A UNIQUE CHIEF SERIES IN THE ARBOREAL GALOIS GROUP OF BEL YI MAPS

WAYNE PENG

Department of Mathematics, University of Rochester Rochester, NY 14627

ABSTRACT. We give a complete description of the normal subgroups of arboreal Galois groups of Belyi maps. The normal groups form a unique chief series. We also carefully compute the discriminant of the iterate of a polynomial minus an algebraic number, which allows us to predict when a such discriminate is a perfect square in the base field or intermediate field for a postcritically finite polynomials (PCF). As a consequence we are able to find another PCF cubic polynomial that has the same arboreal Galois group as the one of Belyi maps.

1. INTRODUCTION

Let $K$ be a number field with $\alpha \in K$, and let $f \in K[z]$ be a polynomial of degree $d \geq 3$. The Galois group of

$$f^n(z) - \alpha$$

where $f^n$ is the $n$-th iterate of $f$. Such a Galois group is called arboreal Galois group or $n$-th dynamical Galois group, denoted by $\text{Gal}_n^f(\alpha) = \text{Gal}(f^n(z) - \alpha / K)$. If $\alpha$ is not an image of $\alpha$ and branch points of $f$ under $f^n$ for some positive integer $n$, then one can make a Galois action an act on a $d$-ary tree. The vertices of the $d$-ary tree is made up of the inverse image of $\alpha$ under $f^{-n}$ for $n = 1, 2, \ldots$, and where we draw an edge on two vertices $x$ and $y$ if $f(x) = y$. With a proper chosen $\alpha$, this tree is rooted at $\alpha$ with the Galois action acting faithfully on the tree. Sometime we call $\alpha$ the base point of the dynamical system of $f$.

The study of arboreal Galois group becomes popular for a while due to its application in number theory. Odoni [18] has showed that the description of the dynamical Galois group give rise to application on the density of primes division in certain dynamically defined sequences (see also [11, 9, 16] and [14]). Generically the $n$-th dynamical Galois group of a degree $d$ polynomial is isomorphic to the group of automorphism of a $d$-ary tree $\text{Aut}(T_n)$ which is isomorphic to the $n$-fold wreath product $[S_d]^n$ of symmetric group $S_d$ on $d$ letters (see [15, 17]). However for a specified chosen $f$ and $\alpha$ the dynamical Galois group can be a lot of smaller than the full wreath product. For example let $f$ be a powering map $x^d$ or a degree $d$ Chebyshev polynomial. These two examples are the simplest examples of post-critical finite polynomial, abbr. PCF. A polynomial or rational function $f$ PCF if all of its critical points $c$, i.e. $f'(c) = 0$, is preperiodic. Jones, Pink and many other authors [12, 20, 7, 3, 13] shows that $\text{Gal}_n^f(\alpha)$ has unbounded index inside $\text{Aut}(T_n)$ as $n$ goes to infinity. The idea of the proof is realizing the $n$-th dynamical Galois group as
a specialization of the arithmetic dynamical Galois group \( \text{Gal}(f^n - t/K(t)) \), where \( t \) is transcendental over \( K \). The latter group is known as the arithmetic Galois group and can be embedded in the profinite monodromy group \( \pi^\text{et}_1(\mathbb{P}^1 \setminus P) \), where \( P \) is strictly postcritical orbit.

The first case [1] that has been explicit computed is the dynamical Galois group of \(-2x^3 + 3x^2\) at a properly chosen base point \( \alpha \). The polynomial is a degree 3 Belyi map, a map that has three fixed critical points. They have shown that the \( n \)-th dynamical Galois group is isomorphic to \( E_n^2 \) (defined in 2.1). Then [2] shows that the degree 3 Belyi map is not a unique example. In fact all odd degree Belyi map with two exceptions are isomorphic to \( E_n^2 \). Unlike the technique using in [2] the first paper use pure algebraic argument to show the isomorphism. Following their observation we shows the following.

**Theorem 1.** Let \( K \) be a number field. Let \( f(z) = 2z^3 - 3z^2 + 1 \), and let \( \alpha \in K \). Suppose there exist primes \( p \) and \( q \) of \( K \) lying above 2 and 3 such that either \( v_q(\alpha) = 1 \) or \( v_q(1-\alpha) = 1 \), and either \( v_p(\alpha) = 1 \) or \( v_p(1-\alpha) = 1 \). Then for each \( n \geq 1 \),

1. The polynomial \( f^n \) is irreducible over \( K \).
2. The \( n \)-th dynamical Galois group \( \text{Gal}_f^n(\alpha) \) is isomorphic to \( E_n^2 \).

Our key observation is using Equation 2 to find when the discriminant of \( f^n - \alpha \) is a perfect square in the base field or an intermediate field. Such an observation give us a universal embedding of dynamical Galois group of PCF map.

**Theorem 2.** Let \( f \) be a PCF polynomial over a number field \( K \), and suppose \( \alpha \) is not periodic. Let \( \mathcal{C}_f \) be the set of all critical points of \( f \). Let \( L \) be the minimum integer such that \( f^L(\mathcal{C}_f) \) is a periodic set, and let \( O \) be the minimum positive integer such that \( f^{L+O}(\mathcal{C}_f) = f^L(\mathcal{C}_f) \).

1. Suppose the degree of \( f \) is odd, and \( L \leq 1 \). Then \( \text{Gal}_f^n(\alpha) \) is a subgroup of \( E_n^{2O} \).
2. Otherwise \( \text{Gal}_f^n(\alpha) \) is a subgroup of \( E_n^{(m_1,m_2)} \) where

\[
(m_1, m_2) = \begin{cases} 
(0+1,1), & L = 0 \text{ and } O \text{ is even}; \\
(0+2,2), & L = 0 \text{ and } O \text{ is odd}; \\
(L + 2O - 1, L - 1), & L > 1 \text{ and } d \text{ is odd}; \\
(L + O, L), & L > 1, d \text{ is odd, and } a_f \text{ is a perfect square or } O \text{ are even}; \\
(L + O + 1, L + O), & L > 1, d \text{ is odd and } a_f \text{ is not a perfect square and } O \text{ is odd}.
\end{cases}
\]

As a consequence, the index of dynamical Galois group of PCF map is unbounded in \( \text{Aut}(T_n) \) as \( n \) goes infinite, follows immediately after this theorem. This provide a pure algebraic proof of this important theorem.

Due to \( E_n^2 \) represents the dynamical Galois group of a large family of polynomials, it makes the author curious about the structure of such groups. One of the purpose of this paper is to provide a pure algebraic point of views on proving that the rank of \( E_n^2 \) is bounded as \( n \) goes to infinity. The rank of a group \( G \), denoted by \( d(G) \), is the cardinality of minimal generating set the group. It is well-known that \( d(G) \geq d(G/N) \) where \( N \) is a normal subgroup of \( G \). Jones uses this lower bound and shows that the abelianization of \( [S_n]^n \) is the \( n \)-fold direct product of \( C_2 \), so the arithmetic Galois groups of PCF maps, which is finite generated group, cannot be of finite index in \( [S_n]^n \).
To obtain an upper bound of \( d(G) \) by subgroups or quotient groups of \( G \) is difficult. In [6] the authors have shown that \( d(G) = d(G/N) \) if and only if \( G/N \) has not too many factors \( G \)-equivalent to \( N \). We don’t need such a strong theorem. Instead [4] shows that \( d(G) = \max\{2, d(G/N)\} \) if \( G \) is not cyclic and \( N \) is the unique minimum subgroup of \( G \). Thus if we can find a unique minimum subgroup \( N \) in \( E_2^2 \) such that we can again find a unique minimum subgroup in the quotient \( E_2^2/N \) and if this process can be repeated until the quotient subgroup is small enough to compute, then we are able to bound the rank of \( E_2^2 \). The similar concept of the above process is chief series of a group \( G \), which is a sequence of normal subgroups \( N \) of the quotient subgroup is small enough to compute, then we are able to bound the rank of \( E_2^2 \). Thus if we can find a unique minimum subgroup \( N \) in the quotient \( E_2^2/N \), which is a sequence of normal subgroups \( N_i \) of \( G \) satisfying

\[
1 = N_1 \lhd N_2 \lhd \cdots \lhd N_k = G
\]

and each chief factor \( N_{i+1}/N_i \) is a minimum normal subgroup of the quotient group \( G/N_i \) (see [10] for details). Our result, in Section 3.2, is the following.

**Theorem 3.** Let \( d \) be odd. The rank of the group \( E_2^2(d) \) is 2 for all \( n \). Moreover \( E_2^2 \) has a unique chief series.

The outline of this paper is as follows. In Section 2 we define the group \( E_n^m \) and \( F_n^{(m_1,m_2)} \), give a brief on the relation between the abelianization and wreath product, and explicitly compute the discriminate of \( f^n - \alpha \). Most stuff in Section 2 is already well-understood. In Section 3 we give our main results. Finally, in Section 3, the author has some open questions and the difficulty to generalize the argument of this paper to more general cases.

We will use the following symbols in this paper.

- 1 is use to denote either the integer 1, an identity map or an identity of a group. If we use 1 to denote an identity, the group will be specified in the context.
- We will use \( \ast \) to denote an arbitrary element. Where the element belongs to will be specified in the context.
- For \( \sigma, \tau \in G \) we denote \( \sigma^\tau \) for the conjugacy \( \tau \sigma \tau^{-1} \).
- Let \( C_f \) be the set of all critical points of \( f \), and \( f(C_f) = \{f(c) \mid c \in C_f \} \).
- The splitting field of \( f^n - \alpha \) is denoted by \( K_f^n(\alpha) \), and the correspondent Galois group is denoted by \( \text{Gal}_f^n(\alpha) \).
- A point or an object \( \alpha \) is preperiodic if \( \{f^n(\alpha) \mid n = 1,2,\ldots\} \) is a finite set. If we say it is periodic, then \( f^n(\alpha) = \alpha \) for some integer \( n \). The tail length of a preperiodic point is the smallest integer such that \( f^n(\alpha) \) becomes a periodic point.

2. Preliminary

2.1. **Wreath product and arboreal representation.** Let \( T_n(d) \) be a regular \( d \)-ary tree of \( n \) levels (see Figure 2.1 as an example). We will omit \( d \) in the notation for simplicity sake. \( T_n \) has \( d^n \) many leaves, vertices on the top of the tree, and has \( 1 + d + \cdots + d^n \) many vertices on the tree. The level of a vertex on a tree is distance between the vertex and the root. For \( m \leq n \) the \( m \)-th level of the tree \( T_d \) is the set of all vertices of level \( m \).

Our result and many arguments will depend on an explicit labeling of the tree. We will make this labeling explicitly for the purpose of rigor, but we won’t commend on it in the rest of this paper. There are two labeling system of a tree. The regular labeling to denote a vertex of level \( m \) is to use a tuple \((l_m, \ldots, l_1)\) in \( \{1,2,\ldots,d\}^m \). Note that the vertex with the label \((l_m, \ldots, l_1)\) has distance 1 to the vertex with the label \((l_{m-1}, \ldots, l_1)\). This gives a recursive relation to label all vertices of a tree.
We are able to identify some canonical subtree using the regular labeling. For example, for each tuple \((l_m, \ldots, l_1)\) with \(m \leq n\), the set of vertex \((*, \ldots, *, l_m, \ldots, l_1)\) is a subtree isomorphic to \(T_{n-m}\) rooting at \((l_m, \ldots, l_1)\). We will call this subtree a level \(n-m\) subtree, and denote by \(T(l_m, \ldots, l_1)\).

The above system of labeling is not convenient sometime, especially when we only talk about the \(m\)-th level of the tree. For each vertex of level \(m\) we label the point by the integer \(l_m + (l_{m-1} - 1)d + (l_{m-2} - 1)d^2 + \cdots + (l_1)d^{m-1}\). We will denote this labeling system by \(I(T_n) = \{1, 2, \ldots, d^m\}\). The tree structure splits \(I(T_n)\) to different blocks. A block of \(T_n\) over \(T_m\), denote by \(B(T_n / T_m)(l_{n-m}, \ldots, l_1)\), are the set of indices that belongs to the same level \(n-m\) subtree, and we use \(B(T_n / T_m)\) be the set of all such blocks. An index \(i\) belongs to a level \(n-m\) subtree \(T(l_m, \ldots, l_1)\) if \(i \in B(T_n / T_m)(l_m, \ldots, l_1)\).

We will omit the strict definition of \(\text{Aut}(T_n)\) and how the group acting on \(T_n\). We refer readers to [1] for details. The labeling systems of the tree \(T_n\) induce an isomorphism \([S_d]_n \subseteq S_{\#I(T_n)}\) where \([S_d]_n\) is the \(n\)-folds wreath product of \(S_d\). On the other hand the embedding to the symmetric group \(S_{d^n}\) of degree \(d^n\) allows us to use all terminologies adhering to the theory of symmetric groups. For example an index \(i \in I(T_n)\) is in the support of \(\sigma \in \text{Aut}(T_n)\) if \(\sigma(i) \neq i\). We also mimic the definition of \(\text{sgn}\) in [1], and use it to construct the group \(E_n^m\) and \(F_{n,m_2}^{(m_1,m_2)}\). We will give the details later.

Let \(G \subseteq S_d\) be a group acting on \(I = \{1, 2, \ldots, d\}\). For an arbitrary group \(H\) the wreath product of \(H\) by \(G\) over \(I\), denoted by \(H \wr I G\), is an extension of groups. As a set the element of \(H \wr I G\) can be expressed as

\[
((h_1, \ldots, h_d); g)
\]

with \(h_i \in H\) and \(g \in G\). The operation of two element is defined as

\[
((h_i); g)((h'_i); g') = ((h_g(i)); h'_i; gg')
\]

Note that the following simple decomposition of an element of wreath product

\[
((h_1, \ldots, h_d); g) = ((1, \ldots, 1); g)(h_1, \ldots, h_d); 1)
\]

will be use frequently in our argument. When the index set \(I\) is obvious in the context, we will omit \(I\). A useful observation is that, for \(n > m\), \(\text{Aut}(T_n) \cong \text{Aut}(T_m) \wr I(T_{n-m})\).
Let \( \text{Aut}(T_{n-m}) \). If we say \( \sigma \in \text{Aut}(T_n) \) or \( \sigma \in G \subseteq \text{Aut}(T_m) \setminus \text{Aut}(T_{n-m}) \), it means we will express \( \sigma \) as

\[
((a_i)_{i \in I(\sigma)}; b)
\]

with \( a_i \in \text{Aut}(T_m) \) and \( b \in \text{Aut}(T_{n-m}) \). There is a natural homomorphism \( \text{res} : H \setminus G \to G \) by projecting the second coordinate to \( G \).

Let me recall that the sign of a permutation is 1, if the permutation is even, or -1 otherwise. One can define a sign on the automorphism of a \( d \)-ary tree by labeling the branches on the \( n \)-th level of the tree. Once a label system is given, it gives an embedding from \( \text{Aut}(T_n) \) to \( S_{d^n} \). Compose with the sign of permutations, it defines a sign on \( \text{Aut}(T_n) \).

Note that for even \( b \) we can set \( \text{sgn}((1)_{i \in I(\sigma)}; a) = \text{sgn}((1)_{i \in I(\sigma)}; a) \text{sgn}((1)_{i \in I(\sigma)}, 1)) \).

Note that if we consider \( \text{Aut}(T_n) \cong \text{Aut}(T_{n-m}) \setminus \text{Aut}(T_m) \) with \( 0 < m < n \), it is natural to define \( \text{sgn}^m : \text{Aut}(T_n) \to \{\pm 1\} \) as

\[
\text{sgn}^m((b_i)_{i \in I(\sigma)}, a) = \prod_{i \in I} \text{sgn}(b_i)
\]

with \( b_i \in \text{Aut}(T_{n-m}) \) and \( a \in \text{Aut}(T_m) \). Obviously this is a group homomorphism.

Let \( n > m_1 > m_2 \). we can also define an alternative sign function as

\[
\text{sgn}^{(m_1, m_2)} = \text{sgn}^{m_2} \circ \text{res}_{m_1}
\]

Proposition 5. We have

\[
\text{sgn}^{(m_1, m_2)} = \text{sgn}_{m_1} \text{sgn}_{m_2}.
\]
Proof. It follows from direct computation. A \( \sigma \in \text{Aut}(T_n) \) with \( n \geq m \) can be expressed as \( ((b_i), a) \in \text{Aut}(T_{n-m}) \backslash \text{Aut}(T_m) \), and note that \( \text{sgn}_m(\sigma) = \text{sgn}(a) \). Thus we have

\[
\text{sgn}(\sigma) \text{sgn}_m(\sigma) = \text{sgn}(a) \prod_{i \in I} \text{sgn}(b_i) \text{sgn}(\sigma) = \prod_{i \in I} \text{sgn}(b_i) = \text{sgn}^m(\sigma).
\]

Thus by Equation 1 we have

\[
\text{sgn}^{(m_1,m_2)} = \text{sgn}^{m_2} \circ \text{res}_{m_1} = (\text{sgn} \cdot \text{sgn}_{m_2}) \circ \text{res}_{m_1} = (\text{sgn} \circ \text{res}_{m_2}) \cdot (\text{sgn}_{m_2} \circ \text{res}_{m_1}) = \text{sgn}_{m_1} \cdot (\text{sgn} \circ \text{res}_{m_2} \circ \text{res}_{m_1}) = \text{sgn}_{m_1} \cdot \text{sgn}_{m_2}.
\]

Now we define the following two subgroups of \( \text{Aut}(T_n) \)

\[
E^m_n = \begin{cases} 
\text{Aut}(T_1), & \text{if } n = 1; \\
E^m_{n-1} \backslash \text{Aut}(T_1), & \text{if } n < m; \\
E^m_{n-1} \backslash \text{Aut}(T_1) \cap \ker(\text{sgn}_m), & \text{if } n \geq m.
\end{cases}
\]

and

\[
F^{(m_1,m_2)}_n = \begin{cases} 
\text{Aut}(T_1), & \text{if } n = 1; \\
F^{(m_1,m_2)}_{n-1} \backslash \text{Aut}(T_1), & \text{if } n < m_1; \\
F^{(m_1,m_2)}_{n-1} \backslash \text{Aut}(T_1) \cap \ker(\text{sgn}^{(m_1,m_2)}), & \text{if } n \geq m_1.
\end{cases}
\]

Example 1. Note that \( E^m_n \) is not isomorphic to \( F^m_n \). For example for \( d = 3 \) the element \(((12), (12), 1), (12)) \) is in \( F^{(2,1)}_2 \) but not in \( E^2_2 \).

Let us compute the order of these groups.

Proposition 6. Let \( E^m_n \) and \( F^m_n \) be subgroups of the automorphism of a \( d \)-ary tree with an odd \( d \). Then

\[
|E^m_n| = |F^m_n| = \frac{(d!)^{d^n-1}}{C(d,n)}
\]

with

\[
C(d,n) = \begin{cases}
0, & \text{if } n < m \\
\frac{d^n-m+1}{d-1}, & \text{o.w.}
\end{cases}
\]

Proof. For \( n \geq m \) we consider the following two compositions

\[
\phi_1 : E^m_{n-1} \backslash \text{Aut}(T_1) \longrightarrow \text{Aut}(T_n) \xrightarrow{\text{sgn}_m} \{\pm 1\}
\]

and

\[
\phi_2 : F^{(m,m')}_{n-1} \backslash \text{Aut}(T_1) \longrightarrow \text{Aut}(T_n) \xrightarrow{\text{sgn}^{(m,m')}} \{\pm 1\}.
\]

We claim that \( \phi_1 \) and \( \phi_2 \) are onto.

Take \( g = ((1)_{i \in I}, \sigma) \in E_{n-1} \backslash \text{Aut}(T_1) \) for odd permutation \( \sigma \), and one computes \( \text{sgn}_m(g) = \text{sgn}(\sigma) = -1 \) by assuming \( d \) is odd.
For $\phi_2$ let us first prove the following assertion: for any $m \geq 1$ if $\text{sgn}_m : F_{n-1}^{(m_1,m_2)} \to C_2$ is onto, then so is $\text{sgn}_{m+1} : F_{n-1}^{(m_1,m_2)} \setminus \text{Aut}(T_1) \to C_2$. Since $\text{sgn}_m$ is onto, we may choose an element $a$ such that $\text{sgn}_m(a) = -1$. Then $b = ((a_i)_{i \in I(T_1)}; 1)$ with $a_1 = a$ and $a_i = 1$ for $i \geq 2$ has $\text{sgn}_{m+1}(b) = -1$. Now we define a homomorphism, for $n \geq m_1 - 1$,
\[
\phi : F_{n-1}^{(m_1,m_2)} \setminus \text{Aut}(T_1) \to C_2^{m_1}
\]
\[
a \mapsto (\text{sgn}_{m_1}(a), \text{sgn}_{m_2}(a), \ldots, \text{sgn}_1(a)).
\]
It is clear that $\phi$ is onto as $n = m_1$ because the domain is a wreath product of $S_d$, so $F_{m_1}^{(m_1,m_2)}$ is the kernel of $\phi_2 = \psi \circ \phi$ where
\[
\psi : C_2^{m_1} \to C_2
\]
\[(c_{m_1}, \ldots, c_1) \mapsto c_{m_1}c_{m_2}
\]
by Proposition 5. Note that $\text{sgn}_m(F_{m_1}^{(m_1,m_2)})$ is onto $C_2$ for all $m$, so $\phi$ is onto for $m_1 + 1$. Thus it shows that $\phi_2 : F_{m_1+1}^{(m_1,m_2)} \to C_2$ is onto. Thus by induction we may show that $\phi_2$ is onto for any $n \geq m_1$.

Finally we calculate the orders of these groups. It is obviously equal to $(d!)^{\frac{d-1}{d-2}}$ for all $n < m$ since $\text{Aut}(T_n) \cong [S_d]^n$. Now we can prove the formula by induction. Suppose the formula is true for all $n$ with $n \geq m - 1$, then
\[
|E_n^m| = \frac{1}{2} |E_n^m \setminus \text{Aut}(T_1)| = \frac{1}{2} \left( \frac{(d!)^{\frac{d-1}{d-2}}}{2^{\frac{m^2-1}{d-1}}} \right) d! = \left( \frac{(d!)^{\frac{d^2-1}{d-1}}}{2^{\frac{m^2-1}{d-1}}} \right).
\]
Similarly the same formula holds for $F_{n_1}^{(m_1,m_2)}$ by the same reasoning. $\square$

**Lemma 7.** For $d > 2$ the $E_n^m$ acts transitively on the correspondent index set. Moreover for two distinct index there exists $\sigma \in E_n^m$ permuting $i$ and $j$.

**Proof.** If we prove the second statement, then the first statement is a consequence. We process the proof of the second statement by induction. Moreover we notice that $E_1^1 \subseteq E_n^m$ for any $m$, so we only need to show the second statement is true for $E_1^1$ for any $n > 0$.

It is trivial for $E_1^1$ because it is isomorphic to $A_d$. For induction hypothesis we assume the statement is true for some $n$. For $i$ and $j$ on the same level $k$ subtree with $k < n$, the statement is true by induction. If $i$ and $j$ does not contain in the same level $k$ subtree with $k < n$, then we may choose a transpose $\tau$ that permutes the subtree of $i$ and the subtree of $j$ and choose a permutation $\sigma_i$ on the subtree of $i$ that taking $\tau(j)$ to $i$ and choose a permutation $\sigma_j$ on the subtree of $j$ that taking $\tau(i)$ to $j$. Then the permutation
\[
\omega = ((1, \ldots, 1, \sigma_i, \ldots, 1, \sigma_j, \ldots, 1), \tau\tau')
\]
where $\sigma_i$ and $\sigma_j$ are at the coordinates correspondent to the subtree of $i$ and $j$ respectively, and $\tau'$ is a transpose disjoint from $\tau$. $\square$

2.2. **Abelianization.** The context in this section is already well-known. We give the statement and proof for the sake of self-contained. The primary goal of this section is to give
the relation between the abelianization and the wreath product. It is an elementary exercise in the course of abstract algebra to show that if $G/N$ is abelian for a normal subgroup $N$ of a group $G$, then $N$ contains the commutator subgroup of $G$. Thus, one can define

**Definition 2.** The **abelianization** of a group $G$, denoted as $G^{ab}$, is the largest abelian quotient group of $G$. More precisely, let $H_1$ and $H_2$ be subgroups of $G$. Let me define $\langle H_1, H_2 \rangle$ to be the subgroup generated by the set $\{h_1 h_2 h_1^{-1} h_2^{-1} \mid h_1 \in H_1$ and $h_2 \in H_2\}$. The commutator subgroup of $G$ is $[G, G]$, and $G^{ab}$ is the quotient group $G/[G, G]$.

Let $K$ be Galois over $L$. A quotient group of a Galois group $Gal(K/L)$ is correspondent to a normal subextension of $L$ in $K$. Therefore, the abelianization of the Galois group is correspondent to the largest abelian and normal subextension of $L$ in $K$.

The following theorem deduce the relation between wreath product and abelianization.

**Lemma 8.** Let $G$ be the semidirect product of $H$ acting on $N$. Then, $G^{ab} = (H \ltimes N)^{ab} = (H^{ab}) \times (N^{ab})_H$ where $(N^{ab})_H$ is the quotient group $N^{ab}/[H, N]$.

**Proof.** Since $[G, G] = \langle [N, N], [N, H], [H, H] \rangle$, we have

$$G^{ab} = \frac{G}{[G, G]} = \frac{G}{\langle [N, N], [N, H], [H, H] \rangle} \cong \frac{H \ltimes (N^{ab})}{\langle [H, N], [H, H] \rangle} \cong H^{ab} \times (N^{ab})_H. \quad \square$$

Using this lemma, we can compute the abelianization of a wreath product.

**Lemma 9.** Let $H$ and $G$ be groups with $G$ acting on $G$ faithfully and transitively. Then, $(G \wr H)^{ab} = G^{ab} \times H^{ab}$.

**Proof.** As before, I denote $B = H^r$, and $G$ is a group acting on the index set of $r$ many elements faithfully, i.e., for any $i$, there is some $g \in G$ such that $g(i) \neq i$. The above lemma implies $G \wr H = G \ltimes B$, and so $(G \wr H)^{ab} = (G^{ab}) \times (B^{ab})_G$. Moreover, $B^{ab} = (H^r)^{ab} = (H^{ab})^r$, so it remains to show that $((H^{ab})^r)_G = H^{ab}$.

Let us define the following map, and show it is a surjective homomorphism with $[G, B]$ as the kernel. Let $\phi : (H^{ab})^r \to H^{ab}$ be

$$\phi((h_i)_i) = \sum_{i=1}^r h_i.$$

Since $H^{ab}$ is abelian, the map is absolutely homomorph. Beside we are able to choose $(h_i)$ such that $h_1$ is any element in $H^{ab}$ and $h_i = 1$ for all $i \neq 1$, so $\phi$ is surjective.

It is clear that $\ker(\phi) \supseteq [(H^{ab})^r, G]$. Conversely, given $\phi((b_i)) = \sum_{i=1}^r b_i = 0$, one has

$$b_1 = - \sum_{i=2}^r b_i.$$

Since $G$ acts on $H$ faithfully and transitively, for each $i$ there is a $g_i$ such that $g_i(i) = 1$. For $i \neq 1$, let us define $b_{i_0} = (b'_i)$ with $b'_i = 1$ for all $i \neq i_0$ and $b'_{i_0} = b_{i_0}$. Thus, I have
so for all $n \geq 1$

Proof. for any $n$.

We have

$$d_i = \prod_{i_0=2}^r g_i \cdot b_i$$

which shows that $(b_i) \in [(H^b)^*, G]$. □

2.3. Discriminant.

Lemma 10. Let $a_f$ be the leading coefficient of a polynomial $f$ over any field $K$. The discriminant

\begin{equation}
\text{disc}(f^n(x) - \alpha) = (-1)^{A(d,n)} d_f B(d,n) d^n \text{disc}(f^{n-1}(x) - \alpha)^d \prod_{c \in (f')^{-1}(0)} (f^n(c) - \alpha).
\end{equation}

where

$$A(d,n) = d^n \left( \frac{d^n - 1}{2} + \frac{d^n - 1}{2} \right)$$

$$B(d,n) = d^{2n-1} - 1$$

for all $n \geq 1$. In particular, we have

$$(-1)^{A(d,n)} = \left( \frac{d}{4} \right) = \begin{cases} 1 & \text{if } d \text{ is even or } \equiv 1 \pmod{4} \\ -1 & \text{o.w.} \end{cases}$$

for any $n$.

Proof. By the definition of the determinant, we have

$$\text{disc}(f^n(x) - \alpha) = (-1)^{d^n(d^n-1)/2} a_f^{d^n-2} \prod_{a \in f^{-n}(a)} (f^n)'(a)$$

$$= (-1)^{d^n(d^n-1)/2} a_f^{d^n-2} \prod_{a \in f^{-n}(a)} (f')(f^{n-1}(a)) f'(f^{n-2}(a)) \cdots f'(f(a)) f'(a)$$

where $d$ is the degree of $f$. In terms of $a_f$, one has

$$a_f = a_f^{d^n-1 + d^{n-2} + \cdots + 1},$$

so

$$a_f^{d^n-2} = a_f^\frac{(d^n-1)(d^n-2)}{d-1}.$$  

Note that

$$\prod_{a \in f^{-n}(a)} (f')(f^{n-1}(a)) f'(f^{n-2}(a)) \cdots f'(f(a)) = \left( \prod_{a \in f^{-n(n-1)}(a)} (f')(f^{n-2}(a)) f'(f^{n-3}(a)) \cdots f'(a) \right)^d$$

$$= \left( (-1)^{d^n(d^n-1)/2} a_f^{-d^n-2} \frac{(d^n-1)(d^n-2)}{d-1} \text{disc}(f^{n-1}(x) - \alpha) \right)^d$$

$$= (-1)^{d^n(d^n-1)/2} a_f^{-d^n-2} \frac{(d^n-1)(d^n-2)}{d-1} \text{disc}(f^{n-1}(x) - \alpha)^d,$$

so we have

$$\text{disc}(f^n(x) - \alpha) = (-1)^{d^n(d^n-1)/2} a_f^{d^n-2} \text{disc}(f^{n-1}(x) - \alpha)^d \prod_{a \in f^{-n}(a)} f'(a).$$
The product in the tail is equal to \( \text{res}(f^n(x) - a, f'(x))/\left(a f_n\right)^{d-1} \), and we can rewrite the resultant in terms of the product of \( f^n(c) \) where \( c \) is a root of \( f' \), a critical point of \( f \). That is

\[
\prod_{a \in f^{-n}(a)} f'(a) = a f_n^{-(d-1)} \text{res}(f^n(x) - a, f'(x)) = a f^{d+1}(-1)^{d-1}(d a f_{n})^{d} \prod_{c \in (f')^{-1}(0)} f^n(c) - a.
\]

Note that \(-1^{d+1} = 1\) for all positive integers \( d \) and \( n \). Putting everything together, we have

\[
\text{disc}(f^n(x) - a) = (-1)^{A(d, n)} a f_n^{B(d, n)} d^{\text{disc}(f^n(x) - a)} \prod_{c \in (f')^{-1}(0)} (f^n(c) - a),
\]

where

\[
A(d, n) = d^n \left( \frac{d^n - 1}{2} + \frac{d^{n-1} - 1}{2} \right),
\]

\[
B(d, n) = d^{2n-1} - 1.
\]

\[\square\]

**Remark 3.** Together Theorem 1 in [8], one can show that \( \text{disc}(f^n(x) - a) \) has a primitive prime for all but finite many \( n \) by assuming \( K \) an \( abc \)-field. This is not surprising at all since Odoni in [19] shows that for generic polynomial \( f \) the dynamical Galois group is isomorphic to the full wreath product.

**Lemma 11.** If \( \text{Gal}_f^n(\alpha) \cong [S_d]^n \), then \( K/\sqrt{\text{disc}(f^m(x) - \alpha) | m = 1, \ldots, n} \) is of index \( 2^n \) over \( K \). In particular, any quadratic subextension of \( K_f^n(\alpha) \) is a subfield of \( K/\sqrt{\text{disc}(f^m(x) - \alpha) | m = 1, \ldots, n} \).

**Proof.** By Lemma 9, the abelianization \( [S_d]_{ab} \) is the \( n \) fold direct product of \( S_{ab} = C_2 \). Therefore, if we can find an abelian extension \( K_{ab} \) of \( K \) contained in \( K_f^n(\alpha) \) with the index \([K_{ab} : K] = 2^n \) and it is built from adjoining square roots, we find all possible quadratic extensions of \( K \) in \( K_f^n(\alpha) \).

It remains to show that \( K/\sqrt{\text{disc}(f^m(x) - \alpha) | m = 1, \ldots, n} \) is a subfield of \( K_f^n(\alpha) \) that is of index \( 2^n \) over \( K \). We will show the following two assertions. We will first show that \( \sqrt{\text{disc}(f^m(x) - \alpha)} \) is not in \( K \) for any \( m = 1, \ldots, n \). Next, we will show that \( K/\sqrt{\text{disc}(f^(m')(x) - \alpha)} \) is not in \( K/\sqrt{\text{disc}(f^m(x) - \alpha)} \) for all \( m' = 1, \ldots, n - 1 \).

Since the Galois group is isomorphic to \([S_d]^n \), \( \text{Gal}_f^n(\alpha) \) is isomorphic to \([S_d]^m \) for all \( m = 1, \ldots, n \). Moreover for any distinct branches \( a, a' \in f^{-m}(\alpha) \), there is a Galois map \( \sigma \in \text{Gal}_f^n(\alpha) \) switching \( a \) and \( a' \) and fixing other roots. Indexing the roots of \( f^{m}(x) - \alpha = 0 \) with integers, denoted as \( a_i \), we have

\[
\prod_{i<j} (a_i - a_j) \xrightarrow{\sigma} - \prod_{i<j} (a_i - a_j).
\]

Hence, we know \( \sqrt{\text{disc}(f^m(x) - \alpha)} \notin K \).

For the second part, we use the fact that \( \text{Gal}_f^n(\alpha) \cong [S_d]^n \) again. It implies we can find a Galois map \( \sigma' \) only switching a pair of branches \( a, a' \in f^{-m}(\alpha) \) and \( f(a) = f(a') \). It
follows that $\sigma'$ fixes $\sqrt{\text{disc}(f^{m'}(x) - \alpha)}$ for all $m' < m$, but does not fix $\sqrt{\text{disc}(f^m(x) - \alpha)}$, which is the desired result.

The consequence of the previews lemma is that if the $\prod_{c \in (f')^{\infty}}(f^n(c) - \alpha)$ is a square, than the Galois group is not isomorphic to $[S_d]^n$. Together with Lemma 10, we can show a well-known result about post-critical finite maps. Since the discriminant of $f^n$ is recurrently defined by multiplying points on the orbit of all critical points, the discriminant of $f^n$ will be a perfect square eventually for all large enough $n$, and it is the following lemma.

Lemma 12. Let $f$ be a PCF polynomial over $K$, and $\alpha \in K$. Let $L$ be the minimum integer such that $f^L(C_f)$ is a periodic set, and let $O$ be the minimum integer such that $f^{L+O}(C_f) = f^L(C_f)$. Then

1. Suppose all critical points are periodic, and the degree of $f$ is odd. Then $\text{disc}(f^{2O} - \alpha)$ is a perfect square in $K$.
2. Suppose all critical points are periodic, and the degree of $f$ is even. If the leading coefficient of $f$ is a perfect square or $O$ is even, then $\text{disc}(f^{O+1} - \alpha)$ is a perfect square in $K_f^1(\alpha)$. Otherwise $\text{disc}(f^{O+2} - \alpha)$ is a perfect square in $K_f^{O+1}(\alpha)$.
3. Suppose a critical point is strictly periodic, and the degree of $f$ is odd. Then $\text{disc}(f^{L+2O-1} - \alpha)$ is a perfect square in $K_f^{L-1}(\alpha)$. In particular $K_f^{L-1}(\alpha) = K$ if $L = 1$.
4. Suppose a critical point is strictly periodic, and the degree of $f$ is even. If the leading coefficient $a_f$ of $f$ is a perfect square or $O$ is even, then $\text{disc}(f^{L+O} - \alpha)$ is a perfect square in $K_f^L$. If $a_f$ is not perfect square and $O$ is odd, then $\text{disc}(f^{L+O+1} - \alpha)$ is a perfect square in $K_f^{L+O}$.

Proof. Let us use an ambiguous terminology, a potential non-perfect square part of a product $a_1^{e_1} \cdots a_n^{e_n}$, to be $a_1^{e'_1} \cdots a_n^{e'_n}$ where $e'_i = 0$ for even $e_i$ and $e'_i = 1$ for odd $e_i$. Note that a potential non-perfect square part of an element $a$ in $K$ is not unique. It is up to how we express $a$ in terms of products. Obviously if a potential non-perfect square part of an element $a$ is a perfect square, then $a$ is a perfect square.

We claim that the potential non-perfect square part of the product $2$ of $\text{disc}(f^n - \alpha)$ over $K$ is

$$\left(\left(\frac{d}{4}\right)^d\right)^{b_n} \prod_{k=1}^{n} \prod_{i=1}^{d-1} f^k(c_i) - \alpha$$

for odd $d$, and is

$$a_f^{b_n} \prod_{i=1}^{d-1} f^n(c_i) - \alpha$$

for even $d$, where $b_n = 0$ if $n$ is even, and $b_n = 1$ otherwise. We will prove this claim in the end, but let us first see what happens if this assertion is true. We will show it case by case.

1. We use Equation 3. It is easy to see that the potential non-perfect square part is a perfect square by plugging $2O$ for $n$. 


2. If $a_f$ is a perfect square, then the coefficient of Equation 2.3 can be ignored. If $O$ is even, then both 1 and $1 + O$ are odd. Then we can see that $\prod f^{O+1}(c_i) - \alpha = \prod f(c_i) - \alpha$ which implies the potential non-perfect square part of $\text{disc}(f^{O+1} - \alpha)$ is a perfect square in $K_f^1(\alpha)$. Note that the square root of $a_f(\prod f(c_i) - \alpha)$ is in $K_f^1(\alpha)$. Thus if $O$ is odd, then we will find the square root of $\prod f(c_i) - \alpha$ in $K_f^{O+1}(\alpha)$ which implies the square root of $a_f$ is also in $K_f^{O+1}(\alpha)$. Then it is clear that $\text{disc}(f^{O+2} - \alpha)$ is a perfect square in $K_f^{O+1}(\alpha)$ by observing Equation 2.3.

3. Note that $f^L(C_f), \ldots, f^{L+2O-1}(C_f)$ repeat twice. Thus the product
\[ \prod_{c \in C_f} f^{k+c} - \alpha \]
is a perfect square. Moreover both $L - 1$ and $L + 2O - 1$ are either even or odd, so we observe Equation 3 by plugging $L + 2O - 1$ for $n$ and conclude that $\text{disc}(f^{L+2O-1} - \alpha)$ is a perfect square in $K_f^{L-1}(\alpha)$.

4. We will only proof the case where $a_f$ is a perfect square. Other cases are similar, and we left the proof for readers. Since $a_f$ is a perfect square, we can ignore $a_f$ in Equation 2.3. Then we notice that $\prod f(c) - \alpha = \prod f^{L+O}(c) - \alpha$, so $\text{disc}(f^{L+O} - \alpha)$ is a perfect square in $K_f^1(\alpha)$.

Now let us clean up the remaining assertion. We will show it by induction. For an odd $d$ the initial case is
\[ \text{disc}(f - \alpha) = \left( \frac{d}{4} \right) a_f^{d+1} d^{d+1} \prod f(c) - \alpha \]
and easy observation shows the initial case hold.

Now suppose $n$ is true for all $n < N$. Easy observation shows that the non-perfect square part of
\[ \text{disc}(f^N - \alpha) = \left( \frac{d}{4} \right) a_f^{2d-1} d^d (\text{disc}(f^{N-1} - \alpha))^{d+1} \prod f(c) - \alpha \]
is
\[ \left( \frac{d}{4} \right) d \text{disc}(f^{N-1} - \alpha) \prod f^N(c) - \alpha = \left( \frac{d}{4} \right) d \left[ \left( \frac{d}{4} \right) \prod f(c) - \alpha \right] \prod f^N(c) - \alpha. \]
Thus the assertion is true for odd $d$. Similar observation will show that the assertion is true for even $d$. \hfill \Box

3. Main results

### 3.1. Universal embedding of dynamical groups of PCF maps.
Intuitively, the dynamical Galois group loses all quadratic extensions given in the above Lemma. Following this idea, we can show the following well-known result.

**Corollary 13.** If $f$ is an odd degree PCF polynomial, then there exists some integer $N$ such that $\text{Gal}_f^N(\alpha)$ is not isomorphic to $[S_d]^N$. Moreover, the index of the arboreal representative of $\text{Gal}_f(\alpha)$ in $[S_d]^{\infty}$ is infinite.
Proof. This directly deduces from Theorem 14 and Proposition 6.

Given an integer $m$, I will need to construct two subgroup of $\text{Aut}(T_n)$, denoted by $E^m_n$ and $F^m_n$, where $T_n$ is a $d$-ary tree to $n$ levels, and show that $|\text{Aut}(T_n)|/|E^m_n|$ and $|\text{Aut}(T_n)|/|F^m_n|$ goes to infinity as $n \to \infty$. In the end, I use a lemma to show that, for some fixed integer $m$ depending on $f$, $\text{Gal}^f_{\alpha}(\alpha)$ is a subgroup of $E^m_n$ or $F^m_n$ for all $n$.

**Theorem 14.** Let $f$ be a PCF polynomial over a number field $K$, and suppose $\alpha$ is not periodic. Let $C_f$ be the set of all critical points of $f$. Let $L$ be the minimum integer such that $f^L(C_f)$ is a periodic set, and let $O$ be the minimum positive integer such that $f^O(C_f)$ is a perfect square in $K$.

1. Suppose the degree of $f$ is odd, and $L \leq 1$. Then $\text{Gal}^f_\alpha(\alpha)$ is a subgroup of $E^{2O}_n$.
2. Otherwise $\text{Gal}^f_\alpha(\alpha)$ is a subgroup of $F^{(m_1,m_2)}_n$ where

\[
(m_1, m_2) = \begin{cases} 
(0+1,1), & L = 0 \text{ and } O \text{ is even}; \\
(0+2,2), & L = 0 \text{ and } O \text{ is odd}; \\
(L + 2O - 1, L - 1), & L > 1 \text{ and } d \text{ is odd}; \\
(L + O, L), & L > 1, d \text{ is odd, and } af \text{ is a perfect square or } O \text{ are even}; \\
(L + O + 1, L + O), & L > 1, d \text{ is odd and } af \text{ is not a perfect square and } O \text{ is odd}.
\end{cases}
\]

**Proof.** Since $\alpha$ is not periodic, the dynamical tree of $f$ at $\alpha$ is graphically isomorphic to a full $d$-ary tree where $d$ is the degree of $f$.

Let us assume $L \leq 1$ and the degree of $f$ is odd. By Lemma 12 the $\text{disc}(f^{2O} - \alpha)$ is a perfect square in $K$, so $\text{Gal}^f_\alpha(\alpha)$ must be isomorphic to a subgroup of $\text{Aut}(T_m) \cap \ker(\text{sgn}_m)$. For $n > m$ we use induction. Let $f^{-1}(\alpha) = \{y_1, \ldots, y_d\}$. By the induction hypothesis the dynamical Galois group of $f$ at $y_i$, $\text{Gal}(K^n_f(y_i)/K(y_i))$ is isomorphic to a subgroup of $E^m_n$.

Clearly $\text{Gal}(K^{n+1}_f(\alpha)/K)$ is isomorphic to a subgroup of $E^m_n \cap \text{Aut}(T_1)$. Using the fact that the discriminant of $f^n - \alpha$ is a perfect square in $K$, it shows that any permutation acting on the $m$-th level of the tree $T_n$ is even when the permutation restricted to the $m$-th level. Thus $\text{Gal}^f_{n+1}(\alpha)$ is in the kernel of $\text{sgn}_m$.

For the rest of cases Lemma 12 implies there exists an integer $m_1$ such that $\text{disc}(f^{m_1} - \alpha)$ is a perfect square in $K^{m_2}(\alpha)$. Thus $\sigma \in \text{Gal}(K^{m_1}_f(\alpha)/K^{m_2}_f(\alpha))$ is an even permutation. To see it more clear, let $f^{-m_1}(\alpha) = \{y_i \mid i \in I(T_{m_1})\}$, the Galois group $\text{Gal}(K^{m_1}_f(\alpha)/K^{m_2}_f(\alpha))$ embeds into a subgroup of the

\[
\prod_{i \in I(T_{m_1})} \text{Gal}(K^{m_1-m_2}_f(y_i)/K^{m_2}_f(\alpha)),
\]

The $\text{Gal}(K^{m_2}_f/K)$ acts on the base point $y_i$, so $\text{Gal}(K^{m_1}_f(\alpha)/K)$ can be embedded, denote the map by $\tau_i$ into $\text{Aut}(T_{m_1-m_2}) \cap \text{Aut}(T_{m_2})$. Since $\sigma$ is an even permutation, we have $\tau(\sigma) \in \ker(\text{sgn}^{(m_1,m_2)})$. Similar to the proof of periodic cases, we can use induction to show that $\text{Gal}^f_\alpha(\alpha)$ can be embedded into $F^{(m_1,m_2)}_n$. \qed

3.2. The rank of $E^2_n$. Let $S$ be a subset of a group $G$. If $G = \langle S \rangle$, we call $S$ a generating set of $G$. It is a long-term goal to determine the cardinality of minimal generating set of $G$. Let

\[
d(G) = \min \{ |S| \mid G = \langle S \rangle \}.
\]
Here we recall an important theorem regarding $d(G)$ by Dalla Volta and Lucchini (see [5]).

**Lemma 15.** If a finite non-cyclic group $G$ contains a unique minimal normal subgroup $M$, then we have

$$d(G) \leq \max\{2, d(G/M)\}.$$

An easy consequence of this lemma is that if there is a tower of normal subgroups, say

$$(1) \triangleleft N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_k \triangleleft G$$

such that for $N \triangleleft G$ we have either $N \triangleleft N_k$ or $N = N_i$ for some $i$. Then $d(G) \leq \max\{2, d(G/N_i)\}$ for all $i$.

In the following we want to show that $E^m_n$ has a tower of normal subgroups satisfying Condition 5. We will argue a proper normal subgroup $N \triangleleft G$ is the unique one by showing:

1. For any proper normal subgroup $N'$ of $G$ we have $N \cap N' \neq \emptyset$.
2. $N$ is a smallest normal subgroup.

**Lemma 16.** For a nontrivial element $\sigma \in E^m_n$ there exists an element $c \in \ker(\res_{n-1} : E^m_n \to E^m_{n-1})$ such that

$$\sigma c \sigma^{-1} c^{-1} \neq 1.$$

For a nontrivial $c \in \ker(\res_{n-1} : E^m_n \to E^m_{n-1})$ there exists an element $\sigma \in E^m_n$ such that

$$\sigma c \sigma^{-1} c^{-1} \in M \setminus \{1\}.$$

**Proof.** Note that for any $\sigma = ((a_i)_{i \in I}; b) \in E^m_n$, let $a = ((a_i)_{i \in I}; 1)$ and $b = ((1)_{i \in I}, b)$, $\sigma = ba$.

Given $\sigma \in E^m_n$, we can write $\sigma c \sigma^{-1}$ as

$$ba \epsilon b^{-1}.$$

If $a$ is identity, we only need to choose $c$ such that $c_i \neq c_j$ where $b^{-1}(i) = j$. If $a$ is not identity, then for $d \geq 5$ we can choose $c_i$ and $c_j$ that is products of different length of disjoint cycles, i.e. a product of two disjoint 2-cycles and a 3-cycle, note that this choice makes $c \in \ker(\res_{n-1})$. For $d = 3$ we may choose $c_1$ be a 3-cycle, $c_2$ and $c_3$ a 2-cycle. Then $a_i c_i a_i^{-1} \neq a_j c_j a_j^{-1}$ by how we choose the permutation. Then $b(\epsilon a \epsilon^{-1} b)$ is back to the case that we assume $a$ is identity. Hence the result follows.

Given $c = ((c_i); 1) \in \ker(\res_{n-1} : E^m_n \to E^m_{n-1})$ and for $\sigma \in E^m_n$, we can write $\sigma c \sigma^{-1}$ as

$$ba \epsilon b^{-1}.$$

If $c_i = c_j$ for all $i$ and $j$, then we may take two transpose $a_1$ and $a_2$ that are not disjoint from $c_1$ and $c_2$. By taking $b$ to be the identity, we again show the desired result.

Now for some distinct indices $i$ and $j$ we have $c_i \neq c_j$, then by Lemma 7 we have $b$ transpose $i$ and $j$. For both $c_i$ and $c_j$ even or odd we take $a$ to be the identity, and it implies $\sigma c \sigma^{-1} c \in M \setminus \{1\}$. Now without lose of generality we may assume $c_i$ is an even permutation and $c_j$ is an odd permutation. Since $c \in E^m_n$, we must have an odd permuation $c_j$ with $j \neq j'$. If $c_j = c_{j'}$, we may process a conjugation on $c_{j'}$ by some even permutation such that $c_j \neq c_{j'}$. Thus we may assume $c_j \neq c_{j'}$. By Lemma 7 we have $b$ transposing $j$ and $j'$. Following the above processes, we find a $\sigma$ such that the desired result holds.

**Proposition 17.** Let $\sigma \in [S_d]^n$. There exists an $\tau \in [S_d]^n$ such that $\sigma \tau = \sigma^{-1}$. 
Proof. We show the statement by induction. For \( n = 1 \) the statement trivially follows from the fact that \( \text{Aut}(S_d) \cong S_d \).

For the sake of induction argument we assume the statement is true for a positive integer \( N \). Given an element \( \sigma \in \text{Aut}(T_{N+1}) \cong \text{Aut}(T_1) \ltimes \text{Aut}(T_N) \) we may write \( \sigma \) as
\[
\sigma = ( (\sigma_i)_{i \in I(T_N)}, \sigma_0 )
\]
for \( \sigma_i \in S_d \). Thus for each \( i \) we have \( \tau_i \) such that \( \sigma_i \tau_i = \sigma_i \inv \) by the fact that \( \text{Aut}(S_d) \cong S_d \) and the induction hypothesis. Now we observe
\[
((\tau_{\sigma_i^{-1}(i)});_{i \in I(T_d)}; 1)(1; \tau_0)(((\sigma_i);_{i \in I(T_d)}; \sigma_0)(1; \tau_0)^{-1}((\tau_{\sigma_i^{-1}(i)});_{i \in I(T_d)}; 1)^{-1}
\]
is the inverse of \( \sigma \).

Lemma 18. Suppose one of the followings holds:

1. Let \( G \) be a group. Assume that, for any \( g \in G \), there exists \( h \) such that \( g^h \neq g^{-1} \).
2. Let \( \text{res}_n : G \rtimes \text{Aut}(T_n) \to \text{Aut}(T_n) \). Assume \( H \subseteq \ker(\text{res}_n) \) is a normal subgroup of \( G \rtimes \text{Aut}(T_n) \), and for any \( h \in H \) there exists \( \sigma \in \text{Aut}(T_n) \) such that \( \sigma(h) \neq h^{-1} \).

Then any proper normal subgroup of \( G \rtimes \text{Aut}(T_n) \) or \( H \rtimes \text{Aut}(T_n) \) respectively contains a non-trivial element in \( \{ (g_1, \ldots, g_n); 1 \mid g_i \in G \} \).

Proof. For any element \( \tau \in N \triangleleft G \rtimes \text{Aut}(T_n) \) there exist \( g = ( (g_i)_i)_{i \in I(T_n)} 1 \) and \( s = (1; \sigma) \) for \( g_i \in G \) and \( \sigma \in \text{Aut}(T_n) \) such that \( \tau = sg \). By Proposition 17 there exists \( t \in G \rtimes \text{Aut}(T_n) \) such that \( tnt^{-1} = s^{-1} \). Thus we have
\[
\tau^t \sigma = ((*) ; 1).
\]

For the first statement one can conjugate some \( g_i \) by a proper \( h \) such that \( g_i^h \neq g_i^{-1} \). Thus we may conjugate \( \tau \) by some proper element \( h \in \ker(\text{res}_n) \) such that \( \tau^t \sigma^h \neq 1 \).

For the second argument since \( \text{Aut}(T_n) \) acts on the index of \( G^{d^m} \) and \( H \) is normal, the natural map \( \phi : \text{Aut}(T_n) \to \text{Aut}(H) \) is an homomorphism which implies \( H \rtimes \text{Aut}(T_n) \) is well-defined. By the assumption we can again construct a nontrivial element in \( \ker(\text{res}_n) \) via a similar manner. \( \square \)

Let \( e_i \in C_2^{d^m-1} \) be an element of the form \((1, \ldots, -1, \ldots, 1)\) where \(-1\) only appears on the \( i \)-th coordinate. Let \( k_i = d^{i-1} + 1 \). We define
\[
X_i = \{ (e_1 + e_{k_i}; 1)\sigma \mid \sigma \in \text{Aut}(T_n) \} \subseteq C_2^{d^m} \rtimes \text{Aut}(T_n)
\]
for \( i = 1, 2, \ldots, n \). We have the following important lemma.

Lemma 19. Let \( H_1 = \langle X_i \rangle \rtimes \text{Aut}(T_n) \), and let \( \text{res}_n : H \to \text{Aut}(T_n) \). Then \( \langle X_1 \rangle \) is the unique minimal normal subgroup of \( H_1 \). In particular, let \( H = \langle X_1 \rangle \rtimes \text{Aut}(T_1) \), we have \( \langle X_1 \rangle = \ker(\text{res}_1) \).

Proof. To show \( H_1 \) is the unique minimum proper subgroups of \( H_1 \) we apply the two-step argument. Firstly we notice that the order of the generators are 2. Secondley \( H_n \) is a subgroup of \( C_2 \rtimes \text{Aut}(T_n) \), and for any \( h \in \langle X_i \rangle \) one can find \( \sigma \text{Aut}(T_n) \) such that \( \sigma(h) \neq h \). By Lemma 18 any proper normal subgroup of \( H_n \) intersecting with the kernel of \( \text{res} : H_n \to \text{Aut}(T_n) \) contains a nontrivial element.

We will use the nontrivial element to construct \( e_1 + e_2 \) by a sequence of conjugation. Since \( \text{Aut}(T_n) \) acts transitively on \( I(T_n) \), we can assume that the nontrivial element \( h \) exists in the intersection has \(-1\), the nontrivial element of \( C_2 \), in the block of \( B(T_n / T_{n-1})(1, \ldots, 1) \).
We also notice that $\sigma = (((12 \cdots d), 1, \ldots, 1); 1)$ shift the block by conjugation, so $h^\sigma h$ has even $-1$ on the first block and $1$ on all entries of the reside blocks. Next we claim that for even $-1$ and odd $1$ on a black with $S_d$ acting on the index, we can always have

$$(-1, \ldots, -1, 1, \ldots, 1)$$

by conjugating an even permutation. If $h$ is already in the desired form, then we are done. Otherwise there are three unceasing index, say $i, i + 1$ and $i + 2$, with $1$ and $-1$ distributing in one of the following layouts

$$1, -1, -1$$
$$-1, 1, -1$$
$$1, -1, 1$$
$$1, 1, -1.$$

One can applying conjugation by the 3-cycle $(i, i + 1, i + 2)$ several times to move the above layouts to either $-1, -1, 1$ or $-1, 1, 1$. If the element after applying conjugation is not in the desired form, we repeat the process. Since there are only finite many indices, we can have the desired from after finite many times of applying the process. Moreover since we apply $3 - \text{cycle}$ each time, the desired result can be achieved by applying an even permutation. Now we can conjugate $(-1, -1, \ldots, -1, 1, \ldots, 1)$ by $(12 \cdots d)$ to get $(1, -1, \ldots, -1, 1, \ldots, 1)$. Note that the multiplication of $(-1, -1, \ldots, -1, 1, \ldots, 1)$ and $(1, -1, \ldots, -1, 1, \ldots, 1)$ gives $(-1, 1, \ldots, 1, -1, 1, \ldots, 1)$. Finally we repeating the second process to get $(-1, -1, 1, \ldots, 1)$. Since an arbitrary proper normal subgroup contains the generator of $H_1$, we shows that $\langle X_1 \rangle$ is the unique minimal normal subgroup of $H_i$. \hfill $\square$

**Remark 4.** The above proof can be written as the following pseudocode.

**Algorithm 1:** The pseudocode of the above proof

```plaintext
Data: A tuple $a = (a_1, \ldots, a_d) \in C^d$ with $\prod a_i = 1$ and odd $d$
Result: The tuple $(1, -1, 1, \ldots, 1)$

1. while $a \neq (-1, -1, 1, \ldots, 1)$ do
   2. $a' = a$;
   3. $b = (-1, \cdots, -1, 1, \cdots, 1)$ with same number of $-1$ as in $a$;
   4. while $a' \neq b$ do
      5. Find the smallest index $i$ such that $a_i' = 1$ and $a_{i+1}' = -1$;
      6. $(a_i', a_{i+1}', a_{i+2}') = (a_{i+1}', a_i', a_{i+2}')$;
   7. end
   8. $a' = (a_i', a_1', a_2', \ldots, a_{d-1}')$;
   9. $a = aa'$;
end

**Proposition 20.** Let $a_1 = (123)$ or $(12 \cdots d)$. Then for $a = ((a_1, a_2, a_3, \ldots, a_d); 1) \in E^2$ there exists $\sigma \in E^2$ such that $a^\sigma = ((a_1, a_2^{-1}, a_3^{-1}, \cdots, a_d^{-1}); 1)$ or $((a_1, a_2, a_3^{-1}, \cdots, a_d^{-1}); 1)$.

**Proof.** For any $a_i$ there exists an element $s_i \in S_d$ such that $a_i^{s_i} = a_i^{-1}$. If $((1, s_2, \ldots, s_d); 1)$ is in $E^2$, then it is done. Otherwise there are odd many odd permutations $s_i$. Without lose of
generality we assume $s_2$ is odd. Then we can conjugate $a$ by $((1, 1, s_3, \ldots, s_d); 1) \in E_2^n$ to get $((a_1, a_2, a_3^{-1}, \ldots, a_d^{-1}); 1)$. □

**Lemma 21.** Let $d$ be an odd integer, and let $\text{res}_n : E_2^n \to E_2^{n-1}$ be the natural restriction from $\text{Aut}(T_{n+1})$ to $\text{Aut}(T_n)$. Let $M_n = ((A_d)_{i \in I}, 1) \subseteq E_{n+1} \subseteq \text{Aut}(T_1) \cap \text{Aut}(T_n)$ where $A_d$ is the alternative group of degree $d$. Then $E_2^n$ has a tower of normal subgroup

$$\{1\} \triangleleft M_n \triangleleft \ker(\text{res}_n) \triangleleft E_2^n$$

satisfying Condition $\mathcal{F}$.

**Proof.** We first need to show that $M_n$ is a normal subgroup. It is clear a subgroup of $E_2^n$. For an element $\sigma \in E_2^n$ one can express $\sigma$ as $((a_i)_{i \in I}, b) \in \text{Aut}(T_1) \cap \text{Aut}(T_n)$. Let $a = ((a_i)_{i \in I}, 1)$ and $b = ((1), b)$. Then we have $\sigma = ba$ and

$$\sigma M_n \sigma^{-1} = ba M_n a^{-1} b^{-1} = b M_n b^{-1} = M_n.$$ 

Since we show $M_n$ is a subgroup of $E_2^n$ and a normal subgroup of a group containing $E_2^n$, $M_n$ is a normal subgroup of $E_2^n$.

Next we shall show that a nontrivial normal subgroup $N$ contains an element in $M_n$. Given an element $\sigma \in N$ and $c = ((c_i)_{i \in I}, 1) \in E_2^n$ we have $\sigma c \sigma^{-1} c^{-1} \in N$. If $\sigma$ is in $M_n$, then it is done. Now we can assume $\sigma \notin M_n$, and Lemma 16 shows that for a given $\sigma$ we have $c \in \ker(\text{res}_{n-1})$ such that

$$\sigma c \sigma^{-1} c^{-1} \neq 1.$$ 

Since $c$ is also in a normal subgroup, it follows that $1 \neq \sigma c \sigma^{-1} c^{-1} \in N \cap \ker(\text{res}_n)$. Denote $\sigma c \sigma^{-1} c^{-1}$ by $\gamma$. Consequently if $\gamma$ has order greater than 2, then we have $\gamma^2 \in N \cap M_n$. Otherwise using the second part of Lemma 16, we have some $\delta \in E_2^n$ such that $\delta \gamma \delta^{-1} \gamma^{-1} \in N \cap M_n$.

If we can further show that $M_n$ is a smallest normal subgroup of $E_2^n$, then we can conclude that $M$ is the unique normal subgroup of $E_2^n$. We will use induction to show that $M_n$ is the smallest normal subgroup of $E_2^n$ for $n \geq 2$. Let

$$\rho_i : \ker(\text{res}_1 : E_2^2 \to E_1^2) \to \text{Aut}(T_1);$$

$$((a_i)_{i \in I}, 1) \mapsto a_i.$$ 

be a homomorphism. If $N$ is a normal subgroup of $E_2^2$, then $M_2 \cap N$ is a normal subgroup of $\ker(\text{res}_1)$ which implies $\rho_i(M_2 \cap N)$ is a normal subgroup of $\text{Aut}(T_1)$. Thus $\rho_i(M_2 \cap N) \cong \{1\}$ and $A_d$. Since $\text{res}_1(E_2^2) = \text{Aut}(T_1)$ acts transitively on the level 2 of the tree, we conclude that $\rho_i(M_2 \cap \ker(\text{res}_1)) \cong A_d$ for all $i$. Without lose of generality we may take $i = 1$, so for any $a_1 \in A_d$ and for $a_i \in S_d$ with $i = 2, \ldots, d$ the element $a = ((a_1, a_2, \ldots, a_d); 1)$ exists in $N \cap M_2$. In particular we may choose $a_1 = (123)$ or $(12 \cdots n)$, where $\{(123), (12 \cdots n)\}$ forms a generating set of $A_d$ for an odd $d$. We claim $a' = (a_1, 1, 1, \ldots, 1; 1)$ exists in the intersection. By Proposition 20 we know we can conjugate $a$ to $a_1 = ((a_1, a_2^{-1}, \ldots, a_d^{-1}); 1)$ or $a_2 = ((a_1, a_2, a_3^{-1}, \ldots, a_d^{-1}); 1)$. If a conjugates to $a_1$, then a power of $aa_1$ is in the desired form. If the result of conjugation is the second case, then we can conjugate $aa_2$ by $((1, 12, (12), 1, \ldots, 1); 1) \in E_2^n$ to get $a' = ((a_1^2, a_2^{-2}, 1, \ldots, 1); 1)$, then the desired result can be achieve by taking a power of
Therefore we prove that \( M_2 \) is a proper minimum subgroup of \( E_2^n \). Let us assume \( M_n \) is a proper minimum subgroup of \( E_2^n \). It implies \( \mathcal{A} = \{(a, 1, \ldots, 1); 1) \in \text{Aut}(T_1) \ltimes \text{Aut}(T_{n-1}) | a \in A_d \} \) is a subgroup of \( M_n \subseteq E_2^n \), and so
\[
\mathcal{A}' = \{(a', 1, \ldots, 1); 1) \in E_2^n \ltimes \text{Aut}(T_1) | a \in A = \{(a, 1, \ldots, 1); 1) \in \text{Aut}(T_1) \ltimes \text{Aut}(T_{n}) | a \in A_d \}
\]
is a subgroup of \( M_{n+1} \). By Lemma 7 it follows that \( M_{n+1} \) is a minimum subgroup of \( E_2^n \). Thus we show that \( M_n \) is the unique proper minimum subgroup of \( E_2^n \) for \( n \geq 2 \).

We claim that \( E_2^n / M_n \) is isomorphic to \( C_2 \ltimes \text{Aut}(T_{n-1}) \). Let us define a homomorphism
\[
\phi : E_2^n \subseteq \text{Aut}(T_1) \ltimes \text{Aut}(T_{n-1}) \rightarrow C_2 \ltimes \text{Aut}(T_{n-1})
\]
\[(a_i)_{i \in I(T_{n-1})}, b) \mapsto ((\text{sgn}(a_i))_{i \in I(T_{n-1})}, b).\]

It is standard to check \( \ker(\phi) \cong M_n \) and \( \phi \) is onto. Finally we apply Lemma 19 to conclude that \( \ker(\text{res}_{n-1}) / M_2 \) is the unique minimal subgroup of \( E_2^n / M \). Now we show every assertion of this lemma.

**Theorem 22.** The rank of the group \( E_2^n \) is 2 for all \( n \). Moreover \( E_2^n \) has a unique chief series.

**Proof.** By Lemma 15 and Lemma 21 we have \( d(E_2^n) \leq \max\{2, d(E_2^n / M_n)\} \) and \( d(E_2^n / M_n) \leq \max\{2, d(E_2^n / \text{res}_n)\} \), so \( E_2^n / \text{res}_n \cong E_2^{n-1} \). Moreover we have \( E_2^n / \text{res}_n \cong E_2^{n-1} \), so we can conclude that
\[
d(E_2^n) \leq \max\{2, d(E_2^{n-1})\} \leq \cdots \leq \max\{2, d(E_2^1)\} = 2.
\]

Lemma 21 also shows that \( M_{n-1} \) is the proper unique minimal normal subgroup of \( E_{n-1} \), so \( \text{res}_{n-1}^{-1}(M_{n-1}) \) is a unique minimal normal subgroup in \( E_n \) that contains the tower of normal subgroup \( M_n \ltimes \ker(\text{res}_n) \). Thus we can recursively construct a unique normal series such that each factor is a chief factor.

**3.3. Examples.** In this section we are going to investigate the arboreal representatives of \( f(z) = 2z^3 - 3z^2 + 1 \) at a proper chosen base point \( x \). The idea of the proof is almost identical to [1].

Let \( K \) be a number field and let \( x \in K \setminus \{0, 1\} \). We assume the pair \((K, x)\) satisfies the following condition:

\[
\text{(5) there exists } p \text{ and } q \text{ of } K \text{ lying above } 2 \text{ and } 3 \text{ such that}
\]

\[
either v_q(x) = 1 \text{ or } v_q(1 - x) = 1, \text{ and either } v_p(1 - x) = 1 \text{ or } v_p(x) = 1
\]

**Lemma 23.** If \((K, x)\) satisfies Condition 5, then \( f^n(z) - x \) is Eisenstein at \( q \) for all \( n \geq 1 \). In particular \( f^n(z) - x \) is irreducible.

**Proof.** For \( n = 1 \) and \( v_q(x) = 1 \) we have
\[
f(z) \equiv (-z^3 + 1) \equiv -(z - 1)^3 \mod q,
\]
so \( f(z - 1) - x \) is Eisenstein. For \( n = 2 \) we have
\[
f^2(z) = -(f(z) - 1)^3 \equiv -(z^3)^3 = z^9 \mod q.
\]
Then it is easy to prove the statement by induction.
For \( v_q(1 - x) = 1 \) we have
\[
f(z) \equiv (-z^3) \mod q.
\]
and
\[ f^2(z) \equiv -f(z)^3 \equiv (z - 1)^3 \mod q. \]

Again the conclusion will follow easily by induction. \( \square \)

**Lemma 24.** Let \((K, x), p\) and \(q\) satisfy Condition 5, and let \(y \in f^{-n}(x)\). Then:
- There are prime \(p'\) and \(q'\) of \(K(y)\) lying above \(p\) and \(q\) respectively such that
  \[ e(p'/p) = 2^n \text{ and } e(q'/q) = 3^n \]
- \((K(y), y)\) satisfies Condition 5.

**Proof.** We first prove the assertion for \(q'\). Suppose \(v_q(x) = 1\), then \(y \in f^{-1}(x)\) has \((y - 1)^3 \mod q\) which implies there exists a unique prime \(q'\) of \(K(y)\) above \(q\) satisfies \(v_q(1 - y) = 1\), i.e. \(e(q'/q) = 3\). On the other hand, if we have \(v_q(1 - x) = 1\), then it implies there exists a unique prime \(q'\) of \(K(y)\) such that \(v_{q'}(y) = 1\).

For \(p'\) we also prove the statement case by case. Let \(v_p(1 - x) = 1\), then we note that the Newton polygon of \(f(z) - x\) has a segment of length 2 and height 1 which implies there exists a prime \(p'\) above \(p\) such that \(e(p'/p) = 2\). Moreover we have \(v_{p'}(y) = 1\) for \(y \in f^{-1}(x)\).

Let \(v_p(x) = 1\), then we have
\[ f(z) - x \equiv -z^2 + 1 \equiv -(z - 1)^2 \mod p. \]

Thus there exists a prime \(p'\) over \(p\) with \(v_{p'}(1 - y) = 1\).

Since \(x\) is arbitrary chosen with an arbitrary \(y \in f^{-1}(x)\) such that \((K(y), y)\) satisfies Condition 5, the statement is true by induction. \( \square \)

**Corollary 25.** Let \((K, x)\) be as in Proposition 24. Then \(6^n|[K^n_f(x) : K]|\). In particular there exists an order 2 and order 3 elements in \(\text{Gal}(K^n_f/K^{n-1}_f)\)

**Proof.** The proof is easy by induction, and we refer readers to [1] for more details. The order 2 and 3 elements exist because Cauchy Theorem. \( \square \)

**Theorem 26.** Let \((K, x)\) satisfies Condition 5. Then for \(n \geq 1\) we have
\[ \text{Gal}^n_f(x) \cong E_n. \]

**Proof.** In [5] they prove their theorem by notice that the existence of elements of order 2 and 3 which implies there is a two 2-cycle permutation in \(\text{Gal}^2_f(x)\) and a 3-cycle in \(\text{Gal}^3_f(x)\) fixing \(f^{-1}(x)\). Thus their proof works exactly the same in our case. \( \square \)

4. **Questions**

There are some questions that the author cannot settle in this paper. We choose the polynomial \(f(z) = 2z^3 - 3z^2 + 1\) because the critical points of \(f\), \(C_f = \{0, 1, \infty\}\), satisfies \(f(C_f) = C_f\). We can define a more general polynomial with the same critical portrait. Let \(B(x)\) be an odd degree Belyi map that has three fixed critical points 0, 1 and \(\infty\), and then \(-B(z) + 1\) will transpose 0 and 1 and fix \(\infty\). By Theorem 14 it is clear that the \(n\)-th dynamical subgroup of \(-B(z) + 1\) is a subgroup of \(E_n^2\). Hence the question is "do we have an isomorphism?".
**Question 5.** Let $K$ be a number field. Let $f \in K[z]$ be an odd degree polynomial. Assume $C_f = \{c_1, c_2, c_3\}$ with the critical portrait

$$c_1 \to c_2, \ c_2 \to c_1, \ c_3 \to c_3.$$ 

Then do we have $\text{Gal}_f^n(\alpha) \cong E_n^2$ with a properly chosen basepoint $\alpha \in K$?

A possible approach is using the method introduced in [2]. The first step is to show that the Geometric Galois group $\text{Gal}(B^n(z) - t/\overline{K}(t))$, where $t$ is transcendental over $K$, is isomorphic to $E_n^2$, and then deduce that the arithmetic Galois group is also isomorphic to $E_n^2$. The last step is to study the ramification condition of $K^\nu_f(\alpha)$ over $K$ to show that with a specified basepoint $\alpha$ we have the desired isomorphism.

My next question is the following.

**Question 6.** Is there a pair of PCF polynomial $f$ over $K$ and a basepoint $\alpha \in K$ such that $\text{Gal}_f^n(\alpha) \cong F_n^{(m_1, m_2)}$?

The first thing we have to solve for this question is that we have to find a proper family of PCF maps that has tail length greater than but not equal to 1. We didn’t see an obvious target that satisfying the requirement.

Finally we would like to know the chief series of $E_n^m$ for $m \geq 3$ and $F_n^{(m_1, m_2)}$. The difficulty of generalize our argument to other cases is the following observation. Recall Lemma 19. Let $H_n = \langle X_n \rangle \text{Aut}(T_n)$ with $n \geq 1$. Then the quotient group $H_n/\langle X_1 \rangle$ correspond to the following exact sequence

$$\{1\} \to \langle X_1 \rangle \to X_n \to H_n \to \text{Aut}(T_n) \to \{1\}.$$ 

Notice that $\ker(\text{res}_{n-1} : \text{Aut}(T_n) \to \text{Aut}(T_m))$ acts trivially on $\langle X_n \rangle/\langle X_1 \rangle$. Thus we have

$$H_n/\langle X_1 \rangle \cong (\langle X_n \rangle/\langle X_1 \rangle \times \ker(\text{res}_{n-1})) \rtimes \text{Aut}(T_{n-1}).$$

Note that both $\langle X_n \rangle/\langle X_1 \rangle$ and $\ker(\text{res}_{n-1})$ are normal subgroup and has trivial intersection. Thus we don’t have a unique tower of normal subgroup satisfying Condition 5. Thus our argument doesn’t work. For $F_n^{(m_1, m_2)}$ the situation seems more complicate, and some part of our argument depends on the fact that $d$ is odd and we have even many $-1$. My question is that

**Question 7.** Can we count the number of chief series in $E_n^m$ for $m \geq 3$? Is there a way to bound the rank of $E_n^m$ from pure algebraic point of views? Do we have a unique chief series in $F_n^{(m_1, m_2)}$ for small $m_1$ and $m_2$?

**Acknowledgments**

The author would like to thank Dr. Alexander Hulpke for very helpful discuss and comments, and Dr. Andrea Lucchini for useful comments on the rank of groups. The author also want to thank his advisor Dr. Thomas Tucker for various support.

**References**

[1] Robert L. Benedetto, Xander Faber, Benjamin Hutz, Jamie Juul, and Yu Yasufuku. A large arboreal Galois representation for a cubic postcritically finite polynomial. *Res. Number Theory*, 3:Art. 29, 21, 2017.

[2] I.I. Bouw, Ö. Ejder, and V. Karemaker. Dynamical belyi maps and arboreal galois groups. *manuscripta math.*, 2020.
[3] Michael R. Bush, Wade Hindes, and Nicole R. Looper. Galois groups of iterates of some unicritical polynomials. *Acta Arith.*, 181(1):57–73, 2017.

[4] Francesca Dalla Volta and Andrea Lucchini. Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc. Ser. A*, 64(1):82–91, 1998.

[5] Francesca Dalla Volta and Andrea Lucchini. Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc. Ser. A*, 64(1):82–91, 1998.

[6] E. Detomi and A. Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra*, 265(2):651–668, 2003.

[7] Richard Gottesman and Kwokfung Tang. Quadratic recurrences with a positive density of prime divisors. *Int. J. Number Theory*, 6(5):1027–1045, 2010.

[8] C. Gratton, K. Nguyen, and T. J. Tucker. ABC implies primitive prime divisors in arithmetic dynamics. *Bull. Lond. Math. Soc.*, 45(6):1194–1208, 2013.

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

[10] I. Martin Isaacs. *Algebra: a graduate course*, volume 100 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009. Reprint of the 1994 original.

[11] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)*, 78(2):523–544, 2008.

[12] Rafe Jones. Galois representations from pre-image trees: an arboreal survey. In *Actes de la Conférence “Théorie des Nombres et Applications”*, volume 2013 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 107–136. Presses Univ. Franche-Comté, Besançon, 2013.

[13] Rafe Jones and Michelle Manes. Galois theory of quadratic rational functions. *Comment. Math. Helv.*, 89(1):173–213, 2014.

[14] J. Juul. Iterates of generic polynomials and generic rational functions. *Trans. Amer. Math. Soc.*, 371(2):809–831, 2019.

[15] Jamie Juul. *Galois Groups of Iterated Rational Maps and their Applications*. ProQuest LLC, Ann Arbor, MI. Thesis (Ph.D.)–University of Rochester.

[16] Nicole Looper. Dynamical Galois groups of trinomials and Odoni’s conjecture. *Bull. Lond. Math. Soc.*, 51(2):278–292, 2019.

[17] R. W. K. Odoni. The Galois theory of iterates and composites of polynomials. *Proc. London Math. Soc. (3)*, 51(3):385–414, 1985.

[18] R. W. K. Odoni. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. *J. London Math. Soc. (2)*, 32(1):1–11, 1985.

[19] R. W. K. Odoni. On the Galois groups of iterated generic additive polynomials. *Math. Proc. Cambridge Philos. Soc.*, 121(1):1–6, 1997.

[20] Richard Pink. Profinite iterated monodromy groups arising from quadratic morphisms with infinite postcritical orbits, 2013.