with $f=g$, $n=0$, and $t=0$. More precisely, $x=0$ is a critical point of g of multiplicity $m-1$, and we have $g(0)^{m-1}=C^{m-1}$. The other critical points are $\zeta^j\eta$ for $1\le j\le d-m$, where η is a $(d-m)$-th root of $-mB/(dA)$, and where ζ is a primitive $(d-m)$-th root of unity. Thus,

$$\begin{aligned}\prod_{j=1}^{d-m} g\left(\zeta^j\eta\right) &= \prod_{j=1}^{d-m}\left(C-\left(\frac{m-d}{d}\right)B\zeta^{jm}\eta^m\right)\\ &= C^{d-m}-\left[\left(\frac{m-d}{d}\right)^{d-m}B^{d-m}\left(-\frac{mB}{dA}\right)^m\right]\\ &= d^{-d}A^{-m}\left[d^dA^mC^{d-m}+(-1)^{d-1}(d-m)^{d-m}m^mB^d\right],\end{aligned} \tag{2}$$

where we have used the fact that d and $(d-m)$ are relatively prime in the second equality, to deduce that

$$\{\zeta^{jm}:1\le j\le d-m\}=\{\zeta^j:1\le j\le d-m\}.$$

Multiplying by $g(0)^{m-1}$ and $(-1)^{d(d-1)/2}d^dA^{d-1}$ as in formula (1), the desired formula for $\Delta(g)$ follows immediately. □

LEMMA 2.2. *Let A,B,C,d,m,g,K,L be as in Lemma 2.1. If a prime $\mathfrak{p}\nmid ABC$ of $\mathcal{O}_{K,S}$ ramifies in $\mathcal{O}_{L,S}$, and if $\mathfrak{q}$ is a prime of the Galois closure of L over K, then $\mathfrak{p}\nmid md(d-m)$, and the ramification group $I(\mathfrak{q}|\mathfrak{p})$ is generated by a single transposition of the roots of g.*

Proof. Let $\mathfrak{p}\nmid ABC$ be a prime of $\mathcal{O}_{K,S}$ which ramifies in $\mathcal{O}_{L,S}$. Then $\mathfrak{p}\mid\Delta(\mathcal{O}_{L,S}/\mathcal{O}_{K,S})$, and hence by Lemma 2.1, we also have $\mathfrak{p}\nmid md(d-m)$, since $(d,m)=1$.

Because $\mathfrak{p}$ ramifies, $g(x)$ must have at least one multiple root modulo $\mathfrak{p}$. On the other hand, if η is a mod-$\mathfrak{p}$ root of multiplicity $\ell>2$, then η is also at least a double root of the derivative $g'(x)\equiv dAx^{d-1}+mBx^{m-1} \pmod{\mathfrak{p}}$. However, since $\mathfrak{p}\nmid ABCdm(d-m)$, this cannot be the case unless $\eta\equiv 0 \pmod{\mathfrak{p}}$; but then η would not have been a root of g itself, since $\mathfrak{p}\nmid C$. Therefore each root of $g(x) \pmod{\mathfrak{p}}$ has at multiplicity at most two.

Now suppose η and ξ are both double roots of $g(x) \pmod{\mathfrak{p}}$. Then both η and ξ are nonzero simple roots of $g'(x) \pmod{\mathfrak{p}}$, and hence

$$\eta^{d-m}\equiv\xi^{d-m}\equiv\frac{-mB}{dA} \pmod{\mathfrak{p}}.$$

Thus, $\eta\equiv\zeta\xi \pmod{\mathfrak{p}}$, where ζ is a $(d-m)$-th root of unity. If $\zeta\not\equiv 1 \pmod{\mathfrak{p}}$, then $\zeta^m\not\equiv 1 \pmod{\mathfrak{p}}$, since $(m,d-m)=1$. Therefore,

$$g(\eta)=C+\big(g(\eta)-C\big)\equiv C+\zeta^m\big(g(\xi)-C\big)\equiv(1-\zeta^m)C\not\equiv 0 \pmod{\mathfrak{p}},$$

a contradiction. Hence, we must have $\eta\equiv\xi \pmod{\mathfrak{p}}$.

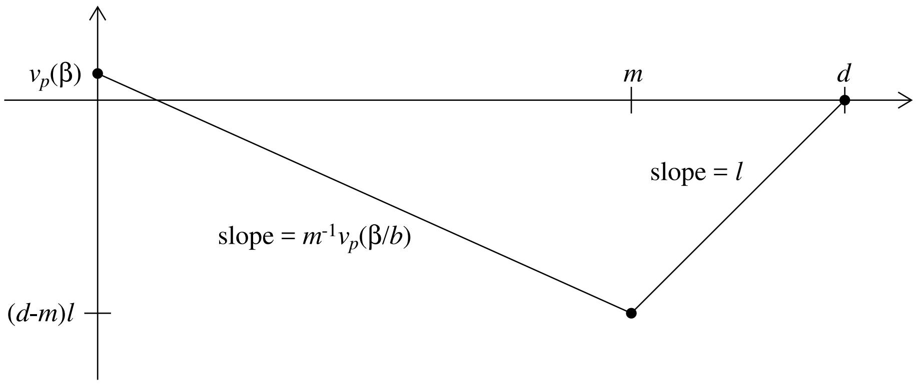

FIGURE 1. *The Newton polygon for $f(x) - \beta$ in Lemma 2.3.*

The two previous paragraphs together yield that g has exactly one multiple root modulo $\mathfrak{p}$, and it is a double root. That is,

$$g(x) \equiv A(x - \eta)^2 g_1(x) \pmod{\mathfrak{p}},$$

where $g_1(x) \in \mathcal{O}_{K,S}/\mathfrak{p}[x]$ is a separable polynomial with $g_1(\eta) \not\equiv 0 \pmod{\mathfrak{p}}$. Since g is irreducible over K, it follows that $I(\mathfrak{q}|\mathfrak{p})$ is generated by a single transposition, for any $\mathfrak{q}$ lying above $\mathfrak{p}$. □

LEMMA 2.3. *Let $d > m \geq 2$, let $b, x_0 \in K$, and suppose there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p} \nmid (d - m)$, and $v_\mathfrak{p}(b) < \min\{v_\mathfrak{p}(x_0), 0\}$, with $(d - m)|v_\mathfrak{p}(b)$ and $\gcd(m, v_\mathfrak{p}(x_0/b)) = 1$. Let $f(x) = x^d - bx^m$, let $n \geq 0$, and let $\alpha \in f^{-n}(x_0)$. Suppose that $f^n(x) - x_0 \in K[x]$ is irreducible over K. Then there is a prime $\mathfrak{P}$ of $K(\alpha)$ lying above $\mathfrak{p}$, and a prime $\mathfrak{Q}$ of $K(f^{-1}(\alpha))$, such that*

- *$\mathfrak{P}$ has ramification index m^n over $\mathfrak{p}$,*
- *$m^n v_\mathfrak{P}(\alpha/b)$ is a positive integer relatively prime to m, where $v_\mathfrak{P}$ is the $\mathfrak{P}$-adic valuation on $K(\alpha)$ extending $v_\mathfrak{p}$,*
- *$\mathfrak{Q}$ lies above $\mathfrak{P}$, and*
- *the ramification group $I(\mathfrak{Q}|\mathfrak{P})$ acts transitively on m roots of $f(x) - \alpha$ and fixes the other $d - m$ roots.*

Proof. **Step 1**. We will prove the first two bullet points by induction on $n \geq 0$. For $n = 0$, we have $\alpha = x_0$; choosing $\mathfrak{P} = \mathfrak{p}$, both points hold trivially.

Assuming they hold for $n - 1$, let $\beta = f(\alpha) \in f^{-(n-1)}(x_0)$. By our hypothesis that $f^n(x) - x_0$ is irreducible over K, the previous iterate $f^{(n-1)}(x) - x_0$ must also be irreducible. By our inductive hypothesis, there is a prime $\mathfrak{P}'$ of $K(\beta)$ with ramification index m^{n-1} over $\mathfrak{p}$, such that $m^{n-1}v_{\mathfrak{P}'}(\beta/b)$ is a positive integer relatively prime to m.

Thus, the Newton polygon of $f(x) - \beta = x^d - bx^m - \beta$ with respect to $v_{\mathfrak{P}'}$ consists of two segments: one of length m and slope $-m^{-1}v_{\mathfrak{P}'}(\beta/b) < 0$, and one of length $d - m$ and slope $-v_\mathfrak{p}(b)/(d - m)$, which is a positive integer; see Figure 1. That is, $f(x) - \beta$ factors over the local field $K(\beta)_{\mathfrak{P}'}$ as $f - \beta = gh$, where $g, h \in K(\beta)_{\mathfrak{P}'}[x]$, with $\deg(g) = m$ and $\deg(h) = d - m$. Moreover, the Newton polygon of each of g and h consists of a single segment, of slopes $-m^{-1}v_{\mathfrak{P}'}(\beta/b)$ and $-v_\mathfrak{p}(b)/(d - m)$, respectively. Since $f^n - x_0$ is irreducible, then considering the Galois extension $K_n := K(f^{-n}(x_0))$, we may apply an appropriate $\sigma \in \mathrm{Gal}(K_n/K)$ to assume that α is a root of g.

Because $v_{\mathfrak{P}'}(\beta/b) = N/m^{n-1}$ for some positive integer N relatively prime to m, and because the Newton polygon of g consists of a single segment of slope $-N/m^n$, it follows that $K(\alpha)$ has a prime $\mathfrak{P}$ of ramification index m over $\mathfrak{P}'$, and hence of index m^n over $\mathfrak{p}$, proving the first bullet point. Letting $v_{\mathfrak{P}}$ denote the $\mathfrak{P}$-adic valuation on $K(\alpha)$ extending $v_{\mathfrak{P}'}$, we have $v_{\mathfrak{P}}(\alpha) = N/m^n > 0$. Since $v_{\mathfrak{P}}(b) = v_{\mathfrak{p}}(b)$ is a negative integer, it follows that $m^n v_{\mathfrak{P}}(\alpha/b)$ is a positive integer relatively prime to m, proving the second bullet point.

Step 2. Let $L := K(f^{-1}(\alpha))$, let $\mathfrak{P}$ be a prime of $K(\alpha)$ satisfying the first two bullet points, and let $v_{\mathfrak{P}}$ be the $\mathfrak{P}$-adic valuation on $K(\alpha)$ extending $v_{\mathfrak{p}}$. As in Step 1, we may factor

$$f(x) - \alpha = g(x)h(x) \quad \text{with } g, h \in K(\alpha)_{\mathfrak{P}}[x],$$

where the Newton polygons of g and h each consist of a single segment, of length m and slope $-m^{-1}v_{\mathfrak{P}}(\alpha/b)$ for g, and of length $d-m$ and slope $\ell := -v_{\mathfrak{p}}(b)/(d-m)$ for h. In fact, if $\pi \in \mathcal{O}_K$ is a uniformizer for $\mathfrak{p}$, then the polynomial

$$F(x) := \pi^{d\ell}\Big(f\big(\pi^{-\ell}x\big) - \alpha\Big) = x^d - \pi^{(d-m)\ell}bx^m - \pi^{d\ell}\alpha \in K(\alpha)[x]$$

has $K(\alpha)_{\mathfrak{P}}$-integral coefficients, with $F \equiv x^m(x^{d-m} - c) \pmod{\mathfrak{P}}$, where $c \not\equiv 0 \pmod{\mathfrak{P}}$. Therefore, the polynomial

$$H(x) := \pi^{(d-m)\ell}h\big(\pi^{-\ell}x\big) \in K(\alpha)_{\mathfrak{P}}[x]$$

also has $K(\alpha)_{\mathfrak{P}}$-integral coefficients, and $H \equiv x^{d-m} - c \pmod{\mathfrak{P}}$. Since $\mathfrak{p} \nmid (d-m)$, the splitting field of H, and hence of h, is unramified over $\mathfrak{P}$.

Let $\mathfrak{Q}$ be any prime of L lying over $\mathfrak{P}$, and let $\gamma_1, \dots, \gamma_d$ be the roots of $f(x) - \alpha$ in the local field $L_{\mathfrak{Q}}$. By the factorization $f - \alpha = gh$ of the previous paragraph, $d - m$ of the roots (without loss, $\gamma_{m+1}, \dots, \gamma_d$) are roots of $h(x)$, and hence they lie in an unramified extension $L'_{\mathfrak{Q}}$ of $K(\alpha)_{\mathfrak{P}}$ contained in $L_{\mathfrak{Q}}$. On the other hand, the remaining roots $\gamma_1, \dots, \gamma_m$ are roots of g, which is totally ramified over $K(\alpha)_{\mathfrak{P}}$ and hence irreducible over $L'_{\mathfrak{Q}}$.

The decomposition group $D(\mathfrak{Q}|\mathfrak{P})$ is canonically isomorphic to the Galois group $\mathrm{Gal}(L_{\mathfrak{Q}}/K(\alpha)_{\mathfrak{P}})$, and the inertia group $I(\mathfrak{Q}|\mathfrak{P})$ is canonically isomorphic to the Galois group $\mathrm{Gal}(L_{\mathfrak{Q}}/L'_{\mathfrak{Q}})$. Thus, $I(\mathfrak{Q}|\mathfrak{P})$ acts transitively on the roots of g, while fixing the roots of h, as desired. □

LEMMA 2.4. *Let $d \geq 3$, let m be an integer relatively prime to d with $d/2 < m < d$, and let $G \subseteq S_d$ be a subgroup that*
- *contains a transposition,*
- *acts transitively on $\{1, 2, \dots, d\}$, and*
- *has a subgroup H that acts trivially $\{m+1, m+2, \dots, d\}$ and transitively on $\{1, 2, \dots, m\}$.*

Then $G = S_d$.

Proof. **Step 1**. Define a relation $\sim$ on $\{1, \dots, d\}$ by $x \sim y$ if either $x = y$, or the transposition (x, y) is an element of G. Clearly $\sim$ is reflexive and symmetric. It is also transitive, because if $x, y, z \in \{1, \dots, d\}$ are distinct with $x \sim y$ and $y \sim z$, then

$$(x, z) = (x, y)(y, z)(x, y) \in G, \quad \text{so } x \sim z.$$

(We also clearly have $x \sim z$ if any two of x, y, z coincide.) Thus, $\sim$ is an equivalence relation.

Step 2. We claim that each equivalence class of $\sim$ has the same size. To see this, given $x, y \in \{1, \dots, d\}$, denote by $[x]$ and $[y]$ the $\sim$-equivalence classes of x and y, respectively. Since G acts transitively, there is some $\sigma \in G$ such that $\sigma(x) = y$. Then σ maps $[x]$ into $[y]$, because for any $t \in [x]$, we have $(x,t) \in G$, and hence

$$\big(y, \sigma(t)\big) = \big(\sigma(x), \sigma(t)\big) = \sigma \circ (x,t) \circ \sigma^{-1} \in G,$$

so that $\sigma(t) \in [y]$. Similarly, σ^{-1} maps $[y]$ into $[x]$. Thus, $\sigma : [x] \to [y]$ is an invertible function, proving the claim.

Step 3. Let j denote the common size of each equivalence class of $\sim$. Then $j \geq 2$, since G contains a transposition. Also, $j|d$ by Step 2, and because $\gcd(m,d) = 1$, it follows that $j \nmid m$. Thus, there must be some $x \in \{1,\ldots,m\}$ such that $[x] \not\subseteq \{1,\ldots,m\}$. That is, there is some $y \in \{m+1,\ldots,d\}$ such that $(x,y) \in G$.

We claim that in fact, $\{1,\ldots,m\} \subseteq [y]$. Indeed, for any $t \in \{1,\ldots,m\}$, there is some $\tau \in H$ such that $\tau(x) = t$; and since H acts trivially on $\{m+1,\ldots,d\}$, we also have $\tau(y) = y$. Thus, $(y,t) = \tau \circ (x,y) \circ \tau^{-1} \in G$. That is, $t \sim y$, proving our claim.

This claim immediately implies that $j \geq m > d/2$. Since $j|d$, we must have $j = d$. Hence, the whole set $\{1,\ldots,d\}$ is a single equivalence class. That is, every transposition belongs to G; therefore, $G = S_d$. □

3. *Sufficient conditions for large arboreal Galois groups*

Our main tools for proving that certain arboreal Galois groups are as large as possible are the following theorems. We will apply the first to polynomials of degree $d \geq 4$, and the second to degrees $d = 2, 3$.

THEOREM 3.1. *Fix integers $d > m \geq 2$ with $(m,d) = 1$ and $m > d/2$. Let $b, x_0 \in K$, where we can write $x_0 = s/t$ and $b = u/w$ with $s,t,u,w \in \mathcal{O}_K$ and $(s,t) = (u,w) = 1$. Suppose that the polynomial*

$$f(x) = x^d - bx^m$$

satisfies the following properties.

(i) *there is a prime $\mathfrak{p}_1$ of $\mathcal{O}_K$ with $v_{\mathfrak{p}_1}(b) \geq 1$ and $v_{\mathfrak{p}_1}(x_0) = 1$;*
(ii) *there is a prime $\mathfrak{p}_2$ of $\mathcal{O}_K$ such that*
  (a) $\mathfrak{p}_2 \nmid (d-m)$,
  (b) $v_{\mathfrak{p}_2}(b) < \min\{v_{\mathfrak{p}_2}(x_0), 0\}$,
  (c) $(d-m)|v_{\mathfrak{p}_2}(b)$,
  (d) $\gcd(m, v_{\mathfrak{p}_2}(x_0/b)) = 1$;
(iii) *for each $n \geq 1$, there is a prime $\mathfrak{p} \nmid stuwd(d-m)$ of $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(\Delta(f^n(x) - x_0)) > 0$ is odd, and such that $v_{\mathfrak{p}}(\Delta(f^\ell(x) - x_0)) = 0$ for all $0 \leq \ell < n$.*

Then for all $n \geq 0$,

$$\mathrm{Gal}\Big(K\big(f^{-n}(x_0)\big)/K\Big) \cong [S_d]^n.$$

For quadratic and cubic polynomials, conditions (i) and (iii) of Theorem 3.1 suffice, as follows.

THEOREM 3.2. *Let $d = 2$ or $d = 3$. Let $b, x_0 \in K$, where we can write $x_0 = s/t$ and $b = u/w$ with $s,t,u,w \in \mathcal{O}_K$ and $(s,t) = (u,w) = 1$. Suppose that the polynomial*

$$f(x) = x^d - bx$$

satisfies properties (i) *and* (iii) *of Theorem 3.1, with $m = 1$. Then for all $n \geq 0$,*

$$\mathrm{Gal}\Big(K\big(f^{-n}(x_0)\big)/K\Big) \cong [S_d]^n.$$

The proofs of Theorems 3.1 and 3.2 rely on the following two results.

PROPOSITION 3.3. *Let $d, m, x_0 = s/t, b = u/w$, and f be as in Theorem 3.1 or Theorem 3.2. Then for any $n \geq 1$ and $\alpha \in f^{-(n-1)}(x_0)$, $\mathrm{Gal}(K(f^{-1}(\alpha))/K(\alpha)) \cong S_d$.*

Proof. For convenience of notation, let $G := \mathrm{Gal}(K(f^{-1}(\alpha))/K(\alpha))$, and let $\beta_1, \ldots, \beta_d$ be the roots of $f(x) - \alpha$.

Observe that $f(x) \equiv x^d \pmod{\mathfrak{p}_1[x]}$, where $\mathfrak{p}_1$ is the prime described in condition (i) of Theorem 3.1. Thus, $f^n(x) \equiv x^{d^n} \pmod{\mathfrak{p}_1[x]}$, and in addition, the constant term of $f^n(x)$ is trivial. Hence, $f^n(x) - x_0$ is Eisenstein at $\mathfrak{p}_1$ and therefore irreducible over K, of degree d^n.

Further, since $f^n(x) - x_0$ is irreducible over K, $f(x) - \alpha$ is irreducible over $K(\alpha)$ by Capelli's Lemma. In particular, G acts transitively on $\{\beta_1, \ldots, \beta_d\}$.

Let $\mathfrak{p}$ be the prime described in condition (iii) of Theorem 3.1 for $\Delta(f^n(x) - x_0)$. By equation (1) and the fact that $\mathfrak{p} \nmid stuwd$, we see that $\mathfrak{p}$ must divide

$$\prod_{i=1}^{d-m} \left(f^n(\zeta^i \eta) - x_0\right) = \prod_{\gamma \in f^{-(n-1)}(x_0)} \left(\prod_{i=1}^{d-m} \left(f(\zeta^i \eta) - \gamma\right) \right)$$

to an odd power, where η is a nonzero critical point of $f(x)$, and ζ is a primitive $(d-m)$-root of unity. Hence, there is some prime $\mathfrak{q}'$ of $K_n := K(f^{-n}(x_0))$ lying above $\mathfrak{p}$, along with some Galois conjugate α' of α, such that $\mathfrak{q}'$ divides $\prod_{i=1}^{d-m}(f(\zeta^i\eta) - \alpha')$ to an odd power. Since α' and α are conjugates, there must also be a prime $\mathfrak{q}$ lying above $\mathfrak{p}$ dividing $\prod_{i=1}^{d-m}(f(\zeta^i\eta) - \alpha)$ to an odd power. Finally, restricting $\mathfrak{q}$ to $K(\alpha)$, we see that there is a prime $\mathfrak{P}$ of $K(\alpha)$ lying above $\mathfrak{p}$ that divides $\Delta(f(x) - \alpha)$ to an odd power. Applying Lemma 2.1 to $\Delta(f(x) - \alpha)$, the prime $\mathfrak{P}$ must ramify in $K(f^{-1}(\alpha))$. By Lemma 2.2, the corresponding inertia subgroup in G must be generated by a single transposition of the roots $\{\beta_1, \ldots, \beta_d\}$.

Thus, $G = \mathrm{Gal}(K(f^{-1}(\alpha))/K(\alpha))$ is a subgroup of S_d that acts transitively on $\{\beta_1, \ldots, \beta_d\}$ and that also contains a transposition. For $d = 2$ or $d = 3$, it follows that $G \cong S_d$, proving the desired result under the hypotheses of Theorem 3.2.

For the remainder of the proof, assume the hypotheses of Theorem 3.1. Let $\mathfrak{p}_2$ be the prime described in condition (2) of that Theorem. Then Lemma 2.3 applied to $\mathfrak{p}_2$ shows that G has a subgroup H that acts transitively on m of the roots of $f(x) - \alpha$, and trivially on the remaining roots. Thus, G satisfies the hypotheses of Lemma 2.4, and hence $G \cong S_d$. □

PROPOSITION 3.4. *Let $d, m, x_0 = s/t, b = u/w$, and f be as in Theorem 3.1 or Theorem 3.2. Fix $n \geq 1$, and let $\alpha_1, \ldots, \alpha_{d^{n-1}}$ denote the roots of $f^{n-1}(x) - x_0$. For each $i = 1, \ldots, d^{n-1}$, let $M_i := K(f^{-1}(\alpha_i))$ and $\widehat{M_i} := \prod_{j \neq i} M_j$. Then $\mathrm{Gal}(K(f^{-n}(x_0))/\widehat{M_i})$ contains an element that acts as a single transposition on the elements of $f^{-1}(\alpha_i)$.*

Proof. Fix $i \in \{1, \ldots, d^{n-1}\}$. Let $\mathfrak{p}$ be the prime described in condition (iii) of Theorem 3.1 for $\Delta(f^n(x) - x_0)$. As in the proof of Proposition 3.3, there must be a prime $\mathfrak{P}$ of $K(\alpha_i)$ lying above $\mathfrak{p}$ that divides $\Delta(f(x) - \alpha_i)$ to an odd power. By Lemma 2.1 applied to $\Delta(f(x) - \alpha_i)$, the prime $\mathfrak{P}$ must ramify in $M_i = K(f^{-1}(\alpha_i))$; and by Lemma 2.2, the inertia group of $\mathfrak{P}$ in $\mathrm{Gal}(M_i/K(\alpha_i))$ is generated by an element that acts as a transposition on $f^{-1}(\alpha_i)$.

In addition, because $\mathfrak{P}$ lies over $\mathfrak{p}$, with $\mathfrak{p} \nmid \Delta(f^{n-1}(x) - x_0)$, the prime $\mathfrak{P}$ does not ramify in $K_{n-1} := K(f^{-(n-1)}(x_0))$. It suffices to show that $\mathfrak{P}$ does not ramify in $\widehat{M_i}$. Indeed, in that case, the inertia group of $\mathfrak{P}$ in $\mathrm{Gal}(\widehat{M_i}/K(\alpha_i))$ is trivial.

Suppose that there is some $j \neq i$ and some prime $\mathfrak{Q}$ of K_{n-1} with $\mathfrak{Q}|\mathfrak{P}$ and which ramifies in $K_{n-1}M_j$. Then α_j is a critical value of f modulo $\mathfrak{Q}$; but so is α_i, since $\mathfrak{P}$ ramifies in M_i. If either α_i or α_j is congruent to 0 or ∞ modulo $\mathfrak{Q}$, then $x_0 = f^{n-1}(\alpha_i) = f^{n-1}(\alpha_j)$ must also be congruent to 0 or ∞ modulo $\mathfrak{Q}$, and hence $\mathfrak{Q} \mid stuw$, contradicting the assumption that $\mathfrak{p} \nmid stuw$. Thus, α_i and α_j must be of the form $f(\eta)$ and $f(\xi)$, respectively, where η, ξ satisfy

$$\eta^{d-m} \equiv \xi^{d-m} \equiv \frac{mb}{d} \pmod{\mathfrak{Q}}.$$

Therefore, as in the proof of Lemma 2.2, there is a $(d-m)$-th root of unity ζ so that $\eta \equiv \zeta\xi \pmod{\mathfrak{Q}}$, and hence

$$\alpha_i \equiv f(\eta) \equiv \zeta^m f(\xi) \equiv \zeta^m \alpha_j \pmod{\mathfrak{Q}}.$$

Applying f^{n-1}, we have

$$x_0 = f^{n-1}(\alpha_i) \equiv \zeta^{m^n} f^{n-1}(\alpha_j) = \zeta^{m^n} x_0 \pmod{\mathfrak{Q}}.$$

Since $\mathfrak{p} \nmid (d-m)$, it follows that $\zeta^{m^n} \equiv 1 \pmod{\mathfrak{Q}}$. Therefore, because $(m, d-m) = 1$, we have $\zeta \equiv 1 \pmod{\mathfrak{Q}}$, and hence $\alpha_i \equiv \alpha_j \pmod{\mathfrak{Q}}$. But in that case, $f^{n-1}(x) - x_0$ has multiple roots modulo $\mathfrak{Q}$, yielding

$$\mathfrak{p} | \Delta(f^{n-1}(x) - x_0),$$

which is a contradiction. Thus, $\mathfrak{P}$ does not ramify in $K_{n-1}M_j$ for any $j \neq i$. Taking the compositum, $\mathfrak{P}$ does not ramify in $\widehat{M_i}$. □

Proof of Theorems 3.1 and 3.2. We proceed by induction on n. The conclusion is trivial for $n = 0$. Assuming it holds for $n-1$, we have in particular that $f^{n-1}(x) - x_0$ is irreducible over K, with roots $\alpha_1, \ldots, \alpha_{d^{n-1}}$. For each $i = 1, \ldots, d^{n-1}$, we claim that $\mathrm{Gal}(K_n/\widehat{M_i}) \cong S_d$, where $K_n := K(f^{-n}(x_0))$, and $\widehat{M_i}$ is as in Proposition 3.4.

To prove the claim, let M_i be as in Proposition 3.4, and note that

$$\mathrm{Gal}(K_n/\widehat{M_i}) \cong \mathrm{Gal}(M_i/\widehat{M_i} \cap M_i), \tag{3}$$

where the isomorphism is not just of abstract groups, but of subgroups of S_d acting on $f^{-1}(\alpha_i)$.

Since M_i and $\widehat{M_i}$ are both Galois extensions of $K(\alpha_i)$, their subfield $M_i \cap \widehat{M_i}$ is also Galois over $K(\alpha_i)$. Hence, $\mathrm{Gal}(M_i/\widehat{M_i} \cap M_i)$ is a normal subgroup of $\mathrm{Gal}(M_i/K(\alpha_i))$, which is isomorphic to S_d, by Proposition 3.3. On the other hand, by Proposition 3.4, the isomorphic group $\mathrm{Gal}(K_n/\widehat{M_i})$ contains a transposition. By equation (3), $\mathrm{Gal}(K_n/\widehat{M_i})$ is a normal subgroup of S_d that contains a transposition, and therefore it is all of S_d, as claimed.

Thus, for each $i = 1, \ldots, d^{n-1}$, we see that $\mathrm{Gal}(K_n/K_{n-1})$ contains a subgroup H_i isomorphic to S_d and which acts trivially on $f^{-1}(\alpha_j)$ for each $j \neq i$. It follows that $\mathrm{Gal}(K_n/K_{n-1})$ contains a subgroup $H := \prod_i H_i$ of order $(d!)^{d^{n-1}}$. Hence, $\mathrm{Gal}(K_n/K)$ is isomorphic to a subgroup of $[S_d]^n$ of order at least

$$\big|\mathrm{Gal}(K_{n-1}/K)\big| \cdot |H| = \big|[S_d]^{d^{n-1}}\big| (d!)^{d^{n-1}} = (d!)^{1+d+\cdots+d^{n-2}+d^{n-1}} = \big|[S_d]^n\big|.$$

Therefore, $\mathrm{Gal}(K_n/K) \cong [S_d]^n$, as desired. □

4. *Proof of Odoni's Conjecture for d even*

We now prove Theorem 1.1 for even degree d:

THEOREM 4.1. *Let K be a number field, and let $d \geq 2$ be an even integer. Then there is a monic polynomial $f(x) \in K[x]$ of degree d and a rational point $x_0 \in K$ such that for all $n \geq 0$,*

$$\mathrm{Gal}\Big(K\big(f^{-n}(x_0)\big)/K\Big) \cong [S_d]^n.$$

Before proving Theorem 4.1, we need one more lemma.

LEMMA 4.2. *Let $d \ge 2$ be an integer, let K be a number field with ring of integers $\mathcal{O}_K$, and let $s,t \in \mathcal{O}_K$. Suppose that $s(d-1)$ and $dt(s^{d-1}+t^{d-1})$ are relatively prime. Let $x_0 = s/t$ and*

$$f(x) = x^d - bx^{d-1} \in K[x], \quad \text{where } b = \frac{x_0^d}{x_0^{d-1}+1} = \frac{s^d}{t(s^{d-1}+t^{d-1})}.$$

Let $\eta = (d-1)b/d$ be the unique nonzero critical point of f. Then for every $n \ge 1$,

$$F_n := s^{-1}\Big(dt\big(s^{d-1}+t^{d-1}\big)\Big)^{d^n}\big[f^n(\eta) - x_0\big] \tag{4}$$

is an $\mathcal{O}_K$-integer relatively prime to $d(d-1)st(s^{d-1}+t^{d-1})$. Moreover, if uF_n is not a square in K for any unit $u \in \mathcal{O}_K^\times$, then there is a prime $\mathfrak{q} \nmid d(d-1)st(s^{d-1}+t^{d-1})$ of $\mathcal{O}_K$ dividing $\Delta(f^n(x)-x_0)$ to an odd power, and such that $v_{\mathfrak{q}}\big(\Delta(f^\ell(x)-x_0)\big) = 0$ for all $0 \le \ell < n$.

Proof. Let $D = s^{d-1}+t^{d-1}$. We claim that for any $n \ge 1$,

$$(dtD)^{d^n} f^n(\eta) = s^{de_n}(d-1)^{(d-1)^n} M_n \tag{5}$$

where $M_n \in \mathcal{O}_K$ is relatively prime to $d(d-1)stD$, and where

$$e_n = (d-1)^n + (d-1)^{n-1} + \cdots + (d-1) + 1.$$

Proceeding by induction on n, a direct computation shows

$$f(\eta) = -(d-1)^{d-1}\Big(\frac{b}{d}\Big)^d = \frac{-(d-1)^{d-1}s^{d^2}}{\big(dtD\big)^d}, \tag{6}$$

proving the claim for $n=1$, with $M_1 = -1$. Given the claim for a particular $n \ge 1$, we have

$$\frac{(dtD)^{d^{n+1}} f^{n+1}(\eta)}{(d-1)^{(d-1)^{n+1}} s^{de_{n+1}} M_n^{d-1}} = (d-1)^{(d-1)^n} s^{d(e_n-1)} M_n - d^{d^n}(tD)^{d^n-1},$$

since $e_{n+1} = (d-1)e_n + 1$. Setting

$$M_{n+1} := M_n^{d-1}\Big((d-1)^{(d-1)^n} s^{d(e_n-1)} M_n - d^{d^n}(tD)^{d^n-1}\Big) \in \mathcal{O}_K,$$

we see that M_{n+1} is relatively prime to $d(d-1)stD$, proving the claim.

Fix $n \ge 1$. It is immediate from equations (4) and (5) that

$$F_n = s^{de_n-1}(d-1)^{(d-1)^n} M_n - d^{d^n}(tD)^{d^n-1} \in \mathcal{O}_K,$$

which is relatively prime to $d(d-1)stD$, as desired.

For the remainder of the proof, assume that uF_n is not a square in $\mathcal{O}_K$ for any unit $u \in \mathcal{O}_K^\times$. Then there is a prime $\mathfrak{q}$ of $\mathcal{O}_K$ dividing F_n to an odd power. We must have $\mathfrak{q} \nmid d(d-1)stD$.

The factor consisting of the product over critical points in discriminant formula (1) for $\Delta(f^n(x)-x_0)$ is

$$(-x_0)^{d-2}(f^n(\eta) - x_0) = \frac{-s^{d-1}F_n}{t^{d^n+d-2}(dD)^{d^n}}.$$

Thus, $\mathfrak{q}$ divides this factor to an odd power. By formula (1), then, it suffices to show that

$$v_{\mathfrak{q}}\Big(\Delta\big(f^\ell(x) - c\big)\Big) = 0 \quad \text{for all} \quad 0 \le \ell \le n-1. \tag{7}$$

Suppose not. Let $0 \le \ell \le n-1$ be the smallest index for which equation (7) fails. Then by formula (1) again, we must have

$$v_{\mathfrak{q}}\big(f^\ell(\eta) - x_0\big) \ge 1, \quad \text{i.e.,} \quad f^\ell(\eta) \equiv x_0 \pmod{\mathfrak{q}}.$$

Thus,

$$f^{\ell+1}(\eta) \equiv b \pmod{\mathfrak{q}}, \quad \text{and} \quad f^{\ell+j}(\eta) \equiv 0 \pmod{\mathfrak{q}} \quad \text{for all} \quad j \geq 2.$$

Therefore, $f^n(\eta)$ is congruent to either b or 0 modulo $\mathfrak{q}$. However, $f^n(\eta) \equiv x_0 \pmod{\mathfrak{q}}$, and $x_0 \not\equiv b, 0 \pmod{\mathfrak{q}}$, since $x_0 - b = -st^{d-2}/D$ and $\mathfrak{q} \nmid stD$. This contradiction proves equation (7) and hence the Lemma. □

Proof of Theorem 4.1. Fix $d \geq 2$ even. It suffices to show that there is some $f(x) \in K[z]$ satisfying the hypotheses of Theorem 3.1 or 3.2, with $\deg(f) = d$.

Step 1. We will show that there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that all units $u \in \mathcal{O}_K^\times$ are squares modulo $\mathfrak{p}$, and so is $1-d$, with $\mathfrak{p} \nmid d(d-1)$. To do so, let $u_1, \ldots, u_r$ be generators of the (finitely-generated) unit group $\mathcal{O}_K^\times$. It suffices to find a prime $\mathfrak{p} \nmid d(d-1)$ for which each of $1-d, u_1, \ldots, u_r$ is a square modulo $\mathfrak{p}$.

Let $L = K(\sqrt{1-d}, \sqrt{u_1}, \ldots, \sqrt{u_r})$, which is a Galois extension of K. By the Chebotarev Density Theorem, there are infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_K$ at which Frobenius acts trivially on L modulo $\mathfrak{p}$. Choosing any such prime $\mathfrak{p}$ that does not ramify in L and does not divide $d(d-1)$, it follows that each of $1-d, u_1, \ldots, u_r$ have square roots modulo $\mathfrak{p}$, as desired.

Step 2. Let $\mathfrak{p}_1$ be a prime of $\mathcal{O}_K$ not dividing $d(d-1)\mathfrak{p}$. Choose $s_0 \in \mathcal{O}_K$ that is not a square modulo $\mathfrak{p}$, and choose $s_1 \in \mathcal{O}_K$ with $v_{\mathfrak{p}_1}(s_1) = 1$. Since the three ideals $d(d-1)$, $\mathfrak{p}$, and $\mathfrak{p}_1^2$ are pairwise relatively prime, the Chinese Remainder Theorem shows that there is some $s \in \mathcal{O}_K$ such that

$$s \equiv 1 \pmod{d(d-1)}, \quad s \equiv s_0 \pmod{\mathfrak{p}}, \quad \text{and} \quad s \equiv s_1 \pmod{\mathfrak{p}_1^2}.$$

Thus, s is not a square modulo $\mathfrak{p}$, and $v_{\mathfrak{p}_1}(s) = 1$.

Choose $t_0 \in \mathcal{O}_K$ with $v_{\mathfrak{p}}(t_0) = 1$. Since the ideals $s(d-1)$ and $\mathfrak{p}^2$ are relatively prime, the Chinese Remainder Theorem shows that there is some $t \in \mathcal{O}_K$ such that

$$t \equiv 1 \pmod{s(d-1)}, \quad \text{and} \quad t \equiv t_0 - s \pmod{\mathfrak{p}^2}.$$

In particular,

$$\begin{aligned} s^{d-1} + t^{d-1} &\equiv s^{d-1} + (t_0 - s)^{d-1} \equiv s^{d-1} + \big(-s^{d-1} + (d-1)s^{d-2}t_0 \big) \\ &\equiv (d-1)s^{d-2}t_0 \pmod{\mathfrak{p}^2}, \end{aligned}$$

and therefore $v_{\mathfrak{p}}(s^{d-1} + t^{d-1}) = v_{\mathfrak{p}}(t_0) = 1$. In addition,

$$s^{d-1} + t^{d-1} \equiv 2 \pmod{d-1},$$

and hence $d-1$ and $s^{d-1} + t^{d-1}$ are relatively prime, since $d-1$ is odd.

Let $\mathfrak{p}_2 = \mathfrak{p}$. By our choices above, note that s and dt are also relatively prime, and so are t and $d-1$. Thus,

$$s(d-1) \quad \text{and} \quad dt(s^{d-1} + t^{d-1}) \quad \text{are relatively prime}$$

as elements of $\mathcal{O}_K$. Hence, setting $x_0 = s/t$ and $b = s^d/(t(s^{d-1} + t^{d-1}))$, we have

$$v_{\mathfrak{p}_1}(x_0) = 1, \quad v_{\mathfrak{p}_1}(b) = d, \quad v_{\mathfrak{p}_2}(x_0) = 0, \quad \text{and} \quad v_{\mathfrak{p}_2}(b) = -1. \tag{8}$$

Define $f \in K[x]$ by $f(x) = x^d - bx^{d-1}$.

Step 3. Let $m = d-1$. If $d = 2$, then f is of the form of Theorem 3.2, and the relations (8) show that f satisfies condition (i) of Theorem 3.1. Similarly, if $d \geq 4$, then f is of the form of Theorem 3.1, and relations (8) show that f satisfies conditions (i) and (ii) of that Theorem. In both cases, we claim that for each $n \geq 1$, the quantity F_n of equation (4) is not a square modulo $\mathfrak{p} = \mathfrak{p}_2$. Since all units of $\mathcal{O}_K$ are squares modulo $\mathfrak{p}$, Lemma 4.2 will then guarantee that condition (iii) of Theorem 3.1 also holds, yielding the desired result. Thus, it suffices to prove our claim: F_n is not a square modulo $\mathfrak{p}$, for every $n \geq 1$.

Write $D = s^{d-1} + t^{d-1}$, so that $b = s^d/(tD)$, and $v_{\mathfrak{p}}(D) = 1$. Let $\eta = (d-1)b/d$, which is the only critical point of f besides 0 and ∞. Then for all $n \geq 1$, observe that

$$(dtD)^{d^n} f^n(\eta) \equiv \Big(-(d-1)^{d-1} s^{d^2} \Big)^{d^{n-1}} \pmod{dtD}. \tag{9}$$

Indeed, for $n = 1$, equation (9) is immediate from equation (6). For $n \geq 2$, we have

$$(dtD)^{d\ell} f\left(\frac{y}{(dtD)^{\ell}} \right) \equiv y^d \pmod{dtD}$$

for $y \in \mathcal{O}_K$ relatively prime to dtD and $\ell \geq 2$, and hence equation (9) follows by induction on n.

Equation (9) shows that $(dtD)^{d^n} f^n(\eta)$ is a nonzero square modulo $\mathfrak{p}$ for every $n \geq 1$. (For $n = 1$, recall that $1 - d$ is a square modulo $\mathfrak{p}$.) In addition, $(dtD)^{d^n} x_0 \equiv 0 \pmod{\mathfrak{p}}$. Thus, from the definition of F_n in equation (4), we see that sF_n is a nonzero square modulo $\mathfrak{p}$. Since s is not a square modulo $\mathfrak{p}$, we have proven our claim and hence the Theorem. □

5. *Proof of Odoni's Conjecture for d odd, for most K*

We now prove Theorem 1.1 for odd degree d:

THEOREM 5.1. *Let $d \geq 3$ be an odd integer, and let K be a number field in which d and $d-2$ are not both squares. Then there is a monic polynomial $f(x) \in K[x]$ of degree d and a rational point $x_0 \in K$ such that for all $n \geq 0$,*

$$\operatorname{Gal}\Big(K\big(f^{-n}(x_0)\big)/K \Big) \cong [S_d]^n.$$

Note that if $[K : \mathbb{Q}]$ is odd, then Theorem 5.1 yields Odoni's conjecture in all odd degrees $d \geq 3$. After all, for $d \geq 3$ odd, at least one of d and $d-2$ is not a square in $\mathbb{Q}$. Thus, any number field of odd degree over $\mathbb{Q}$ cannot contain square roots of both d and $d-2$.

Before proving Theorem 5.1, we need one more lemma.

LEMMA 5.2. *Let $d \geq 3$ be an odd integer, let K be a number field with ring of integers $\mathcal{O}_K$, and let $s, t \in \mathcal{O}_K$. Suppose that $2(d-2)s$ and dt are relatively prime. Let $x_0 = s/t$ and*

$$f(x) = x^d - bx^{d-2} \in \mathbb{Q}[x], \quad \text{where } b = x_0^2 = \frac{s^2}{t^2}.$$

Let $\pm\eta = \pm x_0\sqrt{(d-2)/d}$ be the two nonzero critical points of f. Then for every $n \geq 1$,

$$F_n := s^{-2}\big(dt^2\big)^{d^n} \big[f^n(\eta)^2 - x_0^2 \big] \tag{10}$$

is an $\mathcal{O}_K$-integer relatively prime to $2d(d-2)st$. Moreover, if uF_n is not a square in K for any unit $u \in \mathcal{O}_K^{\times}$, then there is a prime $\mathfrak{q} \nmid 2d(d-2)st$ of $\mathcal{O}_K$ dividing $\Delta(f^n(x) - x_0)$ to an odd power, and such that $v_{\mathfrak{q}}\big(\Delta(f^{\ell}(x) - x_0)\big) = 0$ for all $0 \leq \ell < n$.

Proof. We claim that for any $n \geq 1$,

$$(dt^2)^{d^n} f^n(\eta)^2 = 4^{(d-2)^{n-1}} (d-2)^{(d-2)^n} s^{2e_n} M_n^2 \tag{11}$$

where $M_n \in \mathcal{O}_K$ is relatively prime to $2d(d-2)st$, and where

$$e_n = (d-2)^n + 2(d-2)^{n-1} + \cdots + 2(d-2) + 2.$$

Observe that $f(\sqrt{x})^2 = x^{d-2}(x-b)^2$. Thus, we have $f^n(\eta)^2 = g^n(\eta^2)$, where

$$g(x) = x^{d-2}(x-b)^2.$$

Since $\eta^2 = (d-2)x_0^2/d$, a direct computation shows

$$f(\eta)^2 = g(\eta^2) = \frac{\big((d-2)s^2\big)^{d-2}}{(dt^2)^{d-2}}\left(\frac{(d-2)s^2}{dt^2} - \frac{s^2}{t^2}\right) = \frac{4(d-2)^{d-2}s^{2d}}{(dt^2)^d}, \tag{12}$$

proving the claim for $n=1$, with $M_1 = 1$. Assuming equation (11) holds for a particular $n \geq 1$, we have

$$\frac{(dt^2)^{d^{n+1}} f^{n+1}(\eta)}{4^{(d-2)^n}(d-2)^{(d-2)^{n+1}} s^{2e_{n+1}} M_n^{2(d-2)}} = \Big(4^{(d-2)^{n-1}}(d-2)^{(d-2)^n} s^{2e_n-2} M_n^2 - d^{d^n} t^{2(d^n-1)}\Big)^2,$$

since $e_{n+1} = (d-2)e_n + 2$. Setting

$$M_{n+1} := M_n^{d-2}\Big(4^{(d-2)^{n-1}}(d-2)^{(d-2)^n} s^{2e_n-2} M_n^2 - d^{d^n} t^{2(d^n-1)}\Big) \in \mathcal{O}_K,$$

we see that M_{n+1} is relatively prime to $2std(d-2)$, proving the claim.

Fix $n \geq 1$. It is immediate from equations (10) and (11) that

$$F_n = 4^{(d-2)^{n-1}}(d-2)^{(d-2)^n} s^{2e_n-2} M_n^2 - d^{d^n} t^{2d^n-2} \in \mathcal{O}_K,$$

which is relatively prime to $2d(d-2)st$, as desired.

For the remainder of the proof, assume that uF_n is not a square in $\mathcal{O}_K$ for any unit $u \in \mathcal{O}_K^\times$. Then there is a prime $\mathfrak{q}$ of $\mathcal{O}_K$ dividing F_n to an odd power. We must have $\mathfrak{q} \nmid 2d(d-2)st$.

The factor consisting of the product over critical points in discriminant formula (1) for $\Delta(f^n(x) - x_0)$ is

$$-x_0^{d-3}(f^n(\eta)^2 - x_0^2) = \frac{-s^{d-1}F_n}{d^{d^n}t^{2d^n+d-3}}.$$

Thus, $\mathfrak{q}$ divides this factor to an odd power. By formula (1), then, it suffices to show that

$$v_{\mathfrak{q}}\Big(\Delta\big(f^\ell(x) - c\big)\Big) = 0 \quad \text{for all} \quad 0 \leq \ell \leq n-1. \tag{13}$$

Suppose not. Let $0 \leq \ell \leq n-1$ be the smallest index for which equation (13) fails. Then by formula (1) again, we must have

$$v_{\mathfrak{q}}\big(f^\ell(\eta)^2 - x_0^2\big) \geq 1, \quad \text{i.e.,} \quad f^\ell(\eta) \equiv x_0 \text{ or } f^\ell(-\eta) \equiv x_0 \pmod{\mathfrak{q}}.$$

Without loss, assume $f^\ell(\eta) \equiv x_0 \pmod{\mathfrak{q}}$. Then $f^{\ell+j}(\eta) \equiv 0 \pmod{\mathfrak{q}}$ for all $j \geq 1$. In particular, $f^n(\eta) \equiv 0 \pmod{\mathfrak{q}}$. However,

$$f^n(\eta) \equiv x_0 \not\equiv 0 \pmod{\mathfrak{q}}.$$

This contradiction proves equation (13) and hence the Lemma. □

Proof of Theorem 5.1. Fix $d \geq 3$ odd. It suffices to show that there is some $f(x) \in K[z]$ satisfying the hypotheses of Theorem 3.1 or 3.2, with $\deg(f) = d$.

Case 1: d is not a square in K; Step 1. We first show that there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that all units $u \in \mathcal{O}_K^\times$ are squares modulo $\mathfrak{p}$, with $\mathfrak{p} \nmid 2d(d-2)$, and such that d is not a square modulo $\mathfrak{p}$, by adjusting the method of Step 1 of the proof of Theorem 4.1 with inspiration from well-known argument of Hall [**3**].

Let $\mathfrak{q}$ be a prime of $\mathcal{O}_K$ dividing d to an odd power; note that $\mathfrak{q}$ lies above an odd prime of $\mathbb{Z}$. Let $u_1, \ldots, u_r$ be generators of the (finitely-generated) unit group $\mathcal{O}_K^\times$, and let $L = K(\sqrt{u_1}, \ldots, \sqrt{u_r})$. The discriminant $\Delta(L/K)$ must divide a power of 2, and hence $\mathfrak{q}$ cannot ramify in L. However, $\mathfrak{q}$ ramifies in $K(\sqrt{d})$, and therefore $K(\sqrt{d}) \cap L = K$. It follows that $L(\sqrt{d})/L$ is a quadratic extension.

Therefore, there exists $\sigma \in \mathrm{Gal}(L(\sqrt{d})/L) \subseteq \mathrm{Gal}(L(\sqrt{d})/K)$ that fixes $\sqrt{u_1}, \ldots, \sqrt{u_r}$ but has $\sigma(\sqrt{d}) = -\sqrt{d}$. By the Chebotarev Density Theorem, there are infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_K$ at which Frobenius acts trivially on L modulo $\mathfrak{p}$, but nontrivially on $\sqrt{d}$. Choosing any such prime $\mathfrak{p}_1$ that does not ramify in L and does not divide $2d(d-2)$, it follows that all units of $\mathcal{O}_K$ are squares modulo $\mathfrak{p}_1$, but d is not.

Case 1, Step 2. Let $\mathfrak{p}_1$ be the prime of $\mathcal{O}_K$ found in Step 1, and choose $s \in \mathcal{O}_K$ relatively prime to d such that $v_{\mathfrak{p}_1}(s) = 1$. Let $\mathfrak{p}_2$ be a prime of $\mathcal{O}_K$ not dividing $2d(d-2)s$, and choose $t \in \mathcal{O}_K$ relatively prime to $2(d-2)s$ such that $v_{\mathfrak{p}_2}(t) = 1$. Let $x_0 = s/t$ and $b = x_0^2$, so that

$$v_{\mathfrak{p}_1}(x_0) = 1, \quad v_{\mathfrak{p}_1}(b) = 2, \quad v_{\mathfrak{p}_2}(x_0) = -1, \quad \text{and} \quad v_{\mathfrak{p}_2}(b) = -2. \tag{14}$$

Define $f \in K[x]$ by $f(x) = x^d - bx^{d-1}$.

Case 1, Step 3. Let $m = d-2$. If $d = 3$, then f is of the form of Theorem 3.2, and the relations (14) show that f satisfies condition (i) of Theorem 3.1. Similarly, if $d \geq 5$, then f is of the form of Theorem 3.1, and relations (14) show that f satisfies conditions (i) and (ii) of that Theorem. In both cases, we claim that for each $n \geq 1$, the quantity F_n of equation (10) is not a square modulo $\mathfrak{p} = \mathfrak{p}_1$. Since all units of $\mathcal{O}_K$ are squares modulo $\mathfrak{p}$, Lemma 5.2 will then guarantee that condition (iii) of Theorem 3.1 also holds, yielding the desired result. Thus, it suffices to prove our claim: F_n is not a square modulo $\mathfrak{p}$, for every $n \geq 1$.

Let $\eta = x_0\sqrt{(d-2)/d}$, so that $\pm\eta$ are the only two critical points of f besides 0 and ∞. Then for all $n \geq 1$, observe that

$$s^{-2} f^n(\eta)^2 \equiv 0 \pmod{s}, \tag{15}$$

since equation (11) shows $f^n(\eta)^2$ is divisible by a higher power of s.

Combining the definition of F_n in equation (10) and equation (15), we have

$$F_n \equiv -d^{d^n} t^{2d^n-2} \pmod{\mathfrak{p}},$$

since $\mathfrak{p} = \mathfrak{p}_1 | s$. Since d is odd and not a square modulo $\mathfrak{p}$, we have proven our claim and hence Case 1 of the Theorem.

Case 2: $d-2$ **is not a square in** K**; Step 1**. By the same argument as in Case 1, Step 1, but this time with the odd number $d-2$ in place of d, there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that all units $u \in \mathcal{O}_K^\times$ are squares modulo $\mathfrak{p}$, with $\mathfrak{p} \nmid 2d(d-2)$, and such that $d-2$ is not a square modulo $\mathfrak{p}$.

Case 2, Step 2. Let $\mathfrak{p}_2$ be the prime $\mathfrak{p}$ of $\mathcal{O}_K$ found in Step 1, and choose $t \in \mathcal{O}_K$ relatively prime to $2(d-2)$ such that $v_{\mathfrak{p}_2}(t) = 1$. Let $\mathfrak{p}_1$ be a prime of $\mathcal{O}_K$ not dividing $2d(d-2)t$, and choose $s \in \mathcal{O}_K$ relatively prime to dt such that $v_{\mathfrak{p}_1}(s) = 1$. Let $x_0 = s/t$ and $b = x_0^2$, and define $f \in K[x]$ by $f(x) = x^d - bx^{d-2}$.

Case 2, Step 3. Since $d-2$ is not a square, we have $d \geq 5$. As in Case 1, relations (14) hold, and they show that f satisfies conditions (1) and (2) of Theorem 3.1, with $m = d-2$, and hence $d - m = 2$. Also as in Case 1, it then suffices to prove the following claim: that for each $n \geq 1$, the quantity F_n is not a square modulo $\mathfrak{p} = \mathfrak{p}_2$.

As before, let $\eta = x_0\sqrt{(d-2)/d}$. Then for all $n \geq 1$, observe that

$$(dt^2)^{d^n} f^n(\eta)^2 \equiv \left(4(d-2)^{d-2}s^{2d}\right)^{d^{n-1}} \pmod{dt^2}. \tag{16}$$

Indeed, for $n = 1$, equation (16) is immediate from equation (12). For $n \geq 2$, we have

$$(dt^2)^{d\ell} f\left(\frac{\sqrt{y}}{(dt^2)^{\ell/2}}\right)^2 \equiv y^d \pmod{dt^2}$$

for $y \in \mathcal{O}_K$ relatively prime to dt and for $\ell \geq 2$. Hence, equation (16) follows by induction on n.

Since d is odd and $d-2$ is not a square modulo $\mathfrak{p}$, equation (16) shows that the quantity $s^{-2}(dt^2)^{d^n} f^n(\eta)^2$ is a nonsquare modulo $\mathfrak{p}$ for every $n \geq 1$. In addition, $(dt^2)^{d^n} x_0 \equiv 0 \pmod{\mathfrak{p}}$, since $\mathfrak{p} = \mathfrak{p}_2 | t$. Thus, from the definition of F_n in equation (10), we have proven our claim and hence the Theorem. □

References

1. Wayne Aitken, Farshid Hajir, and Christian Maire, *Finitely ramified iterated extensions*, Int. Math. Res. Not. (2005), no. 14, 855–880.
2. N. Boston and R. Jones, *The image of an arboreal Galois representation*, Pure Appl. Math. Q. **5** (2009), no. 1, 213–225.
3. Marshall Hall, *Quadratic reciprocity in factorizations*, Bull. Amer. Math. Soc. (1933), no. 39, 758–763.
4. G. J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.
5. R. Jones, *Galois representations from pre-image trees: an arboreal survey*, Publ. Math. Besançon (2013), 107–136.
6. J. Juul, *Iterates of generic polynomials and generic rational functions*, Available at `arXiv:1410.3814`, 26 pages, 2017.
7. Borys Kadets, *Large arboreal Galois representations*, Available at `arXiv:1802.09074`, 12 pages, 2018.
8. N.R. Looper, *Dynamical Galois groups of trinomials and Odoni's conjecture*, Available at `arXiv:1609.03398`, 14 pages, 2016.
9. R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414.
10. R. W. K. Odoni, *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \cdots w_n$, J. London Math. Soc. (2) **32** (1985), no. 1, 1–11.
11. Joel Specter, *Polynomials with surjective arboreal Galois representations exist in every degree*, Available at `arXiv:1803.00434`, 16 pages, 2018.
12. M. Stoll, *Galois groups over* $\mathbf{Q}$ *of some iterated polynomials*, Arch. Math. (Basel) **59** (1992), no. 3, 239–244.

Robert L. Benedetto and Jamie Juul
Amherst College, Amherst, MA
USA

rlbenedetto@amherst.edu
jamie.l.rahr@gmail.com