ARBOREAL GALOIS GROUPS OF POSTCRITICALLY FINITE QUADRATIC POLYNOMIALS

ROBERT L. BENEDETTO, DRAGOS GHIOCA, JAMIE JUUL, AND THOMAS J. TUCKER

Abstract. We provide an explicit construction of the arboreal Galois group for the postcritically finite polynomial $f(z) = z^2 + c$, where c belongs to some arbitrary field of characteristic not equal to 2. In this first of two papers, we consider the case that the critical point is periodic.

1. Introduction

Throughout our paper, we let K be a field of characteristic not equal to 2 with algebraic closure $\overline{K}$, and let $f(z) \in K[z]$ be a polynomial of degree 2. After conjugating by a K-rational change of coordinates, we may assume that $f(z) = z^2 + c$ for some $c \in K$.

1.1. **Arboreal Galois groups.** We consider the iterates f^n of f under composition, where $f^0(z) := z$, and where $f^{n+1} = f \circ f^n$ for each integer $n \geq 0$. A point $y \in \overline{K}$ is said to be *fixed* if $f(y) = y$, or *periodic* if $f^n(y) = y$ for some $n \geq 1$, or *preperiodic* if $f^n(y) = f^m(y)$ for some $n > m \geq 0$. If y is periodic, then its *exact period* is the smallest $n \geq 1$ for which $f^n(y) = y$. If y is preperiodic but not periodic, then we say it is *strictly preperiodic*.

Given a point $x_0 \in K$, then for every integer $n \geq 0$, we define

$$K_n := K_{x_0,n} := K(f^{-n}(x_0)) \qquad \text{and} \qquad G_n := G_{x_0,n} := \mathrm{Gal}(K_n/K)$$

to be the n-th preimage field and its associated Galois group. Note that $\cdots K_3/K_2/K_1/K$ is a tower of field extensions, which we view as contained in $\overline{K}$. Thus, we may further define

$$K_\infty := K_{x_0,\infty} := \bigcup_{n\geq 0} K_{x_0,n} \qquad \text{and} \qquad G_\infty := G_{x_0,\infty} := \mathrm{Gal}(K_{x_0,\infty}/K) \cong \varprojlim_n G_{x_0,n}.$$

If the backward orbit

$$\mathrm{Orb}_f^-(x_0) := \bigcup_{n\geq 1} f^{-n}(x_0)$$

contains no critical values of f, then each $f^{-n}(x_0)$ has exactly 2^n elements. If, in addition, x_0 is not periodic under f, then the sets $f^{-n}(x_0)$ are pairwise disjoint, and hence $\mathrm{Orb}_f^-(x_0)$ has the structure of an infinite binary rooted tree T_∞, with $x \in f^{-(n+1)}(x_0)$ connected to $f(x) \in f^{-n}(x_0)$ by an edge. Thus, the action of the Galois group G_∞ on the backward orbit induces an embedding of G_∞ into the automorphism group $\mathrm{Aut}(T_\infty)$ of the tree. Similarly, for each $n \geq 0$, the action of G_n on $f^{-n}(x_0)$ induces an embedding of G_n into the automorphism group $\mathrm{Aut}(T_n)$ of the finite binary rooted tree T_n with n levels. For this reason, the groups G_n and G_∞ have come to be known as *arboreal* Galois groups. Moreover, given our interest in this action, whenever we discuss homomorphisms or isomorphisms between groups acting on trees, we always mean homomorphisms that are equivariant with respect to this action. We note that the problem of fully understanding the arboreal Galois groups has generated a great deal of research in the recent years; see [ABC+22, BDG+21, BFH+17, BGJT23, BJ19, JKMT16, Juu19, Pin13], for example.

2010 *Mathematics Subject Classification.* 37P05, 11G50, 14G25.

1.2. **Postcritically finite quadratic polynomials.** In this paper, we consider the case that f is *postcritically finite*, or PCF, meaning that all of the the critical points of f are preperiodic. Since we have assumed $f(z) = z^2 + c$, the critical points are 0 and ∞, with ∞ necessarily fixed; thus, to say that f is PCF is equivalent to saying that 0 is preperiodic under f. In this case, it is well known that G_∞ is of infinite index in $\mathrm{Aut}(T_\infty)$.

If the critical point 0 is preperiodic, then the values $f(0), f^2(0), \dots, f^r(0)$ are all distinct for some maximal integer $r \geq 1$, with $f^{r+1}(0)$ repeating one of these values. That is, we have $f^{r+1}(0) = f^{s+1}(0)$ for some minimal integers $r > s \geq 0$. Equivalently, since the two preimages of $f(y)$ are $\pm y$, we have $f^r(0) = -f^s(0)$ for minimal integers $r > s \geq 0$. Note that if $s = 0$, then the point 0 is periodic, and r is the cardinality of the *forward orbit*

$$\mathrm{Orb}_f^+(0) := \{f^i(0) : i \geq 0\}$$

of 0 under f. Otherwise, if $s \geq 1$, then 0 is strictly preperiodic, and $|\mathrm{Orb}_f^+(0)| = r + 1$. In the latter case, the point $f^{s+1}(0) = f^{r+1}(0)$ is periodic of exact period $r - s \geq 1$, preceded by a tail $\{0, f(0), \dots, f^s(0)\}$ of cardinality $s + 1 \geq 2$.

1.3. **Previous work on describing the arboreal Galois groups for PCF quadratic polynomials.** In [Pin13], Pink describes the group G_∞ for each of the various choices of r, s when the quadratic polynomial f is PCF, in the case that $K = \overline{k}(t)$ is a rational function field over an algebraically closed field $\overline{k}$, and that the root point of the preimage tree is $x_0 = t$. Pink denotes this group G^{geom}, and he proves that it is isomorphic to a subgroup of $\mathrm{Aut}(T_\infty)$ that he simply calls G, but which we denote $G^{\mathrm{Pink}}_{r,s,\infty}$. (When $s = 0$, we sometimes write simply $G^{\mathrm{Pink}}_{r,\infty}$.) He defines $G^{\mathrm{Pink}}_{r,s,\infty}$ via explicit (topological) generators, each arising from the action of inertia in the context of G^{geom}.

When $K = k(t)$ for k *not* algebraically closed, Pink denotes the resulting group G_∞ as G^{arith}, and he describes how it fits into a short exact sequence

$$1 \longrightarrow G^{\mathrm{Pink}}_{r,s,\infty} \longrightarrow G^{\mathrm{arith}} \longrightarrow \mathrm{Gal}(\overline{k}/k)/N \longrightarrow 1,$$

for some normal subgroup N of $\mathrm{Gal}(\overline{k}/k)$ depending on r, s, and k.

1.4. **Our approach.** This paper is the first of a series of two papers in which we have two main goals. First, for each pair of integers $r > s \geq 0$, we construct subgroups $B_{r,s,\infty} \subseteq M_{r,s,\infty}$ of $\mathrm{Aut}(T_\infty)$, coinciding with Pink's group $G^{\mathrm{Pink}}_{r,s,\infty} \cong G^{\mathrm{geom}} \subseteq G^{\mathrm{arith}}$, and we show that the arboreal Galois group G_∞ is isomorphic to a subgroup of $M_{r,s,\infty}$. Our arguments apply over general fields with arbitrary base points, rather than restricting to the case $K = k(t)$ with base point t. Our approach to this problem is also more concrete than that of Pink; the groups $B_{r,s,\infty}$ and $M_{r,s,\infty}$ are defined not by generators but rather as the set of all $\sigma \in \mathrm{Aut}(T_\infty)$ satisfying certain parity conditions, which are also used to describe how elements of G_∞ act on the roots of unity contained in K_∞. One advantage of this approach is that it can allow us to describe the intersections $K_n \cap k(\mu_{2^\infty})$ with a great deal of precision (see Corollary 6.5).

Our second goal is to present and prove necessary and sufficient conditions for G_∞ to be the whole group $M_{r,s,\infty}$ (see Theorem 1.4). Our results generalize those of [ABC+22], which gives a similar description of $B_{2,0,\infty}$ and $M_{2,0,\infty}$. (This is the so-called Basilica map $f(z) = z^2 - 1$, for which $r = 2$ and $s = 0$, i.e., the critical point at 0 is periodic of period 2).

This paper handles the periodic case $s = 0$ for arbitrary $r \geq 1$, for which we denote the above groups simply as $M_{r,\infty}$ and $B_{r,\infty}$ (see Definition 1.3). We handle the strictly preperiodic cases $s > 0$ in a separate paper; nevertheless, even though additional technical complications arise in the strictly preperiodic cases, the main ideas for all of our constructions already arise in the periodic case considered here.

The next subsection is devoted to some further notation needed to state our main results.

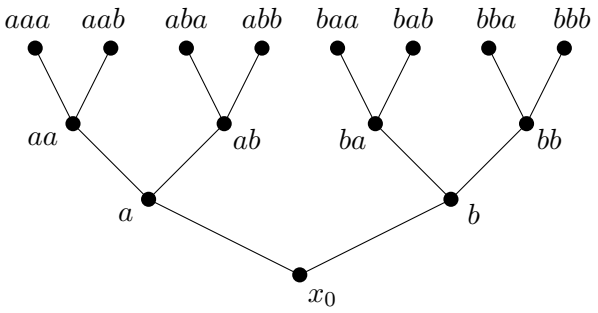

FIGURE 1. A labeling of T_3

1.5. **Some fundamentals.** It will be useful to assign labels to all of the nodes of the binary rooted trees T_n and T_∞, using the two symbols a, b to form words. That is, for each integer $m \geq 0$ and each node y at the m-th level of the tree, we assign y a *label* in the form of a word $w \in \{a,b\}^m$ of length m, in such a way that for every such m and y, the two nodes lying above y have labels $wa, wb \in \{a,b\}^{m+1}$. (Of course, in the tree T_n, this latter restriction is vacuous for nodes y in the top level $m = n$.) See Figure 1 for an example of a labeling of the tree T_3. Although the root node has the empty label (), we will often denote it as x_0.

We usually consider the nodes of T_∞ as corresponding to the backward orbit $\mathrm{Orb}_f^-(x_0) \in \overline{K}$ of $x_0 \in K$ under $f(z) = z^2 + c \in K[z]$. Thus, we will often conflate a point $y \in f^{-n}(x_0)$ with the corresponding node y of the tree. Having assigned a labeling to the tree, we will also sometimes conflate a node y with its label. On the other hand, when further clarity is needed for the backward orbit $\mathrm{Orb}_f^-(x_0) \in \overline{K}$, viewed as a tree of preimages, we will often write the value $y \in f^{-n}(x_0) \subseteq \overline{K}$ corresponding to the node with label $w \in \{a,b\}^n$ as $y = [w]$.

Having labeled the tree, any tree automorphism $\sigma \in \mathrm{Aut}(T_\infty)$ or $\sigma \in \mathrm{Aut}(T_n)$ must satisfy the following.

(1) For every level $m \geq 0$ (up to $m \leq n$ for T_n), σ permutes the labels in $\{a,b\}^m$, and
(2) For every level $m \geq 0$ (up to $m \leq n-1$ for T_n), for each word $s_1 \dots s_m \in \{a,b\}^m$, we have either

$$\sigma(s_1 \cdots s_m a) = \sigma(s_1 \cdots s_m)a \quad \text{and} \quad \sigma(s_1 \cdots s_m b) = \sigma(s_1 \cdots s_m)b$$

or

$$\sigma(s_1 \cdots s_m a) = \sigma(s_1 \cdots s_m)b \quad \text{and} \quad \sigma(s_1 \cdots s_m)b = \sigma(s_1 \cdots s_m)a.$$

For any tree automorphism σ and m-tuple $x \in \{a,b\}^m$, we define the *parity* $\mathrm{Par}(\sigma, x)$ of σ at x to be

$$\mathrm{Par}(\sigma, x) := \begin{cases} 0 & \text{if } \sigma(xa) = \sigma(x)a \text{ and } \sigma(xb) = \sigma(x)b \\ 1 & \text{if } \sigma(xa) = \sigma(x)b \text{ and } \sigma(xb) = \sigma(x)a \end{cases}.$$

Thus, any set of choices of $\mathrm{Par}(\sigma, x)$ for each node x of T_∞ (respectively, T_{n-1}) determines a unique automorphism $\sigma \in \mathrm{Aut}(T_\infty)$ (respectively, $\sigma \in \mathrm{Aut}(T_n)$).

Note that if $\sigma(x) = x$, then $\mathrm{Par}(\sigma, x)$ is 0 if σ fixes the two nodes above x, or 1 if it transposes them. However, $\mathrm{Par}(\sigma, x)$ is defined even if $\sigma(x) \neq x$, although in that case its value depends also on the labeling of the tree.

We also define $\mathrm{sgn}(\sigma, x) = (-1)^{\mathrm{Par}(\sigma,x)}$. We have the following elementary relations:

$$\mathrm{sgn}(\sigma\tau, x) = \mathrm{sgn}\big(\sigma, \tau(x)\big) \cdot \mathrm{sgn}(\tau, x), \tag{1}$$

and hence

$$\mathrm{Par}(\sigma\tau, x) = \mathrm{Par}\big(\sigma, \tau(x)\big) + \mathrm{sgn}\big(\sigma, \tau(x)\big)\,\mathrm{Par}(\tau, x). \tag{2}$$

Equation (2) follows from equation (1) by writing $\mathrm{Par}(\cdot,\cdot) = (1 - \mathrm{sgn}(\cdot,\cdot))/2$, or simply by checking the four possible choices of $\mathrm{Par}(\tau, x)$ and $\mathrm{Par}(\sigma, \tau(x))$.

Definition 1.1. For each $i \geq 1$, define $W(r,i)$ to be the following set of words of length $ri-1$:

$$W(r,i) = \big\{ s_1 s_2 \cdots s_{ri-1} \,:\, s_j \in \{a,b\},\ \text{with } s_j = a \text{ if } r|j \big\}.$$

Definition 1.2. Fix a labeling of T_∞, and let $\sigma \in \mathrm{Aut}(T_\infty)$. For any word x in the symbols $\{a,b\}$, define

$$Q_r(\sigma, x) := \sum_{i \geq 1} 2^i \sum_{w \in W(r,i)} \mathrm{Par}(\sigma, xw) \in 2\mathbb{Z}_2, \tag{3}$$

and

$$P_r(\sigma, x) := (-1)^{\mathrm{Par}(\sigma,x)} + Q_r(\sigma, xb) - Q_r(\sigma, xa) \in \mathbb{Z}_2^\times. \tag{4}$$

Thus, $P_r(\sigma,x)$ is ± 1 plus a weighted sum of $\mathrm{Par}(\sigma, y)$ at certain nodes y. Specifically, the sum counts half the nodes r levels above x, each with weight ± 2; a quarter of the nodes $2r$ levels above x, each with weight ± 4, an eighth of the nodes $4r$ levels above x, each with weight ± 8; and so on. (The $+$ weights are for nodes above xb, and the $-$ weights are for nodes above xa.)

Definition 1.3. Fix a labeling a, b of T_∞. Define $M_{r,\infty}$ to be the subset of $\mathrm{Aut}(T_\infty)$ for which

$$P_r(\sigma, x_1) = P_r(\sigma, x_2) \quad \text{for all nodes } x_1, x_2 \text{ of } T_\infty. \tag{5}$$

For $\sigma \in M_{r,\infty}$, define $P_r(\sigma)$ to be this common value of $P_r(\sigma, \cdot)$. Define

$$B_{r,\infty} := \{\sigma \in M_{r,\infty} : P_r(\sigma) = 1\}.$$

The map P_r from $M_{r,\infty}$ to $\mathbb{Z}_2^\times$ is connected closely to the 2-adic cyclotomic character, as we shall see in Theorem 5.1.

As a final item of notation before stating our main result (Theorem 1.4 in Subsection 1.6), for $0 \leq m \leq n \leq \infty$, it will be convenient to define homomorphisms

$$\mathrm{Res}_{n,m} : \mathrm{Aut}(T_n) \to \mathrm{Aut}(T_m)$$

given by restricting elements of $\mathrm{Aut}(T_n)$ to the m-th level of the tree. In particular, for each integer $n \geq 1$, we may define $B_{r,n} := \mathrm{Res}_{\infty,n}(B_{r,\infty})$ and $M_{r,n} := \mathrm{Res}_{\infty,n}(M_{r,\infty})$.

1.6. **Statement of our main result.**

Theorem 1.4. *Let k be a field of characteristic not equal to 2, and let $f(z) = z^2 + c \in k[z]$ with $f^r(0) = 0$ for some minimal integer $r \geq 1$. Let $x_0 \in k$, and define $K_{x_0,n} = k(f^{-n}(x_0))$, $K_{x_0,\infty} = \bigcup_{n=1}^\infty K_{x_0,n}$, $G_{x_0,n} = \mathrm{Gal}(K_{x_0,n}/k)$, and $G_{x_0,\infty} = \mathrm{Gal}(K_{x_0,\infty}/k)$. Further define $D_1, \ldots, D_r \in k$ by*

$$D_i := \begin{cases} x_0 - c & \text{if } i = 1, \\ f^i(0) - x_0 & \text{if } i \geq 2. \end{cases}$$

Then the following are equivalent.

(1) $[k(\zeta_8, \sqrt{D_1}, \ldots, \sqrt{D_r}) : k] = 2^{r+2}$
(2) $[K_{x_0,2r+1} : k] = |M_{r,2r+1}|$.
(3) $G_{x_0,2r+1} \cong M_{r,2r+1}$.
(4) $G_{x_0,n} \cong M_{r,n}$ *for all* $n \geq 1$.
(5) $G_{x_0,\infty} \cong M_{r,\infty}$.

Remark 1.5. When k contains i, the conditions of Theorem 1.4 can never hold, as condition (1) necessarily fails. However, our methods can still be used to prove a slightly more complicated result involving an appropriate subgroup of $M_{r,\infty}$. Specifically, this subgroup is the inverse image under P_r of the image in $\mathbb{Z}_2^\times$ of the 2-adic cyclotomic character of $\mathrm{Gal}(\bar{k}/k)$.

1.7. **Outline of the paper.** Section 2 concerns a useful elementary result for general quadratic polynomials that underlies many of our subsequent arguments. In Section 3 we present explicit formulas yielding 2-power roots of unity as arithmetic combinations of preimages of an arbitrary root point under our quadratic polynomial $f(z) = z^2 + c$ when the critical point is periodic. Section 4 is devoted to proving that $M_{r,\infty}$ is a subgroup of $\mathrm{Aut}(T_\infty)$ and that $B_{r,\infty}$ is simply the kernel of P_r (this is done in Theorem 4.1), while Section 5 shows how $M_{r,\infty}$ and $B_{r,\infty}$ realize the arboreal Galois action. In Section 6, we prove that our group $B_{r,\infty}$ concides with Pink's group G^{geom}, and that Pink's larger group G^{arith} is contained in our $M_{r,\infty}$. Finally, in Section 7, we prove Theorem 1.4, giving necessary and sufficient conditions for the Galois group G_∞ to be the full group $M_{r,\infty} = G^{\mathrm{arith}}$.

2. An elementary lemma

The following result provides a simple but essential algebraic relationship among elements of a backward orbit under a polynomial of the form $f(z) = z^2 + c$. We have stated it with the language of multiplicity, but in practice we will only apply it to backward orbits with no critical points, for which the relevant equation $f^m(z) = y$ has no repeated roots. Note that in this lemma, we do not make any assumptions about the polynomial $f(z)$ beyond the fact that it is of the form $z^2 + c$, whereas in later sections, we will almost always work exclusively with quadratic polynomials satisfying $f^r(0) = 0$ for some $r \geq 1$.

Proposition 2.1. *Let K be a field of characteristic not equal to 2. Let $c \in K$, define $f(z) = z^2 + c$, let $y \in \overline{K}$, and let $m \geq 1$. Choose $\alpha_1, \ldots, \alpha_{2^{(m-1)}} \in f^{-m}(y)$ so that the roots of $f^m(z) = y$, repeated according to multiplicity, are precisely*

$$\pm\alpha_1, \ldots, \pm\alpha_{2^{(m-1)}}. \tag{6}$$

Then

$$\left(\alpha_1\alpha_2\cdots\alpha_{2^{(m-1)}}\right)^2 = \begin{cases} f^m(0) - y & \text{if } m \geq 2, \\ y - f(0) & \text{if } m = 1. \end{cases}$$

Proof. We may write $f^m(z) - y = g(z^2)$, where $g \in \overline{K}[z]$ is a polynomial of degree 2^{m-1}. Thus, the roots of $f^m(z) - y$ come in plus/minus pairs, justifying the description of the roots in equation (6). Moreover, the roots of g are precisely $\alpha_1^2, \ldots, \alpha_{2^{m-1}}^2$, so that the constant term of g is

$$(\pm 1)^{\deg(g)}(\alpha_1\cdots\alpha_{2^{m-1}})^2. \tag{7}$$

Since $\deg(g) = 2^{m-1}$, we have a $-$ sign in equation (7) if $m = 1$, and a $+$ sign if $m \geq 2$. On the other hand, by definition of g, the constant term of g is $f^m(0) - y$, and the desired conclusion is immediate. □

3. Roots of unity arising in backward orbits

Throughout the rest of the paper we assume $f(z) = z^2 + c$ with $f^r(0) = 0$ for some minimal integer $r \geq 1$.

Lemma 3.1. *Let $x \in \overline{K}$ not in the forward orbit of 0, and let $\pm y$ be its two immediate preimages under f. Let $A_1 = \{y\}$ and $B_1 = \{-y\}$. For each $n \geq 2$, let A_n be a subset of $f^{-r}(A_{n-1})$ such that A_n contains exactly half of the elements of $f^{-r}(A_{n-1})$ and $f^{-r}(A_{n-1}) = \{\pm\alpha : \alpha \in A_n\}$. Similarly, let B_n be a subset of $f^{-r}(B_{n-1})$ containing exactly half of the elements of $f^{-r}(B_{n-1})$ such that $f^{-r}(B_{n-1}) = \{\pm\beta : \beta \in B_n\}$. Then*

$$\gamma_n := \frac{\prod_{\alpha\in A_n}\alpha}{\prod_{\beta\in B_n}\beta}$$

is a primitive 2^n-th root of unity.

Proof. Let $x \in \overline{K}$ not in the forward orbit of 0 and consider its two immediate preimages $\pm y$. First note

$$\gamma_1 = \frac{y}{-y} = -1,$$

so the result holds in this case. Then by Proposition 2.1 and the fact that $f^r(0) = 0$, we have

$$\gamma_2^2 = \frac{\left(\prod_{\alpha \in A_2} \alpha\right)^2}{\left(\prod_{\alpha \in B_2} \beta\right)^2} = \frac{(-1)^{2^{r-1}}(-y)}{(-1)^{2^{r-1}} y} = -1,$$

so that γ_2 is a primitive fourth root of unity.

More generally, suppose γ_{n-1} is a primitive 2^{n-1} root of unity for $n \geq 2$. For any $\alpha' \in A_{n-1}$, we have $f^{-r}(\alpha') = \{\pm\alpha : \alpha \in f^{-r}(\alpha') \cap A_n\}$. Hence

$$\begin{aligned}\gamma_n^2 &= \frac{\left(\prod_{\alpha \in A_n} \alpha\right)^2}{\left(\prod_{\beta \in B_n} \beta\right)^2} = \frac{\prod_{\alpha' \in A_{n-1}} \left(\prod_{\alpha \in A_n \cap f^{-r}(\alpha')} \alpha\right)^2}{\prod_{\beta' \in B_{n-1}} \left(\prod_{\beta \in B_n \cap f^{-r}(\beta')} \beta\right)^2} \\ &= \frac{\prod_{\alpha' \in A_{n-1}} (-1)^{2^{r-1}}(-\alpha')}{\prod_{\beta' \in B_{n-1}} (-1)^{2^{r-1}}(-\beta')} = \frac{\prod_{\alpha' \in A_{n-1}} \alpha'}{\prod_{\beta' \in B_{n-1}} \beta'} = \gamma_{n-1},\end{aligned}$$

where the third equality follows from Proposition 2.1. Hence γ_n is a primitive 2^n-th root of unity. □

In the statement of our next result, recall Definition 1.1 of the set of words $W(r,i)$ of length $ri-1$ satisfying a certain restriction.

Lemma 3.2. *Let $x_0 \in K$ not in the forward orbit of 0, and choose a sequence of primitive 2^n-th roots of unity $\zeta_2, \zeta_4, \zeta_8, \ldots$ such that $\zeta_2 = -1$ and $\zeta_{2^n}^2 = \zeta_{2^{n-1}}$. It is possible to label the tree T_∞ of preimages $\mathrm{Orb}_f^-(x_0)$ in a way such that for every node x of the tree and every integer $i \geq 1$, we have*

$$\frac{\prod_{w \in W(r,i)} [xawa]}{\prod_{w \in W(r,i)} [xbwa]} = \zeta_{2^{i+1}}. \tag{8}$$

Proof. We will label the tree inductively, starting from the root point x_0. Label the tree arbitrarily up to level $r+1$.

For each successive $n \geq r+1$, suppose that we have labeled T_{n-1} so that for every node x at every level $0 \leq \ell \leq n-r-2$ of T_{n-1}, equation (8) holds for each $1 \leq i \leq \lfloor (n-\ell-2)/r \rfloor$. (Note that $\lfloor (n-\ell-2)/r \rfloor$ is the maximum value of i so that the subtree of height $ri+1$ rooted at x is contained in T_{n-1}. In particular, our supposition is vacuous for $n \leq r+1$.) For each node y at level $n-1$, label the two points of $f^{-1}(y)$ arbitrarily as ya and yb. We will now adjust these labels that we have just applied at the n-th level of the tree.

Let $m := \lfloor (n-1)/r \rfloor \geq 1$, so that $n = rm + t$ with $1 \leq t \leq r$. Starting with $i = m$ (and counting down to $i = 1$), for each node x at level $n - (ri+1)$ of the tree, consider the ratio

$$\gamma := \frac{\prod_{w \in W(r,i)} [xawa]}{\prod_{w \in W(r,i)} [xbwa]}$$

of equation (8). Arguing as in the proof of Lemma 3.1, it follows from Proposition 2.1 that

$$\gamma^2 = \frac{\prod_{w \in W(r,i-1)} [xawa]}{\prod_{w \in W(r,i-1)} [xbwa]} \quad \text{if } i \geq 2, \quad \text{or} \quad \gamma^2 = \frac{[xa]}{[xb]} = -1 \quad \text{if } i = 1,$$

which is equal to $\zeta_{2^{i-1}}$ by our induction hypothesis when $i \geq 2$, and by definition of ζ_2 when $i = 1$. Thus, $\gamma = \pm\zeta_{2^i}$. If $\gamma = -\zeta_{2^i}$, exchange the labels of the two level-n nodes $xba^{ri-1}a$ and $xba^{ri-1}b$, where a^j denotes a string of j copies of the symbol a. Since these two nodes are negatives of each other, we now have $\gamma = \zeta_{2^i}$.

Repeat the process above for each x at level $n-(ri+1)$ of the tree for successively smaller $i = m-1, m-2, \ldots, 1$. Note that for any node x at level $n-(ri+1)$, the nodes $xba^{ri-1}a$ and $xba^{ri-1}b$ have a b appearing as the $(ri+1)^{\text{st}}$-to-last-symbol in their labels. On the other hand, for any $j > i$, by definition of $W(r,j)$, all of the nodes appearing in the analog of equation (8) for j in place of i (and a node at level $n-(rj+1)$ in place of x) have the symbol a in that position in their labels. Thus, exchanging the labels of the nodes $xba^{ri-1}a$ and $xba^{ri-1}b$ does not affect the truth of equation (8) for nodes addressed in previous steps. □

4. A preliminary result regarding the associated arboreal subgroup

We now prove that the sets $B_{r,\infty} \subseteq M_{r,\infty} \subseteq \mathrm{Aut}(T_\infty)$ of Definition 1.3 are in fact groups.

Theorem 4.1. *The following hold.*

(1) $M_{r,\infty}$ is a subgroup of $\mathrm{Aut}(T_\infty)$.
(2) The map $P_r : M_{r,\infty} \to \mathbb{Z}_2^\times$ given by $P_r : \sigma \mapsto P_r(\sigma)$ is a group homomorphism with kernel $B_{r,\infty}$.

Proof. **Step 1**. We begin with two simple observations that apply to any $\tau \in \mathrm{Aut}(T_\infty)$ and any node y of T_∞. First, we have $W(r,1) = \{a,b\}^{r-1}$ is the set of all 2^{r-1} words of length $r-1$ in $\{a,b\}$, and hence

$$\{\tau(y)w : w \in W(r,1)\} = \{\tau(yw) : w \in W(r,1)\} \tag{9}$$

are precisely the same set of 2^{r-1} nodes of T_∞. Second, we have

$$Q_r(\tau, y) = 2 \sum_{w \in W(r,1)} \big(\mathrm{Par}(\tau, yw) + Q_r(\tau, ywa)\big), \tag{10}$$

by definition of Q_r (see equation (3)), since for any $i \geq 2$, we have

$$W(r,i) = \{waw' : w \in W(r,1) \text{ and } w' \in W(r,i-1)\}.$$

Step 2. For any $\sigma \in M_{r,\infty}$, any $\tau \in \mathrm{Aut}(T_\infty)$, and any node x of T_∞, define

$$Z_r(\sigma,\tau,x) := Q_r(\sigma,\tau(x)) + P_r(\sigma)Q_r(\tau,x) - Q_r(\sigma\tau,x) \in \mathbb{Z}_2.$$

In Step 3 we will show that Z_r is identically zero, but in this step we claim only that

$$Z_r(\sigma,\tau,x) = 2 \sum_{w \in W(r,1)} Z_r(\sigma,\tau,xwa). \tag{11}$$

To prove the claim of equation (11), expand each appearance of Q_r in the definition of Z_r according to equation (10), to obtain

$$\begin{aligned} Z_r(\sigma,\tau,x) = 2 \sum_{w \in W(r,1)} \Big[&\mathrm{Par}(\sigma,\tau(x)w) + P_r(\sigma)\,\mathrm{Par}(\tau,xw) - \mathrm{Par}(\sigma\tau,xw) \\ &+ Q_r(\sigma,\tau(x)wa) + P_r(\sigma)Q_r(\tau,xwa) - Q_r(\sigma\tau,xwa)\Big] \\ = 2 \sum_{w \in W(r,1)} \Big[&\mathrm{Par}(\sigma,\tau(xw)) + P_r(\sigma)\,\mathrm{Par}(\tau,xw) - \mathrm{Par}(\sigma\tau,xw) \\ &+ Q_r(\sigma,\tau(xw)a) + P_r(\sigma)Q_r(\tau,xwa) - Q_r(\sigma\tau,xwa)\Big] \end{aligned}$$

by applying observation (9) in the second equality. Expanding the first appearance of $P_r(\sigma)$ here as $P_r(\sigma, \tau(xw))$, we have

$$\begin{aligned} Z_r(\sigma,\tau,x) &= 2\sum_{w\in W(r,1)} \Big[\operatorname{Par}(\sigma,\tau(xw)) + (-1)^{\operatorname{Par}(\sigma,\tau(xw))} \operatorname{Par}(\tau,xw) - \operatorname{Par}(\sigma\tau,xw) \\ &\qquad + \operatorname{Par}(\tau,xw)\big(Q_r(\sigma,\tau(xw)b) - Q_r(\sigma,\tau(xw)a)\big) \\ &\qquad + Q_r(\sigma,\tau(xw)a) + P_r(\sigma)Q_r(\tau,xwa) - Q_r(\sigma\tau,xwa)\Big] \\ &= 2\sum_{w\in W(r,1)} \tilde{Z}_r(\sigma,\tau,x,w) \end{aligned}$$

where, after applying equation (2) to $\operatorname{Par}(\sigma\tau, xw)$, we define

$$\begin{aligned} \tilde{Z}_r(\sigma,\tau,x,w) &:= \operatorname{Par}(\tau,xw)\big(Q_r(\sigma,\tau(xw)b) - Q_r(\sigma,\tau(xw)a)\big) \\ &\qquad + Q_r(\sigma,\tau(xw)a) + P_r(\sigma)Q_r(\tau,xwa) - Q_r(\sigma\tau,xwa). \end{aligned}$$

For each $w \in W(r,1)$, we consider two cases. If $\operatorname{Par}(\tau,xw) = 0$, then $\tau(xw)a = \tau(xwa)$, so

$$\tilde{Z}_r(\sigma,\tau,x,w) = 0 + Q_r(\sigma,\tau(xwa)) + P_r(\sigma)Q_r(\tau,xwa) - Q_r(\sigma\tau,xwa) = Z(\sigma,\tau,xwa).$$

On the other hand, if $\operatorname{Par}(\tau,xw) = 1$, then $\tau(xw)b = \tau(xwa)$, so

$$\begin{aligned} \tilde{Z}_r(\sigma,\tau,x,w) &= Q_r(\sigma,\tau(xwa)) - Q_r(\sigma,\tau(xw)a) \\ &\qquad + Q_r(\sigma,\tau(xw)a) + P_r(\sigma)Q_r(\tau,xwa) - Q_r(\sigma\tau,xwa) \\ &= Q_r(\sigma,\tau(xwa)) + P_r(\sigma)Q_r(\tau,xwa) - Q_r(\sigma\tau,xwa) = Z(\sigma,\tau,xwa). \end{aligned}$$

That is, in all cases, we have $\tilde{Z}_r(\sigma,\tau,x,w) = Z(\sigma,\tau,xwa)$. Hence,

$$Z_r(\sigma,\tau,x) = 2\sum_{w\in W(r,1)} \tilde{Z}_r(\sigma,\tau,x,w) = 2\sum_{w\in W(r,1)} Z_r(\sigma,\tau,xwa),$$

proving the claim of equation (11).

Step 3. For σ, τ, x as in Step 2, a straightforward induction on $i \geq 0$ gives

$$Z_r(\sigma,\tau,x) = 2^i \sum_{w\in W(r,i)} Z_r(\sigma,\tau,xwa) \in 2^i\mathbb{Z}_2 \quad \text{for every } i \geq 0.$$

Because $\bigcap_{i\geq 0} 2^i\mathbb{Z}_2 = \{0\}$, it follows that $Z_r(\sigma,\tau,x) = 0$.

Expanding $P_r(\tau,x)$ according to definition (4), we have

$$\begin{aligned} P_r(\sigma)P_r(\tau,x) &= (-1)^{\operatorname{Par}(\tau,x)}P_r(\sigma) + P_r(\sigma)Q_r(\tau,xb) - P_r(\sigma)Q_r(\tau,xa) \\ &= (-1)^{\operatorname{Par}(\tau,x)}\big((-1)^{\operatorname{Par}(\sigma,\tau(x))} + Q_r(\sigma,\tau(x)b) - Q_r(\sigma,\tau(x)a)\big) \\ &\quad + P_r(\sigma)Q_r(\tau,xb) - P_r(\sigma)Q_r(\tau,xa) \\ &= (-1)^{\operatorname{Par}(\sigma\tau,x)} + Q_r(\sigma,\tau(xb)) - Q_r(\sigma,\tau(xa)) \\ &\quad + P_r(\sigma)Q_r(\tau,xb) - P_r(\sigma)Q_r(\tau,xa), \end{aligned}$$

where in the second equality, we expanded the first appearance of $P_r(\sigma)$ as $P_r(\sigma,\tau(x))$, and in the third equality, we applied both equation (2) and the fact that

$$(-1)^{\operatorname{Par}(\tau,x)}\big(Q_r(\sigma,\tau(x)b) - Q_r(\sigma,\tau(x)a)\big) = Q_r(\sigma,\tau(xb)) - Q_r(\sigma,\tau(xa)).$$

Therefore, we have

$$\begin{aligned} P_r(\sigma)P_r(\tau,x) &= (-1)^{\operatorname{Par}(\sigma\tau,x)} + Q(\sigma\tau,xb) - Q(\sigma\tau,xa) + Z_r(\sigma,\tau,xb) - Z_r(\sigma,\tau,xa) \\ &= P_r(\sigma\tau,x) + 0 - 0 = P_r(\sigma\tau,x). \end{aligned}$$

by definition of P_r and the fact that $Z_r = 0$.

Step 4. We now show that $M_{r,\infty}$ is a subgroup of $\mathrm{Aut}(T_\infty)$. The identity $e \in \mathrm{Aut}(T_\infty)$ clearly satisfies $Q_r(e,x) = 0$ and $\mathrm{Par}(e,x) = 0$ for all nodes x, whence $P(e,x) = 1$, so that $e \in M_{r,\infty}$. Given $\sigma, \tau \in M_{r,\infty}$ and $x_1, x_2 \in X$, we have

$$P_r(\sigma\tau, x_1) = P_r(\sigma)P_r(\tau, x_1) = P_r(\sigma)P_r(\tau, x_2) = P_r(\sigma\tau, x_2),$$

where the first and third equalities are by Step 3, and the second is by the fact that $\tau \in M_{r,\infty}$. Thus, $\sigma\tau \in M_{r,\infty}$. Applying Step 3 with σ^{-1} in the role of τ, we also have

$$\begin{aligned} P_r(\sigma)P_r(\sigma^{-1}, x_1) &= P_r(\sigma\sigma^{-1}, x_1) = P_r(e, x_1) = P_r(e, x_2) \\ &= P_r(\sigma\sigma^{-1}, x_2) = P_r(\sigma)P(\sigma^{-1}, x_2). \end{aligned}$$

Multiplying both sides on the left by $P_r(\sigma)^{-1} \in \mathbb{Z}_2^\times$, it follows that

$$P_r(\sigma^{-1}, x_1) = P_r(\sigma^{-1}, x_2),$$

proving that $\sigma^{-1} \in M_{r,\infty}$. Thus, $M_{r,\infty}$ is a subgroup of $\mathrm{Aut}(T_\infty)$.

Finally, the map P_r is a homomorphism by Step 3, and its kernel is clearly $B_{r,\infty}$. □

5. The action of Galois on roots of unity

The following result shows that the group $M_{r,\infty}$ is determined solely by the restriction that a Galois element σ must act consistently on every instance of any root of unity ζ_{2^n}.

Theorem 5.1. *Let $x_0 \in K$ not in the forward orbit of 0, and choose primitive 2^n-th roots of unity $\zeta_2, \zeta_4, \zeta_8, \cdots \in \overline{K}$ such that $\zeta_{2^n}^2 = \zeta_{2^{n-1}}$. Label the tree T_∞ of preimages in $\mathrm{Orb}_f^-(x_0)$ as in Lemma 3.2. Then for any node $x \in \mathrm{Orb}_f^-(x_0)$ and any $\sigma \in G_\infty = \mathrm{Gal}(K_\infty/K)$, we have*

$$\sigma(\zeta_{2^n}) = \zeta_{2^n}^{P_r(\sigma,x)}, \tag{12}$$

for all $n \geq 1$. In particular, the image of G_∞ in $\mathrm{Aut}(T_\infty)$, induced by its action on $\mathrm{Orb}_f^-(x_0)$ via this labeling, is contained in $M_{r,\infty}$. Furthermore, if $\zeta_{2^n} \in K$ for all n, then this Galois image is contained in $B_{r,\infty}$.

Proof. If equation (12) holds for $\sigma \in G_\infty$ for every node $x \in \mathrm{Orb}_f^-(x_0)$, and for all $n \geq 1$, then $\sigma(\zeta_{2^n}) = \zeta_{2^n}^{P_r(\sigma,x)} = \zeta_{2^n}^{P_r(\sigma,x_0)}$ for all $n \geq 1$. It follows that $P_r(\sigma, x) \equiv P_r(\sigma, x_0) \mod 2^n$ for all $n \geq 1$ and hence $\sigma \in M_{r,\infty}$. Further, if $\zeta_{2^n} \in K$ for all n, we must have $\sigma(\zeta_{2^n}) = \zeta_{2^n}^{P_r(\sigma,x)} = \zeta_{2^n}$ for all n, hence $P_r(\sigma, x) = 1$ and $\sigma \in B_{r,\infty}$.

Thus, it suffices to show equation (12) holds for an arbitrary $\sigma \in G_\infty$, arbitrary $x \in \mathrm{Orb}_f^-(x_0)$, and arbitrary $n \geq 1$. The desired equation is trivially true for $n = 1$, as $\zeta_2 = -1$ and $P_r \equiv 1 \pmod 2$. Therefore, we may assume for the rest of the proof that $n \geq 2$. By Lemma 3.2, we can write

$$\zeta_{2^n} = \frac{\prod_{w \in W(r,n-1)} [xawa]}{\prod_{w \in W(r,n-1)} [xbwa]},$$

and hence

$$\sigma(\zeta_{2^n}) = \frac{\prod_{w \in W(r,n-1)} [\sigma(xawa)]}{\prod_{w \in W(r,n-1)} [\sigma(xbwa)]}. \tag{13}$$

We first claim for all $i \geq 0$ and any finite word w (in the alphabet $\{a, b\}$), we have

$$\prod_{w' \in W(r,i)} [\sigma(wa)w'a] = \zeta_{2^{i+1}}^{-\mathrm{Par}(\sigma,w)} \prod_{w' \in W(r,i)} [\sigma(w)aw'a], \tag{14}$$

where for $i = 0$, we interpret this equation as saying $\sigma(wa) = \zeta_2^{-\operatorname{Par}(\sigma,w)}\sigma(w)a$. When $\operatorname{Par}(\sigma, w) = 1$, we have $\sigma(wa) = \sigma(w)b$, so equation (14) follows from Lemma 3.2 applied to $\sigma(w)$. On the other hand, when $\operatorname{Par}(\sigma, w) = 0$, we have $\sigma(wa) = \sigma(w)a$ and hence the set of words in product on the left of the equation is the same as that on the right hand side, so equation (14) is vacuously true in this case.

We also observe for any words w, w',

$$\prod_{w''\in\{a,b\}^{r-1}} [\sigma(ww'')w'] = \prod_{w''\in\{a,b\}^{r-1}} [\sigma(w)w''w'], \tag{15}$$

since the set of words in each product is the same.

Write $S_i := \sum_{w\in W(r,i)} \operatorname{Par}(\sigma, xaw)$. Note, any $w \in W_{(r,j)}$ can be written as $w_1aw_2a\dots w_j$ for $w_1, \dots, w_j \in \{a, b\}^{r-1}$. Then alternately applying equation (14) and equation (15), we have

$$\begin{aligned}
\prod_{w\in W(r,n-1)} [\sigma(xawa)] &= \prod_{w_1,\dots,w_{n-1}\in\{a,b\}} [\sigma(xaw_1aw_2a\dots w_{n-1}a)] \\
&= \zeta_2^{-S_{n-1}} \prod_{w_1,\dots,w_{n-1}\in\{a,b\}^{r-1}} [\sigma(xaw_1a\dots w_{n-1})a] \\
&= \zeta_2^{-S_{n-1}} \prod_{w_1,\dots,w_{n-1}\in\{a,b\}^{r-1}} [\sigma(xaw_1a\dots w_{n-2}a)w_{n-1}a] \\
&= \zeta_2^{-S_{n-1}}\zeta_{2^2}^{-S_{n-2}} \prod_{w_1,\dots,w_{n-1}\in\{a,b\}^{r-1}} [\sigma(xaw_1a\dots w_{n-2})aw_{n-1}a] \\
&\ \ \vdots \\
&= \zeta_2^{-S_{n-1}}\zeta_{2^2}^{-S_{n-2}}\dots\zeta_{2^{n-1}}^{-S_1} \prod_{w_1,\dots,w_{n-1}\in\{a,b\}^{r-1}} [\sigma(xaw_1)aw_2a\dots w_{n-1}a] \\
&= \zeta_2^{-S_{n-1}}\zeta_{2^2}^{-S_{n-2}}\dots\zeta_{2^{n-1}}^{-S_1} \prod_{w_1,\dots,w_{n-1}\in\{a,b\}^{r-1}} [\sigma(xa)w_1aw_2a\dots w_{n-1}a]
\end{aligned}$$

Using the fact that $\zeta_{2^{n-i}} = (\zeta_{2^n})^{2^i}$, we can rewrite

$$\zeta_2^{-S_{n-1}}\zeta_{2^2}^{-S_{n-2}}\dots\zeta_{2^{n-1}}^{-S_1} = \zeta_{2^n}^{-(2S_1+4S_2+\dots+2^{n-1}S_{n-1})} = \zeta_{2^n}^{-Q_r(\sigma,xa)},$$

where the last equation follows from the identity $\sum_{i=1}^{n-1} 2^iS_i \equiv Q_r(\sigma, xa) \pmod{2^n}$. Thus, we have

$$\prod_{w\in W(r,n-1)} [\sigma(xawa)] = \zeta_{2^n}^{-Q_r(\sigma,xa)} \prod_{w\in W(r,n-1)} [\sigma(xa)wa]. \tag{16}$$

Similarly,

$$\prod_{w\in W(r,n-1)} [\sigma(xbwa)] = \zeta_{2^n}^{-Q_r(\sigma,xb)} \prod_{w\in W(r,n-1)} [\sigma(xb)wa]. \tag{17}$$

Plugging equation (16) and equation (17) into equation (13), we see

$$\sigma(\zeta_{2^n}) = \zeta_{2^n}^{-Q_r(\sigma,xa)+Q_r(\sigma,xb)} \frac{\prod_{w\in W(r,n-1)}[\sigma(xa)wa]}{\prod_{w\in W(r,n-1)}[\sigma(xb)wa]}.$$

Finally, applying Lemma 3.2 one last time, we see

$$\frac{\prod_{w\in W(r,n-1)}[\sigma(xa)wa]}{\prod_{w\in W(r,n-1)}[\sigma(xb)wa]} = \left(\frac{\prod_{w\in W(r,n-1)}[\sigma(x)awa]}{\prod_{w\in W(r,n-1)}[\sigma(x)bwa]}\right)^{(-1)^{\mathrm{Par}(\sigma,x)}} = \zeta_{2^n}^{(-1)^{\mathrm{Par}(\sigma,x)}}.$$

Thus,

$$\sigma(\zeta_{2^n}) = \zeta_{2^n}^{(-1)^{\mathrm{Par}(\sigma,x)}-Q_r(\sigma,xa)+Q_r(\sigma,xb)} = \zeta_{2^n}^{P_r(\sigma,x)}. \qquad \square$$

6. The arithmetic and geometric Galois groups

Let k be an arbitrary field not of characteristic 2. In this section, let $K = k(t)$ where t is transcendental over k, let $x_0 = t$, let K_∞ be the resulting arboreal extension of K, and $G_\infty = \mathrm{Gal}(K_\infty/K)$, the corresponding arboreal Galois group. In addition, let $\overline{k}$ be an algebraic closure of k, let $K' := \overline{k}(t)$, let K'_∞ be the corresponding arboreal extension of K' (with root point $x_0 = t$), and let $G'_\infty := \mathrm{Gal}(K'_\infty/K')$ be the corresponding arboreal Galois group for this extension. The groups G_∞ and G'_∞ are called the *arithmetic* and *geometric* arboreal Galois groups for f over k, and they are denoted G^{arith} and G^{geom} respectively.

Note that $K' = k(t)\cdot\bar{k}$ and $K'_\infty = K_\infty\cdot\bar{k}$. Hence, if we define $k_\infty := K_\infty \cap \bar{k}$, then the map $G^{\mathrm{geom}} \to \mathrm{Gal}(K_\infty/k_\infty(t))$ given by restricting elements to K_∞ is an isomorphism. Composing this isomorphism with the injection $\mathrm{Gal}(K_\infty/k_\infty(t)) \to G^{\mathrm{arith}}$ produces a natural injection $G^{\mathrm{geom}} \to G^{\mathrm{arith}}$ with cokernel isomorphic to $\mathrm{Gal}(k_\infty/k)$. That is, we have an exact sequence

$$0 \longrightarrow G^{\mathrm{geom}} \longrightarrow G^{\mathrm{arith}} \longrightarrow \mathrm{Gal}(k_\infty/k) \longrightarrow 0.$$

6.1. **The geometric Galois group.** In this subsection, we show that for each $r \geq 1$, our group $B_{r,\infty}$ coincides with Pink's group $G^{\mathrm{Pink}}_{r,\infty}$. Recall that in [Pin13], Pink proves that this group (which he denotes simply as G) is isomorphic to G^{geom}, for any field k as above.

In [Pin13, Equation (2.0.1)], Pink describes $G^{\mathrm{Pink}}_{r,\infty}$ as the closure of the subgroup of $\mathrm{Aut}(T_\infty)$ generated by elements $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_r \in \mathrm{Aut}(T_\infty)$ given by the recursive relations

$$\boldsymbol{\alpha}_1 = (\boldsymbol{\alpha}_r, 1)\boldsymbol{\tau}, \qquad \text{and} \qquad \boldsymbol{\alpha}_i = (\boldsymbol{\alpha}_{i-1}, 1) \quad \text{for } 2 \leq i \leq r. \tag{18}$$

Here, $\boldsymbol{\tau} \in \mathrm{Aut}(T_\infty)$ denotes the automorphism of order two swapping the subtrees based at a and b, given by

$$\boldsymbol{\tau}(aw) = bw \quad \text{and} \quad \boldsymbol{\tau}(bw) = aw$$

for all infinite words $w \in \{a,b\}^{\mathbb{N}}$. In addition, for any $\sigma_a, \sigma_b \in \mathrm{Aut}(T_\infty)$, the automorphism (σ_a, σ_b) is the element $\sigma \in \mathrm{Aut}(T_\infty)$ given by

$$\sigma(aw) = a\sigma_a(w) \quad \text{and} \quad \sigma(bw) = b\sigma_b(w).$$

Let w_r be the word of length r given by $w_r := ba^{r-1}$, where a^n denotes n copies of the symbol a. A straightforward induction shows that for each $i = 1, \ldots, r$, the automorphism $\boldsymbol{\alpha}_i$ of equation (18) is given by

$$\mathrm{Par}(\boldsymbol{\alpha}_i, w) = \begin{cases} 1 & \text{if } w = a^{i-1}w_r^n \text{ for some } n \geq 0, \\ 0 & \text{otherwise,} \end{cases} \tag{19}$$

for any word w, where w_r^n is the word $w_r \cdots w_r$ of length nr consisting of n copies of w_r. For example, for $r = 3$ and $i = 2$, we have $\mathrm{Par}(\boldsymbol{\alpha}_2, w) = 1$ for

$$w = a,\ abaa,\ abaabaa,\ abaabaabaa, \ldots$$

and $\mathrm{Par}(\boldsymbol{\alpha}_2, w) = 0$ otherwise.

Proposition 6.1. *For every integer $r \geq 1$, Pink's subgroup $G^{\mathrm{Pink}}_{r,\infty}$ is contained in $B_{r,\infty}$.*

Proof. Observe that for any node x of the tree, the map $\sigma \mapsto P_r(\sigma, x)$ is a continuous function from $\mathrm{Aut}(T_\infty)$ to $\mathbb{Z}_2^\times$. Indeed, if $\sigma_1, \sigma_2 \in \mathrm{Aut}(T_\infty)$ agree on the finite subtree extending nr levels above x, then $P_r(\sigma_1, x) \equiv P_r(\sigma_2, x) \pmod{2^{n+1}}$. It follows that $M_{r,\infty}$ and $B_{r,\infty}$ are closed subgroups of $\mathrm{Aut}(T_\infty)$. Thus, it suffices to prove that each of the generators $\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_r$ of Pink's group belongs to $B_{r,\infty}$.

Fix a node x of the tree, and an integer $i \in \{1, \dots, r\}$. We must show that $P_r(\boldsymbol{\alpha}_i, x) = 1$. We consider two cases.

First, suppose that $\mathrm{Par}(\boldsymbol{\alpha}_i, x) = 1$. By equation (19), we must have $x = a^{i-1} w_r^m$ for some integer $m \geq 0$. Thus, the nodes y above x for which $\mathrm{Par}(\boldsymbol{\alpha}_i, y) = 1$ are those of the form $y = x w_r^n$ for some $n \geq 0$. On the other hand, according to Definition 1.2, the value of $P_r(\boldsymbol{\alpha}_i, x)$ is $(-1)^{\mathrm{Par}(\boldsymbol{\alpha}_i, x)} = -1$ plus a weighted sum of $\mathrm{Par}(\boldsymbol{\alpha}_i, y')$ for nodes y' of the form $y' = xaw$ or $y' = xbw$ for $w \in W(r, j)$ with $j \geq 1$. However, none of the strings w_r^n begin with a, and all the ones with $n \geq 2$ have length greater than r, with b rather than a as their $(r+1)$-st symbol. Thus, the only string of the form w_r^n in the sets $aW(r, j)$ or $bW(r, j)$ is $w_r = ba^{r-1}$ itself. Therefore,

$$P_r(\boldsymbol{\alpha}_i, x) = (-1)^{\mathrm{Par}(\boldsymbol{\alpha}_i, x)} + Q_r(\boldsymbol{\alpha}_i, xb) - Q_r(\boldsymbol{\alpha}_i, xa) = -1 + 2 - 0 = 1.$$

Second, we are left with the case that $\mathrm{Par}(\boldsymbol{\alpha}_i, x) = 0$. By equation (19), x is *not* of the form $a^{i-1} w_r^m$, and therefore none of the nodes at any level nr above x are of this form, either. Therefore, $\mathrm{Par}(\boldsymbol{\alpha}_i, y) = 0$ for all nodes y appearing in the formula for $P_r(\boldsymbol{\alpha}_i, x)$ in Definition 1.2, and hence

$$P_r(\boldsymbol{\alpha}_i, x) = (-1)^{\mathrm{Par}(\boldsymbol{\alpha}_i, x)} + Q_r(\boldsymbol{\alpha}_i, xb) - Q_r(\boldsymbol{\alpha}_i, xa) = 1 + 0 - 0 = 1. \qquad \square$$

In fact, we wish to extend Proposition 6.1 to show that $G_{r,\infty}^{\mathrm{Pink}} = B_{r,\infty}$. To this end, for each integer $n \geq 1$, define

$$B_{r,n} := \mathrm{Res}_{\infty,n}(B_{r,\infty}) \quad \text{and} \quad G_{r,n}^{\mathrm{Pink}} := \mathrm{Res}_{\infty,n}(G_{r,\infty}^{\mathrm{Pink}}),$$

as we did at the end of Subsection 1.5. We must show these subgroups of $\mathrm{Aut}(T_n)$ coincide.

Theorem 6.2. *For every integer $r \geq 1$, we have $G_{r,\infty}^{\mathrm{Pink}} = B_{r,\infty}$.*

Proof. For each integer $n \geq 1$, define

$$B'_{r,n} := \left\{ \sigma \in \mathrm{Aut}(T_n) : \forall m < n \text{ and } \forall x \in \{a, b\}^m,\ P_r(\sigma, x) \equiv 1 \,(\mathrm{mod}\ 2^{e(m,n)}) \right\}$$

where $e(m, n) := \lfloor \frac{n-1-m}{r} \rfloor + 1$. (Here, working on the finite tree T_n, we understand the sum defining $P_r(\sigma, x)$ in Definition 1.3 to be truncated to include only those terms that make sense, i.e., only those $\mathrm{Par}(\sigma, y)$ terms for y at level $n-1$ or below.) Observe, in light of Proposition 6.1 and Definition 1.3, that we have

$$G_{r,n}^{\mathrm{Pink}} \subseteq B_{r,n} \subseteq B'_{r,n}.$$

Thus, it suffices to show that $|B'_{r,n}| \leq |G_{r,n}^{\mathrm{Pink}}|$ for all $n \geq 1$.

We proceed by induction on n. For $n \leq r$, we have $e(m, n) = 1$ for all $m < n$, and hence $B'_{r,n} = \mathrm{Aut}(T_n)$. Therefore,

$$\log_2 |B'_{r,n}| = \log_2 |\mathrm{Aut}(T_n)| = 2^n - 1 = \log_2 |G_{r,n}^{\mathrm{Pink}}|,$$

where the final equality is by [Pin13, Proposition 2.3.1].

Now let $n \geq r + 1$, and suppose $|B'_{r,n-1}| \leq |G_{r,n-1}^{\mathrm{Pink}}|$. Let $S_{r,n}$ denote the kernel of the map $\mathrm{Res}_{n,n-1} : B'_{r,n} \to B'_{r,n-1}$. Then

$$|B'_{r,n}| = |\mathrm{Res}_{n,n-1}(B'_{r,n})| \cdot |S_{r,n}| \leq |B'_{r,n-1}| \cdot |S_{r,n}|.$$

Next, we compute the size of $S_{r,n}$. Define Y_n to be the kernel of the map $\mathrm{Res}_{n,n-1} : \mathrm{Aut}(T_n) \to \mathrm{Aut}(T_{n-1})$; that is, Y_n is the set of $\sigma \in \mathrm{Aut}(T_n)$ for which $\mathrm{Par}(\sigma, y) = 0$ for every node y below level $n-1$. Thus, $S_{r,n}$ is the set of $\sigma \in Y_n$ for which

$$P_r(\sigma, x) \equiv 1 \pmod{2^{e(n,m)}} \tag{20}$$

for all $0 \le m < n$ and all $x \in \{a,b\}^m$.

Observe, for any $\sigma \in Y_n$, any integer $0 \le m < n$, and any node x at level m, we have

$$P_r(\sigma, x) \equiv 1 + \sum_{i=1}^{e(n,m)-1} 2^i \sum_{w \in W(r,i)} \big[\mathrm{Par}(\sigma, xbw) - \mathrm{Par}(\sigma, xaw)\big] \pmod{2^{e(n,m)}}.$$

Note that unless $m = n - ri - 1$ for some i, then condition (20) is automatically satisfied by the assumption that σ acts trivially on all of T_{n-1}.

Furthermore, even when $m = n - ri - 1$ for some i, then again for $\sigma \in Y_n$, condition (20) reduces to

$$P_r(\sigma, x) \equiv 1 + 2^i \sum_{w \in W(r,i)} \big[\mathrm{Par}(\sigma, xbw) - \mathrm{Par}(\sigma, xaw)\big] \equiv 1 \pmod{2^{i+1}}.$$

Thus, for any $\sigma \in Y_n$, we have $\sigma \in S_{r,n}$ if and only if

$$\sum_{w \in W(r,i)} \mathrm{Par}(\sigma, xbw) - \sum_{w \in W(r,i)} \mathrm{Par}(\sigma, xaw) \quad \text{is even} \tag{21}$$

for each $i = 1, 2, \ldots, \ell$, and for each node x at level $n - 1 - ri$, where $\ell := \lfloor \frac{n-1}{r} \rfloor$.

To determine whether a given $\sigma \in Y_n$ belongs to $S_{r,n}$, start with $i = \ell$ and count down to $i = 1$. For each node x at level $n - 1 - ri$, the values of $\mathrm{Par}(\sigma, xbw)$ and $\mathrm{Par}(\sigma, xaw)$ for $w \in W(r,i)$ can be arbitrary except for $\mathrm{Par}(\sigma, xba^{ri-1})$, which must be chosen so that the sum in condition (21) is even. Since there are 2^{n-1-ri} nodes at this level, we have 2^{n-1-ri} parity restrictions arising from level i.

Furthermore, note that parity of σ at xba^{ri-1} did not arise in the sum in condition (21) for any previous values of i or x, because of the appearance of the symbol b in that particular location. Thus, the parity restrictions noted above are all independent of one another. With $\sigma \in Y_n$ determined by the parities $\mathrm{Par}(\sigma, y)$ for each of the 2^{n-1} nodes y at level $n-1$, and with 2^{n-1-ri} such restrictions for each $i = 1, 2, \ldots, \ell$, it follows that

$$\log_2 |S_{r,n}| = 2^{n-1} - \sum_{i=1}^{\ell} 2^{n-1-ir}.$$

On the other hand, by [Pin13, Proposition 2.3.1], we have

$$\log_2 |G_{r,n}^{\mathrm{Pink}}| = 2^n - 1 - \sum_{m=0}^{n-1} 2^{n-1-m} \cdot \left\lfloor \frac{m}{r} \right\rfloor.$$

Therefore,

$$\begin{aligned}
&\log_2 \left|G^{\mathrm{Pink}}_{r,n}\right| - \log_2 \left|G^{\mathrm{Pink}}_{r,n-1}\right| \\
&\qquad = \left(2^n - 1 - \sum_{m=0}^{n-1} 2^{n-1-m} \cdot \left\lfloor \frac{m}{r} \right\rfloor\right) - \left(2^{n-1} - 1 - \sum_{m=0}^{n-2} 2^{n-2-m} \cdot \left\lfloor \frac{m}{r} \right\rfloor\right) \\
&\qquad = 2^{n-1} - \sum_{m=0}^{n-1} 2^{n-1-m} \cdot \left\lfloor \frac{m}{r} \right\rfloor + \sum_{m=1}^{n-1} 2^{n-2-(m-1)} \cdot \left\lfloor \frac{m-1}{r} \right\rfloor \\
&\qquad = 2^{n-1} - 2^{n-1-0} \left\lfloor \frac{0}{r} \right\rfloor + \sum_{m=1}^{n-1} 2^{n-1-m} \left(\left\lfloor \frac{m-1}{r} \right\rfloor - \left\lfloor \frac{m}{r} \right\rfloor \right) \\
&\qquad = 2^{n-1} - \sum_{i=1}^{\left\lfloor \frac{n-1}{r} \right\rfloor} 2^{n-1-ir} = \log_2 |S_{r,n}|.
\end{aligned}$$

It follows that $\log_2 |G^{\mathrm{Pink}}_{r,n-1}| + \log_2 |S_{r,n}| = \log_2 |G^{\mathrm{Pink}}_{r,n}|$, and hence

$$\log_2 \left|B'_{r,n}\right| \le \log_2 |B'_{r,n-1}| + \log_2 |S_{r,n}| \le \log_2 |G^{\mathrm{Pink}}_{r,n-1}| + \log_2 |S_{r,n}| = \log_2 |G^{\mathrm{Pink}}_{r,n}|. \qquad \square$$

6.2. **The arithmetic Galois group.** For our field k not of characteristic 2, let μ_{2^∞} denote the set of all 2-power roots of unity in $\overline{k}$.

Lemma 6.3. *With notation as at the start of Section 6, for any polynomial $f(z) = z^2 + c \in k[z]$ with 0 periodic, we have $k_\infty = k(\mu_{2^\infty})$.*

Proof. By Theorem 5.1, there is an equivariant injective homomorphism $\rho : G^{\mathrm{arith}} \hookrightarrow M_{r,\infty}$. Moreover, by Theorem 6.2, restricting this homomorphism to $\mathrm{Gal}(K_\infty/k_\infty(t)) \cong G^{\mathrm{geom}}$ yields an isomorphism $G^{\mathrm{geom}} \cong B_{r,\infty}$.

By Lemma 3.1, k_∞ contains $k(\mu_{2^\infty})$. Hence we may consider the homomorphism

$$\chi : \mathrm{Gal}(k_\infty/k) \to \mathbb{Z}_2^\times$$

given by the 2-adic cyclotomic character. Moreover, by Theorem 4.1, we have a homomorphism $P_r : M_{r,\infty} \to \mathbb{Z}_2^\times$ which makes the following diagram commute:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G^{\mathrm{geom}} & \longrightarrow & G^{\mathrm{arith}} & \longrightarrow & \mathrm{Gal}(k_\infty/k) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \chi} & & \\
0 & \longrightarrow & B_{r,\infty} & \longrightarrow & M_{r,\infty} & \xrightarrow{P_r} & \mathbb{Z}_2^\times & &
\end{array} \tag{22}$$

Since $B_{r,\infty}$ is the kernel of P_r, the induced homomorphism $\bar{P}_r : M_{r,\infty}/B_{r,\infty} \to \mathbb{Z}_2^\times$ is injective. We also have an induced homomorphism $\bar{\rho} : G^{\mathrm{arith}}/G^{\mathrm{geom}} \to M_{r,\infty}/B_{r,\infty}$ given by

$$\bar{\rho}(\sigma G^{\mathrm{geom}}) = \rho(\sigma) B_{r,\infty}.$$

We claim that $\bar{\rho}$ is also injective. To see this, suppose $\bar{\rho}(\sigma_1 G^{\mathrm{geom}}) = \bar{\rho}(\sigma_2 G^{\mathrm{geom}})$. Then $\rho(\sigma_1) B_{r,\infty} = \rho(\sigma_2) B_{r,\infty}$, and hence $\rho(\sigma_1 \sigma_2^{-1}) \in B_{r,\infty}$. Because ρ is injective and $\rho(G^{\mathrm{geom}}) = B_{r,\infty}$, it follows that $\rho^{-1}(B_{r,\infty}) = G^{\mathrm{geom}}$, and hence $\sigma_1 \sigma_2^{-1} \in G^{\mathrm{geom}}$. Now the following diagram commutes:

$$\begin{array}{ccc}
G^{\mathrm{arith}}/G^{\mathrm{geom}} & \xrightarrow{\sim} & \mathrm{Gal}(k_\infty/k) \\
\downarrow{\scriptstyle \bar{\rho}} & & \downarrow{\scriptstyle \chi} \\
M_{r,\infty}/B_{r,\infty} & \xrightarrow{\bar{P}_r} & \mathbb{Z}_2^\times
\end{array}$$

and since $\bar{P}_r \circ \bar{\rho}$ is injective, the homomorphism χ must be injective as well.

Finally, since χ is injective and $\ker\chi = \mathrm{Gal}(k_\infty/k(\mu_{2^\infty}))$, the Galois group $\mathrm{Gal}(k_\infty/k(\mu_{2^\infty}))$ must be trivial, and therefore $k_\infty = k(\mu_{2^\infty})$. □

Note that in general, the maps ρ and χ in the above proof need not be surjective. We now show for a field k, we have $G^{\mathrm{arith}} \cong M_{r,\infty}$ if and only if $[k(\zeta_8) : k] = 4$, and in particular, that the number field $k = \mathbb{Q}(c)$ has this property.

Theorem 6.4. *Suppose $f(z) = z^2 + c \in k[z]$ and 0 is a periodic point of f. Let $K = k(t)$, let $x_0 = t$, let K_∞ be the resulting arboreal extension of K, and let $G^{\mathrm{arith}} := \mathrm{Gal}(K_\infty/K)$. Then the following are equivalent:*

(1) $G^{\mathrm{arith}} \cong M_{r,\infty}$
(2) $[k(\zeta_8) : k] = 4$
(3) $\mathrm{char}\, k = 0$ and $k \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}$.

Moreover, when $k = \mathbb{Q}(c)$, we have $k \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}$ and hence $G^{\mathrm{arith}} \cong M_{r,\infty}$.

Proof. We first prove the final statement: that for $k = \mathbb{Q}(c)$, we have $k \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}$. Since $f(z) = z^2 + c$ satisfies $f^r(0) = 0$, the parameter c is a root of the polynomial

$$\Big(\cdots\Big(\big((x^2+x)^2+x\big)^2+x\Big)^2+\cdots+x\Big)^2+x \in \mathbb{Z}[x],$$

which, reduced modulo 2, is the separable polynomial

$$x^{2^{r-1}} + x^{2^{r-2}} + \cdots + x^2 + x \in \mathbb{F}_2[x].$$

Therefore, the prime 2 is unramified in $k = \mathbb{Q}(c)$. It follows that $k \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}$, as desired.

Before proceeding to the equivalence of statements (1)–(3), we claim that

$$0 \longrightarrow B_{r,\infty} \longrightarrow M_{r,\infty} \xrightarrow{P_r} \mathbb{Z}_2^\times \longrightarrow 0$$

is a short exact sequence. To see this, still using $k = \mathbb{Q}(c)$, we have

$$\mathrm{Gal}(k_\infty/k) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}) \cong \mathbb{Z}_2^\times,$$

and the map $\chi : \mathrm{Gal}(k_\infty/k) \to \mathbb{Z}_2^\times$ is an isomorphism. Thus, the map $P_r : M_{r,\infty} \to \mathbb{Z}_2^\times$ is surjective by the fact that the diagram (22) commutes, and our claim above follows.

Now let k be any field satisfying the hypotheses of the theorem. By the above claim, and again by the fact that the diagram (22) commutes, we have that

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G^{\mathrm{geom}} & \longrightarrow & G^{\mathrm{arith}} & \longrightarrow & \mathrm{Gal}(k_\infty/k) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \chi} & & \\
0 & \longrightarrow & B_{r,\infty} & \longrightarrow & M_{r,\infty} & \xrightarrow{P_r} & \mathbb{Z}_2^\times & \longrightarrow & 0
\end{array}$$

commutes, with both rows exact.

The implication (3)⇒(2) is straightforward. To prove (2)⇒(3), observe that the condition $[k(\zeta_8) : k] = 4$ forces $\mathrm{char}\, k = 0$, because for any prime p, the root of unity ζ_8 has degree at most 2 over $\mathbb{F}_p$. Furthermore, since $\mathbb{Q}(\mu_{2^\infty})$ is a pro-2 extension of $\mathbb{Q}$, the field $k \cap \mathbb{Q}(\mu_{2^\infty})$ is strictly larger than $\mathbb{Q}$ if and only if k contains one of the three quadratic extensions of $\mathbb{Q}$ contained in $\mathbb{Q}(\mu_{2^\infty})$. (These three fields are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$, all of which are contained in $\mathbb{Q}(\zeta_8)$.) However, because $[k(\zeta_8) : k] = 4$, the field k contains none of $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{-2}$. Hence, we have $k \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}$, as desired.

To prove (1)⇒(2), observe that the map $\rho : G^{\mathrm{arith}} \to M_{r,\infty}$ in the diagram above is an isomorphism if and only if the cyclotomic character $\chi : \mathrm{Gal}(k_\infty/k) \to \mathbb{Z}_2^\times$ is surjective, in which case statement (2) follows immediately.

Finally, observe that statement (3) implies $\mathrm{Gal}(k_\infty/k) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}) \cong \mathbb{Z}_2^\times$, and hence χ is surjective. Therefore, ρ is also surjective in the diagram above, from which statement (1) follows. □

Theorem 6.4 also allows us to specify when the various roots of unity ζ_{2^n} first appear in the arboreal tower, as follows.

Corollary 6.5. *If $[k(\zeta_8) : k] = 4$, then $K_n \cap \overline{k} = k(\zeta_{2^e})$ for all $n \geq 1$, where $e = \lfloor \frac{n-1}{r} \rfloor + 1$. In particular, $\zeta_{2^n} \in K_{rn+1}$, and if $n \geq 2$, then $\zeta_{2^n} \notin K_{rn}$.*

Proof. Let $k_n := \overline{k} \cap K_n = k_\infty \cap K_n$. By Lemma 3.1, we have $k(\zeta_{2^e}) \subseteq k_n$, and our hypotheses imply that $[k(\zeta_{2^e}) : k] = |(\mathbb{Z}/2^e\mathbb{Z})^\times|$. Thus, it suffices to show $[k_n : k] = |(\mathbb{Z}/2^e\mathbb{Z})^\times|$.

By Theorem 6.4, we have $G^{\mathrm{arith}} \cong M_{r,\infty}$, and hence

$$G_n^{\mathrm{arith}} := \mathrm{Gal}(K_n/k(t)) \cong M_{r,n} := \mathrm{Res}_{\infty,n}(M_{r,\infty}).$$

Define $P_{r,e} : M_{r,n} \longrightarrow (\mathbb{Z}/2^e\mathbb{Z})^\times$ by setting $P_{r,e}(\sigma) := P_r(\tau) \pmod{2^e}$ for any $\tau \in M_{r,\infty}$ such that $\mathrm{Res}_{\infty,n}(\tau) = \sigma$. Observe that if $\tau_1, \tau_2 \in M_{r,\infty}$ satisfy $\mathrm{Res}_{\infty,n}(\tau_1) = \mathrm{Res}_{\infty,n}(\tau_2)$, then it follows from the construction of P_r in Definition 1.2 that $P_r(\tau_1) \equiv P_r(\tau_2) \pmod{2^e}$. Hence, $P_{r,e}$ is well-defined. It is clearly a homomorphism, and according to the proof of Theorem 6.2, the kernel of $P_{r,e}$ is $B_{r,n}$. Therefore, the following diagram commutes.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B_{r,\infty} & \longrightarrow & M_{r,\infty} & \xrightarrow{P_r} & \mathbb{Z}_2^\times & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{Res}_{\infty,n}} & & \downarrow{\scriptstyle \mathrm{Res}_{\infty,n}} & & \downarrow{\scriptstyle \mathrm{mod}\ 2^e} & & \\
0 & \longrightarrow & B_{r,n} & \longrightarrow & M_{r,n} & \xrightarrow{P_{r,e}} & (\mathbb{Z}/2^e\mathbb{Z})^\times & \longrightarrow & 0
\end{array}$$

In particular, the bottom row is short exact, and

$$\mathrm{Gal}(k_n/k) \cong G_n^{\mathrm{arith}}/G_n^{\mathrm{geom}} \cong M_{r,n}/B_{r,n} \cong (\mathbb{Z}/2^e\mathbb{Z})^\times,$$

as desired. □

7. Obtaining the arboreal Galois groups

We need two more lemmas in order to prove our main result.

Lemma 7.1. *Let k be any field with $[k(\zeta_8) : k] = 4$. Suppose $f(z) = z^2 + c \in k[z]$ is PCF. Let $K = k(t)$, let $x_0 = t$, and let K_∞ be the resulting arboreal extension of K. Let $A \in k$ such that $\sqrt{A} \in K_\infty$. Then $\sqrt{A} \in k(\zeta_8)$.*

Proof. Let $k_\infty := \overline{k} \cap K_\infty$. By Lemma 6.3, we have $k_\infty = k(\mu_{2^\infty})$, and by hypothesis we have $[k(\zeta_8) : k] = 4$. Thus,

$$\mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_2^\times.$$

Since $\mathbb{Z}_2^\times$ has only three index 2 subgroups, k_∞ contains only three quadratic extensions of k (formed by adjoining one of $\sqrt{-1}$, $\sqrt{2}$, or $\sqrt{-2}$), all of which are contained in $k(\zeta_8)$, there are similarly only three quadratic extensions of k in $k(\mu_{2^\infty})$, all contained in $k(\zeta_8)$. Thus, $\sqrt{A} \in k(\zeta_8)$. □

The following argument has been presented in various degrees of generality in [Odo88, Lemma 4.2], [Sto92, Lemmas 1.5 and 1.6], [Jon13, Section 2.2], [BD23, Proposition 5.3, Theorem 6.5]. We include a proof here for completeness.

Lemma 7.2. *Let $f(z) = z^2 + c \in K[z]$ and let $G_n = \mathrm{Gal}(K(f^{-n}(x_0))/K)$. For $n \geq 1$, define $D_i \in K$ by*

$$D_i := \begin{cases} x_0 - c & \text{if } i = 1, \\ f^i(0) - x_0 & \text{if } i \geq 2. \end{cases}$$

Then the following are equivalent.

(1) $G_n \cong \mathrm{Aut}(T_n)$.
(2) For all $1 \leq i \leq n$, $D_i \notin (K(\sqrt{D_1}, \ldots, \sqrt{D_{i-1}}))^2$. (For $i = 1$, this means $D_1 \notin K^2$.)

Proof. First suppose statement (2) fails for some $i \leq n$. Let Δ_i be the polynomial discriminant of $f^i(z) - x_0$. By [AHM05, Proposition 3.2], we have

$$\Delta_i = (-1)^{2^{i-1}} 2^{2^i} \big(f^i(0) - x_0\big) \Delta\big(f^{i-1}(z) - x_0\big)^2.$$

Thus, we have $\Delta_i = c_i^2 D_i$ for some $c_i \in K$, so Δ_i is a square in K. Therefore, every $\sigma \in G_i$ acts as an even permutation of the elements of $f^{-i}(x_0)$, so that $G_i \ncong \mathrm{Aut}(T_i)$, and hence $G_n \ncong \mathrm{Aut}(T_n)$ for all $n \geq i$.

Conversely, assume statement (2). For arbitrary $1 \leq i \leq n$, suppose $G_{i-1} \cong \mathrm{Aut}(T_{i-1})$, which is trivially true when $i = 1$. We claim that D_i is not a square in K_{i-1}. Let

$$L_i := K(\sqrt{D_1}, \ldots, \sqrt{D_i}),$$

which is an abelian extension of K. It follows from statement (2) that $\mathrm{Gal}(L_i/K) \cong \{\pm 1\}^i$. On the other hand, we have

$$K(\sqrt{D_1}, \ldots, \sqrt{D_{i-1}}) \subseteq K_{i-1}.$$

In particular, if $\sqrt{D_i} \in K_{i-1}$, then we would have $L_i \subseteq K_{i-1}$. Because L_i/K is abelian, it would follow that $\mathrm{Gal}(L_i/K) \subseteq G_{i-1}^{\mathrm{ab}}$. That is, we would have

$$\{\pm 1\}^i \cong \mathrm{Gal}(L_i/K) \subseteq G_{i-1}^{\mathrm{ab}} \cong \mathrm{Aut}(T_{i-1})^{\mathrm{ab}} \cong \{\pm 1\}^{i-1},$$

since the abelianization of a wreath product $G_1 \wr G_2$ is $G_1^{\mathrm{ab}} \times G_2^{\mathrm{ab}}$. This contradiction proves our claim, that D_i is not a square in K_{i-1}.

Armed with this claim, we now show that $[K_i : K_{i-1}] = 2^{2^{i-1}}$. (Together with our assumption that $G_{i-1} \cong \mathrm{Aut}(T_{i-1})$, it will then follow that $G_i \cong \mathrm{Aut}(T_i)$, from which statement (1) follows inductively.) Let $\beta_1, \ldots \beta_{2^{i-1}}$ denote the roots of $f^{i-1}(z) - x_0$, and note that K_i is formed by adjoining

$$\sqrt{\beta_1 - c}, \ldots, \sqrt{\beta_{2^{i-1}} - c}$$

to K_{i-1}. By Kummer theory, the degree $[K_i : K_{i-1}]$ is the order of the group generated by the classes of the elements $\beta_j - c$ in $K_{i-1}^\times / (K_{i-1}^\times)^2$. This order is $2^{2^{i-1}} / \#V$, where

$$V = \Big\{ (\epsilon_1, \ldots, \epsilon_{2^{i-1}}) \in \mathbb{F}_2^{2^{i-1}} : \prod_j (b_j - c)^{\epsilon_j} \in (K_{i-1}^\times)^2 \Big\}.$$

Hence, to prove $[K_i : K_{i-1}] = 2^{2^{i-1}}$, it suffices to show that $V = \{0\}$.

Note that V is an $\mathbb{F}_2$-vector space, and that G_{i-1} acts on V through its action on the β_j. That is, for any $\sigma \in G_{i-1}$, we may write σ as a permutation in $S_{2^{i-1}}$ given by its action on the indices of the β_j. For any $v = (\epsilon_1, \ldots, \epsilon_{2^{i-1}}) \in V$, we have $\prod_j (\beta_j - c)^{\epsilon_j} \in (K_{i-1}^\times)^2$, and hence

$$\sigma\bigg(\prod_j (\beta_j - c)^{\epsilon_j} \bigg) = \prod_j \left(\beta_{\sigma(j)} - c\right)^{\epsilon_j} \in (K_{i-1}^\times)^2.$$

The action is given by $\sigma v = (\epsilon_{\sigma^{-1}(1)}, \ldots, \epsilon_{\sigma^{-1}(2^{2^{i-1}})}) \in V$, making V an $\mathbb{F}_2[G_{i-1}]$-module.

By the orbit-stabilizer theorem, every G_{i-1}-orbit in $\mathbb{F}_2^{2^{i-1}}$ has cardinality a power of 2, since this cardinality must divide $|G_{i-1}|$. Because G_{i-1} acts transitively on the β_j, there are only two singleton orbits, and hence only two orbits of any odd cardinality: $(0,\dots,0)$ and $(1,\dots,1)$.

Since V is an $\mathbb{F}_2$-vector space, it contains $0=(0,\dots,0)$. If $V\neq\{0\}$, then $|V|$ is even, and hence V must contain a second G_{i-1}-orbit of odd order, meaning that $(1,\dots,1)\in V$. In that case, therefore, we have $\prod_j(\beta_j-c)\in(K_{i-1}^\times)^2$. However,

$$\prod_j(\beta_j-c)=(-1)^{2^{i-1}}\prod_j(c-\beta_j)=(-1)^{2^{i-1}}(f^{i-1}(c)-x_0)=(-1)^{2^{i-1}}(f^i(0)-x_0)=D_i,$$

which is a contradiction. Hence $V=\{0\}$, as desired. □

We are finally ready to prove Theorem 1.4.

Proof of Theorem 1.4. The implications (5)⇔(4)⇒(3)⇔(2) are trivial. Thus, it suffices to show (1)⇒(5) and (2)⇒(1). Define

$$L:=k(\sqrt{D_1},\dots,\sqrt{D_r}).$$

First assume statement (1), that $[L(\zeta_8):K]=2^{r+2}$. Then we have $[k(\zeta_8):k]=4$ and $[L(\zeta_8):k(\zeta_8)]=2^r$. As at the start of Section 6, let $k_\infty:=K_{t,\infty}\cap\overline{k}$ be the constant field extension in the setting of the function field $k(t)$ with root point t in place of x_0. Let k' denote the compositum of the degree 2 extensions of k contained in k_∞. By Lemma 7.1, we have $k'=k(\zeta_8)$. Moreover, since $[L(\zeta_8):k']=2^r$, Lemma 7.2 implies that

$$\mathrm{Gal}(K_{x_0,r}\cdot k'/k')\cong\mathrm{Aut}(T_r)\cong M_{r,r}.$$

Therefore,

$$|\operatorname{Gal}(K_{x_0,r}\cdot k'/k)|=|\operatorname{Gal}(K_{x_0,r}\cdot k'/k')|\cdot[k':k]=|M_{r,r}|\cdot[k':k]. \tag{23}$$

Noting that the forward orbit of 0 has cardinality r, we now apply [BGJT23, Theorem 4.6] (whose hypotheses assumes k is a number field, but only to ensure that $[k':k_1]$ is finite, a fact which is evident in our case). This result says, given the length r of the forward orbit of 0, along with condition (23), that $G_{x_0,\infty}\cong M_{r,\infty}$, i.e., that statement (5) holds.

Finally, assume statement (2), which implies both that $|G_{x_0,r}|=|M_{r,r}|=|\operatorname{Aut}(T_r)|$ and that $[K_{x_0,r}(\zeta_8):K_{x_0,r}]=4$. Since $|G_{x_0,r}|=|\operatorname{Aut}(T_r)|$, Lemma 7.2 implies that $[L:k]\geq 2^r$. On the other hand, because $L\subseteq K_{x_0,r}$, we have $[L(\zeta_8):L]\geq[K_{x_0,r}(\zeta_8):K_{x_0,r}]=4$. Therefore,

$$2^{r+2}\geq[L(\zeta_8):k]=[L(\zeta_8):L]\cdot[L:k]\geq 2^{r+2},$$

proving statement (1). □

References

[ABC+22] Faseeh Ahmad, Robert L. Benedetto, Jennifer Cain, Gregory Carroll, and Lily Fang, *Wreath products and proportions of periodic points*, J. Number Th. **238** (2022), 842–868.

[AHM05] Wayne Aitken, Farshid Hajir, and Christian Maire, *Finitely ramified iterated extensions*, Int. Math. Res. Not. IMRN **2005** (2005), 855–880.

[BD23] R. L. Benedetto and A. Dietrich, *Arboreal Galois groups for quadratic rational functions with colliding critical points*, Available at arXiv:2307.16284, 2023.

[BDG+21] Andrew Bridy, John R. Doyle, Dragos Ghioca, Liang-Chung Hsia, and Thomas J. Tucker, *Finite index theorems for iterated galois groups of unicritical polynomials*, Trans. Amer. Math. Soc. **374** (2021), no. 1, 733–752.

[BFH+17] 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** (2017), Art. 29, 21.

[BGJT23] Robert L. Benedetto, Dragos Ghioca, Jamie Juul, and Thomas J. Tucker, *Specializations of iterated Galois groups of PCF rational functions*, Available at arXiv:2309.00840, 2023.

[BJ19] Robert L. Benedetto and Jamie Juul, *Odoni's conjecture for number fields*, Bull. Lond. Math. Soc. **51** (2019), 237–250.

[JKMT16] Jamie Juul, Pär Kurlberg, Kalyani Madhu, and Tom J. Tucker, *Wreath products and proportions of periodic points*, Int. Math. Res. Not. IMRN (2016), no. 13, 3944–3969.

[Jon13] R. Jones, *Galois representations from pre-image trees: an arboreal survey*, Publ. Math. Besançon (2013), 107–136.

[Juu19] J. Juul, *Iterates of generic polynomials and generic rational functions*, Trans. Amer. Math. Soc. **371** (2019), no. 2, 809–831.

[Odo88] R. W. K. Odoni, *Realising wreath products of cyclic groups as Galois groups*, Mathematika **35** (1988), no. 1, 101–113.

[Pin13] Richard Pink, *Profinite iterated monodromy groups arising from quadratic polynomials*, Available at arXiv:1307.5678, 2013.

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

Robert L. Benedetto, Department of Mathematics and Statistics, Amherst College, Amherst, MA 01002, USA

Email address: rlbenedetto@amherst.edu

Dragos Ghioca, Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada

Email address: dghioca@math.ubc.ca

Jamie Juul, Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA

Email address: jamie.juul@colostate.edu

Thomas J. Tucker, Department of Mathematics, University of Rochester, Rochester, NY, 14620, USA

Email address: thomas.tucker@rochester.edu