Profinite iterated monodromy groups arising from quadratic polynomials

Richard Pink

Department of Mathematics
ETH Zürich
8092 Zürich
Switzerland
pink@math.ethz.ch

September 1, 2013

Abstract

We study in detail the profinite group G arising as geometric étale iterated monodromy group of an arbitrary quadratic polynomial over a field of characteristic different from two. This is a self-similar closed subgroup of the group of automorphisms of a regular rooted binary tree. (When the base field is $\mathbb{C}$ it is the closure of the finitely generated iterated monodromy group for the usual topology which is also often studied.) Among other things we prove that the conjugacy class and hence the isomorphism class of G depends only on the combinatorial type of the postcritical orbit of the polynomial.

We represent a chosen instance of G by explicit recursively defined generators. The uniqueness up to conjugacy depends on a certain semirigidity property, which ensures that arbitrary conjugates of these generators under the automorphism group of the tree always generate a subgroup that is conjugate to G. We determine the Hausdorff dimension, the maximal abelian factor group, and the normalizer of G using further explicit generators. The description of the normalizer is then used to describe the arithmetic étale iterated monodromy group of the quadratic polynomial.

The methods used are purely group theoretical and do not involve fundamental groups over $\mathbb{C}$ at all.

Contents

0 Introduction

Let f be a polynomial of degree two in one variable with coefficients in a field k of characteristic different from 2. For every integer $n \geqslant 1$ let f^n denote the nth *iterate of f*, obtained by substituting n copies of f into each other. The result is a polynomial of degree 2^n, which we view as a finite morphism from the projective line $\mathbb{P}^1_k$ over k to itself. Let $S \subset \mathbb{P}^1_k$ denote the (strictly) *postcritical orbit* of f, that is, the set of images under all iterates f^n of the critical points of f. Then each f^n is a connected ramified covering of $\mathbb{P}^1_k$ which is unramified over $\mathbb{P}^1_k \smallsetminus S$. As such it is determined up to isomorphism by the action of the étale fundamental group $\pi^{\text{ét}}_1(\mathbb{P}^1_k \smallsetminus S)$ on a certain set with 2^n elements. Varying n, these coverings form an infinite tower $\ldots \xrightarrow{f} \mathbb{P}^1_k \xrightarrow{f} \mathbb{P}^1_k \xrightarrow{f} \mathbb{P}^1_k$ whose structure up to isomorphism is determined by the action of the étale fundamental group on a regular rooted binary tree T. The action corresponds to a homomorphism $\rho\colon \pi^{\text{ét}}_1(\mathbb{P}^1_k \smallsetminus S) \to \operatorname{Aut}(T)$, whose image is the *iterated monodromy group* associated to f which we study in this article.

By construction it is a profinite group. If k is the field of complex numbers one can also define a discrete iterated monodromy group using the usual fundamental group of $\mathbb{P}^1(\mathbb{C}) \smallsetminus S$, whose closure in the automorphism group of the tree is the profinite iterated monodromy group defined above. In the present article we disregard that point of view entirely and work purely algebraically and with profinite groups only.

In particular we do not require k to be algebraically closed. In fact, if $\bar{k}$ denotes a separable closure of k, it is natural to compare the image of $\pi^{\text{ét}}_1(\mathbb{P}^1_k \smallsetminus S)$ with the image of $\pi^{\text{ét}}_1(\mathbb{P}^1_{\bar{k}} \smallsetminus S)$. We call the former the *arithmetic* iterated monodromy group G^{arith} and the latter the *geometric* iterated monodromy group G^{geom} associated to f. Then G^{geom} is a closed normal subgroup of G^{arith}, and the monodromy action induces a natural surjective homomorphism $\bar{\rho}\colon \operatorname{Gal}(\bar{k}/k) \twoheadrightarrow G^{\text{arith}}/G^{\text{geom}}$. Among the main results in this article are the explicit description of G^{geom} and G^{arith} and $\bar{\rho}$.

Our ultimate motivation for this, though not developed at all in the present article, is to understand the arithmetic properties of the tower of coverings which manifest themselves in the iterated monodromy groups. We are intrigued by the analogy between the Galois representation on the tree associated to f, and the linear ℓ-adic Galois representation on the Tate module of an abelian variety or a Drinfeld module or on the ℓ-adic cohomology of an algebraic variety. There are many deep results for the latter, and it would be delightful if counterparts for iterated monodromy groups could be developed as well. Natural candidates for study are for instance the images of Frobenius elements in the case that k is a number field or a finite field.[1]

---

[1] For example: It is not hard to show that the set of conjugacy classes in the automorphism group of the tree has the cardinality of the continuum. On the other hand, the conjugacy class of the image of a Frobenius element depends only on a quadratic polynomial over a finite field and an element of that finite field. Thus the conjugacy classes arising from Frobenius elements form a countable set only. The images of Frobenius elements must therefore satisfy some strong special properties. The question is: which?

Note that for a non-trivial linear ℓ-adic Galois representation the set of conjugacy classes in $\operatorname{GL}_n(\mathbb{Q}_\ell)$ likewise has the same cardinality as $\mathbb{Q}_\ell$, but the characteristic polynomials of Frobenius elements usually have coefficients in a number field, which also leaves only countably many conjugacy classes for them.

Now we describe the methods and results of this article. Note that the monodromy action is ramified at any point ξ_i in the postcritical orbit S. Since G^{geom} is a pro-2-group and the base field has characteristic different from 2, the image of the inertia group at ξ_i is a quotient of the tame pro-2 inertia group and therefore topologically generated by a single element. Let $b_i \in G^{\text{geom}}$ be the image of a chosen generator. Then G^{geom} is topologically generated by the set $\{b_i \mid \xi_i \in S\}$. In particular, if S is finite, then G^{geom} is topologically finitely generated. Moreover, the generator of inertia at $\infty \in S$ can be dropped, essentially because $\mathbb{A}_k^1$ has no non-trivial connected unramified covering which is tame at ∞. For the following discussion we therefore delete ∞ from S.

If we remove the bottom level from the tower of coverings $\ldots \xrightarrow{f} \mathbb{P}_k^1 \xrightarrow{f} \mathbb{P}_k^1 \xrightarrow{f} \mathbb{P}_k^1$ we obtain the same tower again. From this we deduce that the monodromy representation and the iterated monodromy groups are *self-similar* in the sense that a copy arises as a proper subquotient. This implies a weak form of recursion relations for the generators b_i. Namely, on deleting the root, the tree T decomposes into two rooted regular binary trees, each related to the tower of coverings with the bottom level removed. Choosing an isomorphism from T to each of these subtrees, it turns out that each b_i is conjugate in $\text{Aut}(T)$ to an explicit element given in terms of certain other generators acting on the two half trees. Specifically, let $\sigma \in \text{Aut}(T)$ be an element of order 2 that interchanges the two half trees. For any two elements $u, v \in \text{Aut}(T)$ let (u, v) denote the element of $\text{Aut}(T)$ which acts by u on the first half tree and by v on the second. Then b_i is conjugate under $\text{Aut}(T)$ to

$$
(0.1) \qquad
\begin{cases}
\sigma & \text{if } f \text{ is ramified over } \xi_i \text{ and } \xi_i \notin f(S), \\
(b_j, 1)\,\sigma & \text{if } f \text{ is ramified over } \xi_i \text{ and } f(\xi_j) = \xi_i \text{ for } \xi_j \in S, \\
(b_j, 1) & \text{if } f \text{ is unramified over } \xi_i \text{ and } f(\xi_j) = \xi_i \text{ for a unique } \xi_j \in S, \\
(b_j, b_k) & \text{if } f(\xi_j) = f(\xi_k) = \xi_i \text{ for two distinct points } \xi_j, \xi_k \in S,
\end{cases}
$$

(see Proposition 1.7.14).

It turns out that these relations suffice to determine G^{geom} up to conjugacy in $\text{Aut}(T)$, which therefore depends only on the combinatorics of the postcritical orbit. This may be somewhat surprising, because the relations seem so much weaker than the recursion relations one usually has for the generators of discrete iterated monodromy groups over $\mathbb{C}$, which are definite equalities not just up to conjugacy. Nevertheless we prove:

Theorem 0.2 *Any two closed subgroups of* $\text{Aut}(T)$ *which are generated by elements* b_i *satisfying the relations (0.1) associated to the given postcritical orbit* S *are conjugate.*

The analysis of G^{geom} thus reduces to the study of the closed subgroup $G \subset \text{Aut}(T)$ that is topologically generated by any single choice of generators satisfying (0.1). We choose the generators a_i that are uniquely characterized by the recursion relations

$$
(0.3) \qquad a_i =
\begin{cases}
\sigma & \text{if } f \text{ is ramified over } \xi_i \text{ and } \xi_i \notin f(S), \\
(a_j, 1)\,\sigma & \text{if } f \text{ is ramified over } \xi_i \text{ and } f(\xi_j) = \xi_i \text{ for } \xi_j \in S, \\
(a_j, 1) & \text{if } f \text{ is unramified over } \xi_i \text{ and } f(\xi_j) = \xi_i \text{ for a unique } \xi_j \in S, \\
(a_j, a_k) & \text{if } f(\xi_j) = f(\xi_k) = \xi_i \text{ for two distinct points } \xi_j, \xi_k \in S.
\end{cases}
$$

4

To understand G is a purely group theoretical problem that is interesting in its own right. Most of the article is actually devoted to it. The methods used are standard finite and profinite group theory, and time and again the exploitation of the self-similarity properties of G resulting from the recursion relations (0.3).

There is a marked difference in structure depending on the type of S. If S is infinite, one can easily show that $G = G^{\text{geom}} = G^{\text{arith}} = \text{Aut}(T)$. So assume henceforth that S is finite. Then the unique critical point $\neq \infty$ of f is called *periodic* if it is mapped to itself under some iterate of f, otherwise it is called *strictly pre-periodic*. A precise description of the different possibilities for S is given in 1.7.2. As many details differ between these two cases, the main body of the paper is divided accordingly. Among other things:

- We determine the maximal abelian factor group of G: see Theorems 2.2.7 and 3.1.6.

- We calculate the Hausdorff dimension of G: see Theorems 2.3.2 and 3.3.4.

- We prove Theorem 0.2. Actually we show that for any elements $b_i \in \text{Aut}(T)$ satisfying the weak recursion relations (0.1), on conjugating all b_i by a single element of $\text{Aut}(T)$ we can achieve that all b_i lie in G, are conjugate to the respective a_i under G, and topologically generate G. For this combine Proposition 2.4.1 or 3.4.1 with Theorem 2.4.3 or 3.4.3. We view this result as a kind of *semirigidity* property of the generators.

- In one interesting case of a group with two generators, namely the closure of the 'Basilica group', we show a stronger *rigidity* property that on conjugating the b_i by a single element of $\text{Aut}(T)$ we can make them equal to a_i: see Theorem 2.5.1. This rigidity property, and its failure whenever the number of generators is greater than two, had in fact been the motivation for the author to search for a weaker version that would still give G up to conjugacy in the general case, and that he found in the semirigidity property described above.

- We determine the normalizer $N \subset \text{Aut}(T)$ of G and describe it using further explicit generators. This result requires significantly more effort than the others. Let r denote the number of generators of G, that is, the cardinality of S (without ∞). In the periodic case we establish an explicit isomorphism $N/G \cong (\mathbb{Z}_2^\times)^r$, where $\mathbb{Z}_2$ denotes the ring of 2-adic integers: see Theorem 2.6.8. In the strictly pre-periodic case with $r = 2$ the group G is infinite pro-dihedral isomorphic to $\mathbb{Z}_2 \rtimes \{\pm 1\}$ and its normalizer is isomorphic to $\mathbb{Z}_2 \rtimes \mathbb{Z}_2^\times$: see Subsection 3.5. In the strictly pre-periodic case with $r \geqslant 3$ we construct an isomorphism between N/G and a countably infinite product $(\mathbb{F}_2)^\infty$ of copies of the cyclic group of order 2. For technical reasons this requires a further division into subcases: see Theorems 3.6.12, 3.7.18, and 3.8.27.

- We study a particularly useful class of elements of G called *odometers*. We show that their proportion in G is $2^{-r} > 0$ and that they are all conjugate under N: see Proposition 2.7.1 or 3.9.1 and Theorem 2.7.4 or 3.9.4. We describe how the normalizer of any odometer in G sits inside N and how it maps to N/G: see Proposition 2.7.7 or 3.9.14. In the periodic case we can also strengthen the semirigidity theorem

5

mentioned above to include odometers in Theorem 2.7.6, but we do not know how to achieve anything similar in the strictly pre-periodic case.

Let us now return to the iterated monodromy groups associated to a quadratic polynomial. By Theorem 0.2, after conjugating everything by an automorphism of T we may assume that $G^{\text{geom}} = G$. Then G^{arith} is contained in the normalizer N, and describing it is equivalent to describing the subgroup G^{arith}/G of N/G. In fact, we give the composite homomorphism $\bar{\rho}\colon \text{Gal}(\bar{k}/k) \twoheadrightarrow G^{\text{arith}}/G \hookrightarrow N/G$ explicitly in terms of the description of N/G mentioned above.

For this we look at the restriction of ρ to the decomposition group at a postcritical point. The image of the corresponding inertia group is always cyclic or pro-cyclic, and the decomposition group acts on it through the cyclotomic character. Using this we can deduce that $\bar{\rho}$ always factors through the cyclotomic character. Moreover, the image of the inertia group at ∞ is generated by an odometer, so our previously assembled results on odometers in G easily determine $\bar{\rho}$ completely.

Namely, in the periodic case the homomorphism $\bar{\rho}\colon \text{Gal}(\bar{k}/k) \to N/G \cong (\mathbb{Z}_2^\times)^r$ is the cyclotomic character $\text{Gal}(\bar{k}/k) \to \mathbb{Z}_2^\times$ followed by the diagonal embedding: see Theorem 2.8.4. In the strictly pre-periodic case with $r = 2$ the homomorphism $\bar{\rho}\colon \text{Gal}(\bar{k}/k) \to N/G \cong \mathbb{Z}_2^\times/\{\pm 1\}$ is the cyclotomic character followed by the projection $\mathbb{Z}_2^\times \twoheadrightarrow \mathbb{Z}_2^\times/\{\pm 1\}$. In these two cases, therefore, the index $[G^{\text{arith}} : G^{\text{geom}}]$ is infinite if the ground field k is finitely generated over its prime field.

In the strictly pre-periodic case with $r \geqslant 3$ the homomorphism $\bar{\rho}\colon \text{Gal}(\bar{k}/k) \to N/G \cong (\mathbb{F}_2)^\infty$ is the composite of the cyclotomic character with the projection $\mathbb{Z}_2^\times \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^\times$ and a homomorphism $(\mathbb{Z}/8\mathbb{Z})^\times \to (\mathbb{F}_2)^\infty$ that is given precisely in Theorem 3.10.5. In this case the group G^{arith}/G is elementary abelian of order dividing 4, and in fact dividing 2 except in one particular case: see Corollary 3.10.6. Thus G^{arith} depends only very mildly on the field k. Moreover, in this case we have $G^{\text{arith}} = G$ whenever k contains the eighth roots of unity, in particular whenever k is finite and its order is a square. It is conceivable that this state of affairs has some influence on the properties of the images of Frobenius elements.

Let us now point out the relation with existing results in the literature, without any claim of completeness. Although most of those results concern discrete iterated monodromy groups, some of them have a direct relation with the profinite iterated monodromy groups arising as closures of the discrete ones. First, for generalities on self-similar groups acting on regular rooted trees see for instance Nekrashevych [15] or Grigorchuk-Savchuk-Šunić [11].

Next, much is already known in the following small cases: In the periodic case with $r = 1$ the group G is pro-cyclic. In the periodic case with $r = 2$ the group G is the closure of the so-called 'Basilica' group, studied for instance in Grigorchuk-Żuk [9]. In the periodic case with $r = 3$ corresponding to the 'Douady rabbit' some of our results follow from Nekrashevych [17, §8]. In the strictly pre-periodic case with $s = 1$ and $r = 2$ the group G is infinite pro-dihedral. In the strictly pre-periodic case with $s = 1$ and $r = 3$ the group G is the closure of the Grigorchuk group, introduced in Grigorchuk [7] and studied extensively,

among others in Grigorchuk [8, §§12-15], Bartholdi-Grigorchuk [1], Grigorchuk-Sidki [10], Nekrashevych [17].

An important result related to ours is contained in the paper [2] by Bartholdi and Nekrashevych. There the authors describe the discrete iterated monodromy group of an arbitrary quadratic polynomial over $\mathbb{C}$ in terms of generators satisfying explicit recursion relations similar to (0.3). In fact, the difference is only that some of the terms $(a_j, 1)$ may be replaced by $(1, a_j)$, and (a_j, a_k) may be replaced by (a_k, a_j). This goes a large part of the way towards our result that the closure G^{geom} is conjugate to our group G in all cases.

Finally, some arithmetic aspects of iterated monodromy groups associated to quadratic polynomials are studied in Boston-Jones [3], [4], [14]. The author hopes that the results of the present article might shed more light in these directions.

Here are several open questions that one might pursue next. Within the scope of the present paper, can some of the many case distinctions be avoided using a different setup? It would also be interesting to obtain more results about conjugacy of generators and odometers in the strictly pre-periodic case, like an improvement of Proposition 3.4.4 and analogues of Theorem 2.7.4 (b) and Theorem 2.7.6. Again, such results might show the way towards a cleaner overall structure of the material.

Beyond that, a very natural problem is to generalize the results of this article to iterated monodromy groups of rational quadratic morphisms instead of quadratic polynomials. Since the classification of finite postcritical orbits of those involves tuples of four integers, as opposed to two integers for quadratic polynomials, one can expect the complexity to increase roughly by a factor of 2 on a logarithmic scale. ☺

Finally there is the wide open field of applying the present results to the arithmetic properties of iterated quadratic polynomials, especially over a number field or a finite field. A starting point for this might be a study of Frobenius elements in G^{arith}.

At last, the author would like to thank Volodia Nekrashevych for introducing him to important techniques in the area.

1 Generalities

1.1 Basics

Let T be the infinite tree whose vertices are the finite words over the alphabet $\{0,1\}$ and where each vertex t is connnected by an edge to the vertices $0t$ and $1t$. The empty word is called the *root of T*, making T an infinite regular binary tree. For any integer $n \geqslant 0$ we let T_n denote the finite rooted subtree whose vertices are all words of length $\leqslant n$. The words of length n are precisely the vertices at distance n from the root; we call the set of these the *level n of T*. Thus the level n consists of 2^n points.

Unfortunately there do not seem to be established abbreviations for the automorphism groups of T_n and T. In this article we will write $W_n := \operatorname{Aut}(T_n)$ and $W := \operatorname{Aut}(T)$, based on the vague justification that $\operatorname{Aut}(T_n)$ is an iterated $\underline{w}$reath product.

Namely, for any elements $w, w' \in W$ let (w, w') denote the element of W defined by $0t \mapsto 0w(t)$ and $1t \mapsto 1w'(t)$ for any word t. This defines an embedding of $W \times W$ into W which we identify with its image. Let $\sigma \in W$ denote the element of order 2 defined by $0t \mapsto 1t \mapsto 0t$ for any word t, and let $\langle \sigma \rangle$ be the subgroup of W generated by it. Then we can write W as the semidirect product

$$(1.1.1) \qquad\qquad W = (W \times W) \rtimes \langle \sigma \rangle.$$

For any integer $n \geqslant 1$ the same definitions define a semidirect product decomposition

$$(1.1.2) \qquad\qquad W_n = (W_{n-1} \times W_{n-1}) \rtimes \langle \sigma \rangle.$$

Since $W_0 = 1$, this describes W_n as an iterated wreath product. Calculating with this decomposition requires only the basic relations

$$(1.1.3) \qquad\qquad \begin{cases} (w, w')\,(v, v') & = \ (wv, w'v') \\ \sigma\,(w, w') & = \ (w', w)\,\sigma \\ \sigma^2 & = \ 1 \end{cases}$$

for all $w, w', v, v' \in W$.

Every automorphism of T fixes the root and thus stabilizes T_n for every $n \geqslant 0$. The restriction of automorphisms therefore induces a natural homomorphism $W \to W_n$, $w \mapsto w|_{T_n}$. This homomorphism is surjective and induces an isomorphism $W \cong \varprojlim_n W_n$. Since W_n is finite, this description realizes W as a profinite topological group.

All subgroups $G \subset W$ that we study in this article are closed and hence again profinite. Throughout we let G_n denote the image of G in W_n. Since G is closed, we obtain a natural isomorphism $G \cong \varprojlim_n G_n$.

For any subset S of a group we write $\langle S \rangle$ for the subgroup generated by S and abbreviate $\langle w_1, \ldots, w_r \rangle := \langle \{w_1, \ldots, w_r\} \rangle$. If the ambient group is a topological group, the closures of these subgroups are denoted $\langle\!\langle S \rangle\!\rangle$ and $\langle\!\langle w_1, \ldots, w_r \rangle\!\rangle$.

1.2 Size

For any integer $n \geqslant 1$ the decomposition (1.1.2) implies that $|W_n| = 2 \cdot |W_{n-1}|^2$. Since $|W_0| = 1$, by induction on n this easily implies that

$$(1.2.1) \qquad\qquad |W_n| = 2^{2^n - 1} \qquad\qquad \text{for all } n \geqslant 0.$$

In particular W_n is a finite 2-group, and so $W = \varprojlim_n W_n$ is a pro-2-group.

The size of a closed subgroup $G \subset W$ is measured by its *Hausdorff dimension*, which is defined as

$$(1.2.2) \qquad\qquad \lim_{n \to \infty} \frac{\log_2 |G_n|}{\log_2 |W_n|} = \lim_{n \to \infty} \frac{\log_2 |G_n|}{2^n - 1}$$

if this limit exists. Its calculation usually requires some kind of recursive description of G.

1.3 Conjugacy

Lemma 1.3.1 *Let G be a profinite group given as the inverse limit of a filtered system of finite groups G_i such that the projection maps $G \to G_i$ are surjective. Then two elements $g, g' \in G$ are conjugate if and only if their images in G_i are conjugate for all i.*

Proof. The 'only if' part is obvious. For the 'if' part assume that the images of g, g' in G_i are conjugate for all i. For each i let U_i denote the set of elements $u \in G$ for which the images of ugu^{-1} and g' in G_i coincide. Since U_i is a union of cosets under the kernel of $G \twoheadrightarrow G_i$, which is an open subgroup of G, it is a closed subset of G. By assumption it is also non-empty. Moreover, for any transition morphism $G_j \twoheadrightarrow G_i$ in the system we have $U_j \subset U_i$. By the compactness of G it thus follows that the intersection U of all U_i is non-empty. Any element $u \in U$ then satisfies $ugu^{-1} = g'$, as desired. $\square$

The following result uses only the basic relations (1.1.3) and is a good warm up exercise for our later calculations (compare [6, Thm.3.1]).

Proposition 1.3.2 *For any $w \in W$ and any $k \in \mathbb{Z}_2^\times$ the element w^k is conjugate to w.*

Proof. By Lemma 1.3.1 it suffices to prove the corresponding statement in W_n for every $n \geqslant 0$, which we will achieve by induction on n. The statement is trivial in W_0, so assume that $n > 0$ and that it is true in W_{n-1}. Consider an element $w \in W_n$.

If $w = (u, v)$ for $u, v \in W_{n-1}$, by the induction hypothesis there exist $x, y \in W_{n-1}$ such that $xux^{-1} = u^k$ and $yvy^{-1} = v^k$. With $z := (x, y) \in W_n$ we then have

$$zwz^{-1} = (x, y)(u, v)(x, y)^{-1} = (xux^{-1}, yvy^{-1}) = (u^k, v^k) = w^k,$$

as desired. Otherwise we have $w = (u, v)\,\sigma$ for $u, v \in W_{n-1}$. After replacing w by its conjugate

$$(1, v)^{-1}(u, v)\,\sigma\,(1, v) = (1, v^{-1})(u, v)(v, 1)\,\sigma = (uv, 1)\,\sigma$$

we may without loss of generality assume that $v = 1$ and $w = (u, 1)\,\sigma$. Then

$$w^2 \;=\; (u, 1)\,\sigma\,(u, 1)\,\sigma \;=\; (u, 1)\,(1, u)\,\sigma\,\sigma \;=\; (u, u).$$

Writing $k = 2\ell + 1$ with $\ell \in \mathbb{Z}_2$, we deduce that

$$w^k \;=\; (w^2)^\ell\, w \;=\; (u, u)^\ell\,(u, 1)\,\sigma \;=\; (u^{\ell+1}, u^\ell)\,\sigma.$$

On the other hand, the ansatz $z = (x, y)$ with $x, y \in W_{n-1}$ yields

$$zwz^{-1} \;=\; (x, y)\,(u, 1)\,\sigma\,(x, y)^{-1} \;=\; (x, y)\,(u, 1)\,(y^{-1}, x^{-1})\,\sigma \;=\; (xuy^{-1}, yx^{-1})\,\sigma.$$

Together it follows that

$$zwz^{-1} = w^k \iff \left\{ \begin{array}{c} yx^{-1} = u^\ell \quad \text{and} \\ xuy^{-1} = u^{\ell+1} \end{array} \right\} \iff \left\{ \begin{array}{c} y = u^\ell x \quad\quad \text{and} \\ xux^{-1} = u^{2\ell+1} = u^k \end{array} \right\}.$$

But by the induction hypothesis there exists $x \in W_{n-1}$ with $xux^{-1} = u^k$. Thus the equations possess a common solution, as desired. (Compare Remark 1.6.5.) $\qquad\square$

1.4   Recursive construction of elements

Let a_i be distinct new symbols for all i in a set I. For each $i \in I$ suppose that we are given finite words f_i and g_i over the alphabet $\{a_j, a_j^{-1} \mid j \in I\} \sqcup W$ as well as a number $\nu_i \in \{0, 1\}$. Here the empty word is permitted and represents the identity element $1 \in W$, as usual. Then the recursion relations

$$a_i = (f_i, g_i)\,\sigma^{\nu_i} \qquad \text{for all } i \in I$$

define unique elements of W. Indeed, the restrictions $a_i|_{T_0}$ are necessarily trivial, and if for some $n > 0$ the restrictions $a_i|_{T_{n-1}}$ are already known for all i, then the recursion relations uniquely describe the restrictions $a_i|_{T_n}$ for all i. By induction we therefore obtain unique elements $a_i|_{T_n}$ for all $n \geqslant 0$, which combine to give the desired elements $a_i \in W$.

Often f_i and g_i are words only over $\{a_j, a_j^{-1} \mid j \in I\}$, in which case the recursion relations do not involve any previously known elements of W. Nevertheless one can construct very interesting elements in this way, as in (1.6.1), (2.0.1), and (3.0.1). In general one can construct elements with special properties with respect to given elements of W, as in Remark 1.6.5, Proposition 2.6.4, and in (3.8.13).

One must be aware that different recursive descriptions can determine the same elements of W. In particular:

Proposition 1.4.1 *Assume that f_i and g_i are words over $\{a_j, a_j^{-1} \mid j \in I\}$ only and that $\nu_i = 0$ for all $i \in I$. Then $a_i = 1$ for all $i \in I$.*

Proof.   Trivially $a_i|_{T_0} = 1$ for all i, and if $a_i|_{T_{n-1}} = 1$ for all i, the recursion relations imply that $a_i|_{T_n} = 1$ for all i as well. Induction on n thus shows that $a_i = 1$ on the whole tree T. $\qquad\square$

1.5 Signs

For any integer $n \geqslant 0$, any element $w \in W$ fixes the root and thus permutes the level n of T. We let $\mathrm{sgn}_n(w)$ denote the sign of the induced permutation of the level n, which defines a homomorphism

(1.5.1)
$$\mathrm{sgn}_n \colon W \longrightarrow \{\pm 1\}.$$

For any $m \geqslant n$ this homomorphism factors through a homomorphism $W_m \to \{\pm 1\}$, which we again denote by sgn_n. For $n = 0$ the homomorphism is trivial. For $n \geqslant 1$ the definition of the embedding $W \times W \hookrightarrow W$ implies that

(1.5.2)
$$\mathrm{sgn}_n((w, w')) = \mathrm{sgn}_{n-1}(w) \cdot \mathrm{sgn}_{n-1}(w')$$

for all $w, w' \in W$. Also, for $n \geqslant 1$ the element σ of order 2 has no fixed points on level n and hence precisely 2^{n-1} orbits of length 2. Therefore

(1.5.3)
$$\mathrm{sgn}_n(\sigma) = \begin{cases} -1 & \text{if } n = 1, \\ 1 & \text{if } n \neq 1. \end{cases}$$

Together these formulas can be used to calculate the signs of any recursively described elements of W.

Example 1.5.4 Consider the elements $b_1, b_2, \ldots \in W$ defined by the recursion relations

$$\begin{cases} b_1 = \sigma \\ b_i = (b_{i-1}, 1) & \text{for all } i > 1. \end{cases}$$

Then the formula (1.5.2) implies that $\mathrm{sgn}_n(b_i) = \mathrm{sgn}_{n-1}(b_{i-1})$ for all $n \geqslant 1$ and $i > 1$. By (1.5.3) and induction it follows that for all $n, i \geqslant 1$ we have

$$\mathrm{sgn}_n(b_i) = \begin{cases} -1 & \text{if } n = i, \\ 1 & \text{if } n \neq i. \end{cases}$$

Proposition 1.5.5 *For any $n \geqslant 0$ the homomorphism*

$$W_n \to \{\pm 1\}^n, \ w \mapsto (\mathrm{sgn}_m(w))_{m=1}^n$$

induces an isomorphism from the maximal abelian factor group $W_{n,\mathrm{ab}}$ to $\{\pm 1\}^n$.

Proof. Example 1.5.4 implies that the homomorphism is surjective; hence it induces a surjective homomorphism $W_{n,\mathrm{ab}} \twoheadrightarrow \{\pm 1\}^n$. It remains to show that this is an isomorphism. For $n = 0$ that is obvious, so assume that $n > 0$ and that it is an isomorphism for W_{n-1}. Then the decomposition $W_n = (W_{n-1} \times W_{n-1}) \rtimes \langle \sigma \rangle$ implies that $W_{n,\mathrm{ab}}$ is also the maximal abelian factor group of $(W_{n-1,\mathrm{ab}} \times W_{n-1,\mathrm{ab}}) \rtimes \langle \sigma \rangle$. By the induction hypothesis this is isomorphic to the maximal abelian factor group of $(\{\pm 1\}^{n-1} \times \{\pm 1\}^{n-1}) \rtimes \langle \sigma \rangle$, where σ acts

by interchanging the two factors $\{\pm 1\}^{n-1}$. The commutators of σ with $\{\pm 1\}^{n-1} \times \{\pm 1\}^{n-1}$ form the diagonally embedded subgroup $\mathrm{diag}(\{\pm 1\}^{n-1})$, so that the maximal abelian factor group is isomorphic to $\{\pm 1\}^{n-1} \times \langle \sigma \rangle$ and hence to $\{\pm 1\}^n$. For reasons of cardinality the surjective homomorphism $W_{n,\mathrm{ab}} \twoheadrightarrow \{\pm 1\}^n$ is therefore an isomorphism. By induction this now follows for all $n \geqslant 0$. $\qquad\square$

Proposition 1.5.6 *(a) For any subgroup $G_n \subset W_n$ we have $G_n = W_n$ if and only if the combined homomorphism $G_n \to \{\pm 1\}^n$, $g \mapsto (\mathrm{sgn}_m(g))_{m=1}^n$ is surjective.*

(b) For any closed subgroup $G \subset W$ we have $G = W$ if and only if the combined homomorphism $G \to \{\pm 1\}^\infty$, $g \mapsto (\mathrm{sgn}_m(g))_{m=1}^\infty$ is surjective.

Proof. (This is essentially in Stoll [20, p. 241 Thm.].) Since W_n is a finite 2-group, it is nilpotent, and hence a subgroup $G_n \subset W_n$ is equal to W_n if and only if it surjects to the maximal abelian factor group of W_n. Thus part (a) follows from Proposition 1.5.5. Part (b) follows from (a) by taking inverse limits. $\qquad\square$

1.6   Odometers

As another useful preparation for the main part of the article (and for fun) we look at the conjugacy class of a certain special element of W called the *odometer* [12, Ex.1] or *adding machine* [18, 2.5.1]. This is the element $a \in W$ defined by the recursion relation

$$(1.6.1) \qquad\qquad\qquad\qquad a = (a, 1)\, \sigma.$$

More generally we will call any element of W that is conjugate to a an odometer. For a part of the following result compare [12, Prop.3.3]:

Proposition 1.6.2 *For any $w \in W$ the following are equivalent:*

(a) w is conjugate to a.

(b) w is conjugate to $(w, 1)\, \sigma$.

(c) w acts transitively on level n for all $n \geqslant 0$.

(d) $\mathrm{sgn}_n(w) = -1$ for all $n \geqslant 1$.

Proof. If w is conjugate to a, choose $x \in W$ such that $w = xax^{-1}$. Then

$$w \;=\; xax^{-1} \;=\; x(a,1)\,\sigma\, x^{-1} \;=\; x(x^{-1}wx, 1)\,\sigma\, x^{-1} \;=\; x(x,x)^{-1}(w,1)\,\sigma\,(x,x)\, x^{-1},$$

hence w is conjugate to $(w, 1)\, \sigma$. This proves the implication (a)$\Rightarrow$(b).

Next assume that w is conjugate to $(w,1)\,\sigma$. It is trivial that w acts transitively on level 0, so assume that $n \geqslant 1$ and that w acts transitively on level $n-1$. Using the basic relations (1.1.3) we find that w^2 is conjugate to

$$(w,1)\,\sigma\,(w,1)\,\sigma \;=\; (w,1)\,(1,w)\,\sigma\sigma \;=\; (w,w).$$

Since w acts transitively on level $n-1$, that is, on the set of words of length $n-1$, the element $(w,w) \in W$ acts transitively on the set of words of length n beginning with 0, and transitively on the set of words of length n beginning with 1. Its conjugate w^2 then has the same property. But since w is conjugate to $(w,1)\,\sigma$, it interchanges the two vertices on level 1 and thus the two subtrees emanating from them. Together it follows that w acts transitively on the set of all words of length n over $\{0,1\}$, that is, on level n. The implication (b)$\Rightarrow$(c) now follows by induction on n.

Next, if w acts transitively on a level $n \geqslant 1$, it acts by a cycle of length 2^n which has sign -1. This directly yields the implication (c)$\Rightarrow$(d).

The remaining implication (d)$\Rightarrow$(a) results from Lemma 1.3.1 and the following lemma. $\qquad\square$

Lemma 1.6.3 *For any $w \in W$ satisfying (d), the restriction $w|_{T_n}$ is conjugate to $a|_{T_n}$ in W_n for every $n \geqslant 1$.*

Proof. Since W_1 is cyclic of order 2, the assumption $\mathrm{sgn}_1(w) = -1$ implies that $w|_{T_1} = \sigma|_{T_1} = a|_{T_1}$, from which the lemma follows in the case $n = 1$. So assume that $n > 1$ and that the lemma holds for $n-1$ in place of n. Take any $w \in W$ satisfying (d). From $w|_{T_1}$ we already know that $w = (u,v)\,\sigma$ for some $u, v \in W$. Then for all $n \geqslant 1$ the formulas (1.5.2) and (1.5.3) imply that

$$\mathrm{sgn}_n(uv) \;=\; \mathrm{sgn}_n(u) \cdot \mathrm{sgn}_n(v) \cdot \mathrm{sgn}_{n+1}(\sigma) \;=\; \mathrm{sgn}_{n+1}(w) \;=\; -1.$$

By the induction hypothesis applied to uv in place of w it follows that $uv|_{T_{n-1}}$ is conjugate to $a|_{T_{n-1}}$ in W_{n-1}. Write $uv|_{T_{n-1}} = xax^{-1}|_{T_{n-1}}$ for some $x \in W$, and set $y := (x, vx) \in W$. Then

$$yay^{-1} \;=\; (x,vx)\,(a,1)\,\sigma\,(x,vx)^{-1} \;=\; (x,vx)\,(a,1)\,(x^{-1}v^{-1},x^{-1})\,\sigma \;=\; (xax^{-1}v^{-1},v)\,\sigma$$

and hence

$$yay^{-1}|_{T_n} \;=\; (xax^{-1}v^{-1}|_{T_{n-1}}, v|_{T_{n-1}})\,\sigma \;=\; (uvv^{-1}|_{T_{n-1}}, v|_{T_{n-1}})\,\sigma \;=\; ((u,v)\,\sigma)|_{T_n} \;=\; w|_{T_n},$$

proving the lemma for n. By induction the lemma follows for all $n \geqslant 1$. $\qquad\square$

Proposition 1.6.4 *For any odometer $w \in W$ we have:*

(a) *The subgroup $\langle\!\langle w \rangle\!\rangle$ of W is isomorphic to $\mathbb{Z}_2$.*

(b) It is its own centralizer.

(c) Its normalizer is isomorphic to $\mathbb{Z}_2 \rtimes \mathbb{Z}_2^\times$.

Proof. The implication (a)$\Rightarrow$(c) in Proposition 1.6.2 shows that w acts transitively on each level n through a cycle of length 2^n. For $n \to \infty$ this shows that w has infinite order, which implies (a). Assertion (b) results from the fact that in any symmetric group on m letters, any m-cycle generates its own centralizer. For (c) observe that $\mathrm{Aut}(\mathbb{Z}_2) = \mathbb{Z}_2^\times$. Moreover, for any $k \in \mathbb{Z}_2^\times$ the element $w^k \in W$ still has the same properties (c) or (d) from Proposition 1.6.2, and is therefore conjugate to w. This shows that the normalizer of $\langle\!\langle w \rangle\!\rangle$ in W surjects to $\mathrm{Aut}(\langle\!\langle w \rangle\!\rangle) = \mathbb{Z}_2^\times$. Since the centralizer is $\langle\!\langle w \rangle\!\rangle \cong \mathbb{Z}_2$, this implies (c). $\square$

Remark 1.6.5 For any $k \in \mathbb{Z}_2^\times$ we can construct an explicit element $z \in W$ satisfying $zaz^{-1} = a^k$, as follows. We repeat the calculation from the second part of the proof of Proposition 1.3.2 in the special case $w = u = a$. Writing $k = 2\ell + 1$ with $\ell \in \mathbb{Z}_2$ and using the ansatz $z = (x, y)$ we deduce that

$$zaz^{-1} = a^k \iff \left\{ \begin{array}{rl} y = a^\ell x & \text{and} \\ xax^{-1} = a^{2\ell+1} = a^k & \end{array} \right\}.$$

Thus x must satisfy the same condition as z, which suggests that the ansatz might work with $x = z$. Thus consider the recursion relation

$$z = (z, a^\ell z),$$

which yields a well-defined element of W by the construction in Subsection 1.4. To show that it really does have the desired property set $v := zaz^{-1}a^{-k}$. Repeating the calculation with this choice of z yields the recursion relation $v = (v, 1)$. By Proposition 1.4.1 this implies that $v = 1$ and hence that $zaz^{-1} = a^k$, as desired.

Moreover, if we write z_k for the element thus constructed to indicate its dependence on k, one can prove in the same fashion that $z_k \, z_{k'} = z_{kk'}$ for all $k, k' \in \mathbb{Z}_2^\times$. The construction therefore yields an explicit isomorphism $\mathbb{Z}_2 \rtimes \mathbb{Z}_2^\times \cong \mathrm{Norm}_W(\langle\!\langle a \rangle\!\rangle)$.

1.7 Iterated monodromy groups

Let k be a field of characteristic different from 2. Let $f(X) \in k[X]$ be a polynomial of degree two, which we view as a morphism from the projective line $\mathbb{P}^1_k$ over k to itself. For any integer $n \geqslant 1$ we let f^n denote the composite of n copies of f.

The morphism f has precisely two critical points, namely ∞ and, say, $\xi \in k$. The first of these is mapped to itself under f. For the other we abbreviate $\xi_n := f^n(\xi)$ for all $n \geqslant 1$, so that the (strictly) *postcritical orbit* of f is the set

$$(1.7.1) \qquad\qquad S := \{\infty\} \cup \{\xi_n \mid n \geqslant 1\}.$$

This is precisely the set of points of $\mathbb{P}^1_k$ over which some iterate $f^n \colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ is ramified. We view it as the set of vertices of a directed graph with an edge from any point to its image under f. The 'entry points' ∞ and ξ_1 will be specially marked. We distinguish the following three cases:

Cases 1.7.2 (a) **Infinite case:** Here all ξ_n are distinct:
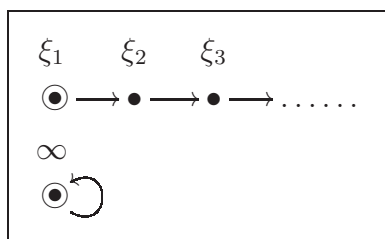
(b) **Periodic case:** Here the critical point ξ is *periodic*, that is, equal to ξ_r for some $r \geqslant 1$. We let r be the smallest such integer, so that the postcritical orbit looks like this:
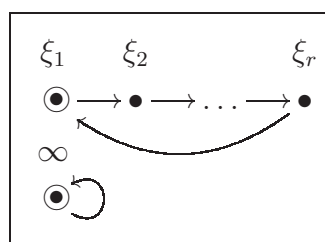
(c) **Strictly pre-periodic case:** Here the critical point ξ is not periodic, but it is *pre-periodic*, that is, it satisfies an equation of the form $\xi_{r+1} = \xi_{s+1}$ for some $r > s \geqslant 0$. We let s and r be the smallest such integers. Then s cannot be 0, because that would imply $\xi_r = \xi$. Thus $r > s \geqslant 1$ and the postcritical orbit looks like this:
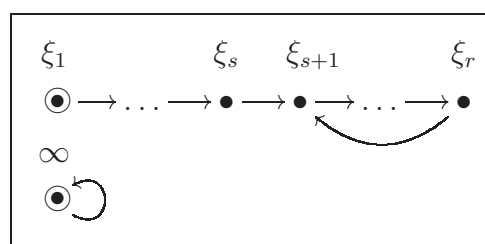
Fix an algebraically closed overfield L of k and a geometric point $x_0 \in \mathbb{P}^1(L) \smallsetminus S$. For instance, any L-valued point that is not algebraic over k is in order. For any $n \geqslant 0$ let $f^{-n}(x_0)$ denote the set of 2^n points $x_n \in \mathbb{P}^1(L)$ with $f^n(x_n) = x_0$. Let T_{x_0} denote the infinite graph whose set of vertices is the external disjoint union $\coprod_{n \geqslant 0} f^{-n}(x_0)$, where any vertex $x_n \in f^{-n}(x_0)$ for $n > 0$ is connected by an edge towards $f(x_n) \in f^{-(n-1)}(x_0)$. By construction this is a regular rooted binary tree with root $x_0 \in f^{-0}(x_0)$ and level n set $f^{-n}(x_0)$ for every n.

For any $n \geqslant 1$ the morphism $f^n \colon \mathbb{P}_k^1 \to \mathbb{P}_k^1$ defines a connected unramified covering of $\mathbb{P}_k^1 \smallsetminus S_n$ for the finite set $S_n := \{\infty, \xi_1, \ldots, \xi_n\}$. Up to isomorphism this covering is determined by the associated monodromy action on $f^{-n}(x_0)$ of the étale fundamental group $\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S_n, x_0)$. Varying n, these actions combine to a natural continuous homomorphism

$$(1.7.3) \qquad \rho \colon \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0) := \varprojlim_n \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S_n, x_0) \longrightarrow \operatorname{Aut}(T_{x_0}),$$

which encodes the Galois theoretic properties of the whole tower of ramified coverings f^n.

Let $\bar{k}$ denote the separable closure of k in L. Then there is a natural short exact sequence

$$(1.7.4) \qquad 1 \longrightarrow \pi_1^{\text{ét}}(\mathbb{P}_{\bar{k}}^1 \smallsetminus S, x_0) \longrightarrow \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0) \longrightarrow \operatorname{Gal}(\bar{k}/k) \longrightarrow 1.$$

We are interested in the images

$$(1.7.5) \qquad G^{\text{geom}} := \rho\big(\pi_1^{\text{ét}}(\mathbb{P}_{\bar{k}}^1 \smallsetminus S, x_0)\big) \subset \operatorname{Aut}(T_{x_0}),$$
$$(1.7.6) \qquad G^{\text{arith}} := \rho\big(\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0)\big) \subset \operatorname{Aut}(T_{x_0}),$$

which are called the *geometric*, respectively *arithmetic, iterated monodromy group* associated to f. By construction G^{geom} is a closed normal subgroup of G^{arith}, and the short exact sequence (1.7.4) induces a surjective homomorphism

$$(1.7.7) \qquad \operatorname{Gal}(\bar{k}/k) \twoheadrightarrow G^{\text{arith}}/G^{\text{geom}}.$$

These groups are independent of the choice of L and x_0 in the sense that they do not change when L is replaced by any algebraically closed overfield, and for a different choice of x_0 there exists an isomorphism between the two resulting trees which is equivariant for the monodromy action. Thus if we identify T_{x_0} with any other regular rooted binary tree, the resulting monodromy groups will be unique up to conjugacy there. Throughout the following we will identify T_{x_0} with the standard tree T from Subsection 1.1.

The group G^{geom} also does not change under extending k. Thus in principle it can be calculated over any field of definition of the quadratic polynomial f. In particular, if k has characteristic zero, then G^{geom} can be calculated over $\mathbb{C}$. It is then the closure of the image of the topological fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) \smallsetminus S, x_0)$. The latter can be described by explicit generators as a self-similar subgroup of $\operatorname{Aut}(T)$ as, say, in Nekrashevych [15], [16, Ch.5], [18], Bartholdi-Nekrashevych [2], Dau [5], Grigorchuk et al. [11]. Moreover, in [19] we showed how this in turn can be used to describe G^{geom} in positive characteristic as well by lifting the given quadratic polynomial to characteristic zero.

In the present article, however, we are only interested in the profinite monodromy groups, and we will determine them using only the self-similarity of the monodromy representation and the combinatorics of the postcritical orbit, as follows.

Let x_1 and x_1' denote the two points in $f^{-1}(x_0)$. Then $f^{-(n+1)}(x_0) = f^{-n}(x_1) \sqcup f^{-n}(x_1')$ for all $n \geqslant 0$, so after deleting the root x_0 the tree T_{x_0} decomposes into the two regular

16

rooted binary trees T_{x_1} and $T_{x_1'}$ with roots x_1 and x_1', respectively. Abbreviate $\tilde{S} := f^{-1}(S)$ $\subset \mathbb{P}_k^1$. Then by functoriality $f : \mathbb{P}_k^1 \to \mathbb{P}_k^1$ induces a homomorphism

$$(1.7.8) \qquad f_* : \pi_1^{\text{ét}}\big(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1\big) \longrightarrow \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0).$$

Its image is the subgroup of index 2 of $\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0)$ which fixes $x_1 \in f^{-1}(x_0)$. It therefore fixes both x_1 and x_1' and acts on each of the subtrees T_{x_1} and $T_{x_1'}$.

To describe the action on these subtrees note that the inclusion $f(S) \subset S$ implies that $S \subset \tilde{S}$ and hence $\mathbb{P}_k^1 \smallsetminus \tilde{S} \subset \mathbb{P}_k^1 \smallsetminus S$. Thus there is a natural surjective homomorphism

$$(1.7.9) \qquad \text{id}_* : \pi_1^{\text{ét}}\big(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1\big) \longrightarrow\!\!\!\!\rightarrow \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_1).$$

The action of $\pi_1^{\text{ét}}\big(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1\big)$ on T_{x_1} through f_* is the same as that obtained by composing (1.7.9) with the natural action of $\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_1)$ on T_{x_1}. On the other hand let τ denote the non-trivial covering automorphism of $f : \mathbb{P}_k^1 \to \mathbb{P}_k^1$, so that $x_1' = \tau(x_1)$. Then τ induces a natural isomorphism

$$(1.7.10) \qquad \tau_* : \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1) \xrightarrow{\sim} \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1').$$

The action of $\pi_1^{\text{ét}}\big(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1\big)$ on $T_{x_1'}$ through f_* is the same as that obtained by composing (1.7.10) with the surjection (1.7.9) for x_1' in place of x_1 and the natural action of $\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_1')$ on $T_{x_1'}$.

Now recall that except for the change of base point, the actions of $\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x)$ on T_x for $x = x_0, x_1, x_1'$ all describe the same inverse system of ramified coverings $f^n : \mathbb{P}_k^1 \to \mathbb{P}_k^1$. Choose isomorphisms $T_{x_1} \cong T_{x_0} \cong T_{x_1'}$ and corresponding identifications of the respective fundamental groups (which over $\mathbb{C}$ usually involves choosing paths from x_0 to x_1 and x_1'). Then the above statements say that the monodromy actions $\rho \circ f_*$ and $(\rho \circ \text{id}_*, \rho \circ \text{id}_* \circ \tau_*)$ of $\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_0)$ on $T_{x_0} \smallsetminus \{x_0\} = T_{x_1} \sqcup T_{x_1'}$ coincide. In particular, with the identifications $T_{x_0} \cong T$ and $\text{Aut}(T_{x_0}) \cong W$ we obtain a commutative diagram:

(1.7.11)

$$
\begin{array}{ccccc}
\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0) & \xrightarrow{\ \rho\ } & \text{Aut}(T_{x_0}) & =\!\!=\!\!\overset{\sim}{=\!\!=\!\!=} & W \\
{\scriptstyle f_*}\big\uparrow & & \big\uparrow & & \big\uparrow \\
\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1) & \longrightarrow & \text{Aut}(T_{x_1}) \times \text{Aut}(T_{x_1'}) & =\!\!=\!\!\overset{\sim}{=\!\!=\!\!=} & W \times W \\
{\scriptstyle \wr}\big\| & & {\scriptstyle \text{pr}_1}\big\downarrow & & {\scriptstyle \text{pr}_1}\big\downarrow \\
\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_0) & & \text{Aut}(T_{x_1}) & =\!\!=\!\!\overset{\sim}{=\!\!=\!\!=} & W \\
{\scriptstyle \text{id}_*}\big\downarrow & & {\scriptstyle \wr}\big\| & & \big\| \\
\pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0) & \xrightarrow{\ \rho\ } & \text{Aut}(T_{x_0}) & =\!\!=\!\!\overset{\sim}{=\!\!=\!\!=} & W
\end{array}
$$

This shows that the monodromy representation ρ is *fractal* or *self-similar* in that a copy of ρ occurs in a proper subquotient. The analysis of ρ and of its geometric and arithmetic monodromy groups therefore lends itself to recursive arguments.

By the construction of G^{arith} the diagram (1.7.11) induces a commutative diagram:

$$
(1.7.12) \qquad
\begin{array}{ccccc}
\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_k^1 \smallsetminus S, x_0) & \xrightarrow{\ \rho\ } & G^{\mathrm{arith}} & \hookrightarrow & W \\[2pt]
\uparrow{\scriptstyle f_*} & & \uparrow & & \uparrow \\[6pt]
\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_k^1 \smallsetminus \tilde{S}, x_1) & \longrightarrow & G^{\mathrm{arith}} \cap (W \times W) & \hookrightarrow & W \times W \\[2pt]
\downarrow{\scriptstyle \mathrm{id}_*} & & \downarrow{\scriptstyle \mathrm{pr}_1} & & \downarrow{\scriptstyle \mathrm{pr}_1} \\[6pt]
\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_k^1 \smallsetminus S, x_0) & \xrightarrow{\ \rho\ } & G^{\mathrm{arith}} & \hookrightarrow & W
\end{array}
$$

Here the lower middle vertical arrow is surjective, because the others in the lower left square are surjective. Thus G^{arith} is *self-similar* in that it is isomorphic to a proper subquotient of itself. With $\bar{k}$ in place of k, the same remarks apply to G^{geom} and the commutative diagram:

$$
(1.7.13) \qquad
\begin{array}{ccccc}
\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_{\bar{k}}^1 \smallsetminus S, x_0) & \xrightarrow{\ \rho\ } & G^{\mathrm{geom}} & \hookrightarrow & W \\[2pt]
\uparrow{\scriptstyle f_*} & & \uparrow & & \uparrow \\[6pt]
\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_{\bar{k}}^1 \smallsetminus \tilde{S}, x_1) & \longrightarrow & G^{\mathrm{geom}} \cap (W \times W) & \hookrightarrow & W \times W \\[2pt]
\downarrow{\scriptstyle \mathrm{id}_*} & & \downarrow{\scriptstyle \mathrm{pr}_1} & & \downarrow{\scriptstyle \mathrm{pr}_1} \\[6pt]
\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_{\bar{k}}^1 \smallsetminus S, x_0) & \xrightarrow{\ \rho\ } & G^{\mathrm{geom}} & \hookrightarrow & W
\end{array}
$$

Note that the groups G^{arith} and G^{geom} and several of the maps in these diagrams depend on the chosen identifications of trees and are therefore unique only up to conjugacy by W.

Now we can describe generators of G^{geom}. Suppose first that S is finite. Let Δ denote the maximal pro-2 factor group of the group $\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_k^1 \smallsetminus S, x_0)$. Since the characteristic of k is different from 2, by Grothendieck's description of the tame fundamental group [13, exp. XIII, Cor. 2.12] there exist generators $\delta_\infty, \delta_{\xi_1}, \ldots, \delta_{\xi_r}$ of the respective pro-2 inertia groups at suitable geometric points above $\infty, \xi_1, \ldots, \xi_r$, such that Δ is the quotient of the free pro-2 group on these elements by the single relation $\delta_\infty \cdot \delta_{\xi_1} \cdots \delta_{\xi_r} = 1$.

For every $1 \leqslant i \leqslant r$ set $b_i := \rho(\delta_{\xi_i}) \in G^{\mathrm{geom}}$. Then $b_\infty := \rho(\delta_\infty) = (b_1 \cdots b_r)^{-1}$, so we can drop it from the list of generators and obtain

$$
G^{\mathrm{geom}} = \langle\!\langle b_1, \ldots, b_r \rangle\!\rangle.
$$

If S is infinite, we can apply the same argument to $\pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_k^1 \smallsetminus S_n, x_0)$ for every $n \geqslant 1$, which naturally acts on the finite tree T_n of level $\leqslant n$. If $b_{i,n} \in W_n = \mathrm{Aut}(T_n)$ denotes the image of a suitable generator of an inertia group above ξ_i, we deduce that $G_n^{\mathrm{geom}} = \langle b_{1,n}, \ldots, b_{n,n} \rangle$.

Passing to the limit over n we obtain elements $b_i \in W$ representing the inertia above x_i for all $i \geqslant 1$, such that
$$G^{\mathrm{geom}} = \langle\!\langle b_1, b_2, b_3, \ldots \rangle\!\rangle.$$
In this case we have $b_\infty := \rho(\delta_\infty) = (b_1 b_2 \cdots)^{-1}$, where the infinite product converges in the profinite group because $b_i \to 1$ for $i \to \infty$.

According to the cases in 1.7.2 the generators enjoy the following recursion relations up to conjugacy:

Proposition 1.7.14 *The following elements are conjugate under W:*

$$\left\{ \begin{array}{l} b_1 \text{ is conjugate to } \sigma \text{ in the cases (a) and (c).} \\ b_1 \text{ is conjugate to } (b_r, 1)\,\sigma \text{ in the case (b).} \\ b_i \text{ is conjugate to } (b_{i-1}, 1) \text{ if } i > 1, \text{ except if } i = s+1 \text{ in the case (c).} \\ b_{s+1} \text{ is conjugate to } (b_s, b_r) \text{ in the case (c).} \\ b_\infty \text{ is conjugate to } (b_\infty, 1)\,\sigma. \end{array} \right\}$$

Proof. First consider the point ξ_i for any $i > 1$. Then the morphism f is unramified over ξ_i, and $f^{-1}(\xi_i)$ consists of ξ_{i-1} and precisely one other point, say, η. The unramifiedness means that the inertia group above ξ_i acts trivially on the covering $f\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$, and hence that b_i acts trivially on level 1 of the tree T. Thus $b_i = (c, d)$ for certain elements $c, d \in W$. Also, under the functoriality of the fundamental group f_* sends a generator of an inertia group above ξ_{i-1} to a generator of an inertia group above ξ_i. This means that T with the action of $\delta_{\xi_{i-1}}$ is isomorphic to one half subtree of T with the action of δ_{ξ_i}, or equivalently, that c or d is conjugate to b_{i-1}. The other of the two entries c, d arises in the same way from the inertia at η. For this there are two possibilities.

If $i = s+1$ in the case 1.7.2 (c), the diagram there shows that $\eta = \xi_r$. In this case the same argument as above shows that the other entry among c, d is conjugate to b_r. Thus $b_i = b_{s+1}$ is conjugate to (b_s, b_r) or to (b_r, b_s). As these two elements of W are already conjugate to each other under $\sigma \in W$, it follows that anyway b_{s+1} is conjugate to (b_s, b_r).

In all other cases with $i > 1$ we have $\eta \notin S$. Then the whole tower of coverings is unramified above η, and so the other entry is 1. In that case we find that b_i is conjugate to $(b_{i-1}, 1)$ or $(1, b_{i-1})$, and hence anyway to $(b_{i-1}, 1)$.

Next consider the point ξ_1. Here the morphism f is ramified over ξ_1, so that $f^{-1}(\xi_1)$ consists of one point only, say, of η. The ramifiedness means that the inertia group above ξ_1 acts non-trivially on the covering $f\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$, and hence that b_1 acts non-trivially on level 1 of the tree T. Thus $b_1 = (c, d)\,\sigma$ for certain elements $c, d \in W$. Also, since f has ramification degree 2 at η, under the functoriality of the fundamental group f_* sends a generator of an inertia group above η to the square of a generator of an inertia group above ξ_1. Since $b_1^2 = (c, d)\,\sigma\,(c, d)\,\sigma = (cd, dc)$, we deduce that the image of a generator of an inertia group above η is conjugate to cd. Again there are now two possibilities.

In the case 1.7.2 (b) we have $\eta = \xi_r$. The same argument as above then shows that cd is conjugate to b_r. Writing $cd = w b_r w^{-1}$ for some $w \in W$, we then find that

$$
\begin{aligned}
b_1 \;=\; (c, d)\,\sigma \;&=\; (w b_r w^{-1} d^{-1}, d)\,\sigma \\
&=\; (w, dw)\,(b_r, 1)\,(w^{-1} d^{-1}, w^{-1})\,\sigma \\
&=\; (w, dw)\,(b_r, 1)\,\sigma\,(w, dw)^{-1}.
\end{aligned}
$$

Thus b_1 is conjugate to $(b_r, 1)\,\sigma$ in this case.

In the cases 1.7.2 (a) and (c) we have $\eta \notin S$; hence the same argument as above now shows that $cd = 1$. Thus

$$
b_1 \;=\; (c, d)\,\sigma \;=\; (c, c^{-1})\,\sigma \;=\; (c, 1)\,\sigma\,(c, 1)^{-1},
$$

and so b_1 is conjugate to σ in this case.

Finally consider the point ∞, which is ramified and mapped to itself under f. The ramifiedness means that $b_\infty = (c, d)\,\sigma$ for some $c, d \in W$. Also, under the functoriality of the fundamental group f_* sends a generator of an inertia group above ∞ to the square of a generator of an inertia group above ∞. Since $b_\infty^2 = (c, d)\,\sigma\,(c, d)\,\sigma = (cd, dc)$, we find that cd is conjugate to b_∞. The same calculation as above thus shows that b_∞ is conjugate to $(b_\infty, 1)\,\sigma$. We have therefore proved the proposition in all cases. $\qquad\square$

The determination of G^{geom} will be based solely on the recursion relations from Proposition 1.7.14. The results in the respective cases are Theorems 1.8.2, 2.8.2, and 3.10.2. For the description of G^{arith} see Theorems 1.8.2, 2.8.4, 3.10.5, and Corollary 3.10.6.

Also note that by Proposition 1.6.2, the last line of Proposition 1.7.14 means that b_∞ is an odometer. This fact will be exploited in Sections 2.8 and 3.10.

1.8 Infinite case

This is the case where f has an infinite postcritical orbit. Thus $G^{\mathrm{geom}} = \langle\!\langle b_1, b_2, b_3, \ldots \rangle\!\rangle$, where by Proposition 1.7.14 the generators satisfy:

(1.8.1)
$$
\left\{
\begin{array}{l}
b_1 \text{ is conjugate to } \sigma \text{ under } W, \text{ and} \\
b_i \text{ is conjugate to } (b_{i-1}, 1) \text{ under } W \text{ for any } i > 1.
\end{array}
\right\}
$$

Theorem 1.8.2 *In this case $G^{\mathrm{geom}} = G^{\mathrm{arith}} = W$.*

Proof. The same calculation as in Example 1.5.4 shows that for all $n, i \geqslant 1$ we have

$$
\mathrm{sgn}_n(b_i) \;=\;
\left\{
\begin{array}{ll}
-1 & \text{if } n = i, \\
1 & \text{if } n \neq i
\end{array}
\right.
$$

Thus Proposition 1.5.6 (b) implies that $G^{\mathrm{geom}} = W$. Since $G^{\mathrm{geom}} \subset G^{\mathrm{arith}} \subset W$, both inclusions must be equalities. $\qquad\square$

2 Periodic case

Throughout this section we fix an integer $r \geqslant 1$. Using the construction from Subsection 1.4 we define elements $a_1, \ldots, a_r \in W$ by the recursion relations

$$(2.0.1) \qquad \left\{ \begin{array}{ll} a_1 = (a_r, 1)\, \sigma, \\ a_i = (a_{i-1}, 1) & \text{for } 2 \leqslant i \leqslant r. \end{array} \right\}$$

We will study the subgroup $G := \langle\!\langle a_1, \ldots, a_r \rangle\!\rangle \subset W$ and its images $G_n \subset W_n$ for all n. The recursion relations are only one choice encoding the qualitative recursive behavior of the generators described by the diagram

$$(2.0.2)$$

where the vertices are now marked by the generators and the superfluous generator corresponding to the critical point ∞ is dropped: see Subsection 1.7. In Subsection 2.4 we will show that many other choices yield the same group G up to conjugacy in W.

2.1 Basic properties

Proposition 2.1.1 *For all $n \geqslant 1$ and all $1 \leqslant i \leqslant r$ we have*

$$\mathrm{sgn}_n(a_i) = \left\{ \begin{array}{ll} -1 & \text{if } n \equiv i \bmod r, \\ 1 & \text{if } n \not\equiv i \bmod r. \end{array} \right.$$

Proof. The definition of a_i implies that $\mathrm{sgn}_1(a_1) = -1$ and $\mathrm{sgn}_1(a_i) = 1$ for all $2 \leqslant i \leqslant r$; hence the proposition holds for $n = 1$. For $n > 1$ the formulas (1.5.2) and (1.5.3) imply that $\mathrm{sgn}_n(a_1) = \mathrm{sgn}_{n-1}(a_r)$ and $\mathrm{sgn}_n(a_i) = \mathrm{sgn}_{n-1}(a_{i-1})$ for all $2 \leqslant i \leqslant r$. Thus the proposition for $n-1$ implies the proposition for n, and so we are done by induction. $\qquad\square$

Proposition 2.1.2 *For any $n \geqslant 0$ we have $G_n = W_n$ if and only if $n \leqslant r$.*

Proof. Direct consequence of Propositions 1.5.6 (a) and 2.1.1. $\qquad\square$

Proposition 2.1.3 *The group G acts transitively on the level n of T for every $n \geqslant 0$.*

Proof. Consider the element $w := a_1 \cdots a_r \in G$. Proposition 2.1.1 implies that $\mathrm{sgn}_n(w) = -1$ for all $n \geqslant 1$; hence w already acts transitively on every level by Proposition 1.6.2. $\qquad\square$

Proposition 2.1.4 *Each generator a_i has infinite order.*

Proof. If not, there exist $1 \leqslant i \leqslant r$ and $n \geqslant 0$ with $a_i^{2^n} = 1$. Among all such pairs (i, n) select one for which $i + rn$ is minimal. If $i > 1$, the recursion relation implies that $(a_{i-1}^{2^n}, 1) = a_i^{2^n} = 1$ and hence $a_{i-1}^{2^n} = 1$, contradicting the minimality of $i + rn$. Thus we must have $i = 1$. Since $a_1 \neq 1$, we then have $n \geqslant 1$. We can therefore calculate

$$1 = a_1^{2^n} = (a_1^2)^{2^{n-1}} = \big((a_r, 1)\, \sigma\, (a_r, 1)\, \sigma\big)^{2^{n-1}} = \big((a_r, a_r)\big)^{2^{n-1}} = (a_r^{2^{n-1}}, a_r^{2^{n-1}})$$

and deduce that $a_r^{2^{n-1}} = 1$. Since $r + r(n-1) = rn < 1 + rn$, this again contradicts the minimality of $i + rn$. Thus we have a contradiction in all cases, as desired. $\qquad\square$

Lemma 2.1.5 *For any $1 \leqslant i \leqslant r$ and $n \geqslant 0$ we have $a_i|_{T_n} = 1$ if and only if $n < i$.*

Proof. Direct consequence of the recursion relations (2.0.1). $\qquad\square$

More precise statements about the generators are given in Lemma 2.2.5 (a) below.

2.2 Useful subgroups

First we consider the subgroup of index 2 which acts trivially on level 1:

$$(2.2.1) \qquad\qquad G^1 \;:=\; G \cap (W \times W).$$

Let pr_1 and $\mathrm{pr}_2\colon W \times W \to W$ denote the two projections. We have the following self-similarity properties:

Proposition 2.2.2 *(a) $G \subset (G \times G) \rtimes \langle \sigma \rangle$.*

   (b) $G^1 \subset (G \times G)$.

   (c) $\mathrm{pr}_1(G^1) = \mathrm{pr}_2(G^1) = G$.

Proof. By the recursion relations (2.0.1), the generators of G lie in $(G \times G) \rtimes \langle \sigma \rangle$, hence so does G, proving (a). Also, (a) directly implies (b). In particular G^1 contains the elements $a_1^2 = (a_r, 1)\, \sigma\, (a_r, 1)\, \sigma = (a_r, a_r)$ as well as $a_i = (a_{i-1}, 1)$ for all $2 \leqslant i \leqslant r$. Thus $\mathrm{pr}_1(G^1)$ contains the elements a_r as well as a_{i-1} for all $2 \leqslant i \leqslant r$, that is, all the generators of G, proving that $\mathrm{pr}_1(G^1) = G$. Finally, conjugation by the element $a_1 = (a_r, 1)\, \sigma \in G$ interchanges the two factors of $W \times W$ and normalizes G^1; hence also $\mathrm{pr}_2(G^1) = G$, and we are done. $\qquad\square$

Next, for every $1 \leqslant i \leqslant r$ we consider the subgroup

$$(2.2.3) \qquad\qquad H^{(i)} \;:=\; \left\{ \begin{array}{l} \text{closure of the subgroup of } G \text{ generated} \\ \text{by all } G\text{-conjugates of } a_j \text{ for all } j \neq i. \end{array} \right\}.$$

By construction this is a normal subgroup of G, and G is the product $H^{(i)} \cdot \langle\!\langle a_i \rangle\!\rangle$.

Lemma 2.2.4 *(a) $H^{(1)} = H^{(r)} \times H^{(r)}$.*

(b) For any $i > 1$ we have $H^{(i)} \cap (W \times W) \subset (H^{(i-1)} \times H^{(i-1)}) \cdot \langle\!\langle\!\langle (a_{i-1}, a_{i-1}^{-1}) \rangle\!\rangle\!\rangle$.

Proof. By definition $H^{(1)}$ is the closure of the subgroup generated by the conjugates $z a_j z^{-1}$ for all $2 \leqslant j \leqslant r$ and $z \in G$. In the case $z = (x, y) \in G^1$ these conjugates are

$$z a_j z^{-1} = (x, y) (a_{j-1}, 1) (x, y)^{-1} = (x a_{j-1} x^{-1}, 1).$$

Here Proposition 2.2.2 (c) shows that x runs through all of G, so the closure of the subgroup generated by the G^1-conjugates only is $H^{(r)} \times 1$. Conjugating this by $a_1 = (a_r, 1)\, \sigma$ yields the subgroup $1 \times H^{(r)}$. Thus all G-conjugates together yield the subgroup $H^{(r)} \times H^{(r)}$, proving (a).

Now consider the case $i > 1$. Then $H^{(i-1)} \times H^{(i-1)}$ is a closed normal subgroup of $(G \times G) \rtimes \langle \sigma \rangle$, and the group $(\langle\!\langle a_{i-1} \rangle\!\rangle \times \langle\!\langle a_{i-1} \rangle\!\rangle) \rtimes \langle \sigma \rangle$ surjects to the associated factor group. Also, the subgroup $\langle\!\langle (a_{i-1}, a_{i-1}^{-1}) \rangle\!\rangle$ is normal in $(\langle\!\langle a_{i-1} \rangle\!\rangle \times \langle\!\langle a_{i-1} \rangle\!\rangle) \rtimes \langle \sigma \rangle$ and the factor group is abelian. Therefore $K := (H^{(i-1)} \times H^{(i-1)}) \cdot \langle\!\langle (a_{i-1}, a_{i-1}^{-1}) \rangle\!\rangle$ is a closed normal subgroup of $(G \times G) \rtimes \langle \sigma \rangle$ with an abelian factor group.

For all $2 \leqslant j \leqslant r$ with $j \neq i$ we have $a_{j-1} \in H^{(i-1)}$ and hence $a_j = (a_{j-1}, 1) \in K$. Also, we have $a_r \in H^{(i-1)}$ and hence $a_1^2 = ((a_r, 1)\, \sigma)^2 = (a_r, a_r) \in K$. Moreover, since the factor group $((G \times G) \rtimes \langle \sigma \rangle)/K$ is abelian, the subgroup $\tilde{K} := K \cdot \langle a_1 \rangle$ is again normal in $(G \times G) \rtimes \langle \sigma \rangle$. In particular Proposition 2.2.2 (a) implies that $\tilde{K}$ is normalized by G. As we have just seen that $a_j \in \tilde{K}$ for all $1 \leqslant j \leqslant r$ with $j \neq i$, from the definition of $H^{(i)}$ we deduce that $H^{(i)} \subset \tilde{K}$. Since $a_1 \notin W \times W$, but $a_1^2 \in K$, we can conclude that $H^{(i)} \cap (W \times W) \subset \tilde{K} \cap (W \times W) = K$, as desired. $\qquad\square$

Lemma 2.2.5 *For any $n \geqslant 0$ and $1 \leqslant i \leqslant r$ let $H_n^{(i)}$ denote the image of $H^{(i)}$ in W_n.*

(a) The element $a_i|_{T_n}$ of G_n has order $2^{\lfloor \frac{n+r-i}{r} \rfloor}$.

(b) We have a semidirect product $G_n = H_n^{(i)} \rtimes \langle a_i|_{T_n} \rangle$.

Proof. The assertions are trivially true for $n = 0$, so assume that $n > 0$ and that they hold for $n - 1$ and all i.

Since a_1 acts non-trivially on level 1, its restriction $a_1|_{T_n}$ has order > 1. From the induction hypothesis we can deduce that $(a_1|_{T_n})^2 = (a_r|_{T_{n-1}}, a_r|_{T_{n-1}})$ has order $2^{\lfloor \frac{(n-1)+r-r}{r} \rfloor} = 2^{\lfloor \frac{n-1}{r} \rfloor}$. Together this implies that $a_1|_{T_n}$ has order $2 \cdot 2^{\lfloor \frac{n-1}{r} \rfloor} = 2^{\lfloor \frac{n+r-1}{r} \rfloor}$, proving (a) for $i = 1$. Also, Lemma 2.2.4 (a) implies that $H_n^{(1)} = H_{n-1}^{(r)} \times H_{n-1}^{(r)}$, which in particular shows that $a_1|_{T_n} \notin H_n^{(1)}$. Since we have $H_{n-1}^{(r)} \cap \langle a_r|_{T_{n-1}} \rangle = 1$ by the induction hypothesis, we can deduce that

$$H_n^{(1)} \cap \langle a_1|_{T_n} \rangle \;=\; H_n^{(1)} \cap \langle (a_1|_{T_n})^2 \rangle \;=\; \big(H_{n-1}^{(r)} \times H_{n-1}^{(r)}\big) \cap \langle (a_r|_{T_{n-1}}, a_r|_{T_{n-1}}) \rangle \;=\; 1.$$

Thus the product $G_n = H_n^{(1)} \cdot \langle a_1|_{T_n} \rangle$ is semidirect, proving (b) for $i = 1$.

Now consider $i > 1$. Then the induction hypothesis shows that $a_i|_{T_n} = (a_{i-1}|_{T_{n-1}}, 1)$ has order $2^{\lfloor \frac{(n-1)+r-(i-1)}{r} \rfloor} = 2^{\lfloor \frac{n+r-i}{r} \rfloor}$, as desired in (a). Moreover, Lemma 2.2.4 (b) implies that $H_n^{(i)} \cap (W_{n-1} \times 1) \subset H_{n-1}^{(i-1)} \times 1$, and since $H_{n-1}^{(i-1)} \cap \langle a_{i-1}|_{T_{n-1}} \rangle = 1$ by the induction hypothesis, it follows that $H_n^{(i)} \cap \langle a_i|_{T_n} \rangle = 1$. Thus the product $G_n = H_n^{(i)} \cdot \langle a_i|_{T_n} \rangle$ is semidirect, as desired in (b).

This proves the assertions for the given n and all i, and so they follow in general by induction. $\qquad \square$

Proposition 2.2.6 *For any $1 \leqslant i \leqslant r$ we have a semidirect product $G = H^{(i)} \rtimes \langle\!\langle a_i \rangle\!\rangle$, where $\langle\!\langle a_i \rangle\!\rangle \cong \mathbb{Z}_2$.*

Proof. Take the limit over n in Lemma 2.2.5. $\qquad \square$

Theorem 2.2.7 *The closure of the commutator subgroup of G is $H^{(1)} \cap \ldots \cap H^{(r)}$, and the maximal profinite abelian factor group of G is*

$$ G_{\mathrm{ab}} \;=\; G/(H^{(1)} \cap \ldots \cap H^{(r)}) \; \overset{\sim}{\longrightarrow} \; G/H^{(1)} \times \ldots \times G/H^{(r)} \;\cong\; \mathbb{Z}_2^r. $$

Proof. The isomorphisms in the middle and on the right hand side are direct consequences of Proposition 2.2.6 and the fact that $a_j \in H^{(i)}$ whenever $j \neq i$. On the other hand, since G is topologically generated by $a_1, \ldots, a_r$, its maximal abelian factor group is topologically generated by the images of $a_1, \ldots, a_r$. As their images form a basis of $\mathbb{Z}_2^r$, this is already the maximal profinite abelian factor group of G, as desired. $\qquad \square$

In the following we abbreviate

$$ (2.2.8) \qquad\qquad\qquad\qquad H := H^{(r)} $$

which by definition is the closure of the subgroup generated by all G-conjugates of a_j for all $1 \leqslant j < r$. We let H_n denote its image in W_n, and G_n^1 the image of G^1 in W_n.

Lemma 2.2.9 *We have the semidirect product decompositions:*

(a) *$G_n = H_n \rtimes \langle a_r|_{T_n} \rangle$ where $a_r|_{T_n}$ has order $2^{\lfloor \frac{n}{r} \rfloor}$.*

(b) *$G_n = (H_{n-1} \times H_{n-1}) \rtimes \langle a_1|_{T_n} \rangle$ where $a_1|_{T_n}$ has order $2^{\lfloor \frac{n+r-1}{r} \rfloor}$.*

(c) *$G_n^1 = (H_{n-1} \times H_{n-1}) \rtimes \langle (a_r|_{T_{n-1}}, a_r|_{T_{n-1}}) \rangle$ where $a_r|_{T_{n-1}}$ has order $2^{\lfloor \frac{n-1}{r} \rfloor}$.*

Proof. Part (a) is the special case $i = r$ of Lemma 2.2.5, and (b) is the special case $i = 1$ of Lemma 2.2.5 combined with Lemma 2.2.4 (a). Part (c) follows from (b) and the fact that $a_1|_{T_n} \notin G_n^1$ and has square $(a_r|_{T_{n-1}}, a_r|_{T_{n-1}}) \in G_n^1$. $\qquad \square$

In the limit over n this implies the following more specific self-similarity properties of G:

Proposition 2.2.10 *We have the semidirect product decompositions:*

(a) *$G = H \rtimes \langle\!\langle a_r \rangle\!\rangle$.*

(b) *$G = (H \times H) \rtimes \langle\!\langle a_1 \rangle\!\rangle$.*

(c) *$G^1 = (H \times H) \rtimes \langle\!\langle (a_r, a_r) \rangle\!\rangle$.*

24

2.3 Size

Proposition 2.3.1 *For all $n \geqslant 0$ we have*

$$\log_2 |G_n| \;=\; 2^n - 1 - \sum_{m=0}^{n-1} 2^{n-1-m} \cdot \left\lfloor \frac{m}{r} \right\rfloor.$$

Proof. For $n > 0$ Lemma 2.2.9 (a) and (b) imply that

$$\log_2 |G_{n-1}| \;=\; \log_2 |H_{n-1}| + \left\lfloor \frac{n-1}{r} \right\rfloor \quad \text{and}$$
$$\log_2 |G_n| \;=\; 2 \cdot \log_2 |H_{n-1}| + \left\lfloor \frac{n+r-1}{r} \right\rfloor.$$

Together this yields the recursion formula

$$\log_2 |G_n| \;=\; 2 \cdot \left(\log_2 |G_{n-1}| - \left\lfloor \frac{n-1}{r} \right\rfloor \right) + \left\lfloor \frac{n+r-1}{r} \right\rfloor \;=\; 2 \cdot \log_2 |G_{n-1}| + 1 - \left\lfloor \frac{n-1}{r} \right\rfloor.$$

Since $\log_2 |G_0| = 1$, a direct induction on n yields the desired formula. $\qquad\square$

Theorem 2.3.2 *The Hausdorff dimension of G exists and is $1 - \frac{1}{2^r - 1}$.*

Proof. Proposition 2.3.1 implies that

$$\frac{\log_2 |G_n|}{2^n - 1} \;=\; 1 - \frac{2^n}{2^n - 1} \cdot \sum_{m=0}^{n-1} 2^{-1-m} \cdot \left\lfloor \frac{m}{r} \right\rfloor.$$

By (1.2.2) the Hausdorff dimension is its limit for $n \to \infty$, which comes out as

$$
\begin{aligned}
1 - \sum_{m=0}^{\infty} 2^{-1-m} \cdot \left\lfloor \frac{m}{r} \right\rfloor \;&=\; 1 - \sum_{i=0}^{r-1} \sum_{j=0}^{\infty} 2^{-1-(i+rj)} \cdot \left\lfloor \frac{i+rj}{r} \right\rfloor \\
&=\; 1 - \sum_{i=0}^{r-1} 2^{-1-i} \cdot \sum_{j=0}^{\infty} j \cdot 2^{-rj} \\
&=\; 1 - \left(1 - 2^{-r}\right) \cdot \frac{2^{-r}}{(1 - 2^{-r})^2} \;=\; 1 - \frac{1}{2^r - 1},
\end{aligned}
$$

as desired. $\qquad\square$

2.4 Conjugacy of generators

The recursion relations (2.0.1) are only one choice among many describing the same qualitative recursive behavior of the generators, and besides their simplicity there is nothing inherently better in them to set them apart from similar choices (for instance, compare [2, §3]). In this subsection we show in a precise sense that up to conjugacy in W the group G

25

is actually the same for all recursion relations that are conjugate to the given ones. We can thus say that G really depends only on the combinatorics of the diagram (2.0.2), perhaps in the same way as a symplectic group of matrices of a given size n depends up to conjugacy only on n but not on the alternating form, even though the choice of an alternating form cannot be avoided.

Proposition 2.4.1 *For any elements $b_1, \ldots, b_r \in W$ the following are equivalent:*

(a) b_i is conjugate to a_i under W for each i.

(b) $\left\{ \begin{array}{l} b_1 \text{ is conjugate to } (b_r, 1)\,\sigma \text{ under } W, \text{ and} \\ b_i \text{ is conjugate to } (b_{i-1}, 1) \text{ under } W \text{ for all } 2 \leqslant i \leqslant r. \end{array} \right\}$

Proof. Assume (a) and choose $x_i \in W$ such that $b_i = x_i a_i x_i^{-1}$ for all $1 \leqslant i \leqslant r$. Then

$$b_1 = x_1 a_1 x_1^{-1} = x_1 (a_r, 1)\,\sigma\, x_1^{-1} = x_1 (x_r^{-1} b_r x_r, 1)\,\sigma\, x_1^{-1} = x_1 (x_r, x_r)^{-1} (b_r, 1)\,\sigma\, (x_r, x_r)\, x_1^{-1},$$

hence b_1 is conjugate to $(b_r, 1)\,\sigma$. Likewise, for all $2 \leqslant i \leqslant r$ we have

$$b_i = x_i a_i x_i^{-1} = x_i (a_{i-1}, 1)\, x_i^{-1} = x_i (x_{i-1}^{-1} b_{i-1} x_{i-1}, 1)\, x_i^{-1} = x_i (x_{i-1}, 1)^{-1} (b_{i-1}, 1)\, (x_{i-1}, 1)\, x_i^{-1},$$

hence b_i is conjugate to $(b_{i-1}, 1)\,\sigma$. This proves the implication (a)$\Rightarrow$(b).

Conversely assume (b). To deduce (a), by Lemma 1.3.1 it suffices to show that $b_i|_{T_n}$ is conjugate to $a_i|_{T_n}$ in W_n for all i and n. This is trivial for $n = 0$, so assume that $n > 0$ and that it holds for $n - 1$ and all i. Choose $x_i \in W$ with $b_i|_{T_{n-1}} = x_i a_i x_i^{-1}|_{T_{n-1}}$ for all i. Then by assumption $b_1|_{T_n}$ is conjugate to

$$\begin{aligned} \left((b_r, 1)\,\sigma\right)\big|_{T_n} &= (b_r|_{T_{n-1}}, 1)\,\sigma = (x_r a_r x_r^{-1}|_{T_{n-1}}, 1)\,\sigma = \left((x_r a_r x_r^{-1}, 1)\,\sigma\right)\big|_{T_n} \\ &= \left((x_r, x_r)\,(a_r, 1)\,\sigma\,(x_r, x_r)^{-1}\right)\big|_{T_n} = \left((x_r, x_r)\, a_1\,(x_r, x_r)^{-1}\right)\big|_{T_n} \end{aligned}$$

and hence to $a_1|_{T_n}$. Similarly, for all $2 \leqslant i \leqslant r$ by assumption $b_i|_{T_n}$ is conjugate to

$$\begin{aligned} (b_{i-1}, 1)|_{T_n} &= (b_{i-1}|_{T_{n-1}}, 1) = (x_{i-1} a_{i-1} x_{i-1}^{-1}|_{T_{n-1}}, 1) = (x_{i-1} a_{i-1} x_{i-1}^{-1}, 1)|_{T_n} \\ &= \left((x_{i-1}, 1)\,(a_{i-1}, 1)\,(x_{i-1}, 1)^{-1}\right)\big|_{T_n} = \left((x_{i-1}, 1)\, a_i\,(x_{i-1}, 1)^{-1}\right)\big|_{T_n} \end{aligned}$$

and hence to $a_i|_{T_n}$. Thus the desired assertion holds for n and all i; and so it follows for all $n \geqslant 0$ by induction. This proves the implication (b)$\Rightarrow$(a). $\qquad \square$

Proposition 2.4.2 *Consider any elements $b_1, \ldots, b_r \in G$ such that b_i is conjugate to a_i under W for every i. Then $G = \langle\!\langle b_1, \ldots, b_r \rangle\!\rangle$.*

Proof. Let $\Phi(G)$ denote the Frattini subgroup of G, that is, the intersection of all maximal proper closed subgroups of G. Since G is a pro-2 group, the quotient $G/\Phi(G)$ is abelian of exponent 2. The description of the maximal abelian quotient of G from Theorem 2.2.7 therefore implies that $G/\Phi(G)$ is an elementary abelian 2-group for which the images of $a_1, \ldots, a_r$ form a basis. Moreover, since $\mathrm{sgn}_i(a_j) = (-1)^{\delta_{i,j}}$ (Kronecker delta) for all $1 \leqslant i, j \leqslant r$, we find that $(\mathrm{sgn}_i)_{i=1}^r$ induces an isomorphism $G/\Phi(G) \xrightarrow{\sim} \{\pm1\}^r$.

Since each b_j is conjugate to a_j under W, we have $\mathrm{sgn}_i(b_j) = \mathrm{sgn}_i(a_j) = (-1)^{\delta_{i,j}}$ for all $1 \leqslant i, j \leqslant r$. Thus the images of $b_1, \ldots, b_r$ generate $\{\pm1\}^r$ and hence $G/\Phi(G)$. By the fundamental property of the Frattini subgroup this implies that $\langle\!\langle b_1, \ldots, b_r \rangle\!\rangle = G$, as desired. $\qquad\square$

Theorem 2.4.3 *Consider any elements $b_1, \ldots, b_r \in W$ such that b_i is conjugate to a_i under W for each i. Then there exist $w \in W$ and $x_1, \ldots, x_r \in G$ such that $b_i = (wx_i)a_i(wx_i)^{-1}$ for each i, and we then have $\langle\!\langle b_1, \ldots, b_r \rangle\!\rangle = wGw^{-1}$.*

Proof. The second assertion is a direct consequence of the first and Proposition 2.4.2. The first follows by taking the limit over n from the following assertion for all $n \geqslant 0$: For any elements $b_1, \ldots, b_r \in W_n$ such that b_i is conjugate to $a_i|_{T_n}$ under W_n for each i, there exist $w \in W_n$ and $x_1, \ldots, x_r \in G_n$ such that $b_i = (wx_i)(a_i|_{T_n})(wx_i)^{-1}$ for each i. This assertion is trivial for $n = 0$, so assume that $n > 0$ and that the assertion is universally true for $n - 1$. Take elements $b_1, \ldots, b_r \in W_n$ such that b_i is conjugate to $a_i|_{T_n}$ under W_n for each i.

Since $a_1 = (a_r, 1)\,\sigma$ and $a_i = (a_{i-1}, 1)$ for all $i > 1$, the b_i have the form $b_1 = (*, *)\,\sigma$ and $b_i = (*, 1)$ or $(1, *)$ for $i > 1$, where $*$ stands for some elements of W_{n-1}. Set

$$b_i' := \begin{cases} b_i & \text{if } i = 1 \text{ or } b_i = (*, 1), \\ b_1^{-1} b_i b_1 & \text{if } i > 1 \text{ and } b_i = (1, *), \end{cases}$$

which in either case is conjugate to $a_i|_{T_n}$ under W_n. Suppose that the desired assertion is true for $b_1', \ldots, b_r'$, so that there exist $w \in W_n$ and $x_1', \ldots, x_r' \in G_n$ such that $b_i' = (wx_i')(a_i|_{T_n})(wx_i')^{-1}$ for each i. Set

$$x_i := \begin{cases} x_i' & \text{if } i = 1 \text{ or } b_i = (*, 1), \\ x_1'(a_1|_{T_n})\, x_1'^{-1} x_i' & \text{if } i > 1 \text{ and } b_i = (1, *), \end{cases}$$

which always lies in G_n. Then if $i = 1$ or $b_i = (*, 1)$, we have $b_i = b_i' = (wx_i)(a_i|_{T_n})(wx_i)^{-1}$; otherwise we have

$$
\begin{aligned}
b_i &= b_1 b_i' b_1^{-1} \\
&= (wx_1')(a_1|_{T_n})(wx_1')^{-1} \cdot (wx_i')(a_i|_{T_n})(wx_i')^{-1} \cdot (wx_1')(a_1|_{T_n})(wx_1')^{-1} \\
&= wx_1'(a_1|_{T_n})\, x_1'^{-1} x_i' \cdot (a_i|_{T_n}) \cdot x_i'^{-1} x_1'(a_1|_{T_n})\, x_1'^{-1} w^{-1} \\
&= (wx_i)(a_i|_{T_n})(wx_i)^{-1}.
\end{aligned}
$$

27

Thus the desired assertion holds for $b_1, \ldots, b_r$ with $x_1, \ldots, x_r$ in place of $x'_1, \ldots, x'_r$. On replacing $b_1, \ldots, b_r$ by $b'_1, \ldots, b'_r$ we have thus reduced ourselves to the case that $b_i = (*, 1)$ for all $i > 1$.

For each $i > 0$ write $b_i = (c_{i-1}, 1)$ with $c_{i-1} \in W_{n-1}$. The fact that b_i is conjugate to $a_i|_{T_n} = (a_{i-1}|_{T_{n-1}}, 1)$ under W_n implies that c_{i-1} is conjugate to $a_{i-1}|_{T_{n-1}}$ under W_{n-1}. Also, choose an element $f \in W_n$ such that $b_1 = f(a_1|_{T_n})f^{-1}$. If f acts non-trivially on level 1, we can replace it by $f(a_1|_{T_n})$ without changing the conjugate $b_1 = f(a_1|_{T_n})f^{-1}$. Afterwards f has the form $f = (d, e)$ for some elements $d, e \in W_{n-1}$. We then have

$$b_1 \;=\; f(a_1|_{T_n})f^{-1} \;=\; (d, e)\,(a_r|_{T_{n-1}}, 1)\,\sigma\,(d, e)^{-1} \;=\; \left(d(a_r|_{T_{n-1}})e^{-1}, ed^{-1}\right)\sigma.$$

Set $c_r := d(a_r|_{T_{n-1}})d^{-1} \in W_{n-1}$. Then for every $1 \leqslant i \leqslant r$ the element c_i is conjugate to $a_i|_{T_{n-1}}$ under W_{n-1}. By the induction hypothesis there therefore exist $u \in W_{n-1}$ and $x_i \in G_{n-1}$ such that $c_i = (ux_i)(a_i|_{T_{n-1}})(ux_i)^{-1}$ for each i. Put $w := (ux_r, ed^{-1}ux_r) \in W_n$. Then

$$\begin{aligned}
w^{-1}b_1 w &= \left(x_r^{-1}u^{-1}, x_r^{-1}u^{-1}de^{-1}\right)\left(d(a_r|_{T_{n-1}})e^{-1}, ed^{-1}\right)\sigma\left(ux_r, ed^{-1}ux_r\right)\\
&= \left(x_r^{-1}u^{-1}d(a_r|_{T_{n-1}})e^{-1}ed^{-1}ux_r, x_r^{-1}u^{-1}de^{-1}ed^{-1}ux_r\right)\sigma\\
&= \left(x_r^{-1}u^{-1}d(a_r|_{T_{n-1}})d^{-1}ux_r, 1\right)\sigma\\
&= \left(x_r^{-1}u^{-1}c_r ux_r, 1\right)\sigma\\
&= \left(x_r^{-1}u^{-1}(ux_r)(a_r|_{T_{n-1}})(ux_r)^{-1}ux_r, 1\right)\sigma\\
&= (a_r|_{T_{n-1}}, 1)\,\sigma\\
&= a_1|_{T_n}.
\end{aligned}$$

Also, for each $i > 1$ we have

$$\begin{aligned}
w^{-1}b_i w &= \left(x_r^{-1}u^{-1}, x_r^{-1}u^{-1}de^{-1}\right)\left(c_{i-1}, 1\right)\left(ux_r, ed^{-1}ux_r\right)\\
&= \left(x_r^{-1}u^{-1}c_{i-1}ux_r, 1\right)\\
&= \left(x_r^{-1}u^{-1}(ux_{i-1})(a_{i-1}|_{T_{n-1}})(ux_{i-1})^{-1}ux_r, 1\right)\\
&= \left((x_r^{-1}x_{i-1})(a_{i-1}|_{T_{n-1}})(x_r^{-1}x_{i-1})^{-1}, 1\right).
\end{aligned}$$

Since $x_r^{-1}x_{i-1} \in G_{n-1}$, by Proposition 2.2.2 (c) we can find $y_{i-1} \in W_{n-1}$ such that $z_i := (x_r^{-1}x_{i-1}, y_{i-1})$ lies in G_n. Then

$$\begin{aligned}
w^{-1}b_i w &= (x_r^{-1}x_{i-1}, y_{i-1})\,(a_{i-1}|_{T_{n-1}}, 1)\,(x_r^{-1}x_{i-1}, y_{i-1})^{-1}\\
&= z_i(a_i|_{T_n})z_i^{-1}.
\end{aligned}$$

With $z_1 := 1$ we have thus shown that $w^{-1}b_i w = z_i(a_i|_{T_n})z_i^{-1}$ or equivalently that $b_i = (wz_i)(a_i|_{T_n})(wz_i)^{-1}$ for all $1 \leqslant i \leqslant r$, where $w \in W_n$ and $z_i \in G_n$. This proves the desired assertion for n, and so we are done by induction. $\qquad\square$

Proposition 2.4.4 *For any single $1 \leqslant i \leqslant r$ and any $b_i \in G$ that is conjugate to a_i under W, there exists $k \in \mathbb{Z}_2^\times$ such that b_i is conjugate to a_i^k under G.*

Proof. By Lemma 1.3.1 it suffices to show that for any $n \geqslant 0$, any $1 \leqslant i \leqslant r$, and any $b_i \in G_n$ that is conjugate to $a_i|_{T_n}$ under W_n, there exists $k \in \mathbb{Z}_2^\times$ such that b_i is conjugate to $a_i^k|_{T_n}$ under G_n. This is trivial for $n = 0$, so assume that $n > 0$ and that the statement is universally true for $n - 1$ in place of n. Consider an element $b_i \in G_n$ that is conjugate to $a_i|_{T_n}$ under W_n, and choose an element $w \in W_n$ such that $b_i = w\,(a_i|_{T_n})\,w^{-1}$.

Suppose first that $i \geqslant 2$. If w acts non-trivially on level 1, we replace b_i by its G_n-conjugate $(a_1|_{T_n})\,b_i\,(a_1|_{T_n})^{-1}$ and w by $(a_1|_{T_n})\,w$, which does not change the desired assertion. Afterwards w has the form $w = (u, v)$ for some elements $u, v \in W_{n-1}$. Then the recursion relation yields

$$b_i = w\,(a_i|_{T_n})\,w^{-1} = (u, v)\,(a_{i-1}|_{T_{n-1}}, 1)\,(u, v)^{-1} = \big(u(a_{i-1}|_{T_{n-1}})u^{-1}, 1\big).$$

By assumption b_i lies in G_n, so Proposition 2.2.2 shows that $b_{i-1} := u(a_{i-1}|_{T_{n-1}})u^{-1}$ lies in G_{n-1}. Thus b_{i-1} is an element of G_{n-1} that is conjugate to $a_{i-1}|_{T_{n-1}}$ under W_{n-1}; hence by the induction hypothesis there exist $k \in \mathbb{Z}_2^\times$ and $x \in G_{n-1}$ such that $b_{i-1} = x(a_{i-1}^k|_{T_{n-1}})x^{-1}$. By Proposition 2.2.2 (c) we can choose an element $y \in G_{n-1}$ for which $z := (x, y)$ lies in G_n. Then

$$b_i = (b_{i-1}, 1) = \big(x(a_{i-1}^k|_{T_{n-1}})x^{-1}, 1\big) = (x, y)\,(a_{i-1}^k|_{T_{n-1}}, 1)\,(x, y)^{-1} = z\,(a_i^k|_{T_n})\,z^{-1},$$

which proves that b_i is conjugate to $a_i^k|_{T_n}$ under G_n, as desired.

Now suppose that $i = 1$. If w acts non-trivially on level 1, we can replace it by $w\,(a_1|_{T_n})$ without changing the conjugate $b_1 = w\,(a_1|_{T_n})\,w^{-1}$. Afterwards w has the form $w = (u, v)$ for some elements $u, v \in W_{n-1}$. Then the recursion relation yields

$$b_1^2 = w\,(a_1^2|_{T_n})\,w^{-1} = (u, v)\,(a_r|_{T_{n-1}}, a_r|_{T_{n-1}})\,(u, v)^{-1} = \big(u(a_r|_{T_{n-1}})u^{-1}, v(a_r|_{T_{n-1}})v^{-1}\big).$$

By assumption b_1 and hence b_1^2 lie in G_n, so Proposition 2.2.2 shows that $b_r := u(a_r|_{T_{n-1}})u^{-1}$ lies in G_{n-1}. Thus b_r is an element of G_{n-1} that is conjugate to $a_r|_{T_{n-1}}$ under W_{n-1}; hence by the induction hypothesis there exist $k \in \mathbb{Z}_2^\times$ and $x \in G_{n-1}$ such that $b_r = x(a_r^k|_{T_{n-1}})x^{-1}$. By Proposition 2.2.2 (c) we can choose an element $y \in G_{n-1}$ for which $z := (x, y)$ lies in G_n. Then $b_1^2 = z\,(a_r|_{T_{n-1}}, *)^k\,z^{-1}$, where $*$ represents an element of W_{n-1} that we do not care about for the moment. Set $c_1 := z^{-1}\,b_1^{k^{-1}}z$, so that $c_1^2 = (a_r|_{T_{n-1}}, *)$. Since b_1 and z lie in G_n, so does c_1. Moreover, Proposition 1.3.2 implies that b_1 is conjugate to $b_1^{k^{-1}}$ and hence to c_1 under W_n. Thus c_1 is again conjugate to $a_1|_{T_n}$ under W_n. Since $b_1 = zc_1^kz^{-1}$ with $z \in G_n$, the desired assertion for b_1 now reduces to that for c_1. We can therefore replace b_1 by c_1, after which we are reduced to the special case that $b_1^2 = (a_r|_{T_{n-1}}, *)$.

Now we begin again by choosing a (new) element $w \in W_n$ such that $b_1 = w\,(a_1|_{T_n})\,w^{-1}$. If w acts non-trivially on level 1, we replace it by $w\,(a_1|_{T_n})$ without changing the conjugate $b_1 = w\,(a_1|_{T_n})\,w^{-1}$. Afterwards w has the form $w = (u, v)$ for some elements $u, v \in W_{n-1}$. Then the same calculation as before shows that $(a_r|_{T_{n-1}}, *) = b_1^2 = (u(a_r|_{T_{n-1}})u^{-1}, *)$; hence

u commutes with $a_r|_{T_{n-1}}$. Therefore

$$\begin{aligned}
b_1 &= w\left(a_1|_{T_n}\right)w^{-1} = (u,v)\left(a_r|_{T_{n-1}},1\right)\sigma\,(u,v)^{-1} \\
&= \left(u(a_r|_{T_{n-1}})v^{-1}, vu^{-1}\right)\sigma \\
&= \left((a_r|_{T_{n-1}})uv^{-1}, vu^{-1}\right)\sigma \\
&= \left(a_r|_{T_{n-1}},1\right)\sigma\left(vu^{-1},uv^{-1}\right) = \left(a_1|_{T_n}\right)\left(vu^{-1},uv^{-1}\right).
\end{aligned}$$

Since b_1 lies in G_n by assumption, this shows that $\left(vu^{-1}, uv^{-1}\right)$ lies in G_n^1. By Lemma 2.2.9 (c) this means that $vu^{-1} = h\left(a_r|_{T_{n-1}}\right)^m$ for some $h \in H_{n-1}$ and $m \in \mathbb{Z}$ such that $\left(a_r|_{T_{n-1}}\right)^{-m} = \left(a_r|_{T_{n-1}}\right)^m$. Therefore

$$\begin{aligned}
b_1 &= \left(a_1|_{T_n}\right)\left(vu^{-1}, uv^{-1}\right) \\
&= \left(a_1|_{T_n}\right)\left(h\left(a_r|_{T_{n-1}}\right)^m, \left(a_r|_{T_{n-1}}\right)^{-m}h^{-1}\right) \\
&= \left(a_r|_{T_{n-1}},1\right)\sigma\,(h,1)\left(\left(a_r|_{T_{n-1}}\right)^m, \left(a_r|_{T_{n-1}}\right)^m\right)\left(1,h^{-1}\right) \\
&= \left(a_r|_{T_{n-1}},1\right)(1,h)\,\sigma\left(a_r|_{T_{n-1}}, a_r|_{T_{n-1}}\right)^m\left(1,h\right)^{-1} \\
&= (1,h)\left(a_r|_{T_{n-1}},1\right)\sigma\left(a_1|_{T_n}\right)^{2m}\left(1,h\right)^{-1} \\
&= (1,h)\left(a_1|_{T_n}\right)^{1+2m}\left(1,h\right)^{-1}.
\end{aligned}$$

Since $(1,h) \in G_n$ by Lemma 2.2.9 (b), this shows that b_1 is conjugate to $a_1^{1+2m}|_{T_n}$ under G_n, thereby finishing the proof. $\square$

2.5 Small cases

In the case $r = 1$ the element a_1 is the odometer from Subsection 1.6, and $G = \langle\!\langle a_1 \rangle\!\rangle \cong \mathbb{Z}_2$. In all other cases the group G has positive Hausdorff dimension and is very non-abelian. The next smallest case $r = 2$ is the closure of the so-called 'Basilica group'; see Grigorchuk-Żuk [9]. For the case $r = 3$ corresponding to the 'Douady rabbit' some of the results of the preceding subsection were obtained by Nekrashevych [17, §8].

The case $r = 2$ stands out among the others by the following rigidity property, which is stronger than the semirigidity from Theorem 2.4.3. The analogous statement does not hold for any $r > 2$.

Theorem 2.5.1 *Assume that $r = 2$. Consider any element $b_1 \in W$ which is conjugate to a_1 under W, and any element $b_2 \in W$ which is conjugate to a_2 under W. Then there exists an element $w \in W$ such that $b_1 = wa_1w^{-1}$ and $b_2 = wa_2w^{-1}$.*

Proof. We will prove a similar statement in W_n by induction on n. Let $\mathrm{Conj}_{W_n}(a_i|_{T_n})$ denote the conjugacy class of $a_i|_{T_n}$ in W_n.

Lemma 2.5.2 *For every $n \geqslant 1$ we have*

$$\left|\mathrm{Conj}_{W_n}(a_1|_{T_n}) \times \mathrm{Conj}_{W_n}(a_2|_{T_n})\right| = 2^{2^n-2}.$$

Proof. Abbreviate $\gamma_{i,n} := \log_2\left|\mathrm{Conj}_{W_n}(a_i|_{T_n})\right|$. Since $\log_2|W_n| = 2^n - 1$ by (1.2.1), we have $\log_2\left|\mathrm{Cent}_{W_n}(a_i|_{T_n})\right| = 2^n - 1 - \gamma_{i,n}$. For $n = 1$ observe that W_1 is abelian; hence $\gamma_{i,1} = 0$ for both $i = 1, 2$. For $n > 1$ note first that $a_2|_{T_n} = (a_1|_{T_{n-1}}, 1)$ with $a_1|_{T_{n-1}}$ non-trivial; hence

$$(2.5.3) \qquad \mathrm{Cent}_{W_n}(a_2|_{T_n}) = \mathrm{Cent}_{W_{n-1}}(a_1|_{T_{n-1}}) \times W_{n-1}.$$

Therefore

$$
\begin{aligned}
2^n - 1 - \gamma_{2,n} &= \log_2\left|\mathrm{Cent}_{W_n}(a_2|_{T_n})\right| \\
&= \log_2\left|\mathrm{Cent}_{W_{n-1}}(a_1|_{T_{n-1}})\right| + 2^{n-1} - 1 \\
&= 2^{n-1} - 1 - \gamma_{1,n-1} + 2^{n-1} - 1,
\end{aligned}
$$

and so $\gamma_{2,n} = \gamma_{1,n-1} + 1$.

Next the element $a_1|_{T_n}$ is contained in its own centralizer and acts non-trivially on level 1; hence

$$\left|\mathrm{Cent}_{W_n}(a_1|_{T_n})\right| = 2 \cdot \left|\mathrm{Cent}_{W_{n-1} \times W_{n-1}}(a_1|_{T_n})\right|.$$

Also, an element $w = (u, v) \in W_{n-1} \times W_{n-1}$ commutes with $a_1|_{T_n}$ if and only if

$$
\begin{aligned}
(a_1|_{T_n})\, w &= (a_2|_{T_{n-1}}, 1)\, \sigma\, (u, v) = ((a_2|_{T_{n-1}})v, u)\, \sigma \\
&\quad\| \\
w\, (a_1|_{T_n}) &= (u, v)\, (a_2|_{T_{n-1}}, 1)\, \sigma = (u(a_2|_{T_{n-1}}), v)\, \sigma,
\end{aligned}
$$

that is, if and only if $u = v$ and u commutes with $a_2|_{T_{n-1}}$. Thus

$$(2.5.4) \qquad \mathrm{Cent}_{W_{n-1} \times W_{n-1}}(a_1|_{T_n}) = \mathrm{diag}\left(\mathrm{Cent}_{W_{n-1}}(a_2|_{T_{n-1}})\right).$$

Therefore

$$
\begin{aligned}
2^n - 1 - \gamma_{1,n} &= \log_2\left|\mathrm{Cent}_{W_n}(a_1|_{T_n})\right| \\
&= 1 + \log_2\left|\mathrm{Cent}_{W_{n-1}}(a_2|_{T_{n-1}})\right| \\
&= 1 + 2^{n-1} - 1 - \gamma_{2,n-1},
\end{aligned}
$$

and so $\gamma_{1,n} = \gamma_{2,n-1} + 2^{n-1} - 1$.

Finally, set $\gamma_n := \gamma_{1,n} + \gamma_{2,n}$. Then $\gamma_1 = 0$, and the above formulas imply that $\gamma_n = \gamma_{n-1} + 2^{n-1}$ for all $n > 1$. By induction on n it follows that $\gamma_n = 2^n - 2$ for all $n \geqslant 1$, as desired. $\qquad \square$

Lemma 2.5.5 *For every $n \geqslant 1$ the centralizer of G_n in W_n has order 2.*

Proof. Since W_1 is abelian of order 2, the assertion holds for $n = 1$. For $n > 1$ observe that since $a_1|_{T_n}$ and $a_2|_{T_n}$ generate G_n, the equations (2.5.3) and (2.5.4) from the preceding

proof imply that

$$
\begin{aligned}
\mathrm{Cent}_{W_n}(G) &= \mathrm{Cent}_{W_n}(a_1|_{T_n}) \cap \mathrm{Cent}_{W_n}(a_2|_{T_n}) \\
&= \big(\mathrm{Cent}_{W_{n-1}}(a_1|_{T_{n-1}}) \times W_{n-1}\big) \cap \mathrm{diag}\big(\mathrm{Cent}_{W_{n-1}}(a_2|_{T_{n-1}})\big) \\
&= \mathrm{diag}\big(\mathrm{Cent}_{W_{n-1}}(a_1|_{T_{n-1}}) \cap \mathrm{Cent}_{W_{n-1}}(a_2|_{T_{n-1}})\big) \\
&= \mathrm{diag}\big(\mathrm{Cent}_{W_{n-1}}(G_{n-1})\big).
\end{aligned}
$$

Thus the order of the centralizer is independent of n and hence is always equal to 2. $\quad\square$

Now we let W_n act on $\mathrm{Conj}_{W_n}(a_1|_{T_n}) \times \mathrm{Conj}_{W_n}(a_2|_{T_n})$ by joint conjugation. Lemma 2.5.5 means that the stabilizer of the pair $(a_1|_{T_n}, a_2|_{T_n})$ has order 2; hence its orbit has length $|W_n|/2 = 2^{2^n-2}$. From Lemma 2.5.2 it thus follows that this orbit fills out all of $\mathrm{Conj}_{W_n}(a_1|_{T_n}) \times \mathrm{Conj}_{W_n}(a_2|_{T_n})$; in other words the action of W_n is transitive.

Finally, taking the inverse limit over n implies that the action of W on $\mathrm{Conj}_W(a_1) \times \mathrm{Conj}_W(a_2)$ is transitive, which is precisely Theorem 2.5.1, and we are done. $\quad\square$

2.6 Normalizer

In this subsection we determine the normalizer

$$
(2.6.1) \qquad\qquad\qquad N := \mathrm{Norm}_W(G).
$$

Recall from Theorem 2.2.7 that $K := H^{(1)} \cap \ldots \cap H^{(r)}$ is the closure of the commutator subgroup of G and that we have a natural isomorphism $G_{\mathrm{ab}} = G/K \cong \mathbb{Z}_2^r$. Let $\pi\colon G \twoheadrightarrow G_{\mathrm{ab}}$ denote the natural projection, so that the elements $\pi(a_i)$ for $1 \leqslant i \leqslant r$ form a basis of G_{ab} as a module over $\mathbb{Z}_2$.

Lemma 2.6.2 *For any $w \in N$ and any $1 \leqslant i \leqslant r$ there exists $k_i \in \mathbb{Z}_2^\times$ such that $\pi(wa_iw^{-1}) = \pi(a_i^{k_i})$.*

Proof. Since wa_iw^{-1} lies in G, by Proposition 2.4.4 there exists $k_i \in \mathbb{Z}_2^\times$ such that wa_iw^{-1} is conjugate to $a_i^{k_i}$ under G. Thus $\pi(wa_iw^{-1}) = \pi(a_i^{k_i})$, as desired. $\quad\square$

Lemma 2.6.3 *For any tuple $(k_i) \in (\mathbb{Z}_2^\times)^r$ there exists $w \in N$ such that $\pi(wa_iw^{-1}) = \pi(a_i^{k_i})$ for each $1 \leqslant i \leqslant r$.*

Proof. By Proposition 1.3.2 the element $a_i^{k_i}$ is conjugate to a_i under W for each i. Thus by Theorem 2.4.3 there exist $w \in W$ and $x_1, \ldots, x_r \in G$ such that $a_i^{k_i} = (wx_i)a_i(wx_i)^{-1}$ for each i and $\langle\!\langle a_1^{k_1}, \ldots, a_r^{k_r} \rangle\!\rangle = wGw^{-1}$. But $\langle\!\langle a_1^{k_1}, \ldots, a_r^{k_r} \rangle\!\rangle = \langle\!\langle a_1, \ldots, a_r \rangle\!\rangle = G$; hence w lies in N. Also $\pi(wa_iw^{-1}) = \pi((wx_i)a_i(wx_i)^{-1}) = \pi(a_i^{k_i})$ for each i, as desired. $\quad\square$

We can actually construct explicit elements with the property in Lemma 2.6.3, as follows.

Proposition 2.6.4 *For any tuple $(k_i) \in (\mathbb{Z}_2^\times)^r$ write $k_i = 1 + 2\ell_i$ with $\ell_i \in \mathbb{Z}_2$. Define elements $w_i \in W$ by the recursion relations $w_i = (w_{i-1}, a_r^{\ell_{1-i}} w_{i-1})$ for all integers i modulo r. Then for all i and j modulo r we have $w_i a_j w_i^{-1} = a_j^{k_{j-i}}$. In particular the element $w := w_r$ has the property in Lemma 2.6.3.*

Proof. For all i and j set $y_{i,j} := w_i a_j w_i^{-1} a_j^{-k_{j-i}}$. Then for $j > 1$ we have

$$
\begin{aligned}
y_{i,j} &= (w_{i-1}, a_r^{\ell_{1-i}} w_{i-1})(a_{j-1}, 1)(w_{i-1}, a_r^{\ell_{1-i}} w_{i-1})^{-1}(a_{j-1}, 1)^{-k_{j-i}} \\
&= (w_{i-1} a_{j-1} w_{i-1}^{-1} a_{j-1}^{-k_{j-i}}, 1) \\
&= (y_{i-1,j-1}, 1),
\end{aligned}
$$

and for $j = 1$ we have

$$
\begin{aligned}
y_{i,1} &= w_i a_1 w_i^{-1} a_1^{-1}(a_1^2)^{-\ell_{1-i}} \\
&= (w_{i-1}, a_r^{\ell_{1-i}} w_{i-1})(a_r, 1)\,\sigma\,(w_{i-1}, a_r^{\ell_{1-i}} w_{i-1})^{-1}\sigma^{-1}(a_r, 1)^{-1}(a_r, a_r)^{-\ell_{1-i}} \\
&= (w_{i-1}, a_r^{\ell_{1-i}} w_{i-1})(a_r, 1)(w_{i-1}^{-1} a_r^{-\ell_{1-i}}, w_{i-1}^{-1})(a_r^{-1}, 1)(a_r^{-\ell_{1-i}}, a_r^{-\ell_{1-i}}) \\
&= (w_{i-1} a_r w_{i-1}^{-1} a_r^{-1-2\ell_{1-i}}, 1) \\
&= (y_{i-1,r}, 1).
\end{aligned}
$$

These recursion relations for the $y_{i,j}$ satisfy the conditions of Proposition 1.4.1; hence $y_{i,j} = 1$ for all i, j. $\qquad\square$

Now let M denote the kernel of the natural homomorphism $N \to \mathrm{Aut}(G_{\mathrm{ab}})$.

Lemma 2.6.5 $M \subset (M \times M) \cdot G$.

Proof. Take any element $w \in M$. If w acts non-trivially on level 1 of T, we can replace it by wa_1, after which we have $w = (u, v)$ for certain $u, v \in W$. Then (u, v) normalizes $G^1 = G \cap (W \times W)$; hence u normalizes $\mathrm{pr}_1(G^1) = G$ by Proposition 2.2.2 (c), in other words we have $u \in N$. We claim that $u \in M$.

For this consider first any $1 < i \leqslant r$. Then, since $w \in M$, the commutator

$$
[a_i^{-1}, w] = (a_{i-1}, 1)^{-1}(u, v)(a_{i-1}, 1)(u, v)^{-1} = (a_{i-1}^{-1} u a_{i-1} u^{-1}, 1) = ([a_{i-1}^{-1}, u], 1)
$$

lies in K. By Theorem 2.2.7 it therefore lies in $H^{(j)}$ for all $1 \leqslant j \leqslant r$. In particular it lies in $H^{(1)} = H^{(r)} \times H^{(r)}$ by Lemma 2.2.4 (a); hence $[a_{i-1}^{-1}, u]$ lies in $H^{(r)}$. Also, for any $1 < j \leqslant r$ the element $([a_{i-1}^{-1}, u], 1)$ lies in $H^{(j)} \cap (W \times W) \subset (H^{(j-1)} \times H^{(j-1)}) \cdot \langle\!\langle (a_{j-1}, a_{j-1}^{-1})\rangle\!\rangle$ by Lemma 2.2.4 (b), where the product is semidirect by Proposition 2.2.6. This implies that $[a_{i-1}^{-1}, u]$ lies in $H^{(j-1)}$. Together this shows that $[a_{i-1}^{-1}, u]$ lies in $H^{(1)} \cap \ldots \cap H^{(r)} = K$.

Next, since $w \in M$, the commutator

$$
\begin{aligned}
[a_1^{-1}, w] &= \sigma\,(a_r, 1)^{-1}(u, v)(a_r, 1)\,\sigma\,(u, v)^{-1} \\
&= (1, a_r^{-1})(v, u)(1, a_r)(u^{-1}, v^{-1}) \\
&= (vu^{-1}, a_r^{-1} u a_r v^{-1})
\end{aligned}
$$

33

also lies in K, and hence in $H^{(j)}$ for all $1 \leqslant j \leqslant r$. In particular it lies in $H^{(1)} = H^{(r)} \times H^{(r)}$ by Lemma 2.2.4 (a); hence

$$(2.6.6) \qquad\qquad a_r^{-1} u a_r v^{-1} \text{ and } v u^{-1} \text{ lie in } H^{(r)},$$

and so their product $a_r^{-1} u a_r u^{-1} = [a_r^{-1}, u]$ lies in $H^{(r)}$. Also, for any $1 < j \leqslant r$ the element $(vu^{-1}, a_r^{-1} u a_r v^{-1})$ lies in $H^{(j)} \cap (W \times W) \subset (H^{(j-1)} \times H^{(j-1)}) \cdot \langle\!\langle (a_{j-1}, a_{j-1}^{-1}) \rangle\!\rangle$ by Lemma 2.2.4 (b). Thus there exists $m \in \mathbb{Z}_2$ such that

$$\left\{ \begin{array}{ll} a_r^{-1} u a_r v^{-1} \in H^{(j-1)} \cdot a_{j-1}^{-m} & \text{and} \\ \quad v u^{-1} \ \ \in H^{(j-1)} \cdot a_{j-1}^{m} = a_{j-1}^{m} \cdot H^{(j-1)}. \end{array} \right\}$$

Therefore their product $a_r^{-1} u a_r u^{-1} = [a_r^{-1}, u]$ lies in $H^{(j-1)}$. Together this shows that $[a_r^{-1}, u]$ lies in $H^{(1)} \cap \ldots \cap H^{(r)} = K$.

We have thus shown that the commutator $[a_i^{-1}, u]$ lies in K for every $1 \leqslant i \leqslant r$. This means that $u \in M$, as claimed.

Finally, the same arguments applied to the element

$$a_1^{-1} w a_1 = \sigma \, (a_r, 1)^{-1} (u, v) \, (a_r, 1) \, \sigma = (1, a_r^{-1}) \, (v, u) \, (1, a_r) = (v, a_r^{-1} u a_r)$$

in place of w show that $v \in M$. Thus $w = (u, v) \in M \times M$, and we are done. $\qquad\square$

Lemma 2.6.7 $M = G$.

Proof. It suffices to prove that for any $n \geqslant 0$ and any element $w \in M$ the restriction $w|_{T_n}$ lies in G_n. This is trivial for $n = 0$, so assume that $n > 0$ and that the assertion holds universally for $n - 1$. We will then prove it for n and any $w \in M$.

By Lemma 2.6.5 we can write $w = (u, v)g$ with $u, v \in M$ and $g \in G$. By the induction hypothesis applied to v there exists an element $y \in G$ such that $v|_{T_{n-1}} = y|_{T_{n-1}}$. By Proposition 2.2.2 (c) we can choose an element $x \in G$ such that $z := (x, y) \in G$. Then $w = (ux^{-1}, vy^{-1}) \, zg$ with $(vy^{-1})|_{T_{n-1}} = 1$ and $zg \in G$. To prove the desired assertion we may replace w by $w(zg)^{-1}$. Afterwards we have $w = (u, v)$ with new elements $u, v \in M$ such that $v|_{T_{n-1}} = 1$.

Now recall from (2.6.6) that vu^{-1} lies in $H^{(r)}$. Since $v|_{T_{n-1}} = 1$, this implies that $u^{-1}|_{T_{n-1}}$ and hence $u|_{T_{n-1}}$ lies in $H_{n-1}^{(r)}$. Thus $w|_{T_n} = (u|_{T_{n-1}}, v|_{T_{n-1}}) = (u|_{T_{n-1}}, 1)$ lies in $H_{n-1}^{(r)} \times 1$ and hence, by Lemma 2.2.9 (b), in G_n. This proves the desired assertion for n. By induction it therefore follows for all $n \geqslant 0$. $\qquad\square$

Theorem 2.6.8 *The natural homomorphism $N \to \mathrm{Aut}(G_{\mathrm{ab}})$ induces an isomorphism*

$$N/G \xrightarrow{\sim} (\mathbb{Z}_2^{\times})^r \subset \mathrm{Aut}(\mathbb{Z}_2^r) \cong \mathrm{Aut}(G_{\mathrm{ab}}).$$

Proof. Lemma 2.6.7 shows that the homomorphism factors through an injection $N/G \hookrightarrow \mathrm{Aut}(G_{\mathrm{ab}})$, and Lemmas 2.6.2 and 2.6.3 describe its image. $\qquad\square$

2.7 Odometers

In this subsection we study the set of odometers in G, in particular concerning conjugacy. First we show that odometers are abundant in G. By the *proportion* of a measurable subset $X \subset G$ we mean the ratio $\mu(X)/\mu(G)$ for any Haar measure μ on G.

Proposition 2.7.1   *(a) For any W-conjugates b_i of a_i and any permutation ρ of $\{1, \ldots, r\}$ the product $b_{\rho 1} \cdots b_{\rho r}$ is an odometer.*

  (b) The set of odometers in G is open and closed in G and has proportion 2^{-r}.

Proof.   Consider the continuous homomorphism $\psi := (\mathrm{sgn}_i)_{i=1}^r \colon G \to \{\pm 1\}^r$. Proposition 2.1.1 implies that ψ is surjective and that $\psi^{-1}((-1, \ldots, -1))$ is the set of elements $x \in G$ satisfying $\mathrm{sgn}_i(x) = -1$ for all $i \geqslant 1$. Thus by Proposition 1.6.2 it is the set of odometers in G, and (b) follows. Proposition 2.1.1 also implies that this subset contains the element $b_{\rho 1} \cdots b_{\rho r}$ in (a), which is therefore an odometer.   □

In particular the (somewhat arbitrarily chosen) element

$$(2.7.2) \qquad\qquad\qquad a_0 := a_1 \cdots a_r$$

is an odometer in G. From (2.0.1) we deduce the recursion relation

$$(2.7.3) \qquad a_1^{-1}\, a_0\, a_1 \;=\; a_2 \cdots a_r\, a_1 \;=\; (a_1, 1) \cdots (a_{r-1}, 1)\, (a_r, 1)\, \sigma \;=\; (a_0, 1)\, \sigma.$$

Theorem 2.7.4   *(a) All odometers in G are conjugate under N.*

  (b) Any two odometers in G with the same image in G_{ab} are conjugate under G.

Proof.   Let $[[G, G]]$ denote the closure of the commutator subgroup of G. Then Proposition 2.2.6 and Theorem 2.2.7 show that G is the disjoint union of the cosets $[[G, G]] \cdot a_1^{k_1} \cdots a_r^{k_r}$ for all $(k_1, \ldots, k_r) \in \mathbb{Z}_2^r$. Moreover, by the same argument as in the proof of Proposition 2.7.1 the set of odometers in G is the union of those cosets with $(k_1, \ldots, k_r) \in (\mathbb{Z}_2^\times)^r$. As N permutes these cosets transitively by Theorem 2.6.8, assertion (a) reduces to assertion (b), and assertion (b) reduces to the special case $(k_1, \ldots, k_r) = (1, \ldots, 1)$. In view of (2.7.2) we must therefore prove that any element of the coset $[[G, G]] \cdot a_0$ is conjugate to a_0 under G. As a preparation we show:

Lemma 2.7.5 *Any element $c \in [[G, G]] \cdot a_0$ is conjugate under G to an element of the form $(d, 1)\, \sigma$ for some $d \in [[G, G]] \cdot a_0$.*

Proof.   From (2.7.3) we deduce that

$$[[G, G]] \cdot a_0 = [[G, G]] \cdot a_1^{-1}\, a_0\, a_1 = [[G, G]] \cdot (a_0, 1)\, \sigma.$$

35

Also, by Theorem 2.2.7 and Lemma 2.2.4 (a) we have $[[G,G]] \subset H^{(1)} = H \times H$ with $H = H^{(r)}$. Taken together we therefore find that $c = (ha_0, h')\,\sigma$ for some $h, h' \in H$. Then $(h', 1)$ lies in G, so that we can replace c by its conjugate

$$(h', 1)\, c\, (h', 1)^{-1} = (h'ha_0, 1)\,\sigma.$$

Thus we may without loss of generality assume that $c \in (W \times 1) \cdot (a_0, 1)\,\sigma$. On the other hand Lemma 2.2.4 (b) implies that $H^{(i)} \cap (W \times 1) \subset H^{(i-1)} \times 1$ for all $1 < i \leqslant r$. Thus from Theorem 2.2.7 we deduce that

$$[[G,G]] \cap (W \times 1) = H^{(1)} \cap \ldots \cap H^{(r)} \cap (W \times 1) \subset \left(H^{(1)} \cap \ldots \cap H^{(r)} \right) \times 1 = [[G,G]] \times 1,$$

and so $c \in \left([[G,G]] \times 1 \right) \cdot (a_0, 1)\,\sigma$, as desired. $\qquad\square$

To prove Theorem 2.7.4, by Lemma 1.3.1 it suffices to show that for any $n \geqslant 0$ and any element $c \in [[G,G]] \cdot a_0$, the restriction $c|_{T_n}$ is conjugate to $a_0|_{T_n}$ under G_n. This is trivial for $n = 0$, so assume that $n > 0$ and that the statement is universally true for $n - 1$ in place of n.

Consider any element $c \in [[G,G]] \cdot a_0$. Since we may replace c by an arbitrary conjugate under G, by Lemma 2.7.5 we may assume that $c = (d, 1)\,\sigma$ for some $d \in [[G,G]] \cdot a_0$. By the induction hypothesis there then exists an element $x \in G$ with $(xa_0x^{-1})|_{T_{n-1}} = d|_{T_{n-1}}$. Next observe that by the definitions (2.2.8) and (2.7.2) of H and a_0 we have $Ha_r = Ha_0$. Thus Proposition 2.2.10 (a) implies that $G = H \cdot \langle\!\langle a_r \rangle\!\rangle = H \cdot \langle\!\langle a_0 \rangle\!\rangle$. Therefore $x \in Ha_0^{\ell}$ for some $\ell \in \mathbb{Z}_2$, and after replacing x by $xa_0^{-\ell}$, which does not change the conjugate xa_0x^{-1}, we may without loss of generality assume that $x \in H$. Then $z := (x, x)\, a_1^{-1}$ is an element of G, which by the recursion relation (2.7.3) satisfies

$$z\, a_0\, z^{-1} = (x, x)\, a_1^{-1}\, a_0\, a_1\, (x, x)^{-1} = (x, x)\, (a_0, 1)\,\sigma\, (x, x)^{-1} = (xa_0x^{-1}, 1)\,\sigma.$$

Thus

$$(z\, a_0\, z^{-1})|_{T_n} = \left((xa_0x^{-1})|_{T_{n-1}}, 1 \right)\,\sigma = (d|_{T_{n-1}}, 1)\,\sigma = c|_{T_n},$$

proving the desired assertion for n. By induction it follows for all $n \geqslant 0$. $\qquad\square$

Now we can extend Theorem 2.4.3 as follows:

Theorem 2.7.6 *Consider any elements $b_1, \ldots, b_r \in W$ such that b_i is conjugate to a_i under W for each i, and set $b_0 = b_1 \cdots b_r$. Then:*

(a) *There exist $w \in W$ and $x_0, \ldots, x_r \in G$ such that $b_i = (wx_i)a_i(wx_i)^{-1}$ for each i.*

(b) *For any w as in (a) we have $\langle\!\langle b_0, \ldots, b_r \rangle\!\rangle = \langle\!\langle b_1, \ldots, b_r \rangle\!\rangle = wGw^{-1}$.*

(c) *The coset wG for w as in (a) is uniquely determined.*

Proof. By Theorem 2.4.3 we find $w \in W$ and $x_1, \ldots, x_r \in G$ such that $b_i = (wx_i)a_i(wx_i)^{-1}$ for all $1 \leqslant i \leqslant r$. Then $c := w^{-1}b_0w = (x_1a_1x_1^{-1}) \cdots (x_ra_rx_r^{-1})$ is an element of G with the same image in G_{ab} as $a_0 = a_1 \cdots a_r$ and is therefore an odometer. So by Theorem 2.7.4 there exists $x_0 \in G$ with $c = x_0a_0x_0^{-1}$ and hence $b_0 = (wx_0)a_0(wx_0)^{-1}$. This proves (a). Again (b) follows from Proposition 2.4.2.

For (c) consider two elements $w, w' \in W$ with the properties in (a). Then there exist $x_0, x_0' \in G$ with $b_0 = (wx_0)a_0(wx_0)^{-1} = (w'x_0')a_0(w'x_0')^{-1}$. The element $(wx_0)^{-1}(w'x_0') \in W$ then commutes with a_0, and so by Proposition 1.6.4 (b) it lies in $\langle\!\langle a_0 \rangle\!\rangle$ and hence in G. Therefore $w'G = w'x_0'G = wx_0G = wG$, proving (c). (Note that in (a) we can always replace $w, x_0, \ldots, x_r$ by $wy, y^{-1}x_0, \ldots, y^{-1}x_r$ for an arbitrary element $y \in G$, so that (c) is optimal.) $\qquad\square$

We can also describe how the normalizer of any odometer in G sits inside N:

Proposition 2.7.7 *Consider any odometer $c \in G$ and any $\ell \in \mathbb{Z}_2^\times$.*

(a) *There exists an element $w \in N$ with $wcw^{-1} = c^\ell$.*

(b) *Every element $w \in W$ with $wcw^{-1} = c^\ell$ lies in N.*

(c) *For any such w, the image of the coset wG under the isomorphism $N/G \xrightarrow{\sim} (\mathbb{Z}_2^\times)^r$ of Theorem 2.6.8 is $(\ell, \ldots, \ell)$.*

Proof. Since c^ℓ is another odometer in G, part (a) follows from Theorem 2.7.4 (a). Next consider two elements $w, w' \in W$ with $wcw^{-1} = w'cw'^{-1} = c^\ell$. Then $w^{-1}w' \in W$ commutes with c. By Proposition 1.6.4 (b) it therefore lies in $\langle\!\langle c \rangle\!\rangle$ and hence in G. Thus $wG = w'G$. Since $w \in N$ for some choice of w, it follows that $w \in N$ for every choice, proving (b).

Recall from the proof of Theorem 2.7.4 that the image of c under the isomorphism $G_{\mathrm{ab}} \cong \mathbb{Z}_2^r$ of Theorem 2.2.7 is an element of the form $(k_1, \ldots, k_r) \in (\mathbb{Z}_2^\times)^r$. The image of $wcw^{-1} = c^\ell$ is then equal to $(\ell k_1, \ldots, \ell k_r)$; hence the image of w under the isomorphism of Theorem 2.6.8 is $(\ell, \ldots, \ell)$. $\qquad\square$

2.8 Iterated monodromy groups

Now let $G^{\mathrm{geom}} \subset G^{\mathrm{arith}} \subset W$ be the geometric and arithmetic fundamental groups associated to a quadratic polynomial over k, as described in Subsection 1.7, and assume that we are in the periodic case 1.7.2 (b). Then $G^{\mathrm{geom}} = \langle\!\langle b_1, \ldots, b_r \rangle\!\rangle$, where by Proposition 1.7.14 the generators satisfy the recursion relations

$$(2.8.1) \qquad \left\{ \begin{array}{l} b_1 \text{ is conjugate to } (b_r, 1)\,\sigma \text{ under } W, \text{ and} \\ b_i \text{ is conjugate to } (b_{i-1}, 1) \text{ under } W \text{ for all } 2 \leqslant i \leqslant r. \end{array} \right\}$$

By combining Proposition 2.4.1 and Theorem 2.4.3 we deduce:

Theorem 2.8.2 *There exists $w \in W$ such that $G^{\mathrm{geom}} = wGw^{-1}$ and b_i is conjugate to wa_iw^{-1} under G^{geom} for every $1 \leqslant i \leqslant r$.*

For the following we change the identification of trees used in Subsection 1.7 by the automorphism w, after which we have $G^{\mathrm{geom}} = G$, and b_i is conjugate to a_i under G for every $1 \leqslant i \leqslant r$. Then G^{arith} is contained in the normalizer N, and to describe it it suffices to describe the factor group $G^{\mathrm{arith}}/G \subset N/G$. More precisely we will determine the composite homomorphism

$$(2.8.3) \qquad \bar{\rho} \colon \mathrm{Gal}(\bar{k}/k) \twoheadrightarrow G^{\mathrm{arith}}/G \subset N/G \cong (\mathbb{Z}_2^\times)^r$$

obtained from (1.7.7) and Theorem 2.6.8.

Theorem 2.8.4   (a) *The homomorphism $\bar{\rho}$ is the cyclotomic character $\mathrm{Gal}(\bar{k}/k) \to \mathbb{Z}_2^\times$ followed by the diagonal embedding $\mathbb{Z}_2^\times \hookrightarrow (\mathbb{Z}_2^\times)^r$.*

(b) *If k is finitely generated over its prime field, then G^{arith}/G is a subgroup of finite index of $\mathrm{diag}(\mathbb{Z}_2^\times) \subset (\mathbb{Z}_2^\times)^r$.*

Proof.   For any $1 \leqslant i \leqslant r$ let $I_{\xi_i} \subset D_{\xi_i} \subset \pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_k^1 \setminus S, x_0)$ denote the inertia group, respectively the decomposition group at a point above ξ_i. Since ξ_i is a k-rational point, we have a commutative diagram with exact rows

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & I_{\xi_i} & \longrightarrow & D_{\xi_i} & \longrightarrow & \mathrm{Gal}(\bar{k}/k) & \longrightarrow & 1 \\
 & & \cup & & \cup & & \| & & \\
1 & \longrightarrow & \pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_{\bar{k}}^1 \setminus S, x_0) & \longrightarrow & \pi_1^{\mathrm{\acute{e}t}}(\mathbb{P}_k^1 \setminus S, x_0) & \longrightarrow & \mathrm{Gal}(\bar{k}/k) & \longrightarrow & 1 \\
 & & {\scriptstyle \rho}\downarrow & & {\scriptstyle \rho}\downarrow & & {\scriptstyle \bar{\rho}}\downarrow & & \\
1 & \longrightarrow & G & \longrightarrow & G^{\mathrm{arith}} & \longrightarrow & G^{\mathrm{arith}}/G & \longrightarrow & 1.
\end{array}
$$

Since the target of the homomorphism ρ is a pro-2 group, the restriction $\rho|_{I_{\xi_i}}$ factors through the maximal pro-2 quotient of I_{ξ_i}. As the characteristic of k is different from 2, this quotient is the pro-2 tame inertia group above ξ_i and hence isomorphic $\mathbb{Z}_2$. Moreover, $D_{\xi_i}/I_{\xi_i} \cong \mathrm{Gal}(\bar{k}/k)$ acts on it through the cyclotomic character. Thus $\mathrm{Gal}(\bar{k}/k)$ acts on the subgroup $\langle\!\langle \pi(b_i) \rangle\!\rangle \subset G_{\mathrm{ab}}$ through the cyclotomic character. But since b_i is conjugate to a_i under G, we have $\pi(b_i) = \pi(a_i)$, and by Theorem 2.2.7 these elements for all i form a basis of G_{ab} as a module over $\mathbb{Z}_2$. Thus $\mathrm{Gal}(\bar{k}/k)$ acts on G_{ab} diagonally through the cyclotomic character, proving (a).

(An alternative argument uses only the image of the inertia group at ∞, a generator of which is $b_\infty = (b_1 \cdots b_r)^{-1}$ by Subsection 1.7 and therefore an odometer. The homomorphism $D_\infty \to N/G$ can then be determined directly using Proposition 2.7.7. Compare Subsection 3.10.)

For (b) let $\mathbb{F}$ denote the prime field of k and consider the cyclotomic character $\mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F}) \to \mathbb{Z}_2^\times$. In the case $\mathbb{F} = \mathbb{Q}$ this is surjective. Otherwise $\mathbb{F} = \mathbb{F}_p$ for an odd prime p, and the

cyclotomic character sends Frob_p to $p \in \mathbb{Z}_2^\times$. Since $p \neq \pm 1$, it topologically generates an open subgroup of $\mathbb{Z}_2^\times$. Thus in both cases the cyclotomic character has an open image. As k is a finitely generated extension of $\mathbb{F}$, the natural homomorphism $\mathrm{Gal}(\bar{k}/k) \to \mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F})$ also has an open image. Thus (b) follows from (a). $\qquad\square$

3 Strictly pre-periodic case

Throughout this section we fix integers $r > s \geqslant 1$. Using the construction from Subsection 1.4 we define elements $a_1, \ldots, a_r \in W$ by the recursion relations

$$(3.0.1) \qquad \begin{cases} a_1 & = \sigma, \\ a_{s+1} & = (a_s, a_r), \\ a_i & = (a_{i-1}, 1) \quad \text{for } i \neq 1, s+1. \end{cases}$$

We will study the subgroup $G := \langle\!\langle a_1, \ldots, a_r \rangle\!\rangle \subset W$ and its images $G_n \subset W_n$ for all n. The recursion relations are only one choice encoding the qualitative recursive behavior of the generators described by the diagram

$$(3.0.2)$$
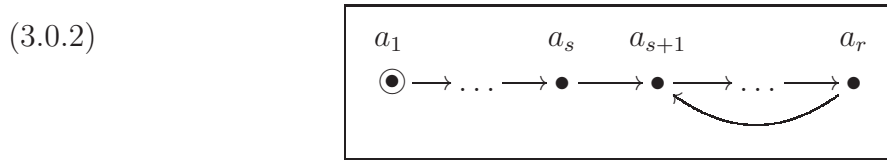
where the vertices are now marked by the generators and the superfluous generator corresponding to the critical point ∞ is dropped: see Subsection 1.7. In Subsection 3.4 we will show that many other choices yield the same group G up to conjugacy in W.

3.1 Basic properties

Proposition 3.1.1 *For all $n \geqslant 1$ and all $1 \leqslant i \leqslant r$ we have*

$$\mathrm{sgn}_n(a_i) \;=\; \begin{cases} -1 & \text{if } n = i \leqslant s, \\ -1 & \text{if } n \geqslant i > s \text{ and } n \equiv i \bmod (r-s), \\ 1 & \text{otherwise.} \end{cases}$$

Proof. The definition of a_i implies that $\mathrm{sgn}_1(a_1) = -1$ and $\mathrm{sgn}_1(a_i) = 1$ for all $2 \leqslant i \leqslant r$; hence the formula holds for $n = 1$. Assume that $n > 1$ and that the formula holds for $n-1$ in place of n. Then the formulas (1.5.2) and (1.5.3) imply the recursion relations

$$\begin{cases} \mathrm{sgn}_n(a_1) & = \mathrm{sgn}_n(\sigma) = 1 \\ \mathrm{sgn}_n(a_{s+1}) & = \mathrm{sgn}_{n-1}(a_s) \cdot \mathrm{sgn}_{n-1}(a_r) \\ \mathrm{sgn}_n(a_1) & = \mathrm{sgn}_{n-1}(a_{i-1}) \qquad \text{for } i \neq 1, s+1. \end{cases}$$

Using these one directly verifies by case distinction that the formula is correct for n. Thus the proposition follows by induction on n. $\qquad\square$

Proposition 3.1.2 *For any $n \geqslant 0$ we have $G_n = W_n$ if and only if $n \leqslant r$.*

Proof. Direct consequence of Propositions 1.5.6 (a) and 3.1.1. $\qquad\square$

Proposition 3.1.3 *The group G acts transitively on the level n of T for every $n \geqslant 0$.*

Proof. Consider the element $w := a_1 \cdots a_r \in G$. Proposition 3.1.1 implies that $\operatorname{sgn}_n(w) = -1$ for all $n \geqslant 1$; hence w already acts transitively on every level by Proposition 1.6.2. $\square$

Proposition 3.1.4 *Each generator a_i has order 2.*

Proof. By Proposition 3.1.1 we have $\operatorname{sgn}_i(a_i) = -1$ and hence $a_i \neq 1$ for every $1 \leqslant i \leqslant r$. On the other hand the elements $b_i := a_i^2$ satisfy the recursion relations

$$\left\{ \begin{array}{ll} b_1 & = \sigma^2 = 1, \\ b_{s+1} & = (b_s, b_r), \\ b_i & = (b_{i-1}, 1) \quad \text{for } i \neq 1, s+1. \end{array} \right\}$$

By Proposition 1.4.1 we therefore have $b_i = 1$ for all i. Thus each a_i has precise order 2. $\square$

Lemma 3.1.5 *For any $1 \leqslant i \leqslant r$ and $n \geqslant 0$ we have $a_i|_{T_n} = 1$ if and only if $n < i$.*

Proof. Direct consequence of the recursion relations (3.0.1) and Proposition 3.1.1. $\square$

Theorem 3.1.6 *Let G_{ab} denote the maximal profinite abelian factor group of G. Then the homomorphism $(\operatorname{sgn}_i)_{i=1}^r|_G$ induces an isomorphism $G_{\mathrm{ab}} \xrightarrow{\sim} \{\pm 1\}^r$.*

Proof. As the elements $a_1, \ldots, a_r$ topologically generate G, their images topologically generate the abelian group G_{ab}, and since the generators have order 2, we find that G_{ab} is a finite elementary abelian 2-group generated by r elements. On the other hand the continuous homomorphism $(\operatorname{sgn}_i)_{i=1}^r \colon G \to \{\pm 1\}^r$ has an abelian group as target and therefore factors through G_{ab}. Since $\operatorname{sgn}_i(a_j) = (-1)^{\delta_{i,j}}$ (Kronecker delta) for all $1 \leqslant i, j \leqslant r$ by Proposition 3.1.1, the generators $a_1, \ldots, a_r$ map to a basis of $\{\pm 1\}^r$. Together we deduce that $G_{\mathrm{ab}} \to \{\pm 1\}^r$ is an isomorphism. $\square$

Remark 3.1.7 Any two distinct indices $1 \leqslant i, j \leqslant r$ yield distinct elements a_i and a_j of order two; hence the subgroup generated by them is dihedral (including infinite pro-dihedral) of order at least 4. Specifically, we have $\langle\!\langle a_i, a_j \rangle\!\rangle = \langle\!\langle a_i a_j \rangle\!\rangle \rtimes \langle a_i \rangle$ with $a_i(a_i a_j)a_i^{-1} = (a_i a_j)^{-1} = a_j a_i$. The order of this dihedral group is determined by the order of its cyclic part:

Lemma 3.1.8 *For any distinct $1 \leqslant i, j \leqslant r$ we have*

$$(a_i a_j)^2 = \left\{ \begin{array}{ll} ((a_{i-1}a_{j-1})^2, 1) & \text{if } i, j \neq 1, \\ (a_{j-1}, a_{j-1}) & \text{if } i = 1 \text{ and } j \neq s+1, \\ (a_r a_s, a_s a_r) & \text{if } i = 1 \text{ and } j = s+1. \end{array} \right.$$

Proof. If both i, j are $\neq 1, s+1$, we have $(a_i a_j)^2 = \big((a_{i-1}, 1)(a_{j-1}, 1)\big)^2 = ((a_{i-1}a_{j-1})^2, 1)$. If $i \neq 1, s+1$ but $j = s+1$, we have $(a_i a_j)^2 = \big((a_{i-1}, 1)(a_{j-1}, a_r)\big)^2 = ((a_{i-1}a_{j-1})^2, a_r^2)$, which is again equal to $((a_{i-1}a_{j-1})^2, 1)$ because $a_r^2 = 1$. A similar calculation applies when $i = s+1$ and $j \neq 1, s+1$. This proves the first formula.

For $j \neq 1, s+1$ we calculate $(a_1 a_j)^2 = \sigma(a_{j-1}, 1)\,\sigma(a_{j-1}, 1) = (a_{j-1}, a_{j-1})$, proving the second formula. Finally $(a_1 a_{s+1})^2 = \sigma(a_s, a_r)\,\sigma(a_s, a_r) = (a_r a_s, a_s a_r)$, proving the last. $\qquad\square$

Proposition 3.1.9 *For any $1 \leqslant i < j \leqslant r$ we have*

$$
\mathrm{ord}(a_i a_j) = \mathrm{ord}(a_j a_i) = \begin{cases} 4 & \text{if } j \neq i+s, \\ 8 & \text{if } j = i+s \text{ and } r \neq 2s, \\ \infty & \text{if } j = i+s \text{ and } r = 2s. \end{cases}
$$

In particular we have

$$
\mathrm{ord}(a_s a_r) = \mathrm{ord}(a_r a_s) = \begin{cases} 4 & \text{if } r \neq 2s, \\ \infty & \text{if } r = 2s. \end{cases}
$$

Proof. The first formula in Lemma 3.1.8 shows that $\mathrm{ord}(a_i a_j) = \mathrm{ord}(a_{i-1} a_{j-1})$ if $i, j > 1$. By induction on i this implies that

$$(3.1.10) \qquad\qquad \mathrm{ord}(a_i a_j) = \mathrm{ord}(a_1 a_{j-i+1}) \quad \text{for all } 1 \leqslant i < j \leqslant r.$$

For $j \neq s+1$ the second formula in Lemma 3.1.8 shows that $\mathrm{ord}(a_1 a_j) = 2 \cdot \mathrm{ord}(a_{j-1}) = 4$. This together with (3.1.10) implies the desired formula in the case $j \neq i+s$.

The third formula in Lemma 3.1.8 shows that $\mathrm{ord}(a_1 a_{s+1}) = 2 \cdot \mathrm{ord}(a_s a_r)$. If $r \neq 2s$, by the case already proved this implies that $\mathrm{ord}(a_1 a_{s+1}) = 2 \cdot 4 = 8$. With (3.1.10) we thus obtain the desired formula in the case $j = i+s$ and $r \neq 2s$. On the other hand, if $r = 2s$, using (3.1.10) we find that $\mathrm{ord}(a_1 a_{s+1}) = 2 \cdot \mathrm{ord}(a_s a_r) = 2 \cdot \mathrm{ord}(a_1 a_{r-s+1}) = 2 \cdot \mathrm{ord}(a_1 a_{s+1})$. Thus $\mathrm{ord}(a_1 a_{s+1}) = \infty$ in this case, and with (3.1.10) we deduce the desired formula in the last case. $\qquad\square$

3.2 Useful subgroups

First we consider the subgroup of index 2 which acts trivially on level 1:

$$(3.2.1) \qquad\qquad G^1 \;:=\; G \cap (W \times W).$$

Let pr_1 and $\mathrm{pr}_2 \colon W \times W \to W$ denote the two projections. We have the following self-similarity properties:

Proposition 3.2.2 *(a)* $G \subset (G \times G) \rtimes \langle \sigma \rangle$.

(b) $G^1 \subset (G \times G)$.

(c) $\mathrm{pr}_1(G^1) = \mathrm{pr}_2(G^1) = G$.

Proof. Essentially the same as that of Proposition 2.2.2. □

Next we consider the following normal subgroup of G:

$$(3.2.3) \qquad H \; := \; \left\{ \begin{array}{l} \text{closure of the subgroup of } G \text{ generated} \\ \text{by all } G\text{-conjugates of } a_i \text{ for all } i \neq s, r. \end{array} \right\}.$$

Proposition 3.2.4 *We have:*

(a) $G = H \cdot \langle\!\langle a_s, a_r \rangle\!\rangle$.

(b) $G = (H \times H) \cdot \langle\!\langle \sigma, (a_s, a_r) \rangle\!\rangle$.

(c) $G^1 = (H \times H) \cdot \langle\!\langle (a_s, a_r), (a_r, a_s) \rangle\!\rangle$.

Proof. Assertion (a) is a direct consequence of the definition of H.

For (b) let H' denote the closure of the subgroup of G generated by all G-conjugates of a_i for all $i \neq 1, s+1$. Then by the same token we have $G = H' \cdot \langle\!\langle a_1, a_{s+1} \rangle\!\rangle = H' \cdot \langle\!\langle \sigma, (a_s, a_r) \rangle\!\rangle$. On the other hand, the generators of H' are precisely the G-conjugates of $a_i = (a_{i-1}, 1)$ for all $2 \leqslant i \leqslant r$ with $i \neq s+1$, or in other words the G-conjugates of $(a_j, 1)$ for all $1 \leqslant j \leqslant r$ with $j \neq s, r$. Proposition 3.2.2 implies that the conjugates of these elements under G^1 alone form the set of all $(x, 1)$ where x runs through all G-conjugates of a_j for all $j \neq s, r$. These elements topologically generate the subgroup $H \times 1 \subset G$. Its conjugate by σ is $1 \times H$; hence together we find that $H' = H \times H$. This proves (b).

Finally, since $\sigma (a_s, a_r) \sigma^{-1} = (a_r, a_s)$, the intersection of $\langle\!\langle \sigma, (a_s, a_r) \rangle\!\rangle$ with $W \times W$ is $\langle\!\langle (a_s, a_r), (a_r, a_s) \rangle\!\rangle$; hence (b) implies (c). □

Next we consider the following closed normal subgroup of G:

$$(3.2.5) \qquad\qquad\qquad K \; := \; H \cdot \langle\!\langle a_s a_r \rangle\!\rangle.$$

As the index of $\langle\!\langle a_s a_r \rangle\!\rangle$ in $\langle\!\langle a_s, a_r \rangle\!\rangle$ is 2, Proposition 3.2.4 (a) implies that the index of K in G is at most 2. On the other hand, Proposition 3.1.1 shows that the signs sgn_s and sgn_r are trivial on all generators of H, and the product $\mathrm{sgn}_s \, \mathrm{sgn}_r$ is also trivial on $a_s a_r$. Thus K is contained in the subgroup $\mathrm{Ker}(\mathrm{sgn}_s \, \mathrm{sgn}_r |_G)$ of index 2 of G. Together this shows that

$$(3.2.6) \qquad\qquad K = \mathrm{Ker}(\mathrm{sgn}_s \, \mathrm{sgn}_r |_G) \;\; \text{and has index 2 in } G.$$

Lemma 3.2.7 *The set* $\{xy^{-1} \mid (x, y) \in G^1\}$ *is equal to* K.

Proof. Using Remark 3.1.7 we can write Proposition 3.2.4 (c) in the form

$$G^1 = (H \times H) \cdot \langle\!\langle (a_s a_r, a_r a_s) \rangle\!\rangle \cdot \langle (a_s, a_r) \rangle.$$

Thus an arbitrary element of G^1 has the form

$$(x, y) = (h, h') \, (a_s a_r, a_r a_s)^\lambda (a_s, a_r)^\mu = \left(h(a_s a_r)^\lambda a_s^\mu, h'(a_r a_s)^\lambda a_r^\mu \right)$$

for arbitrary $h, h' \in H$ and $\lambda \in \mathbb{Z}_2$ and $\mu \in \{0, 1\}$. Then

$$xy^{-1} = h(a_s a_r)^\lambda a_s^\mu a_r^{-\mu} (a_r a_s)^{-\lambda} h'^{-1} = h(a_s a_r)^\lambda (a_s a_r)^\mu (a_s a_r)^\lambda h'^{-1} = h(a_s a_r)^{2\lambda + \mu} h'^{-1}.$$

Here $2\lambda + \mu$ runs through all of $\mathbb{Z}_2$, and since H is normal in G and h, h' are arbitrary elements of H, the set of elements obtained is precisely $H \cdot \langle\!\langle a_s a_r \rangle\!\rangle = K$, as desired. $\qquad\square$

Lemma 3.2.8 *For any $u \in W$ we have $(u, u^{-1}) \in G$ if and only if $u \in K$.*

Proof. If the element lies in G, it must already lie in G^1. But by Proposition 3.2.4 (c) we have

$$G^1 = (H \times H) \cdot \langle\!\langle (a_s, a_r), (a_r, a_s) \rangle\!\rangle = (H \times H) \cdot \langle\!\langle (a_s a_r, a_r a_s) \rangle\!\rangle \cdot \langle (a_s, a_r) \rangle.$$

Thus (u, u^{-1}) lies in G^1 if and only if there exist $\lambda \in \mathbb{Z}_2$ and $\mu \in \{0, 1\}$ such that

$$(u, u^{-1}) \in (H \times H) \cdot (a_s a_r, a_r a_s)^\lambda \cdot (a_s, a_r)^\mu$$

$$\Longleftrightarrow \quad \left\{ \begin{array}{ll} u & \in \quad H(a_s a_r)^\lambda a_s^\mu \quad \text{and} \\ u^{-1} & \in \quad H(a_r a_s)^\lambda a_r^\mu \end{array} \right\}$$

$$\Longleftrightarrow \quad u \quad \in \quad H(a_s a_r)^\lambda a_s^\mu \cap a_r^{-\mu} (a_r a_s)^{-\lambda} H.$$

Since sgn_s is trivial on H and a_r, but not on a_s, the last condition requires that $\lambda + \mu \equiv -\lambda$ modulo 2, in other words that $\mu = 0$. Since already $(a_s a_r)^\lambda = (a_r a_s)^{-\lambda}$, the condition is therefore equivalent to $u \in H(a_s a_r)^\lambda$ for some $\lambda \in \mathbb{Z}_2$, and thus to $u \in K$, as desired. $\qquad\square$

Next we consider the following closed normal subgroup of G:

$$(3.2.9) \qquad L := \left\{ \begin{array}{l} \text{closure of the subgroup of } G \text{ generated} \\ \text{by all } G\text{-conjugates of } a_1 = \sigma. \end{array} \right\}.$$

Lemma 3.2.10 *Let $[[K, K]]$ denote the closure of the commutator subgroup of K. Let* anti$\colon W \to W \times W$ *denote the 'antidiagonal' map $w \mapsto (w, w^{-1})$ (which is not a homomorphism!). Then*

$$L = \left(\left([[K, K]] \times [[K, K]] \right) \cdot \mathrm{anti}(K) \right) \rtimes \langle \sigma \rangle.$$

Proof. The definition of L means equivalently that L is the closure of the subgroup generated by σ and the commutators $[g, \sigma]$ for all $g \in G$. Since $G = G^1 \rtimes \langle \sigma \rangle$, these commutators are the same as those for all $g \in G^1$. For $(x, y) \in G^1$ we have

$$(x, y)\, \sigma\, (x, y)^{-1} \sigma^{-1} = (xy^{-1}, yx^{-1}) = \mathrm{anti}(xy^{-1}),$$

hence by Lemma 3.2.7 the set of these commutators is precisely $\mathrm{anti}(K)$. For any $u, v \in K$ we calculate

$$\mathrm{anti}(u)\, \mathrm{anti}(v)\, \mathrm{anti}(u^{-1}v^{-1}) = (u, u^{-1})\,(v, v^{-1})\,(u^{-1}v^{-1}, vu) = (uvu^{-1}v^{-1}, 1).$$

Thus the closure of the subgroup generated by $\mathrm{anti}(K)$ contains $[[K, K]] \times 1$. Using this and its conjugate under σ we deduce that $[[K, K]] \times [[K, K]] \subset L$. Now the composite map

$$\mathrm{anti}\colon K \hookrightarrow K \times K \twoheadrightarrow K/[[K, K]] \times K/[[K, K]]$$

is a homomorphism, because the target group is abelian. Thus $\big([[K, K]] \times [[K, K]]\big) \cdot \mathrm{anti}(K)$ is already a subgroup, and since K is closed and hence compact, it is also already closed. Thus this product is the closure of the subgroup generated by $\mathrm{anti}(K)$. Recombining this with σ we deduce the desired formula in the lemma. $\qquad\square$

Lemma 3.2.11 *(a) For any $i, j \neq s, r$ we have $(a_i a_j)^2 \in [[K, K]]$.*

(b) For any $i, j \neq 1, s+1$ we have $(a_i a_j)^2 \in L$.

Proof. In (a) the assumption $i, j \neq s, r$ implies that a_i and a_j lie in H and hence in K. They also have order 2, so that $(a_i a_j)^2 = [a_i, a_j] \in [[K, K]]$, as desired.

In (b) the assumption $i, j \neq 1, s+1$ shows that $i-1, j-1 \neq s, r$ and hence $(a_{i-1}a_{j-1})^2 \in [[K, K]]$ by (a). Thus $(a_i a_j)^2 = \big((a_{i-1}a_{j-1})^2, 1\big) \in [[K, K]] \times 1 \subset L$ by Lemma 3.2.10, proving (b). $\qquad\square$

Proposition 3.2.12 *If $s \geqslant 2$ and $r \geqslant 4$, then $(a_s a_r)^2 \in H$.*

Proof. If $s \geqslant 2$ and $r > s+1$, Lemma 3.2.11 (b) directly shows that $(a_s a_r)^2 \in L$. But as $s > 1$, the definitions of L and H imply that $L \subset H$, whence the proposition in this case.

If $r = s+1$, we first note that $(a_s a_r)^2 = ((a_{s-1}a_s)^2, 1)$ by Lemma 3.1.8. The assumption $r \geqslant 4$ now implies that $s \geqslant 3$ and therefore $s - 1, s \neq 1, s+1$. Thus $(a_{s-1}a_s)^2 \in L$ by Lemma 3.2.11 (b). The fact that $s \geqslant 3$ also implies that all G-conjugates of $a_2 = (a_1, 1)$ are among the generators of H. Using Proposition 3.2.2 we find that the G^1-conjugates of $(a_1, 1)$ are precisely the elements $(x, 1)$ for all G-conjugates x of $a_1 = \sigma$. Thus by definition of L implies that $L \times 1 \subset H$. Together this shows that $(a_s a_r)^2 = \big((a_{s-1}a_s)^2, 1\big) \in L \times 1 \subset H$, as desired. $\qquad\square$

We will also need some results on finite levels. As before, for any subgroup $X \subset W$ we let X_n denote its image in W_n.

Lemma 3.2.13 *For any $n \geqslant r$ we have*

   (a) $H_n \subset \mathrm{Ker}(\mathrm{sgn}_s|_{G_r}) \cap \mathrm{Ker}(\mathrm{sgn}_r|_{G_r})$.

   (b) $H_n \cap \langle a_s|_{T_n}, a_r|_{T_n} \rangle \subset \langle (a_s a_r)^2|_{T_n} \rangle$.

   (c) $\left[\langle a_s|_{T_n}, a_r|_{T_n} \rangle : \langle (a_s a_r)^2|_{T_n} \rangle \right] = 4$.

Proof. For $n \geqslant r$ both sgn_s and sgn_r factor through W_n and are trivial on all generators of H; hence they are trivial on H_n. This proves (a). On the other hand $\mathrm{sgn}_s(a_s|_{T_n}) = \mathrm{sgn}_r(a_r|_{T_n}) = -1$ and $\mathrm{sgn}_s(a_r|_{T_n}) = \mathrm{sgn}_r(a_s|_{T_n}) = 1$. Since $\langle a_s|_{T_n}, a_r|_{T_n} \rangle$ is a dihedral group, this and the assertion (a) implies (b) and (c). $\qquad\square$

Proposition 3.2.14 *If $s = 2$ and $r = 3$, then $(a_s a_r)^2|_{T_r} \in H_r$, whereas $(a_s a_r)^2|_{T_n} \notin H_n$ for all $n \geqslant r + 1 = 4$.*

Proof. Since $s = 2$ and $r = 3$, Lemma 3.1.8 implies that $(a_s a_r)^2 = (a_2 a_3)^2 = ((a_1 a_2)^2, 1) = ((a_1, a_1), 1) = ((\sigma, \sigma), 1)$. By the definitions of H and L the assumptions $s = 2$ and $r = 3$ also imply that $H = L$. Thus Lemma 3.2.10 shows that

$$H_n \cap (W_{n-1} \times W_{n-1}) \;=\; \big([K_{n-1}, K_{n-1}] \times [K_{n-1}, K_{n-1}]\big) \cdot \mathrm{anti}(K_{n-1})$$

where $[K_{n-1}, K_{n-1}]$ denotes the commutator subgroup of K_{n-1}. This in turn implies that

$$H_n \cap (W_{n-1} \times 1) \;=\; [K_{n-1}, K_{n-1}] \times 1.$$

Therefore $(a_s a_r)^2|_{T_n} \in H_n$ if and only if $(\sigma, \sigma) \in [K_{n-1}, K_{n-1}]$.

Suppose first that $n = 3$. Then $n - 1 = 2$, and $a_3|_{T_2} = 1$. Thus $K_{n-1} = K_2$ contains the elements $a_1|_{T_2} = \sigma$ and $(a_2 a_3)|_{T_2} = (a_1, 1)|_{T_2} = (\sigma, 1)$; in particular we have $K_2 = W_2$. It follows that $(\sigma, \sigma) = [\sigma, (\sigma, 1)] \in [K_2, K_2]$, and so $(a_s a_r)^2|_{T_3} \in H_3$, as desired.

Suppose next that $n = 4$. Then $[W_3 : K_3] = 2$ and a straightforward finite calculation, left to the gracious reader, shows that $[K_3, K_3]$ is the subgroup of order 8 generated by

$$((\sigma, \sigma), 1) \quad \text{and} \quad (1, (\sigma, \sigma)) \quad \text{and} \quad ((\sigma, 1)\sigma, (\sigma, 1)\sigma).$$

It follows that $(\sigma, \sigma) \notin [K_3, K_3]$, and so $(a_s a_r)^2|_{T_4} \notin H_4$.

Finally, since K_4 is the image of K_n in W_4 for any $n \geqslant 4$, this also implies that $(a_s a_r)^2|_{T_n} \notin H_n$ for any $n \geqslant 4$, as desired. $\qquad\square$

Lemma 3.2.15 *If $s \geqslant 2$, then:*

   (a) $H_r = \mathrm{Ker}(\mathrm{sgn}_s|_{W_r}) \cap \mathrm{Ker}(\mathrm{sgn}_r|_{W_r})$ *and has index 4 in W_r.*

(b) $H_r \times H_r$ is a normal subgroup of $W_{r+1} = (W_r \times W_r) \rtimes \langle \sigma \rangle$, and there is an isomorphism

$$W_{r+1}/(H_r \times H_r) \xlongequal{\sim} (W_r/H_r \times W_r/H_r) \rtimes \langle \sigma \rangle \xrightarrow{\sim} \mathrm{Mat}_{2 \times 2}(\{\pm 1\}) \rtimes \langle \sigma \rangle,$$

$$(uH_r, vH_r) \cdot \sigma^\lambda \longmapsto \left(\begin{smallmatrix} \mathrm{sgn}_s(u) & \mathrm{sgn}_s(v) \\ \mathrm{sgn}_r(u) & \mathrm{sgn}_r(v) \end{smallmatrix} \right) \cdot \sigma^\lambda,$$

where σ acts on a 2×2-matrix by interchanging the columns.

(c) The image of $G_{r+1}/(H_r \times H_r)$ under this isomorphism is the subgroup

$$\left\langle \left(\begin{smallmatrix} -1 & 1 \\ 1 & -1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix} \right) \right\rangle \rtimes \langle \sigma \rangle.$$

(d) The normalizer of this last subgroup in $\mathrm{Mat}_{2 \times 2}(\{\pm 1\}) \rtimes \langle \sigma \rangle$ is

$$\left\langle \left(\begin{smallmatrix} -1 & 1 \\ 1 & -1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix} \right), \left(\begin{smallmatrix} -1 & 1 \\ -1 & 1 \end{smallmatrix} \right) \right\rangle \rtimes \langle \sigma \rangle.$$

In particular, the index of G_{r+1} in its normalizer in W_{r+1} is 2.

Proof. By Propositions 3.2.12 and 3.2.14 we have $(a_s a_r)^2|_{T_r} \in H_r$ whenever $s \geqslant 2$. Thus the inclusion in Lemma 3.2.13 (b) is an equality. On the other hand, by Propositions 3.1.2 and 3.2.4 (a) we have $G_r = W_r = H_r \cdot \langle a_s|_{T_r}, a_r|_{T_r} \rangle$. Combining this with the remaining information in Lemma 3.2.13 implies (a).

From (a) we readily obtain the isomorphism in (b). Next Proposition 3.2.4 implies that $G_{r+1} = G_{r+1}^1 \rtimes \langle \sigma \rangle$ with $G_{r+1}^1 = (H_r \times H_r) \cdot \langle (a_s|_{T_r}, a_r|_{T_r}), (a_r|_{T_r}, a_s|_{T_r}) \rangle$, which directly implies (c). The last part (d) is an easy direct calculation that is left to the reader. $\square$

Proposition 3.2.16 *If $s = 1$, then $(a_s a_r)^2|_{T_n} \notin H_n$ for all $n \geqslant r$.*

Proof. If $r = 2$, then $H = 1$ by definition and the assertion holds trivially. So assume that $s \geqslant 3$. Then by definition H is the closure of the subgroup generated by all G-conjugates of $a_i = (a_{i-1}, 1)$ for all $i \neq 1, s+1, r$ and of $a_{s+1} = (a_s, a_r)$. In other words it is the closure of the subgroup generated by all G-conjugates of $(a_j, 1)$ for all $j \neq s, r-1, r$ and of $(a_s, a_r) = (a_1, a_r)$. Thus if H' denotes the closure of the subgroup generated by all G-conjugates of a_i for all $i \neq r-1$, from Proposition 3.2.2 we deduce that $H \subset H' \times H'$. This in turn implies that $H_n \subset H'_{n-1} \times H'_{n-1}$.

Now $(a_s a_r)^2 = (a_1 a_r)^2 = (a_{r-1}, a_{r-1})$ by Lemma 3.1.8, because $r > 2 = s + 1$. Thus $(a_s a_r)^2|_{T_n} = (a_{r-1}|_{T_{n-1}}, a_{r-1}|_{T_{n-1}})$, and so to prove the proposition it suffices to show that $a_{r-1}|_{T_{n-1}} \notin H'_{n-1}$.

For this recall from Proposition 3.1.1 that $\mathrm{sgn}_{r-1}(a_{r-1}) = -1$, while $\mathrm{sgn}_{r-1}(a_i) = 1$ for all $i \neq r-1$. Thus sgn_{r-1} is trivial on all the generators of H' and hence on H'. Moreover, the assumption $n \geqslant r$ implies that $n-1 \geqslant r-1$; hence sgn_{r-1} factors through W_{n-1}. Thus the resulting function $W_{n-1} \to \{\pm 1\}$ is identically 1 on H'_{n-1} but not on $a_{r-1}|_{T_{n-1}}$; hence $a_{r-1}|_{T_{n-1}} \notin H'_{n-1}$, as desired. $\square$

Proposition 3.2.17 *For any $n \geqslant 0$ we have*

$$H_n \cap \langle a_s|_{T_n}, a_r|_{T_n} \rangle = \begin{cases} 1 & \text{if } n < r, \\ 1 & \text{if } s = 1, \\ 1 & \text{if } s = 2 \text{ and } r = 3 \text{ and } n \geqslant 4, \\ \langle (a_s a_r)^2|_{T_n} \rangle & \text{if } s = 2 \text{ and } r = 3 \text{ and } n = 3, \\ \langle (a_s a_r)^2|_{T_n} \rangle & \text{if } s \geqslant 2 \text{ and } r \geqslant 4 \text{ and } n \geqslant r. \end{cases}$$

Proof. If $n < s$ then $a_s|_{T_n} = a_r|_{T_n} = 1$ and the assertion holds trivially. If $s \leqslant n < r$ then $a_r|_{T_n} = 1$, and so the question concerns $H_n \cap \langle a_s|_{T_n} \rangle$. But then sgn_s factors through W_n and is trivial on all generators of H; hence sgn_s is trivial on H_n. On the other hand $\mathrm{sgn}_s(a_s|_{T_n}) = -1$, and $a_s|_{T_n}$ is an element of order 2; hence the intersection is trivial, as desired.

For the rest of the proof assume that $n \geqslant r$. Then by Lemma 3.2.13 (b) we have $H_n \cap \langle a_s|_{T_n}, a_r|_{T_n} \rangle \subset \langle (a_s a_r)^2|_{T_n} \rangle$.

If $s \geqslant 2$ and $r \geqslant 4$, then Proposition 3.2.12 implies that this inclusion is an equality, as desired. If $s = 2$ and $r = 3$ and $n = r = 3$, the same follows from Proposition 3.2.14.

If $s = 2$ and $r = 3$ and $n \geqslant r+1 = 4$, then $(a_s a_r)^2|_{T_n} \notin H_n$ by Proposition 3.2.14. Since $(a_s a_r)^4 = 1$ by Proposition 3.1.9 in this case, it follows that the intersection is trivial, as desired.

Finally, if $s = 1$, then $(a_s a_r)^2|_{T_n} \notin H_n$ by Proposition 3.2.16. If in addition $r \geqslant 3$, then $(a_s a_r)^4 = 1$ by Proposition 3.1.9; hence the intersection is trivial, as desired. If $r = 2$, then already $H = 1$ by construction and hence $H_n = 1$ and the intersection is again trivial. This finishes the proof in all cases. $\qquad\square$

3.3 Size

Lemma 3.3.1 *For any $n \geqslant r \geqslant 3$ we have*

$$[G_n : H_n] = \begin{cases} 8 & \text{if } s = 1, \\ 8 & \text{if } s = 2 \text{ and } r = 3 \text{ and } n \geqslant 4, \\ 4 & \text{if } s = 2 \text{ and } r = 3 \text{ and } n = 3, \\ 4 & \text{if } s \geqslant 2 \text{ and } r \geqslant 4. \end{cases}$$

Proof. In all cases, Proposition 3.2.4 (a) implies that $G_n = H_n \cdot \langle a_s|_{T_n}, a_r|_{T_n} \rangle$ and hence

$$[G_n : H_n] = [\langle a_s|_{T_n}, a_r|_{T_n} \rangle : H_n \cap \langle a_s|_{T_n}, a_r|_{T_n} \rangle].$$

If $s = 1$, the assumption $r \geqslant 3$ and Lemma 3.1.8 show that $(a_s a_r)^2|_{T_n} = (a_{r-1}|_{T_{n-1}}, a_{r-1}|_{T_{n-1}})$, where $a_{r-1}|_{T_{n-1}}$ has order 2 by Lemma 3.1.5. Thus $\langle a_s|_{T_n}, a_r|_{T_n} \rangle$ has order 8 in this case, and the desired assertion follows from the case $s = 1$ of Proposition 3.2.17.

If $s = 2$ and $r = 3$, then Lemma 3.1.8 implies that $(a_s a_r)^2|_{T_n} = ((a_1 a_2)^2|_{T_{n-1}}, 1)$ and that $(a_1 a_2)^2|_{T_{n-1}} = (a_1|_{T_{n-2}}, a_1|_{T_{n-2}})$. Since $n \geqslant 3$, the element $a_1|_{T_{n-2}} = \sigma|_{T_{n-2}}$ has order 2;

hence so does $(a_s a_r)^2|_{T_n}$. Thus $\langle a_s|_{T_n}, a_r|_{T_n} \rangle$ has order 8 in this case. Again the desired assertions follows from the corresponding cases of Proposition 3.2.17.

Finally, from Lemma 3.2.13 (c) we already know that $\left[\langle a_s|_{T_n}, a_r|_{T_n} \rangle : \langle (a_s a_r)^2|_{T_n} \rangle \right] = 4$ in all cases. Thus the last case is a direct consequence of the corresponding case in Proposition 3.2.17. $\qquad\square$

Lemma 3.3.2 *For any $n \geqslant r$ we have*

$$[G_{n+1} : H_n \times H_n] = 2 \cdot [G_n : H_n].$$

Proof. By Proposition 3.2.4 (c) we have $G_{n+1}^1 = (H_n \times H_n) \cdot \langle (a_s|_{T_n}, a_r|_{T_n}), (a_r|_{T_n}, a_s|_{T_n}) \rangle$. Here $\langle (a_s|_{T_n}, a_r|_{T_n}), (a_r|_{T_n}, a_s|_{T_n}) \rangle$ is a dihedral group which maps isomorphically to the dihedral group $\langle a_s|_{T_n}, a_r|_{T_n} \rangle$ under both projections. From Lemma 3.2.13 (b) we already know that $H_n \cap \langle a_s|_{T_n}, a_r|_{T_n} \rangle$ is contained in $\langle (a_s a_r)^2|_{T_n} \rangle$. Since moreover $\left((a_s|_{T_n}, a_r|_{T_n})(a_r|_{T_n}, a_s|_{T_n}) \right)^2 = \left((a_s a_r)^2|_{T_n}, (a_r a_s)^2|_{T_n} \right)$, where the second entry is the inverse of the first, we deduce that $(H_n \times H_n) \cap \langle (a_s|_{T_n}, a_r|_{T_n}), (a_r|_{T_n}, a_s|_{T_n}) \rangle$ maps isomorphically to $H_n \cap \langle a_s|_{T_n}, a_r|_{T_n} \rangle$ under both projections. Thus

$$
\begin{aligned}
[G_{n+1}^1 : H_n \times H_n] &= \left[\langle (a_s|_{T_n}, a_r|_{T_n}), (a_r|_{T_n}, a_s|_{T_n}) \rangle : (H_n \times H_n) \cap \langle (a_s|_{T_n}, a_r|_{T_n}), (a_r|_{T_n}, a_s|_{T_n}) \rangle \right] \\
&= \left[\langle a_s|_{T_n}, a_r|_{T_n} \rangle : H_n \cap \langle \langle a_s|_{T_n}, a_r|_{T_n} \rangle \right] \\
&= [G_n : H_n].
\end{aligned}
$$

Finally, since $n + 1 > 0$ we have $[G_{n+1} : G_{n+1}^1] = 2$, and the proposition follows. $\qquad\square$

Proposition 3.3.3 *For all $n \geqslant 0$ we have*

$$
\log_2 |G_n| = \begin{cases}
2^n - 1 & \text{if } n \leqslant r, \\
n + 1 & \text{if } s = 1 \text{ and } r = 2 \text{ and } n \geqslant 2, \\
2^n - 3 \cdot 2^{n-r} + 2 & \text{if } s = 1 \text{ and } r \geqslant 3 \text{ and } n \geqslant r, \\
2^n - 5 \cdot 2^{n-4} + 2 & \text{if } s = 2 \text{ and } r = 3 \text{ and } n \geqslant 4, \\
2^n - 2^{n-r+1} + 1 & \text{if } s \geqslant 2 \text{ and } r \geqslant 4 \text{ and } n \geqslant r.
\end{cases}
$$

Proof. The first case $n \geqslant r$ results from Proposition 3.1.2 and the formula (1.2.1).

In the case $s = 1$ and $r = 2$ we have $G_n = \langle a_s|_{T_n}, a_r|_{T_n} \rangle$ and will calculate directly. Here $a_1 a_2 = \sigma(a_1, a_2)$ is non-trivial on level 1 and hence on T_n for every $n \geqslant 1$. This and the fact that $(a_1 a_2)^2 = (a_2 a_1, a_1 a_2)$ implies that $\operatorname{ord}(a_1 a_2|_{T_n}) = 2 \cdot \operatorname{ord}(a_1 a_2|_{T_{n-1}})$ for all $n \geqslant 1$. By induction on n we deduce that $\operatorname{ord}(a_1 a_2|_{T_n}) = 2^n$ for all $n \geqslant 0$. For all $n \geqslant r = 2$ it follows that $G_n \cong D_{2^n}$ and hence $|G_n| = 2^{n+1}$, as desired.

In the other cases, for all $n \geqslant r$ Lemma 3.3.2 implies that

$$|G_{n+1}| = 2 \cdot [G_n : H_n] \cdot |H_n|^2 = |G_n|^2 \cdot 2 \cdot [G_n : H_n]^{-1}.$$

49

From this and Lemma 3.3.1 we deduce that

$$\log_2 |G_{n+1}| \;=\; 2 \cdot \log_2 |G_n| - \begin{cases} 2 & \text{if } s = 1, \\ 2 & \text{if } s = 2 \text{ and } r = 3 \text{ and } n \geqslant 4, \\ 1 & \text{if } s = 2 \text{ and } r = 3 \text{ and } n = 3, \\ 1 & \text{if } s \geqslant 2 \text{ and } r \geqslant 4. \end{cases}$$

We use this recursion relation to deduce the remaining formulas by induction on n.

In the case $s = 1$ and $r \geqslant 3$ observe first that $2^n - 3 \cdot 2^{n-r} + 2 = 2^n - 1$ for $n = r$; hence $\log_2 |G_n| = 2^n - 3 \cdot 2^{n-r} + 2$ for $n = r$. If the same formula holds for some $n \geqslant r$, the above recursion relation implies that $\log_2 |G_{n+1}| = 2 \cdot (2^n - 3 \cdot 2^{n-r} + 2) - 2 = 2^{n+1} - 3 \cdot 2^{n+1-r} + 2$; hence the same formula holds for $n + 1$ in place of n. The formula therefore holds for all $n \geqslant r$, as desired.

In the case $s = 2$ and $r = 3$ we already know that $\log_2 |G_3| = 2^3 - 1 = 7$. Thus the recursion relation implies that $\log_2 |G_4| = 2 \cdot 7 - 1 = 13$. This coincides with the value of $2^n - 5 \cdot 2^{n-4} + 2$ for $n = 4$. If $\log_2 |G_n| = 2^n - 5 \cdot 2^{n-4} + 2$ for some $n \geqslant r$, the above recursion relation implies that $\log_2 |G_{n+1}| = 2 \cdot (2^n - 5 \cdot 2^{n-4} + 2) - 2 = 2^{n+1} - 5 \cdot 2^{n+1-4} + 2$; hence the same formula holds for $n + 1$ in place of n. The formula therefore holds for all $n \geqslant 4$, as desired.

Finally, in the case $s \geqslant 2$ and $r \geqslant 4$ we already have $\log_2 |G_n| = 2^n - 1 = 2^n - 2^{n-r+1} + 1$ in the case $n = r$. If $\log_2 |G_n| = 2^n - 2^{n-r+1} + 1$ for some $n \geqslant r$, the above recursion relation implies that $\log_2 |G_{n+1}| = 2 \cdot (2^n - 2^{n-r+1} + 1) - 1 = 2^{n+1} - 2^{n+1-r+1} + 1$; hence the same formula holds for $n + 1$ in place of n. The formula therefore holds for all $n \geqslant r$, as desired. This finishes the proof in all cases. $\qquad\square$

Theorem 3.3.4 *The Hausdorff dimension of G exists and is*

$$\begin{cases} 0 & \text{if } s = 1 \text{ and } r = 2, \\ 1 - 3 \cdot 2^{-r} & \text{if } s = 1 \text{ and } r \geqslant 3, \\ 1 - 5 \cdot 2^{-4} & \text{if } s = 2 \text{ and } r = 3, \\ 1 - 2^{1-r} & \text{if } s \geqslant 2 \text{ and } r \geqslant 4. \end{cases}$$

Proof. By (1.2.2) the Hausdorff dimension of G is the limit of $\frac{\log_2 |G_n|}{2^n - 1}$ for $n \to \infty$. Thus the given formulas follow directly from Proposition 3.3.3. $\qquad\square$

3.4 Conjugacy of generators

The same remarks as in Subsection 2.4 apply here to the recursion relations (3.0.1). Essentially the same proof as for Proposition 2.4.1 yields:

Proposition 3.4.1 *For any elements $b_1, \ldots, b_r \in W$ the following are equivalent:*

(a) b_i is conjugate to a_i under W for each i.

$$(b) \begin{cases} b_1 \text{ is conjugate to } \sigma \text{ under } W, \\ b_{s+1} \text{ is conjugate to } (b_s, b_r) \text{ under } W, \text{ and} \\ b_i \text{ is conjugate to } (b_{i-1}, 1) \text{ under } W \text{ for all } i \neq 1, s+1. \end{cases}$$

Likewise the same proof as for Proposition 2.4.2 yields:

Proposition 3.4.2 *Consider any elements $b_1, \dots, b_r \in G$ such that b_i is conjugate to a_i under W for every i. Then $G = \langle\!\langle b_1, \dots, b_r \rangle\!\rangle$.*

Theorem 3.4.3 *Consider any elements $b_1, \dots, b_r \in W$ such that b_i is conjugate to a_i under W for each i. Then there exist $w \in W$ and $x_1, \dots, x_r \in G$ such that $b_i = (wx_i)a_i(wx_i)^{-1}$ for each i, and we then have $\langle\!\langle b_1, \dots, b_r \rangle\!\rangle = wGw^{-1}$.*

Proof. The second assertion is a direct consequence of the first and Proposition 3.4.2. The first follows by taking the limit over n from the following assertion for all $n \geqslant 0$: For any elements $b_1, \dots, b_r \in W_n$ such that b_i is conjugate to $a_i|_{T_n}$ under W_n for each i, there exist $w \in W_n$ and $x_1, \dots, x_r \in G_n$ such that $b_i = (wx_i)(a_i|_{T_n})(wx_i)^{-1}$ for each i. This is trivial for $n = 0$, so assume that $n > 0$ and that the assertion is universally true for $n-1$. Take elements $b_1, \dots, b_r \in W_n$ such that b_i is conjugate to $a_i|_{T_n}$ under W_n for each i.

Since b_1 is conjugate to $a_1|_{T_n} = \sigma|_{T_n}$, after conjugating everything by a single element of W_n we may assume that $b_1 = \sigma|_{T_n}$.

For each $i \neq 1, s+1$ the element b_i is conjugate to $a_i|_{T_n} = (a_{i-1}|_{T_{n-1}}, 1)$ under W_n. Thus it is conjugate to $(a_{i-1}|_{T_{n-1}}, 1)$ or $(1, a_{i-1}|_{T_{n-1}})$ under the subgroup $W_{n-1} \times W_{n-1}$. In the second case we can replace b_i by its conjugate $b_1 b_i b_1^{-1}$, which, as in the proof of Theorem 2.4.3, does not change the assertion to be proved. Thus without loss of generality we may assume that b_i is conjugate to $(a_{i-1}|_{T_{n-1}}, 1)$ under $W_{n-1} \times W_{n-1}$. This means that $b_i = (c_{i-1}, 1)$ for some $c_{i-1} \in W_{n-1}$ which is conjugate to $a_{i-1}|_{T_{n-1}}$ under W_{n-1}.

Likewise the element b_{s+1} is conjugate to $a_{s+1}|_{T_n} = (a_s|_{T_{n-1}}, a_r|_{T_{n-1}})$ under W_n. By the same argument as above, after possibly replacing b_{s+1} by its conjugate $b_1 b_{s+1} b_1^{-1}$ we may without loss of generality assume that b_{s+1} is conjugate to $(a_s|_{T_{n-1}}, a_r|_{T_{n-1}})$ under $W_{n-1} \times W_{n-1}$. This means that $b_{s+1} = (c_s, c_r)$, where $c_s \in W_{n-1}$ is conjugate to $a_s|_{T_{n-1}}$ under W_{n-1}, and $c_r \in W_{n-1}$ is conjugate to $a_r|_{T_{n-1}}$ under W_{n-1}.

Thus for every $1 \leqslant i \leqslant r$ we have found an element $c_i \in W_{n-1}$ which is conjugate to $a_i|_{T_{n-1}}$ under W_{n-1}. By the induction hypothesis there therefore exist $u \in W_{n-1}$ and $x_1, \dots, x_r \in G_{n-1}$ such that $c_i = (ux_i)(a_i|_{T_{n-1}})(ux_i)^{-1}$ for every i.

Now observe that the definition (3.2.5) of K implies that $G = K \cdot \langle a_r \rangle$. Using this and Lemma 3.2.7, we can write the element $x_s^{-1} x_r \in G_n$ in the form $x_s^{-1} x_r = xy^{-1}(a_r^\nu|_{T_{n-1}})$ for some $(x, y) \in G_n^1$ and $\nu \in \{0, 1\}$. Set $v := ux_s x \in W_{n-1}$, so that $ux_s = vx^{-1}$ and $ux_r = ux_s xy^{-1}(a_r^\nu|_{T_{n-1}}) = vy^{-1}(a_r^\nu|_{T_{n-1}})$. Then

$$\begin{aligned} b_{s+1} &= \left(\; (ux_s)(a_s|_{T_{n-1}})(ux_s)^{-1} \; , \; (ux_r)(a_r|_{T_{n-1}})(ux_r)^{-1} \; \right) \\ &= \left((vx^{-1})(a_s|_{T_{n-1}})(vx^{-1})^{-1}, (vy^{-1})(a_r|_{T_{n-1}})(vy^{-1})^{-1} \right). \end{aligned}$$

Thus with $w := (v, v) \in W_n$ and $z_{s+1} := (x^{-1}, y^{-1}) \in G_n^1 \subset G_n$ we find that

$$b_{s+1} = (wz_{s+1}) (a_s|_{T_{n-1}}, a_r|_{T_{n-1}})(wz_{s+1})^{-1} = (wz_{s+1}) (a_{s+1}|_{T_n}) (wz_{s+1})^{-1}.$$

Also, the element $w = (v, v)$ commutes with $\sigma|_{T_n}$; hence with $z_1 := 1 \in G_n$ we have

$$b_1 = \sigma|_{T_n} = (wz_1) (a_1|_{T_n}) (wz_1)^{-1}.$$

Furthermore, for any $i \neq 1, s+1$ we have $ux_{i-1} = vx^{-1}x_s^{-1}x_{i-1}$ with $x^{-1}x_s^{-1}x_{i-1} \in G_{n-1}$. By Proposition 3.2.2 we can therefore find an element $y_{i-1} \in G_{n-1}$ such that $z_i := (x^{-1}x_s^{-1}x_{i-1}, y_{i-1})$ lies in G_n. Then

$$
\begin{aligned}
b_i &= (\qquad (ux_{i-1})(a_{i-1}|_{T_{n-1}})(ux_{i-1})^{-1} \qquad , \qquad 1 \qquad) \\
&= ((vx^{-1}x_s^{-1}x_{i-1})(a_{i-1}|_{T_{n-1}})(vx^{-1}x_s^{-1}x_{i-1})^{-1}, (vy_{i-1})(vy_{i-1})^{-1}) \\
&= (wz_i) (a_{i-1}|_{T_{n-1}}, 1) (wz_i)^{-1} \\
&= (wz_i) (a_i|_{T_n}) (wz_i)^{-1}.
\end{aligned}
$$

Altogether we have thus found an element $w \in W_n$ and elements $z_i \in G_n$ such that $b_i = (wz_i)(a_i|_{T_n})(wz_i)^{-1}$ for all $1 \leqslant i \leqslant r$. This proves the desired assertion for n, and so we are done by induction. $\qquad \square$

Proposition 3.4.4 *Consider any $1 \leqslant i \leqslant r$. Assume that $i \leqslant s$ or $s = 1$. Then any element $b_i \in G$ that is conjugate to a_i under W is conjugate to a_i under G.*

The author does not know whether the proposition holds without the extra assumptions on i and s.

Proof. First we consider the case $i = 1$. An arbitrary W-conjugate of $a_1 = \sigma$ has the form $b_1 = (u, v) \sigma (u, v)^{-1} = (uv^{-1}, vu^{-1}) \sigma$ for $u, v \in W$. Thus it lies in G if and only if (uv^{-1}, vu^{-1}) lies in G. By Lemmas 3.2.8 and Lemma 3.2.7 this is equivalent to $uv^{-1} = xy^{-1}$ for some $(x, y) \in G^1$. But then b_1 is equal to $(xy^{-1}, yx^{-1}) = (x, y) \sigma (x, y)^{-1}$ and hence conjugate to σ under G, as desired.

Next we consider the case $2 \leqslant i \leqslant s$. By induction on i we may assume that the proposition holds for $i - 1$ in place of i. Take any element $w \in W$ such that $b_i := wa_iw^{-1}$ lies in G. If w acts non-trivially on level 1, we replace b_i by its G-conjugate $a_1b_ia_1^{-1}$ and w by a_1w, which does not change the desired assertion. Afterwards we have $w = (u, v)$ for some elements $u, v \in W$. Then the recursion relation yields

$$b_i = wa_iw^{-1} = (u, v) (a_{i-1}, 1) (u, v)^{-1} = (ua_{i-1}u^{-1}, 1).$$

Since b_i lies in G, Proposition 3.2.2 (b) implies that $b_{i-1} := ua_{i-1}u^{-1}$ lies in G. By the induction hypothesis we therefore have $b_{i-1} = xa_{i-1}x^{-1}$ for some element $x \in G$. By Proposition 3.2.2 (c) we can choose an element $y \in G$ for which $z := (x, y)$ lies in G. Then

$$b_i = (b_{i-1}, 1) = (xa_{i-1}x^{-1}, 1) = (x, y) (a_{i-1}, 1) (x, y)^{-1} = za_iz^{-1},$$

52

which proves that b_i is conjugate to a_i under G, as desired.

The remaining cases require an infinite recursion, which we realize as an induction over finite levels of the tree T. By Lemma 1.3.1 it suffices to show that for any $n \geqslant 0$ and any $s + 1 \leqslant i \leqslant r$, any element $b_i \in G_n$ that is conjugate to $a_i|_{T_n}$ under W_n is conjugate to $a_i|_{T_n}$ under G_n. This is trivial for $n = 0$, so assume that $n > 0$ and that the statement is universally true for $n - 1$ in place of n. Consider an element $b_i \in G_n$ that is conjugate to $a_i|_{T_n}$ under W_n, and choose an element $w \in W_n$ such that $b_i = w\,(a_i|_{T_n})\,w^{-1}$.

If $i > s + 1$, the same argument as in the induction step above reduces the statement for i and n to that for $i - 1$ and $n - 1$, as in the proof of Proposition 2.4.4. So it remains to deal with the case $i = s + 1$. This is where the extra assumption on s is used.

First, if w acts non-trivially on level 1, we replace w by $(a_1|_{T_n})\,w$ and b_{s+1} by its G_n-conjugate $(a_1|_{T_n})\,b_{s+1}\,(a_1|_{T_n})^{-1}$, which does not change the desired assertion. Afterwards we have $w = (u, v)$ for some elements $u, v \in W_{n-1}$. Next the recursion relation yields

$$b_{s+1} = w\,(a_{s+1}|_{T_n})\,w^{-1} = (u, v)\,(a_s|_{T_{n-1}}, a_r|_{T_{n-1}})\,(u, v)^{-1} = \big(u(a_s|_{T_{n-1}})u^{-1}, v(a_r|_{T_{n-1}})v^{-1}\big).$$

Since b_{s+1} lies in G_n, Proposition 3.2.2 (b) shows that $v(a_r|_{T_{n-1}})v^{-1}$ lies in G_{n-1}. By the induction hypothesis we therefore have $v(a_r|_{T_{n-1}})v^{-1} = y(a_r|_{T_{n-1}})y^{-1}$ for some $y \in G_{n-1}$. By Proposition 3.2.2 (c) we can choose an element $x \in G_{n-1}$ for which $z := (x, y)$ lies in G_n. After replacing b_{s+1} by its G_n-conjugate $z^{-1}b_{s+1}z$ and w by $z^{-1}w$, and hence u by $x^{-1}u$, which does not change the desired assertion, we may therefore assume that

$$b_{s+1} = \big(u(a_s|_{T_{n-1}})u^{-1}, a_r|_{T_{n-1}}\big).$$

Next, since b_{s+1} lies in G_n, Proposition 3.2.2 (b) shows that $u(a_s|_{T_{n-1}})u^{-1}$ lies in G_{n-1}. By the induction hypothesis we can therefore find a new element $x \in G_{n-1}$ such that $u(a_s|_{T_{n-1}})u^{-1} = x(a_s|_{T_{n-1}})x^{-1}$. By Proposition 3.2.4 we can write this in the form $x = h((a_s a_r)^\lambda a_s^\mu)|_{T_{n-1}}$ for some $h \in H_{n-1}$ and $\lambda \in \mathbb{Z}$ and $\mu \in \{0, 1\}$. Then

$$\begin{aligned}
b_{s+1} &= \big(h((a_s a_r)^\lambda a_s^\mu a_s a_s^{-\mu}(a_s a_r)^{-\lambda})|_{T_{n-1}}h^{-1}, a_r|_{T_{n-1}}\big) \\
&= \big(h((a_s a_r)^{2\lambda} a_s)|_{T_{n-1}}h^{-1}, a_r|_{T_{n-1}}\big) \\
&\in (H_{n-1} \times 1) \cdot \big(((a_s a_r)^{2\lambda})|_{T_{n-1}}, 1\big) \cdot (a_s, a_r)|_{T_n}.
\end{aligned}$$

The fact that b_{s+1} lies in G_n thus implies that $\big(((a_s a_r)^{2\lambda})|_{T_{n-1}}, 1\big)$ lies in G_n, and hence in G_n^1. Now, and only now, we use the assumption $s = 1$. By it and Proposition 3.2.17, we then have $H_{n-1} \cap \langle a_s|_{T_{n-1}}, a_r|_{T_{n-1}}\rangle = 1$. By Proposition 3.2.4 (c) this implies that

$$G_n^1 = (H_{n-1} \times H_{n-1}) \rtimes \big\langle (a_s|_{T_{n-1}}, a_r|_{T_{n-1}}), (a_r|_{T_{n-1}}, a_s|_{T_{n-1}})\big\rangle.$$

The fact that $\big(((a_s a_r)^{2\lambda})|_{T_{n-1}}, 1\big)$ lies in G_n is therefore equivalent to $((a_s a_r)^{2\lambda})|_{T_{n-1}} = 1$. By the above calculation this means that

$$b_{s+1} = \big(h(a_s|_{T_{n-1}})h^{-1}, a_r|_{T_{n-1}}\big) = (h, 1)\,(a_s|_{T_{n-1}}, a_r|_{T_{n-1}})\,(h, 1)^{-1} = (h, 1)\,(a_{s+1}|_{T_n})\,(h, 1)^{-1}.$$

Since $(h, 1) \in H_{n-1} \times 1$ lies in G_n by Proposition 3.2.4 (b), this proves that b_{s+1} is conjugate to $a_{s+1}|_{T_n}$ under G_n, as desired. Thus finishes the induction step and thus proves the required statement for all $n \geqslant 0$. $\qquad\square$

3.5 Small cases

In the smallest possible case

$$(3.5.1) \qquad\qquad s = 1 \ \text{ and } \ r = 2$$

we have $G = \langle\!\langle a_1, a_2 \rangle\!\rangle$, where both generators have order two. Thus $G = \langle\!\langle a_1 a_2 \rangle\!\rangle \rtimes \langle a_1 \rangle$ is infinite dihedral by Proposition 3.1.9. Moreover $a_1 a_2$ is an odometer by Proposition 3.9.1 below. Thus by Proposition 1.6.4 the normalizer of $\langle\!\langle a_1 a_2 \rangle\!\rangle$ in W is isomorphic to $\mathbb{Z}_2 \rtimes \mathbb{Z}_2^\times$. Since G is contained in it, we deduce that this is also the normalizer of G. This provides all the information that we will need in this case.

The case $s = 1$ and $r = 2$ is also the only one among the strictly pre-periodic cases where the strong rigidity in the sense of Theorem 2.5.1 holds. In fact, the rigidity is easy to verify directly in this case using the structure of G as a dihedral group.

The next smallest case $s = 1$ and $r = 3$ is the closure of the Grigorchuk group, first introduced by Grigorchuk [7]. Grigorchuk [8, §§12-15] and Grigorchuk-Sidki [10] obtain results for the Grigorchuk group similar to the ones we obtain for its closure, for instance a description of the normalizer. Also, the results of Nekrashevych [17] imply some of the results of the preceding subsection in this case.

3.6 Normalizer, subcase (a)

Next we will determine the normalizer

$$(3.6.1) \qquad\qquad N := \mathrm{Norm}_W(G).$$

Throughout this subsection we assume:

$$(3.6.2) \qquad\qquad s \geqslant 2 \ \text{ and } \ r \geqslant 4.$$

Lemma 3.6.3 *In this case we have:*

(a) $H \cap \langle\!\langle a_s, a_r \rangle\!\rangle = \langle\!\langle (a_s a_r)^2 \rangle\!\rangle$

(b) G/H *is of order 4 and generated by the images of a_s and a_r.*

(c) $H = \mathrm{Ker}(\mathrm{sgn}_r |_G) \cap \mathrm{Ker}(\mathrm{sgn}_s |_G)$.

Proof. Part (a) follows from Proposition 3.2.12 and Lemma 3.2.13, and it implies (b). For (c) observe that the proof of Lemma 3.2.13, without restriction to T_n, shows that H is contained in the subgroup $\mathrm{Ker}(\mathrm{sgn}_r |_G) \cap \mathrm{Ker}(\mathrm{sgn}_s |_G)$ of index 4 of G. Since H already has index 4 in the present case, it is therefore equal to that subgroup. $\qquad\square$

Lemma 3.6.4 *The group N normalizes H and acts trivially on G/H.*

Proof. Direct consequence of Lemma 3.6.3 (c) and the fact that sgn_s and sgn_r are defined on all of W. $\qquad\square$

As before, let $\mathrm{diag}\colon W \to W \times W$, $w \mapsto (w, w)$ denote the diagonal embedding.

Lemma 3.6.5 *We have $N = G \cdot \mathrm{diag}(N)$.*

Proof. Consider any element $w \in W$ and write it in the form $\sigma^\lambda (u, v)$ with $\lambda \in \{0, 1\}$ and $u, v \in W$. Since $\sigma \in G$, we have $w \in N$ if and only if $(u, v) \in N$. If that is so, then (u, v) normalizes $G^1 = G \cap (W \times W)$; so by Proposition 3.2.2 both u and v normalize $\mathrm{pr}_1(G^1) = \mathrm{pr}_2(G^1) = G$. Thus a necessary condition is that $u, v \in N$.

Conversely assume that $u, v \in N$. Then (u, v) already normalizes $H \times H$ by Lemma 3.6.4. It also acts trivially on $(G \times G)/(H \times H)$, and so the conjugate $(u, v)(a_s, a_r)(u, v)^{-1}$ lies in $(H \times H) \cdot (a_s, a_r)$. From Proposition 3.2.4 (b) it thus follows that (u, v) normalizes G if and only if the conjugate $(u, v)\sigma(u, v)^{-1}$ lies in G. Since $\sigma \in G$, this is so if and only if the commutator $(u, v)\sigma(u, v)^{-1}\sigma^{-1} = (uv^{-1}, vu^{-1})$ lies in G. By Lemma 3.2.8 this is equivalent to $uv^{-1} \in K$, and hence by Lemma 3.2.7 to the existence of $(x, y) \in G^1$ such that $uv^{-1} = xy^{-1}$. But that last equality is equivalent to

$$w \;=\; \sigma^\lambda(u, v) \;=\; \sigma^\lambda(xy^{-1}v, v) \;=\; \sigma^\lambda(x, y)(y^{-1}v, y^{-1}v),$$

or equivalently to $w \in z\,\mathrm{diag}(N)$ for $z := \sigma^\lambda(x, y) \in G$. $\qquad\square$

Now we recursively define elements

$$(3.6.6) \qquad \left\{ \begin{aligned} w_1 \ &:= \ (a_s, a_s), \\ w_{i+1} \ &:= \ (w_i, w_i) \quad \text{for all } i \geqslant 1. \end{aligned} \right\}$$

Since $a_s \in G \subset N$, by induction Lemma 3.6.5 implies that $w_i \in N$ for all $i \geqslant 1$. Also, since a_s has order two, by induction the same follows for all w_i. Moreover, by induction we find that the restriction $w_i|_{T_n}$ is trivial for all $i \geqslant n$; hence the sequence $w_1, w_2, \dots$ converges to 1 within N. Thus the following map is well-defined:

$$(3.6.7) \qquad \varphi\colon \prod_{i=1}^{\infty} \mathbb{F}_2 \longrightarrow N, \quad (k_1, k_2, \dots) \mapsto w_1^{k_1} w_2^{k_2} \cdots.$$

By construction it is continuous, but not a homomorphism. Note that it satisfies the basic formula

$$(3.6.8) \qquad \varphi(k_1, k_2, \dots) \;=\; w_1^{k_1} \cdot \mathrm{diag}(\varphi(k_2, k_3, \dots)).$$

Lemma 3.6.9 *The map φ induces a homomorphism $\bar\varphi\colon \prod_{i=1}^{\infty} \mathbb{F}_2 \to N/G$.*

Proof. It suffices to show that for all $1 \leqslant i < j$ the images of w_i and w_j in N/G commute with each other, or in other words that the commutator $[w_i, w_j]$ lies in G. We will prove this by induction on i.

If $i = 1$, we have $[w_1, w_j] = \mathrm{diag}([a_s, w_{j-1}])$. By Lemma 3.6.4 the element w_{j-1} normalizes H and acts trivially on G/H; hence $[a_s, w_{j-1}]$ lies in H. Therefore $[w_1, w_j]$ lies in $H \times H \subset G$, as desired.

For $i > 1$ we have $[w_i, w_j] = \mathrm{diag}([w_{i-1}, w_{j-1}])$, and by the induction hypothesis we already know that $[w_{i-1}, w_{j-1}] \in G$. On the other hand, as a commutator in W, the element $[w_{i-1}, w_{j-1}]$ lies in the kernel of both sgn_s and sgn_r. By Lemma 3.6.3 (c) it therefore lies in H, and so $[w_i, w_j]$ lies in $H \times H \subset G$, as desired. $\qquad\square$

Lemma 3.6.10 *The homomorphism $\bar{\varphi}$ is injective.*

Proof. Let $(k_1, k_2, \ldots)$ be an element of the kernel of $\bar{\varphi}$. Then $w := \varphi(k_1, k_2, \ldots)$ lies in G. We first prove that $k_1 = 0$.

Suppose to the contrary that $k_1 = 1$. Then the definition of φ implies that $w = w_1 \cdot \mathrm{diag}(u)$ for some element $u \in \mathrm{diag}(N)$. Thus $w = (a_s u, a_s u)$ actually lies in G^1. By Proposition 3.2.4 (c) and Lemma 3.6.3 there therefore exist $\lambda, \mu \in \{0, 1\}$ such that

$$(a_s u, a_s u) \in (H \times H) \cdot (a_s, a_r)^\lambda \cdot (a_r, a_s)^\mu$$

$$\Longleftrightarrow \qquad a_s u \in H a_s^\lambda a_r^\mu \cap H a_r^\lambda a_s^\mu.$$

By the structure of G/H the last condition requires that $\lambda = \mu$ and is therefore equivalent to

$$a_s u \in H a_s^\lambda a_r^\lambda.$$

Now the fact that $u = (v, v)$ for some $v \in W$ implies that $\mathrm{sgn}_s(u) = \mathrm{sgn}_r(u) = 1$. Since sgn_s is also trivial on H and on a_r, but not on a_s, the condition implies that $\lambda = 1$. On the other hand, since sgn_r is also trivial on H and on a_s, but not on a_r, the condition implies that $\lambda = 0$. We have thus reached a contradiction and thereby proved that $k_1 = 0$.

Since $k_1 = 0$, the formula (3.6.8) shows that $w = \mathrm{diag}(w')$ for $w' := \varphi(k_2, k_3, \ldots)$. Thus $w = (w', w')$ actually lies in G^1, and so w' lies in G by Proposition 3.2.2 (c). This means that $(k_2, k_3, \ldots)$ also lies in the kernel of $\bar{\varphi}$.

For every element $(k_1, k_2, \ldots)$ of the kernel of $\bar{\varphi}$ we have thus proved that $k_1 = 0$ and that $(k_2, k_3, \ldots)$ again lies in the kernel of $\bar{\varphi}$. By an induction on i we can deduce from this that for every $i \geqslant 1$ and every element $(k_1, k_2, \ldots)$ of the kernel of $\bar{\varphi}$ we have $k_i = 0$. This means that the kernel of $\bar{\varphi}$ is trivial, and so the homomorphism $\bar{\varphi}$ is injective, as desired. $\qquad\square$

Lemma 3.6.11 *The homomorphism $\bar{\varphi}$ is surjective.*

Proof. We first claim that $G \cdot \mathrm{diag}(G) = G \cdot \langle w_1 \rangle$. To see this, recall that $G = H \cdot \langle\!\langle a_s, a_r \rangle\!\rangle$ with $H \triangleleft G$ of index 4. This implies that

$$
\begin{aligned}
(H \times H) \cdot \mathrm{diag}(G) &= (H \times H) \cdot \langle\!\langle (a_s, a_s), (a_r, a_r) \rangle\!\rangle \\
&= (H \times H) \cdot \langle\!\langle (a_s a_r, a_s a_r) \rangle\!\rangle \cdot \langle w_1 \rangle.
\end{aligned}
$$

Since $(a_s a_r)^2 \in H$ in the present case, we have $a_s a_r \in H a_r a_s$ and hence

$$(H \times H) \cdot \operatorname{diag}(G) \;=\; (H \times H) \cdot \langle\!\langle (a_s a_r, a_r a_s) \rangle\!\rangle \cdot \langle w_1 \rangle.$$

As $(a_s a_r, a_r a_s) = (a_s, a_r)(a_r, a_s) \in G$, it follows that

$$G \cdot \operatorname{diag}(G) \;=\; G \cdot \langle\!\langle (a_s a_r, a_r a_s) \rangle\!\rangle \cdot \langle w_1 \rangle \;=\; G \cdot \langle w_1 \rangle,$$

as claimed.

For the surjectivity we must prove that $N = G \cdot \varphi\big(\prod_{i=1}^{\infty} \mathbb{F}_2\big)$. For this it suffices to show that $N_n = G_n \cdot \varphi\big(\prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_n}$ for all $n \geqslant 0$. This is trivial for $n = 0$, so assume that $n > 0$ and that the equality holds for $n - 1$. Using, in turn, Lemma 3.6.5, the induction hypothesis, the above claim, and the formula (3.6.8) we deduce that

$$
\begin{aligned}
N_n \;&=\; G_n \cdot \operatorname{diag}(N_{n-1}) \\
&=\; G_n \cdot \operatorname{diag}\big(G_{n-1} \cdot \varphi\big(\textstyle\prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}}\big) \\
&=\; G_n \cdot \langle w_1|_{T_n} \rangle \cdot \operatorname{diag}\big(\varphi\big(\textstyle\prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}}\big) \\
&=\; G_n \cdot \langle w_1|_{T_n} \rangle \cdot \varphi\big(\{0\} \times \textstyle\prod_{i=2}^{\infty} \mathbb{F}_2\big)|_{T_n} \\
&=\; G_n \cdot \varphi\big(\textstyle\prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_n},
\end{aligned}
$$

so the equality holds for n. Thus it follows for all $n \geqslant 0$ by induction, and we are done. $\quad\square$

Combining Lemmas 3.6.9 through 3.6.11 now implies:

Theorem 3.6.12 *In the case (3.6.2) the map φ induces an isomorphism*

$$\bar{\varphi} \colon \prod_{i=1}^{\infty} \mathbb{F}_2 \xrightarrow{\;\sim\;} N/G.$$

3.7 Normalizer, subcase (b)

Throughout this subsection we assume:

(3.7.1) $$s = 1 \quad \text{and} \quad r \geqslant 3.$$

Lemma 3.7.2 *In this case we have:*

(a) $\langle a_s, a_r \rangle$ *is a finite dihedral group of order 8 with center $\langle (a_s a_r)^2 \rangle$.*

(b) $G = H \rtimes \langle a_s, a_r \rangle$.

(c) $G = (H \times H) \rtimes \langle \sigma, (a_s, a_r) \rangle$.

(d) $H^+ := H \rtimes \langle (a_s a_r)^2 \rangle = \operatorname{Ker}(\operatorname{sgn}_s|_G) \cap \operatorname{Ker}(\operatorname{sgn}_r|_G)$.

Proof. Part (a) follows from Proposition 3.1.9, part (b) from Proposition 3.2.17, and part (c) from Proposition 3.2.4 (b). Part (d) follows by the same arguments as in the proof of Lemma 3.6.3. $\qquad\square$

Lemma 3.7.3 *The group N normalizes H and induces only inner automorphisms on G/H.*

Proof. Recall from (3.2.3) that H is the closure of the subgroup of G generated by all G-conjugates of a_i for all $i \neq s, r$. By Proposition 3.4.4 these G-conjugates are precisely the W-conjugates of a_i which lie in G. The set of these is therefore preserved under conjugation by N; hence H is normalized by N, as desired.

Next, the same argument as in the proof of Lemmas 3.6.3 (c) and 3.6.4 shows that N normalizes H^+ and acts trivially on G/H^+. This means that the action of N on the dihedral group $G/H \cong D_4$ is trivial modulo the center of D_4. But every automorphism of D_4 which is trivial modulo its center is inner. $\qquad\square$

Let M denote the subgroup of all elements of N which induce the identity on G/H.

Lemma 3.7.4 *We have $\operatorname{diag}(M) \subset N$.*

Proof. Consider any element $u \in M$. Then $\operatorname{diag}(u) = (u, u)$ normalizes $H \times H$ by Lemma 3.7.3, and it evidently centralizes σ. Moreover, since u acts trivially on G/H, the conjugate $(u, u)(a_s, a_r)(u, u)^{-1} = (ua_su^{-1}, ua_ru^{-1})$ lies in $Ha_s \times Ha_r = (H \times H) \cdot (a_s, a_r)$ and hence in G. By Lemma 3.7.2 (c) the element (u, u) therefore conjugates G into itself and thus lies in N, as desired. $\qquad\square$

Lemma 3.7.5 *We have $N \cap (1 \times W) = 1 \times H^+$.*

Proof. We take any element $v \in W$ and ask under which conditions $(1, v)$ normalizes G.

First the conjugate $(1, v)\sigma(1, v)^{-1} = \sigma(v, v^{-1})$ must lie in G. This is equivalent to $(v, v^{-1}) \in G$, and hence by Lemma 3.2.8 to $v \in K$. By the definition (3.2.5) of K this means that $v \in H \cdot (a_sa_r)^\lambda$ for some $\lambda \in \mathbb{Z}_2$. Granting this, we in particular have $v \in G$; hence $(1, v)$ normalizes $H \times H$. We also have

$$va_rv^{-1} \in H \cdot (a_sa_r)^\lambda a_r(a_sa_r)^{-\lambda} = H \cdot a_r(a_sa_r)^{-2\lambda}$$

and hence

$$(1, v)(a_s, a_r)(1, v)^{-1} = (a_s, va_rv^{-1}) \in (1 \times H) \cdot (a_s, a_r) \cdot \left(1, (a_sa_r)^{-2\lambda}\right).$$

By Lemma 3.7.2 (c) the last condition is that this conjugate lies in G, which therefore means that $\left(1, (a_sa_r)^{-2\lambda}\right)$ lies in G. By Lemma 3.7.2 this is equivalent to $(a_sa_r)^{-2\lambda} = 1$ and hence to $2\lambda \equiv 0 \bmod 4$. Thus λ must be even, and so $(1, v)$ normalizes G if and only if $v \in H \cdot \langle (a_sa_r)^2 \rangle = H^+$, as desired. $\qquad\square$

Lemma 3.7.6 *We have $N = G \cdot \langle (1, (a_s a_r)^2) \rangle \cdot \mathrm{diag}(M)$.*

Proof. By Lemma 3.7.4 we have $\mathrm{diag}(M) \subset N$, and by Lemma 3.7.5 we in particular have $\langle (1, (a_s a_r)^2) \rangle \subset N$. Together this implies the inclusion "$\supset$".

To prove the inclusion "$\subset$" consider an arbitrary element $w \in N$. Write it in the form $w = \sigma^\lambda (u, v)$ for some $\lambda \in \{0, 1\}$ and $u, v \in W$. Then (u, v) normalizes G and hence $G^1 = G \cap (W \times W)$, and so Proposition 3.2.2 shows that u normalizes $\mathrm{pr}_1(G^1) = G$. Thus u lies in N.

By Lemma 3.7.3 the element u therefore induces an inner automorphism on the dihedral group G/H. Choose $\mu, \nu \in \{0, 1\}$ such that $a_s^\mu a_r^\nu$ induces the same inner automorphism on G/H. Then $(a_s, a_r)^\mu (a_r, a_s)^\nu$ lies in G, and so we can write $w = \sigma^\lambda (a_s, a_r)^\mu (a_r, a_s)^\nu w'$ for another element $w' = (u', v') \in N$, where now u' induces the trivial automorphism on G/H. By the definition of M this means that $u' \in M$.

By Lemma 3.7.4 we therefore have $(u', u') \in N$, and so $w' = w'' (u', u')$ for some element $w'' \in N \cap (1 \times W)$. By Lemma 3.7.5 this means that $w'' \in 1 \times H^+ = 1 \times (H \cdot \langle (a_s a_r)^2 \rangle)$. Altogether we therefore have

$$
\begin{aligned}
w \;\in\; & G \cdot \big(1 \times (H \cdot \langle (a_s a_r)^2 \rangle)\big) \cdot \mathrm{diag}(M) \\
=\; & G \cdot (1 \times H) \cdot \langle (1, (a_s a_r)^2) \rangle \cdot \mathrm{diag}(M) \\
=\; & G \cdot \langle (1, (a_s a_r)^2) \rangle \cdot \mathrm{diag}(M),
\end{aligned}
$$

as desired. $\qquad\square$

Lemma 3.7.7 *We have $\mathrm{diag}(H^+) \subset H^+$.*

Proof. Since $(a_s a_r)^2 = (a_r a_s)^2$, we have

$$
\begin{aligned}
\mathrm{diag}(H^+) \;=\; \mathrm{diag}\big(H \cdot \langle (a_s a_r)^2 \rangle\big) \;=\; & \mathrm{diag}(H) \cdot \langle ((a_s a_r)^2, (a_r a_s)^2) \rangle \\
=\; & \mathrm{diag}(H) \cdot \langle ((a_s, a_r)(a_r, a_s))^2 \rangle \;\subset\; G.
\end{aligned}
$$

On the other hand, both sgn_s and sgn_r are trivial on all elements of the form (u, u). Thus Lemma 3.7.2 (d) implies that $\mathrm{diag}(H^+) \subset H^+$, as desired. $\qquad\square$

Lemma 3.7.8 *We have $\langle (1, (a_s a_r)^2) \rangle \subset M$.*

Proof. From Lemma 3.7.6 we already know that $(1, (a_s a_r)^2)$ normalizes G. By Lemma 3.7.3 it therefore normalizes H, and it remains to show that conjugation by it induces the identity on G/H. For this it suffices to show that the commutators $[(1, (a_s a_r)^2), a_s]$ and $[(1, (a_s a_r)^2), a_r]$ lie in H. Since $r \geqslant 3 > 2 = s + 1$ and therefore $a_r = (a_{r-1}, 1)$, the second commutator is trivial. Since $a_s = a_1 = \sigma$, the first commutator is

$$
\big((a_1 a_r)^{-2}, (a_1 a_r)^2\big) \;=\; \big((a_r a_1)^2, (a_1 a_r)^2\big) \;=\; \big((a_r, a_1)(a_1, a_r)\big)^2 \;=\; \big(\sigma\, a_2\, \sigma^{-1}\, a_2\big)^2.
$$

As a_2 and $\sigma\, a_2\, \sigma^{-1}$ lie in H by the definition of H, it follows that this commutator lies in H, as desired. $\qquad\square$

Lemma 3.7.9 *We have* $\operatorname{diag}(M) \subset M$.

Proof. Consider any element $u \in M$. From Lemma 3.7.4 we already know that (u, u) normalizes G. By Lemma 3.7.3 it therefore normalizes H, and it remains to show that conjugation by it induces the identity on G/H. For this we must show that the commutators $[(u, u), a_s]$ and $[(u, u), a_r]$ lie in H.

Since $s = 1$, we have $a_s = a_1 = \sigma$, and the first commutator is trivial. Since $r > s + 1$, the second commutator is equal to $[(u, u), (a_{r-1}, 1)] = ([u, a_{r-1}], 1)$. From Lemma 3.7.3 we know that (u, u) induces an inner automorphism on G/H. Thus the commutator already lies in $H \cdot \langle (a_s a_r)^2 \rangle$. As $(a_s a_r)^2 = (\sigma(a_{r-1}, 1))^2 = (a_{r-1}, a_{r-1})$, which is of order 2, we therefore have

$$(3.7.10) \qquad ([u, a_{r-1}], 1) \in H \cdot (a_{r-1}, a_{r-1})^\lambda \qquad \text{for some } \lambda \in \{0, 1\}.$$

Now recall that H is the closure of the subgroup generated by all G-conjugates of a_i for all $i \neq s, r$, in other words for all $2 \leqslant i \leqslant r - 1$. Here $a_i = (a_{i-1}, 1)$ for $i > 2$ and $a_2 = (a_1, a_r)$. Thus all generators have the form $(x, y) \in W \times W$ with $\operatorname{sgn}_{r-1}(x) = \operatorname{sgn}_{r-1}(y) = 1$, and so all elements of H have the same property. Since the element $([u, a_{r-1}], 1)$ does so, too, the relation (3.7.10) implies that $(a_{r-1}, a_{r-1})^\lambda$ does as well, and hence that $\lambda = 0$. Thus the commutator lies in H, as desired. $\qquad \square$

Now we recursively define elements

$$(3.7.11) \qquad \left\{ \begin{array}{ll} w_1 & := (1, (a_s a_r)^2), \\ w_{i+1} := (w_i, w_i) & \text{for all } i \geqslant 1. \end{array} \right\}$$

Since $w_1 \in M$ by Lemma 3.7.8, by induction Lemma 3.7.9 implies that $w_i \in M$ for all $i \geqslant 1$. Also, since $(a_s a_r)^2$ has order two, so does w_1, and by induction the same follows for all w_i. Moreover, by induction we find that the restriction $w_i|_{T_n}$ is trivial for all $i \geqslant n$; hence the sequence $w_1, w_2, \ldots$ converges to 1 within N. Thus the following map is well-defined:

$$(3.7.12) \qquad \varphi \colon \prod_{i=1}^{\infty} \mathbb{F}_2 \longrightarrow M, \quad (k_1, k_2, \ldots) \mapsto w_1^{k_1} w_2^{k_2} \cdots .$$

By construction it is continuous, but not a homomorphism. Note that it satisfies the basic formula

$$(3.7.13) \qquad \varphi(k_1, k_2, \ldots) = w_1^{k_1} \cdot \operatorname{diag}(\varphi(k_2, k_3, \ldots)).$$

Lemma 3.7.14 *The map* φ *induces a homomorphism* $\bar{\varphi} \colon \prod_{i=1}^{\infty} \mathbb{F}_2 \to N/G$.

Proof. It suffices to show that for all $1 \leqslant i < j$ the images of w_i and w_j in N/G commute with each other; in other words that the commutator $[w_i, w_j]$ lies in G. We will prove this by induction on i. If $i = 1$, we have

$$[w_1, w_j] = \big[(1, (a_s a_r)^2), (w_{j-1}, w_{j-1}) \big] = \big(1, [(a_s a_r)^2, w_{j-1}] \big).$$

Since $(a_s a_r)^2 \in G$ and $w_{j-1} \in M$, the commutator $[(a_s a_r)^2, w_{j-1}]$ lies in H, and so $[w_1, w_j]$ lies in $1 \times H \subset G$, as desired. For $i > 1$ we have $[w_i, w_j] = \mathrm{diag}([w_{i-1}, w_{j-1}])$, and by the induction hypothesis we already know that $[w_{i-1}, w_{j-1}] \in G$. But being a commutator, it also lies in the kernel of both sgn_s and sgn_r; hence we have $[w_{i-1}, w_{j-1}] \in H^+$ by Lemma 3.7.2 (d). Thus Lemma 3.7.7 implies that $[w_i, w_j] \in H^+ \subset G$, as desired. $\qquad\square$

Lemma 3.7.15 *The homomorphism $\bar\varphi$ is injective.*

Proof. Let $(k_1, k_2, \ldots)$ be an element of the kernel of $\bar\varphi$. Then $w := \varphi(k_1, k_2, \ldots)$ lies in G. We first prove that $k_1 = 0$.

Suppose to the contrary that $k_1 = 1$. Then the definition of φ implies that $w = w_1 \cdot \mathrm{diag}(u)$ for some element $u \in M$. Thus $w = (u, (a_s a_r)^2 u)$ actually lies in G^1. By Proposition 3.2.4 (c) and Lemma 3.7.2 there therefore exist $\lambda \in \mathbb{Z}$ and $\mu \in \{0, 1\}$ such that

$$(u, (a_s a_r)^2 u) \quad \in \quad (H \times H) \cdot (a_s a_r, a_r a_s)^\lambda \cdot (a_s, a_r)^\mu$$

$$\Longleftrightarrow \qquad \left\{ \begin{array}{l} u \quad \in \quad H(a_s a_r)^\lambda a_s^\mu \quad \text{and} \\ (a_s a_r)^2 u \in \quad H(a_r a_s)^\lambda a_r^\mu \end{array} \right\}$$

$$\Longleftrightarrow \qquad u \quad \in \quad H(a_s a_r)^\lambda a_s^\mu \cap (a_s a_r)^{-2} H(a_r a_s)^\lambda a_r^\mu.$$

In particular $u \in G$ and therefore $u \in G \cap M = H^+ = H \rtimes \langle (a_s a_r)^2 \rangle$. Therefore $\mu = 0$ and λ is even, and $H(a_s a_r)^\lambda = (a_s a_r)^{-2} H(a_r a_s)^\lambda$. But this contradicts the fact that $(a_s a_r)^2 = (a_r a_s)^2 \notin H$. We have thus reached a contradiction and thereby proved that $k_1 = 0$.

Since $k_1 = 0$, the formula (3.7.13) shows that $w = \mathrm{diag}(w')$ for $w' := \varphi(k_2, k_3, \ldots) \in M$. Thus $w = (w', w') \in G$ actually lies in G^1, and so w' lies in G by Proposition 3.2.2 (c). This means that $(k_2, k_3, \ldots)$ also lies in the kernel of $\bar\varphi$.

For every element $(k_1, k_2, \ldots)$ of the kernel of $\bar\varphi$ we have thus proved that $k_1 = 0$ and that $(k_2, k_3, \ldots)$ again lies in the kernel of $\bar\varphi$. By an induction on i we can deduce from this that for every $i \geqslant 1$ and every element $(k_1, k_2, \ldots)$ of the kernel of $\bar\varphi$ we have $k_i = 0$. This means that the kernel of $\bar\varphi$ is trivial, and so the homomorphism $\bar\varphi$ is injective, as desired. $\qquad\square$

Lemma 3.7.16 *The homomorphism $\bar\varphi$ is surjective.*

Proof. We must prove that $N = G \cdot \varphi\big(\prod_{i=1}^\infty \mathbb{F}_2\big)$. For this it suffices to show the equality $N_n = G_n \cdot \varphi\big(\prod_{i=1}^\infty \mathbb{F}_2\big)|_{T_n}$ for all $n \geqslant 0$, which we will achieve by induction on n. If $n \leqslant r$, Proposition 3.1.2 implies that $G_n = N_n$, from which the equality follows. Thus we may assume that $n > r$ and that $N_{n-1} = G_{n-1} \cdot \varphi\big(\prod_{i=1}^\infty \mathbb{F}_2\big)|_{T_{n-1}}$.

Since $\varphi\big(\prod_{i=1}^\infty \mathbb{F}_2\big) \subset M$ by construction, the induction hypothesis implies that $M_{n-1} = (G_{n-1} \cap M_{n-1}) \cdot \varphi\big(\prod_{i=1}^\infty \mathbb{F}_2\big)|_{T_{n-1}}$. We claim that $G_{n-1} \cap M_{n-1} = H_{n-1}^+$ and consequently

$$(3.7.17) \qquad\qquad M_{n-1} = H_{n-1}^+ \cdot \varphi\big(\prod_{i=1}^\infty \mathbb{F}_2\big)|_{T_{n-1}}.$$

To show the claim observe that under the given assumptions on s, r, n, Proposition 3.2.16 implies that $G_{n-1} = H_{n-1} \rtimes \langle a_s|_{T_{n-1}}, a_r|_{T_{n-1}} \rangle$ and that restriction to T_{n-1} induces an isomorphism $\langle a_s, a_r \rangle \xrightarrow{\sim} \langle a_s|_{T_{n-1}}, a_r|_{T_{n-1}} \rangle$. Thus the restriction induces an isomorphism $G/H \xrightarrow{\sim} G_{n-1}/H_{n-1}$. It follows that M is the subgroup of all elements of N which induce the identity on G_{n-1}/H_{n-1}. Consequently $G_{n-1} \cap M_{n-1}$ is the subgroup of all elements of G_{n-1} which induce the identity on G_{n-1}/H_{n-1}, which by the same semidirect product decomposition is $H_{n-1}^+ = H_{n-1} \rtimes \langle (a_s a_r)^2|_{T_{n-1}} \rangle$. Thus $G_{n-1} \cap M_{n-1} = H_{n-1}^+$, as claimed.

Now we can perform the induction step. Using, in turn, Lemma 3.7.6, the equality (3.7.17), Lemma 3.7.7, and the formula (3.7.13) we deduce that

$$
\begin{aligned}
N_n &= G_n \cdot \langle w_1|_{T_n} \rangle \cdot \mathrm{diag}(M_{n-1}) \\
&= G_n \cdot \langle w_1|_{T_n} \rangle \cdot \mathrm{diag}\big(H_{n-1}^+ \cdot \varphi\big(\textstyle\prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}}\big) \\
&= G_n \cdot \langle w_1|_{T_n} \rangle \cdot \mathrm{diag}\big(\varphi\big(\textstyle\prod_{i=1}^{\infty} \mathbb{F}_2\big)\big)|_{T_n} \\
&= G_n \cdot \varphi\big(\textstyle\prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_n},
\end{aligned}
$$

so the desired equality holds for n, and we are done. $\qquad\square$

Combining Lemmas 3.7.14 through 3.7.16 now implies:

Theorem 3.7.18 *In the case (3.7.1) the map φ induces an isomorphism*

$$
\bar{\varphi} \colon \prod_{i=1}^{\infty} \mathbb{F}_2 \xrightarrow{\sim} N/G.
$$

3.8 Normalizer, subcase (c)

Throughout this subsection we assume:

(3.8.1) $$s = 2 \quad \text{and} \quad r = 3.$$

Thus we have $G = \langle\!\langle a_1, a_2, a_3 \rangle\!\rangle$ with $a_1 = \sigma$ and $a_2 = (a_1, 1)$ and $a_3 = (a_2, a_3)$, and the definitions (3.2.3) and (3.2.9) of H and L imply that $H = L$. Surprisingly, the determination of the normalizer requires more work in this case than in any of the other cases. Perhaps it is a kind of mixture of the cases in the two preceding subsections.

Lemma 3.8.2 *In this case we have:*

(a) $\langle a_s, a_r \rangle$ *is a finite dihedral group of order 8 with center $\langle (a_s a_r)^2 \rangle$.*

(b) $G = H \rtimes \langle a_s, a_r \rangle$.

(c) $G = (H \times H) \rtimes \langle \sigma, (a_s, a_r) \rangle$.

(d) $H^+ := H \rtimes \langle (a_s a_r)^2 \rangle = \mathrm{Ker}(\mathrm{sgn}_s|_G) \cap \mathrm{Ker}(\mathrm{sgn}_r|_G)$.

Proof. Same as that of Lemma 3.7.2. $\qquad\square$

Lemma 3.8.3 *The group N normalizes H and induces only inner automorphisms on G/H.*

Proof. By definition H is the closure of the subgroup of G generated by all G-conjugates of a_1. By Proposition 3.4.4 these generators are precisely the W-conjugates of a_1 which lie in G. The set of these is therefore preserved under conjugation by N, and hence H is normalized by N. The rest of the proof proceeds as that of Lemma 3.7.3. $\qquad\square$

Let M denote the subgroup of all elements of N which induce the identity on G/H. The same proofs as those of Lemmas 3.7.4 through 3.7.7 yield the next four lemmas:

Lemma 3.8.4 *We have $\mathrm{diag}(M) \subset N$.*

Lemma 3.8.5 *We have $N \cap (1 \times W) = 1 \times H^+$.*

Lemma 3.8.6 *We have $N = G \cdot \langle (1, (a_s a_r)^2) \rangle \cdot \mathrm{diag}(M)$.*

Lemma 3.8.7 *We have $\mathrm{diag}(H^+) \subset H^+$.*

At this point things begin to differ with respect to Subsection 3.7. First we recall the relation between the subgroups $H_n \subset H_n^+ \subset G_n$ which, as usual, denote the images of $H \subset H^+ \subset G$ in W_n.

Lemma 3.8.8 *For all $n \geqslant 4$ we have:*

(a) $G_n = H_n \rtimes \langle a_s|_{T_n}, a_r|_{T_n} \rangle$ with $\langle a_s|_{T_n}, a_r|_{T_n} \rangle \cong \langle a_s, a_r \rangle \cong G/H$ dihedral of order 8.

(b) $H_n^+ = H_n \rtimes \langle (a_s a_r)^2|_{T_n} \rangle$ with $\langle (a_s a_r)^2|_{T_n} \rangle \cong \langle (a_s a_r)^2 \rangle$ cyclic of order 2.

(c) But $(a_s a_r)^2|_{T_3} \in H_3$.

Proof. Since $(a_s a_r)^2$ has order 2, so does its restriction $(a_s a_r)^2|_{T_n}$ for all $n \geqslant 4$ by Proposition 3.2.14. Using this, Lemma 3.8.2 implies both (a) and (b). Assertion (c) is part of Proposition 3.2.14. $\qquad\square$

Lemma 3.8.9 *We have $\langle (1, (a_s a_r)^2) \rangle \subset M$.*

Proof. From Lemma 3.8.6 we already know that $(1, (a_s a_r)^2)$ normalizes G. By Lemma 3.8.3 it therefore normalizes H, and it remains to show that conjugation by it induces the identity on G/H. For this it suffices to show that the commutators $[(1, (a_s a_r)^2), a_s]$ and $[(1, (a_s a_r)^2), a_r]$ lie in H. Since $a_s = a_2 = (a_1, 1)$ in this case, the first commutator is trivial. Since $a_r = a_3 = (a_s, a_r)$, and $(a_s a_r)^2$ commutes with a_r by Lemma 3.8.2 (a), the second commutator is trivial as well, and we are done. $\qquad\square$

Lemma 3.8.10 *For any $u \in M$ with $u|_{T_3} = 1$ we have $\mathrm{diag}(u) \in M$.*

Proof. From Lemma 3.8.4 we already know that (u, u) normalizes G. By Lemma 3.8.3 it therefore normalizes H. On the other hand the assumption implies that $(u, u)|_{T_4} = 1$; hence conjugation by it induces the identity on G_4/H_4. Thus Lemma 3.8.8 (a) implies that conjugation by (u, u) induces the identity on G/H; hence $(u, u) \in M$, as desired. $\qquad\square$

As in Subsection 3.7 we recursively define elements

$$(3.8.11) \qquad \left\{ \begin{array}{ll} w_1 & := (1, (a_s a_r)^2), \\ w_{i+1} := (w_i, w_i) & \text{for all } i \geqslant 1. \end{array} \right\}$$

Lemma 3.8.12 *(a) For all $i \geqslant 1$ we have $w_i \in M$.*

(b) For all $i \geqslant 1$ we have $w_i|_{T_4} \in G_4$.

Proof. First observe that $(a_1 a_2)^2|_{T_1} = 1$ because it is a square. Therefore $(a_2 a_3)^2|_{T_2} = ((a_1, 1)(a_2, a_3))^2|_{T_2} = ((a_1 a_2)^2, 1)|_{T_2} = 1$, and hence $w_1|_{T_3} = 1$. By induction on i it follows that $w_i|_{T_3} = 1$ for all $i \geqslant 1$ and that $w_i|_{T_4} = 1$ for all $i \geqslant 2$.

Since $w_1 \in M$ by Lemma 3.8.9, by induction Lemma 3.8.10 now implies that $w_i \in M$ for all $i \geqslant 1$, proving (a). Also, from Lemma 3.8.8 (c) we deduce that $w_1|_{T_4} = (1, (a_s a_r)^2|_{T_3})$ lies in $1 \times H_3$, and hence in G_4 by Lemma 3.8.2 (c). For $i \geqslant 2$ the element $w_i|_{T_4} = 1$ trivially lies in G_4. This proves (b). $\qquad\square$

To describe N we will need one more element $w_0 \in W$, defined by the recursion relation

$$(3.8.13) \qquad\qquad w_0 = (a_2 w_0, a_3 w_0) = a_3 (w_0, w_0).$$

Lemma 3.8.14 *We have $[w_0, a_2] = [[a_3, a_1], a_2] \in H$.*

Proof. The fact that (w_0, w_0) commutes with $a_1 = \sigma$ implies that

$$[a_2 w_0, a_1] = [a_2 a_3 (w_0, w_0), \sigma] = [a_2 a_3, a_1].$$

From this we deduce that

$$[w_0, a_2] = [(a_2 w_0, a_3 w_0), (a_1, 1)] = ([a_2 w_0, a_1], 1) = ([a_2 a_3, a_1], 1) = [(a_2 a_3, a_3 a_2), (a_1, 1)].$$

Since

$$(a_2 a_3, a_3 a_2) = (a_2, a_3)(a_3, a_2)^{-1} = [(a_2, a_3), \sigma] = [a_3, a_1],$$

it follows that $[w_0, a_2] = [[a_3, a_1], a_2]$. But by definition a_1 lies in H, and H is a normal subgroup of G; hence $[[a_3, a_1], a_2] \in H$, as desired. $\qquad\square$

Lemma 3.8.15 *We have $[w_0, a_3] \in H$.*

64

Proof. Set $x := [w_0, a_3]$. Then

$$x = [(a_2 w_0, a_3 w_0), (a_2, a_3)] = ([a_2 w_0, a_2], [a_3 w_0, a_3]) = (a_2[w_0, a_2]a_2^{-1}, a_3[w_0, a_3]a_3^{-1}),$$

which using Lemma 3.8.14 implies that

$$(3.8.16) \qquad\qquad x = \big(a_2[[a_3, a_1], a_2]a_2^{-1}, a_3 x a_3^{-1}\big).$$

This recursion relation determines x uniquely and independently of w_0. Thus we must show that the element $x \in W$ characterized by (3.8.16) lies in H. We will show by induction that $x|_{T_n}$ lies in H_n for all $n \geqslant 0$.

As a preparation for this we calculate

$$[a_1 a_3 a_1^{-1}, a_2] = \big[\sigma(a_2, a_3)\sigma^{-1}, (a_1, 1)\big] = [(a_3, a_2), (a_1, 1)] = ([a_3, a_1], 1),$$

whence

$$
\begin{aligned}
a_3[[a_1 a_3 a_1^{-1}, a_2], a_3]a_3^{-1} &= (a_2, a_3)\big[([a_3, a_1], 1), (a_2, a_3)\big](a_2, a_3)^{-1} \\
&= (a_2, a_3)\big([[a_3, a_1], a_2], 1\big)(a_2, a_3)^{-1} \\
&= \big(a_2[[a_3, a_1], a_2]a_2^{-1}, 1\big).
\end{aligned}
$$

Now observe that, since $a_3|_{T_2} = 1$, we also have $(a_2[[a_3, a_1], a_2]a_2^{-1})|_{T_2} = 1$, and hence $x|_{T_3} = 1$. This and the above calculation together imply that

$$x|_{T_4} = \big(a_2[[a_3, a_1], a_2]a_2^{-1}), 1\big)|_{T_4} = \big(a_3[[a_1 a_3 a_1^{-1}, a_2], a_3]a_3^{-1}\big)|_{T_4}.$$

But $[a_1 a_3 a_1^{-1}, a_2]$ lies in the commutator group of G and hence in H^+. Since H^+/H is the center of G/H, we have $[H^+, G] \subset H$, and therefore $a_3[[a_1 a_3 a_1^{-1}, a_2], a_3]a_3^{-1}$ lies in H. Together this shows that $x|_{T_4}$ lies in H_4.

To finish the proof by induction, assume that $n > 4$ and that $x|_{T_{n-1}}$ lies in H_{n-1}. Then

$$x|_{T_n} = \big((a_2[[a_3, a_1], a_2]a_2^{-1})|_{T_{n-1}}, (a_3 x a_3^{-1})|_{T_{n-1}}\big),$$

where the first entry lies in H_{n-1} by Lemma 3.8.14, and the second entry lies in H_{n-1} by the induction hypothesis. Thus $x|_{T_n}$ lies in $H_{n-1} \times H_{n-1}$ and hence in G_n. On the other hand, Lemma 3.8.8 (a) implies that the restriction to T_4 induces an isomorphism $G_n/H_n \xrightarrow{\sim} G_4/H_4$, and we already know that $x|_{T_4}$ lies in H_4. Together this implies that $x|_{T_n}$ lies in H_n, as desired. $\qquad \square$

Lemma 3.8.17 *We have $w_0 \in M$.*

Proof. Lemmas 3.8.14 and 3.8.15 already imply that $w_0 a_2 w_0^{-1}$ and $w_0 a_3 w_0^{-1}$ lie in G. Moreover, the definition (3.8.13) of w_0 shows that

$$w_0 a_1 w_0^{-1} = (a_2 w_0, a_3 w_0)\sigma(a_2 w_0, a_3 w_0)^{-1} = (a_2, a_3)\sigma(a_2, a_3)^{-1} = a_3 a_1 a_3^{-1} \in G.$$

Since $G = \langle\!\langle a_1, a_2, a_3 \rangle\!\rangle$, it follows that $w_0 G w_0^{-1} \subset G$ and hence $w_0 G w_0^{-1} = G$. Thus w_0 lies in N. From Lemmas 3.8.14 and 3.8.15 it now follows that w_0 lies in M. $\qquad \square$

Lemma 3.8.18 *We have $w_0^2 \in G$.*

Proof. It suffices to show that $w_0^2|_{T_n}$ lies in G_n for all $n \geqslant 0$. For $n \leqslant 3$ this follows from the fact that $G_n = W_n$. So assume that $n > 3$ and that $w_0^2|_{T_{n-1}}$ lies in G_{n-1}. Since $w_0^2|_{T_{n-1}}$ is a square, it lies in the kernel of sgn_2 and sgn_3, and therefore already in H_{n-1}^+. By Lemma 3.8.7 this implies that $(w_0^2, w_0^2)|_{T_n}$ lies in $H_n^+ \subset G_n$. But by the construction (3.8.13) of w_0 we have

$$w_0^2 \;=\; \left(a_2 w_0 a_2 w_0, a_3 w_0 a_3 w_0\right) \;=\; \left(a_2[w_0, a_2]a_2^{-1}w_0^2, a_3[w_0, a_3]a_3^{-1}w_0^2\right).$$

Since $[w_0, a_2]$ and $[w_0, a_3]$ lie in H by Lemmas 3.8.14 and 3.8.15, it follows that $w_0^2 \in (H \times H) \cdot (w_0^2, w_0^2) \subset G \cdot (w_0^2, w_0^2)$. Therefore $w_0^2|_{T_n} \in G_n \cdot (w_0^2, w_0^2)|_{T_n} = G_n$, as desired. $\qquad \square$

Lemma 3.8.19 *We have $[w_0, w_i] \in G$ for all $i \geqslant 1$.*

Proof. The constructions (3.8.11) and (3.8.13) of w_0 and w_1 imply that

$$[w_0, w_1] = \left[(a_2 w_0, a_3 w_0), (1, (a_2 a_3)^2)\right] = \left(1, [a_3 w_0, (a_2 a_3)^2]\right).$$

Since w_0 lies in M, conjugation by it fixes the image of $(a_2 a_3)^2$ in G/H. Since a_3 commutes with $(a_2 a_3)^2$, it follows that conjugation by $a_3 w_0$ also fixes the image of $(a_2 a_3)^2$ in G/H. Therefore $[a_3 w_0, (a_2 a_3)^2]$ lies in H, and hence $[w_0, w_1]$ lies in $1 \times H \subset G$. This proves the desired assertion for $i = 1$.

Assume that $i > 1$ and that $[w_0, w_{i-1}]$ lies in G. Being a commutator, this element lies in the kernel of sgn_2 and sgn_3, and therefore already in H^+. By Lemma 3.8.7 this implies that $[(w_0, w_0), w_i] = ([w_0, w_{i-1}], [w_0, w_{i-1}])$ lies in $H^+ \subset G$. Since a_3 lies in G, and G is normalized by w_0 and w_i, it follows that $[w_0, w_i] = [a_3(w_0, w_0), w_i]$ lies in G as well. Thus the lemma follows for all $i \geqslant 1$ by induction on i. $\qquad \square$

Lemma 3.8.20 *We have $N_4 = G_4 \cdot \langle w_0|_{T_4} \rangle$ and $[N_4 : G_4] = 2$.*

Proof. The defining relation $w_0 = (a_2 w_0, a_3 w_0)$ recursively implies that

$$
\begin{aligned}
\operatorname{sgn}_1(w_0) &= 1, \\
\operatorname{sgn}_2(w_0) &= \operatorname{sgn}_1(a_2 w_0) \cdot \operatorname{sgn}_1(a_3 w_0) = 1, \quad \text{and} \\
\operatorname{sgn}_3(w_0) &= \operatorname{sgn}_2(a_2 w_0) \cdot \operatorname{sgn}_2(a_3 w_0) = -1.
\end{aligned}
$$

Thus the image of the residue class of $w_0|_{T_4}$ under the isomorphism from Lemma 3.2.15 (b) is the matrix

$$\begin{pmatrix} \operatorname{sgn}_2(a_2 w_0) & \operatorname{sgn}_2(a_3 w_0) \\ \operatorname{sgn}_3(a_2 w_0) & \operatorname{sgn}_3(a_3 w_0) \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}.$$

By Lemma 3.2.15 (c) this does not lie in the image of G_4; hence $w_0|_{T_4} \notin G_4$. Also, since N normalizes G, its restriction N_4 normalizes G_4; and hence Lemma 3.2.15 (d) implies that

$[N_4 : G_4] \leqslant 2$. Since we already have $w_0|_{T_4} \in N_4$ by Lemma 3.8.17, this leaves only the possibility $[N_4 : G_4] = 2$ with $N_4 = G_4 \cdot \langle w_0|_{T_4} \rangle$, as desired. $\qquad\square$

Now we can put everything together. Lemmas 3.8.12 (a) and 3.8.17 imply that $w_i \in M$ for all $i \geqslant 0$. By induction on i we find that the restriction $w_i|_{T_n}$ is trivial for all $i \geqslant n$; hence the sequence $w_0, w_1, w_2, \ldots$ converges to 1 within M. Moreover, although in fact $w_0^2 \neq 1$, let us by abuse of notation for all $i \geqslant 0$ and $k \in \mathbb{F}_2$ define

$$w_i^k := \begin{cases} 1 & \text{if } k = 0 \text{ in } \mathbb{F}_2, \\ w_i & \text{if } k = 1 \text{ in } \mathbb{F}_2. \end{cases}$$

Then the following map is well-defined:

$$(3.8.21) \qquad \varphi \colon \prod_{i=0}^{\infty} \mathbb{F}_2 \longrightarrow M, \quad (k_0, k_1, k_2, \ldots) \mapsto w_0^{k_0} w_1^{k_1} w_2^{k_2} \cdots.$$

By construction it is continuous, but not a homomorphism. By the construction (3.8.11) of $w_1, w_2, \ldots$ it satisfies the basic formula

$$(3.8.22) \quad \varphi(k_0, k_1, k_2, \ldots) \;=\; w_0^{k_0} \cdot \varphi(0, k_1, k_2, \ldots) \;=\; w_0^{k_0} \cdot w_1^{k_1} \cdot \operatorname{diag}(\varphi(0, k_2, k_3, \ldots)).$$

Lemma 3.8.23 *The map φ induces a homomorphism $\bar{\varphi} \colon \prod_{i=0}^{\infty} \mathbb{F}_2 \to N/G$.*

Proof. It suffices to show that the images of all w_i in N/G have order dividing 2 and commute with each other; in other words that w_i^2 and $[w_i, w_j]$ lie in G for all $i, j \geqslant 0$. Since $(a_s a_r)^2$ has order 2, the construction (3.8.11) implies that $w_1^2 = 1$ and hence $w_i^2 = 1$ for all $i \geqslant 1$. Also, the same proof as that of Lemma 3.7.14 shows that $[w_i, w_j] \in G$ for all $i, j \geqslant 1$. On the other hand, by Lemmas 3.8.18 and 3.8.19 the elements w_0^2 and $[w_0, w_i]$ lie in G for all $i \geqslant 1$. Thus all cases are covered. $\qquad\square$

Lemma 3.8.24 *The homomorphism $\bar{\varphi}$ is injective.*

Proof. Let $(k_0, k_1, k_2, \ldots)$ be an element of the kernel of $\bar{\varphi}$. Then $w := \varphi(k_0, k_1, k_2, \ldots)$ lies in G. In particular $w|_{T_4}$ lies in G_4. But by Lemma 3.8.12 (b), the definition of φ implies that $w|_{T_4} = w_0^{k_0}|_{T_4}$. Since $w_0|_{T_4} \notin G_4$ by Lemma 3.8.20, it follows that $k_0 = 0$. The same arguments as in the proof of Lemma 3.7.16 now show that $k_1 = 0$ and that $(0, k_2, k_3, \ldots)$ also lies in the kernel of $\bar{\varphi}$. By an induction on i we can deduce from this that for every $i \geqslant 0$ and every element $(k_0, k_1, k_2, \ldots)$ of the kernel of $\bar{\varphi}$ we have $k_i = 0$. This means that the kernel of $\bar{\varphi}$ is trivial, and so the homomorphism $\bar{\varphi}$ is injective, as desired. $\qquad\square$

Lemma 3.8.25 *The homomorphism $\bar{\varphi}$ is surjective.*

Proof. We must prove that $N = G \cdot \varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big)$. For this it suffices to show the equality $N_n = G_n \cdot \varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big)|_{T_n}$ for all $n \geqslant 0$. For $n \leqslant 4$ this follows from Lemma 3.8.20. So assume that $n > 4$ and that $N_{n-1} = G_{n-1} \cdot \varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}}$.

Since $n - 1 \geqslant 4$, the same argument as in the proof of Lemma 3.7.15 with Lemma 3.8.8 in place of Proposition 3.2.16 shows that $G_{n-1} \cap M_{n-1} = H_{n-1}^+$. As $\varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big) \subset M$ by Lemmas 3.8.12 (a) and 3.8.17, the induction hypothesis implies that

$$(3.8.26) \qquad M_{n-1} \;=\; (G_{n-1} \cap M_{n-1}) \cdot \varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}} \;=\; H_{n-1}^+ \cdot \varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}}.$$

Using Lemma 3.8.6, the equality (3.8.26), the formula (3.8.22), Lemma 3.8.7, the fact that $w_0 = a_3(w_0, w_0)$, and rearranging factors because N_n/G_n is commutative, we deduce that

$$
\begin{aligned}
N_n \;&=\; G_n \cdot \langle w_1|_{T_n} \rangle \cdot \mathrm{diag}(M_{n-1}) \\
&=\; G_n \cdot \langle w_1|_{T_n} \rangle \cdot \mathrm{diag}\big(H_{n-1}^+ \cdot \varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}}\big) \\
&=\; G_n \cdot \langle w_1|_{T_n} \rangle \cdot \mathrm{diag}(H_{n-1}^+) \cdot \{1, (w_0, w_0)|_{T_n}\} \cdot \mathrm{diag}\big(\varphi\big(\{0\} \times \prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_{n-1}}\big) \\
&=\; G_n \cdot \mathrm{diag}(H_{n-1}^+) \cdot \{1, (w_0, w_0)|_{T_n}\} \cdot \langle w_1|_{T_n} \rangle \cdot \varphi\big(\{0\}^2 \times \prod_{i=2}^{\infty} \mathbb{F}_2\big)|_{T_n} \\
&=\; G_n \cdot \{1, w_0|_{T_n}\} \cdot \varphi\big(\{0\} \times \prod_{i=1}^{\infty} \mathbb{F}_2\big)|_{T_n} \\
&=\; G_n \cdot \varphi\big(\prod_{i=0}^{\infty} \mathbb{F}_2\big)|_{T_n},
\end{aligned}
$$

so the desired equality holds for n. By induction it therefore follows for all $n \geqslant 0$, as desired. $\qquad\square$

Combining Lemmas 3.8.23 through 3.8.25 now implies:

Theorem 3.8.27 *In the case (3.8.1) the map φ induces an isomorphism*

$$\bar{\varphi} \colon \prod_{i=0}^{\infty} \mathbb{F}_2 \xrightarrow{\;\sim\;} N/G.$$

3.9 Odometers

In this subsection we study the set of odometers in G, in particular concerning conjugacy. First we show that odometers are abundant in G. By the *proportion* of a measurable subset $X \subset G$ we mean the ratio $\mu(X)/\mu(G)$ for any Haar measure μ on G.

Proposition 3.9.1   *(a) For any W-conjugates b_i of a_i and any permutation ρ of $\{1, \dots, r\}$ the product $b_{\rho 1} \cdots b_{\rho r}$ is an odometer.*

  (b) The set of odometers in G is open and closed in G and has proportion 2^{-r}.

Proof. Same as for Proposition 2.7.1, using Proposition 3.1.1 instead of 2.1.1. $\qquad\square$

In the special case $s = 1$ and $r = 2$ recall that $G = \langle\!\langle a_1 a_2 \rangle\!\rangle \rtimes \langle a_1 \rangle \cong \mathbb{Z}_2 \rtimes \{\pm 1\}$ where $a_1 a_2$ is an odometer. Thus the odometers in G are precisely the elements $(a_1 a_2)^k$ for all $k \in \mathbb{Z}_2^{\times}$, and they are all conjugate to $a_1 a_2$ by an element of $N \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2^{\times}$. This directly implies Theorem 3.9.4 and Proposition 3.9.14 below in this case. For the rest of this subsection we therefore exclude the case $(s, r) = (1, 2)$, except where explicitly mentioned.

Lemma 3.9.2 *Any odometer in G is conjugate under N to an element of $(Ha_s \times \{a_r\})\, \sigma$.*

Proof. Any odometer c in G acts non-trivially on T_1 and is therefore equal to $(x, y)\,\sigma$ for some $(x, y) \in G^1$. Recall from Proposition 3.2.4 (c) that $G^1 = (H \times H) \cdot \langle\!\langle (a_s, a_r), (a_r, a_s) \rangle\!\rangle$. Since $\mathrm{sgn}_s(xy) = \mathrm{sgn}_{s+1}(c) = -1$ and $\mathrm{sgn}_s |H = 1$, it follows that (x, y) is an element of $H \times H$ times an odd number of factors (a_s, a_r) and/or (a_r, a_s). After possibly replacing c by its conjugate under $\sigma = a_1 \in G$, we may without loss of generality assume that the factor (a_s, a_r) occurs an odd number of times and the factor (a_r, a_s) an even number of times. Then $(x, y)\,(a_s, a_r)^{-1}$ is a product of an even number of each kind of factors. Since both a_s and a_r have order two, we deduce that

$$(x, y)\,(a_s, a_r)^{-1} \;=\; \big((a_s, a_r)\,(a_r, a_s)\big)^{2\lambda} \;=\; \big((a_s a_r)^{2\lambda}, (a_r a_s)^{2\lambda}\big) \;=\; (v^\lambda, v^{-\lambda})$$

for some $\lambda \in \mathbb{Z}_2$, where for brevity we write $v := (a_s a_r)^2$. Thus

$$c \;\in\; (H \times H) \cdot (v^\lambda a_s, v^{-\lambda} a_r) \cdot \sigma.$$

Next, if $s \geqslant 2$ and $r \geqslant 4$, then $v = (a_s a_r)^2 \in H$ by Proposition 3.2.12, and so c already lies in $(H \times H) \cdot (a_s, a_r) \cdot \sigma$. Otherwise, the element $(1, v) = (1, (a_s a_r)^2)$ lies in N by Lemma 3.7.6 or 3.8.6, and so we may replace c by its conjugate

$$\begin{aligned}
(1, v^\lambda)\, c\, (1, v^{-\lambda}) \;&\in\; (1, v^\lambda) \cdot (H \times H) \cdot (v^\lambda a_s, v^{-\lambda} a_r) \cdot \sigma \cdot (1, v^{-\lambda}) \\
&=\; (H \times H) \cdot (v^\lambda a_s v^{-\lambda}, a_r) \cdot \sigma \\
&=\; (H \times H) \cdot (v^{2\lambda} a_s, a_r) \cdot \sigma.
\end{aligned}$$

Since in this case $v^2 = (a_s a_r)^4 = 1$ by Lemma 3.7.2 (a) or 3.8.2 (a), we can then drop the term $v^{2\lambda}$. In either case have may thus without loss of generality assume that

$$c \;\in\; (H \times H) \cdot (a_s, a_r) \cdot \sigma.$$

Now write $c = (h' a_s, h a_r)\,\sigma$ with $h', h \in H$. Then $(1, h) \in G$; hence we may replace c by its conjugate

$$(1, h)^{-1}\, (h' a_s, h a_r)\, \sigma\, (1, h) \;=\; (h' a_s h, a_r)\, \sigma.$$

Since $h' a_s h \in H a_s$, the element c then has the required form. $\qquad\square$

Lemma 3.9.3 *For any $u \in N$ we have $(1, [a_r, u]) \in N$.*

Proof. Since u normalizes G, the commutator $[a_r, u]$ lies in G. Being a commutator, all its signs are $+1$. If $s \geqslant 2$ and $r \geqslant 4$, by Lemma 3.6.3 (c) this implies that $[a_r, u] \in H$; hence $(1, [a_r, u])$ lies in $G \subset N$, as desired. Otherwise Lemma 3.7.2 (d) or 3.8.2 (d) implies that $[a_r, u] \in H \cdot \langle\!\langle (a_s a_r)^2 \rangle\!\rangle$, and hence

$$(1, [a_r, u]) \;\in\; (1 \times H) \cdot \langle\!\langle (1, (a_s a_r)^2) \rangle\!\rangle.$$

But in this case $(1, (a_s a_r)^2) \in N$ by Lemma 3.7.6 or 3.8.6, and since $1 \times H \subset G \subset N$, we again deduce that $(1, [a_r, u]) \in N$, as desired. $\qquad\square$

Theorem 3.9.4 *All odometers in G are conjugate under N.*

Proof. (At the beginning of this subsection this was already shown for $(s, r) = (1, 2)$, so the following proof concerns the remaining cases.) By Lemma 1.3.1 it suffices to show that for any $n \geqslant 0$ and any odometers $c, c' \in G$, there exists $w \in N$ with $wcw^{-1}|_{T_n} = c'|_{T_n}$. For $n \leqslant r$ this is a direct consequence of the fact that $G_r = W_r$. So assume that $n > r$ and that the assertion is universally true for $n - 1$ in place of n.

Consider any odometers $c, c' \in G$. By Lemma 3.9.2 we may without loss of generality assume that $c = (ha_s, a_r)\, \sigma$ and $c' = (h'a_s, a_r)\, \sigma$ for some $h, h' \in H$. Then

$$c^2 = (ha_s, a_r)\, \sigma\, (ha_s, a_r)\, \sigma = (ha_s a_r, a_r ha_s) \in G,$$

and so $d := ha_s a_r$ is again an odometer, which lies in G by Proposition 3.2.2. Likewise the element $d' := h'a_s a_r$ is an odometer in G. Thus by the induction hypothesis we can choose an element $u \in N$ with $udu^{-1}|_{T_{n-1}} = d'|_{T_{n-1}}$. For later use observe that we can replace u by ud^λ for any $\lambda \in \mathbb{Z}_2$ without losing the equality. But for the moment we fix u and set $w := (u, a_r u a_r^{-1}) \in W$. Since $c = (da_r^{-1}, a_r)\, \sigma$ and $c' = (d'a_r^{-1}, a_r)\, \sigma$, we find that

$$wcw^{-1} = (u, a_r u a_r^{-1})\, (da_r^{-1}, a_r)\, \sigma\, (u^{-1}, a_r u^{-1} a_r^{-1}) = (udu^{-1}a_r^{-1}, a_r)\, \sigma$$

and deduce that

$$wcw^{-1}|_{T_n} = \left((udu^{-1}a_r^{-1})|_{T_{n-1}}, a_r|_{T_{n-1}}\right)\sigma = \left((d'a_r^{-1})|_{T_{n-1}}, a_r|_{T_{n-1}}\right)\sigma = c'|_{T_n}.$$

It remains to show that we can choose $u \in N$ such that w lies in N. For this observe that

$$w = (u, a_r u a_r^{-1}) = (1, [a_r, u]) \cdot (u, u).$$

By Lemma 3.9.3 the first factor always lies in N, so we must choose u such that $(u, u) \in N$. If $s \geqslant 2$ and $r \geqslant 4$, this already follows from Lemma 3.6.5, and we are done. For the rest of the proof we therefore assume that $s = 1$ or $r = 3$.

Since $n > r$, we have $n - 1 \geqslant r$. Let us postpone the case $(s, r, n) = (2, 3, 4)$ to the end of the proof and exclude it for now. Then Lemma 3.7.2 and Proposition 3.2.16 if $s = 1$, respectively Lemma 3.8.2 and Proposition 3.2.14 if $s = 2$, imply that that $G_{n-1} = H_{n-1} \rtimes \langle a_s|_{T_{n-1}}, a_r|_{T_{n-1}}\rangle$ and that restriction to T_{n-1} induces an isomorphism $\langle a_s, a_r\rangle \xrightarrow{\sim} \langle a_s|_{T_{n-1}}, a_r|_{T_{n-1}}\rangle$. Thus the restriction induces an isomorphism $G/H \xrightarrow{\sim} G_{n-1}/H_{n-1}$.

Recall that M was defined as the subgroup of all elements of N which induce the identity on G/H, and that $N = MG$ by Lemma 3.7.3 or 3.8.3. Recall also that $uha_s a_r u^{-1}|_{T_{n-1}} = udu^{-1}|_{T_{n-1}} = d'|_{T_{n-1}} = h'a_s a_r|_{T_{n-1}}$. It follows that $H_{n-1}(ua_s a_r u^{-1})|_{T_{n-1}} = H_{n-1}(a_s a_r)|_{T_{n-1}}$, in other words, the action of u on G_{n-1}/H_{n-1} induced by conjugation fixes the image of $a_s a_r$. The same is therefore true for the action of u on G/H. As G/H is dihedral with cyclic part $\langle a_s a_r\rangle$ of order 4, this action is also induced by an element of $\langle a_s a_r\rangle$. Since $u \in N = MG$, it follows that $u \in M\langle a_s a_r\rangle$. But the fact that $d \in Ha_s a_r$ implies that $M\langle a_s a_r\rangle = M\langle d\rangle$. After replacing u by ud^λ for a suitable $\lambda \in \mathbb{Z}_2$ we can therefore assume that $u \in M$. Then $(u, u) \in N$ by Lemma 3.7.4 or 3.8.4, and we are done.

It remains to finish the induction step in the case $(s, r, n) = (2, 3, 4)$. For this we use the description of $G_{r+1}/(H_r \times H_r) \subset W_{r+1}/(H_r \times H_r) \cong \mathrm{Mat}_{2\times2}(\{\pm1\}) \rtimes \langle\sigma\rangle$ from Lemma 3.2.15. Since $c = (ha_s, a_r)\,\sigma$ and $c = (h'a_s, a_r)\,\sigma$ with $h, h' \in H$, the image of both elements under the map from 3.2.15 (b) is

$$\left(\begin{smallmatrix} -1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \cdot \sigma.$$

Since any two odometers are conjugate under W, we can choose an element $v \in W$ with $vcv^{-1} = c'$. Then the image of v in $\mathrm{Mat}_{2\times2}(\{\pm1\}) \rtimes \langle\sigma\rangle$ commutes with $\left(\begin{smallmatrix} -1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \cdot \sigma$. By direct calculation the centralizer of this element is

$$\left\langle \left(\begin{smallmatrix} -1 & -1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \cdot \sigma \right\rangle.$$

From 3.2.15 (d) we see that this centralizer is contained in the normalizer of the image of G_{r+1}. Moreover, Lemma 3.8.20 implies that this normalizer is equal to the image of N_{r+1} in $\mathrm{Mat}_{2\times2}(\{\pm1\}) \rtimes \langle\sigma\rangle$. Thus the image of N_{r+1} contains the image of v. Since $r + 1 = 4 = n$, this is equivalent to $v|_{T_n} \in N_n$. But this in turn means that there exists a new element $w \in N$ with $w|_{T_n} = v|_{T_n}$. The equation $vcv^{-1} = c'$ then implies that $wcw^{-1}|_{T_n} = vcv^{-1}|_{T_n} = c'|_{T_n}$, as desired. This finishes the proof of Theorem 3.9.4. $\qquad\square$

The author does not know which analogues of Theorem 2.7.4 (b) and Theorem 2.7.6, if any, might hold in the strictly pre-periodic case. However, we can describe how the normalizer of any odometer in G sits inside N.

Proposition 3.9.5 *Consider any odometer $c \in G$ and any $k \in \mathbb{Z}_2^\times$.*

  (a) There exists an element $w \in N$ with $wcw^{-1} = c^k$.

  (b) Every element $w \in W$ with $wcw^{-1} = c^k$ lies in N.

  (c) For any such w the coset wG depends only on k.

Proof. As c^k is another odometer in G, part (a) follows from Theorem 3.9.4. Next consider two elements $w, w' \in W$ with $wcw^{-1} = w'cw'^{-1} = c^k$. Then $w^{-1}w' \in W$ commutes with c. By Proposition 1.6.4 (b) it therefore lies in $\langle\!\langle c \rangle\!\rangle$ and hence in G. Thus $wG = w'G$. Since $w \in N$ for some choice of w, it follows that $w \in N$ for every choice, proving (b). It also follows that the coset wG is independent of w. Moreover, as all odometers are conjugate under N by Theorem 3.9.4, the conjugacy class of wG in N/G is independent of c. Since N/G is abelian, it follows that the coset wG itself is independent of c, proving (c). (The statement and proof also applies when $(s, r) = (1, 2)$.) $\qquad\square$

For the rest of this subsection we fix elements c, k, w as in Proposition 3.9.5. Like the description of N itself, the determination of the coset wG depends on the respective subcases. Recall that since $(s, r) \neq (1, 2)$, Theorem 3.6.12, 3.7.18, or 3.8.27 yields an isomorphism $\bar\varphi$ between N/G and $\prod_{i=1}^\infty \mathbb{F}_2$ or $\prod_{i=0}^\infty \mathbb{F}_2$. Let

(3.9.6)
$$\left\{ \begin{array}{ll} (k_1, k_2, \dots) \in \prod_{i=1}^\infty \mathbb{F}_2, & \text{resp.} \\ (k_0, k_1, k_2, \dots) \in \prod_{i=0}^\infty \mathbb{F}_2, & \end{array} \right\}$$

be the tuple corresponding to the coset wG.

Lemma 3.9.7 *The elements k_i for $i \geqslant 1$ are all equal.*

Proof. After possibly replacing w by wc we may without loss of generality assume that $w = (u, u') \in W \times W$. Write $c^2 = (d, d')$. Then d is another odometer in G, and the equation $wcw^{-1} = c^k$ implies that $udu^{-1} = d^k$. By Proposition 3.9.5 we therefore have $u \in N$ and $uG = wG$.

Suppose first that $(s, r) \neq (2, 3)$. Since $w \in W \times W$, the choice (3.9.6) then means that $w \in G^1 \cdot \varphi(k_1, k_2, \ldots)$. Note that by the definition (3.6.6) or (3.7.11) of w_1 we have $w_1 \in W \times W$ and

$$\mathrm{pr}_1(w_1) \;=\; \left\{ \begin{array}{ll} \mathrm{pr}_1((a_s, a_s)) = a_s & \text{if } s \geqslant 2 \text{ and } r \geqslant 4, \\ \mathrm{pr}_1((1, (a_s a_r)^2)) = 1 & \text{if } s = 1 \text{ and } r \geqslant 3. \end{array} \right\} \;\in\; G.$$

Using the functional equation (3.6.8) or (3.7.13) and the fact that $\mathrm{pr}_1(G^1) = G$ by Proposition 3.2.2 (d), we deduce that

$$\begin{aligned} G \cdot \varphi(k_1, k_2, \ldots) \;=\; Gw \;&=\; Gu \;=\; G \cdot \mathrm{pr}_1(w) \\ &=\; G \cdot \mathrm{pr}_1\big(G^1 \cdot w_1^{k_1} \cdot \mathrm{diag}(\varphi(k_2, k_3, \ldots))\big) \\ &=\; G \cdot \varphi(k_2, k_3, \ldots). \end{aligned}$$

Therefore $k_1 = k_2 = k_3 = \ldots$, as desired.

Suppose now that $(s, r) = (2, 3)$. Then (3.9.6) means that $w \in G^1 \cdot \varphi(k_0, k_1, k_2, \ldots)$. Also, by the definitions (3.8.11) and (3.8.13) of w_1 and w_0 we have $w_1, w_0 \in W \times W$ and

$$\left\{ \begin{array}{l} \mathrm{pr}_1(w_1) = \mathrm{pr}_1((1, (a_s a_r)^2)) = 1, \quad \text{and} \\ \mathrm{pr}_1(w_0) = \mathrm{pr}_1((a_2 w_0, a_3 w_0)) = a_2 w_0 \in Gw_0. \end{array} \right.$$

Using the functional equation (3.8.22) and the fact that $\mathrm{pr}_1(G^1) = G$, we deduce that

$$\begin{aligned} G \cdot \varphi(k_0, k_1, k_2, \ldots) \;=\; Gw \;&=\; Gu \;=\; G \cdot \mathrm{pr}_1(w) \\ &=\; G \cdot \mathrm{pr}_1\big(G^1 \cdot w_0^{k_0} \cdot w_1^{k_1} \cdot \mathrm{diag}(\varphi(0, k_2, k_3, \ldots))\big) \\ &=\; G \cdot w_0^{k_0} \cdot \varphi(0, k_2, k_3, \ldots) \\ &=\; G \cdot \varphi(k_0, k_2, k_3, \ldots). \end{aligned}$$

Therefore again $k_1 = k_2 = k_3 = \ldots$, as desired. $\qquad\qquad\square$

By Lemma 3.9.7 it remains to determine k_1, respectively k_1 and k_0. The first tool for this is a closer look at the subgroups $G_{r+1} \subset N_{r+1} \subset W_{r+1}$ in the next two lemmas:

Lemma 3.9.8 *(a) If $s = 2$ and $r = 3$, we have $N_4 = G_4 \cdot \langle w_0|_{T_4} \rangle$ and $[N_4 : G_4] = 2$ and $w_i|_{T_4} \in G_4$ for all $i \geqslant 1$.*

(b) If $s \geqslant 2$ and $r \geqslant 4$, we have $N_{r+1} = G_{r+1} \cdot \langle w_1|_{T_{r+1}} \rangle$ and $[N_{r+1} : G_{r+1}] = 2$ and $w_i|_{T_{r+1}} \in G_{r+1}$ for all $i \geqslant 2$.

Proof. Part (a) is just a repetition of Lemmas 3.8.12 (b) and 3.8.20. For (b) recall from the construction (3.6.6) that $w_0 = (a_s, a_s)$; hence the image of the residue class of $w_0|_{T_{r+1}}$ under the isomorphism from Lemma 3.2.15 (b) is the matrix

$$\begin{pmatrix} \mathrm{sgn}_s(a_s) & \mathrm{sgn}_s(a_s) \\ \mathrm{sgn}_r(a_s) & \mathrm{sgn}_r(a_s) \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}.$$

By Lemma 3.2.15 (c) this matrix does not lie in the image of G_{r+1}, which proves that $w_0|_{T_{r+1}} \notin G_{r+1}$. Also, since N normalizes G, its restriction N_{r+1} normalizes G_{r+1}; and hence Lemma 3.2.15 (d) implies that $[N_{r+1} : G_{r+1}] \leqslant 2$. Since $w_1|_{T_{r+1}}$ already lies in N_{r+1}, but not in G_{r+1}, this leaves only the possibility $[N_{r+1} : G_{r+1}] = 2$ with $N_{r+1} = G_{r+1} \cdot \langle w_1|_{T_{r+1}} \rangle$. Finally, for all $i \geqslant 2$ the construction (3.6.6) implies that $w_i = (w_{i-1}, w_{i-1})$ with $w_{i-1} \in \mathrm{diag}(W)$ and hence $\mathrm{sgn}_s(w_{i-1}) = \mathrm{sgn}_r(w_{i-1}) = 1$. Thus the image of the residue class of $w_i|_{T_{r+1}}$ under the isomorphism from Lemma 3.2.15 (b) is the trivial matrix, which shows that $w_i|_{T_{r+1}}$ lies in G_{r+1}. All parts of (b) are now proved. $\qquad\square$

Lemma 3.9.9 *If $s \geqslant 2$, then $w|_{T_{r+1}} \in G_{r+1}$ if and only if $\frac{k-1}{2}$ is even.*

Proof. Abbreviate $\ell := \frac{k-1}{2} \in \mathbb{Z}_2$. As a preparation let $a \in W$ be the standard odometer from (1.6.1) and $z \in W$ the element satisfying $zaz^{-1} = a^k$ from Remark 1.6.5. Recall that z was characterized by the recursion relation $z = (z, a^\ell z)$. Thus we have $\mathrm{sgn}_1(z) = 1$, and for all $n \geqslant 2$ we can calculate

$$\mathrm{sgn}_n(z) = \mathrm{sgn}_{n-1}(z) \cdot \mathrm{sgn}_{n-1}(a^\ell z) = \mathrm{sgn}_{n-1}(a)^\ell = (-1)^\ell.$$

Since $r > s \geqslant 2$, the image of $z|_{T_{r+1}}$ in $\mathrm{Mat}_{2 \times 2}(\{\pm 1\}) \rtimes \langle \sigma \rangle$ under the map from Lemma 3.2.15 (b) is therefore the matrix

$$\begin{pmatrix} \mathrm{sgn}_s(z) & \mathrm{sgn}_s(a^\ell z) \\ \mathrm{sgn}_r(z) & \mathrm{sgn}_r(a^\ell z) \end{pmatrix} = \begin{pmatrix} (-1)^\ell & 1 \\ (-1)^\ell & 1 \end{pmatrix}.$$

The conjugacy class of this element in $\mathrm{Mat}_{2 \times 2}(\{\pm 1\}) \rtimes \langle \sigma \rangle$ is the subset

$$X := \left\{ \begin{pmatrix} (-1)^\ell & 1 \\ (-1)^\ell & 1 \end{pmatrix}, \begin{pmatrix} 1 & (-1)^\ell \\ 1 & (-1)^\ell \end{pmatrix} \right\}.$$

Now recall that a is conjugate to c under W. Proposition 1.6.4 therefore implies that z is conjugate to wc^m under W for some $m \in \mathbb{Z}_2$. It follows that the image of $wc^m|_{T_{r+1}}$ in $\mathrm{Mat}_{2 \times 2}(\{\pm 1\}) \rtimes \langle \sigma \rangle$ is contained in X. Using the description of the image of G_{r+1} from Lemma 3.2.15 (c), we find that X is a subset of the image of G_{r+1} if ℓ is even, and disjoint from it if ℓ is odd. Thus the image of $wc^m|_{T_{r+1}}$ is contained in the image of G_{r+1} if and only if ℓ is even. This means that $wc^m|_{T_{r+1}} \in G_{r+1}$ if and only if ℓ is even. As $c|_{T_{r+1}}$ itself lies in G_{r+1}, it follows that $w|_{T_{r+1}} \in G_{r+1}$ if and only if ℓ is even, as desired. $\qquad\square$

The second tool is a closer study of $G/(H \times H)$ in the following two lemmas:

Lemma 3.9.10 *Assume that either $s = 1$ and $r \geqslant 3$, or $s = 2$ and $r = 3$. Then:*

(a) *$G = (H \times H) \rtimes \langle \sigma, (a_s, a_r) \rangle$ where $\langle \sigma, (a_s, a_r) \rangle$ is a dihedral group with the maximal cyclic subgroup $\langle \sigma(a_s, a_r) \rangle$ of order 8.*

(b) *The subgroup $H \times H$ is normalized by N.*

(c) *Conjugation by w_1 induces the automorphism $x \mapsto x^5$ on the cyclic subgroup of order 8 of $G/(H \times H)$.*

(d) *For every $i \geqslant 2$, conjugation by w_i induces the trivial automorphism on $G/(H \times H)$.*

(e) *If $s = 2$ and $r = 3$, conjugation by w_0 induces an inner automorphism on $G/(H \times H)$.*

Proof. The semidirect product decomposition in (a) is a reminder from Lemmas 3.7.2 (c) and 3.8.2 (c), and the element $\sigma(a_s, a_r) = a_1 a_{s+1}$ has order 8 by Proposition 3.1.9 in both cases, proving (a).

Next, by (3.7.11) and (3.8.11) we have $w_1 = (1, (a_s a_r)^2)$ in both cases. Since $(a_s a_r)^2 = (a_r a_s)^2$ generates the center of $\langle a_s, a_r \rangle$ by Lemma 3.7.2 (a) or 3.8.2 (a), it follows that w_1 commutes with (a_s, a_r). On the other hand we calculate

$$(\sigma(a_s, a_r))^4 = (a_r a_s, a_s a_r)^2 = ((a_r a_s)^2, (a_s a_r)^2) = ((a_s a_r)^2, (a_s a_r)^2) = [w_1, \sigma].$$

Together this implies that

$$w_1 \cdot \sigma(a_s, a_r) \cdot w_1^{-1} = w_1 \sigma w_1^{-1} \sigma^{-1} \cdot \sigma(a_s, a_r) = (\sigma(a_s, a_r))^4 \sigma(a_s, a_r) = (\sigma(a_s, a_r))^5.$$

Also, since $(a_s a_r)^2$ normalizes H, the element w_1 normalizes $H \times H$, and together this shows (c).

By (3.7.11) and (3.8.11) in both cases we also have $w_i = (w_{i-1}, w_{i-1})$ for all $i \geqslant 2$. This element trivially commutes with σ, and since conjugation by $w_{i-1} \in M$ normalizes H and acts trivially on G/H, it follows that conjugation by w_i normalizes $H \times H$ and fixes the coset $(a_s, a_r)(H \times H)$. This implies (d).

In the case $s = 2$ and $r = 3$ we have $w_0 = a_3(w_0, w_0)$ by the construction (3.8.13). Also since $w_0 \in M$ by Lemma 3.8.17, conjugation by w_0 normalizes H and acts trivially on G/H. Thus conjugation by (w_0, w_0) normalizes $H \times H$ and fixes the coset $(a_s, a_r)(H \times H)$. Since (w_0, w_0) also commutes with σ, it follows that conjugation by it induces the trivial automorphism of $G/(H \times H)$. This implies that $w_0 = a_3(w_0, w_0)$ normalizes $H \times H$ and induces the same inner automorphism of $G/(H \times H)$ as a_3, proving (e).

Finally, since N is generated by G and all the elements w_i considered, and all these elements normalize $H \times H$, this implies (b). $\qquad \square$

Lemma 3.9.11 *In the situation of Lemma 3.9.10, the image of c in the dihedral group $G/(H \times H)$ generates the maximal cyclic subgroup of order 8.*

Proof. Since all odometers in G are conjugate under N by Theorem 3.9.4, and N normalizes $H \times H$ by Lemma 3.9.10 (b), it suffices to prove this for any one choice of c. We will prove it for $c = a_1 \cdots a_r$, which is an odometer in G by Proposition 3.9.1 (a). Recall that $a_i = (a_{i-1}, 1) \in H \times 1$ for all $i \neq 1, s+1$. Thus the image of $a_1 \cdots a_r$ in $G/(H \times H)$ is equal to the image of $a_1 a_{s+1} = \sigma(a_s, a_r)$. By Lemma 3.9.10 (a) this image generates the maximal cyclic subgroup of $G/(H \times H)$, as desired. $\qquad\square$

Now we can reap the fruits of the preceding efforts:

Lemma 3.9.12

(a) *If $s \geqslant 2$ and $r \geqslant 4$, we have $k_1 \equiv \frac{k-1}{2} \bmod 2$.*

(b) *If $s = 1$ and $r \geqslant 3$, we have $k_1 \equiv \frac{k^2-1}{8} \bmod 2$.*

(c) *If $s = 2$ and $r = 3$, we have $k_0 \equiv \frac{k-1}{2} \bmod 2$.*

(d) *If $s = 2$ and $r = 3$, we have $k_1 \equiv \frac{k^2-1}{8} \bmod 2$.*

Proof. If $s \geqslant 2$ and $r \geqslant 4$, the definition (3.6.7) of φ implies that

$$w \in G \cdot \varphi(k_1, k_2, \ldots) = G \, w_1^{k_1} w_2^{k_2} \cdots .$$

By Lemma 3.9.8 (b) it follows that $w|_{T_{r+1}} \in G_{r+1} \cdot (w_1|_{T_{r+1}})^{k_1}$ with $w_1|_{T_{r+1}} \notin G_{r+1}$. But by Lemma 3.9.9 we have $w|_{T_{r+1}} \in G_{r+1}$ if and only if $\frac{k-1}{2} \equiv 0 \bmod 2$. Thus $k_1 \equiv \frac{k-1}{2} \bmod 2$, proving (a).

If $s = 1$ and $r \geqslant 3$, the definition (3.7.12) of φ again implies that

$$w \in G \cdot \varphi(k_1, k_2, \ldots) = G \, w_1^{k_1} w_2^{k_2} \cdots .$$

From Lemma 3.9.10 (c–d) we find that conjugation by $w_1^{k_1} w_2^{k_2} \cdots$ induces the automorphism $x \mapsto x^{1+4k_1}$ on the maximal cyclic subgroup of order 8 of $G/(H \times H)$. Moreover, as $G/(H \times H)$ is a dihedral group, the automorphism of the maximal cyclic subgroup induced by any element of G has the form $x \mapsto x^{\pm 1}$. On the other hand, by Lemma 3.9.11 this subgroup is generated by the image of c, and so conjugation by w induces the automorphism $x \mapsto x^k$ on it. Together this implies that $x^{\pm(1+4k_1)} = x^k$, or equivalently $1 + 4k_1 \equiv \pm k \bmod 8$. Therefore $k_1 \equiv \frac{k^2-1}{8} \bmod 2$, proving (b).

If $s = 2$ and $r = 3$, the definition (3.8.21) of φ implies that

$$w \in G \cdot \varphi(k_0, k_1, k_2, \ldots) = G \, w_0^{k_0} w_1^{k_1} w_2^{k_2} \cdots .$$

By Lemma 3.9.8 (a) it follows that $w|_{T_4} \in G_4 \cdot (w_0|_{T_4})^{k_0}$ with $w_0|_{T_4} \notin G_4$. But by Lemma 3.9.9 we have $w|_{T_4} \in G_4$ if and only if $\frac{k-1}{2} \equiv 0 \bmod 2$. Thus $k_0 \equiv \frac{k-1}{2} \bmod 2$, proving (c).

Moreover, from Lemma 3.9.10 (c–d) we find that conjugation by $w_1^{k_1} w_2^{k_2} \cdots$ induces the automorphism $x \mapsto x^{1+4k_1}$ on the maximal cyclic subgroup of order 8 of $G/(H \times H)$.

With Lemma 3.9.10 (e) we also deduce that the automorphism induced by any element of $Gw_0^{k_0}$ has the form $x \mapsto x^{\pm 1}$. Continuing exactly as in the proof of (b) now shows (d). $\quad\square$

To combine everything consider the two homomorphisms

$$(3.9.13) \qquad \left\{ \begin{array}{l} \vartheta_1 \colon \mathbb{Z}_2^\times \twoheadrightarrow \mathbb{F}_2, \ k \mapsto \frac{k-1}{2} \bmod 2, \\ \vartheta_2 \colon \mathbb{Z}_2^\times \twoheadrightarrow \mathbb{F}_2, \ k \mapsto \frac{k^2-1}{8} \bmod 2. \end{array} \right\}$$

Reincluding the case $(s, r) = (1, 2)$, recall that Theorem 3.6.12, 3.7.18, or 3.8.27, respectively Proposition 1.6.4 yields an isomorphism between N/G and $\prod_{i=1}^\infty \mathbb{F}_2$ or $\prod_{i=0}^\infty \mathbb{F}_2$, respectively $\mathbb{Z}_2^\times/\{\pm 1\}$.

Proposition 3.9.14 *Consider any odometer $c \in G$ and any element $w \in N$ with $wcw^{-1} = c^k$ for some $k \in \mathbb{Z}_2^\times$. Then the coset $wG \in N/G$ corresponds to the element*

$$\left\{ \begin{array}{ll} (\vartheta_1, \vartheta_1, \ldots)(k) \ \in \ \prod_{i=1}^\infty \mathbb{F}_2 \cong N/G & \text{if } s \geqslant 2 \text{ and } r \geqslant 4, \\ (\vartheta_2, \vartheta_2, \ldots)(k) \ \in \ \prod_{i=1}^\infty \mathbb{F}_2 \cong N/G & \text{if } s = 1 \text{ and } r \geqslant 3, \\ (\vartheta_1, \vartheta_2, \vartheta_2, \ldots)(k) \ \in \ \prod_{i=0}^\infty \mathbb{F}_2 \cong N/G & \text{if } s = 2 \text{ and } r = 3, \\ k \bmod \{\pm 1\} \ \in \ \mathbb{Z}_2^\times/\{\pm 1\} \cong N/G & \text{if } s = 1 \text{ and } r = 2. \end{array} \right\}$$

Proof. The first three cases follow by combining the formula (3.9.6) with Lemmas 3.9.7 and 3.9.12, the last case from the remarks at the beginning of this subsection. $\quad\square$

3.10 Iterated monodromy groups

Now let $G^{\mathrm{geom}} \subset G^{\mathrm{arith}} \subset W$ be the geometric and arithmetic fundamental groups associated to a quadratic polynomial over k, as described in Subsection 1.7, and assume that we are in the strictly pre-periodic case 1.7.2 (c). Then $G^{\mathrm{geom}} = \langle\!\langle b_1, \ldots, b_r \rangle\!\rangle$, where by Proposition 1.7.14 the generators satisfy the recursion relations

$$(3.10.1) \qquad \left\{ \begin{array}{l} b_1 \text{ is conjugate to } \sigma \text{ under } W, \\ b_{s+1} \text{ is conjugate to } (b_s, b_r) \text{ under } W, \text{ and} \\ b_i \text{ is conjugate to } (b_{i-1}, 1) \text{ under } W \text{ for all } 2 \leqslant i \leqslant r \text{ with } i \neq s+1. \end{array} \right\}$$

By combining Proposition 3.4.1 and Theorem 3.4.3 we deduce:

Theorem 3.10.2 *There exists $w \in W$ such that $G^{\mathrm{geom}} = wGw^{-1}$ and b_i is conjugate to wa_iw^{-1} under G^{geom} for every $1 \leqslant i \leqslant r$.*

For the following we change the identification of trees used in Subsection 1.7 by the automorphism w, after which we have $G^{\mathrm{geom}} = G$, and b_i is conjugate to a_i under G for every $1 \leqslant i \leqslant r$. Then G^{arith} is contained in the normalizer N, and to describe it it

suffices to describe the factor group $G^{\text{arith}}/G \subset N/G$. More precisely we will determine the composite homomorphism

$$(3.10.3) \qquad\qquad \bar\rho\colon \operatorname{Gal}(\bar k/k) \twoheadrightarrow G^{\text{arith}}/G \hookrightarrow N/G$$

obtained from (1.7.7). Consider the cyclotomic character

$$\operatorname{cycl}\colon \operatorname{Gal}(\bar k/k) \longrightarrow \mathbb{Z}_2^\times,\ \tau \mapsto \operatorname{cycl}(\tau).$$

Lemma 3.10.4 *The element $b_\infty := (b_1 \cdots b_r)^{-1}$ is an odometer in G, and for any $\tau \in \operatorname{Gal}(\bar k/k)$ we have $\bar\rho(\tau) = wG$ for some element $w \in N$ which satisfies $wb_\infty w^{-1} = b_\infty^{\operatorname{cycl}(\tau)}$.*

Proof. Recall from Subsection 1.7 that b_∞ is a generator of the image of an inertia group $I_\infty \subset \pi_1^{\text{ét}}(\mathbb{P}_{\bar k}^1 \smallsetminus S, x_0)$ above $\infty \in \mathbb{P}_k^1$. Let D_∞ be the associated decomposition group. Since ∞ is a k-rational point, we have a commutative diagram with exact rows

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & I_\infty & \longrightarrow & D_\infty & \longrightarrow & \operatorname{Gal}(\bar k/k) & \longrightarrow & 1 \\
& & \cap\downarrow & & \cap\downarrow & & \| & & \\
1 & \longrightarrow & \pi_1^{\text{ét}}(\mathbb{P}_{\bar k}^1 \smallsetminus S, x_0) & \longrightarrow & \pi_1^{\text{ét}}(\mathbb{P}_k^1 \smallsetminus S, x_0) & \longrightarrow & \operatorname{Gal}(\bar k/k) & \longrightarrow & 1 \\
& & \rho\downarrow & & \rho\downarrow & & \bar\rho\downarrow & & \\
1 & \longrightarrow & G & \longrightarrow & G^{\text{arith}} & \longrightarrow & G^{\text{arith}}/G & \longrightarrow & 1.
\end{array}
$$

Since the target of the homomorphism ρ is a pro-2 group, the restriction $\rho|_{I_\infty}$ factors through the maximal pro-2 quotient of I_∞. As the characteristic of k is different from 2, this quotient is the pro-2 tame inertia group above ∞ and hence isomorphic $\mathbb{Z}_2$ and generated by b_∞. Moreover, $D_\infty/I_\infty \cong \operatorname{Gal}(\bar k/k)$ acts on it through the cyclotomic character. Thus for any $\delta \in D_\infty$ with image $\tau \in \operatorname{Gal}(\bar k/k)$ the element $w := \rho(\delta) \in G^{\text{arith}} \subset N$ satisfies $wb_\infty w^{-1} = b_\infty^{\operatorname{cycl}(\tau)}$. Since b_∞ is an odometer by Proposition 3.9.1, the lemma follows. $\square$

Finally recall that Theorem 3.6.12, 3.7.18, or 3.8.27, respectively Proposition 1.6.4 yields an isomorphism between N/G and $\prod_{i=1}^\infty \mathbb{F}_2$ or $\prod_{i=0}^\infty \mathbb{F}_2$, respectively $\mathbb{Z}_2^\times/\{\pm 1\}$. By combining Lemma 3.10.4 with Proposition 3.9.14 we deduce:

Theorem 3.10.5 *The homomorphism $\bar\rho\colon \operatorname{Gal}(\bar k/k) \to N/G$ has the form*

$$
\left\{
\begin{array}{ll}
(\vartheta_1, \vartheta_1, \ldots) \circ \operatorname{cycl} : \operatorname{Gal}(\bar k/k) \xrightarrow{\bar\rho} N/G \cong \prod_{i=1}^\infty \mathbb{F}_2 & \text{if } s \geqslant 2 \text{ and } r \geqslant 4, \\
(\vartheta_2, \vartheta_2, \ldots) \circ \operatorname{cycl} : \operatorname{Gal}(\bar k/k) \xrightarrow{\bar\rho} N/G \cong \prod_{i=1}^\infty \mathbb{F}_2 & \text{if } s = 1 \text{ and } r \geqslant 3, \\
(\vartheta_1, \vartheta_2, \vartheta_2, \ldots) \circ \operatorname{cycl} : \operatorname{Gal}(\bar k/k) \xrightarrow{\bar\rho} N/G \cong \prod_{i=0}^\infty \mathbb{F}_2 & \text{if } s = 2 \text{ and } r = 3, \\
\operatorname{cycl} \bmod\{\pm 1\} : \operatorname{Gal}(\bar k/k) \xrightarrow{\bar\rho} N/G \cong \mathbb{Z}_2^\times/\{\pm 1\} & \text{if } s = 1 \text{ and } r = 2.
\end{array}
\right\}
$$

Corollary 3.10.6

(a) *If $s \geqslant 2$ and $r \geqslant 4$, the order of G^{arith}/G divides 2.*

(b) *If $s \geqslant 2$ and $r \geqslant 4$ and k contains the fourth roots of unity, then $G^{\mathrm{arith}} = G$.*

(c) *If $s = 1$ and $r \geqslant 3$, the order of G^{arith}/G divides 2.*

(d) *If $s = 1$ and $r \geqslant 3$ and k contains a square root of 2, then $G^{\mathrm{arith}} = G$.*

(e) *If $s = 2$ and $r = 3$, the order of G^{arith}/G divides 4.*

(f) *If $s = 2$ and $r = 3$ and k contains the eighth roots of unity, then $G^{\mathrm{arith}} = G$.*

(g) *If $s = 1$ and $r = 2$ and k is finitely generated over its prime field, then G^{arith}/G a subgroup of finite index of $\mathbb{Z}_2^{\times}/\{\pm 1\}$.*

Proof. Parts (a–f) are direct consequences of Theorem 3.10.5; part (g) follows by the same argument as in the proof of Theorem 2.8.4 (b). $\qquad\square$

References

[1] Bartholdi, L., Grigorchuk, R.: On parabolic subgroups and Hecke algebras of some fractal groups. *Serdica Math. J.* **28** (2002), no. 1, 47–90.

[2] Bartholdi, L., Nekrashevych, V.: Iterated monodromy groups of quadratic polynomials. I. *Groups Geom. Dyn.* **2** (2008), no. 3, 309–336.

[3] Boston, N., Jones, R.: Arboreal Galois representations. *Geom. Dedicata* **124** (2007), 27–35.

[4] Boston, N., Jones, R.: The image of an arboreal Galois representation. *Pure Appl. Math. Q.* **5**, no. 1, (2009) 213–225.

[5] Dau, T. T.: *Quadratische Morphismen.* Diplomarbeit ETH Zürich (2002), 65p. http://www.math.ethz.ch/~pink/Theses/2002-Diplom-Tan-Truong-Dau.pdf

[6] Gawron, P., Nekrashevych, V., Sushchansky, V.: Conjugation in tree automorphism groups. *Internat. J. Algebra Comput.* **11** no. 5 (2001), 529–547.

[7] Grigorchuk, R.: On Burnside's problem on periodic groups. (Russian) *Funktsional. Anal. i Prilozhen.* **14** (1980), no. 1, 53–54. English translation: *Functional Anal. Appl.* **14** (1980), no. 1, 41–43.

[8] Grigorchuk, R.: Just infinite branch groups. in: *New horizons in pro-p groups*, Progr. Math. 184, Boston: Birkhäuser (2000), 121–179.

[9] Grigorchuk, R. Żuk, A.: On a torsion-free weakly branch group defined by a three state automaton. *Internat. J. Algebra Comput.* **12** (2002), no. 1-2, 223–246.

[10] Grigorchuk, R., Sidki, S.: The group of automorphisms of a 3-generated 2-group of intermediate growth. *Internat. J. Algebra Comput.* **14** no. 5-6, (2004), 667–676.

[11] Grigorchuk, R., Savchuk, D., Šunić, Z.: The spectral problem, substitutions and iterated monodromy. In: *Probability and mathematical physics.* CRM Proc. Lecture Notes, 42, Amer. Math. Soc., Providence, RI (2007), 225–248.

[12] Grigorchuk, R., Šunić, Z.: Self-similarity and branching in group theory. in *Groups St. Andrews 2005.* Vol. 1, London Math. Soc. Lecture Note Ser., 339, Cambridge Univ. Press, Cambridge, 2007, 36–95.

[13] Grothendieck, A.: *Revetements étales et groupe fondamental (SGA 1).* Lecture Notes in Mathematics, Vol. 224. Berlin: Springer (1971).

[14] Jones, R., Boston, N.: Settled polynomials over finite fields. *Proc. Amer. Math. Soc.* **140** (2012), no. 6, 1849–1863.

[15] Nekrashevich, V.: *Iterated monodromy groups.* (2003) 39p. arXiv:math/0312306

[16] Nekrashevych, V.: *Self-similar groups.* Mathematical Surveys and Monographs, 117. American Mathematical Society, Providence, RI, 2005.

[17] Nekrashevich, V.: A minimal Cantor set in the space of 3-generated groups. *Geom. Dedicata* **124** (2007), 153–190.

[18] Nekrashevych, V.: Iterated monodromy groups. In: *Groups St Andrews 2009 in Bath. Volume 1.* London Math. Soc. Lecture Note Ser., 387, Cambridge Univ. Press, Cambridge (2011), 41–93.

[19] Pink, R.: *Finiteness and liftability of postcritically finite quadratic morphisms in arbitrary characteristic.* Preprint (version 3, August 2013), 36p. `arXiv:1305.2841 [math.AG]`

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