THE ARITHMETIC BASILICA: A QUADRATIC PCF ARBOREAL GALOIS GROUP

FASEEH AHMAD, ROBERT L. BENEDETTO, JENNIFER CAIN, GREGORY CARROLL, AND LILY FANG

Abstract. The arboreal Galois group of a polynomial f over a field K encodes the action of Galois on the iterated preimages of a root point $x_0 \in K$, analogous to the action of Galois on the ℓ-power torsion of an abelian variety. We compute the arboreal Galois group of the postcritically finite polynomial $f(z) = z^2 - 1$ when the field K and root point x_0 satisfy a simple condition. We call the resulting group the *arithmetic basilica group* because of its relation to the basilica group associated with the complex dynamics of f. For $K = \mathbb{Q}$, our condition holds for infinitely many choices of x_0.

Let K be a field with algebraic closure $\overline{K}$, let $x_0 \in K$, and let $f \in K[z]$ be a polynomial of degree $d \geq 2$. For each $n \geq 0$, let f^n denote the n-th iterate $f \circ \cdots \circ f$ of f under composition, with $f^0(z) = z$ and $f^1(z) = f(z)$. The *backward orbit* of x_0 under f is

$$\mathrm{Orb}_f^-(x_0) := \coprod_{n \geq 0} f^{-n}(x_0) \subseteq \overline{K},$$

where $f^{-n}(y)$ is the set of roots of the equation $f^n(z) = y$ in $\overline{K}$.

If $f^n(z) - x_0$ is a separable polynomial, then $f^{-n}(x_0)$ has exactly d^n elements, and the field $K_n := K(f^{-n}(x_0)) \subseteq \overline{K}$ is a Galois extension of K, with Galois group

$$G_n := \mathrm{Gal}(K_n/K).$$

If $f^n(z) - x_0$ is separable for all $n \geq 0$, then we also define

$$G_\infty := \mathrm{Gal}(K_\infty/K), \quad \text{where} \quad K_\infty := \bigcup_{n \geq 0} K_n.$$

The backward orbit $\mathrm{Orb}_f^-(x_0)$ has the structure of an infinite d-ary rooted tree $T_{d,\infty}$, formed by connecting each $y \in f^{-(n+1)}(x_0)$ to $f(y) \in f^{-n}(x_0)$ via an edge. Thus, G_∞ is isomorphic to a subgroup of $\mathrm{Aut}(T_{d,\infty})$, and G_n is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(T_{d,n})$, where $T_{d,n}$ is the subtree of just the bottom n levels of $T_{d,\infty}$. The resulting action of Galois on the tree is analogous to the action of Galois on the ℓ-power torsion of an abelian variety A, since the ℓ-power torsion is precisely the backward orbit of the identity point O under the morphism $[\ell] : A \to A$.

Odoni introduced the study of such Galois groups in 1985 in [24], and Boston and Jones in 2007 called them "arboreal" in [6], since they act on trees. These groups have attracted increasing attention over the years; see [1, 2, 8, 9, 10, 11, 13, 14, 15, 17, 20, 28, 29] for a (very limited) selection. See also [16] for a survey of the field. Many examples have been found where G_∞ is the full group $\mathrm{Aut}(T_{d,\infty})$, as in [5, 18, 21, 22, 24, 27, 28]. More generally, the expectation has emerged that when K is a global field, G_∞ should usually

Date: August 30, 2019.

2010 *Mathematics Subject Classification.* 37P05, 11R32, 14G25.

have finite index in $\mathrm{Aut}(T_{d,\infty})$; see [16, Conjecture 3.11] for a precise conjecture when $d = 2$, and [7, 12, 19] for conditional results for $d = 2, 3$. By analogy, Serre's Open Image Theorem [26] states that for an elliptic curve over a number field, the action of Galois on the ℓ-power torsion has finite index in the appropriate automorphism group $GL(2, \mathbb{Z}_\ell)$.

However, just as Serre's Theorem excludes the special case of CM elliptic curves, there are special situations where G_∞ necessarily has infinite index in $\mathrm{Aut}(T_{d,\infty})$. One such case is that the map f is *postcritically finite*, or PCF, meaning that for every ramification point c of f, the forward orbit $\{f^n(c)|n \geq 0\}$ is finite; equivalently, every critical point of f is preperiodic. (See, for example, [16, Theorem 3.1].)

It is natural to ask whether a given PCF map has an associated subgroup of $\mathrm{Aut}(T_{d,\infty})$ that always contains, and in some cases equals, the arboreal Galois group G_∞. In [4], this question was answered in the affirmative for the PCF cubic polynomial $-2z^3 + 3z^2$, including an explicit computation of the subgroup $E_\infty \subsetneq \mathrm{Aut}(T_{3,\infty})$ and a simple sufficient condition on K and x_0 for G_∞ to be all of E_∞. In the present paper, we do the same for the PCF quadratic polynomial $z^2 - 1$.

For the rest of the paper, then, let $f(z) = z^2 - 1$, and let T_∞ and T_n denote the binary rooted trees $T_{2,\infty}$ and $T_{2,n}$, respectively. The two critical points $0, \infty$ of f are both periodic, with $\infty \mapsto \infty$ and $0 \mapsto -1 \mapsto 0$. Over the function field $K = \mathbb{C}(t)$ with $x_0 = t$, a setting in which arboreal Galois groups are often known as *profinite iterated monodromy groups*, G_∞ is isomorphic to the closure $\overline{B}_\infty$ of a well-understood subgroup B_∞ of $\mathrm{Aut}(T_\infty)$ called the *basilica group*. (See [23, Section 6.12.1], as well as [3, Section 5], especially Theorem 5.8 and following.) Here and throughout this paper, when we say that two groups that act on a tree are isomorphic, we mean not only that they are isomorphic as abstract groups, but that the isomorphism respects the action on the tree.

More generally, in [25, Theorem 2.5.6], Pink showed for *any* algebraically closed field $\overline{k}$ not of characteristic 2, then with $K = \overline{k}(t)$ and $x_0 = t$, the arboreal Galois group G_∞ is isomorphic to $\overline{B}_\infty$. Pink also showed that for function fields $K = k(t)$ where k is *not* algebraically closed, the arboreal Galois group G_∞ is an extension of $\overline{B}_\infty$ by a subgroup of the 2-adic multiplicative group $\mathbb{Z}_2^\times$, via the cyclotomic character $\mathrm{Gal}(\overline{k}/k) \to \mathbb{Z}_2^\times$. (See [25, Theorem 2.8.4].) We define and discuss $\overline{B}_\infty$ in Section 2.

However, our interest extends to the case that the field K is a number field, where Pink's results in [25] are suggestive but do not apply directly. Instead, we give an explicit definition of a subgroup $M_\infty \subsetneq \mathrm{Aut}(T_\infty)$ that we call the *arithmetic basilica group* and which is an extension of $\overline{B}_\infty$ by $\mathbb{Z}_2^\times$. More specifically, for each $\sigma \in \mathrm{Aut}(T_\infty)$ and each node x of the tree T_∞, we define a quantity $P(\sigma, x) \in \mathbb{Z}_2^\times$, which in turn we use to define M_∞. Our main results can be summarized as follows.

Main Theorem. *Let K be a field of characteristic different from 2, and let $x_0 \in K$. Let G_∞ be the arboreal Galois group for $f(z) = z^2 - 1$ over K, rooted at x_0. Then:*

(1) *G_∞ is isomorphic to a subgroup of the arithmetic basilica group M_∞.*
(2) *The following are equivalent:*
   (a) *$G_\infty \cong M_\infty$.*
   (b) *$G_5 \cong M_5$.*
   (c) *$[K(\sqrt{-x_0}, \sqrt{1 + x_0}, \zeta_8) : K] = 16$.*

Here, M_n denotes the quotient of M_∞ formed by restricting to its action on the subtree T_n, and ζ_8 denotes a primitive eighth root of unity.

The above theorem shows that, like the map $z \mapsto -2z^3 + 3z^2$ of [4], the PCF map $f(z) = z^2 - 1$ has an associated subgroup $M_\infty \subsetneq \mathrm{Aut}(T_\infty)$ that always contains and sometimes equals the arboreal Galois group G_∞. Condition (2b) shows that this equality is attained for the entire tree if it is already attained at the fifth level, and condition (2c) is very easy to check in practice.

We note that if $[K(\zeta_8) : K] = 4$, then by Hilbert's irreducibility theorem, there are many choices of $x_0 \in K$ for which $[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] = 16$, since the set of $x_0 \in K$ failing this condition is a thin set, in the sense of Serre. For example, if $K = \mathbb{Q}$, then the condition holds for

$$x_0 \text{ or } -1 - x_0 \text{ in } \{5, 6, 10, 11, 12, 13, 14, 19, 20, 21, 22, 23 \ldots\}$$

among (infinitely) many other examples.

On the other hand, even when $[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] < 16$, our computations suggest the following conjecture.

Conjecture 1. *Let K be a number field. Then for all but finitely many choices of $x_0 \in K$, the associated arboreal Galois group G_∞ has finite index in M_∞.*

We must allow for finitely many exceptional x_0 in Conjecture 1; for example, it is not hard to see that $[M_\infty : G_\infty] = \infty$ if x_0 is periodic. More generally, in light of our main theorem and the results of [4], as well as [17, Conjecture 1.1] and [8, Theorem 1.1], we propose the following broader conjecture.

Conjecture 2. *Let $\phi(z) \in \overline{\mathbb{Q}}(z)$ be a rational function of degree $d \geq 2$. Then there is a subgroup $G(\phi) \subseteq \mathrm{Aut}(T_{d,\infty})$ with the following property:*

Let K be a number field over which ϕ is defined, and let $x_0 \in \mathbb{P}^1(K)$. Then the associated arboreal Galois group G_∞ is isomorphic to a subgroup of $G(\phi)$. Moreover, it is possible to choose K and x_0 so that G_∞ is the full group $G(\phi)$.

If Conjecture 2 is true, then one can ask for sufficient conditions that $[G(\phi) : G_\infty] < \infty$. Besides periodic x_0, we also have $[G(\phi) : G_\infty] = \infty$ if some $\mathrm{Orb}_\phi^-(x_0)$ contains a critical point of f; if ϕ is not PCF, then this can happen for an infinite (but thin) set of $x_0 \in K$. Another example arises for $f(z) = z^2$: for $x_0 = -1$, we have $K_\infty = L$, where $L = K(\zeta_{2^\infty})$, but for $x_0 = 3$, we have $K_\infty = L(3^{1/2^\infty})$, which is an infinite extension of L.

The outline of the paper is as follows. The first three sections are purely group-theoretic. In Section 1, given a labeling of the tree $T_\infty := T_{2,\infty}$, we define the quantity $P(\sigma, x) \in \mathbb{Z}_2$ mentioned just before our Main Theorem earlier. We then use P to define the arithmetic basilica group $M_\infty \subseteq \mathrm{Aut}(T_\infty)$. In Theorem 1.4, we prove that M_∞ is indeed a group, and that the restriction of P to M_∞ is a homomorphism. In Section 2, we recall the definition and some properties of the closed basilica group $\overline{B}_\infty$. We also study the finite groups M_n and B_n formed by restricting M_∞ and $\overline{B}_\infty$ to the finite subtree T_n. Via a number of technical lemmas, we prove Theorem 2.7, giving sufficient conditions for generating certain subgroups of B_n. Furthermore, in Corollary 2.12, we show that the kernel of $P : M_\infty \to \mathbb{Z}_2^\times$ is precisely $\overline{B}_\infty$. Section 3 concerns the relationships among $\overline{B}_\infty$, M_∞, B_n, and M_n, encapsulated in Theorems 3.1, 3.2, and 3.3.

In the remaining two sections, we discuss the action of Galois on the tree $\mathrm{Orb}_f^-(x_0)$. In Section 4, we relate M_∞ to the arboreal Galois group G_∞ of $f(z) = z^2 - 1$. Specifically,

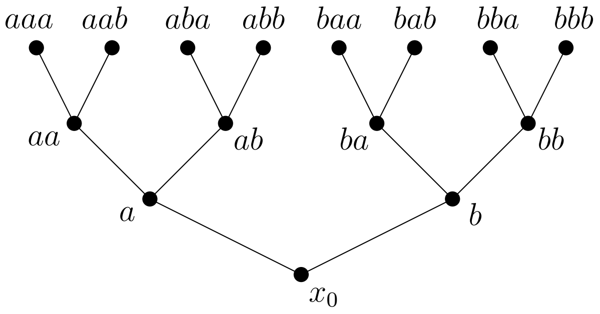

Figure 1. A labeling of T_3

Theorem 4.4 shows that G_∞ embeds in M_∞ after an appropriate labeling of the tree $\mathrm{Orb}_f^-(x_0)$, proving statement (1) of our Main Theorem. Section 5 is devoted to the proof of Theorem 5.4, that the condition $[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] = 16$ implies $G_\infty \cong M_\infty$. Finally, Corollary 5.5 proves statement (2) of our Main Theorem.

1. A special infinite sum on the tree

Let T_∞ denote a rooted binary tree, extending infinitely above the root point x_0. For each $n \geq 0$, let T_n denote the finite subtree of T_∞ from x_0 up to the n-th level above x_0.

Definition 1.1. A *labeling* of T_∞ is a choice of two tree morphisms $a, b : T_\infty \to T_\infty$ such that a maps T_∞ bijectively onto the subtree rooted at one of the two nodes connected to x_0, and b maps T_∞ bijectively onto the subtree rooted at the other.

For any integer $n \geq 1$, a labeling of T_n is a choice of two injective tree morphisms $a, b : T_{n-1} \to T_n$ with the same property.

To see why the choice of maps a, b in Definition 1.1 should be considered a "labeling" of each node of the tree, consider a node y at the m-th level of T_∞. By our choice of the maps a, b, there is a unique ordered m-tuple $(s_1, \ldots, s_m) \in \{a, b\}^m$ such that $y = s_1 \circ \cdots \circ s_m(x_0)$. Thus, it makes sense to label the node y with the m-tuple $(s_1, \ldots, s_m)$. The node directly underneath y then has label $(s_1, \ldots, s_{m-1})$. We will usually dispense with the punctuation and write $s_1 s_2 \cdots s_m$ instead of $(s_1, \ldots, s_m)$. We will also frequently abuse notation and refer to a node x and its label in $\{a, b\}^m$ interchangeably.

Note that the order we have written the m-tuple $(s_1, \ldots, s_m)$ is also the order we trace up the tree when following the path from x_0 to y. That is, s_1 tells us whether to go left (a) or right (b) to get from the root node to level 1; s_2 tells us whether to go left or right from there to level 2; and so on until we arrive at y. See Figure 1.

For any level $m \geq 0$, a tree automorphism $\sigma \in \mathrm{Aut}(T_\infty)$ or $\sigma \in \mathrm{Aut}(T_n)$ must satisfy the following properties.

(1) σ permutes the labels in $\{a, b\}^m$, and
(2) for each $(s_1, \ldots, s_m) \in \{a, b\}^m$, 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* $\operatorname{Par}(\sigma,x)$ of σ at x to be

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

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

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

Definition 1.2. Fix a labeling of T_∞, and let $\sigma \in \operatorname{Aut}(T_\infty)$. For any node x of T_∞, define

$$Q(\sigma,x) := \sum_{i\geq 0} 2^i \sum_{s_1,\ldots,s_i \in \{a,b\}} \operatorname{Par}(\sigma, xas_1as_2\cdots as_i) \in \mathbb{Z}_2, \tag{2}$$

and

$$P(\sigma,x) := (-1)^{\operatorname{Par}(\sigma,x)} + 2\sum_{t\in\{a,b\}} Q(\sigma,xbt) - 2\sum_{t\in\{a,b\}} Q(\sigma,xat) \in \mathbb{Z}_2^\times. \tag{3}$$

In addition, for any $n \geq m \geq 0$, any node x at level m of T_n, and any $\tau \in \operatorname{Aut}(T_n)$, set $j := \lfloor (n-m+1)/2 \rfloor$, and define $P(\tau,x) \in (\mathbb{Z}/2^j\mathbb{Z})^\times$ to be

$$P(\tau,x) :\equiv P(\tilde{\tau},x) \pmod{2^j}, \tag{4}$$

where $\tilde{\tau} \in \operatorname{Aut}(T_\infty)$ is any extension of τ to all of T_∞.

Regarding equation (4), note that every $\tau \in \operatorname{Aut}(T_n)$ has infinitely many extensions $\tilde{\tau} \in \operatorname{Aut}(T_\infty)$, since we may choose the parity $\operatorname{Par}(\tilde{\tau},y)$ at each node y at levels $n+1$ and higher to be either 0 or 1 as we please. However, the definition of $P(\tau,x)$ in equation (4) is independent of the extension $\tilde{\tau}$, since the contributions of $\operatorname{Par}(\tilde{\tau},y)$ for nodes y at levels $n+1$ and higher from equations (2) and (3) all have coefficients divisible by 2^j. That is, when computing $P(\tau,x)$, we may simply truncate the sums in equations (2) and (3) to include only the contributions from nodes at levels $n-1$ and below.

It is immediate from equation (2) that

$$Q(\sigma,x) = \operatorname{Par}(\sigma,x) + 2\sum_{s\in\{a,b\}} Q(\sigma,xas), \tag{5}$$

where we understand this equation to be an equality in $\mathbb{Z}_2^\times$ in the T_∞ case, and a congruence modulo an appropriate power of 2 in the T_n case.

To help explain Definition 1.2, observe that $P(\sigma,x)$ is ± 1 plus a weighted sum of $\operatorname{Par}(\sigma,y)$ at certain nodes y, chosen based on the labeling of the tree. For example, Figure 2 shows the nodes in question up to level 5. To compute $P = P(\sigma,x)$ in that case, we count the highlighted nodes as follows:

- count gray circles y for which $\operatorname{Par}(\sigma,y) = 1$ with weight -2,
- count white circles y for which $\operatorname{Par}(\sigma,y) = 1$ with weight 2,
- count gray squares y for which $\operatorname{Par}(\sigma,y) = 1$ with weight -4,
- count white squares y for which $\operatorname{Par}(\sigma,y) = 1$ with weight 4,

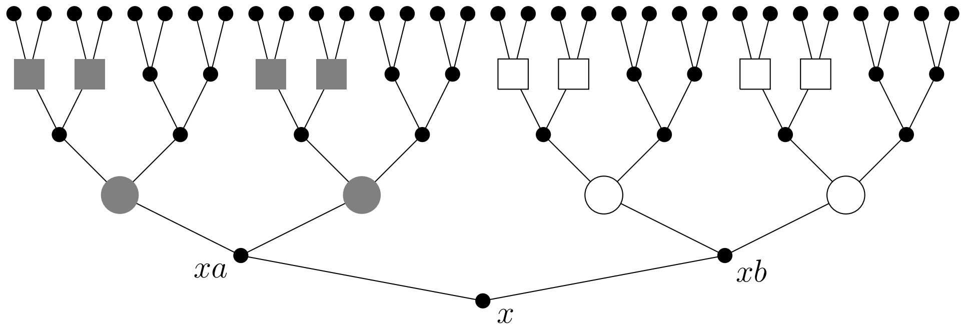

FIGURE 2. $P(\sigma,x)$ is a weighted sum of $\mathrm{Par}(\sigma,y)$ at the highlighted nodes y.

and so on up the tree. Finally, add 1 if $\mathrm{Par}(\sigma,x)=0$ or add -1 if $\mathrm{Par}(\sigma,x)=1$.

The strange form of $P(\sigma,x)$ in Definition 1.2 turns out to be exactly what is needed to carve out the correct subgroup of $\mathrm{Aut}(T_\infty)$ to serve as our arithmetic basilica group. More precisely, as we will see in Theorem 4.4, if ζ is a primitive 2^j-th root of unity, then an arboreal Galois element σ maps ζ to $\zeta^{P(\sigma,x)}$. The correct group, then, must consist only of those tree automorphisms σ for which $P(\sigma,x)$ is the same for every node x in the tree, as follows.

Definition 1.3. Fix a labeling a,b of T_∞. Let x_0 denote the (empty) label of the root point of the tree. Define the *arithmetic basilica group* M_∞ to be the set of all $\sigma\in\mathrm{Aut}(T_\infty)$ for which

$$P(\sigma,x)=P(\sigma,x_0)\quad\text{for every node } x\in T_\infty.$$

Similarly, given $n\geq 1$ and a labeling a,b of T_n, define M_n to be the set of all $\sigma\in\mathrm{Aut}(T_n)$ for which the following condition holds: for every $m\geq 0$, we have

$$P(\sigma,x)\equiv P(\sigma,x_0)\pmod{2^j}\quad\text{for every node } x\in\{a,b\}^m, \tag{6}$$

where $j:=\lfloor (n-m+1)/2\rfloor$.

Theorem 1.4. *The following hold.*

1. *M_∞ is a subgroup of* $\mathrm{Aut}(T_\infty)$.
2. *For every $n\geq 1$, M_n is a subgroup of* $\mathrm{Aut}(T_n)$.
3. *The map $P: M_\infty\to\mathbb{Z}_2^\times$ given by $P:\sigma\mapsto P(\sigma,x_0)$ is a group homomorphism.*
4. *For every $n\geq 1$, the map $P: M_n\to(\mathbb{Z}/2^j\mathbb{Z})^\times$ given by $P:\sigma\mapsto P(\sigma,x_0)$, where $j:=\lfloor (n+1)/2\rfloor$, is a group homomorphism.*

Proof. We prove statements (1) and (3); the proofs of statements (2) and (4) are similar.

Step 1. For any $\sigma\in\mathrm{Aut}(T_\infty)$ and any node x of T_∞, define

$$\mathrm{sgn}_1(\sigma,x):=(-1)^{\mathrm{Par}(\sigma,x)}=1-2\,\mathrm{Par}(\sigma,x). \tag{7}$$

It is immediate from equation (1) that for any $\sigma,\tau\in\mathrm{Aut}(T_\infty)$ and any node x of T_∞, we have

$$\mathrm{sgn}_1(\sigma\tau,x)=\mathrm{sgn}_1\big(\sigma,\tau(x)\big)\cdot\mathrm{sgn}_1(\tau,x). \tag{8}$$

We also have

$$\mathrm{Par}(\sigma\tau,x)=\mathrm{Par}\big(\sigma,\tau(x)\big)+\mathrm{sgn}_1\big(\sigma,\tau(x)\big)\,\mathrm{Par}(\tau,x). \tag{9}$$

Equation (9) follows from equation (8) by writing $\mathrm{Par}(\cdot,\cdot) = (1-\mathrm{sgn}_1(\cdot,\cdot))/2$, or simply by checking the four possible choices of $\mathrm{Par}(\tau, x)$ and $\mathrm{Par}(\sigma, \tau(x))$.

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

$$Z_{\sigma,\tau}(x) := Q\big(\sigma, \tau(x)\big) + P(\sigma)Q(\tau, x) - Q(\sigma\tau, x),$$

where $P(\sigma)$ is the constant value of $P(\sigma, w)$ for all nodes w of T_∞. We claim that

$$Z_{\sigma,\tau}(x) = 2Z_{\sigma,\tau}(xaa) + 2Z_{\sigma,\tau}(xab).$$

To see this, expand each appearance of Q in the definition of $Z_{\sigma,\tau}(x)$ according to equation (5), yielding

$$\begin{aligned} Z_{\sigma,\tau}(x) &= \mathrm{Par}\left(\sigma, \tau(x)\right) + P(\sigma)\,\mathrm{Par}(\tau, x) - \mathrm{Par}(\sigma\tau, x) \\ &\qquad + 2\sum_{s\in\{a,b\}} \Big[Q\big(\sigma, \tau(x)as\big) + P(\sigma)Q(\tau, xas) - Q(\sigma\tau, xas)\Big] \\ &= \mathrm{Par}\left(\sigma, \tau(x)\right) + \mathrm{sgn}_1\left(\sigma, \tau(x)\right)\mathrm{Par}(\tau, x) - \mathrm{Par}(\sigma\tau, x) \qquad (10) \\ &\qquad + 2\,\mathrm{Par}(\tau, x)\sum_{s\in\{a,b\}} \Big[Q\big(\sigma, \tau(x)bs\big) - Q\big(\sigma, \tau(x)as\big)\Big] \qquad (11) \\ &\qquad + 2\sum_{s\in\{a,b\}} \Big[Q\big(\sigma, \tau(x)as\big) + P(\sigma)Q(\tau, xas) - Q(\sigma\tau, xas)\Big], \qquad (12) \end{aligned}$$

where in the second equality, we expanded the first appearance of $P(\sigma)$ as $P(\sigma, \tau(x))$. The expression on line (10) is zero by equation (9). Next, observe that

$$\big\{\tau(x)aa, \tau(x)ab\big\} = \begin{cases} \big\{\tau(xaa), \tau(xab)\big\} & \text{if } \mathrm{Par}(\tau, x) = 0, \\ \big\{\tau(xba), \tau(xbb)\big\} & \text{if } \mathrm{Par}(\tau, x) = 1, \end{cases} \qquad (13)$$

and similarly for the set $\{\tau(x)ba, \tau(x)bb\}$. Thus, the expression on line (11) is

$$\begin{cases} 0 & \text{if } \mathrm{Par}(\tau, x) = 0, \\ 2\displaystyle\sum_{s\in\{a,b\}} \Big[Q\big(\sigma, \tau(xas)\big) - Q\big(\sigma, \tau(xbs)\big)\Big] & \text{if } \mathrm{Par}(\tau, x) = 1. \end{cases}$$

and the expression on line (12) is

$$\begin{cases} 2\displaystyle\sum_{s\in\{a,b\}} \Big[Q\big(\sigma, \tau(xas)\big) + P(\sigma)Q(\tau, xas) - Q(\sigma\tau, xas)\Big], & \text{if } \mathrm{Par}(\tau, x) = 0, \\ 2\displaystyle\sum_{s\in\{a,b\}} \Big[Q\big(\sigma, \tau(xbs)\big) + P(\sigma)Q(\tau, xas) - Q(\sigma\tau, xas)\Big], & \text{if } \mathrm{Par}(\tau, x) = 1. \end{cases}$$

For either possible value of $\mathrm{Par}(\tau, x)$, then, we have

$$\begin{aligned} Z_{\sigma,\tau}(x) &= 2\sum_{s\in\{a,b\}} \Big[Q\big(\sigma, \tau(xas)\big) + P(\sigma)Q(\tau, xas) - Q(\sigma\tau, xas)\Big] \\ &= 2Z_{\sigma,\tau}(xaa) + 2Z_{\sigma,\tau}(xab), \end{aligned}$$

proving our claim.

Step 3. As in Step 2, consider $\sigma \in M_\infty$ and $\tau \in \mathrm{Aut}(T_\infty)$. We claim that

$$Q\big(\sigma, \tau(x)\big) + P(\sigma)Q(\tau, x) = Q(\sigma\tau, x) \qquad (14)$$

for every node x of T_∞. That is, we are claiming that $Z_{\sigma,\tau}(x) = 0$ for every x. To prove this, it suffices to show, for each $j \geq 0$, that for every node x, we have $Z_{\sigma,\tau}(x) \in 2^j\mathbb{Z}_2$.

We proceed by induction on j. The base case $j = 0$ is immediate from the fact that $P(\cdot,\cdot), Q(\cdot,\cdot) \in \mathbb{Z}_2$. Assuming the statement holds for all x for some particular $j \geq 0$, then for any node x, Step 2 yields

$$Z_{\sigma,\tau}(x) = 2\big(Z_{\sigma,\tau}(xaa) + Z_{\sigma,\tau}(xab)\big) \in 2\big(2^j\mathbb{Z}_2\big) = 2^{j+1}\mathbb{Z}_2,$$

completing the induction and proving our claim.

Step 4. As in the previous two steps, consider $\sigma \in M_\infty$ and $\tau \in \mathrm{Aut}(T_\infty)$, and consider a node x in T_∞. We claim that

$$P(\sigma)P(\tau, x) = P(\sigma\tau, x). \tag{15}$$

Indeed, expanding $P(\tau, x)$ yields

$$\begin{aligned} P(\sigma)P(\tau,x) &= \mathrm{sgn}_1(\tau,x)P(\sigma) + 2\sum_{t\in\{a,b\}} P(\sigma)Q(\tau,xbt) - 2\sum_{t\in\{a,b\}} P(\sigma)Q(\tau,xat) \\ &= \mathrm{sgn}_1(\tau,x)\Big[\mathrm{sgn}_1\big(\sigma,\tau(x)\big) + 2\sum_{t\in\{a,b\}} Q\big(\sigma,\tau(x)bt\big) - 2\sum_{t\in\{a,b\}} Q\big(\sigma,\tau(x)at\big)\Big] \\ &\qquad + 2\sum_{t\in\{a,b\}} P(\sigma)Q(\tau,xbt) - 2\sum_{t\in\{a,b\}} P(\sigma)Q(\tau,xat), \end{aligned}$$

where we have also expanded the first appearance of $P(\sigma)$ as $P(\sigma,\tau(x))$. Applying equations (8) and (13), then, we have

$$\begin{aligned} P(\sigma)P(\tau,x) &= \mathrm{sgn}_1(\sigma\tau,x) + 2\sum_{t\in\{a,b\}} \Big[Q\big(\sigma,\tau(xbt)\big) + P(\sigma)Q(\tau,xbt)\Big] \\ &\qquad - 2\sum_{t\in\{a,b\}} \Big[Q\big(\sigma,\tau(xat)\big) + P(\sigma)Q(\tau,xat)\Big] \\ &= \mathrm{sgn}_1(\sigma\tau,x) + 2\sum_{t\in\{a,b\}} Q(\sigma\tau,xbt) - 2\sum_{t\in\{a,b\}} Q(\sigma\tau,xat) = P(\sigma\tau,x), \end{aligned}$$

where we used identity (14) twice in the second equality, thus proving our claim.

Step 5. To prove statement (1), first observe that the identity automorphism $e \in \mathrm{Aut}(T_\infty)$ belongs to M_∞, since $\mathrm{Par}(e,y) = 0$ for all nodes y, and hence $P(e,x) = 1$ for all nodes x of T_∞. Next, given $\sigma,\tau \in M_\infty$, it follows from identity (15) that for any node x of T_∞, we have

$$P(\sigma\tau,x) = P(\sigma)P(\tau,x) = P(\sigma)P(\tau,x_0) = P(\sigma\tau,x_0),$$

and hence $\sigma\tau \in M_\infty$. Finally, given $\sigma \in M_\infty$, consider $\sigma^{-1} \in \mathrm{Aut}(T_\infty)$. Then for any node x of T_∞, identity (15) again yields

$$1 = P(e,x) = P(\sigma\sigma^{-1},x) = P(\sigma)P(\sigma^{-1},x).$$

Thus,

$$P\big(\sigma^{-1},x\big) = P(\sigma)^{-1} = P\big(\sigma^{-1},x_0\big),$$

and therefore $\sigma^{-1} \in M_\infty$. That is, M_∞ is indeed a subgroup of $\mathrm{Aut}(T_\infty)$.

Finally, the fact that $P : M_\infty \to \mathbb{Z}_2^\times$ is a homomorphism is immediate from identity (15), proving statement (2). □

2. The basilica group and finite subtrees

For any $0 \leq n \leq m \leq \infty$, define a function $R_{m,n} : \operatorname{Aut}(T_m) \to \operatorname{Aut}(T_n)$ by restricting $\sigma \in \operatorname{Aut}(T_m)$ to T_n. Clearly $R_{m,n}$ is a homomorphism.

The group $\operatorname{Aut}(T_\infty)$ has a topological structure, as follows. For each $m \geq 0$, let $W_m := \ker(R_{\infty,m})$. That is, W_m consists of all $\sigma \in \operatorname{Aut}(T_\infty)$ that act trivially on levels 0 through n of the tree. The cosets of the normal subgroups W_m form a basis for a topology on $\operatorname{Aut}(T_\infty)$, making $\operatorname{Aut}(T_\infty)$ compact and Hausdorff. For $n \geq m \geq 0$, we will often abuse notation and write W_m for the subgroup $R_{\infty,n}(W_m)$.

For any node x of T_∞, it is immediate from Definition 1.2 that $\sigma \mapsto P(\sigma, x)$ is a continuous function from $\operatorname{Aut}(T_\infty)$ to $\mathbb{Z}_2^\times$. It follows that M_∞ is a closed and hence compact subgroup of $\operatorname{Aut}(T_\infty)$.

Fix a labeling of the tree T_∞. Define two particular automorphisms $\alpha, \beta \in \operatorname{Aut}(T_\infty)$ by specifying that

- $\operatorname{Par}(\alpha, bb\cdots b) = 1$ for any node whose label is a string of an odd number of b's,
- $\operatorname{Par}(\beta, bb\cdots b) = 1$ for any node whose label is a string of an even number of b's,
- $\operatorname{Par}(\alpha, y) = \operatorname{Par}(\beta, y) = 0$ for all other nodes y of T_∞.

The maps α and β can be equivalently defined by the recursive relations

$$\alpha(aw) = aw, \quad \alpha(bw) = b\beta(w), \qquad \beta(aw) = bw, \quad \beta(bw) = a\alpha(w)$$

for any word w in the symbols a, b.

Definition 2.1. The *basilica group* is the subgroup B_∞ of $\operatorname{Aut}(T_\infty)$ generated by α and β. The *closed basilica group* is the topological closure $\overline{B}_\infty$ of B_∞ in $\operatorname{Aut}(T_\infty)$.

Remark 2.2. Consider $\sigma \in W_1$, i.e., consider $\sigma \in \operatorname{Aut}(T_\infty)$ that fixes level 1 of the tree. Then σ acts on the subtree $T_{\infty,a}$ rooted at a as some automorphism $\sigma_a \in \operatorname{Aut}(T_\infty)$, and similarly on the subtree $T_{\infty,b}$ rooted at b as some $\sigma_b \in \operatorname{Aut}(T_\infty)$. That is, we may write $\sigma = (\sigma_a, \sigma_b)$.

In this notation, we have $\beta = (e, \alpha)$, where e is the identity element of $\operatorname{Aut}(T_\infty)$. Similarly, $\alpha^{-1}\beta\alpha$ and α^2 also belong to W_1, and simple computations show that $\alpha^{-1}\beta\alpha = (\alpha, e)$ and $\alpha^2 = (\beta, \beta)$.

Consider $\sigma \in B_\infty \cap W_1$. Then σ must be a finite product of α and β involving an even number of copies of α. (The parity condition on α is because $\sigma \in W_1$). Any such product can also be written as a product of powers of α^2, β, and $\alpha^{-1}\beta\alpha$. Thus, writing $\sigma = (\sigma_a, \sigma_b)$, we must have $\sigma_a, \sigma_b \in B_\infty$. Conversely, for any $\sigma_b \in B_\infty$, there is some $\sigma_a \in B_\infty$ such that $(\sigma_a, \sigma_b) \in B_\infty \cap W_1$. For this reason, the basilica group B_∞ is said to be a *self-similar group*. See [23] for more on self-similar groups, especially Sections 3.10.2, 5.2.2, and 6.12.1, which specifically concern B_∞.

Definition 2.3. Fix $n \geq 1$ and a labeling of T_∞. Define

(1) $B_n := R_{\infty,n}(B_\infty) = R_{\infty,n}(\overline{B}_\infty)$.
(2) $B'_n := R_{\infty,n}(\ker(P : M_\infty \to \mathbb{Z}_2^\times))$.
(3) $B''_n := \ker(P : M_n \to (\mathbb{Z}/2^j\mathbb{Z})^\times)$, where $j := \lfloor (n+1)/2 \rfloor$.
(4) $E_n := W_{n-1} \cap B_n, \quad E''_n := W_{n-1} \cap B''_n, \quad$ and $U_n := W_{n-1} \cap M_n$.

In addition, define $B_0 = B'_0 = B''_0 = E_0 = E''_0 = U_0 := R_{\infty,0}(\operatorname{Aut}(T_\infty))$, which is the trivial group acting on the trivial tree.

Recall from Theorem 1.4 that the maps P used to define B'_n and B''_n above are indeed homomorphisms, so that all three of B_n, B'_n, and B''_n are subgroups of $\operatorname{Aut}(T_n)$. Moreover, a simple computation shows $P(\alpha) = P(\beta) = 1$ for every node x of the tree T_∞. Thus, we have $B_n \subseteq B'_n \subseteq B''_n$. (In fact, as we will see in Corollary 2.12, these three groups coincide.)

Note that E_n is a normal subgroup of B_n, because W_{n-1} is a normal subgroup of $\operatorname{Aut}(T_\infty)$. In addition, once we know that $\overline{B}_\infty = \ker(P : M_\infty \to \mathbb{Z}_2^\times)$, it follows immediately that both E_n and B_n are normal subgroups of M_n. However, none of B_n, E_n, or M_n is a normal subgroup of $\operatorname{Aut}(T_n)$, because conjugation by an arbitrary element of $\operatorname{Aut}(T_n)$ has the effect of relabeling the tree, which in turn changes the function P.

Definition 2.4. Let $n \geq m \geq 1$, let $\sigma \in E''_n$, and let $x \in \{a,b\}^{n-m}$. If m is odd, write $m = 2i+1$, and define

$$\operatorname{sgn}_m(\sigma, x) := (-1)^{Q'(\sigma,x)},$$

where

$$Q'(\sigma, x) := \sum_{s_1,\ldots,s_i \in \{a,b\}} \operatorname{Par}(\sigma, xas_1as_2\cdots as_i) \in \mathbb{Z},$$

and where we understand $Q'(\sigma,x) = \operatorname{Par}(\sigma,x)$ if $m=1$. If m is even, define

$$\operatorname{sgn}_m(\sigma, x) := \operatorname{sgn}_{m-1}(\sigma, xa) \cdot \operatorname{sgn}_{m-1}(\sigma, xb). \tag{16}$$

The quantities Q' of Definition 2.4 and Q of equation (2) are related as follows. Suppose $\sigma \in E''_n$ and that x is a node at level $n-m$ where $m = 2i+1$. Then for any extension $\tilde{\sigma}$ of σ to the full tree T_∞, we have $2^{-i}Q(\tilde{\sigma}, x) \equiv Q'(\sigma, x) \pmod 2$.

When $m = 1$, the quantity $\operatorname{sgn}_1(\sigma, x)$ above coincides with our previous definition of $\operatorname{sgn}_1(\sigma, x) : 1 - 2\operatorname{Par}(\sigma, x)$ from equation (7). On the other hand, in [25, Section 1.5], Pink defines a notation $\operatorname{sgn}_n(\sigma)$ which is completely different from the quantity $\operatorname{sgn}_m(\sigma, x)$ in Definition 2.4 above.

Lemma 2.5. *Let $n \geq m \geq 1$, let $\sigma_1, \sigma_2 \in E''_n$, let $\tau \in M_n$, and let $x \in \{a,b\}^{n-m}$. Then*

(1) $\operatorname{sgn}_m(\sigma_1\sigma_2, x) = \operatorname{sgn}_m(\sigma_1, x) \cdot \operatorname{sgn}_m(\sigma_2, x)$. *That is,* $\operatorname{sgn}_m(\cdot, x) : E''_n \to \{\pm 1\}$ *is a group homomorphism.*
(2) *If $m \geq 3$ is odd, then* $\operatorname{sgn}_{m-1}(\sigma_1, xa) = \operatorname{sgn}_{m-1}(\sigma_1, xb) = \operatorname{sgn}_m(\sigma_1, x)$.
(3) $\tau\sigma_1\tau^{-1} \in E''_n$, *and* $\operatorname{sgn}_m(\tau\sigma_1\tau^{-1}, \tau(x)) = \operatorname{sgn}_m(\sigma_1, x)$.

Proof. **(1)**: By equation (9), we have

$$\operatorname{Par}(\sigma_1, y) + \operatorname{Par}(\sigma_2, y) \equiv \operatorname{Par}(\sigma_1\sigma_2, y) \pmod 2 \quad \text{for all nodes } y \in \{a,b\}^{n-1}.$$

For m odd, it follows immediately that $Q'(\sigma_1, x) + Q'(\sigma_2, x) \equiv Q'(\sigma_1\sigma_2, x) \pmod 2$, and therefore that $\operatorname{sgn}_m(\sigma_1\sigma_2, x) = \operatorname{sgn}_m(\sigma_1, x) \cdot \operatorname{sgn}_m(\sigma_2, x)$. For m even, we have

$$\begin{aligned}\operatorname{sgn}_m(\sigma_1\sigma_2, x) &= \operatorname{sgn}_{m-1}(\sigma_1\sigma_2, xa) \cdot \operatorname{sgn}_{m-1}(\sigma_1\sigma_2, xb) \\ &= \operatorname{sgn}_{m-1}(\sigma_1, xa)\operatorname{sgn}_{m-1}(\sigma_2, xa)\operatorname{sgn}_{m-1}(\sigma_1, xb)\operatorname{sgn}_{m-1}(\sigma_2, xb) \\ &= \operatorname{sgn}_m(\sigma_1, x)\operatorname{sgn}_m(\sigma_2, x).\end{aligned}$$

(2): By definition of Q', we have

$$\begin{aligned}Q'(\sigma_1, x) &= \sum_{s_2,\ldots,s_i \in \{a,b\}} \operatorname{Par}(\sigma_1, xaaas_2\cdots as_i) + \sum_{s_2,\ldots,s_i \in \{a,b\}} \operatorname{Par}(\sigma_1, xabas_2\cdots as_i) \\ &= Q'(\sigma_1, xaa) + Q'(\sigma_1, xab),\end{aligned}$$

and hence

$$\operatorname{sgn}_m(\sigma_1, x) = \operatorname{sgn}_{m-2}(\sigma_1, xaa)\operatorname{sgn}_{m-2}(\sigma_1, xab) = \operatorname{sgn}_{m-1}(\sigma_1, xa).$$

Write $m = 2i+1$. Since $\sigma_1 \in E''_n$, we have $P(\sigma_1, x) \equiv 1 \pmod{2^{i+1}}$, and therefore

$$2^iQ(\sigma_1, xaa) + 2^iQ(\sigma_1, xab) \equiv 2^iQ(\sigma_1, xba) + 2^iQ(\sigma_1, xbb) \pmod{2^{i+1}}.$$

Thus, $Q'(\sigma_1, xaa) + Q'(\sigma_1, xab) \equiv Q'(\sigma_1, xba) + Q'(\sigma_1, xbb) \pmod 2$, and hence

$$\begin{aligned}\operatorname{sgn}_{m-1}(\sigma_1, xa) &= \operatorname{sgn}_{m-1}(\sigma_1, xaa) + \operatorname{sgn}_{m-1}(\sigma_1, xab)\\ &= \operatorname{sgn}_{m-1}(\sigma_1, xba) + \operatorname{sgn}_{m-1}(\sigma_1, xbb) = \operatorname{sgn}_{m-1}(\sigma_1, xb).\end{aligned}$$

(3): The inclusion $\tau\sigma_1\tau^{-1} \in E''_n$ is immediate from the facts that $B''_n \subseteq M_n$ and $W_{n-1} \subseteq \operatorname{Aut}(T_n)$ are both kernels of homomorphisms. To prove the desired identity, we proceed by induction on m. For $m = 1$, we have $\operatorname{sgn}_1(\tau\sigma_1\tau^{-1}, \tau(x)) = \operatorname{sgn}_1(\sigma_1, x)$ by equation (8).

For $m \geq 2$, assuming the statement is true for $m-1$, suppose first that m is even. By equation (16) of Definition 2.4, we have

$$\begin{aligned}\operatorname{sgn}_m\left(\tau\sigma_1\tau^{-1}, \tau(x)\right) &= \operatorname{sgn}_{m-1}\left(\tau\sigma_1\tau^{-1}, \tau(x)a\right)\operatorname{sgn}_{m-1}\left(\tau\sigma_1\tau^{-1}, \tau(x)b\right)\\ &= \operatorname{sgn}_{m-1}\left(\tau\sigma_1\tau^{-1}, \tau(xa)\right)\operatorname{sgn}_{m-1}\left(\tau\sigma_1\tau^{-1}, \tau(xb)\right)\\ &= \operatorname{sgn}_{m-1}(\sigma, xa)\operatorname{sgn}_{m-1}(\sigma, xb) = \operatorname{sgn}_m(\sigma, x),\end{aligned}$$

where the second equality is by swapping the order of the two multiplicands if necessary, and the third is by our inductive hypothesis. On the other hand, if m is odd, then by part (2), we have

$$\begin{aligned}\operatorname{sgn}_m\left(\tau\sigma_1\tau^{-1}, \tau(x)\right) &= \operatorname{sgn}_{m-1}\left(\tau\sigma_1\tau^{-1}, \tau(x)s\right) \quad \text{for both } s = a, b\\ &= \operatorname{sgn}_{m-1}\left(\tau\sigma_1\tau^{-1}, \tau(xa)\right) = \operatorname{sgn}_{m-1}(\sigma_1, xa) = \operatorname{sgn}_m(\sigma_1, a) \qquad \square\end{aligned}$$

Remark 2.6. For $n = 2i+1$ odd, a simple computation shows that $R_{\infty,n}(\alpha)^{2^i} \in \operatorname{Aut}(T_n)$ is given by

$$\operatorname{Par}\left(R_{\infty,n}(\alpha)^{2^i}, y\right) = \begin{cases}1 & \text{if } y = s_1bs_2b\cdots s_ib \text{ for some } s_1,\ldots,s_i \in \{a,b\},\\ 0 & \text{else,}\end{cases}$$

and hence

$$R_{\infty,n}(\alpha)^{2^i} \in E_n, \quad \text{with} \quad \operatorname{sgn}_n\left(R_{\infty,n}(\alpha)^{2^i}, x_0\right) = -1.$$

Similarly, for $n = 2i$ even, we have

$$\operatorname{Par}\left(R_{\infty,n}(\beta)^{2^{(i-1)}}, y\right) = \begin{cases}1 & \text{if } y = bs_1bs_2b\cdots s_{i-1}b \text{ for some } s_1,\ldots,s_{i-1} \in \{a,b\},\\ 0 & \text{else,}\end{cases}$$

and hence

$$R_{\infty,n}(\beta)^{2^{(i-1)}} \in E_n, \quad \text{with} \quad \operatorname{sgn}_n\left(R_{\infty,n}(\beta)^{2^{(i-1)}}, x_0\right) = -1.$$

In particular, $\operatorname{sgn}_n(\cdot, x_0)$ is a nontrivial map.

Theorem 2.7. *Let $n \geq 1$, and let $G \subseteq B''_n$ be a subgroup satisfying*

1. *$R_{n,n-1}(G \cap B_n) \supseteq B_{n-1}$, and*
2. *there is some $\lambda \in G \cap E_n$ such that $\operatorname{sgn}_n(\lambda, x_0) = -1$.*

Then $E''_n = G \cap E_n = E_n$.

The proof of Theorem 2.7 relies on the following lemmas.

Lemma 2.8. *For every $n \geq m \geq 0$, B_n acts transitively on the 2^m nodes at level m of T_n.*

Proof. We proceed by induction on $m \geq 0$. The statement is trivial for $m = 0$.

For $m \geq 1$, assume the statement holds for $m-1$. Given nodes x, y at level m, after possibly applying α to one or both, we may assume that $x = bv$ and $y = bw$ for $v, w \in \{a, b\}^{m-1}$. By our inductive hypothesis, there is some $\sigma_b \in B_\infty$ such that $\sigma_b(v) = w$. Therefore, as noted in Remark 2.2, there is some $\sigma_a \in B_\infty$ such that the automorphism $\sigma := (\sigma_a, \sigma_b) \in W_1$ lies in B_∞. We have $\sigma(x) = y$, as desired. □

Lemma 2.9. *Fix integers $n > m \geq 0$. Let $\sigma \in E''_n$ and $\tau \in M_n$. Define $\mu := \sigma\tau\sigma^{-1}\tau^{-1}$. For any node w at level m of the tree for which $\tau(w) = w$, we have $\operatorname{sgn}_{n-m-1}(\mu, wa) = \operatorname{sgn}_{n-m-1}(\mu, wb)$, and this common value is*

- -1 *if* $\operatorname{sgn}_{n-m-1}(\sigma, wa) \neq \operatorname{sgn}_{n-m-1}(\sigma, wb)$ *and* $\operatorname{Par}(\tau, w) = 1$, *or*
- $+1$ *otherwise.*

Proof. If $\operatorname{Par}(\tau, w) = 0$, then $\tau(wa) = wa$ and $\tau(wb) = wb$. By Lemma 2.5.(3), then, we have

$$\operatorname{sgn}_{n-m-1}(\tau\sigma^{-1}\tau^{-1}, wa) = \operatorname{sgn}_{n-m-1}(\sigma^{-1}, wa) = \operatorname{sgn}_{n-m-1}(\sigma, wa),$$

and hence by Lemma 2.5.(1), we have

$$\begin{aligned}\operatorname{sgn}_{n-m-1}(\mu, wa) &= \operatorname{sgn}_{n-m-1}(\sigma, wa) \cdot \operatorname{sgn}_{n-m-1}(\tau\sigma^{-1}\tau^{-1}, wa) \\ &= \operatorname{sgn}_{n-m-1}(\sigma, wa) \cdot \operatorname{sgn}_{n-m-1}(\sigma, wa) = +1,\end{aligned}$$

and similarly $\operatorname{sgn}_{n-m-1}(\mu, wb) = +1$, as desired.

Assume for the remainder of the proof that $\operatorname{Par}(\tau, w) = 1$, and hence that $\tau(wa) = wb$ and $\tau(wb) = wa$. By Lemma 2.5.(3) again, we have

$$\operatorname{sgn}_{n-m-1}(\tau\sigma^{-1}\tau^{-1}, wa) = \operatorname{sgn}_{n-m-1}(\sigma^{-1}, wb) = \operatorname{sgn}_{n-m-1}(\sigma, wb).$$

Therefore, by Lemma 2.5.(1), we have

$$\begin{aligned}\operatorname{sgn}_{n-m-1}(\mu, wa) &= \operatorname{sgn}_{n-m-1}(\sigma, wa) \cdot \operatorname{sgn}_{n-m-1}(\tau\sigma^{-1}\tau^{-1}, wa) \\ &= \operatorname{sgn}_{n-m-1}(\sigma, wa) \cdot \operatorname{sgn}_{n-m-1}(\sigma, wb),\end{aligned}$$

which is $+1$ if $\operatorname{sgn}_{n-m-1}(\sigma, wa) = \operatorname{sgn}_{n-m-1}(\sigma, wb)$, and -1 otherwise. A similar computation yields the same result for $\operatorname{sgn}_{n-m-1}(\mu, wb)$, completing the proof. □

Lemma 2.10. *Fix integers $n > m \geq 0$, and let $G \subseteq B''_n$ be a subgroup satisfying*

1. $R_{n,n-1}(G \cap B_n) \supseteq B_{n-1}$, *and*
2. *for every $\sigma \in E''_n$, there exists $\tau \in G \cap E_n$ such that*

$$\operatorname{sgn}_{n-m}(\tau, w) = \operatorname{sgn}_{n-m}(\sigma, w) \quad \textit{for all nodes } w \textit{ at level } m. \tag{17}$$

Suppose that $n - m$ is even. Then for every node w at level m, there exists $\mu_w \in G \cap E_n$ such that for each node y at level $m+1$, we have

$$\operatorname{sgn}_{n-m-1}(\mu_w, y) = \begin{cases} -1 & \textit{if } y = wa \textit{ or } y = wb, \\ +1 & \textit{otherwise.} \end{cases} \tag{18}$$

Proof. **Case 1**: n is odd. Write $n = 2\ell + 1$ and $m = 2j + 1$ for integers $\ell > j \geq 0$. By hypothesis (2) applied to $R_{\infty,n}(\alpha^{2^\ell}) \in E_n \subseteq E''_n$, there is some $\gamma \in G \cap E_n$ such that

$$\operatorname{sgn}_{n-m}(\gamma, w) = \operatorname{sgn}_{n-m}\left(\alpha^{2^\ell}, w\right) \quad \text{for all nodes } w \text{ at level } m.$$

By hypothesis (1), there is some $\delta \in G \cap B_n$ such that

$$R_{n,n-1}(\delta) = R_{\infty,n-1}\big(\beta^{2^j}\big).$$

Let $\mu := \gamma\delta\gamma^{-1}\delta^{-1}$. Note that $\mu \in G \cap E_n$, since $\gamma \in G \cap E_n$, and E_n is normal subgroup of B_n.

A slight generalization of Remark 2.6 shows that for any node y at level $m + 1$, we have

$$\operatorname{sgn}_{n-m-1}(\gamma, y) = \begin{cases} -1 & \text{if } y = s_0bs_1b\cdots bs_j \text{ for some } s_0, \ldots, s_j \in \{a, b\}, \\ +1 & \text{otherwise,} \end{cases}$$

and for any node w at level m, we have

$$\operatorname{Par}(\delta, w) = \begin{cases} 1 & \text{if } w = bt_1bt_2\cdots bt_j \text{ for some } t_1, \ldots, t_j \in \{a, b\}, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, by Lemma 2.9, for any node y at level $m + 1$, we have

$$\operatorname{sgn}_{n-m-1}(\mu, y) = \begin{cases} -1 & \text{if } y = bb\cdots bs \text{ for some } s \in \{a, b\}, \\ +1 & \text{otherwise.} \end{cases}$$

Thus, μ is the desired automorphism μ_x for the node $x = bb\cdots b$ at level m of the tree.

By Lemma 2.8 and hypothesis (1), the group $G \cap B_n$ acts transitively on the nodes of T_n at level m. Thus, for each node w at level m, there is some $\rho_w \in G \cap B_n$ such that $\rho_w(bb\cdots b) = w$. By Lemma 2.5.(3), the automorphism $\mu_w := \rho_w\mu\rho_w^{-1} \in G \cap E_n$ satisfies equation (18), and we are done.

Case 2: n is even. Write $n = 2\ell$ and $m = 2j$ for integers $\ell > j \geq 0$. Hypothesis (2) yields the existence of some $\gamma \in G \cap E_n$ such that

$$\operatorname{sgn}_{n-m}(\gamma, w) = \operatorname{sgn}_{n-m}\left(\beta^{2^{\ell-1}}, w\right) \quad \text{for all nodes } w \text{ at level } m,$$

and hypothesis (1) yields some $\delta \in G \cap B_n$ such that

$$R_{n,n-1}(\delta) = R_{\infty,n-1}\big(\alpha^{2^j}\big).$$

As before, let $\mu := \gamma\delta\gamma^{-1}\delta^{-1} \in G \cap E_n$. By similar reasoning as in Case 1, it follows that μ is the desired μ_x for the node $x = bb\cdots b$, and then that conjugating yields the desired μ_w for each node w at level m. □

Lemma 2.11. *Fix integers $m \geq 0$ and $n \geq m + 2$, and let $G \subseteq B''_n$ be a subgroup satisfying hypotheses (1) and (2) of Lemma 2.10. Then for every $\sigma \in E''_n$, there exists $\tilde{\tau} \in G \cap E_n$ such that*

$$\operatorname{sgn}_{n-m-1}(\tilde{\tau}, y) = \operatorname{sgn}_{n-m-1}(\sigma, y) \quad \textit{for all nodes } y \textit{ at level } m + 1.$$

Proof. We consider two cases.

Case 1: $n-m\geq 3$ is odd. Given $\sigma\in E''_n$, we may choose $\tau\in G\cap E_n$ satisfying equation (17), by hypothesis (2). Let $\tilde{\tau}:=\tau$. For any node y at level $m+1$, let w be the node immediately below y on level m, so that either $y=wa$ or $y=wb$. Then by Lemma 2.5.(2),

$$\operatorname{sgn}_{n-m-1}(\tilde{\tau},y)=\operatorname{sgn}_{n-m}(\tilde{\tau},w)=\operatorname{sgn}_{n-m}(\sigma,w)=\operatorname{sgn}_{n-m-1}(\sigma,y).$$

Case 2: $n-m\geq 2$ is even. Given $\sigma\in E''_n$, we may choose $\tau\in G\cap E_n$ satisfying equation (17), by hypothesis (2). For each node w at level m, therefore, according to equation (16) of Definition 2.4, we have

$$\operatorname{sgn}_{n-m-1}(\tau,wa)\operatorname{sgn}_{n-m-1}(\tau,wb)=\operatorname{sgn}_{n-m-1}(\sigma,wa)\operatorname{sgn}_{n-m-1}(\sigma,wb).$$

Thus, for each such w, we have

$$\frac{\operatorname{sgn}_{n-m-1}(\tau,wa)}{\operatorname{sgn}_{n-m-1}(\sigma,wa)}=\frac{\operatorname{sgn}_{n-m-1}(\tau,wb)}{\operatorname{sgn}_{n-m-1}(\sigma,wb)}\in\{\pm 1\}\tag{19}$$

Let $w_1,\ldots,w_r$ be all the nodes w at level m for which the value in equation (19) is -1, and define

$$\tilde{\tau}:=\tau\mu_{w_1}\mu_{w_2}\cdots\mu_{w_r}\in G\cap E_n,$$

where each $\mu_w\in G\cap E_n$ is the automorphism given by equation (18) of Lemma 2.10. Then by Lemma 2.5.(1), all the values in equation (19) become $+1$ when we replace τ by $\tilde{\tau}$, proving the desired conclusion. □

Proof of Theorem 2.7. **Step 1**. We claim that for each $m=0,\ldots,n-1$, hypothesis (2) of Lemma 2.10 holds. For $m=0$, there is only one node at level 0, and $e,\lambda\in G\cap E_n$ attain the two possible values $\operatorname{sgn}_n(e,x_0)=+1$ and $\operatorname{sgn}_n(\lambda,x_0)=-1$, where λ is the element assumed to exist in the statement of Theorem 2.7. Proceeding inductively, assuming the claim holds for some $m\in\{0,\ldots,n-2\}$, the hypotheses of Lemma 2.11 hold, since hypothesis (1) is already one of the assumptions of Theorem 2.7. Thus, Lemma 2.11 verifies that hypothesis (2) holds for $m+1$, proving the claim.

Step 2. For any $\sigma\in E''_n$, the claim of Step 1 for $m=n-1$ shows that there is some $\tau\in G\cap E_n$ such that

$$\operatorname{sgn}_1(\tau,w)=\operatorname{sgn}_1(\sigma,w)\quad\text{for all nodes } w \text{ at level } n-1.$$

Since $\sigma,\tau\in\operatorname{Aut}(T_n)$ fix all nodes at levels below n, it follows that $\sigma=\tau\in G\cap E_n$. Thus,

$$E''_n\subseteq G\cap E_n\subseteq E_n\subseteq E''_n,$$

and hence these three groups coincide, as desired. □

Corollary 2.12. *For every $n\geq 0$, we have $B_n=B'_n=B''_n$ and $E_n=E''_n$. Moreover, the closed basilica group $\overline{B}_\infty$ is precisely* $\ker(P:M_\infty\to\mathbb{Z}_2^\times)$.

Proof. **First statement**: For $n=0$, the relevant groups trivially coincide by Definition 2.3. Proceeding inductively for $n\geq 1$, suppose the desired equalities hold for $n-1$, and let $G:=B''_n$. Then

$$R_{n,n-1}(G\cap B_n)=R_{n,n-1}(B_n)=B_{n-1},$$

so that hypothesis (1) of Theorem 2.7 holds. Hypothesis (2) is immediate from Remark 2.6, and hence Theorem 2.7 yields $E''_n = E_n$.

The restriction of $R_{n,n-1}$ to B''_n is a surjective homomorphism $\rho'' : B''_n \to B''_{n-1}$ with kernel E''_n. Similarly, the restriction of $R_{n,n-1}$ to B_n is a surjective homomorphism $\rho : B_n \to B_{n-1}$ with kernel E_n. We have $B_{n-1} = B''_{n-1}$ by our inductive hypothesis, and $E_n = E''_n$ by the previous paragraph; therefore, since ρ is the restriction of ρ'' to $B_n \subseteq B''_n$, we have $B_n = B''_n$. The first statement now follows from the fact that $B_n \subseteq B'_n \subseteq B''_n$.

Second statement: As noted near the start of Section 2, the map $P : M_\infty \to \mathbb{Z}_2^\times$ is continuous. Therefore, since $\alpha, \beta \in \ker(P)$, we have $\overline{B}_\infty \subseteq \ker(P)$.

Conversely, given $\sigma \in \ker(P)$, define $\sigma_n := R_{\infty,n}(\sigma) \in B'_n$ for each $n \geq 1$. By the first statement, we have $\sigma_n \in B_n$, and hence there exists $\tau_n \in B_\infty$ such that $R_{\infty,n}(\tau_n) = \sigma_n$. For any integers $n \geq m \geq 1$, the automorphisms $\sigma, \tau_n \in \mathrm{Aut}(T_\infty)$ agree on T_{m-1} and hence belong to the same coset of the subgroup W_{m-1}. Thus, we have

$$\sigma = \lim_{n\to\infty} \tau_n \in \overline{B}_\infty.$$

□

Corollary 2.13. *Let $n \geq 1$, and let G be a subgroup of $\mathrm{Aut}(T_n)$. Suppose that*

(1) *$R_{n,n-1}(G \cap B_n) \supseteq B_{n-1}$, and*
(2) *there is some $\lambda \in G \cap E_n$ such that $\mathrm{sgn}_n(\lambda, x_0) = -1$.*

Then G contains B_n.

Proof. Let $G' := G \cap B_n$. Then G' satisfies the hypotheses of Theorem 2.7, and hence $E_n \subseteq G' \subseteq G$. Since E_n is the kernel of the homomorphism $R_{n,n-1} : B_n \twoheadrightarrow B_{n-1}$, it follows that $B_n \subseteq G$. □

3. From the basilica to the arithmetic basilica

Fix a labeling of T_∞. As in Section 2, we now define two more particular automorphisms $\varepsilon, \theta \in \mathrm{Aut}(T_\infty)$, as follows. The definition of ε is simple: we specify that:

$$\mathrm{Par}(\varepsilon, x) = 1 \text{ for all nodes } x \text{ of } T_\infty. \tag{20}$$

It is immediate from Definition 1.2 that $Q(\varepsilon, x) = 1 + 4 + 4^2 + \cdots = -1/3 \in \mathbb{Z}_2$ for every node x, and hence that $P(\varepsilon, x) = -1 \in \mathbb{Z}_2$. In particular, $\varepsilon \in M_\infty$, with $P(\varepsilon) = -1$.

The definition of θ is more involved, proceeding inductively up the tree. First, define

$$\mathrm{Par}(\theta, x_0) := \mathrm{Par}(\theta, a) := \mathrm{Par}(\theta, b) := 0,$$

so that θ acts trivially on T_2. Then, once we have defined $\mathrm{Par}(\theta, x)$ at a particular node x, define $\mathrm{Par}(\theta, y)$ for each node y two levels above x by:

$$\begin{aligned} \mathrm{Par}(\theta, xaa) &:= \mathrm{Par}(\theta, xab) := 0, \\ \mathrm{Par}(\theta, xba) &:= 1, \quad \text{and} \\ \mathrm{Par}(\theta, xbb) &:= \mathrm{Par}(\theta, x). \end{aligned} \tag{21}$$

Because $\mathrm{Par}(\theta, yaa) = \mathrm{Par}(\theta, yab) = 0$ for any node y, we have $Q(\theta, x) = \mathrm{Par}(\theta, x)$ for all nodes x of the tree. Thus, according to Definition 1.2 and equation (21), we have

$$P(\theta, x) = \begin{cases} (-1)^0 + 2(1 + 0 - 0 - 0) = 3 & \text{if } \mathrm{Par}(\theta, x) = 0, \\ (-1)^1 + 2(1 + 1 - 0 - 0) = 3 & \text{if } \mathrm{Par}(\theta, x) = 1. \end{cases}$$

Thus, $\theta \in M_\infty$, with $P(\theta) = 3$.

Theorem 3.1. *The homomorphism $P : M_\infty \to \mathbb{Z}_2^\times$ is surjective, with kernel $\overline{B}_\infty$. That is, we have the short exact sequence*

$$0 \longrightarrow \overline{B}_\infty \longrightarrow M_\infty \xrightarrow{P} \mathbb{Z}_2^\times \longrightarrow 0$$

Proof. By Theorem 1.4, the map P is a homomorphism, and by Corollary 2.12, its kernel is $\overline{B}_\infty$. It remains to show that P is surjective.

Because the automorphisms ε, θ defined in equations (20) and (21) belong to M_∞, with $P(\varepsilon) = -1$ and $P(\theta) = 3$, the image of P contains the subgroup $\langle -1, 3\rangle$ of $\mathbb{Z}_2^\times$ generated by -1 and 3. In fact, since P is continuous and M_∞ is compact, it follows that the image of P contains the closure of the subgroup $\langle -1, 3\rangle$. However, $\{-1, 3\}$ is a set of topological generators for $\mathbb{Z}_2^\times$; therefore, the image of P is all of $\mathbb{Z}_2^\times$. □

Theorem 3.2. *Fix $n \geq 1$. Then*

(1) *E_n is a subgroup of U_n, with* $[U_n : E_n] = \begin{cases} 1 & \textit{if } n = 1 \textit{ or } n \textit{ is even,} \\ 2 & \textit{if } n \geq 3 \textit{ is odd.} \end{cases}$

(2) *$M_n = R_{\infty,n}(M_\infty)$.*

(3) *If $n \geq 2$, then $U_n \cong E_{n-1} \times E_{n-1}$.*

As usual, the isomorphism of Theorem 3.2.(3) is of groups acting on T_n, not just of abstract groups. For $E_{n-1} \times E_{n-1}$, we mean that the first copy of E_{n-1} acts on the copy of T_{n-1} rooted at node a, and the second acts on the copy of T_{n-1} rooted at b.

Proof of Theorem 3.2. **(1)**: From Definitions 1.3 and 2.3, and by Corollary 2.12, we have

$$E_n = \ker(P : U_n \to (\mathbb{Z}/2^j\mathbb{Z})^\times), \quad \text{where } j := \lfloor (n+1)/2 \rfloor.$$

In particular, E_n is a subgroup of U_n. Observe that

$$P(\sigma, x_0) \equiv 1 \pmod{2^\ell} \quad \text{for all } \sigma \in U_n, \quad \text{where } \ell := \lfloor n/2 \rfloor. \tag{22}$$

If n is even, then $\ell = j$, and hence $P(\sigma, x_0) \equiv 1 \pmod{2^j}$ for all $\sigma \in U_n$, whence $U_n = E_n$. Similarly, if $n = 1$, then because both of the conditions $P(\sigma, x_0) \equiv 1 \pmod{2^0}$ and $P(\sigma, x_0) \equiv 1 \pmod{2^1}$ are vacuous, we have $E_1 = U_1 = \text{Aut}(T_1)$.

For $n \geq 3$ odd, we have $\ell = j - 1 \geq 1$. Thus, by equation (22), restricting $P : M_n \to (\mathbb{Z}/2^j\mathbb{Z})^\times$ to U_n yields a homomorphism

$$P : U_n \to \{1 + 2^\ell + 2^j\mathbb{Z}, 1 + 2^j\mathbb{Z}\} \cong \mathbb{Z}/2\mathbb{Z}.$$

By Corollary 2.12, the kernel of this map is precisely E_n. We claim it is also surjective. Indeed, by Theorem 3.1, there is some $\tau \in M_\infty$ with $P(\tau, x_0) = 1 + 2^\ell$. Because $P(\tau, x_0) \equiv 1 \pmod{2^\ell}$, we have $R_{\infty,n-1}(\tau) \in B_{n-1}$, and hence there exists $\eta \in B_\infty$ for which $R_{\infty,n-1}(\tau) = R_{\infty,n-1}(\eta)$. Let $\sigma := R_{\infty,n}(\tau\eta^{-1})$. Then

$$\sigma \in U_n, \quad \text{and} \quad P(\sigma, x_0) = 1 + 2^\ell + 2^j\mathbb{Z},$$

proving the claim. Thus, $[U_n : E_n] = |\mathbb{Z}/2\mathbb{Z}| = 2$.

(2): It is immediate from Definition 1.3 that $M_n \supseteq R_{\infty,n}(M_\infty)$.

Conversely, given $\sigma \in M_n$, there is some $\tau \in M_\infty$ such that $P(\tau, x_0) \equiv P(\sigma, x_0) \pmod{2^j}$, by the surjectivity of P in Theorem 3.1. (As before, we have $j := \lfloor (n+1)/2 \rfloor$.) Let $\eta := \sigma R_{\infty,n}(\tau^{-1}) \in M_n$, which satisfies $P(\eta, x_0) \equiv 1 \pmod{2^j}$. By Corollary 2.12, then, we have $\eta \in B_n$, and in fact $\eta = R_{\infty,n}(\tilde{\eta})$ for some $\tilde{\eta} \in B_\infty$. Hence, $\tilde{\eta}\tau \in M_\infty$, and $\sigma = R_{\infty,n}(\tilde{\eta}\tau)$, as desired.

(3): Because $n \geq 2$, each $\sigma \in U_n$ fixes both nodes a and b at level 1 of the tree T_n. As in Remark 2.2, restricting σ to the subtrees rooted at each of a and b yields automorphisms $\sigma_a, \sigma_b \in \operatorname{Aut}(T_{n-1})$. In fact, it is immediate from the definition of M_n that $\sigma_a, \sigma_b \in M_{n-1}$, since $\sigma \in M_{n-1}$. Moreover, we have $\sigma_a, \sigma_b \in U_{n-1}$, since σ_a and σ_b act trivially on the subtrees of $n-2$ levels above each of a and b. Furthermore, because σ acts trivially on the T_{n-1} rooted at x_0, we have

$$P(\sigma, a) \equiv P(\sigma, b) \equiv P(\sigma, x_0) \equiv 1 \pmod{2^{\lfloor n/2 \rfloor}},$$

and hence $\sigma_a, \sigma_b \in E_{n-1}$. Thus, the function $\sigma \mapsto (\sigma_a, \sigma_b)$ maps U_n into $E_{n-1} \times E_{n-1}$, and it is clearly a homomorphism, with trivial kernel.

It remains to show that this function is onto. Given $\sigma_a, \sigma_b \in E_{n-1}$, define

$$\sigma := (\sigma_a, \sigma_b) \in \operatorname{Aut}(T_n)$$

in the notation of Remark 2.2. That is, σ fixes the two nodes a and b at level 1, acts as σ_a on the subtree rooted at a, and acts as σ_b on the subtree rooted at b. It suffices to show that $\sigma \in U_n$. Clearly σ acts trivially on the bottom $n-1$ levels of T_n, so it remains to show that σ satisfies condition (6) of Definition 1.3 for every $0 \leq m \leq n-1$.

Let $c := P(\sigma, x_0)$, and let $\ell := \lfloor n/2 \rfloor$. Considering the (trivial) action of σ on the copy of T_{n-1} comprising the bottom $n-1$ levels of T_n, we have

$$c = P(\sigma, x_0) \equiv 1 \pmod{2^\ell} \tag{23}$$

by Definition 1.2, because all of the nodes y of T_{n-1} for which $\operatorname{Par}(\sigma, y) = 1$ lie at level $n-1$. If n is even, these nodes do not appear in the formula (3) defining $P(\sigma, x_0)$. If n is odd, their terms show up with a coefficient of $\pm 2^\ell$ and hence do not affect equation (23). Thus, for any $0 \leq m \leq n-1$ and any node x of T_n at level n, then setting $j := \lfloor (n-m+1)/2 \rfloor$, we have three cases, as follows.

First, if $x = x_0$, then clearly $P(\sigma, x) = c \equiv c \pmod{2^j}$. Second, if $x = ay$ for some $y \in \{a, b\}^{m-1}$, then $j \leq \ell$, and hence

$$P(\sigma, x) = P(\sigma_a, y) \equiv 1 \equiv c \pmod{2^j}$$

by equation (23). Third, if $x = by$ for some $y \in \{a, b\}^{m-1}$, then $P(\sigma, x) = c \pmod{2^j}$ by the same reasoning as in the $x = ay$ case, this time applied to σ_b. Thus, we have verified condition (6) for σ, and hence $\sigma \in U_n$, as desired. □

Theorem 3.3. *Fix $n \geq 2$. Then $|E_n| = 2^{e_n}$, $|U_n| = 2^{u_n}$, and $|M_n| = 2^{m_n}$, where*

$$\begin{aligned} e_n &= \frac{2^n}{3} + \begin{cases} 2/3 & \text{if } n \text{ is even,} \\ 1/3 & \text{if } n \text{ is odd,} \end{cases} \\ u_n &= \frac{2^n}{3} + \begin{cases} 2/3 & \text{if } n \text{ is even,} \\ 4/3 & \text{if } n \text{ is odd and } n \geq 3, \\ 1/3 & \text{if } n = 1 \end{cases} \\ m_n &= \frac{2^{n+1}}{3} + n - \begin{cases} 5/3 & \text{if } n \text{ is even,} \\ 4/3 & \text{if } n \text{ is odd.} \end{cases} \end{aligned} \tag{24}$$

Proof. For $n \geq 1$, let e_n, u_n, m_n be the integers given by formulas (24), and define

$$e'_n := \log_2 |E_n|, \quad u'_n := \log_2 |u_n|, \quad m'_n := \log_2 |M_n|.$$

We must show that $e'_n = e_n$, $u'_n = u_n$, and $m'_n = m_n$ for all $n \geq 1$. For $n = 1$, we have $E_n = U_n = M_n = \operatorname{Aut}(T_1) \cong \mathbb{Z}/2\mathbb{Z}$, so that $e'_n = u'_n = m'_n = 1$. Clearly $e_n = u_n = m_n = 1$ as well.

Proceeding inductively, given $n \geq 2$, assume the equalities for $n-1$. By Theorem 3.2.(3), we have $|U_n| = |E_{n-1}|^2$, and hence

$$u'_n = 2e'_{n-1} = 2e_{n-1} = u_n,$$

where the identity $2e_{n-1} = u_n$ is immediate from formulas (24). Next, Theorem 3.2.(1) yields $u'_n = e'_n$ for n even, and $u'_n = e'_n + 1$ for $n \geq 3$ odd. Thus,

$$\begin{aligned} e'_n &= u'_n = u_n = e_n && \text{if } n \text{ is even, and} \\ e'_n &= u'_n - 1 = u_n - 1 = e_n && \text{if } n \text{ is odd,} \end{aligned}$$

where again, each closing equality is by formulas (24). Finally, since $R_{n,n-1} : M_n \to M_{n-1}$ is a surjective homomorphism with kernel U_n, we have $m'_n = m'_{n-1} + u'_n$, and hence

$$m'_n = m'_{n-1} + u'_n = m_{n-1} + u_n = m_n,$$

where again, the last equality is by formulas (24). □

To help clarify formulas (24), the following table gives the orders of the groups E_n, U_n, M_n, and $\operatorname{Aut}(T_n)$ for some small values of n.

n	1	2	3	4	5	6	7	8	9	10
$\lvert E_n \rvert$	2^1	2^2	2^3	2^6	2^{11}	2^{22}	2^{43}	2^{86}	2^{171}	2^{342}
$\lvert U_n \rvert$	2^1	2^2	2^4	2^6	2^{12}	2^{22}	2^{44}	2^{86}	2^{172}	2^{342}
$\lvert M_n \rvert$	2^1	2^3	2^7	2^{13}	2^{25}	2^{47}	2^{91}	2^{177}	2^{349}	2^{691}
$\lvert \operatorname{Aut}(T_n) \rvert$	2^1	2^3	2^7	2^{15}	2^{31}	2^{63}	2^{127}	2^{255}	2^{511}	2^{1023}

4. Embedding arboreal Galois groups in the arithmetic basilica

We now return from abstract subgroups of $\operatorname{Aut}(T_n)$ to arboreal Galois groups. We remind the reader of the following notation, which we set for the remainder of the paper.

K:	a field of characteristic different from 2, with algebraic closure $\overline{K}$
f:	the polynomial $f(z) = z^2 - 1$
x_0:	an element of K, to serve as the root of our preimage tree.
K_n:	for each $n \geq 0$, the extension field $K_n := K(f^{-n}(x_0))$
K_∞:	the union $K_\infty = \bigcup_{n \geq 1} K_n$ in $\overline{K}$
G_n:	the Galois group $G_n := \operatorname{Gal}(K_n/K_0)$
G_∞:	the Galois group $G_\infty := \operatorname{Gal}(K_\infty/K_0)$

In this section, we show that the arboreal Galois groups G_n embed in the arithmetic basilica groups M_n.

Lemma 4.1. *Let $y \in \overline{K}$, and let $\alpha_1, \alpha_2 \in f^{-2}(y)$ with $f(\alpha_2) = -f(\alpha_1)$. Then*

$$(\alpha_1\alpha_2)^2 = -y.$$

Proof. Write $u = f(\alpha_1)$. Then $\alpha_1^2 = u + 1$ and $\alpha_2^2 = -u + 1$. (See Figure 3.) Thus,

$$(\alpha_1\alpha_2)^2 = (u+1)(-u+1) = -(u^2 - 1) = -f(u) = -y. \qquad \square$$

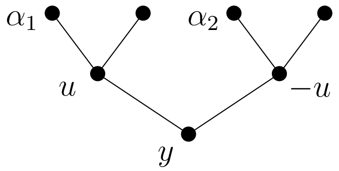

FIGURE 3. Lemma 4.1: $(\alpha_1\alpha_2)^2 = -y$

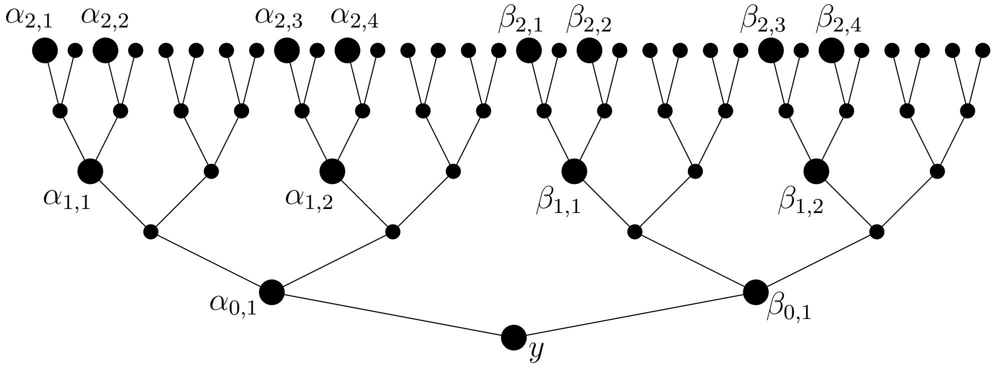

FIGURE 4. Lemma 4.2 for $m = 2$.

Lemma 4.2. *Let $m \geq 0$, and let $y \in \overline{K}$. Let $\alpha_{0,1} \in f^{-1}(y)$, and define $\beta_{0,1} := -\alpha_{0,1}$. For each $i = 1, \ldots, m$, choose points $\{\alpha_{i,j}, \beta_{i,j} : 1 \leq j \leq 2^i\} \subseteq f^{-(2i+1)}(y)$ so that*

$$f^{-2}\big(\alpha_{i-1,\ell}\big) = \{\pm\alpha_{i,2\ell-1}, \pm\alpha_{i,2\ell}\} \quad \textit{and} \quad f^{-2}\big(\beta_{i-1,\ell}\big) = \{\pm\beta_{i,2\ell-1}, \pm\beta_{i,2\ell}\}$$

for each $\ell = 1, \ldots, 2^{i-1}$, as in Figure 4. Define

$$\gamma_m := \prod_{j=1}^{2^m} \alpha_{m,j} \quad \textit{and} \quad \delta_m := \prod_{j=1}^{2^m} \beta_{m,j}.$$

Then $(-\gamma_m)^{2^m} = \beta_{0,1}$ and $(-\delta_m)^{2^m} = \alpha_{0,1}$. Moreover, γ_m/δ_m is a primitive 2^{m+1}-th root of unity.

Proof. The conclusion is trivially true for $m = 0$. Proceeding inductively, consider $m \geq 1$, and assume it holds for $m-1$. For each $\ell = 1, \ldots, 2^{m-1}$, we have

$$\big(\alpha_{m,2\ell-1}\alpha_{m,2\ell}\big)^2 = -\alpha_{m-1,\ell} \quad \text{and} \quad \big(\beta_{m,2\ell-1}\beta_{m,2\ell}\big)^2 = -\beta_{m-1,\ell}$$

by Lemma 4.1. It follows immediately that

$$(-\gamma_m)^2 = \begin{cases} \gamma_{m-1} & \text{if } m \geq 2, \\ -\gamma_{m-1} & \text{if } m = 1, \end{cases} \quad \text{and} \quad (-\delta_m)^2 = \begin{cases} \delta_{m-1} & \text{if } m \geq 2, \\ -\delta_{m-1} & \text{if } m = 1. \end{cases}$$

Raising each to the power 2^{m-1}, which is 1 if $m = 1$ and even for $m \geq 2$, we have

$$(-\gamma_m)^{2^m} = (-\gamma_{m-1})^{2^{m-1}} = \beta_{0,1} \quad \text{and} \quad (-\delta_m)^{2^m} = (-\delta_{m-1})^{2^{m-1}} = \alpha_{0,1},$$

as desired. The final statement is immediate from the fact that $\beta_{0,1}/\alpha_{0,1} = -1$. □

By Lemma 4.2, the field K_∞ formed by adjoining all preimages $f^{-n}(x_0)$ to K_0 contains all 2-power roots of unity. We now use these roots of unity to label the tree T_∞ of preimages $\mathrm{Orb}_f^-(x_0)$ to be compatible with the action of Galois.

Lemma 4.3. *Choose a sequence $\{\zeta_2, \zeta_4, \zeta_8, \ldots\}$ of primitive 2-power roots of unity in $\overline{K}$, in such a way that $(\zeta_{2^m})^2 = \zeta_{2^{m-1}}$ for each $m \geq 1$. It is possible to label the tree T_∞ of preimages $\mathrm{Orb}_f^-(x_0)$ in such a way that for every node y of the tree and for every $i \geq 0$, we have*

$$\left(\prod_{s_1,\ldots,s_i \in \{a,b\}} [yas_1as_2 \cdots as_ia] \right) \left(\prod_{s_1,\ldots,s_i \in \{a,b\}} [ybs_1as_2 \cdots as_ia] \right)^{-1} = \zeta_{2^{i+1}}, \tag{25}$$

where $[w]$ denotes the element of $\overline{K}$ that appears in the tree as a node with label w.

Lemma 4.3 says that it is always possible to choose a labeling of the tree of preimages $\mathrm{Orb}_f^-(x_0)$ so that for the nodes $\alpha_{i,j}$ and $\beta_{i,j}$ highlighted in such in Figure 4, we have

$$\frac{\alpha_{2,1}\alpha_{2,2}}{\beta_{2,1}\beta_{2,2}} = \zeta_4, \quad \frac{\alpha_{3,1}\alpha_{3,2}\alpha_{3,3}\alpha_{3,4}}{\beta_{3,1}\beta_{3,2}\beta_{3,3}\beta_{3,4}} = \zeta_8, \quad \text{and so on.}$$

In fact, it says that we can label the tree so that these relationships hold for the subtree based at each node y of the full tree. By contrast, Lemma 4.2 says that even after applying an arbitrary automorphism τ of T_∞, any such product of elements of $f^{-(2m+1)}(y)$ is *some* primitive 2^{m+1}-root of unity, albeit not necessarily the particular root $\zeta_{2^{m+1}}$.

Proof of Lemma 4.3. We will label the tree of preimages inductively, starting from the root point x_0 and working our way up. To begin, label the two preimages of x_0 arbitrarily as a and b. Similarly, arbitrarily label the two preimages of a as aa and ab, and the two preimages of b as ba and bb. Thus, we have a labeling on the copy of T_2 rooted at x_0. For each of the nodes $y \in \{x_0, a, b\}$, we have $(ya)/(yb) = -1 = \zeta_2$. Thus, the desired identity (25) holds at every node of T_1 for $i = 0$.

For each successive $n \geq 3$, suppose that we have labeled T_{n-1} in such a way that for every node y at every level $0 \leq \ell \leq n-2$ of T_{n-1}, and for every $0 \leq i \leq \lfloor (n-\ell-2)/2 \rfloor$, the identity of equation (25) holds. For each node x at level $n-1$, label the two points of $f^{-1}(x)$ arbitrarily as xa and xb. We will now adjust these labels that we have just applied at the n-th level of the tree.

If $n = 2m+1$ is odd, consider the product on the left side of equation (25) for $y = x_0$ with $i = m$; or if $n = 2m+2$ is even, consider the product on the left side of equation (25) for each of $y = x_0a$ and $y = x_0b$ with $i = m$. As in the proof of Lemma 4.2, it is immediate from Lemma 4.1 that the square of this product is precisely the corresponding quantity for y with $i = m-1$. (When $m = 1$ each half has a negative sign, but the negatives cancel in that case.) By our successful labeling of T_{n-1}, this square is ζ_{2^m}. Thus, the original product is $\pm\zeta_{2^{m+1}}$. If it is $-\zeta_{2^{m+1}}$, exchange the labels of the two level-n nodes $ybaa \cdots aa$ and $ybaa \cdots ab$; otherwise, make no label changes for now. Since these two points in $f^{-n}(x_0)$ are negatives of each other, we have ensured that equation (25) holds for y with $i = m$.

Next, consider the product on the left side of equation (25) with $i = m-1$ for each node y at level 2 of the tree (if n is odd) or at level 3 (if n is even). By Lemma 4.1 and our labeling of T_{n-1} again, the square of this product is $\zeta_{2^{m-1}}$, and hence the product itself is $\pm\zeta_{2^m}$. If it is $-\zeta_{2^m}$, exchange the labels of the two level-n nodes $ybaa\cdots aa$ and $ybaa\cdots ab$; otherwise, make no label changes for now. Since these two points in $f^{-n}(x_0)$ are negatives of each other, we have ensured that equation (25) holds for y with $i = m-1$. In addition, because both of these nodes have labels beginning $yb\cdots$, they did not show up in the product of equation (25) for nodes lower on the tree than y, so we have not disrupted our previous arrangements.

Continue in this fashion, considering nodes at successive even levels ℓ of the tree (if n is odd) or odd levels ℓ of the tree (if n is even). For each such node y, choose whether or not to switch the labels of $ybaa\cdots aa$ and $ybaa\cdots ab$ to ensure that equation (25) holds for y with $i = (n-\ell-1)/2$. Once we have finished working our way up through level $\ell = n-1$, we have labeled T_n so that for every node y at every level $0 \le \ell \le n-1$ of T_n, and for every $0 \le i \le \lfloor (n-\ell-1)/2 \rfloor$, the identity of equation (25) holds. Thus, our inductive construction is complete. □

The following result is a strengthened version of statement (1) of our Main Theorem.

Theorem 4.4. *With the notation given at the start of Section 4, choose a sequence* $\{\zeta_2, \zeta_4, \zeta_8, \ldots\}$ *of primitive* 2*-power roots of unity in* K_∞*, with* $(\zeta_{2^m})^2 = \zeta_{2^{m-1}}$ *for each* $m \ge 1$*. Label the tree* T_∞ *of preimages* $\operatorname{Orb}_f^-(x_0)$ *as in Lemma 4.3.*

Consider the embedding of G_∞ *in* $\operatorname{Aut}(T_\infty)$ *induced by its action on* $\operatorname{Orb}_f^-(x_0)$ *Then the image of this embedding is contained in the arithmetic basilica group* M_∞*. Moreover,*

$$\sigma(\zeta) = \zeta^{P(\sigma)} \qquad \textit{for every 2-power root of unity } \zeta \in K_\infty \textit{ and every } \sigma \in G_\infty,$$

where $P(\sigma) = P(\sigma, x_0)$ *is the map of Definition 1.2.*

Proof. It suffices to show that $\sigma(\zeta_{2^m}) = \zeta_{2^m}^{P(\sigma,y)}$ for every $\sigma \in G_\infty$, every $m \ge 1$, and every $y \in \operatorname{Orb}_f^-(x_0)$ Throughout the proof, then, fix such σ, m, and y.

By hypothesis, for any point $w \in \operatorname{Orb}_f^-(x_0)$ and any $i \ge 0$, we have

$$\prod_{t_1,\ldots,t_i} \big[\sigma(wa)t_1at_2\cdots at_ia\big] = \zeta_{2^{i+1}}^{-\operatorname{Par}(\sigma,w)} \prod_{t_1,\ldots,t_i} \big[\sigma(w)at_1at_2\cdots at_ia\big], \tag{26}$$

by equation (25) of Lemma 4.3 applied to $\sigma(w)$, and by equation (1) applied to $\operatorname{Par}(\sigma, w)$. Each product in equation (26) is over $t_1, \ldots, t_i \in \{a, b\}$; and for $i = 0$, we understand it to say $[\sigma(wa)[= \zeta_2^{-\operatorname{Par}(\sigma,w)}[\sigma(w)a]$.

In addition, since the two-element sets $\{\sigma(wa), \sigma(wb)\}$ and $\{\sigma(w)a, \sigma(w)b\}$ always coincide, we have

$$\prod_{s\in\{a,b\}} \big[\sigma(w_1s)w_2\big] = \prod_{s\in\{a,b\}} \big[\sigma(w_1)sw_2\big]. \tag{27}$$

for any strings w_1 and w_2 of the symbols a, b. Thus, if we define

$$P_j(\sigma, w) := \sum_{t_1,\ldots,t_j\in\{a,b\}} \operatorname{Par}(\sigma, wt_1at_2a\cdots at_j),$$

then for any node x of the tree and any $m \geq 1$, we have

$$\begin{aligned}\prod \big[\sigma(xs_1as_2\cdots as_{m-1}a)\big] &= \zeta_2^{-P_{m-1}(\sigma,x)} \prod \big[\sigma(xs_1as_2\cdots as_{m-1})a\big] \\ &= \zeta_2^{-P_{m-1}(\sigma,x)} \prod \big[\sigma(xs_1as_2\cdots a)s_{m-1}a\big] \\ &= \zeta_2^{-P_{m-1}(\sigma,x)}\zeta_4^{-P_{m-2}(\sigma,x)} \prod \big[\sigma(xs_1as_2\cdots s_{m-2})as_{m-1}a\big] \\ &= \cdots \\ &= \left(\prod_{j=1}^{m-1} \zeta_{2^{m-j}}^{-P_j(\sigma,x)}\right) \prod \big[\sigma(x)s_1as_2\cdots as_{m-1}a\big],\end{aligned} \tag{28}$$

where each undecorated product is over $s_1,\ldots,s_{m-1} \in \{a,b\}$. In proving equation (28), we have alternately applied equations (26) and (27). Specifically, we used equation (26) with $i = 0$ and $w = xs_1a\cdots as_{m-1}$ at the first equality, then with $i = 1$ and $w = xs_1a\cdots as_{m-2}$ at the third, and so on through $i = m-2$ with $w = x$. We then used (27) at the second equality with $w_1 = xs_1a\cdots as_{m-2}a$ and $w_2 = a$, then with $w_1 = xs_1a\cdots as_{m-3}a$ and $w_2 = as_{m-1}a$ at the fourth, and so on.

Applying equation (28) to both $x = ya$ and $x = yb$, and substituting the results in equation (25) with $i = m-1$, we obtain

$$\begin{aligned}\sigma(\zeta_{2^m}) &= \frac{\prod\big[\sigma(yas_1as_2\ldots as_{m-1}a)\big]}{\prod\big[\sigma(ybs_1as_2\ldots as_{m-1}a)\big]} \\ &= \prod_{j=1}^{m-1} \zeta_{2^{m-j}}^{P_j(\sigma,yb)-P_j(\sigma,ya)} \cdot \frac{\prod\big[\sigma(ya)s_1as_2\ldots as_{m-1}a\big]}{\prod\big[\sigma(yb)s_1as_2\ldots as_{m-1}a\big]},\end{aligned} \tag{29}$$

where each undecorated product is again over $s_1,\ldots,s_{m-1} \in \{a,b\}$. Since $\zeta_{2^i}^2 = \zeta_{2^{i-1}}$ for each i, the first product in expression (29) is $\zeta_{2^m}^M$, where

$$\begin{aligned}M &:= \sum_{j=1}^{m-1} 2^j\big(P_j(\sigma,yb) - P_j(\sigma,ya)\big) \\ &\equiv 2\sum_{t\in\{a,b\}} Q(\sigma,ybt) - 2\sum_{t\in\{a,b\}} Q(\sigma,yat) \pmod{2^m}.\end{aligned}$$

where $Q(\sigma,x)$ is as defined in equation (2). On the other hand, by equation (25) applied to $\sigma(y)$, the quotient of two products in expression (29) is ζ_{2^m} if $\mathrm{Par}(\sigma,y) = 0$, or $\zeta_{2^m}^{-1}$ if $\mathrm{Par}(\sigma,y) = 1$. Thus, equation (29) becomes

$$\sigma(\zeta_{2^m}) = \zeta_{2^m}^P, \quad \text{where} \quad P = (-1)^{\mathrm{Par}(\sigma,y)} + M = P(\sigma,y). \qquad \square$$

Corollary 4.5. *Fix notation and a tree labeling as in Theorem 4.4. Let $n \geq 1$, and let $m := \lfloor (n+1)/2 \rfloor$, so that $\zeta_{2^m} \in K_n$. Consider the embedding of $G_n = \mathrm{Gal}(K_n/K)$ in $\mathrm{Aut}(T_n)$ induced by its action on $\coprod_{i=0}^n f^{-i}(x_0)$. Then*

1. *The image of G_n under this embedding is contained in M_n.*
2. *The image of $\mathrm{Gal}(K_n/K(\zeta_{2^m})) \subseteq G_n$ under this embedding is contained in B_n.*

Proof. We have the following commutative diagram

$$\begin{tikzcd} G_\infty \arrow[r] \arrow[d] & \mathrm{Aut}(T_\infty) \arrow[d, "R_{\infty,n}"] \\ G_n \arrow[r] & \mathrm{Aut}(T_n) \end{tikzcd}$$

where the horizontal maps are the embeddings induced by the action of G_n and G_∞ on the tree of preimages, the vertical map on the left is the quotient induced by restricting to K_n, and the vertical map on the right is the quotient $R_{\infty,n}$ induced by restricting to T_n. By Theorem 4.4, the image of the top map is contained in $M_\infty \subsetneq \mathrm{Aut}(T_\infty)$, and by Theorem 3.2, we have $R_{\infty,n}(M_\infty) = M_n$. Since the quotient $G_\infty \to G_n$ is surjective, the image of the bottom map is contained in M_n, proving statement (1).

Given $\sigma \in \mathrm{Gal}(K_n/K(\zeta_{2^m}))$, we have

$$\zeta_{2^m}^{P(\sigma,x_0)} = \sigma(\zeta_{2^m}) = \zeta_{2^m},$$

where the first equality is by Theorem 4.4, and the second is because σ fixes $K(\zeta_{2^m})$. Therefore, $P(\sigma, x_0) \equiv 1 \pmod{2^m}$, and hence the image of σ in M_n lies in the subgroup B_n'' from Definition 2.3.(3). Thus, by Corollary 2.12, the image of σ lies in B_n, proving statement (2). □

5. Surjectivity of the Galois group in the arithmetic basilica

Having shown that the arboreal Galois group $G_\infty := \mathrm{Gal}(K_\infty/K)$ of $f(z) = z^2 - 1$ embeds in the arithmetic basilica M_∞, we now wish to prove that the embedding is surjective under certain conditions. The following variant of Lemma 4.2 will prove useful to that end. As in Corollary 4.5, by restricting to T_n, we may consider $G_n := \mathrm{Gal}(K_n/K)$ to be a subgroup of M_n. In particular, the subgroup $\mathrm{Gal}(K_n/K_{n-1})$ is simply $G_n \cap U_n$, which, for n even, is the same as $G_n \cap E_n$, by Theorem 3.2.(1).

Lemma 5.1. *Let $m \geq 1$, and let $\alpha_{0,1} \in K$. For each $i = 1, \ldots, m$, choose points $\{\alpha_{i,j} : 1 \leq j \leq 2^i\} \subseteq f^{-(2i)}(\alpha_{0,1})$ so that*

$$f^{-2}\big(\alpha_{i-1,\ell}\big) = \{\pm\alpha_{i,2\ell-1}, \pm\alpha_{i,2\ell}\} \quad \textit{for each } \ell = 1, \ldots, 2^{i-2}.$$

Define $\gamma_m := \prod_{j=1}^{2^m} \alpha_{m,j} \in K_{2m}$. Then

(1) $\gamma_m^{2^m} = -\alpha_{0,1}$.

(2) *Let $\sigma \in \mathrm{Gal}(K_{2m}/K_{2m-1}) = G_{2m} \cap E_{2m}$. Then*

$$\frac{\sigma(\gamma_m)}{\gamma_m} = \mathrm{sgn}_{2m}(\sigma, \alpha_{0,1}).$$

Proof. **(1)**: The statement is true for $m = 1$ by Lemma 4.1. Proceeding inductively, consider $m \geq 2$, and assume it holds for $m - 1$. For each $\ell = 1, \ldots, 2^{m-1}$, we have $(\alpha_{m,2\ell-1}\alpha_{m,2\ell})^2 = -\alpha_{m-1,\ell}$ by Lemma 4.1. Since $m - 1 \geq 1$, it follows immediately that $(\gamma_m)^2 = \gamma_{m-1}$, and hence $(\gamma_m)^{2^m} = \gamma_{m-1}^{2^{m-1}} = -\alpha_{0,1}$.

(2): The two preimages of $\alpha_{0,1}$ are $w := f(\alpha_{1,1})$ and $-w = f(\alpha_{1,2})$. By Definition 2.4 and Lemma 2.5.(2), we have

$$\begin{aligned} \operatorname{sgn}_{2m}(\sigma, \alpha_{0,1}) &= \operatorname{sgn}_{2m-1}(\sigma, w) \operatorname{sgn}_{2m-1}(\sigma, -w) \\ &= \operatorname{sgn}_{2m-2}(\sigma, \alpha_{1,1}) \operatorname{sgn}_{2m-2}(\sigma, \alpha_{1,2}). \end{aligned} \tag{30}$$

For $m = 1$, we have $\gamma_1 = \alpha_{1,1}\alpha_{1,2}$, and hence

$$\frac{\sigma(\gamma_1)}{\gamma_1} = \frac{\sigma(\alpha_{1,1})}{\alpha_{1,1}} \cdot \frac{\sigma(\alpha_{1,2})}{\alpha_{1,2}} = \operatorname{sgn}_1(\sigma, w) \operatorname{sgn}_1(\sigma, -w) = \operatorname{sgn}_2(\sigma, \alpha_{0,1}).$$

Proceeding inductively, assume now that $m \geq 2$, and that statement (2) is true for $m-1$. In particular, assume that it holds for the tree with root point $\alpha_{1,i}$ over the field $K(\alpha_{1,i})$, for each of $i = 1, 2$. Define

$$\delta_{m-1,1} := \prod_{j=1}^{2^{m-1}} \alpha_{m,j} \quad \text{and} \quad \delta_{m-1,2} := \prod_{j=2^{m-1}+1}^{2^m} \alpha_{m,j},$$

so that $\gamma_m = \delta_{m-1,1}\delta_{m-1,2}$. By our inductive hypothesis and equation (30), then,

$$\frac{\sigma(\gamma_m)}{\gamma_m} = \frac{\sigma(\delta_{m-1,1})}{\delta_{m-1,1}} \cdot \frac{\sigma(\delta_{m-1,2})}{\delta_{m-1,2}} = \operatorname{sgn}_{2m-2}(\sigma, \alpha_{1,1}) \operatorname{sgn}_{2m-2}(\sigma, \alpha_{1,2}) = \operatorname{sgn}_{2m}(\sigma, \alpha_{0,1}). \quad \square$$

Lemma 5.2. *Let $n \geq 2$, and suppose that $G_n \cong M_n$; if $n = 2$, suppose further that $i \notin K_n$, where $i = \zeta_4$ denotes a primitive fourth root of unity. Let $y \in K_{n-2}$ with the property that y has no square root in $K_{n-2}(i)$. Then y has no fourth root in $K_n(i)$.*

Proof. **Case 1**. Suppose first that $n \geq 5$, so that $i \in K_3 \subseteq K_{n-2}$. If y has a fourth root $\gamma \in K_n$, then $K_{n-2}(\gamma)/K_{n-2}$ is a cyclic extension of degree 4, since $\gamma^2 \notin K_{n-2}$ by hypothesis. Thus, $H := \operatorname{Gal}(K_n/K_{n-2})$ has a quotient J isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Let $\sigma \in H$ be an element such that the image of σ in J has order 4.

Observe that H acts as $M_2 = \operatorname{Aut}(T_2)$ on each of the 2^{n-2} copies of T_2 rooted at points of $f^{-(n-2)}(x_0)$. Since the image of σ in J has order 4, the resulting composition

$$H \twoheadrightarrow \operatorname{Aut}(T_2) \to J$$

must be surjective for at least one such copy of T_2. Thus, we have a surjective homomorphism $\operatorname{Aut}(T_2) \twoheadrightarrow J$. However, $\operatorname{Aut}(T_2)$ is isomorphic to the 8-element dihedral group D_4, which has no quotients isomorphic to $\mathbb{Z}/4\mathbb{Z}$. This contradiction completes the proof for $n \geq 5$.

Case 2. Suppose $n = 2$. Let $H := \operatorname{Gal}(K_2(i)/K_0(i))$, which is isomorphic to a subgroup of $M_2 = \operatorname{Aut}(T_2)$. Since $[K_2(i) : K_2] = [K_0(i) : K_0] = 2$ and $\operatorname{Gal}(K_2/K_0) \cong M_2$, we must have $H \cong M_2$. If y has a fourth root $\gamma \in K_2(i)$, then as in Case 1, $M_2 \cong D_4$ would have a quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$, a contradiction.

Case 3. Suppose $n = 3$. Let $H := \operatorname{Gal}(K_3/K_1(i))$, which must be

$$H = \ker(R_{3,1} : M_3 \to M_1) \cap B_3,$$

since its elements fix i and the points of $f^{-1}(x_0)$, with no other restrictions. Thus, H acts as M_2 on each of the two copies of T_2 rooted at the points of $f^{-1}(x_0)$, although any $\tau \in H$ must act as an even permutation on the eight points of $f^{-3}(x_0)$.

If y has a fourth root $\gamma \in K_3$, then as in Case 1, at least one of the two copies of $M_2 \cong D_4$ would have a quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$, a contradiction.

Case 4. Suppose $n = 4$. Let $H := \mathrm{Gal}(K_4/K_2(i))$, which must be

$$H = \ker(R_{4,2} : M_4 \to M_2) \cap B_4,$$

since its elements fix i and the points of $f^{-2}(x_0)$, with no other restrictions. Thus, H again acts as M_2 on each of the four copies of T_2 rooted at the points of $f^{-2}(x_0)$. The same argument as in Case 1 therefore applies: if y has a fourth root in K_4, then at least one of the four copies of $M_2 \cong D_4$ would have a quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$, a contradiction. □

Lemma 5.3. *Suppose that* $[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] = 16$. *Then*

(1) $[K(i, \sqrt{1+x_0}) : K] = 4$, *so that* $K(i)$ *does not contain a square root of* $1 + x_0$.
(2) $K_1(i)$ *does not contain a square root of* $-x_0$.
(3) K_2 *does not contain a primitive fourth root of* 1.
(4) *Assuming* $G_3 \cong M_3$, *then* K_3 *does not contain a primitive eighth root of* 1.
(5) *Assuming* $G_4 \cong M_4$, *then* K_4 *does not contain a primitive eighth root of* 1.

Proof. **(1)**: If $[K(i, \sqrt{1+x_0}) : K] < 4$, then $\sqrt{1+x_0} \in K(i)$, and hence

$$[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] = [K(\sqrt{-x_0}, \zeta_8) : K] \le 8,$$

a contradiction. Therefore, $[K(i, \sqrt{1+x_0}) : K] = 4$, and $\sqrt{1+x_0} \notin K(i)$.

(2): Since $f^{-1}(x_0) = \{\pm\sqrt{1+x_0}\}$, we have $K_1 = K(\sqrt{1+x_0})$. We must have $[K(\sqrt{-x_0}, \sqrt{1+x_0}, i) : K] \ge 8$, or else $[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] < 16$. If $K_1(i)$ contains a square root of $-x_0$, then $[K(\sqrt{-x_0}, \sqrt{1+x_0}, i) : K] \le 4$, again a contradiction. Thus, $K_1(i)$ does not contain a square root of $-x_0$.

(3): By Lemma 5.1 for $\alpha_{0,1} = x_0$ and $m = 1$, we have $\sqrt{-x_0} \in K_2$, whence $K(\sqrt{-x_0}, \sqrt{1+x_0}) \subseteq K_2$. As in part (2), we have $[K(\sqrt{-x_0}, \sqrt{1+x_0}, i) : K] \ge 8$. If $i \in K_2$, then K_2 contains $K(\sqrt{-x_0}, \sqrt{1+x_0}, i)$, which is an abelian extension of K of degree 8. However, $\mathrm{Gal}(K_2/K)$ is a subgroup of $\mathrm{Aut}(T_2)$, which is a nonabelian extension of K of degree 8. By this contradiction, K_2 cannot contain i.

(4): Label the tree T_3 as in Figure 1. Let C be the commutator subgroup of $M_3 = \mathrm{Aut}(T_3)$. We claim that $|C| \ge 2^4$, and hence the abelianization $M_3^{\mathrm{ab}} := M_3/C$ has order $|M_3|/|C| \le 2^3$. (In fact, $|C| = 2^4$, but we only need the inequality here.)

Consider the elements $\alpha, \beta \in B_3 \subseteq M_3$ defined early in Section 2. As we saw in the proof of Lemma 2.10, the commutator $\lambda_1 := \alpha\beta\alpha^{-1}\beta^{-1} \in C$ has

$$\mathrm{Par}(\lambda_1, x_0) = 0, \quad \text{and} \quad \mathrm{Par}(\lambda_1, a) = \mathrm{Par}(\lambda_1, b) = 1.$$

Similarly, the commutator $\lambda_2 := \beta\alpha^2\beta^{-1}\alpha^{-2} \in C$ acts on T_3 by

$$\mathrm{Par}(\lambda_2, y) = \begin{cases} 1 & \text{if } y = ba \text{ or } bb, \\ 0 & \text{otherwise} \end{cases} \quad \text{for all nodes } y \text{ of } T_2.$$

Define $\sigma, \tau \in M_3$ by

$$\mathrm{Par}(\sigma, y) = \begin{cases} 1 & \text{if } y = bb, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad \mathrm{Par}(\tau, y) = \begin{cases} 1 & \text{if } y = x_0, \\ 0 & \text{otherwise,} \end{cases}$$

for all nodes y of T_2. Then the commutator $\lambda_3 := \sigma\tau\sigma^{-1}\tau^{-1} \in C$ acts on T_3 by

$$\mathrm{Par}(\lambda_3, y) = \begin{cases} 1 & \text{if } y = ab \text{ or } bb, \\ 0 & \text{otherwise} \end{cases} \quad \text{for all nodes } y \text{ of } T_2.$$

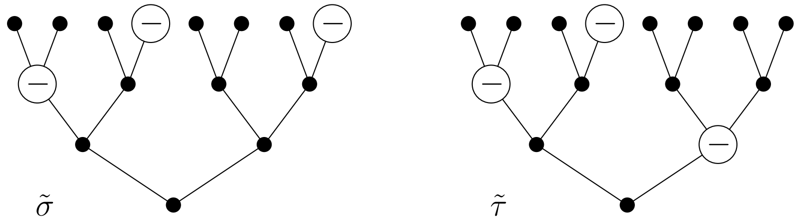

FIGURE 5. The maps $\tilde{\sigma}$ and $\tilde{\tau}$ in Lemma 5.3.(5)

The commutators λ_2, $\lambda_2' := \alpha^{-1}\lambda_2\alpha$, and λ_3 together generate the 8-element group E_3, which does not contain $\lambda_1 \in C$. Thus, $|C| \geq 16$, and hence $|M_3^{\text{ab}}| \leq 8$, as claimed.

As noted in the proofs of parts (2) and (3) above, we have

$$K(\sqrt{-x_0}, \sqrt{1+x_0}) \subseteq K_2 \subseteq K_3.$$

If K_3 contains a primitive eighth root of 1, then $K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) \subseteq K_3$. However, $K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8)/K$ is an abelian extension, and by hypothesis, it has degree 16. Therefore, the abelianization of $G_3 = \text{Gal}(K_3/K) \cong M_3$ must have order at least 16, contradicting our claim. Thus, K_3 cannot contain a primitive eighth root of 1.

(5): Let C be the commutator subgroup of M_4. We claim that $|C| \geq 2^{10}$, and hence the abelianization $M_4^{\text{ab}} := M_4/C$ has order $|M_4|/|C| \leq 2^3$. (In fact, $|C| = 2^{10}$, but as in the proof of (4), we only need the inequality here.)

Since $R_{4,3} : M_4 \to M_3$ is surjective, all of the automorphisms of T_3 in the proof of part (4) can be lifted to M_4, and hence the restriction $R_{4,3}(C)$ of C to T_3 has order at least 16. Therefore, to prove the claim, it suffices to show that $E_4 \subseteq C$, since E_4 is a 2^6-element subgroup of $\ker(R_{4,3})$.

As in the proof of Lemma 2.10, the commutator $\mu_{bb} := \alpha^2\beta^2\alpha^{-2}\beta^{-2} \in C$ has

$$\text{Par}(\mu_{bb}, y) = \begin{cases} 1 & \text{if } y = bba \text{ or } bbb, \\ 0 & \text{otherwise} \end{cases} \quad \text{for all nodes } y \text{ of } T_3.$$

Since M_4 acts transitively on the second level of T_3, conjugating μ_{bb} yields three more automorphisms $\mu_{aa}, \mu_{ab}, \mu_{ba} \in C$, where

$$\text{Par}(\mu_{st}, y) = \begin{cases} 1 & \text{if } y = sta \text{ or } stb, \\ 0 & \text{otherwise} \end{cases} \quad \text{for all nodes } y \text{ of } T_3.$$

Define $\tilde{\sigma}, \tilde{\tau} \in M_4$ by

$$\text{Par}(\tilde{\sigma}, y) = \begin{cases} 1 & \text{if } y \in \{aa, abb, bbb\} \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad \text{Par}(\tau, y) = \begin{cases} 1 & \text{if } y \in \{b, aa, abb\}, \\ 0 & \text{otherwise,} \end{cases}$$

for all nodes y of T_3; see Figure 5, where the nodes for which Par $= 1$ are marked. Define

$$\lambda_b := \tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-1} \in C \quad \text{and} \quad \lambda_a := \alpha^{-1}\lambda_b\alpha \in C.$$

Both $\tilde{\sigma}$ and $\tilde{\tau}$ fix the nodes a and b, and they coincide on the subtree rooted at a, so that λ_b acts trivially on this subtree. On the other hand, on the subtree rooted at b, they act like the automorphisms σ and τ from the proof of part (4). Thus, the commutators λ_a

and λ_b act on T_4 by

$$\mathrm{Par}(\lambda_a, y) = \begin{cases} 1 & \text{if } y = aab \text{ or } abb, \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \mathrm{Par}(\lambda_b, y) = \begin{cases} 1 & \text{if } y = bab \text{ or } bbb, \\ 0 & \text{otherwise} \end{cases}$$

for all nodes y of T_3. Therefore, the six automorphisms

$$\lambda_a, \lambda_b, \mu_{aa}, \mu_{ab}, \mu_{ba}, \mu_{bb} \in C \cap E_4$$

together generate all 2^6 elements of E_4. Thus, $|C| \geq 2^{10}$, and hence $|M_4^{\mathrm{ab}}| \leq 8$, as claimed.

As in the proof of part (4) above, if K_4 contains a primitive eighth root of 1, then $K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8)/K$ is an abelian subextension of degree 16, by hypothesis. However, the abelianization of $G_4 = \mathrm{Gal}(K_4/K) \cong M_4$ has order at most 8, by the claim. Therefore, by this contradiction, K_4 cannot contain a primitive eighth root of 1. □

Theorem 5.4. *Fix notation as at the start of Section 4, and fix roots of unity ζ_{2^m} and a tree labeling as in Lemma 4.3. Suppose that $[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] = 16$. Then*

1. *For every $n = 2m+1 \geq 1$ odd,*
   - (a) *K_n contains all the 2^{m+1}-roots of unity but no primitive 2^{m+2}-roots of unity.*
   - (b) *K_n contains a 2^m-root of $-x_0$ but no 2^{m+1}-root of $-x_0$.*
   - (c) *K_n contains a 2^{m+1}-root of $1+x_0$ but no 2^{m+2}-root of $1+x_0$.*
   - (d) $\mathrm{Gal}\big(K_n/K(\zeta_{2^{m+1}})\big) \cong B_n$.
   - (e) $\mathrm{Gal}(K_n/K) \cong M_n$
2. *For every $n = 2m \geq 2$ even,*
   - (a) *K_n contains all the 2^m-roots of unity but no primitive 2^{m+1}-roots of unity.*
   - (b) *K_n contains a 2^m-root of $-x_0$ but no 2^{m+1}-root of $-x_0$.*
   - (c) *K_n contains a 2^m-root of $1+x_0$ but no 2^{m+1}-root of $1+x_0$.*
   - (d) $\mathrm{Gal}\big(K_n/K(\zeta_{2^m})\big) \cong B_n$.
   - (e) $\mathrm{Gal}(K_n/K) \cong M_n$

Proof. We proceed by induction on $n \geq 1$. For $n = 1, 2$, we strengthen the second statement of (1c) and (2c) to say that $K_1(i)$ and $K_2(i)$ do not contain a fourth root of $1+x_0$. This strengthening will be relevant near the end of Cases 3 and 2, respectively.

Case 1: For $n = 1$, i.e., $n = 2m+1$ with $m = 0$, clearly K_1 contains $\zeta_2 = -1$, which is a primitive 2-root of 1, and $-x_0$, which is a 2^0-root of $-x_0$. In addition, $K_1 = K(\sqrt{1+x_0})$ contains a 2^1-root $\sqrt{1+x_0}$ of $1+x_0$.

On the other hand, by Lemma 5.3.(3), K_2 does not contain a primitive fourth root of unity, and hence neither does K_1. By Lemma 5.3.(2), $K_1(i)$ does not contain a square root of $-x_0$, and hence neither does K_1.

By Lemma 5.3.(1), $[K(i, \sqrt{1+x_0}) : K] = 4$, which implies both that $[K_1(i) : K(i)] = 2$ and that $\sqrt{1+x_0} \notin K(i)$. If $\sqrt[4]{1+x_0} \in K_1(i)$, then $K_1(i)/K(i)$ would be a cyclic extension of degree 4, a contradiction. Thus, $K_1(i)$ does not contain a fourth root of $1+x_0$.

We have proven statements (a)–(c), including the strengthened version of (c). Finally, since $[K_1 : K] = 2$ and $\zeta_2 = -1$, we have

$$\mathrm{Gal}(K_1/K) = \mathrm{Gal}(K_1/K(\zeta_2)) \cong \mathbb{Z}/2\mathbb{Z} \cong B_2 \cong M_2,$$

proving statements (d) and (e) as well.

Case 2: Suppose $n = 2m \geq 2$ is even, and suppose the theorem holds for all smaller n. Let $\ell := 2^m$. By the inductive hypothesis, K_{n-1} contains a primitive ℓ-root of unity ζ_ℓ and an ℓ-root of $1 + x_0$, and therefore K_n does as well, proving the first half of statements (a) and (c).

By Corollary 4.5.(1), $G_n = \operatorname{Gal}(K_n/K)$ is isomorphic to a subgroup of M_n, not just as abstract groups, but also respecting the action on the tree T_n, identified with the tree of preimages of x_0 under f^{-n}. We will therefore abuse notation in the rest of this proof and view G_n as a subgroup of M_n. Similarly, by Corollary 4.5.(2), $G'_n := \operatorname{Gal}(K_n/K(\zeta_\ell))$ is a subgroup of B_n. Since K_{n-1} also contains ζ_ℓ, it follows that $\operatorname{Gal}(K_n/K_{n-1})$ is a subgroup of E_n.

By Lemma 5.1.(1) applied to $\alpha_{0,1} := x_0$, K_n also contains an ℓ-root γ of $-x_0$, proving the first half of statement (b). By the inductive hypothesis again, we have $\gamma \notin K_{n-1}$. On the other hand, γ^2 is a 2^{m-1}-root of $-x_0$ and hence lies in K_{n-1}. (Indeed, K_{n-1} contains at least one such root, and hence it contains all such roots, as it is a Galois extension of K.) Therefore, K_n contains the quadratic extension $K_{n-1}(\gamma)$ of K_{n-1}, and hence there exists $\lambda \in \operatorname{Gal}(K_n/K_{n-1}) = G'_n \cap E_n$ such that $\lambda(\gamma) = -\gamma$. By Lemma 5.1.(2), we have $\operatorname{sgn}_n(\lambda, x_0) = -1$. In addition, by our inductive assumption of (d) for $n - 1$, we have

$$R_{n,n-1}(G'_n \cap B_n) = \operatorname{Gal}\big(K_{n-1}/K(\zeta_\ell)\big) = B_{n-1}.$$

Therefore, by Corollary 2.13, we have $G'_n \supseteq B_n$, and hence $G'_n = \operatorname{Gal}(K_n/K(\zeta_\ell)) = B_n$, proving statement (d).

Furthermore, it follows that $\operatorname{Gal}(K_n/K_{n-1}) = E_n$, and hence, by Theorem 3.2.(1), that $\operatorname{Gal}(K_n/K_{n-1}) = U_n$. By our inductive hypothesis, we also have $\operatorname{Gal}(K_{n-1}/K) = M_{n-1}$. Thus, we must have $\operatorname{Gal}(K_n/K) = M_n$, proving statement (e).

It remains to show the second half of each of statements (a–c). For (a), Lemma 5.3.(3) suffices for $n = 2$, and Lemma 5.3.(5) suffices for $n = 4$. For $n \geq 6$, i.e. $m \geq 3$, let $y = \zeta_{2^{m-1}}$ be a primitive 2^{m-1}-root of unity. By our inductive hypothesis, we have $y \in K_{n-2}$ but y has no square root in $K_{n-2} = K_{n-2}(i)$. Therefore, by Lemma 5.2, y has no fourth root in $K_n(i) = K_n$; that is, K_n does not contain a primitive 2^{m+1}-root of unity.

For (b) and (c), we claim that neither $1 + x_0$ nor $-x_0$ has a 2^m-root in $K_{n-2}(i)$. For $n \geq 6$, this is true by our inductive hypothesis and the fact that $K_{n-2} = K_{n-2}(i)$. For $n = 2$, it is true for $1 + x_0$ by Lemma 5.3.(1), and for $-x_0$ by Lemma 5.3.(2). For $n = 4$, our inductive hypothesis says that $-x_0$ has no fourth root in K_3 and hence in $K_2(i)$. Finally, the strengthened version of statement (2c) in our inductive hypothesis says that $1 + x_0$ has no fourth root in $K_2(i)$, proving our claim.

Thus, letting $y \in K_{n-2}$ be a 2^{m-1}-root of $-x_0$ (for (b)), or a 2^{m-1}-root of $1 + x_0$ (for (c)), the above claim shows that y has no square root in $K_{n-2}(i)$. Therefore, by Lemma 5.2, y has no fourth root in $K_n(i)$, yielding the desired conclusion that K_n contains no 2^{m+1}-roots of $-x_0$ or $1 + x_0$, and, for $n = 2$, that $K_2(i)$ contains no fourth root of $1 + x_0$.

Case 3: Suppose $n = 2m + 1 \geq 3$ is odd, and suppose the theorem holds for all smaller n. Let $\ell := 2^m$. By the inductive hypothesis, K_{n-1} contains an ℓ-root of $-x_0$, and therefore K_n does as well, proving the first half of statement (b). By Lemma 4.2 with $y = x_0$, which has preimages $f^{-1}(x_0) = \{\pm\sqrt{1 + x_0}\}$, we see that K_n contains a

2^{m+1}-root of $1 + x_0$ and a primitive 2^{m+1}-root of unity $\zeta_{2\ell}$. Thus, we have proven the first half of statements (a) and (c) as well.

As in Case 2, by Corollary 4.5, $G_n = \mathrm{Gal}(K_n/K)$ is isomorphic to a subgroup of M_n, and $G'_n := \mathrm{Gal}(K_n/K(\zeta_{2\ell}))$ is isomorphic to a subgroup of B_n. We again abuse notation and view G_n and G'_n as subgroups of M_n and B_n, respectively. It follows that $\mathrm{Gal}(K_n/K_{n-1}(\zeta_{2\ell})) \subseteq G'_n$ is a subgroup of E_n.

Consider $G'' := \mathrm{Gal}(K_{n-1}(\zeta_{2\ell})/K(\zeta_{2\ell}))$. We claim that $G'' \cong B_{n-1}$. To prove this claim, observe first that G'' is isomorphic to a subgroup of B_{n-1}, by Corollary 4.5.(2). Observe further that $[K_{n-1}(\zeta_{2\ell}) : K_{n-1}] = 2$, since $\zeta_\ell := \zeta_{2\ell}^2 \in K_{n-1}$ but $\zeta_{2\ell} \notin K_{n-1}$, by our inductive hypothesis. Therefore,

$$\begin{aligned}|B_{n-1}| \cdot 2 &\geq [K_{n-1}(\zeta_{2\ell}) : K(\zeta_{2\ell})][K(\zeta_{2\ell}) : K(\zeta_\ell)] = [K_{n-1}(\zeta_{2\ell}) : K(\zeta_\ell)] \\ &= [K_{n-1}(\zeta_{2\ell}) : K_{n-1}][K_{n-1} : K(\zeta_\ell)] = 2 \cdot |B_{n-1}|,\end{aligned}$$

and hence $|G''| = [K_{n-1}(\zeta_{2\ell}) : K(\zeta_{2\ell})] = |B_{n-1}|$. Therefore, G'' must be isomorphic to the full group B_{n-1}, proving the claim.

Recall from above that K_n contains a 2^{m+1}-root γ of $1 + x_0$. By the inductive hypothesis, we have $\gamma \notin K_{n-1}$. We make a second claim, that $\gamma \notin K_{n-1}(\zeta_{2\ell})$. To see this, it suffices to show that the two quadratic extensions $L := K_{n-1}(\gamma)$ and $K_{n-1}(\zeta_{2\ell})$ of K_{n-1} do not coincide. If they did, then $\mathrm{Gal}(L/K_{n-1})$ would be a two-element group $\{e, \tau\}$ with $\tau(\gamma) = -\gamma$ and $\tau(\zeta_{2\ell}) = -\zeta_{2\ell}$. In that case, the product $\zeta_{2\ell}\gamma \in L$ would be fixed by both e and τ, and hence $\zeta_{2\ell}\gamma \in K_{n-1}$. However, $\zeta_{2\ell}\gamma$ is a 2^{m+1}-root of $1 + x_0$, contradicting the inductive hypothesis and proving our second claim.

Thus, K_n contains the quadratic extension $K_{n-1}(\zeta_{2\ell}, \gamma)$ of $K_{n-1}(\zeta_{2\ell})$, and hence there exists $\lambda \in \mathrm{Gal}(K_n/K_{n-1}(\zeta_{2\ell})) = G'_n \cap E_n$ such that $\lambda(\gamma) = -\gamma$. By Lemma 5.1.(2) applied to $\alpha_{0,1} := \sqrt{1 + x_0} \in f^{-1}(x_0)$, we have $\mathrm{sgn}_{n-1}(\lambda, \sqrt{1 + x_0}) = -1$, and therefore $\mathrm{sgn}_n(\lambda, x_0) = -1$ by Lemma 2.5.(2). In addition,

$$R_{n,n-1}(G'_n \cap B_n) = \mathrm{Gal}\left(K_{n-1}(\zeta_{2\ell})/K(\zeta_{2\ell})\right) = G'' = B_{n-1},$$

where the last equality is by our first claim. Therefore, by Corollary 2.13, we have $G'_n \supseteq B_n$, and hence $G'_n = \mathrm{Gal}(K_n/K(\zeta_{2\ell})) = B_n$, proving statement (d).

It follows that $\mathrm{Gal}(K_n/K_{n-1}(\zeta_{2\ell})) = E_n$. On the other hand, $\mathrm{Gal}(K_n/K_{n-1}) \subseteq U_n$, since G_n is a subgroup of M_n. We must therefore have $\mathrm{Gal}(K_n/K_{n-1}) = U_n$, because

$$[K_{n-1}(\zeta_{2\ell}) : K_{n-1}] = 2 = [U_n : E_n],$$

where the first equality is by our inductive hypothesis, and the second is by Theorem 3.2.(1). Also by our inductive hypothesis, we have $\mathrm{Gal}(K_{n-1}/K) = M_{n-1}$. It follows that $\mathrm{Gal}(K_n/K) = M_n$, proving statement (e).

It remains to show the second half of each of statements (a–c). For (a), Lemma 5.3.(4) suffices for $n = 3$. For $n \geq 5$, i.e. $m \geq 2$, let $y = \zeta_{2^m}$ be a primitive 2^m-root of unity. By our inductive hypothesis, we have $y \in K_{n-2}$ but y has no square root in $K_{n-2} = K_{n-2}(i)$. Therefore, by Lemma 5.2, y has no fourth root in K_n; that is, K_n does not contain a primitive 2^{m+2}-root of unity.

For (b), let y be a 2^{m-1}-root of $-x_0$, or for (c), let y be a 2^m-root of $1 + x_0$. If $n = 3$, then y has no square root in $K_{n-2}(i)$, by Lemma 5.3.(2) for $-x_0$, and by our strengthened version of (1c) for $1 + x_0$. If $n \geq 5$, then by our inductive hypothesis, y has no square root in $K_{n-2} = K_{n-2}(i)$. Therefore, by Lemma 5.2, y has no fourth root in K_n. That is, K_n contains no 2^{m+1}-roots of $-x_0$ or $1 + x_0$. □

We close with the following strengthening of statement (2) of our Main Theorem.

Corollary 5.5. *Fix notation as at the start of Section 4, and fix roots of unity ζ_{2^m} and a tree labeling as in Lemma 4.3. The following are equivalent.*

(1) $[K(\sqrt{-x_0}, \sqrt{1+x_0}, \zeta_8) : K] = 16$.
(2) $[K_5 : K] = 2^{25}$.
(3) $G_5 \cong M_5$.
(4) $G_n \cong M_n$ *for all* $n \geq 1$.
(5) $G_\infty \cong M_\infty$.

(As always, the isomorphisms of statements (3)–(5) are of groups acting on trees, not just of abstract groups.)

Proof. We have (1)⇒(4) by Theorem 5.4. Taking inverse limits, we have (4)⇒(5), since

$$G_\infty \cong \varprojlim G_n \cong \varprojlim M_n \cong M_\infty.$$

The implications (5)⇒(4)⇒(3) are trivial. Since $|G_5| = [K_5 : K]$ and $|M_5| = 2^{25}$ (by Theorem 3.3), we have (3)⇒(2). In addition, by Corollary 4.5.(1), G_5 is isomorphic to a subgroup of M_5, and hence (2)⇒(3). It suffices to show (3)⇒(1).

Assume that $G_5 \cong M_5$, and therefore that $G_n \cong M_n$ for $n = 1, 2, 3, 4, 5$.

If K contains a square root of $1 + x_0$, then $K_1 = K(\sqrt{1+x_0}) = K$, whence $|G_1| = 1$, contradicting the fact that $|M_1| = 2$. Thus, $[K(\sqrt{1+x_0} : K] = 2$.

If $K(\sqrt{1+x_0})$ contains a square root of $-x_0$, then any $\sigma \in \text{Gal}(K_2/K_1)$ fixes $-x_0$. By Lemma 5.1, we have $\text{sgn}_2(\sigma, x_0) = +1$ for any such σ. However, the isomorphism $G_2 \cong M_2$ restricts to $\text{Gal}(K_2/K_1) \cong U_2$, and $\beta \in U_2$ satisfies $\text{sgn}_2(\beta, x_0) = -1$, a contradiction. Thus,

$$[K(\sqrt{1+x_0}, \sqrt{-x_0}) : K(\sqrt{1+x_0})] = 2,$$

and hence $[K(\sqrt{1+x_0}, \sqrt{-x_0}) : K] = 4$.

If $K(\sqrt{1+x_0}, \sqrt{-x_0}) \subseteq K_2$ contains a primitive fourth root of unity i, then every $\sigma \in \text{Gal}(K_3/K_2)$ fixes i. Via the isomorphism $G_3 \cong M_3$, this would mean that every $\sigma \in U_3$ also lies in E_3. However, $[U_3 : E_3] = 2$ by Theorem 3.2, a contradiction. Thus,

$$[K(\sqrt{1+x_0}, \sqrt{-x_0}, i) : K(\sqrt{1+x_0}, \sqrt{-x_0})] = 2,$$

and hence $[K(\sqrt{1+x_0}, \sqrt{-x_0}, i) : K] = 8$.

Finally, if $K(\sqrt{1+x_0}, \sqrt{-x_0}, i) \subseteq K_3$ contains a primitive eighth root of unity ζ_8, then every $\sigma \in \text{Gal}(K_5/K_4)$ fixes ζ_8. Via the isomorphism $G_5 \cong M_5$, this would mean that every $\sigma \in U_5$ also lies in E_5. However, $[U_5 : E_5] = 2$ by Theorem 3.2, a contradiction. Thus,

$$[K(\sqrt{1+x_0}, \sqrt{-x_0}, \zeta_8) : K(\sqrt{1+x_0}, \sqrt{-x_0}, i)] = 2,$$

and hence $[K(\sqrt{1+x_0}, \sqrt{-x_0}, \zeta_8) : K] = 16$, as desired. □

Acknowledgements. The results of this paper grew out of an REU project at Amherst College. Our theorems were originally suggested by computations using Magma. Authors RB, JC, and GC gratefully acknowledge the support of NSF grant DMS-1501766. Authors FA and LF gratefully acknowledge the support of Amherst College's Gregory S. Call student research funding. We thank Harris Daniels and Jamie Juul for helpful discussions. A particular thanks goes to Rafe Jones, for proposing this problem, for providing useful background, and for suggestions surrounding Conjectures 1 and 2.

References

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

[2] Jacqueline Anderson, Irene I. Bouw, Ozlem Ejder, Neslihan Girgin, Valentijn Karemaker, and Michelle Manes, Dynamical Belyi maps, in *Women in numbers Europe II*, Springer, Cham (2018), 57–82.

[3] Laurent Bartholdi, Rostislav Grigorchuk, and Volodymyr Nekrashevych, From fractal groups to fractal sets, in *Fractals in Graz 2001*, 25–118, Birkhäuser, Basel, 2003.

[4] 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.

[5] Robert L. Benedetto and Jamie Juul, Odoni's conjecture for number fields, *Bull. Lond. Math. Soc.* **51** (2019), 237–350.

[6] Nigel Boston and Rafe Jones, Arboreal Galois representations, *Geom. Dedicata* **124** (2007), 27–35.

[7] Andrew Bridy and Thomas J. Tucker, *Finite index theorems for iterated Galois groups of cubic polynomials*, *Math. Ann.* **373** (2019), 37–72.

[8] Michael R. Bush, Wade Hindes, and Nicole R. Looper, Galois groups of iterates of some unicritical polynomials, *Acta Arith.* **181** (2017), 57–73.

[9] Andrea Ferraguti and Giacomo Micheli, An equivariant isomorphism theorem for mod $\mathfrak{p}$ reductions of arboreal Galois representations, preprint, 2019. Available at `arXiv:1905.00506`.

[10] Andrea Ferraguti, Carlo Pagano, and Daniele Casazza, The inverse problem for arboreal Galois representations of index two, preprint, 2019. Available at `arXiv:1907.08608`.

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

[12] Chad Gratton, Khoa Nguyen, and Thomas J. Tucker, *ABC* implies primitive prime divisors in arithmetic dynamics, *Bull. Lond. Math. Soc.* **45** (2013), 1194–1208.

[13] Wade Hindes, Average Zsigmondy sets, dynamical Galois groups, and the Kodaira-Spencer map, *Trans. Amer. Math. Soc.* **370** (2018), 6391–6410.

[14] Wade Hindes, Classifying Galois groups of small iterates via rational points, *Int. J. Number Theory* **14** (2018), 1403–1426.

[15] Patrick Ingram, Arboreal Galois representations and uniformization of polynomial dynamics, *Bull. Lond. Math. Soc.* **45** (2013), 301–308.

[16] Rafe Jones, Galois representations from pre-image trees: an arboreal survey, in *Actes de la Conférence "Théorie des Nombres et Applications", Pub. Math. Besançon* (2013), 107-136.

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

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

[19] Jamie Juul, Holly Krieger, Nicole Looper, Michelle Manes, Bianca Thompson, and Laura Walton, Arboreal representations for rational maps with few critical points, preprint, 2018. Available at `arXiv:1804.06053`.

[20] Jamie Juul, Pär Kurlberg, Kalyani Madhu, and Tom J. Tucker, Wreath products and proportions of periodic points, *Int. Math. Res. Not. IMRN* **2016**, 3944–3969.

[21] Borys Kadets, Large arboreal Galois representations, preprint, 2018. Available at `arXiv:1802.09074`.

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

[23] Volodymyr Nekrashevych, *Self-Similar Groups*, American Mathematical Society, Providence, 2005.

[24] R. W. K. Odoni, The Galois theory of iterates and composites of polynomials, *Proc. London Math. Soc. (3)* **51** (1985), no. 3, 385–414.

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

[26] Jean-Pierre Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[27] Joel Specter, Polynomials with Surjective Arboreal Galois Representations Exist in Every Degree, preprint, 2018. Available at `arXiv:1803.00434`.

[28] Michael Stoll, Galois groups over **Q** of some iterated polynomials, *Arch. Math. (Basel)* **59** (1992), 239–244.

[29] Ashvin A. Swaminathan, On arboreal Galois representations of rational functions, *J. Algebra* **448** (2016), 104–126.

Amherst College, Amherst, MA 01002, USA
Email address: `faseehirfan@gmail.com`

Email address: `rlbenedetto@amherst.edu`

Email address: `jentcain@gmail.com`

Email address: `gcarroll19@amherst.edu`

Email address: `lilycfang@yahoo.com`