ITERATES OF GENERIC POLYNOMIALS AND GENERIC RATIONAL FUNCTIONS

J. JUUL AND R.W.K. ODONI

Abstract. In [Odo85], Odoni shows that in characteristic 0 the Galois group of the $n$-th iterate of the generic polynomial is as large as possible. We generalize this result to positive characteristic, as well as to the generic rational function. This work was partially completed by the late Odoni in an unpublished paper.

1. Introduction

If $\varphi(x)$ is any polynomial in $K[x]$, where $K$ is a field, $\text{Gal}(\varphi(x)/K)$ 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

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

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

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

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

Let $k(s) = k(s_0, s_1, \ldots, s_{d-1})$ and $k(s,u) = k(s_0, s_1, \ldots, s_{d-1}, u_0, u_1, \ldots, u_d)$. In [Odo85], Odoni shows that if $\text{char} \ k = 0$, then $\text{Gal}(G^n(x)/k(s)) \cong [S_d]^n$, the $n$-th wreath power of the symmetric group $S_d$. However, some of the arguments used in this paper 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 in $\mathbb{C}$. Here, we instead use algebraic and Galois theoretic arguments to show the following.

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

It can be easily shown that, $\text{Gal}(\Phi^n(x)/k(s))$ and $\text{Gal}(\Phi^n(x)/k(s,u))$ must be contained in $[S_d]^n$. So the majority of the work in this paper involves showing that this is a lower bound 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. If $f(x) \in k[x]$ is any polynomial with degree $d$, $t$ is transcendental over $k$, and $g(x) := f(x + t) - t$, then $g^n(x) = f^n(x + t) - t$ for any $n \in \mathbb{N}$. So it follows that, $\text{Gal}(g^n(x)/k(t)) =$
Gal(f^n(x) - t/k(t)) for any n ∈ N. Then, since g^n(x) is a specialization of both G^n(x) and Φ^n(x), for any n, and Galois groups cannot increase under specializations, it suffices to show that there exists some f(x) ∈ k[x] such that Gal(f^n(x) - t/k(t)) ≃ [S_d]^n.

In Theorem 3.1, we give sufficient conditions on f(x) to ensure Gal(f^n(x) - t/k(t)) ≃ [S_d]^n. Then in Theorem 3.6, 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, in each subextension of the splitting field of f^n(x) − t there is a prime that ramifies in no other subextension. The arguments here are similar to the arguments given in [?].

We give some necessary preliminary results in Section 2. Then we prove Theorem 1.1 in Section 4. In Section 5, we handle the case char k = d = 2. In this case it is notable 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 postcritically finite.

In Section 6, we extend Odoni’s application on primes dividing orbits to global fields in any characteristic ([Odo85], Lemma 9.1). Finally, in Section 7, we apply Theorem 3.6, with k = F_q, along with the Chebotarev density theorem to prove function fields for the following application.

Let π = (1)^{r_1}...(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 ≤ i ≤ m. Then if π is a cycle pattern in S_d^n and A(q,b,d,n,π) is the set of all f(x) ∈ F_q[x] such that

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

we have the following.

**Theorem 1.2.** There is an M = M(d,n) > 0 in R and q_0(d,n) ≥ 1 in N such that

|#A(q,b,d,n,π) − q^dρ(π)| ≤ Mq^{d−\frac{1}{2}}

whenever (d, char F_q) ≠ (2, 2), d ≥ 2, n ≥ 1, b ≠ 0 in F_q, π is a cycle pattern in S_d^n and q ≥ q_0. Where ρ(π) 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 \{α_1, ..., α_d\} and \{β_1, ..., β_l\} respectively. The set \{(π, τ_1, ..., τ_d) | π ∈ G, τ_1, ..., τ_d ∈ H\}
forms a group called the **wreath product of** $G$ by $H$, denoted $G[H]$. $G[H]$ acts on the set $\{\alpha_1, \ldots, \alpha_d\} \times \{\beta_1, \ldots, \beta_\ell\}$ by $(i, r) \mapsto (\pi(i), \tau_r(r))$.

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

**Proof.** Let $\{\alpha_1, \ldots, \alpha_d\}$ be the zeros of $\varphi(x)$ then $\varphi(\psi(x)) = \prod_{i=1}^d (\psi(x) - \alpha_i)$ and the zeros of $\varphi(\psi(x))$ are $\{\beta_{i,r} | i = 1, \ldots, d, r = 1, \ldots, \ell\}$ where $\{\beta_{i,r} | r = 1, \ldots, \ell\}$ is the set of zeros of $\psi(x) - \alpha_i$. Let $\sigma \in \text{Gal}(\varphi(\psi(x))/K)$. Let $F$ be the splitting field of $\varphi(x)$ over $K$, then $\sigma$ induces a permutation $\pi := \sigma|_F$ on $\{\alpha_1, \ldots, \alpha_d\}$ (i.e. $\pi \in G$). We can think of $\pi$ as a permutation on the indices $\{1, \ldots, d\}$ defined by $\alpha_{\pi(i)} := \pi(\alpha_i)$. Now fix $i$, and note that $\sigma(\beta_{i,r}) = \beta_{\pi(i), s}$ for some $s$ since $\psi(\sigma(\beta_{i,r})) = \sigma(\psi(\beta_{i,r})) = \sigma(\alpha_i) = \pi(\alpha_i) = \alpha_{\pi(i)}$, which implies $\sigma(\beta_{i,r}) = \beta_{\pi(i), s}$ for some $s$. This defines a map $\tau \mapsto s$ which is a permutation of $\{1, \ldots, \ell\}$, we call this map $\tau_\pi$. Then, $\sigma$ is given by $\sigma(\beta_{i,r}) = \beta_{\pi(i), \tau_\pi(r)}$. Thus, we can define a map $\text{Gal}(\varphi(\psi(x))/K) \to G[S_\ell]$ by $\sigma \mapsto (\pi, \tau_1, \ldots, \tau_\ell)$ which is easily shown to be an injective homomorphism. □

**Corollary 2.3.** If $\varphi(x)$ is a rational function in $K(x)$, $\deg(\varphi) = d$, and $\varphi^n(x)$ has $d^n$ distinct zeros in $\bar{K}$, then $\text{Gal}(\varphi^n(x)/K)$ can be embedded in $S_d^n$.

### 2.2. Discriminants and Ramification

Let $M/K$ be a finite Galois extension. If $p$ is a prime of $K$ and $q$ is any prime of $M$ extending $p$, we define $e(q|p)$ to be the inertia degree of $q$ over $p$ and $f(q|p)$ to be the residue degree of $q$ over $p$.

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

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

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

where $D(\tau(q)|\mathfrak{P})$ is the decomposition group of $\tau(q)$ over $\mathfrak{P}$. So, the orbit/stabilizer theorem implies
\[
\# Y = \frac{\# D(q|p)}{\# \text{Stab}_{D(q|p)}(H\tau)} = \frac{\# D(q|p)}{\# D(\tau(q)|\mathfrak{P})} = \frac{\# D(q|p)}{\# D(q|\mathfrak{P})} = e(\mathfrak{P}|p)f(\mathfrak{P}|p).
\]

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 \( D(q|p) \), then \( \exists \gamma \in D(q|p) \) such that \( H\tau\gamma = H\sigma \) which implies \( \tau\gamma\sigma^{-1} \in H \). So \( \sigma(q) \cap L = \tau\gamma\sigma^{-1}(\sigma(q) \cap L) = \tau(q) \cap L \) and the map is well-defined. Clearly the map is surjective, since \( G \) permutes the primes of \( M \) lying above \( p \) transitively. To see that this map is one-to-one suppose \( \tau(q) \cap L = \sigma(q) \cap L = \mathfrak{P} \). Then \( \tau(q), \sigma(q) \) 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 \( \gamma\tau(q) = \sigma(q) \). Then, \( \sigma^{-1}\gamma\tau(q) = q \) so \( \sigma^{-1}\gamma\tau \in D(q|p) \). 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 \( D(q|p) \).

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

\[
\text{Stab}_{I(q|p)}(H\tau) = \{ \gamma \in I(q|p) | H\tau\gamma = H\tau \} = I(\tau(q)|\mathfrak{P})
\]

where \( I(\tau(q)|\mathfrak{P}) \) is the inertia group of \( \tau(q) \) over \( \mathfrak{P} \). Using the orbit/stabilizer theorem again,

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

\[\square\]

Remark 2.5. The set \( G/H \) is the set of \( K \) homomorphisms \( L \to M \). In the case \( L \cong K(\theta) \) where \( \theta \) is a root of some \( f \in K[x] \), this corresponds to the set of zeros of \( f \) in \( M \).

Let \( A \) be a Dedekind domain, \( K \) the field of fractions of \( A \), \( L \) a separable extension of \( K \), and \( B \) the integral closure of \( A \) in \( L \). It is a standard result that any prime of \( A \) that ramifies in the integral closure of \( B \) 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 \( p \subseteq A \) be a prime and \( pB = \prod q_i^{e_i}, f_i = f(q_i|p) \) the residue degree, then the power of \( p \) in \( \Delta(B/A) \) is greater than or equal to \( \sum (e_i - 1)f_i \) with equality if and only if \( \text{char } K \) does not divide \( e_i \).

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 \( \theta \) be a root of \( P(x) \), and let \( L = K(\theta) \), if \( B = A[\theta] \), that is, if \( A[\theta] \) 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 \( p \) ramifies in \( B \) then \( v_p(\Delta(P(x))) = v_p(\Delta(B/A)) \). We assume this is the case for the rest of this section and let \( M \) be the splitting field of \( P(x) \) over \( K \).

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

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

**Corollary 2.9.** If \( \text{char}(K) = 2 \) and \( p^2||\Delta(P(x)) \) in \( A \), then for any prime \( q \) of \( M \) lying over \( p \), the action of \( I(q|p) \) 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 \( pB = \mathfrak{P}_1^2\mathfrak{P}_2 \ldots \mathfrak{P}_m \) where \( f(\mathfrak{P}_i|p) = 1 \), or \( pB = \mathfrak{P}_1^3\mathfrak{P}_2 \ldots \mathfrak{P}_m \) where \( f(\mathfrak{P}_i|p) = 1 \), for some primes \( \mathfrak{P}_1, \ldots, \mathfrak{P}_m \) in \( B \). If \( q \) is a prime of \( M \) lying over \( p \), then by Lemma 2.4, the action of \( I(q|p) \) on \( \{\alpha_1, \ldots, \alpha_d\} \) consists of a single transposition, or a single three cycle, respectively.

The following result is standard (see [Sti09], for example).

**Lemma 2.10.** 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 \( p \in \mathbb{P}_{k(t)} \setminus \{p_\infty\} \) and tamely ramified at \( p_\infty \), here \( \mathbb{P}_{k(t)} \) denotes the set of primes of \( k(t) \).

**Proof.** Let \( F \) be any extension of \( k(t) \) with field of constants \( k \) and let \( d = [F : k(t)] \). For the prime \( p_\infty \) of \( k(t) \), \( \sum_{q||p_\infty}(e(q|p_\infty) - 1) \deg q \leq d - 1 \) where the sum ranges over all \( q \) extending \( p_\infty \). Let \( g' \) be the genus of \( F \). From the Riemann Hurwitz formula we have

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

\[
2g' - 2 \leq -2d + \sum_{p \in \mathbb{P}_{k(t)}} \sum_{p' \mid p, p \neq p_\infty} (e(p'|p) - 1) \deg p' + d - 1,
\]
where the second sum is taken over all \( p' \) extending \( p \) in \( F \). Then since \( g' \geq 0 \),

\[
d - 1 \leq \sum_{p \in \mathbb{P}(k)} \sum_{p' \mid p, p \neq p_\infty} (e(p' \mid p) - 1) \deg p'.
\]

Since \( d \geq 2 \), some prime in \( \mathbb{P}(k) \setminus \{p_\infty\} \) must ramify in \( F \). \( \square \)

### 2.3. Results on subgroups of \( S_d \)

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] that can be found in [Coh91].

**Lemma 2.11.** ([Coh91], Lemma 3.1) A separable polynomial \( f \) 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 \( G_a = \text{Stab}_G(a) \subseteq G_S = \{\sigma \in G | \sigma(S) = S\} \). So \( G_a \) 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 (non-linear) rational functions \( g, h \) with coefficients in \( F \). Then, since \( f = g(h) \) we can find \( g, h \) (non-linear) polynomials with coefficients in \( F \). Thus, \( f \) is decomposable over \( F \).

Conversely, if \( f = g(h) \) is decomposable then the relation \( a \sim b \) if \( h(a) = h(b) \) gives a nontrivial partition of \( \{a_1, \ldots, a_d\} \) preserved by \( G \). \( \square \)

**Lemma 2.12.** 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 \( G = S_d \). \( \square \)

**Lemma 2.13.** If \( G \) is a transitive subgroup of \( S_d \), with \( d > 1 \), that is generated by transpositions then \( G = S_d \).

**Proof.** Let \( S \) be the set of all subgroups \( H \) of \( G \), such that \( H \cong S_k \) some \( k = 1, \ldots, d \). \( S \) is nonempty since there are subgroups of \( G \) which are isomorphic to \( S_1 \) and \( S_2 \). Let \( m \in \{1, \ldots, d\} \) be maximal such that there exists \( H \in S \) with \( H \cong S_m \). 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 \( m \). \( \square \)

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

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

3. \( f^n(x) - t \)

In this section, let \( k \) be an algebraically closed field with characteristic \( p \) (where \( p \) is allowed to be 0). Let \( x, t \) be algebraically independent variables over \( k \), and let \( f(x) \in k[x] \) be a polynomial with degree \( d > 1 \), where \( (d, p) \neq (2, 2) \). Then, for \( n \in \mathbb{N} \), \( f^n(x) - t \) is irreducible, and if \( \frac{d}{dx}f(x) \neq 0 \) then \( f^n(x) - t \) is \( x \)-separable, since \( \frac{d}{dx}(f^n(x) - t) = \frac{d}{dx}f^n(x) \neq 0 \) by induction on \( n \). Fix \( n \in \mathbb{N} \), we give conditions on \( f(x) \) that ensure \( \text{Gal}(f^n(x) - t/k(t)) \cong [S_d]^N \). Then we show that the set of all \( f(x) \in k[x] \) of degree \( d \) with the property \( \text{Gal}(f^n(x) - t/k(t)) \cong [S_d]^N \) contains a Zariski open subset of \( P_d(k) \).

**Theorem 3.1.** Let \( f(x) \in k[x] \) with \( \text{Gal}(f(x) - t/k(t)) \cong S_d \). If char \( k \neq 2 \), \( f \) has some critical point \( a \) with multiplicity one such that \( f^n(a) \neq f^m(b) \) for all \( m < n \leq N \) and all critical points \( b \neq a \), then \( \text{Gal}(f^n(x) - t/k(t)) \cong [S_d]^N \). If char \( k = 2 \), \( f \) has some critical point \( a \) such that \( f^n(a) \neq f^m(b) \) for all \( m < n \leq N \) and all critical points \( b \neq a \), and \( I(q, f(a) - t) \) consists of a single transposition for any prime \( q \) lying above \( (f(a) - t) \) in the splitting field of \( f(x) - t \) over \( k(t) \), then \( \text{Gal}(f^n(x) - t/k(t)) \cong [S_d]^N \).

Before we prove the theorem we fix some notation and prove a lemma. Let \( K_n \) be the splitting field of \( f^n(x) - t \) over \( k(t) \), \( \alpha_1, ..., \alpha_{d^n} \) be the roots of \( f^n(x) - t \), \( M_i \) be the splitting field of \( f(x) - \alpha_i \) over \( k(\alpha_i) \), and \( \tilde{M}_i = K_n \prod_{j \neq i} M_j \).

**Lemma 3.2.** Let \( n < N \), the prime \( (f(a) - \alpha_i) \) of \( k[\alpha_i] \) does not ramify in \( \tilde{M}_i \).

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

We have assumed that \( f^{n+1}(a) - t \neq f^m(b) - t \) for any \( m \leq n \) and any critical points \( b \) of \( f \) with \( b \neq a \). Thus, we see that \( (f^{n+1}(a) - t) \) does not ramify in \( K_n \) since the only primes of \( k(t) \) that ramify in \( K_n \) must divide
\[ \Delta(f^n(x) - t) = \prod_{b \in f_c} \left( (f(b) - t)^{d^n-1} (f^2(b) - t)^{d^n-2} \ldots (f^n(b) - t) \right)^{e(b|f(b))}. \]

Where \( f_c \) is the set of critical points of \( f \), and \( e(b|f(b)) \) is the ramification index of \( b \) over \( f(b) \). Since \( (f(a) - \alpha_i) \) extends \( (f^{n+1}(a) - t) \) in \( k(\alpha_i)/k(t) \), it follows that \( (f(a) - \alpha_i) \) does not ramify in \( K_n \).

We can also see that that \( (f(a) - \alpha_i) \) does not ramify in \( M_jK_n \) for \( j \neq i \) since the primes of \( K_n \) ramifying in \( M_jK_n \) are those dividing
\[ \Delta(f(x) - \alpha_j) := \prod_{b \in f_c} (f(b) - \alpha_j)^{e(b|f(b))}. \]

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

**Proof.** (Proof of Theorem 3.1) We use induction on \( n \). The result holds in the case \( n = 1 \) by hypothesis.

Let \( 1 < n < N \), suppose \( \text{Gal}(f^n(x) - t/k(t)) \cong [S_d]^n \). Let \( \alpha_1, \ldots, \alpha_{dn} \) be the distinct roots of \( f^n(x) - t \). \( \text{Gal}(M_i/k(\alpha_i)) \cong \text{Gal}(f(x) - t/k(t)) \cong S_d \) where \( M_i \) is the splitting field of \( f(x) - \alpha_i \) over \( k(\alpha_i) = k(\alpha_i, t) \).

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

Note, the extension \( M_i \cap \widehat{M_i}/k(\alpha_i) \) is Galois, so \( \Gamma := \text{Gal}(M_i/M_i \cap \widehat{M_i}) \) is a normal subgroup of \( \text{Gal}(M_i/k(\alpha_i)) \cong S_d \). So either \( \Gamma \cong S_d \), or \( \Gamma \) is isomorphic to a subgroup of \( A_d \). Let \( p \) be the prime \( (f(a) - \alpha_i) \) of \( k[\alpha_i] \). If \( p \neq 2 \) and \( p||\Delta(f(x) - \alpha_i) = \prod_{b \in f_c} (f(b) - \alpha_j)^{e(b|f(b))} \). Thus, if \( q \) is any prime of \( M_i \) lying over \( p \), then by Lemma 2.8, \( I(q|p) \) consists of a single transposition. If \( p = 2 \), then by hypothesis, \( I(q|p) \) consists of a single transposition. Now fix a prime \( q \) of \( M_i \) lying over \( p \), and let \( p' := q \cap (M_i \cap \widehat{M_i}) \). By Lemma 3.2, we see that \( p \) does not ramify in \( \widehat{M_i} \) which implies \( p' \) is unramified over \( p \). Hence, \( e(q|p') = e(q|p) = 2 \), which implies \( I(q|p') \) is isomorphic to \( I(q|p) \), so \( \Gamma \) must contain a transposition. Thus, \( \Gamma \not\subseteq A_d \) and we have \( \Gamma \cong S_d \) as desired. \( \square \)
Next, we show that the conditions in Theorem 3.1 are not too restrictive and in fact “most” polynomials satisfy the more restrictive conditions listed below.

**Definition 3.3.** Define $H(d, N, k)$ to be the set of all $f(x) \in k[x]$ such that

1. $\deg f'(x) = d - 1$ if $p \nmid d$, $\deg f'(x) = d - 2$ if $p \mid d$,
2. there is a separable polynomial $g(x)$ such that $f'(x) = g(x)$ if $p \neq 2$ and $f'(x) = g(x)^2$ if $p = 2$,
3. if $w_1, \ldots, w_r$ are the roots of $g(x)$ 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 $p \mid d$, we add;

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

**Remark 3.4.** We could impose conditions 4 and 5 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 3.5.** $H(d, N, k)$ is a nonempty Zariski open subset of $\mathcal{P}_d(k)$.

**Proof.** First let $H_N$ be the set of all $f(x) \in \mathcal{P}_d(k)$ satisfying conditions 1-3 above. Let $x, y_1, y_2, \ldots, y_r, u_0, u_1, \ldots, u_d, v$ be algebraically independent variables over $k$ and define

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

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

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

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

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 $\sum_{j} j u_j x^{j-1} = \sum_{j} v_i x^i$.

If $p = 2$, then we let $D$ as above but specialize $v_j$ so that $\sum_{j} u_j x^{j-1} = (\sum v_i x^i)^2 = \sum v_i^2 x^{2i}$. In either case, $D$ specializes to a polynomial $h(u_0, \ldots, u_d) \in k[u_1, \ldots, u_d]$. It is clear that if $h(u_0, \ldots, u_d) \neq 0$ then $f(x) = \sum a_i x^i \in H_N$ 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

- $\deg f'(x) = d - 1$ if $p \nmid d$, $\deg f'(x) = d - 2$ if $p \mid d$,
• $f'(x) = g(x)$ if $p \neq 2$, $f'(x) = g(x)^2$ if $p = 2$ where $g$ is a separable, and
• if $w_1, \ldots, w_r$ are the roots of $g(x)$ then $f(w_i) \neq f(w_j)$ unless $i = j$.

We first show that $H_1$ is nonempty. If $p = 0$, $p \nmid d(d - 1)$, or $p = 2$ and $d \equiv 3 \pmod{4}$, and $f(x) = a_d x^d + a_1 x + a_0$ with $a_0 a_1 a_d \neq 0$, then $f(x) \in H_1$.

In the case, $p > 2$ and $p|d$, we have, $d \geq p \geq 3$ and $p \nmid d - 1$. If $f(x) = a_d x^d + a_{d-1} + a_1 x + a_0$ with $a_0 a_1 a_{d-1} a_d \neq 0$, then $f(x) \in H_1$. If $p > 2$ and $p|d - 1$, then $d \geq p + 1 \geq 4$, and $f(x) \in H_1$ for any $f(x) = a_d x^d + a_2 x^2 + a_0$ with $a_0 a_2 a_d \neq 0$.

Finally, we consider the case $p = 2$ and $d \not\equiv 3 \pmod{4}$. If $d \equiv 0 \pmod{4}$ and $f(x) = a_d x^d + a_{d-1} x^{d-1} + a_1 x + a_0$ with $a_0 a_1 a_{d-1} a_d \neq 0$, then $f(x) \in H_1$. If $d \equiv 1 \pmod{4}$ then $f(x) = a_d x^d + a_3 x^3 + a_0$ with $a_0 a_3 a_d \neq 0$ will lie in $H_1$. If $d \equiv 2 \pmod{4}$, $f(x) \in H_1$ if $f(x) = a_d x^d + a_{d-1} x^{d-1} + a_3 x^3 + a_0$ with $a_0 a_3 a_{d-1} a_d \neq 0$.

We will show that there is some $f(x) \in H_1$ such that $f(x)$ satisfies $f^i(w_i) \neq f^j(w_j)$, for all $1 \leq i, j \leq r$ and $m, n \leq N$, unless $m = n$ and $i = j$. 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 $k$ is infinite, we may choose $\lambda, \mu$ so that $f^*(x) \in H_N$. Thus, $H_N \neq \emptyset$.

Now, if $p = 2$, consider the set of $f(x) \in \mathcal{P}_d(k)$ satisfying condition 4 above. Let $s, v, u_0, \ldots, u_{d-3}, y_0, \ldots, y_d, x$ be algebraically independent variables over $k$, and define $\pi_0, \ldots, \pi_d \in k[s, v, u_0, \ldots, u_d]$ so that

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

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, $R/\mathfrak{P} \cong k[s, v, u_0, \ldots, u_d]$, 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 $F(k[y_0, \ldots, y_d]/\mathfrak{p})$ over $k$ does not exceed $d$, where $F(k[y_0, \ldots, y_d]/\mathfrak{p})$ is the field of fractions of $k[y_0, \ldots, y_d]/\mathfrak{p}$. Let $V$ be the variety in $A_{k+1}^{k+1}$ corresponding to $\mathfrak{p}$. Then $V$ is Zariski closed and not equal to $A_{k+1}^{k+1}$. It is clear that if $f(x) = a_d x^d + \ldots + a_0$ fails to satisfy the fourth property then $(a_0, \ldots, a_d) \in V$. Thus, the set $V^c$ is a nonempty Zariski open set on which condition 4 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 $k[x]$ 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. Now we introduce algebraically independent variables $x, y_0, \ldots, y_d, s_0, \ldots, s_e, t_0, \ldots, t_{f-1}$.
over $k$ and define $\pi_0, \ldots, \pi_d \in k[s_0, \ldots, s_e, t_0, \ldots, t_{f-1}]$ so that
\[ \sum_{j=0}^{d} \pi_j x^j = \sum_{i=0}^{e} s_i \left( x^f + \sum_{i=0}^{e-1} t_i x^i \right)^i. \]

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

If $d = 4$ and $e = f = 2$ we need a different argument. First, if char $k = 2$ and $a_4 a_3 \neq 0$, then it is easy to see that $f(x) = a_4 x^4 + \ldots + a_0$ is indecomposable.

If 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 $d g = 2$. Then $f(c + x) = f(c - x)$, so if we write $f(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$, 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 $16a_4 a_2^3 - 8a_2 a_3 a_4 + 3a_3^2 a_4 - a_3^3 = 0$.

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

**Theorem 3.6.** If $f(x) \in H(d, N, k)$, then $\text{Gal}(f^N(x) - t/k(t)) \cong [S_d]^N$.

**Proof.** We show that if $f(x)$ satisfies the hypotheses of Theorem 3.1. If $p \neq 2$ then $\Delta(f(x) - t) = \prod_{i=1}^{r} (f(w_i) - t)$ which is squarefree in $k[t]$ since we assumed that $f(w_1), \ldots, f(w_r)$ are all distinct. Thus, by Corollary 2.8, the result holds.

If $p = 2$, then $\Delta(f(x) - t) = \prod_{i=1}^{r} (f(w_i) - t)^2$. So Corollary 2.9 implies that $I(q|p)$ consists of a transposition or a three cycle for any ramified prime $p = f(w_i) - t$ and any $q$ lying over $p$. Now, property 4 in the definition of $H(d, N, k)$ implies that the reduction $f(x) - t \mod p$ is cube free. Which by a standard result in number theory (see [Jan96], for example) implies that, in fact we cannot have $pk[\alpha] = \mathfrak{P}_1^{3} \mathfrak{P}_2 \ldots \mathfrak{P}_m$, where $\alpha$ is a root of $f(x) - t$, so it must be that $pk[\alpha] = \mathfrak{P}_1^{2} \mathfrak{P}_2 \ldots \mathfrak{P}_m$ with $f(\mathfrak{P}_1|p) = 1$. Then Lemma 2.6 implies $I(q|p)$ consists of a single transposition.

Now we show $\text{Gal}(f(x) - t/k(t)) \cong S_d$. First, we consider the case $p \nmid d$. Let $M$ be the splitting field of $f(x)$ over $k(t)$, and let $I \subseteq G$ be the subgroup generated by $\{ I(q|p) : q|p, q \in \mathcal{P}_M, \text{ and } p \in \mathcal{P}_{k(t)} \setminus \{p_\infty\} \}$. Then $M^I$ is unramified over all primes of $k(t)$, so by Lemma 2.10, $M^I = k[t]$. Thus, $G = I$. So $G$ is a transitive subgroup of $S_d$ generated by transpositions so Lemma 2.13 implies $G \cong S_d$. 


If $p|d$, then property 5 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, Lemma 2.11 and Lemma 2.12 imply $G \cong S_d$, as desired. Also, by the above arguments we see that $f(x)$ satisfies the hypotheses of Theorem 3.1 for any critical point $a$ of $f$. □

4. GENERIC POLYNOMIALS AND GENERIC RATIONAL FUNCTIONS

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

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

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

$$\Phi(x) = \frac{x^d + s_{d-1}x^{d-1} + \ldots + s_0}{u_dx^d + u_{d-1}x^{d-1} + \ldots + u_0}$$

is the generic rational function of degree $d$ over $k$. We use the notation, $s := \{s_0, s_1, \ldots, s_{d-1}\}$ and $s, u := \{s_0, s_1, \ldots, s_{d-1}, u_0, u_1, \ldots, u_d\}$.

We will prove Theorem 1.1, first we need a lemma.

**Lemma 4.1.** ([Od95], Lemma 2.4) Let $A$ be an integrally closed domain with field of fractions $K$, let $K'$ be any field, and let $\psi : A \to K'$ be a ring homomorphism. Define $\tilde{\psi} : A[x] \to K'[x]$ by $a_dx^d + a_{d-1}x^{d-1} + \ldots + a_0 \mapsto \psi(a_d)x^d + \psi(a_{d-1})x^{d-1} + \ldots + \psi(a_0)$. If $f(x) = a_dx^d + \ldots + a_0$ is a polynomial in $A[x]$, $d \geq 1$, $a_d \neq 0$, and $a_d \notin \ker(\psi)$, such that $\tilde{\psi}(f(x))$ is separable over $K'$ then $f(x)$ is separable over $K$ and $\text{Gal}(\tilde{\psi}(f(x))|K')$ is isomorphic to a subgroup of $\text{Gal}(f(x)|K)$.

Now we prove Theorem 1.1 for $(d, p) \neq (2, 2)$, the result follows almost immediately from Lemma 3.6.

**Proof.** (Proof of Theorem 1.1) Let $k$ be any field (not necessarily algebraically closed). Let $f(x) \in H(d, n, \bar{k})$. If $b \in \bar{k}$ then it is easy to see that $f^*(x) = b^{-1}f(bx) \in H(d, n, \bar{k})$ so without loss of generality we can assume $f(x)$ is monic. Then by Lemma 3.6, $\text{Gal}(f^n(x) - t/\bar{k}(t)) \cong [S_d]^n$. Now let $g(x) := f(x + t) - t$. Then $g^n(x) = f^n(x + t) - t$, so $\text{Gal}(g^n(x)/\bar{k}(t)) \cong \text{Gal}(f^n(x) - t/\bar{k}(t)) \cong [S_d]^n$.

Now consider the maps $\psi_1 : \bar{k}[s] \to \bar{k}(t)$ and $\psi_2 : \bar{k}[s, u] \to \bar{k}(t)$, 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 $\psi_1 : \bar{k}[s][x] \to \bar{k}(t)[x]$ and $\psi_2 : \bar{k}[s, u][x] \to \bar{k}(t)[x]$ to $\tilde{\psi}_1$ and $\tilde{\psi}_2$ in the natural way. Let $P_n(x)$ be the numerator of $\Phi^n(x)$ then $\tilde{\psi}_1(\Phi(x)) = \tilde{\psi}_2(P_n(x)) = g(x)$. Then, Lemma 4.1 implies $\text{Gal}(\Phi^n(x)/\bar{k}(s)) \supseteq [S_d]^n$ and $\text{Gal}(\Phi^n(x)/\bar{k}(s, u)) \supseteq [S_d]^n$. On the other hand, by Corollary 2.3, $\text{Gal}(\Phi^n(x)/\bar{k}(s)) \subseteq [S_d]^n$ and $\text{Gal}(\Phi^n(x)/\bar{k}(s, u)) \subseteq [S_d]^n$. Thus, we get equality in both cases.

□

We handle the case $d = p = 2$ in Section 5.
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. As in Section 3, discriminants will play an important role here. Let \(\varphi(x) \in k(x)\) be a rational function, then we can write \(\varphi(x) = \frac{p(x)}{q(x)}\) for some \(p(x), q(x) \in k[x]\). Let \(t\) be transcendental over \(k\) and consider the case where \(L\) is the splitting field of \(\varphi(x) - t\) over \(k(t)\). Then \(L\) is the splitting field of \(p(x) - tq(x)\), so any prime of \(k[t]\) that ramifies in \(L\) must divide \(\Delta(p(x) - tq(x))\). In order to make our computations easier we use the following result of Cullinan and Hajir [CH12], which shows that one may calculate the discriminant in terms of the critical points of \(\varphi(x)\).

**Lemma 5.1.** ([CH12, Proposition 1])

\[
\Delta(p(x) - tq(x)) = C \text{Res}(p'(x)q(x) - p(x)q'(x), p(x) - tq(x)) = C' \prod_{a \in \varphi_t} (\varphi(a) - t)^{e(a/\varphi(a))}
\]

where \(C, C' \in k\) are constants, \(\varphi_t = \{a : \varphi'(a) = 0\}\), and \(e(a/\varphi(a))\) is the ramification index of a over \(\varphi(a)\).

Thus, we see that any prime \(p\) of \(k[t]\) that ramifies in a splitting field for \(p(x) - tq(x)\) must divide \(\prod_{a \in \varphi_t} (\varphi(a) - t)^{e(a/\varphi(a))}\).

**Theorem 5.2.** Let \(k\) be an algebraically closed field with characteristic 2, for any \(N \in \mathbb{N}\), there is a Zariski open subset, \(H\), of \(\text{Rat}_2(k)\) such that for any \(\varphi(x) \in H\), \(\text{Gal}(\varphi^N(x) - t/k(t)) \cong [S_2]^N\).

The proof here is similar to the arguments above.

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

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

If \(\varphi(x) = \frac{ax^2 + bx + c}{dx^2 + ex + f}\) then \(\varphi'(x) = \frac{(a_1b_2 - a_2b_1)x^2 + (a_1b_3 - a_3b_1)}{(b_2x^2 + b_1x + b_0)^2}\), so \(\varphi\) has a finite critical point if \(a_1b_2 - a_2b_1 \neq 0\). Using the same arguments as in the proof of Lemma 3.5, we see that \(H\) is Zariski open. To see that \(H\) is nonempty, note that if \(\varphi(x) = x^2 + a_1x + a_0\) where \(\frac{a_1}{a_0} \neq 0\), then the second property holds up to the first iterate. To see that this property holds for any \(N\), we again refer to the arguments from Lemma 3.5.

Let \(p_n(x), q_n(x)\) be the numerator and denominator of the \(n\)-th iterate of \(\varphi(x)\) respectively. Then, the splitting field of \(\varphi^n(x) - t\) is the splitting field of \(p_n(x) - tq_n(x)\). Using the discriminant formula in Lemma 5.1, the same arguments used in the proof of Theorem 3.6 can be applied to complete the proof. Here the fact that \(G_1 = S_2\) and the existence of a transposition
in the inertia subgroup follow immediately from the fact that the group is nontrivial and contained in $S_2$. 

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

**Proof.** 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 Theorem 1.1. □

### 5.2. Polynomial functions.

The above arguments for rational functions depend on the fact that we can find rational functions $\varphi$ for which the critical point of $\varphi$ has an infinite orbit. However, for polynomials of degree two in characteristic two, the situation is much different. Since in characteristic two any separable polynomial of degree two is ramified only at infinity, which is a fixed point, that is, the polynomial is post critically finite. Thus, we can expect the result to be much different in this case.

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

**Theorem 5.4.** $\text{Gal}(\Phi(x)/k(s, t)) \cong R_n \times R_n^s$ where $R_n = \mathbb{F}_2[Y]/(Y^n)$ and $R_n \times R_n^s$ is the group of invertible affine linear transformations of $R_n$.

**Proof.** Let $E$ be an algebraic closure of $k(s, t, x)$ and let $K \subset E$ be an algebraic closure of $k(s)$. Let $L : E \rightarrow E$ be the map defined by $L(\xi) = \xi^2 + s\xi$. Then $L$ is $\mathbb{F}_2$-linear and surjective, furthermore, for every $\eta \in E$, there are exactly two distinct $\xi \in E$ with $L(\xi) = \eta$, and their sum is $s$. It follows that $\dim_{\mathbb{F}_2}(\ker(L^n)) = n$ for all $n \in \mathbb{N}$. Let $v_1 = s$ and define a sequence $\{v_n\}_{n \in \mathbb{N}}$ via $L(v_{n+1})$ for all $n \in \mathbb{N}$. Then it is easy to see that $v_1, v_2, ..., v_n$ forms a basis for $\ker(L^n) \subseteq K$. Define $H_n = k(s, \ker(L^n)) = k(s, v_n)$. Let $\sigma$ be any $k(s)$-automorphism of $K$. Clearly, $\sigma(\ker(L^n)) = \ker(L^n)$ so $H_n/k(s)$ is a normal extension. Furthermore, since $H_{n+1}$ is obtained from $H_n$ by adjoining $v_{n+1}$, which satisfies $v_{n+1}^2 + sv_{n+1} = v_n$, while $v_1 \in k(s)$, we see that $H_n/k(s)$ is finite Galois, for all $n$.

Now let $n \geq 2$, then $L^{n-1}(v_n) = v_1 = s$. This can be expressed as $g(v_n) = 0$ where $g(x) \in k[s, x]$ is an $s$-Eisenstein polynomial of $x$-degree $2^{n-1}$. In particular, $g(x)$ is irreducible in $k(s)[x]$ of $x$-degree $2^{n-1}$, so that $\# \, \text{Gal}(H_n/k(s)) = [H_n : k(s)] = 2^{n-1}$.

We will prove that $\text{Gal}(H_n/k(s)) \cong R_n^s$. Note that $\text{Gal}(H_n/k(s))$ is uniquely determined by its action on $\ker(L^n)$. For any $\sigma \in \text{Gal}(H_n/k(s))$, let $M(\sigma)$ be the matrix in $M_{n \times n}(\mathbb{F}_2)$ describing $\sigma$ in terms of $v_n, ..., v_1$. Then $M(\text{Gal}(H_n/k(s)))$ commutes with $L \in M_{n \times n}(\mathbb{F}_2)$ describing $L$ in terms of
\[ L = \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}. \]

Hence, \( M(\text{Gal}(H_n/k(s))) \) lies in the \( \mathbb{F}_2 \)-algebra \( C \) of all matrices in \( M_{n \times n}(\mathbb{F}_2) \) commuting with \( L \), while \( C \cong \mathbb{F}_2[Y]/(Y^n) = R_n \), so \( M(\text{Gal}(H_n/k(s))) \subseteq R_n^* \). Clearly, \( M \) is a group homomorphism \( \text{Gal}(H_n/k(s)) \to R_n^* \) and \( \ker M = \{ \text{id} \} \). Then, since \( \#R_n^* = 2^{n-1} = \#(\text{Gal}(H_n/k(s))) \), we have \( \text{Gal}(H_n/k(s)) \cong R_n^* \) as desired.

Now, suppose \( \alpha \) and \( \beta \) are zeros of \( \mathcal{G}^n(x) \) in the algebraic closure of \( k(s,t) \). Then \( \alpha + \beta \in \ker(\mathcal{L}^n) \subseteq K \). Conversely, if \( \lambda \in \ker(\mathcal{L}^n) \) then \( \mathcal{G}^n(\alpha + \lambda) = 0 \). Hence, the set of \( x \)-zeros of \( \mathcal{G}^n(x) \) is precisely \( \alpha + \ker(\mathcal{L}^n) \).

Consider the specialization of \( \mathcal{G}(x) \) to \( \tilde{\mathcal{G}}(x) = \tilde{k}[t][x] \), given by \( s \mapsto 0 \). Then \( \tilde{\mathcal{G}}^n(x) \) is \( t \)-Eisenstein in \( \tilde{k}[t][x] \), so it is irreducible. Thus, by Lemma 4.1, \( \tilde{\mathcal{G}}^n(x) \) is irreducible over \( K(t) \), and hence over \( H_n(t) \).

Fix some root \( \alpha \) of \( \mathcal{G}^n(x) \), then \( K_n = H_n(\alpha) \). So we have \( [K_n : k(s,t)] = [H_n(t,\alpha) : H_n(t)][H_n(t) : k(s,t)] = 2^n2^{n-1} = \#R_n \times R_n^* \).

For \( \sigma \in \text{Gal}(\mathcal{G}^n(x)/k(s,t)) \), we have \( \sigma(\alpha) = \alpha + v_{\sigma} \) for some \( v_{\sigma} \in \ker \mathcal{L}^n \). Then, for \( v \in \ker \mathcal{L}^n \), we have

\[ \sigma(\alpha + v) = \sigma(\alpha) + \sigma(v) = \alpha + v_{\sigma} + \sigma(v), \]

where \( \tilde{\sigma} = \sigma|_{H_n} \) is the restriction of \( \sigma \) to \( H_n \).

Define a group homomorphism from \( \text{Gal}(\mathcal{G}^n(x)/k(s,t)) \) to \( B \), where \( B \) is the group of all maps of the form \( v \mapsto v' + \tau v \), where \( \tau \in \text{Gal}(H_n/k(s)) \cong R_n^* \), and \( v' \) is arbitrary in \( V \). Clearly \( B \cong R_n \times R_n^* \) and \( \#B = \#(R_n \times R_n^*) = 2^{n-1} = \#(\text{Gal}(\mathcal{G}^n(x)/k(s,t))) \), so it suffices to show that this map is injective. Let \( \sigma \) be in the kernel of the map. Then \( \sigma \) fixes \( \alpha \) and fixes \( v \) for all \( v \in V \), so \( \sigma = \text{id} \) and the proof is complete. \( \square \)

We can see that the group \( R_n \times R_n^* \) cannot be obtained as the Galois group of \( f^n(x) - t \) over \( \tilde{k}[t] \) for a polynomial \( f(x) \in \tilde{k}[x] \) as in the other cases.

**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 \( \text{Gal}(f^n(x) - t/k(t)) = (C_2)^n \) for all \( n \in \mathbb{N} \), where \( C_2 \) is the cyclic group of order 2.

**Proof.** Let \( E \) be an algebraically closed extension of \( k(x,t) \). Consider the \( \mathbb{F}_2 \)-linear map \( \mathcal{L} : E \to E \) by \( \mathcal{L}(\xi) = a_2\xi^2 + a_1\xi \). For each \( \eta \in E \) there are exactly two \( \xi \in E \) with \( \mathcal{L}(\xi) = \eta \). It follows that \( \dim_{\mathbb{F}_2}(\ker \mathcal{L}^n) = n \) for all \( n \in \mathbb{N} \). Let \( v_1 = a_1a_2^{-1} \) and define a sequence \( \{v_n\}_{n \in \mathbb{N}} \) via \( \mathcal{L}(v_{n+1}) \) for all \( n \in \mathbb{N} \). Then it is easy to see that \( v_1, v_2, \ldots, v_n \) forms a basis for \( \ker(\mathcal{L}^n) \subseteq k \).

Now let \( \alpha \) and \( \beta \) be zeros of \( f^n(x) - t \) in the algebraic closure of \( k(t) \). Then \( \alpha + \beta \in \ker(\mathcal{L}^n) \subseteq k \). Conversely, if \( \lambda \in \ker(\mathcal{L}^n) \) then \( f^n(\alpha + \lambda) = 0 \).
Hence, the set of $x$-zeros of $f^n(x) - t$ is precisely $\alpha + \ker(L^n)$. Thus, the splitting field of $f^n(x) - t$ over $k(t)$ is $k(t, \alpha)$, and $\text{Gal}(f^n(x) - t/k(t))$ has order $[k(t, \alpha) : k(t)] = 2^n$.

It remains to show that $\text{Gal}(f^n(x) - t/k(t))$ is elementary abelian. Since the splitting field of $f^n(x) - t$ is $k(t, \alpha)$, the group $\text{Gal}(f^n(x) - t/k(t))$ is determined by its action on $\alpha$. Let $\sigma \in \text{Gal}(f^n(x) - t/k(t))$. Then $\sigma(\alpha) = \alpha + v_\sigma$ for some $v_\sigma \in \ker(L^n) \subseteq k \subseteq k(t)$. Also, for any $\sigma, \tau \in \text{Gal}(f^n(x) - t/k(t))$,

$$(\tau \sigma)(\alpha) = \tau(\alpha + v_\sigma) = \tau(\alpha) + \tau(v_\sigma) = \alpha + v_\tau + v_\sigma.$$  

Thus, the map $\psi : \sigma \mapsto v_\sigma$ is a homomorphism from $\text{Gal}(f^n(x) - t/k(t))$ to the additive group $\ker(L^2)$. Now, if $\sigma \in \ker \psi$ then $\sigma(\alpha) = \alpha$, so $\sigma$ is the identity in $\text{Gal}(f^n(x) - t/k(t))$. Hence, $\ker \psi$ is trivial and $\psi$ injects $\text{Gal}(f^n(x) - t/k(t))$ into the additive group $\ker(L^n)$. The latter is elementary abelian of order $2^n$. Since $\# \text{Gal}(f^n(x) - t/k(t)) = 2^n$, $\psi$ is an isomorphism, and $\text{Gal}(f^n(x) - t/k(t))$ is also elementary abelian, as required. $\Box$

6. Application: Primes Dividing Orbits

Suppose $k$ is 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 $v_p(f^n(a_0)) \neq 0$ for some $n$. For any set of primes $S$, we define the natural density of $D(S)$ by

$$D(S) = \lim_{x \to \infty} \frac{\# \{p \in S : N(p) < x \}}{\# \{p \in \mathbb{P}^1(k) : N(p) < x \}}.$$  

Following the work in [Odo85], we show that for any $\epsilon > 0$, “most” polynomials $f(x) \in k(x)$ satisfy $D(P_f(a_0)) < \epsilon$, for any $a_0 \in k$.

Since $k$ is a global field, $k$ is Hilbertian (see [F.J08], for example), so we can apply the following generalization of [Odo85], Lemma 6.1.

**Lemma 6.1.** Let $F$ be a Hilbertian field, and let $t_1, \ldots, t_r, x$ be independent indeterminants over $F$. Suppose that in $F[t, x]$, $f(t, x)$ is $x$-monic and squarefree. Then, there is a Hilbert set $\mathcal{H}$ in $F^r$ such that for all $t' \in \mathcal{H}$, $f(t', x)$ is squarefree in $F[x]$ and $\text{Gal}(f(t', x)/F) \cong \text{Gal}(f(t, x)/F(t))$.

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

**Lemma 6.2.** ([Odo85], Lemma 4.3) Let $\text{FPP}([S_d]^n)$ denote the proportion of elements of $[S_d]^n$ with a fixed point. Then

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

**Theorem 6.3.** If $k$ is a global field, then for all $\epsilon > 0$, there is a Hilbert set $\mathcal{H}$ in $k^{d-1}$, such that for all $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0$ with $(c_{d-1}, \ldots, c_0) \in \mathcal{H}$, $D(P_f(a_0)) < \epsilon$, for any $a_0 \in k$. 

Proof. By Lemma 6.2, we can choose $n_0$ so that $\text{FPP}([S_d]^{n_0}) < \epsilon$. Then by Theorem 1.1, $\text{Gal}(\mathcal{S}^{n_0}(x)/k(s,t)) \cong [S_d]^{n_0}$. Thus, by Lemma 6.1, there is a Hilbert set $\mathcal{H}$ such that for all $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0$ with $(c_{d-1}, \ldots, c_0) \in \mathcal{H}$, $\text{Gal}(f^{n_0}(x)/k) \cong [S_d]^{n_0}$.

Let $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0$ with $(c_{d-1}, \ldots, c_0) \in \mathcal{H}$, and let $a_0 \in k$. Now, let $P_f(a_0)$ denote the set of primes of $k$ such that $\nu_p(f^{n_0}(a_0)) \neq 0$ for some $n$, as before. We split $P_f(a_0)$ into three sets, $P_1 = \{p : \nu_p(f^{n_0}(a_0)) < 0 \text{ for some } n \in \mathbb{N}\}$, $P_2 = \{p : p \mid (f(a_0) \ldots f^{n_0}(a_0)\Delta(f^{n_0}(x)))\}$, and $P_3 = \{p : p \mid \Delta(f^{n_0}(x)), p \mid f^m(x) \text{ for some } m \geq n_0\}$.

$P_1$ consists of the set of primes for which $\nu_p(a_0) < 0$ or $\nu_p(c_i) < 0$ for some $i$, so clearly $P_1$ is a finite set. Also, $P_2$ is clearly finite.

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

$$D(P_3) \leq \text{FPP}([S_d]^{n_0}).$$

Then since $P_1$ and $P_2$ are finite,

$$D(P_f(a_0)) \leq \text{FPP}([S_d]^{n_0}) < \epsilon.$$

\[\square\]

7. Application: Factorizations of Iterates over $\mathbb{F}_q$

Let $F$ be any field and let $f(x) \in F[x]$ be squarefree with degree $m \geq 1$. 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 $i$ [Coh72]. 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.

**Definition 7.1.** Let $\pi = (1)^{r_1} \ldots (m)^{r_m}$ be a cycle pattern in $S_m$. We say that a squarefree polynomial $f(x)$ of degree $m$ in $F[x]$ has cycle pattern $\pi$ if $f(x)$ has exactly $r_i$ irreducible factors of degree $i$ for all $1 \leq i \leq m$.

The wreath power $[S_d]^n$ has a natural action on the symbols $1, \ldots, d^n$ induced by the action of $S_d$ on $1, \ldots, d$, this gives an injection $\iota : [S_d]^n \to S_{d^n}$. The map $\iota$ depends only on the choice of the labeling of the symbols $1, \ldots, d$, but relabeling $1, \ldots, d$ 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 $C$ or $S_{d^n}$, the value of $\#C \cap \iota([S_d]^n)$ is independent of the choice of $\iota$. 
Fix any $\iota$ as above. Let $\pi$ 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 $\pi$. We define

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

Then $\rho(\pi)$ is a nonnegative polynomial such that $\rho(\pi) = 1$ whenever $(d,p) \neq (2,2)$.

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 $b$;
- $f^n(x)$ is squarefree;
- $f^n(x)$ has cycle pattern $\pi$.

**Theorem 7.2.** There is an $M = M(d,n) > 0$ in $\mathbb{R}$ and $q_0(d,n) \geq 1$ in $\mathbb{N}$ such that

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

whenever $(d, \text{char} \mathbb{F}_q) \neq (2,2), d \geq 2, n \geq 1, b \neq 0$ in $\mathbb{F}_q$, $\pi$ is a cycle pattern in $S_{d^n}$ and $q \geq q_0$.

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

- $\deg f(x) = d$;
- $f^n(x) - t$ is irreducible in $\mathbb{F}_q[x,t]$ and $x$-separable over $\mathbb{F}_q(t)$;
- $\text{Gal}(f^n(x) - t/k(t)) \cong [S_d]^n$.

By Section 3 and Theorem 3.6, $\Omega(d,n,\mathbb{F}_q)$ contains a Zariski open subset of $\mathcal{P}_d(\mathbb{F}_q)$.

**Proof.** Let $B(q,b,d,n)$ be the set of all $f(x) \in \mathbb{F}_q[x]$, with leading coefficient $b$ and $f(x) \in \Omega(d,n,\mathbb{F}_q)$.

We first find an estimate for $\# B(q,b,d,n)$. We have seen that $\Omega(d,n,\mathbb{F}_q)$ is a $\mathbb{Z}$-basis for $\mathcal{P}_d(\mathbb{F}_q)$. A more careful examination of the proof of Lemma 3.5 actually shows that there is a nonzero polynomial $\Theta = \Theta(u_0,u_1,\ldots,u_d)$ with coefficients in the prime field $\mathbb{F}_p$ where $p = \text{char} \mathbb{F}_q$ and the total degree of $\Theta$ is bounded by some constant $C$ depending only on $d,n$.

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

By a standard number theory argument, for each $s \in S$ the number of $(a_0,\ldots,a_{d-1})$ in $(\mathbb{F}_q)^d$ for which $\Theta(a_0,\ldots,a_{d-1},s) = 0$ is bounded above by $D q^{d-1}$ where $D$ is a constant depending only on $d,n$. So we see that

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

for $s \in S$.

We will now show that the above estimate holds for all $b$ in $\mathbb{F}_q^*$ for sufficiently large $q$. 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,

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

Let \( H \) be the subgroup of all \( d - 1 \) powers in \( \mathbb{F}_q^* \). Then \( #H = (q - 1)/e \) where \( e = \gcd(q - 1, d - 1) \). Consider \( SH \), the union of all the cosets of \( H \) containing elements of \( S \). Note \( #SH = #S^q - 1/e \), so clearly, \( #S \leq e \). Also, \( #SH \geq #S \geq (q - 1) - C \). So \( #S \geq q - C - \frac{C}{q^2} \). Thus, there is some \( q_0 = q_0(d, n) \) such that \( #S = e \) for all \( q \geq q_0 \).

If we take \( q \geq q_0 \), then we have \( #SH = q - 1 \) so \( SH = \mathbb{F}_q^* \) and hence,

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

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

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

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

Let \( b \in \mathbb{F}_q^* \) and fix \( f(x) \in B(q, b, d, n) \). Then \( \text{Gal}(f^n(x) - t/\mathbb{F}_q^* \cong [S_d]^n \).

It follows that \( \text{Gal}(f^n(x) - t/\mathbb{F}_q^* \cong [S_d]^n \) as well. Thus, the splitting field \( L \)

of \( f^n(x) - t \) over \( \mathbb{F}_q(t) \) is a geometric extension, that is, \( L \cap \mathbb{F}_q(t) = \mathbb{F}_q(t) \), and there is no extension of the constant field.

Since the degree of the different \( D_L/\mathbb{K} \) 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 \( L \).

Let \( \pi \) 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 \( \pi \) if and only if \( \text{Frob}_{\mathbb{L}/\mathbb{K}} (\frac{L/\mathbb{K}}{\frac{\alpha}{\alpha}}) \) has cycle pattern \( \pi \). Applying a version of the Chebotarev density theorem for function fields (see [CO77], Proposition A.3), we see that the number of \( \alpha \in \mathbb{F}_q \) such that \( f^n(x) - \alpha \) is squarefree with cycle pattern \( \pi \) is

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

Now we treat \( q, b, d, n \) as fixed and let \( A = \{ f(x) \in \mathbb{F}_q[x] : \deg f(x) = d \text{ and } f(x) \text{ has leading coefficient } b \} \). Let \( A(\pi) = A(q, b, d, n, \pi) \) and \( B = B(q, b, d, n) \). For \( \alpha \in \mathbb{F}_q \), let \( D(\alpha, \pi) = \{ f(x) \in A : f(x + \alpha) - \alpha \in A(\pi) \} \).

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

We will find an estimate for \( \#D(\alpha, \pi) \) and hence for \( A(\pi) \) by examining the set \( E(\alpha, \pi) = B \cap D(\alpha, \pi) \). Fix \( f(x) \in B \). For \( \alpha \in \mathbb{F}_q \), \( f(x) \) is in \( E(\alpha, \pi) \) if and only if the \( n \)-th iterate of \( f(x + \alpha) - \alpha \) is squarefree with cycle pattern \( \pi \). That is, if and only if \( f^n(x + \alpha) - \alpha \) is squarefree with cycle pattern \( \pi \).

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 \( \pi \).
Hence, by equation (2),
\[ \# \{ \alpha \in \mathbb{F}_q : f(x) \in E(\alpha, \pi) \} = q \rho(\pi) + O(q^{\frac{d}{2}}), \text{ for all } f(x) \in B. \]

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

By equation (1), \( \# D(\alpha, \pi) = \# E(\alpha, \pi) + O(q^{\frac{1}{2}}). \) So
\[ \sum_{\alpha \in \mathbb{F}_q} \# D(\alpha, \pi) = q^{d+1} \rho(\pi) + O(q^{d+\frac{1}{2}}). \]

Hence,
\[ \# A(\pi) = q^d \rho(\pi) + O(q^{d-\frac{1}{2}}) \]
as desired. \( \square \)

Remarks 7.3.

(1) There is a formula due to Polya [Pòl37], which allows one to calculate \( \rho(\pi) \) for every cycle pattern \( \pi \) of \( S_{dn} \) (see [Tom75]). However, this formula is complicated. In the cases \( \pi = (1)^{dn} \) 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, we can avoid the use of this formula. Clearly we have, \( \rho((1)^{dn}) = (\# [S_d]^{dn})^{-1}, \) while an inductive argument on \( n \) gives \( \rho((d^n)^1) = d^{-n}. \)

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

References

[CH12] J. Cullinan and F. Hajir, Ramification in iterated towers for rational functions, Manuscripta Math. 137 (2012), no. 3-4, 273-286.

[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. MR 0432597 (55 #5584)

[Coh72] S. D. Cohen, The distribution of polynomials over finite fields. II, Acta Arith. 20 (1972), 53–62. MR 0291135 (45 #229)

[Coh91] ______, Permutation polynomials and primitive permutation groups, Arch. Math. (Basel) 57 (1991), no. 5, 417–423. MR 1129514 (92j:11145)

[FJ08] M. D. Fried and M. Jarden, Field arithmetic, third ed., 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, Revised by Jarden. MR 2445111 (2009j:12007)

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

[Jan96] G. J. Janusz, Algebraic number fields, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

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

[Nek05] V. Nekrashevych, Self-similar groups, Mathematical Surveys and Monographs, vol. 117, American Mathematical Society, Providence, RI, 2005. MR 2162164 (2006e:20047)
ITERATES OF GENERIC POLYNOMIALS AND RATIONAL FUNCTIONS

[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. MR 805714 (87c:12005)

[Pól37] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen*, Acta Math. 68 (1937), no. 1, 145–254. MR 1577579

[Sti09] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR 2464941 (2010d:14034)

[Tom75] I. Tomescu, *Introduction to combinatorics*, Collet's Publishers Ltd., London, 1975. Translated from the Romanian by I. Tomescu and S. Rudeanu, Edited by E. Keith Lloyd. MR 0396275 (53 #143)

JAMIE JUUL, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ROCHESTER, ROCHESTER, NY 14627, USA

*E-mail address: jamie.l.rahr@gmail.com*