TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 371, Number 2, 15 January 2019, Pages 809–831
http://dx.doi.org/10.1090/tran/7229
Article electronically published on April 25, 2018

ITERATES OF GENERIC POLYNOMIALS AND GENERIC RATIONAL FUNCTIONS

J. JUUL

Dedicated to R.W.K. Odoni

Abstract. In 1985, Odoni showed that in characteristic 0 the Galois group of the n-th iterate of the generic polynomial with degree d is as large as possible. That is, he showed that this Galois group is the n-th wreath power of the symmetric group S_d. We generalize this result to positive characteristic, as well as to the generic rational function. These results can be applied to prove certain density results in number theory, two of which are presented here. This work was partially completed by the late R.W.K. Odoni in an unpublished paper.

Several of the results proven in this paper were stated and proven by R.W.K. Odoni in an unpublished preprint, including the polynomial versions of the Galois theoretic results and the application presented in Section 6.2. Although the results and arguments given by Odoni in that manuscript are presented somewhat differently here, his work on this project was invaluable in the completion of this paper.

1. Introduction

Given a field K and a rational function $\varphi \in K(x)$, we can form a sequence of fields by adjoining the roots of successive iterates of φ. The Galois groups of these field extensions have been studied since the 1980's beginning with the work of R.W.K. Odoni [Odo85]. The area has seen a recent surge of interest due to its many applications to density questions in number theory [Sto92] [Jon08] [HJM15] [JM14] [JKMT16].

In his original paper [Odo85], Odoni showed that if K is a number field, or more generally a Hilbertian field with characteristic 0, then for any n, most polynomials will have the property that the Galois group of the field extension formed by adjoining the roots of the n-th iterate is as large as possible. This follows directly from his result that the generic polynomial over any field of characteristic 0 has this property. We generalize this result to rational functions defined over Hilbertian fields with arbitrary characteristic and polynomial functions defined over Hilbertian fields when the degree of the polynomial and the characteristic of the field are not both 2. A *Hilbertian field* is a field K in which for any irreducible polynomial $f(t_1, \ldots, t_r, x) \in K[t_1, \ldots, t_r, x]$ there exists $a_1, \ldots, a_r \in K$ such that

Received by the editors May 13, 2015, and, in revised form, March 16, 2016 and January 22, 2017.

2010 *Mathematics Subject Classification.* Primary 37P05; Secondary 11G35, 14G25, 12F10.

This work was partially supported by NSF grant DMS-1200749.

$f(a_1, \ldots, a_r, x)$ is irreducible in $K[x]$. Examples of Hilbertian fields include $\mathbb{Q}$, number fields, and finite extensions of $k(t)$ for any field k [FJ08].

If $\varphi(x)$ is any rational function in $K(x)$, where K is a field, $\mathrm{Gal}(\varphi(x)/K)$ will denote the Galois group of the splitting field of $\varphi(x)$ over K. Let k be any field and let $s_0, s_1, \ldots, s_{d-1}, u_0, u_1, \ldots, u_d, x$ be independent indeterminants over k. The polynomial

$$\mathfrak{G}(x) = x^d + s_{d-1}x^{d-1} + \cdots + s_0$$

is the *generic monic polynomial* of degree d over k. The rational function

$$\Phi(x) = \frac{x^d + s_{d-1}x^{d-1} + \cdots + s_0}{u_d x^d + u_{d-1}x^{k-1} + \cdots + u_0}$$

is the *generic rational function* of degree d over k.

Define the field $k(\mathbf{s})$ by $k(\mathbf{s}) := k(s_0, s_1, \ldots, s_{d-1})$ and similarly define $k(\mathbf{s},\mathbf{u}) := k(s_0, s_1, \ldots, s_{d-1}, u_0, u_1, \ldots, u_d)$. In [Odo85], Odoni shows that if $\operatorname{char} k = 0$, then $\mathrm{Gal}(\mathfrak{G}^n(x)/k(\mathbf{s}))$ is isomorphic to $[S_d]^n$, the n-th wreath power of the symmetric group S_d. This group can be thought of as the group of automorphisms of the d-ary rooted tree up to the n-th level. Wreath products are defined in Section 2.1.

Some of the arguments used in [Odo85] do not extend to positive characteristic, such as those dealing with the theory of monodromy groups on compact Riemann surfaces and branch points of algebraic functions over $\mathbb{C}$. Here, we instead use algebraic and Galois theoretic arguments to show the following.

Theorem 1.1. *For any field k, $d > 1$, and $n \in \mathbb{N}$,* $\mathrm{Gal}(\Phi^n(x)/k(\boldsymbol{s},\boldsymbol{u})) \cong [S_d]^n$ *and if $(d,p) \neq (2,2)$, then* $\mathrm{Gal}(\mathfrak{G}^n(x)/k(\boldsymbol{s})) \cong [S_d]^n$.

It can be easily shown that $\mathrm{Gal}(\mathfrak{G}^n(x)/k(\mathbf{s}))$ and $\mathrm{Gal}(\Phi^n(x)/k(\mathbf{s},\mathbf{u}))$ must be contained in $[S_d]^n$. The majority of the work in this paper involves showing that these Galois groups contain $[S_d]^n$ as well.

First, note that by passing to an algebraic closure of k these Galois groups can only decrease in size. So we may replace k with an algebraic closure of k and prove the result in this case. Let $f(x) \in k[x]$ be any polynomial with degree d, and let t be transcendental over k. If we define $g(x) := f(x+t)-t$, then $g^n(x) = f^n(x+t)-t$ for any $n \in \mathbb{N}$. So it follows that $\mathrm{Gal}(g^n(x)/k(t)) \cong \mathrm{Gal}(f^n(x) - t/k(t))$ for any $n \in \mathbb{N}$. Then, since $g^n(x)$ is a specialization of both $\mathfrak{G}^n(x)$ and $\Phi^n(x)$, for any n, and Galois groups cannot increase under specializations, it will suffice to show that there exists some $f(x) \in k[x]$ such that $\mathrm{Gal}(f^n(x) - t/k(t)) \cong [S_d]^n$.

In Theorem 3.1, we give sufficient conditions on rational functions $\varphi(x) \in k(x)$ to ensure that $\mathrm{Gal}(\varphi^n(x) - t/k(t)) \cong [S_d]^n$. Then in Theorem 3.7, we show that in fact "most" polynomials in $k[x]$ satisfy these conditions.

The proof of Theorem 3.1 is by induction on n. The main tool used in the inductive step is "disjoint ramification" of primes; that is, we show that in each subextension of the splitting field of $\varphi^n(x) - t$ formed by adjoining α and $\varphi^{-1}(\alpha)$ where $\alpha \in \varphi^{-(n-1)}(t)$, there is a prime that ramifies which ramifies in no other such subextension. The arguments here are similar to the arguments given in [JKMT16].

We give some preliminary results in Section 2. We prove Theorem 1.1 in Section 4. In Section 5, we handle the case $\operatorname{char} k = d = 2$. In this case it is worth noting that rational functions behave as in all the other cases, whereas the results for polynomials are markedly different. The difference follows from the fact that these polynomials are always post-critically finite.

Finally, in Section 6 we give two applications using these results along with appropriate versions of the Chebotarev Density Theorem. We first use Theorem 1.1 to extend Odoni's application on primes dividing orbits ([Odo85], Lemma 9.1) to global fields in any characteristic, where by global field we mean a number field or a function field of an algebraic curve over a finite field.

In the second application, we consider factorizations of iterates of polynomials. Let $\pi = (1)^{r_1} \dots (m)^{r_m}$ be a cycle pattern in S_m. We say that a squarefree polynomial $f(x)$ of degree m has cycle pattern π if $f(x)$ has exactly r_i irreducible factors of degree i for all $1 \leq i \leq m$. If π is a *cycle pattern* in S_{d^n}, let $A(q,b,d,n,\pi)$ be the set of all $f(x) \in \mathbb{F}_q[x]$ such that $\deg f(x) = d$, $f(x)$ has leading coefficient b, $f^n(x)$ is squarefree, and $f^n(x)$ has cycle pattern π. We show there is an $M = M(d,n) > 0$ in $\mathbb{R}$ and $q_0(d,n) \geq 2$ in $\mathbb{N}$ such that

$$|\#A(q,b,d,n,\pi) - q^d\rho(\pi)| \leq Mq^{d-\frac{1}{2}}$$

whenever $(d, \operatorname{char} \mathbb{F}_q) \neq (2,2)$, $d \geq 2$, $n \geq 1$, $b \in \mathbb{F}_q^*$, and $q \geq q_0$. Here $\rho(\pi)$ is the proportion of elements of $[S_d]^n$ with cycle pattern π.

2. Preliminaries

2.1. **Wreath products.** We first define the wreath product of groups acting on finite sets. For a more detailed description see [Nek05].

Definition 2.1. Let G and H be groups acting on the finite sets $\{\alpha_1, \dots, \alpha_d\}$ and $\{\beta_1, \dots, \beta_\ell\}$ respectively. The set $\{(\pi, \tau_1, \dots, \tau_d) | \pi \in G, \tau_1, \dots, \tau_d \in H\}$ forms a group called the *wreath product of G by H*, denoted $G[H]$. $G[H]$ acts on the set $\{\alpha_1, \dots, \alpha_d\} \times \{\beta_1, \dots, \beta_\ell\}$ by $(\alpha_i, \beta_r) \mapsto (\alpha_{\pi(i)}, \beta_{\tau_i(r)})$.

Lemma 2.2 ([Odo85], Lemma 4.1). *Let $\varphi(x), \psi(x)$ be rational functions with coefficients in a field K with* $\deg(\varphi) = d$ *and* $\deg(\psi) = \ell$, *and $d, \ell \geq 1$, such that $\varphi(\psi(x))$ has $d\ell$ distinct roots in $\bar{K}$. Let $G =$* $\mathrm{Gal}(\varphi(x)/K)$. *Then* $\mathrm{Gal}(\varphi(\psi(x))/K)$ *is isomorphic to a subgroup of $G[S_\ell]$.*

Proof. Let $\{\alpha_1, \dots, \alpha_d\}$ be the roots of $\varphi(x)$. Then the roots of $\varphi(\psi(x))$ are the roots of $(\psi(x) - \alpha_i)$ for $i = 1, \dots, d$. So we can write the set of roots of $\varphi(\psi(x))$ as $\{\beta_{i,r} | i = 1, \dots, d, r = 1, \dots, \ell\}$ where $\{\beta_{i,r} | r = 1, \dots, \ell\}$ is the set of zeros of $\psi(x) - \alpha_i$. Let $\sigma \in \mathrm{Gal}(\varphi(\psi(x))/K)$. Let F be the splitting field of $\varphi(x)$ over K. Then σ induces a permutation $\pi := \sigma|_F$ on $\{\alpha_1, \dots, \alpha_d\}$, that is, $\pi \in G$. We can think of π as a permutation on the indices $\{1, \dots, d\}$ defined by $\alpha_{\pi(i)} := \pi(\alpha_i)$. Now fix i, and note that since $\psi(\sigma(\beta_{i,r})) = \sigma(\psi(\beta_{i,r})) = \sigma(\alpha_i) = \pi(\alpha_i) = \alpha_{\pi(i)}$, we must have $\sigma(\beta_{i,r}) = \beta_{\pi(i),s}$ for some s. This defines a map $r \mapsto s$ which is a permutation of $\{1, \dots, \ell\}$; we call this map τ_i. Hence, the map σ is given by $\sigma(\beta_{i,r}) = \beta_{\pi(i),\tau_i(r)}$ for $\pi \in G$ and $\tau_i \in S_\ell$. Thus, we can define a map $\mathrm{Gal}(\varphi(\psi(x))/K) \longrightarrow G[S_\ell]$ by $\sigma \mapsto (\pi, \tau_1, \dots, \tau_d)$, which is easily shown to be an injective homomorphism. □

We define the *n-th wreath power of a group G* recursively by $[G]^1 = G$ and $[G]^n = [G]^{n-1}[G]$.

Corollary 2.3. *If $\varphi(x)$ is a rational function in $K(x)$ with degree d and $\alpha \in K$ such that $\varphi^n(x) - \alpha$ has d^n distinct zeros in $\bar{K}$, then* $\mathrm{Gal}(\varphi^n(x) - \alpha/K)$ *can be embedded in $[S_d]^n$.*

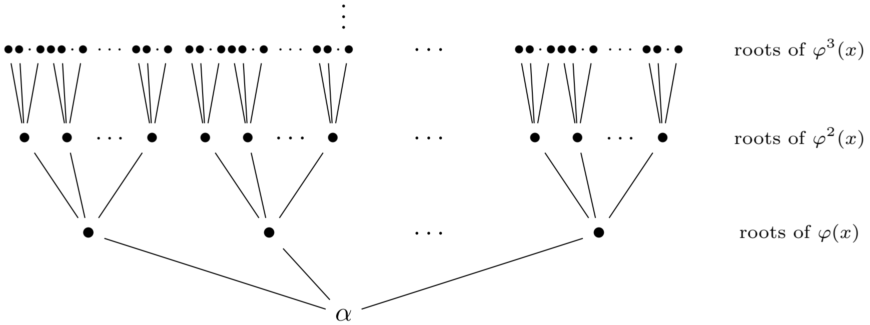

FIGURE 1. Tree diagram for the roots of $\varphi^n(x)$.

The group $[S_d]^n$ has a nice interpretation as the automorphism group of the d-ary rooted tree up to the n-th level [Nek05], [BJ09]. Suppose $\varphi^n(x) - \alpha$ has d^n distinct roots for each $n \geq 1$. Since the image of any root of $\varphi^n(x) - \alpha$ under φ is a root of $\varphi^{n-1}(x) - \alpha$, we can define a tree structure on the roots of $\varphi^n(x) - \alpha$ as follows. If $\beta \in \varphi^{-n}(\alpha)$, then β lies in the n-th level of the tree. If $\varphi(\beta) = \gamma$, then β lies above γ in the tree; that is, there is a branch connecting β to γ. The diagram is shown in Figure 1.

The group $\mathrm{Gal}(\varphi^n(x) - \alpha/K)$ acts on the tree up to the n-th level by permuting the branches so $\mathrm{Gal}(\varphi^n(x) - \alpha/K)$ is isomorphic to a subgroup of $\mathrm{Aut}(T_{d,n})$, the automorphism group of the tree up to the n-th level.

2.2. **Discriminants and ramification.** Let M/K be a finite Galois extension. If $\mathfrak{p}$ is a prime of K and $\mathfrak{q}$ is any prime of M extending $\mathfrak{p}$, we define $e(\mathfrak{q}|\mathfrak{p})$ to be the inertia degree of $\mathfrak{q}$ over $\mathfrak{p}$ and $f(\mathfrak{q}|\mathfrak{p})$ to be the residue degree of $\mathfrak{q}$ over $\mathfrak{p}$. The next result is useful in determining the structure of inertia groups; similar results can be found in [GTZ07], [vdW35].

Lemma 2.4. *Let M/K be a finite Galois extension with Galois group G. Let H be a subgroup of G and let $L = M^H$ be the corresponding intermediate field. Let $\mathfrak{q}$ be a prime of M and let $\mathfrak{p} := \mathfrak{q} \cap K$. Let X be the transitive G-set G/H. Then there is a bijection between the set of orbits of X under the action of $D(\mathfrak{q}|\mathfrak{p})$, the decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$, and the set of extensions $\mathfrak{P}$ of $\mathfrak{p}$ to L with the property: If $\mathfrak{P}$ corresponds to Y, then the length of Y is $e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$ and Y is the disjoint union of $f(\mathfrak{P}|\mathfrak{p})$ orbits of length $e(\mathfrak{P}|\mathfrak{p})$ under the action of $I(\mathfrak{q}|\mathfrak{p})$, the inertia group of $\mathfrak{q}$ over $\mathfrak{p}$.*

Proof. For $\tau \in G$ we will show that the length of the orbit of the coset $H\tau$ under the action of $D(\mathfrak{q}|\mathfrak{p})$ is $e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$, where $\mathfrak{P} = \tau(\mathfrak{q}) \cap L$. Let Y be the orbit of $H\tau$ and let $\mathrm{Stab}_{D(\mathfrak{q}|\mathfrak{p})}(H\tau)$ be the stabilizer of $H\tau$ under the action of $D(\mathfrak{q}|\mathfrak{p})$. Then,

$$\begin{aligned}\mathrm{Stab}_{D(\mathfrak{q}|\mathfrak{p})}(H\tau) &= \{\gamma \in D(\mathfrak{q}|\mathfrak{p}) | H\tau\gamma = H\tau\} = \{\gamma \in D(\mathfrak{q}|\mathfrak{p}) | \tau\gamma\tau^{-1} \in H\} \\ &= H \cap \tau D(\mathfrak{q}|\mathfrak{p})\tau^{-1} = H \cap D(\tau(\mathfrak{q})|\mathfrak{p}) = D(\tau(\mathfrak{q})|\mathfrak{P}),\end{aligned}$$

where $D(\tau(\mathfrak{q})|\mathfrak{P})$ is the decomposition group of $\tau(\mathfrak{q})$ over $\mathfrak{P}$. So, the Orbit/Stabilizer Theorem implies that

$$\#Y = \frac{\#D(\mathfrak{q}|\mathfrak{p})}{\#\operatorname{Stab}_{D(\mathfrak{q}|\mathfrak{p})}(H\tau)} = \frac{\#D(\mathfrak{q}|\mathfrak{p})}{\#D(\tau(\mathfrak{q})|\mathfrak{P})} = \frac{\#D(\mathfrak{q}|\mathfrak{p})}{\#D(\mathfrak{q}|\mathfrak{P})} = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p}).$$

Now, we must show that this correspondence is well-defined and bijective. Suppose $H\tau$ and $H\sigma$ are in the same orbit under the action of $D(\mathfrak{q}|\mathfrak{p})$. Then $\exists\gamma \in D(\mathfrak{q}|\mathfrak{p})$ such that $H\tau\gamma = H\sigma$, which implies $\tau\gamma\sigma^{-1} \in H$. So $\sigma(\mathfrak{q}) \cap L = \tau\gamma\sigma^{-1}(\sigma(\mathfrak{q}) \cap L) = \tau(\mathfrak{q}) \cap L$ and the map $Y \mapsto \tau(q) \cap L$ is well-defined. Clearly the map is surjective, since G permutes the primes of M lying above $\mathfrak{p}$ transitively. To see that this map is one-to-one suppose $\tau(\mathfrak{q}) \cap L = \sigma(\mathfrak{q}) \cap L = \mathfrak{P}$. Then $\tau(\mathfrak{q}), \sigma(\mathfrak{q})$ both lie above $\mathfrak{P}$, and since H acts transitively on the primes of M lying above $\mathfrak{P}$, $\exists\gamma \in H$ such that $\gamma\tau(\mathfrak{q}) = \sigma(\mathfrak{q})$. Then, $\sigma^{-1}\gamma\tau(\mathfrak{q}) = \mathfrak{q}$ so $\sigma^{-1}\gamma\tau \in D(\mathfrak{q}|\mathfrak{p})$. Since $H\sigma(\sigma^{-1}\gamma\tau) = H\tau$, this shows that $H\sigma$ and $H\tau$ are in the same orbit under the action of $D(\mathfrak{q}|\mathfrak{p})$.

It remains to show that Y is the disjoint union of $f(\mathfrak{P}|\mathfrak{p})$ orbits of length $e(\mathfrak{P}|\mathfrak{p})$ under the action of $I(\mathfrak{q}|\mathfrak{p})$. Let Z be the orbit of $H\tau$ under $I(\mathfrak{q}|\mathfrak{p})$. It suffices to show that $\#Z$ is $e(\mathfrak{P}|\mathfrak{p})$. Let $\operatorname{Stab}_{I(\mathfrak{q}|\mathfrak{p})}(H\tau)$ be the stabilizer of $H\tau$ under the action of $I(\mathfrak{q}|\mathfrak{p})$. Then, arguing as before, we see that

$$\operatorname{Stab}_{I(\mathfrak{q}|\mathfrak{p})}(H\tau) = \{\gamma \in I(\mathfrak{q}|\mathfrak{p}) | H\tau\gamma = H\tau\} = I(\tau(\mathfrak{q})|\mathfrak{P}),$$

where $I(\tau(\mathfrak{q})|\mathfrak{P})$ is the inertia group of $\tau(\mathfrak{q})$ over $\mathfrak{P}$. Using the Orbit/Stabilizer Theorem again, we get

$$\#Z = \frac{\#I(\mathfrak{q}|\mathfrak{p})}{\#\operatorname{Stab}_{I(\mathfrak{q}|\mathfrak{p})}(H\tau)} = e(\mathfrak{P}|\mathfrak{p}).$$

□

Remark 2.5. The set G/H is the set of K homomorphisms of L into M. In the case $L \cong K(\theta)$ where θ is a root of some $f \in K[x]$, this corresponds to the set of zeros of f in M, so there is a one-to-one correspondence between the set of orbits of the roots of $f(x)$ under the action of the decomposition group $D(\mathfrak{q}|\mathfrak{p})$ and the set of extension of $\mathfrak{p}$ to L with the property from Lemma 2.4.

Let A be a Dedekind domain, let K be the field of fractions of A, let L be a separable extension of K, and let B be the integral closure of A in L. It is a standard result that any prime of A that ramifies in B must contain $\Delta(B/A)$, the discriminant ideal of the extension B/A. The following two results on discriminants are standard; see [Jan96] or [Lan64], for example.

Lemma 2.6. *Let $\mathfrak{p} \subseteq A$ be a prime, let $\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$, and let $f_i = f(\mathfrak{q}_i|\mathfrak{p})$ be the residue degree. Then the power of $\mathfrak{p}$ in $\Delta(B/A)$ is greater than or equal to $\sum(e_i - 1)f_i$ with equality if and only if* char K *does not divide e_i for any i.*

For computational purposes it is often easier to work with polynomial discriminants, which we will do here.

Lemma 2.7. *Let $P(x)$ be an irreducible polynomial in $A[x]$, let θ be a root of $P(x)$, and let $L = K(\theta)$ if $B = A[\theta]$. That is, if $A[\theta]$ is integrally closed in L, then $\Delta(B/A) = (\Delta(P(x)))$, where $\Delta(P(x))$ is the usual polynomial discriminant of $P(x)$ and $(\Delta(P(x)))$ is the ideal generated by $\Delta(P(x))$.*

Thus, if $B = A[\theta]$, then the only primes of A ramifying in B must divide $\Delta(P(x))$, and furthermore, if $\mathfrak{p}$ ramifies in B, then $v_{\mathfrak{p}}(\Delta(P(x)) = v_{\mathfrak{p}}(\Delta(B/A))$. In the next two corollaries we assume this is the case and let M be the splitting field of $P(x)$ over K.

Corollary 2.8. *If $\mathfrak{p}||\Delta(P(x))$ in A, then for any prime $\mathfrak{q}$ of M lying over $\mathfrak{p}$, the action of the inertia group $I(\mathfrak{q}|\mathfrak{p})$ on the roots of $P(x)$ consists of a single transposition.*

Proof. Let $\{\alpha_1, \ldots, \alpha_d\}$ be the roots of $P(x)$ in M and let $L = K(\alpha_i)$ for some i. Since $\mathfrak{p}||\Delta(P(x))$, Lemma 2.7 implies that $\mathfrak{p}||\Delta(B/A)$, where B is the integral closure of A in L. Then by Lemma 2.6, $\mathfrak{p}B = \mathfrak{P}_1^2\mathfrak{P}_2 \ldots \mathfrak{P}_m$ where $f(\mathfrak{P}_1|\mathfrak{p}) = 1$ for some primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ in B. If $\mathfrak{q}$ is a prime of M lying over $\mathfrak{p}$, then by Lemma 2.4, the action of $I(\mathfrak{q}|\mathfrak{p})$ on $\{\alpha_1, \ldots, \alpha_d\}$ consists of a single transposition. □

Corollary 2.9. *If $\operatorname{char}(K) = 2$ and $\mathfrak{p}^2||\Delta(P(x))$ in A, then for any prime $\mathfrak{q}$ of M lying over $\mathfrak{p}$, the action of $I(\mathfrak{q}|\mathfrak{p})$ on the roots of $P(x)$ consists of a single transposition or a single three cycle.*

Proof. With notation as in the proof of Corollary 2.8, Lemma 2.6 implies that $\mathfrak{p}B = \mathfrak{P}_1^2\mathfrak{P}_2 \ldots \mathfrak{P}_m$ where $f(\mathfrak{P}_1|\mathfrak{p}) = 1$ or $\mathfrak{p}B = \mathfrak{P}_1^3\mathfrak{P}_2 \ldots \mathfrak{P}_m$ where $f(\mathfrak{P}_1|\mathfrak{p}) = 1$, for some primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ in B. Then, if $\mathfrak{q}$ is a prime of M lying over $\mathfrak{p}$, by Lemma 2.4, the action of $I(\mathfrak{q}|\mathfrak{p})$ on $\{\alpha_1, \ldots, \alpha_d\}$ consists of a single transposition or a single three cycle, respectively. □

We often work with splitting fields of rational functions. In this case we need the following useful result of Cullinan and Hajir [CH12]. Let t be transcendental over a field k and let $\psi(x) = p(x)/q(x)$ be a rational function with coefficients in k and $p(x), q(x) \in k[x]$. Then the splitting field of $\psi(x) - t$ over $k(t)$ is the splitting field of the polynomial $p(x) - tq(x)$ over $k(t)$.

Lemma 2.10 ([CH12], Proposition 1). *We have*

$$\begin{aligned}\Delta(p(x) - tq(x)) &= C \operatorname{Res}(p'(x)q(x) - p(x)q'(x), p(x) - tq(x)) \\ &= C' \prod_{a \in \psi_{\mathfrak{c}}} (\psi(a) - t)^{e(a|\psi(a))-1},\end{aligned}$$

where $C, C' \in k$ are constants, $\psi_{\mathfrak{c}} = \{a \in \bar{k} : \psi'(a) = 0\}$, and $e(a|\psi(a))$ is the ramification index of a over $\psi(a)$.

Thus, we see that any prime $\mathfrak{p}$ of $k[t]$ that ramifies in a splitting field for $p(x) - tq(x)$ must divide $\prod_{a \in \psi_{\mathfrak{c}}} (\psi(a) - t)^{e(a|\psi(a))-1}$. We will use the notation

$$\Delta(\psi(x) - t) := \prod_{a \in \psi_{\mathfrak{c}}} (\psi(a) - t)^{e(a|\psi(a))-1}.$$

The following result is a standard consequence of the Rieman–Hurwitz formula (see [Sti09], for example).

Lemma 2.11. *For any field k, $k(t)$ has no finite separable extensions with constant field k of degree $d \geq 2$ which are unramified over all $\mathfrak{p} \in \mathbb{P}_{k(t)} \setminus \{\mathfrak{p}_\infty\}$ and tamely ramified at $\mathfrak{p}_\infty$. Here $\mathbb{P}_{k(t)}$ denotes the set of primes of $k(t)$.*

Proof. Let F be any finite extension of $k(t)$ with field of constants k and let $d = [F : k(t)]$. For the prime $\mathfrak{p}_\infty$ of $k(t)$, $\sum_{\mathfrak{q}|\mathfrak{p}_\infty}(e(\mathfrak{q}|\mathfrak{p}_\infty)-1)\deg\mathfrak{q} \leq d-1$ where the sum ranges over all $\mathfrak{q}$ extending $\mathfrak{p}_\infty$. Let g be the genus of F. From the Riemann–Hurwitz formula we have

$$2g-2 = -2d + \sum_{\mathfrak{p}\in\mathbb{P}_{k(t)}} \sum_{\mathfrak{p}'|\mathfrak{p}} (e(\mathfrak{p}'|\mathfrak{p})-1)\deg\mathfrak{p}',$$

$$2g-2 \leq -2d + \sum_{\substack{\mathfrak{p}\in\mathbb{P}_{k(t)}\\ \mathfrak{p}\neq\mathfrak{p}_\infty}} \sum_{\mathfrak{p}'|\mathfrak{p}} (e(\mathfrak{p}'|\mathfrak{p})-1)\deg\mathfrak{p}' + d - 1,$$

where the second sum is taken over all $\mathfrak{p}'$ extending $\mathfrak{p}$ in F. Then since $g \geq 0$,

$$d-1 \leq \sum_{\substack{\mathfrak{p}\in\mathbb{P}_{k(t)}\\ \mathfrak{p}\neq\mathfrak{p}_\infty}} \sum_{\mathfrak{p}'|\mathfrak{p}} (e(\mathfrak{p}'|\mathfrak{p})-1)\deg\mathfrak{p}'.$$

Since $d \geq 2$, some prime in $\mathbb{P}_{k(t)} \setminus \{\mathfrak{p}_\infty\}$ must ramify in F. □

2.3. **Results on subgroups of S_d.** Let F be any field. We say a polynomial $f(x) \in F[x]$ is *indecomposable* if $f(x)$ cannot be written as $f(x) = g(h(x))$ for $g, h \in F[x]$ with $\deg g, \deg h > 1$. A group G acting on a set S is said to be *primitive* if it acts transitively and preserves no nontrivial partition of S. The following is a result of Fried [Fri70] as referenced in [Coh91].

Lemma 2.12 ([Coh91], Lemma 3.1). *A separable polynomial $f(x)$ over a field F is indecomposable if and only if the Galois group G of $f(x)-t$ over $F(t)$ is primitive on the roots of $f(x)-t$.*

Proof. Let $\{a_1, \ldots, a_d\}$ be the roots of $f(x)-t$. Since $f(x)-t$ is irreducible over $F(t)$, G must be transitive. Suppose G is imprimitive. Then there is some nontrivial partition of $\{a_1, \ldots, a_d\}$ into disjoint subsets $S_1, \ldots, S_n$ preserved by G. Let $S = S_i$ be one of these subsets with $\#S_i > 1$. If $a \in S$, then $\mathrm{Stab}_G(a) \subsetneq \{\sigma \in G | \sigma(S) = S\}$. So $\mathrm{Stab}_G(a)$ is not a maximal subgroup of G. Hence, there is a field strictly between $F(t)$ and $F(a)$, which by Luroth's Theorem must be of the form $F(u)$. Thus, $u = h(a)$ and $t = g(u)$ for (nonlinear) rational functions g, h with coefficients in F. Then since $f(a) = g(h(a))$, we can find (nonlinear) polynomials g_1, h_1 with coefficients in F such that $f(x) = g_1(h_1(x))$. Thus, f is decomposable over F.

Conversely, if f is decomposable, then we can write $f(x) = g(h(x))$ for nonlinear $g(x), h(x) \in F[x]$. Then the relation $a \sim b$ if $h(a) = h(b)$ gives a nontrivial partition of $\{a_1, \ldots, a_d\}$ preserved by G. □

The next two results are standard and are provided here for completeness.

Lemma 2.13. *If G is a primitive subgroup of S_d that contains a transposition, then $G = S_d$.*

Proof. Define a relation on $\{1, \ldots, d\}$ by $i \sim j$ if either $i = j$ or G contains the transposition (ij). This is clearly a G-invariant equivalence relation. Since G contains a transposition, there are fewer than d equivalence classes. Then since G is primitive, there must be only one equivalence class. So G contains all the transpositions, which implies $G = S_d$. □

Lemma 2.14. *If G is a transitive subgroup of S_d that is generated by transpositions, then $G = S_d$.*

Proof. Let $\mathcal{S}$ be the set of all k such that there exists some subgroup H of G isomorphic to S_k. $\mathcal{S}$ is nonempty since there are subgroups of G which are isomorphic to S_1 and S_2. Let $m \in \mathcal{S}$ be maximal. Suppose $m \neq d$. After renumbering elements of $\{1, 2, \ldots, d\}$ we can assume that H acts on $\{1, 2, \ldots, m\}$. Now, since G is transitive and generated by transpositions, there is some $(ij) \in G$ such that $i \in \{1, \ldots, m\}$ and $j > m$. But then the subgroup of G generated by $H \cup \{(ij)\}$ is isomorphic to S_{m+1}, contradicting the maximality of m. □

2.4. **The Zariski topology on $\mathcal{P}_d(k)$ and $\mathrm{Rat}_d(k)$.** Let k be an algebraically closed field. Given a point $(a_0, \ldots, a_d)$ in $\mathbb{A}^{d+1}(k)$ with $a_d \neq 0$, $a_d x^d + \cdots + a_0$ is a polynomial of degree d in $k[x]$. We denote the set of all such $(a_0, \ldots, a_d)$ by $\mathcal{P}_d(k)$ and give $\mathcal{P}_d(k)$ the subspace topology inherited from the Zariski topology on $\mathbb{A}^{d+1}(k)$.

Similarly, given a point $(a_0, \ldots, a_d, b_0, \ldots, b_d)$ in $\mathbb{A}^{2d+2}(k)$, we set $p = a_d x^d + \cdots + a_0$, $q = b_d x^d + \cdots + b_0$, and $\varphi = p/q$. If the resultant of p and q is nonzero and either a_d or b_d is nonzero, then φ is a rational function of degree d in $k(x)$. We denote the set of such $(a_0, \ldots, a_d, b_0, \ldots, b_d)$ by $\mathrm{Rat}_d(k)$ and give $\mathrm{Rat}_d(k)$ the subspace topology inherited from the Zariski topology on $\mathbb{A}^{2d+2}(k)$.

3. Galois groups of $\varphi^n(x) - t$

In this section, let k be a field with characteristic p (where p is allowed to be 0), let x, t be algebraically independent variables over k, and let $\varphi(x) \in k(x)$ be a rational function with degree $d > 1$. Then, for $n \in \mathbb{N}$, $\varphi^n(x) - t$ is irreducible, and if $\frac{d}{dx}\varphi(x) \neq 0$, then $\varphi^n(x) - t$ is x-separable, since $\frac{d}{dx}(\varphi^n(x) - t) = \frac{d}{dx}\varphi^n(x) \neq 0$ by induction on n. For fixed $N \in \mathbb{N}$, we give conditions on $\varphi(x)$ that ensure that $\mathrm{Gal}(\varphi^N(x) - t/k(t)) \cong [S_d]^N$. Then we show that these conditions are not too restrictive as long as $(d, p) \neq (2, 2)$ by showing that when k is algebraically closed the set of all $f(x) \in k[x]$ of degree d with the property $\mathrm{Gal}(f^N(x) - t/k(t)) \cong [S_d]^N$ contains a nonempty Zariski-open subset of $\mathcal{P}_d(k)$.

Theorem 3.1. *Let $\varphi(x) \in k(x)$ with $\mathrm{Gal}(\varphi(x) - t/k(t)) \cong S_d$. If $\mathrm{char}\, k \neq 2$, suppose φ has some critical point $a \in k$ with multiplicity one such that $\varphi^n(a) \neq \varphi^m(b)$ for all $m \leq n \leq N$, unless $m = n$ and $b = a$; and if $\mathrm{char}\, k = 2$, suppose φ has some critical point a such that $\varphi^n(a) \neq \varphi^m(b)$ for all $m \leq n \leq N$, unless $m = n$ and $b = a$ and $I(\mathfrak{q}|\mathfrak{p})$ consists of a single transposition for any prime $\mathfrak{q}$ lying above $\mathfrak{p} = k(t) \cap (\varphi(a) - t)$ in the splitting field of $\varphi(x) - t$ over $k(t)$. Then $\mathrm{Gal}(\varphi^N(x) - t/k(t)) \cong [S_d]^N$.*

The following proposition follows almost immediately from Theorem 3.1.

Proposition 3.2. *Suppose $\mathrm{char}\, k \neq 2$ and $d \nmid \mathrm{char}\, k$. Then if $\varphi(x)$ is any rational function with degree d such that each of the critical points in $\overline{k}$ have multiplicity one and there is some critical point a such that $\varphi^n(a) \neq \varphi^m(b)$ for any critical point $b \neq a$ and any $m \leq n$, we have $\mathrm{Gal}(\varphi^N(x) - t/k(t)) \cong [S_d]^N$ for all N.*

Proof. By Theorem 3.1 we only need to show that $G = \mathrm{Gal}(\varphi(x) - t/k(t)) \cong S_d$. Let K_1 be the splitting field of $\varphi(x) - t$ over $k(t)$. By Lemma 2.10 the discriminant of $\varphi(x) - t$ is squarefree, so Corollary 2.8 implies that for any ramified prime $\mathfrak{q}$ lying over a prime $\mathfrak{p}$, $I(\mathfrak{q}|\mathfrak{p})$ consists of a single transposition. Let $I \subseteq G$ be the subgroup generated by $\{I(\mathfrak{q}|\mathfrak{p}) : \mathfrak{q}|\mathfrak{p}, \mathfrak{q} \in \mathbb{P}_{K_1},$ and $\mathfrak{p} \in \mathbb{P}_{k(t)} \setminus \{\mathfrak{p}_\infty\}\}$. Then K_1^I is unramified over all primes of $k[t]$, and by Lemma 2.11, $K_1^I = k(t)$. Thus, $G = I$.

So G is a transitive subgroup of S_d generated by transpositions, and Lemma 2.14 implies that $G \cong S_d$. □

Before we prove Theorem 3.1, which gives conditions ensuring that

$$\mathrm{Gal}(\varphi^N(x) - t/k(t))$$

is isomorphic to $[S_d]^N$, we fix some notation and prove a lemma. For $n < N$, let K_n be the splitting field of $\varphi^n(x) - t$ over $k(t)$, let $\alpha_1, \ldots, \alpha_{d^n}$ be the roots of $\varphi^n(x) - t$, let M_i be the splitting field of $\varphi(x) - \alpha_i$ over $k(\alpha_i) = k(\alpha_i, t)$, and let $\widehat{M_i} := K_n \prod_{j \neq i} M_j$.

In order to work with discriminants as in Lemma 2.10 we need to make a few reductions. First note that for any extension k' of k, we have $\mathrm{Gal}(K_N \cdot k'/k'(t)) \subseteq \mathrm{Gal}(K_N/k(t))$, so it suffices to show that $\mathrm{Gal}(K_N \cdot k'/k'(t)) \cong [S_d]^N$ for some extension k' of k. Hence, we may assume that k is algebraically closed. Since k is then infinite and a change of variables on φ does not affect $\mathrm{Gal}(K_N/k(t))$, we may assume that if $m \leq N$, then $\varphi^m(a)$ is not the point at infinity. Furthermore, we may assume that every prime in $k[t]$ is of the form $(z - t)$ for some $z \in k$.

Lemma 3.3. *For $n < N$, the prime $(\varphi(a) - \alpha_i)$ of $k[\alpha_i]$ does not ramify in $\widehat{M_i}$.*

Proof. We will show that $(\varphi(a) - \alpha_i)$ does not ramify in K_n and that the primes extending $(\varphi(a) - \alpha_i)$ in K_n do not ramify in $M_j K_n$ if $i \neq j$.

We have assumed that $\varphi^{n+1}(a) - t \neq \varphi^m(b) - t$ for any $m \leq n$ and any critical point $b \neq a$ of φ. Thus, we see that $(\varphi^{n+1}(a) - t)$ does not ramify in K_n since the only primes of $k(t)$ that ramify in K_n must divide

$$\Delta(\varphi^n(x) - t) = \prod_{b \in \varphi_{\mathfrak{c}}} \left((\varphi(b) - t)^{d^{n-1}} (\varphi^2(b) - t)^{d^{n-2}} \ldots (\varphi^n(b) - t) \right)^{e(b|\varphi(b)) - 1}.$$

Since $(\varphi(a) - \alpha_i)$ extends $(\varphi^{n+1}(a) - t)$ in $k(\alpha_i)/k(t)$, it follows that $(\varphi(a) - \alpha_i)$ does not ramify in K_n.

We can also see that $(\varphi(a) - \alpha_i)$ does not ramify in $M_j K_n$ for $j \neq i$ since the primes of K_n ramifying in $M_j K_n$ are those dividing

$$\Delta(\varphi(x) - \alpha_j) = \prod_{b \in \varphi_{\mathfrak{c}}} (\varphi(b) - \alpha_j)^{e(b|\varphi(b)) - 1}.$$

Suppose a prime $\mathfrak{p}$ of K_n extending $(\varphi(a) - \alpha_i)$ in $K_n/k(\alpha_i)$ ramifies in $M_j K_n$. Then $\mathfrak{p}$ divides $\Delta(\varphi(x) - \alpha_j)$, so $\mathfrak{p}$ divides $(\varphi(b) - \alpha_j)$ for some critical point b of φ. Hence, $\mathfrak{p}$ divides $(\varphi(a) - \alpha_i)$ and $(\varphi(b) - \alpha_j)$. Thus, $\mathfrak{p}$ divides $(\varphi^{n+1}(a) - t)$ and $(\varphi^{n+1}(b) - t)$, so we must have $\varphi^{n+1}(a) = \varphi^{n+1}(b)$ (since $\mathfrak{p}$ can extend exactly one prime in $K_n/k(t)$). This means that $b = a$, since we assumed $\varphi^{n+1}(a) \neq \varphi^{n+1}(b)$ if $b \neq a$. Thus, $\mathfrak{p}$ divides both $(\varphi(a) - \alpha_i)$ and $(\varphi(a) - \alpha_j)$. Then $\mathfrak{p}^2$ divides $\varphi^{n+1}(a) - t = \prod_{i=1}^{d^n} (\varphi(a) - \alpha_i)$. So the prime $\mathfrak{p}$ of K_n ramifies over $(\varphi^{n+1}(a) - t)$, which is a contradiction. □

Proof of Theorem 3.1. We use induction on n to prove $\mathrm{Gal}(\varphi^n(x) - t/k(t)) \cong [S_d]^n$ for all $n \leq N$. The result holds in the case $n = 1$ by hypothesis.

Let $n < N$, and suppose $\mathrm{Gal}(\varphi^m(x) - t/k(t)) \cong [S_d]^n$, for all $m \leq n$. Let $\alpha_1, \ldots, \alpha_{d^n}$ be the distinct roots of $\varphi^n(x) - t$ as before. Then since α_i is transcendental over k, $\mathrm{Gal}(M_i/k(\alpha_i)) \cong \mathrm{Gal}(\varphi(x) - t/k(t)) \cong S_d$ where M_i is the splitting field of $\varphi(x) - \alpha_i$ over $k(\alpha_i) = k(\alpha_i, t)$.

Let K_{n+1} be the splitting field of $\varphi^{n+1}(x) - t$ over $k(t)$, so $K_{n+1} = \prod M_j$. To complete the proof it is enough to show that $\mathrm{Gal}(M_i/M_i \cap \widehat{M_i}) \cong S_d$ for each i, as then $\mathrm{Gal}(K_{n+1}/\widehat{M_i}) \cong S_d$ for each i, and this implies that K_{n+1} has degree $(d!)^{d^n}$ over K_n and $[K_{n+1} : K_n][K_n : k(t)] = (d!)^{d^n}|[S_d]^n| = |[S_d]^{n+1}|$. Since $\mathrm{Gal}(K_{n+1}/k(t))$ must be isomorphic to a subgroup of $[S_d]^{n+1}$, we have equality.

Note that the extension $M_i \cap \widehat{M_i}/k(\alpha_i)$ is Galois, so $\Gamma := \mathrm{Gal}(M_i/M_i \cap \widehat{M_i})$ is a normal subgroup of $\mathrm{Gal}(M_i/k(\alpha_i)) \cong S_d$. So either $\Gamma \cong S_d$ or Γ is isomorphic to a subgroup of A_d. Let $\mathfrak{p}$ be the prime $(\varphi(a) - \alpha_i)$ of $k[\alpha_i]$. If $p \neq 2$, then $\mathfrak{p}||\Delta(\varphi(x) - \alpha_i) = \prod_{b \in \varphi_c}(\varphi(b) - \alpha_i)^{e(b|\varphi(b))-1}$. Thus, if $\mathfrak{q}$ is any prime of M_i lying over $\mathfrak{p}$, then by Lemma 2.8, $I(\mathfrak{q}|\mathfrak{p})$ consists of a single transposition. If $p = 2$, then by hypothesis, $I(\mathfrak{q}|\mathfrak{p})$ consists of a single transposition. Now fix a prime $\mathfrak{q}$ of M_i lying over $\mathfrak{p}$, and let $\mathfrak{p}' := \mathfrak{q} \cap (M_i \cap \widehat{M_i})$. By Lemma 3.3, we see that $\mathfrak{p}$ does not ramify in $\widehat{M_i}$, which implies $\mathfrak{p}'$ is unramified over $\mathfrak{p}$. Hence, $e(\mathfrak{q}|\mathfrak{p}') = e(\mathfrak{q}|\mathfrak{p}) = 2$, which implies $I(\mathfrak{q}|\mathfrak{p}')$ also consists of a single transposition. Thus, Γ contains a transposition, so $\Gamma \not\subseteq A_d$ and we have $\Gamma \cong S_d$ as desired. □

Next, we show that as long as $(d, p) \neq (2, 2)$, the conditions in Theorem 3.1 are not too restrictive and in fact "most" polynomials satisfy the more restrictive conditions listed below. For the rest of this section let k be algebraically closed.

Definition 3.4. Define $H(d, N, k)$ to be the set of all $f(x) \in k[x]$ such that

(1) $f'(x)$ is separable if $p \neq 2$ and $f'(x)$ is the square of a separable polynomial if $p = 2$;
(2) if $w_1, \dots, w_r$ are the distinct critical points of $f(x)$, then $f^n(w_i) \neq f^m(w_j)$ for all $1 \leq i, j \leq r$, and $m, n \leq N$, unless $m = n$ and $i = j$.

If $p = 2$ or $p|d$, we impose further conditions:

(3) if $p = 2$, whenever $b, c \in k$, $(x - b)^3$ does not divide $f(x) - c$ in $k[x]$, and
(4) if $p|d$, $f(x)$ is indecomposable in $k(x)$ and $\deg f'(x) = d - 2$.

Remark 3.5. We could impose condition (3) and the indecomposability condition in any characteristic to get an appropriate Zariski-open set. However, they are unnecessary in the cases not listed above, so we choose not to do so.

Lemma 3.6. *$H(d, N, k)$ is a nonempty Zariski-open subset of $\mathcal{P}_d(k)$.*

Proof. Let H_N be the set of all $f(x) \in \mathcal{P}_d(k)$ satisfying (1) and (2) above and if $p|d$ satisfying $\deg f'(x) = d - 2$. Let $x, y_1, y_2, \dots, y_r, u_0, u_1, \dots, u_d, v$ be algebraically independent variables over k, where $r = d - 1$ if $p \neq 2$ and $p \nmid d$, $r = d - 2$ if $p \neq 2$ and $p|d$, $r = \frac{d-1}{2}$ if $p = 2$ and $p \nmid d$, and $r = \frac{d-2}{2}$ if $p = 2$ and $p|d$. Define

$$F(x, u_0, \dots, u_d) = \sum_{i=0}^{d} u_i x^i,$$

$$G(x, v, y_1, \dots, y_r) = v \prod_{i=1}^{r} (x - y_i).$$

If $\sigma_0, \sigma_1, \dots, \sigma_r$ are the elementary symmetric polynomials in $y_1, \dots, y_r$ and we set $v_i = v\sigma_i$, then $u_0, u_1, \dots, u_d, v_0, v_1, \dots, v_r$ are algebraically independent over k. Let $F^m(x) = F^m(x, u_0, \dots, u_d)$ be the m-th x-iterate of $F(x, u_0, \dots, u_d)$, and let

$$D = \prod_{1 \leq i < j \leq r} \prod \prod_{0 \leq \ell, m \leq N} \prod [F^\ell(y_i) - F^m(y_j)].$$

Then D is expressible as a polynomial in $u_0, \ldots, u_d, v_0, \ldots, v_r$. If $p \neq 2$, we specialize $G(x)$ to $F'(x)$, that is, specialize the v_i so that $\sum_j ju_jx^{j-1} = \sum_i v_{r-i}x^i$. If $p = 2$, then we let D be as above but specialize the v_j so that $\sum_j ju_jx^{j-1} = (\sum v_{r-i}x^i)^2 = \sum v_{r-i}^2 x^{2i}$. In either case, D specializes to a polynomial $h(u_0, \ldots, u_d)$ in the ring $k[u_1, \ldots, u_d]$. It is clear that if $h(a_0, \ldots, a_d) \neq 0$, then $f(x) = \sum_i a_ix^i \in H_N$ so H_N is a Zariski-open set in $\mathcal{P}_d(k)$.

We now show that H_N is nonempty. Let H_1 be the set of all $f(x) \in \mathcal{P}_d(k)$ satisfying

- if $p|d$, $\deg f'(x) = d - 2$,
- $f'(x)$ is separable if $p \neq 2$ and $f'(x)$ is the square of a separable polynomial if $p = 2$, and
- if $w_1, \ldots, w_r$ are the distinct critical points of $f(x)$, then $f(w_i) \neq f(w_j)$ unless $i = j$.

We first show that H_1 is nonempty. To do so we consider many different cases. If $p = 0$, $p \nmid d(d-1)$, or $p = 2$ and $d \equiv 3 \mod 4$, then any $f(x)$ of the form $f(x) = a_dx^d + a_1x + a_0$ with $a_0a_1a_d \neq 0$ belongs to H_1. In the case $p > 2$ and $p|d$, we have $d \geq p \geq 3$ and $p \nmid d-2$. If $f(x) = a_dx^d + a_{d-1}x^{d-1} + a_1x + a_0$ with $a_0a_1a_{d-1}a_d \neq 0$, then $f(x) \in H_1$. If $p > 2$ and $p|d-1$, then $d \geq p+1 \geq 4$, and any $f(x) = a_dx^d + a_2x^2 + a_0$ with $a_0a_2a_d \neq 0$ belongs to H_1.

Finally, we consider the cases where $p = 2$ and $d \not\equiv 3 \mod 4$. If $d \equiv 0 \mod 4$ and $f(x) = a_dx^d + a_{d-1}x^{d-1} + a_1x + a_0$ with $a_0a_1a_{d-1}a_d \neq 0$, then $f(x) \in H_1$. If $d \equiv 1 \mod 4$, then $f(x) = a_dx^d + a_3x^3 + a_0$ with $a_0a_3a_d \neq 0$ will lie in H_1. If $d \equiv 2 \mod 4$, $f(x) \in H_1$ if $f(x) = a_dx^d + a_{d-1}x^{d-1} + a_3x^3 + a_0$ with $a_0a_3a_{d-1}a_d \neq 0$.

Now we will show that H_N is nonempty by showing there is some $f(x) \in H_1$ such that $f(x)$ satisfies condition (2). Let $f(x) \in H_1$, and let $\lambda, \mu \in k$ with $\mu \neq 0$. It is easy to see that $f^*(x) = f(\mu x + \lambda)$ also lies in H_1, since if w_i is a critical point of f, then $\frac{w_i - \lambda}{\mu}$ is a critical point of f^* and $f^*\left(\frac{w_i-\lambda}{\mu}\right) = f(w_i)$. Now note, for each i, j, n, m with $i \neq j$ and $m \neq n$, the set of $(\lambda, \mu) \in \mathbb{A}^2$ such that $(f^*)^n\left(\frac{w_i-\lambda}{\mu}\right) = (f^*)^m\left(\frac{w_j-\lambda}{\mu}\right)$ is a dimension one subvariety of $\mathbb{A}^2$. Thus, since k is infinite, we may choose $(\lambda, \mu) \in \mathbb{A}^2(k)$ so that $(f^*)^n\left(\frac{w_i-\lambda}{\mu}\right) \neq (f^*)^m\left(\frac{w_j-\lambda}{\mu}\right)$, for all $1 \leq i, j \leq r$, and $m, n \leq N$, unless $m = n$ and $i = j$, which implies that $f^*(x) \in H_N$, and H_N is nonempty.

Now, if $p = 2$, consider the set of $f(x) \in \mathcal{P}_d(k)$ satisfying condition (3). Let $s, v, u_0, \ldots, u_{d-3}, y_0, \ldots, y_d, x$ be algebraically independent variables over k, and define $\pi_0, \ldots, \pi_d \in k[s, v, u_0, \ldots, u_{d-3}]$ so that

$$\sum_{j=1}^{d} \pi_jx^j = s + (x-v)^3(u_0 + \cdots + u_{d-3}x^{d-3}).$$

Working in the ring $R := k[s, v, u_0, \ldots, u_{d-3}, y_0, \ldots, y_d]$, let $\mathfrak{P}$ be the ideal generated by $y_0 - \pi_0, \ldots, y_d - \pi_d$. Clearly, $R/\mathfrak{P} \cong k[s, v, u_0, \ldots, u_{d-3}]$, so $\mathfrak{P}$ is a prime ideal. Then $\mathfrak{p} = \mathfrak{P} \cap k[y_0, \ldots, y_d]$ is prime in $k[y_0, \ldots, y_d]$. Moreover, the transcendence degree of $k[y_0, \ldots, y_d]/\mathfrak{p}$ over k does not exceed d since $k[y_0, \ldots, y_d]/\mathfrak{p} \subseteq R/\mathfrak{P}$. Let $\mathcal{V}$ be the variety in $\mathbb{A}_k^{d+1}$ corresponding to $\mathfrak{p}$. Then $\mathcal{V}$ is Zariski closed and not equal to $\mathbb{A}_k^{d+1}$. It is clear that if $f(x) = a_dx^d + \cdots + a_0$ fails to satisfy the third property, then $(a_0, \ldots, a_d) \in \mathcal{V}$. Thus, the set $\mathcal{V}^c$ is a nonempty Zariski-open set on which condition (3) holds.

Finally, suppose $p|d$. It remains to show that the set of indecomposable polynomials with degree d contains a nonempty Zariski-open set. It suffices to show that for each ordered pair $(e, f) \in \mathbb{N}^2$ with $e, f \geq 2$ and $ef = d$, the set of polynomials in $\mathcal{P}_d(k)$ that can be expressed as $g(h(x))$ in $k[x]$ with $\deg g = e$ and $\deg h = f$ is contained in a proper Zariski-closed set. If d is prime the result is trivial.

First, we assume $d \geq 6$ leaving the case $d = 4$ until later. Note that whenever $f(x) = g(h(x))$ we can adjust $g(x)$ and $h(x)$ so that $h(x)$ is monic. Let $x, y_0, \ldots, y_d, s_0, \ldots, s_e, t_0, \ldots, t_{f-1}$ be algebraically independent variables over k and define $\pi_0, \ldots, \pi_d \in k[s_0, \ldots, s_e, t_0, \ldots, t_{f-1}]$ so that

$$\sum_{j=0}^{d} \pi_j x^j = \sum_{i=0}^{e} s_i \left(x^f + \sum_{\ell=0}^{e-1} t_\ell x^\ell \right)^i .$$

Let $\mathfrak{P}$ be the ideal in $R := k[y_o, \ldots, y_d, s_0, \ldots, s_e, t_0, \ldots, t_{f-1}]$ generated by $y_0 - \pi_0, \ldots, y_d - \pi_d$. Then $R/\mathfrak{P} \cong k[s_0, \ldots, s_e, t_0, \ldots, t_{f-1}]$, so $\mathfrak{P}$ is a prime ideal. Then $\mathfrak{p} = \mathfrak{P} \cap k[y_0, \ldots, y_d]$ is prime in $k[y_0, \ldots, y_d]$ and the transcendence degree of $k[y_0, \ldots, y_d]/\mathfrak{p}$ over k is less that or equal to $e + f + 1$. Let $\mathcal{W}$ be the variety in $\mathbb{A}_k^{d+1}$ corresponding to $\mathfrak{p}$. Then $\dim \mathcal{W} \leq e + f + 1 < ef + 1 = d + 1$ since $d > 4$. Thus, $\mathcal{W}$ is a proper, Zariski-closed subset of $\mathbb{A}_k^{d+1}$, and clearly, if $f(x) = a_d x^d + \cdots + a_0$ is decomposable as $g(h(x))$ with $\deg g = e$ and $\deg h = f$, then $(a_0, \ldots, a_d) \in \mathcal{W}$.

Now consider the case $d = 4$ and $e = f = 2$. Note that if $\operatorname{char} k = 2$ and $a_4 a_3 \neq 0$, then it is easy to see that $f(x) = a_4 x^4 + \cdots + a_0$ is indecomposable. If $\operatorname{char} k \neq 2$ and f is decomposable, then by completing the square we can write $f(x) = g((x - c)^2)$ with $c \in k$ and $\deg g = 2$. Then $f(c + x) = f(c - x)$. So if we write $f(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$, expand $f(c + x) - f(c - x) = 0$, and examine the coefficients we see that

$$4a_4 c + a_3 = 0 = 4a_4 c^3 + 3a_3 c^2 + 2a_2 c + a_1.$$

Then since $a_4 \neq 0$, we must have $c = -a_3/4a_4$, so that

$$16 a_1 a_4^2 - 8 a_2 a_3 a_4 + 3 a_3^3 a_4 - a_3^3 = 0.$$

Clearly this does not hold for all $f(x) \in \mathcal{P}_4(k)$, and this completes the proof. □

Theorem 3.7. *If $f(x) \in H(d, N, k)$, then* $\operatorname{Gal}(f^N(x) - t/k(t)) \cong [S_d]^N$.

Proof. We will show that $f(x)$ satisfies the hypotheses of Theorem 3.1, which gives the desired result. First note that for any critical point a of $f(x)$, $f^n(a) \neq f^n(b)$ for all $m \leq n \leq N$, unless $m = n$ and $b = a$ by definition. Also, if $p \neq 2$, then each critical point has multiplicity one.

If $p = 2$, then $\Delta(f(x) - t) = \prod_{i=1}^{r} (f(w_i) - t)^2$. So Corollary 2.9 implies that $I(\mathfrak{q}|\mathfrak{p})$ consists of a transposition or a three cycle for any ramified prime $\mathfrak{p} = (f(w_i) - t)$ and any prime $\mathfrak{q}$ of K_1 lying over $\mathfrak{p}$. Recall that K_1 is defined to be the splitting field of $f(x) - t$ over $k(t)$. Now, condition (3) in the definition of $H(d, N, k)$ implies that the reduction of $f(x) - t \mod \mathfrak{p}$ is cube free, which, by Kummer's Theorem (see [Jan96, Theorem 7.4], for example), implies that we cannot have $\mathfrak{p} k[\alpha] = \mathfrak{P}_1^3 \mathfrak{P}_2 \ldots \mathfrak{P}_m$, where α is a root of $f(x) - t$. So $I(\mathfrak{q}|\mathfrak{p})$ cannot consist of a three cycle, and we must have that $I(\mathfrak{q}|\mathfrak{p})$ consists of a single transposition.

It remains to show that $\operatorname{Gal}(f(x) - t/k(t)) \cong S_d$. Note that for any ramified prime $\mathfrak{p}$ we now have $I(\mathfrak{q}|\mathfrak{p})$ consists of a single transposition. First, we consider the case $p \nmid d$. Let $I \subseteq G$ be the subgroup generated by $\{I(\mathfrak{q}|\mathfrak{p}) : \mathfrak{q}|\mathfrak{p}, \mathfrak{q} \in \mathbb{P}_{K_1}$, and $\mathfrak{p} \in \mathbb{P}_{k(t)} \setminus \{\mathfrak{p}_\infty\}\}$. Then K_1^I is unramified over all primes of $k[t]$, so by Lemma 2.11, $K_1^I = k[t]$. Thus, $G = I$. So G is a transitive subgroup of S_d generated by transpositions and Lemma 2.14 implies that $G \cong S_d$.

If $p|d$, then property (4) in the definition of $H(d, N, k)$ guarantees that $f(x)$, and hence $f(x) - t$, is indecomposable. Then since G contains a transposition, Lemmas 2.12 and 2.13 imply that $G \cong S_d$, as desired. □

4. Generic polynomials and generic rational functions

In this section we prove Theorem 1.1 for $(d, p) \neq (2, 2)$; we handle the case $d = p = 2$ in Section 5. First we give a lemma, which can be found in [Odo85].

Lemma 4.1 ([Odo85], Lemma 2.4). *Let A be an integrally closed domain with field of fractions K, let K' be any field, and let $\psi : A \longrightarrow K'$ be a ring homomorphism. Define $\widetilde{\psi} : A[x] \longrightarrow K'[x]$ by $a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 \mapsto \psi(a_d)x^d + \psi(a_{d-1})x^{d-1} + \cdots + \psi(a_0)$. If $f(x) = a_d x^d + \cdots + a_0$ is a polynomial in $A[x]$ with $d \geq 1$, $a_d \neq 0$, and $a_d \notin \ker(\psi)$, such that $\widetilde{\psi}(f(x))$ is separable over K', then $f(x)$ is separable over K and $\mathrm{Gal}(\widetilde{\psi}(f(x))/K')$ is isomorphic to a subgroup of $\mathrm{Gal}(f(x)/K)$.*

Proof of Theorem 1.1. We now prove Theorem 1.1 in the case $(d, p) \neq (2, 2)$. The case $(d, p) = (2, 2)$ is handled in Section 5, Corollary 5.2.

The result follows almost immediately from Theorem 3.7. Let k be any field (not necessarily algebraically closed). Let $f(x) \in H(d, n, \overline{k})$. If $b \in \overline{k}$, then it is easy to see that $f^*(x) = b^{-1}f(bx) \in H(d, n, \overline{k})$, so without loss of generality we can assume $f(x)$ is monic. By Lemma 3.7, $\mathrm{Gal}(f^n(x) - t/\overline{k}(t)) \cong [S_d]^n$. Now define $g(x) := f(x + t) - t$. Then, $g^n(x) = f^n(x + t) - t$, so $\mathrm{Gal}(g^n(x)/\overline{k}(t)) \cong \mathrm{Gal}(f^n(x) - t/\overline{k}(t)) \cong [S_d]^n$.

Now consider the maps $\psi_1 : \overline{k}[\mathbf{s}] \longrightarrow \overline{k}(t)$ and $\psi_2 : \overline{k}[\mathbf{s},\mathbf{u}] \longrightarrow \overline{k}(t)$ given by mapping s_i to the i-th coefficient of $g(x)$ and mapping u_0 to 1 and u_i to 0 for $i \neq 0$. We can extend ψ_1 and ψ_2 to $\widetilde{\psi_1} : \overline{k}[\mathbf{s}][x] \longrightarrow \overline{k}(t)[x]$ and $\widetilde{\psi_2} : \overline{k}[\mathbf{s},\mathbf{u}][x] \longrightarrow \overline{k}(t)[x]$ in the natural way. Let $P_n(x)$ be the numerator of $\Phi^n(x)$. Then $\widetilde{\psi_1}(\mathfrak{G}^n(x)) = \widetilde{\psi_2}(P_n(x)) = g^n(x)$, so Lemma 4.1 implies that $\mathrm{Gal}(\mathfrak{G}^n(x)/\overline{k}(\mathbf{s})) \supseteq [S_d]^n$ and $\mathrm{Gal}(\Phi^n(x)/\overline{k}(\mathbf{s},\mathbf{u})) \supseteq [S_d]^n$. On the other hand, by Corollary 2.3, $\mathrm{Gal}(\mathfrak{G}^n(x)/k(\mathbf{s})) \subseteq [S_d]^n$ and $\mathrm{Gal}(\Phi^n(x)/k(\mathbf{s},\mathbf{u})) \subseteq [S_d]^n$. Thus, we have $[S_d]^n \subseteq \mathrm{Gal}(\mathfrak{G}^n(x)/\overline{k}(\mathbf{s})) \subseteq \mathrm{Gal}(\mathfrak{G}^n(x)/k(\mathbf{s})) \subseteq [S_d]^n$ and $[S_d]^n \subseteq \mathrm{Gal}(\Phi^n(x)/\overline{k}(\mathbf{s},\mathbf{u})) \subseteq \mathrm{Gal}(\Phi^n(x)/k(\mathbf{s},\mathbf{u})) \subseteq [S_d]^n$. Hence, it follows that $\mathrm{Gal}(\mathfrak{G}^n(x)/k(\mathbf{s})) \cong [S_d]^n$ and $\mathrm{Gal}(\Phi^n(x)/k(\mathbf{s},\mathbf{u})) \cong [S_d]^n$ as desired. □

Let k be any field, let $t_1, \ldots, t_r, x_1, \ldots, x_n$ be independent indeterminants over k, let $f_1(\mathbf{x}, \mathbf{t}), \ldots, f_m(\mathbf{x}, \mathbf{t})$ be irreducible polynomials in $\mathbf{x}$ with coefficients in $k(\mathbf{t})$, and let $g(\mathbf{t}) \in k[\mathbf{t}]$ be a nonzero polynomial. We define the subset $\mathcal{H}_k(f_1, \ldots, f_m; g)$ of k^r to be the set of all $\mathbf{a} = (a_1, \ldots, a_r) \in k^r$ such that $f_i(\mathbf{a}, \mathbf{x})$ is irreducible for all i and $g(\mathbf{a}) \neq 0$. A *Hilbert subset* of k^r is any subset of this form.

If every Hilbert subset of k^r is nonempty for every integer $r \geq 1$, then we say that k is a *Hilbertian field.* In a Hilbertian field any Hilbert subset of k^r is Zariski dense in k^r (see [FJ08], for example).

The following is a generalization of [Odo85, Lemma 6.1].

Lemma 4.2. *Let k be a Hilbertian field, and let $t_1, \ldots, t_r, x$ be independent indeterminants over k. Suppose that in $k[\boldsymbol{t}, x]$, $f(\boldsymbol{t}, x)$ is x-monic, irreducible, and* *separable. Then, there is a Hilbert subset $\mathcal{H}$ of k^r such that for all $\boldsymbol{t'} \in \mathcal{H}$, $f(\boldsymbol{t'}, x)$ is monic, irreducible, and separable in $k[x]$ and* $\operatorname{Gal}(f(\boldsymbol{t'}, x)/k) \cong \operatorname{Gal}(f(\boldsymbol{t}, x)/k(\boldsymbol{t}))$.

Corollary 4.3. *Let k be a Hilbertian field and let $d > 1$ be an integer with $(d, \operatorname{char} k) \neq (2,2)$. Then there are Hilbert subsets $\mathcal{H}_1$ and $\mathcal{H}_2$ of k^d and k^{2d-1}, respectively, such that* $\operatorname{Gal}(f^n(x)/k) \cong [S_d]^n$ *for any $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $(a_{d-1}, \ldots, a_0) \in \mathcal{H}_1$, and* $\operatorname{Gal}(\varphi^n(x)/k) \cong [S_d]^n$ *for any $\varphi(x) = \frac{x^d + a_{d-1}x^{d-1} + \cdots + a_0}{b_d x^d + b_{d-1}x^{d-1} + \cdots + b_0}$ with $(a_{d-1}, \ldots, a_0, b_d, \ldots, b_0) \in \mathcal{H}_2$.*

5. The case $(d, p) = (2, 2)$

In the case $d = p = 2$, we get different results for polynomials and rational functions so we examine these cases separately. First we look at rational functions since this case is much like the cases we have already examined.

5.1. Rational functions.

Theorem 5.1. *Let k be an algebraically closed field with characteristic 2. For any $N \in \mathbb{N}$, there is a nonempty Zariski-open subset, H, of* $\operatorname{Rat}_2(k)$ *such that for any $\varphi(x) \in H$,* $\operatorname{Gal}(\varphi^N(x) - t/k(t)) \cong [S_2]^N$.

Proof. Let H be the set of degree two rational functions with coefficients in k such that

- $\varphi(x)$ has a finite critical point w, and
- $\varphi^m(w) \neq \varphi^n(w)$, for $0 \leq n, m \leq N$, unless $n = m$.

If $\varphi(x) = \frac{a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x + b_0}$, then $\varphi'(x) = \frac{(a_1b_2 - a_2b_1)x^2 + (a_1b_0 - a_0b_1)}{(b_2x^2 + b_1x + b_0)^2}$, so φ has a finite critical point if $a_1b_2 - a_2b_1 \neq 0$. Using similar arguments to those in the proof of Lemma 3.6, we see that H is Zariski-open. To see that H is nonempty, note that if $\varphi(x) = \frac{x^2 + a_1x + a_0}{b_1x}$ where $\left(\frac{a_1}{b_1}\right)^2 \neq a_0$, then the second property holds up to the first iterate. To see that there exists $\varphi(x)$ such that this property holds for any N, we again refer to the arguments from Lemma 3.6.

Let $\varphi(x) \in H$. Since $\varphi(w) - t$ ramifies in the splitting field of $\varphi(x) - t$, the inertia subgroup $I(\mathfrak{q}|\varphi(w) - t)$ is nontrivial, where $\mathfrak{q}$ is the prime extending $\varphi(w) - t$. Also, $I(\mathfrak{q}|\varphi(w) - t)$ is clearly contained in S_2. Thus, Theorem 3.1 implies that $\operatorname{Gal}(\varphi^N(x) - t/k(t)) \cong [S_2]^N$. □

Now, let k be any field of characteristic 2 and let $\Phi(x)$ be the generic rational function of degree 2 over k as defined in Section 4.

Corollary 5.2. *In the case $(d, p) = (2, 2)$,* $\operatorname{Gal}(\Phi^n(x) - t/k(t)) \cong [S_2]^n$.

Proof. It suffices to show that the result holds in the case k is algebraically closed. This follows from specializing the coefficients of $\Phi^n(x)$ to the coefficients of $\varphi^n(x + t) - t$ for any $\varphi \in H$, as in the proof of the other cases of Theorem 1.1. □

5.2. **Polynomial functions.** The above arguments for rational functions depend on the fact that we can find rational functions φ for which the critical point of φ has an infinite orbit. However, for polynomials of degree 2 in characteristic 2, the situation is much different. In characteristic 2 any separable polynomial of degree 2 is ramified only at infinity which is a fixed point; thus, the polynomial is post-critically finite. Thus, we can expect the result to be much different in this case. The extensions obtained in this section, particularly those discussed in Theorem 5.5, are Artin-Schreier type extensions; which are a characteristic p analog to Kummer extensions; see [GS07], [Lan64].

Let k be any field of characteristic 2, and let $\mathfrak{G}(x)$ be the generic monic polynomial of degree 2 defined over k. Then $\mathfrak{G}(x) = x^2 + sx + t$ for s, t algebraically independent over k.

Theorem 5.3. $\mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t)) \cong R_n \rtimes R_n^*$, *where* $R_n = \mathbb{F}_2[Y]/(Y^n)$ *and* $R_n \rtimes R_n^*$ *is the group of invertible affine linear transformations of* R_n.

Proof. Let E be an algebraic closure of $k(s,t)$ and let $K \subset E$ be an algebraic closure of $k(s)$. Consider the surjective $\mathbb{F}_2$-linear map $\mathcal{L} : E \longrightarrow E$ by $\mathcal{L}(\xi) = \xi^2 + s\xi$. Note that every $\eta \in E$ has exactly two distinct preimages under $\mathcal{L}$ in E. If $\mathcal{L}(\xi) = \eta$, then the other preimage of η is $\xi + s$. It follows that $\dim_{\mathbb{F}_2}(\ker(\mathcal{L}^n)) = n$ for all $n \in \mathbb{N}$. Let $v_1 = s$ and define a sequence $\{v_n\}_{n\in\mathbb{N}}$ via $\mathcal{L}(v_{n+1}) = v_n$ for all $n \in \mathbb{N}$. Then it is easy to see that $v_1, v_2, \ldots, v_n$ forms a basis for $\ker(\mathcal{L}^n) \subseteq K$ over $\mathbb{F}_2$. Define $F_n = k(s, \ker(\mathcal{L}^n)) = k(s, v_n)$. If σ is any $k(s)$-automorphism of K, then $\sigma(\ker(\mathcal{L}^n)) = \ker(\mathcal{L}^n)$ so $F_n/k(s)$ is a normal extension. Furthermore, for $n \geq 2$, we have $\mathcal{L}^{n-1}(v_n) = v_1 = s$, so $F_n/k(s)$ is finite Galois, for all n.

For $n \geq 2$, define $g_n(x) = \mathcal{L}^{n-1}(x) - s$. Then $g(v_n) = 0$ where $g(x) \in k[s,x]$ is an s-Eisenstein polynomial of x-degree 2^{n-1}. In particular, $g_n(x)$ is irreducible in $k(s)[x]$ of x-degree 2^{n-1}, so that $\#\,\mathrm{Gal}(F_n/k(s)) = [F_n : k(s)] = 2^{n-1}$.

Now, suppose α and β are zeros of $\mathfrak{G}^n(x)$ in the algebraic closure of $k(s,t)$. Then $\alpha + \beta \in \ker(\mathcal{L}^n)$. Conversely, if $\lambda \in \ker(\mathcal{L}^n)$, then $\mathfrak{G}^n(\alpha + \lambda) = 0$. Hence, the set of x-zeros of $\mathfrak{G}^n(x)$ is precisely $\alpha + \ker(\mathcal{L}^n)$, and $K_n = F_n(\alpha)$, for any root α of $\mathfrak{G}^n(x)$.

Consider the specialization of $\mathfrak{G}(x)$ to $\widetilde{\mathfrak{G}}(x) \in \overline{k}[t][x]$ given by $s \mapsto 0$. Then $\widetilde{\mathfrak{G}}^n(x)$ is t-Eisentein in $\overline{k}[t][x]$, so it is irreducible. Thus, by Lemma 4.1, $\mathfrak{G}^n(x)$ is irreducible over $K(t)$ and hence over $F_n(t)$. Fix some root α of $\mathfrak{G}^n(x)$. Then $K_n = F_n(\alpha)$. So we have $[K_n : k(s,t)] = [F_n(t,\alpha) : F_n(t)][F_n(t) : k(s,t)] = 2^n 2^{n-1} = \#(R_n \rtimes R_n^*)$.

For $\sigma \in \mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t))$, if $\sigma(\alpha) = \alpha + v_\sigma$ for some $v_\sigma \in \ker \mathcal{L}^n$, then for any $v \in \ker \mathcal{L}^n$, we have

$$\sigma(\alpha + v) = \sigma(\alpha) + \sigma(v) = \alpha + v_\sigma + \overline{\sigma}(v),$$

where $\overline{\sigma} = \sigma|_{F_n}$ is the restriction of σ to F_n.

Thus, $\mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t)) \cong B$, where B is the group of all maps of the form $v \mapsto v' + \tau(v)$, where $\tau \in \mathrm{Gal}(F_n/k(s))$ and v' is arbitrary in $\ker(\mathcal{L}^n)$. We will show that $B \cong R_n \rtimes R_n^*$. Since $\ker(\mathcal{L}^n)$ and R_n are isomorphic as additive groups it suffices to show that $\mathrm{Gal}(F_n/k(s)) \cong R_n^*$. Note that $\mathrm{Gal}(F_n/k(s))$ is uniquely determined by its action on $\ker(\mathcal{L}^n)$, and since any $\tau \in \mathrm{Gal}(F_n/k(s))$ must commute with $\mathcal{L}$, it is uniquely determined by its action on v_n. We will define a map ψ from $\mathrm{Gal}(F_n/k(s))$ to R_n. If $\tau(v_n) = a_n v_n + a_{n-1}v_{n-1} + \cdots + a_1 v_1 = a_n v_n + a_{n-1}\mathcal{L}(v_n) + \cdots + a_1\mathcal{L}^{n-1}(v_n)$, then we must have $\tau(v) = a_n v + a_{n-1}\mathcal{L}(v) + \cdots + a_1\mathcal{L}^{n-1}(v)$ for all $v \in \ker(\mathcal{L}^n)$. We define $\psi(\tau) = a_n + a_{n-1}y + \cdots + a_1 y^{n-1}$. The map ψ is clearly well-defined and injective and is easily checked to be a homomorphism. Further, since any $\tau \in \mathrm{Gal}(F_n/k(s))$ is invertible, we must have $\psi(\tau) = a_n + a_{n-1}y + \cdots + a_1 y^{n-1}$ where $a_n = 1$. So, $\psi(\mathrm{Gal}(F_n/k(s))) \subseteq R_n^*$, and since $\#\,\mathrm{Gal}(F_n/k(s)) = 2^{n-1} = \#R_n^*$, ψ maps $\mathrm{Gal}(F_n/k(s))$ onto R_n^* and $\mathrm{Gal}(F_n/k(s)) \cong R_n^*$ as desired. □

In many applications we wish to study the proportion of elements in a Galois group G which fix some root of the polynomial, which we call the fixed point proportion of G, and denote it by $\mathrm{FPP}(G)$. One application which involves studying the fixed point proportions of Galois groups of generic iterates is detailed in Section 6.1. In that section we will consider the fixed point proportion of the Galois groups of iterates of generic monic polynomials in the cases where $(d,p) \neq (2,2)$. We consider the case $(d,p) = (2,2)$ here for completeness.

Theorem 5.4. *We have*

$$\lim_{n\to\infty} \mathrm{FPP}(\mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t)) = \frac{1}{3}.$$

Proof. We have seen that $\mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t)) \cong B \cong R_n \rtimes R_n^*$. Moreover, if we identify elements of $\mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t))$ with elements of B of the form $v' + \tau$ for $v' \in \ker(\mathcal{L}^n)$ and $\tau \in \mathrm{Gal}(F_n/k(s))$ and identify the elements of $\ker(\mathcal{L}^n)$ with elements of R_n by $a_n v_n + a_{n-1}v_{n-1} + \cdots + a_1 v_1 \leftrightarrow a_n + a_{n-1}y + \cdots + a_1 y^{n-1}$, then it is easy to check that $v \mapsto v' + \tau(v)$ corresponds to $v \mapsto v' + \psi(\tau)\cdot v$, where ψ is defined as in the previous proof and $\cdot$ is multiplication in R_n. Thus, $v' + \tau$ has a fixed point if and only if $v' + \psi(\tau)\cdot v = v$ for some v. That is, if and only if $v' = v(1-\psi(\tau))$ for some v, which holds if and only if $1 - \psi(\tau)$ divides v' in R_n.

If $\psi(\tau) - 1 = 0$, then the only possible choice for v' is 0. If $\psi(\tau) - 1 = y^i +$ higher order terms, then $\psi(\tau) - 1$ divides v' if and only if y^i divides v'. There are 2^{n-i-1} choices for $\psi(\tau)$ which have this form and 2^{n-i} such v'. Thus, the total number of elements of $\mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t))$ which have fixed points is

$$1 + \sum_{i=1}^{n} 2^{n-i}2^{n-i-1} = 1 + \frac{2^{2n-1}}{3}\left(1 - \left(\frac{1}{4}\right)^n\right).$$

So the fixed point proportion is

$$\frac{1}{2^{2n-1}} + \frac{1}{3}\left(1 - \left(\frac{1}{4}\right)^n\right),$$

which approaches $\frac{1}{3}$ as n approaches ∞. □

We can see that unlike in the other cases $\mathrm{Gal}(\mathfrak{G}^n(x)/k(s,t))$ cannot be obtained as the Galois group of $f^n(x) - t$ over $\overline{k}[t]$ for a polynomial $f(x) \in \overline{k}[x]$ as in the other cases. In other words, there are no specializations of s to k preserving the Galois group such that the resulting extension of $k[t]$ is geometric.

Theorem 5.5. *Let k be an algebraically closed field with characteristic* 2 *and let $f(x) = a_2x^2 + a_1x + a_0 \in k[x]$, with $a_2a_1 \neq 0$. Then* $\mathrm{Gal}(f^n(x) - t/k(t)) = (C_2)^n$ *for all $n \in \mathbb{N}$, where C_2 is the cyclic group of order* 2.

Proof. Clearly $f^n(x) - t$ is irreducible in $k(t)[x]$; also, since $a_1 \neq 0$, $f^n(x) - t$ is separable. Let E be an algebraically closed extension of $k(t)$. We can make a change of variables so that $f(x)$ is monic; thus we may assume it has the form $f(x) = x^2 + ax + b$. Consider the $\mathbb{F}_2$-linear map $\mathcal{L} : E \longrightarrow E$ defined by $\mathcal{L}(\xi) = \xi^2 + a\xi$. Using similar arguments to those at the beginning of the proof of Theorem 5.3, we see that $\dim_{\mathbb{F}_2}(\ker(\mathcal{L}^n)) = n$. Further, if α is any x-zero of $f^n(x) - t$ the set of x-zeros of $f^n(x) - t$ is precisely $\alpha + \ker(\mathcal{L}^n)$. Since k is algebraically closed, $\ker(\mathcal{L}^n) \subset k$. Thus, the splitting field of $f^n(x) - t$ over $k(t)$ is $k(t,\alpha)$, and $\mathrm{Gal}(f^n(x) - t/k(t))$ has order $[k(t,\alpha) : k(t)] = 2^n$.

Since the splitting field of $f^n(x) - t$ is $k(t,\alpha)$, the group $\mathrm{Gal}(f^n(x) - t/k(t))$ is determined by its action on α. Let $\sigma \in \mathrm{Gal}(f^n(x) - t/k(t))$. Then $\sigma(\alpha) = \alpha + v_\sigma$

for some $v_\sigma \in \ker(\mathcal{L}^n) \subseteq k \subseteq k(t)$. The map from $\mathrm{Gal}(f^n(x) - t/k(t))$ to the additive group $\ker(\mathcal{L}^n)$ defined by $\sigma \mapsto v_\sigma$ is easily seen to be an isomorphism. Thus, $\mathrm{Gal}(f^n(x) - t/k(t)) \cong \ker(\mathcal{L}^n) \cong (C_2)^n$. □

6. Applications

6.1. **Primes dividing orbits.** Define a *global field* to be a number field or a finite extension of $\mathbb{F}_q(t)$ for some finite field $\mathbb{F}_q$. Let k be a global field, let $f(x) \in k[x]$, and let $a_0 \in k$. We define the sequence $\{f^n(a_0)\}_{n\in\mathbb{N}}$ and let $P_f(a_0)$ denote the set of primes of k such that $v_\mathfrak{p}(f^n(a_0)) \neq 0$ for some n. Following the work in [Odo85], we show that for any $\epsilon > 0$, "most" polynomials $f(x) \in k(x)$ satisfy $\delta_N(P_f(a_0)) < \epsilon$, for any $a_0 \in k$, where $\delta_N(P_f(a_0))$ is the natural density of $P_f(a_0)$.

Definition 6.1. For a global field K, denote the set of prime ideals of $\mathfrak{o}_K$ by $P(K)$, and let A be a subset of $P(K)$. Then the *Dirichlet density* $\delta_D(A)$ is defined by

$$\delta_D(A) := \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in A}(N(\mathfrak{p}))^{-s}}{\sum_{\mathfrak{p}\in P(K)}(N(\mathfrak{p}))^{-s}},$$

and the *natural density* $\delta_N(A)$ is defined by

$$\delta_N(A) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in A |\, \mathrm{N}(\mathfrak{p}) < x\}}{\#\{\mathfrak{p} \in \mathbb{P}^1(k) |\, \mathrm{N}(\mathfrak{p}) < x\}},$$

where $N(\mathfrak{p})$ denotes the size of the residue field at $\mathfrak{p}$.

Theorem 6.2 (The Chebotarev Density Theorem; see [FJ08], [SL96], [KMS94])**.** *Let F be a global field, let K be a finite Galois extension of F, and let $G =$* $\mathrm{Gal}(K/F)$*. For any conjugacy class C of G, the Dirichlet density of the set of primes $\mathfrak{p}$ of F for which* $\mathrm{Frob}\left(\frac{K/F}{\mathfrak{p}}\right) = C$ *exists and is equal to $\#C/\#G$. Furthermore, if F is a number field or F is a function field whose constant field is algebraically closed in K, then the natural density of this set also exists and is equal to $\#C/\#G$.*

We will use the following easy lemma from [Odo85].

Lemma 6.3 ([Odo85], Lemma 4.3)**.** *Let* $\mathrm{FPP}([S_d]^n)$ *denote the proportion of elements of $[S_d]^n$ with a fixed point. Then*

$$\lim_{n\to\infty} \mathrm{FPP}([S_d]^n) = 0.$$

Since we assume k is a global field, k is Hilbertian and we can apply Lemma 4.2. We will make use of the following lemma in the proof of Theorem 6.5 to argue that if k is a function field, then for any n there exists a Hilbert set $\mathcal{H}$ in k^d such that for all $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$ with $(c_{d-1}, \ldots, c_0) \in \mathcal{H}$, $\mathrm{Gal}(f^n(x)/k) \cong [S_d]^n$ and the splitting field of $f^n(x)$ over k is a geometric extension.

Lemma 6.4 ([FJ08], Corollary 12.2.3)**.** *Let L be a finite separable extension of a field K. Then every Hilbert subset of L^r contains a Hilbert subset of K^r.*

Theorem 6.5. *If k is a global field $d \geq 2$, with $(d, \mathrm{char}\, k) \neq (2, 2)$, then for all $\epsilon > 0$, there is a Hilbert subset $\mathcal{H}$ of k^d, such that for all $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$ with $(c_{d-1}, \ldots, c_0) \in \mathcal{H}$, $\delta_D(P_f(a_0)) = \delta_N(P_f(a_0)) < \epsilon$, for any $a_0 \in k$.*

The arguments provided here are essentially the same as those given in [Odo85] and [Jon08].

Proof. By Lemma 6.3, we can choose n_0 so that $\mathrm{FPP}([S_d]^{n_0}) < \epsilon$. First suppose k is a number field; by Theorem 1.1, $\mathrm{Gal}(\mathfrak{G}^{n_0}(x)/k(\mathbf{s})) \cong [S_d]^{n_0}$. Then, by Lemma 4.2, there is a Hilbert subset of k^d such that for all $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$ with $(c_{d-1}, \ldots, c_0)$ in this set, $\mathrm{Gal}(f^{n_0}(x)/k) \cong [S_d]^{n_0}$. Define $\mathcal{H}$ to be this subset.

On the other hand, if k is a global function field with full field of constants $\mathbb{F}_q$, consider the constant field extension $k' = \mathbb{F}_{q^{d^{n_0}!}} \cdot k$ of k. We choose k' in this way so that any extension of $\mathbb{F}_q$ contained in the splitting field of a specialization of $\mathfrak{G}^{n_0}(x)$ to $k[x]$ must be contained in k'. By Theorem 1.1, $\mathrm{Gal}(\mathfrak{G}^{n_0}(x)/k'(\mathbf{s})) \cong [S_d]^{n_0}$. So by Lemma 4.2, there is a Hilbert subset $\mathcal{H}'$ of $(k')^d$ such that for all $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$ with $(c_{d-1}, \ldots, c_0)$ in this set, $\mathrm{Gal}(f^{n_0}(x)/k') \cong [S_d]^{n_0}$. Now, by Lemma 6.4 there is a Hilbert subset $\mathcal{H}$ of k^d such that $\mathcal{H} \subset \mathcal{H}'$. So for all $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$ with $(c_{d-1}, \ldots, c_0) \in \mathcal{H} \subset \mathcal{H}'$ we have $\mathrm{Gal}(f^{n_0}(x)/k) \cong \mathrm{Gal}(f^{n_0}(x)/k') \cong [S_d]^{n_0}$. Also, if L is the splitting field of $f^{n_0}(x)$ over k, then $L \cap \overline{k} = k$, as otherwise $L \cap k' \supsetneq k$, which would imply $[L : k] > [L : k']$ and $\mathrm{Gal}(f^{n_0}(x)/k) \supsetneq \mathrm{Gal}(f^{n_0}(x)/k') \cong [S_d]^n$, which is a contradiction.

With $\mathcal{H}$ as above, let $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0$ for $(c_{d-1}, \cdots, c_0) \in \mathcal{H}$ and let $a_0 \in k$. Now, let $P_f(a_0)$ denote the set of primes of k such that $v_{\mathfrak{p}}(f^n(a_0)) \neq 0$ for some n. We split $P_f(a_0)$ into three sets:

$$P_1 = \{\mathfrak{p} : v_{\mathfrak{p}}(f^n(a_0)) < 0 \text{ for some } n \in \mathbb{N}\},$$
$$P_2 = \{\mathfrak{p} : \mathfrak{p} | f(a_0) \ldots f^{n_0-1}(a_0)\Delta(f^{n_0}(x))\},$$
$$P_3 = \{\mathfrak{p} : \mathfrak{p} \nmid \Delta(f^{n_0}(x)), \mathfrak{p} | f^m(a_0) \text{ for some } m \geq n_0\}.$$

The set P_1 consists of the primes for which $v_{\mathfrak{p}}(a_0) < 0$ or $v_{\mathfrak{p}}(c_i) < 0$ for some i, so clearly P_1 is a finite set. The set P_2 is also clearly finite.

Let K_{n_0} denote the splitting field of $f^{n_0}(x)$. Then, if $\mathfrak{p} \in P_3$, $\mathfrak{p} \nmid \Delta(f^{n_0}(x))$ so $\mathfrak{p}$ does not ramify in K_{n_0} and the Frobenius conjugacy class $\mathrm{Frob}\left(\frac{K_{n_0}/k}{\mathfrak{p}}\right)$ is defined. Note that if $\mathfrak{p} \in P_3$, then $\mathfrak{p}$ divides $f^m(a_0) = f^{n_0}(f^{m-n_0}(a_0))$ for some $m \geq n_0$. So, if $\mathfrak{p} \in P_3$, then $f^{n_0}(x)$ has a root mod $\mathfrak{p}$, which holds if and only if $f^{n_0}(x)$ has a linear factor mod $\mathfrak{p}$. This implies that $\mathfrak{p}$ has at least one prime ideal factor of residue degree one. Thus, $\mathrm{Frob}\left(\frac{K_{n_0}/k}{\mathfrak{p}}\right)$ fixes some root of $f^{n_0}(x)$. So we see that the union of the Frobenius conjugacy classes $\mathrm{Frob}\left(\frac{K_{n_0}/k}{\mathfrak{p}}\right)$ for $\mathfrak{p} \in P_3$ is contained in the set of elements of $[S_d]^{n_0}$ fixing at least one point. The proportion of such elements is $\mathrm{FPP}([S_d]^{n_0})$ defined above. Applying the Chebotarev Density Theorem (Theorem 6.2) we see that

$$\delta_N(P_3) \leq \mathrm{FPP}([S_d]^{n_0}) < \epsilon.$$

Then since P_1 and P_2 are finite,

$$\delta_D(P_f(a_0)) = \delta_N(P_f(a_0)) = \delta_N(P_3) \leq \mathrm{FPP}([S_d]^{n_0}) < \epsilon. \qquad \square$$

Remark 6.6. Note that the proof of Theorem 6.5 can be simplified if we only want to prove the result for the Dirichlet density, since in this case we can define the set $\mathcal{H}$ for function fields in the same way we did for number fields.

6.2. **Factorizations of iterates over $\mathbb{F}_q$.** Let F be any field and let $f(x) \in F[x]$ be squarefree with degree $m \geq 1$. Recall that we say that a permutation in S_m has *cycle pattern* $(1)^{r_1} \ldots (m)^{r_m}$ if, when it is written as a product of disjoint cycles, it consists of r_i cycles of length i for each $1 \leq i \leq m$. Note that each r_i is a nonnegative integer and $\sum_i ir_i = m$. Two permutations in S_m are conjugate if and only if they have the same cycle pattern. We will discuss the concept of cycle patterns of squarefree polynomials due to Cohen [Coh72].

Definition 6.7. Let $\pi = (1)^{r_1} \dots (m)^{r_m}$ be a cycle pattern in S_m. We say that a squarefree polynomial $f(x)$ of degree m in $F[x]$ has *cycle pattern* π if $f(x)$ has exactly r_i irreducible factors of degree i for all $1 \leq i \leq m$.

We have seen that the wreath power $[S_d]^n$ has a natural action on the d-ary rooted tree up to the n-th level. Labeling the branches at the top of the tree $1, \dots, d^n$, we can view $[S_d]^n$ as a subgroup of S_{d^n}. More precisely, we can define an injection $\iota : [S_d]^n \longrightarrow S_{d^n}$. The map ι depends only on the choice of the labeling; relabeling the tree will replace $\iota([S_d]^n)$ with a subgroup of S_{d^n} that is S_{d^n} conjugate to $\iota([S_d]^n)$. Hence, for any conjugacy class C in S_{d^n}, the size of $C \cap \iota([S_d]^n)$ is independent of the choice of ι.

Fix any ι as above. Let π be a cycle pattern in S_{d^n}, and let C be the conjugacy class of S_{d^n} consisting of permutations with cycle pattern π. Define

$$\rho(\pi) = \#(C \cap \iota([S_d]^n))/\#[S_d]^n.$$

Then $\rho(\pi)$ is a nonnegative rational number and $\sum_\pi \rho(\pi) = 1$.

Now let $\mathbb{F}_q$ be the finite field of order q and characteristic p, let $b \in \mathbb{F}_q^*$, and let π be a cycle pattern in S_{d^n}. Suppose $d \geq 2$, $n \geq 1$, and $(d,p) \neq (2,2)$. Define $A(q,b,d,n,\pi)$ to be the set of all $f(x) \in \mathbb{F}_q[x]$ such that

- $\deg f(x) = d$;
- $f(x)$ has leading coefficient $b \neq 0$;
- $f^n(x)$ is squarefree;
- $f^n(x)$ has cycle pattern π.

Theorem 6.8. *There is an $M = M(d,n) > 0$ in $\mathbb{R}$ and $q_0(d,n) \geq 2$ in $\mathbb{N}$ such that*

$$|\#A(q,b,d,n,\pi) - q^d \rho(\pi)| \leq M q^{d-\frac{1}{2}}$$

whenever $(d, \operatorname{char} \mathbb{F}_q) \neq (2,2)$, $d \geq 2$, $n \geq 1$, $b \in \mathbb{F}_q^*$, π is a cycle pattern in S_{d^n}, and $q \geq q_0$.

Proof. Let $\Omega(d,n,\overline{\mathbb{F}}_q)$ be the subset of $\mathcal{P}_d(\overline{\mathbb{F}}_q)$ consisting of those $f(x)$ such that

- $\deg(f(x)) = d$;
- $f^n(x) - t$ is x-separable over $\overline{\mathbb{F}}_q(t)$;
- $\operatorname{Gal}(f^n(x) - t/\overline{\mathbb{F}}_q(t)) \cong [S_d]^n$.

Let $B(q,b,d,n)$ be the set of all $f(x) \in \mathbb{F}_q[x]$, with leading coefficient b such that $f(x) \in \Omega(d,n,\overline{\mathbb{F}}_q)$. We first find an estimate for $\#B(q,b,d,n)$. By Theorem 3.7, $\Omega(d,n,\overline{\mathbb{F}}_q)$ contains a Zariski-open subset, namely $H(d,n,\overline{\mathbb{F}}_q)$. A more careful examination of the proof of Lemma 3.6 actually shows that there is a nonzero polynomial $\Theta(u_0,u_1,\dots,u_d)$ with coefficients in $\mathbb{F}_p$ where $p = \operatorname{char} \mathbb{F}_q$ and the total degree of Θ is bounded by some constant C depending only on d,n, such that if $\Theta(a_0,a_1,\dots,a_d) \neq 0$, then $f(x) = a_d x^d + a_{d-1}x^{d-1} + \dots + a_0 \in H(d,n,\overline{\mathbb{F}}_q)$.

The number of distinct $\beta \neq 0$ in $\overline{\mathbb{F}}_q$ such that $(u_d - \beta)$ divides $\Theta(u_0,\dots,u_d)$ in $\overline{\mathbb{F}}_q$ is clearly bounded above by C. Thus, there is a subset S of $\mathbb{F}_q^*$ with $\#S \geq (q-1) - C$ such that $\Theta(u_0,\dots,u_{d-1},s)$ is not the zero polynomial whenever $s \in S$.

By a standard number theory argument, there is a constant D, depending only on d,n, such that for each $s \in S$ the number of $(a_0,\dots,a_{d-1})$ in $(\mathbb{F}_q)^d$ for which

$\Theta(a_0, \ldots, a_{d-1}, s) = 0$ is bounded above by Dq^{d-1}. Thus, for each $s \in S$,

$$\#B(q, s, d, n) \geq q^d - Dq^{d-1}.$$

We will now show that for sufficiently large q, the above estimate holds for all b in $\mathbb{F}_q^*$. Let $s \in S$, $f(x) \in B(q, s, d, n)$, and $c \in \mathbb{F}_q^*$. It is clear that if $f(x) \in B(q, s, d, n)$, then $c^{-1}f(cx) \in B(q, sc^{d-1}, d, n)$, so the map $f(x) \mapsto c^{-1}f(cx)$ injects $B(q, s, d, n)$ into $B(q, sc^{d-1}, d, n)$. Thus,

$$\#B(q, sc^{d-1}, d, n) \geq \#B(q, s, d, n).$$

Now, let H be the subgroup of all $d-1$ powers in $\mathbb{F}_q^*$ and let $e = \gcd(q-1, d-1)$; then $\#H = (q-1)/e$. Consider the set $SH \subseteq \mathbb{F}_q^*$ the union of all the cosets of H containing elements of S. We will show that for sufficiently large q, $SH = \mathbb{F}_q^*$ and hence

$$\#B(q, b, d, n) \geq q^d - Dq^{d-1}$$

for all $b \in \mathbb{F}_q^*$.

Let r be the number of distinct cosets in SH. Note that $\#SH = r\frac{q-1}{e}$, so clearly, $r \leq e$. On the other hand, $r\#H = \#SH \geq \#S \geq (q-1) - C$. So $r \geq \frac{(q-1)-C}{\#H} = e - \frac{Ce}{q-1}$. Thus, there is some $q_0 = q_0(d, n)$ such that $r = e$ for all $q \geq q_0$.

Now, since clearly $\#B(q, b, d, n) \leq q^d$, we get the estimate

$$\#B(q, b, d, n) = q^d + O(q^{d-1}), \text{ for all } b \in \mathbb{F}_q^*. \tag{6.1}$$

Here the implied constant in the above equation depends only on d and n.

Fix $b \in \mathbb{F}_q^*$ and $f(x) \in B(q, b, d, n)$. Then by assumption we have

$$\mathrm{Gal}(f^n(x) - t/\overline{\mathbb{F}}_q(t)) \cong [S_d]^n.$$

It follows that $\mathrm{Gal}(f^n(x) - t/\mathbb{F}_q(t)) \cong [S_d]^n$ as well. Thus, the splitting field L of $f^n(x) - t$ over $\mathbb{F}_q(t)$ is a geometric extension; that is, $L \cap \overline{\mathbb{F}}_q = \mathbb{F}_q$, and there is no extension of the constant field.

Let π be any cycle pattern in $[S_d]^n$ and let C be the union of the corresponding conjugacy classes in $[S_d]^n$. Let $\alpha \in \mathbb{F}_q$. Then $f^n(x) - \alpha$ has cycle pattern π if and only if $\mathrm{Frob}\left(\frac{L/\mathbb{F}_q(t)}{t-\alpha}\right)$ has cycle pattern π. Applying an effective version of the Chebotarev Density Theorem for geometric function field extensions (see [CO77, Proposition A.3] or [KMS94]), we see that the number of $\alpha \in \mathbb{F}_q$ such that $f^n(x) - \alpha$ is squarefree with cycle pattern π is

$$q\frac{\#C}{\#[S_d]^n} + O(q^{\frac{1}{2}}) = q\rho(\pi) + O(q^{\frac{1}{2}}). \tag{6.2}$$

Here the implied constant above depends only on d, n, and the genus of L. Since the degree of the different $D_{L/\mathbb{F}_q(t)}$ can be bounded above by a constant depending only on d, n, the Riemann-Hurwitz genus formula implies that the same is true for the genus of L. Hence, the implied constant in equation 6.2 depends only on d and n.

Now treat q, b, d, n as fixed and to shorten notation write $A(\pi) = A(q, b, d, n, \pi)$ and $B = B(q, b, d, n)$. Let

$$A = \{f(x) \in \mathbb{F}_q[x] : \deg f(x) = d \text{ and } f(x) \text{ has leading coefficient } b\}.$$

For $\alpha \in \mathbb{F}_q$, let $D(\alpha,\pi) = \{f(x) \in A : f(x+\alpha) - \alpha \in A(\pi)\}$. Then

$$\sum_{\alpha\in\mathbb{F}_q} \#D(\alpha,\pi) = q\#A(\pi). \tag{6.3}$$

We will find an estimate for $\#D(\alpha,\pi)$ and hence for $A(\pi)$ by examining the set $E(\alpha,\pi) = B \cap D(\alpha,\pi)$. Note that for $f(x) \in B$ and $\alpha \in \mathbb{F}_q$, the n-th iterate of $f(x+\alpha)-\alpha$ is $f^n(x+\alpha)-\alpha$. Hence, $f(x)$ is in $E(\alpha,\pi)$ if and only if $f^n(x+\alpha)-\alpha$ is squarefree with cycle pattern π. Since clearly $f^n(x)-\alpha$ has the same cycle pattern as $f^n(x+\alpha)-\alpha$, we see that $f(x) \in E(\alpha,\pi)$ if and only if $f^n(x)-\alpha$ is squarefree with cycle pattern π. Hence, for fixed $f(x)$ equation (6.2) implies that $\#\{\alpha \in \mathbb{F}_q : f(x) \in E(\alpha,\pi)\} = q\rho(\pi) + O(q^{\frac{1}{2}})$, for all $f(x) \in B$.

Thus,

$$\sum_{\alpha\in\mathbb{F}_q} \#E(\alpha,\pi) = \sum_{f(x)\in B} \#\{\alpha\in\mathbb{F}_q : f(x)\in E(\alpha,\pi)\} = q^{d+1}\rho(\pi) + O(q^{d+\frac{1}{2}}).$$

By equation (6.1), we see that $\#D(\alpha,\pi) = \#E(\alpha,\pi) + O(q^{\frac{1}{2}})$. Hence,

$$\sum_{\alpha\in\mathbb{F}_q} \#D(\alpha,\pi) = q^{d+1}\rho(\pi) + O(q^{d+\frac{1}{2}}).$$

The desired result follows easily from equation (6.3):

$$\#A(\pi) = q^d\rho(\pi) + O(q^{d-\frac{1}{2}}).$$

□

Remark 6.9.

(1) In the cases $\pi = (1)^{d^n}$ and $\pi = (d^n)^1$, corresponding to the cases where $f^n(x)$ splits completely into distinct monic factors and $f^n(x)$ is irreducible, $\rho(\pi)$ is easy to calculate. Clearly we have $\rho((1)^{d^n}) = (\#[S_d]^n)^{-1}$, while an inductive argument on n gives $\rho((d^n)^1) = d^{-n}$. There is a formula due to Polya [Pól37] which allows one to calculate $\rho(\pi)$ for every cycle pattern π of S_{d_n} (see [Tom]). However, this formula is complicated.

(2) This result definitely does not hold for $\operatorname{char}\overline{\mathbb{F}}_q = d = 2$, since it is easily seen that $f^3(x)$ is always reducible in $\mathbb{F}_q[x]$ when q is even and $\deg f = 2$, whereas $\rho(\pi) > 0$ for $\pi = (d^n)^1$ in S_{d_n}.

Acknowledgments

This paper is dedicated to R.W.K. Odoni for his work on this project and many others that led to the development of a rich subject area. The author would also like to thank Thomas J. Tucker for suggesting this project and for many useful conversations, and Michael Zieve for finding and providing her with the preprint containing R.W.K. Odoni's unpublished work. Thanks are due to S.D. Cohen, with whom R.W.K Odoni shared many useful discussions about this project.

References

[BJ09] Nigel Boston and Rafe Jones, *The image of an arboreal Galois representation*, Pure Appl. Math. Q. **5** (2009), no. 1, 213–225, DOI 10.4310/PAMQ.2009.v5.n1.a6. MR2520459

[Coh72] Stephen D. Cohen, *The distribution of polynomials over finite fields. II*, Acta Arith. **20** (1972), 53–62. MR0291135

[Coh91] Stephen D. Cohen, *Permutation polynomials and primitive permutation groups*, Arch. Math. (Basel) **57** (1991), no. 5, 417–423, DOI 10.1007/BF01246737. MR1129514

[CO77] S. D. Cohen and R. W. K. Odoni, *The Farey density of norm subgroups of global fields. II*, Glasgow Math. J. **18** (1977), no. 1, 57–67, DOI 10.1017/S0017089500003037. MR0432597

[CH12] John Cullinan and Farshid Hajir, *Ramification in iterated towers for rational functions*, Manuscripta Math. **137** (2012), no. 3-4, 273–286, DOI 10.1007/s00229-011-0460-y. MR2875279

[Fri70] Michael Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55. MR0257033

[FJ08] Michael D. Fried and Moshe Jarden, *Field arithmetic*, 3rd ed., revised by Jarden, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. MR2445111

[GS07] Arnaldo Garcia and Henning Stichtenoth (eds.), *Topics in geometry, coding theory and cryptography*, Algebra and Applications, vol. 6, Springer, Dordrecht, 2007. MR2265387

[GTZ07] Robert M. Guralnick, Thomas J. Tucker, and Michael E. Zieve, *Exceptional covers and bijections on rational points*, Int. Math. Res. Not. IMRN **1** (2007), Art. ID rnm004, 20, DOI 10.1093/imrn/rnm004. MR2331902

[HJM15] Spencer Hamblen, Rafe Jones, and Kalyani Madhu, *The density of primes in orbits of $z^d + c$*, Int. Math. Res. Not. IMRN **7** (2015), 1924–1958, DOI 10.1093/imrn/rnt349. MR3335237

[Jan96] Gerald J. Janusz, *Algebraic number fields*, 2nd ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR1362545

[Jon08] Rafe Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. Lond. Math. Soc. (2) **78** (2008), no. 2, 523–544, DOI 10.1112/jlms/jdn034. MR2439638

[JM14] Rafe Jones and Michelle Manes, *Galois theory of quadratic rational functions*, Comment. Math. Helv. **89** (2014), no. 1, 173–213, DOI 10.4171/CMH/316. MR3177912

[JKMT16] Jamie Juul, Pär Kurlberg, Kalyani Madhu, and Tom J. Tucker, *Wreath products and proportions of periodic points*, Int. Math. Res. Not. IMRN **13** (2016), 3944–3969, DOI 10.1093/imrn/rnv273. MR3544625

[KMS94] Vijaya Kumar Murty and John Scherk, *Effective versions of the Chebotarev density theorem for function fields* (English, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528. MR1298275

[Lan64] Serge Lang, *Algebraic numbers*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London, 1964. MR0160763

[Nek05] Volodymyr Nekrashevych, *Self-similar groups*, Mathematical Surveys and Monographs, vol. 117, American Mathematical Society, Providence, RI, 2005. MR2162164

[Odo85] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414, DOI 10.1112/plms/s3-51.3.385. MR805714

[Pól37] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen* (German), Acta Math. **68** (1937), no. 1, 145–254, DOI 10.1007/BF02546665. MR1577579

[SL96] P. Stevenhagen and H. W. Lenstra Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37, DOI 10.1007/BF03027290. MR1395088

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941

[Sto92] Michael Stoll, *Galois groups over $\mathbf{Q}$ of some iterated polynomials*, Arch. Math. (Basel) **59** (1992), no. 3, 239–244, DOI 10.1007/BF01197321. MR1174401

[Tom] Ioan Tomescu, *Introduction to combinatorics.* translated from the Romanian by I. Tomescu and S. Rudeanu, edited by E. Keith Lloyd, Collet's Publishers Ltd., London, 1975. MR0396275

[vdW35] B. L. van der Waerden, *Die Zerlegungs-und Trägheitsgruppe als Permutationsgruppen* (German), Math. Ann. **111** (1935), no. 1, 731–733, DOI 10.1007/BF01472249. MR1513024

Department of Mathematics and Statistics, Amherst College, Amherst, Massachusetts 01002

Email address: jamie.l.rahr@gmail.com