Gaussian groups and Garside groups, two generalisations of Artin groups

Patrick Dehornoy and Luis Paris

September 10, 1998

Abstract. It is known that a number of algebraic properties of the braid groups extend to arbitrary finite Coxeter type Artin groups. Here we show how to extend the results to more general groups that we call Garside groups.

Define a Gaussian monoid to be a finitely generated cancellative monoid where the expressions of a given element have bounded lengths, and where left and right lower common multiples exist. A Garside monoid is a Gaussian monoid in which the left and right l.c.m.'s satisfy an additional symmetry condition. A Gaussian group and a Garside group are respectively the group of fractions of a Gaussian monoid and of a Garside monoid. Braid groups and, more generally, finite Coxeter type Artin groups are Garside groups. We determine algorithmic criterions in terms of presentations for recognizing Gaussian and Garside monoids and groups, and exhibit infinite families of such groups. We describe simple algorithms that solve the word problem in a Gaussian group, show that theses algorithms have a quadratic complexity if the group is a Garside group, and prove that Garside groups have quadratic isoperimetric inequalities. We construct normal forms for Gaussian groups, and prove that, in the case of a Garside group, the language of normal forms is regular, symmetric, and geodesic, has the 5-fellow traveller property, and has the uniqueness property. This shows in particular that Garside groups are geodesically fully biautomatic. Finally, we consider an automorphism of a finite Coxeter type Artin group derived from an automorphism of its defining Coxeter graph, and prove that the subgroup of elements fixed by this automorphism is also a finite Coxeter type Artin group that can be explicitely determined.

Mathematics Subject Classification. Primary 20F05, 20F36. Secondary 20B40, 20M05

1. Introduction

The *positive braid monoid* (on $n+1$ strings) is the monoid B_+ that admits the presentation

$$\langle x_1, \dots, x_n \mid x_i x_j = x_j x_i \text{ if } |i-j| \geq 2,\ x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \text{ if } i = 1, \dots, n-1 \rangle \ .$$

It was considered by Garside in [18] and plays a prominent rôle in the theory of braid groups. In particular, several properties of the braid groups are derived from extensive investigations of the positive braid monoids (see for example [2], [16], [17]).

A first observation is that the defining relations of B_+ are homogeneous. Thus, one may deal with a length function $\nu : B_+ \to \mathbf{N}$ which associates to a in B_+ the length of any expression of a. For a, b in B_+, we say that a is a *left divisor* of b or, equivalently, that b is a *right multiple* of a if there exists c in B_+ such that b is ac. The existence of the length function guarantees that left divisibility is a partial order on B_+. It was actually proved in [18] that any two elements of B_+ have a lowest common right multiple. Moreover, B_+ has *left and right cancellation properties*, namely, $ab = ac$ implies $b = c$, and $ba = ca$ implies $b = c$. Ore's criterion says: if a monoid M has left and right cancellation properties, and if any two elements of M have a common right multiple, then M embeds in its *group of (right) fractions* (see [10, Theorem 1.23]). This group is $(M * M^{-1})/\equiv$, where M^{-1} is the dual monoid of M, and $\equiv$ is the congruence relation generated by the pairs $(xx^{-1}, 1)$ and $(x^{-1}x, 1)$, x in M. By the previous considerations, B_+ satisfies Ore's conditions, and, therefore, embeds in its group of fractions. This is the braid group on $n+1$ strings.

The *fundamental element* of B_+, usually denoted by Δ, is the lowest common right multiple of $x_1, \dots, x_n$. It is also the lowest common left multiple of $x_1, \dots, x_n$, and Δ^2 generates the center of the braid group. Furthermore, the set of left divisors of Δ is equal to the set of right divisors of Δ.

This situation was simultaneously generalised by Brieskorn and Saito [5], and by Deligne [15], to a family of monoids and groups called finite Coxeter type Artin monoids and groups. Like the braid groups, these groups have nice normal forms (see [5] and [15]), have fast word problem solutions (see [29]), and are biautomatic (see [8] and [9]), all these properties being proved through a deep study of the Artin monoids.

In this paper, we shall extend the previous results to a larger class of monoids and groups, which we naturally propose to term *Garside*. These groups are characterized as being groups of fractions for monoids in which the divisibility relations form lattices of a certain type. Equivalently, these monoids are characterized by the fact that they admit a presentation of the type $\langle S \mid R \rangle$ where R is a list of relations of the form

$$\{x \dots = y \dots ; x, y \in S\}$$

(subject to additional conditions), i.e., for every pair of generators (x, y), there is exactly one relation that prescribes how to complete x and y on the right in order to obtain equal elements. Observe that, in such cases, the graph $LR(S, R)$ of [26] is a clique, so these presentations are quite different from those for which Adjan has proved in [1] an embeddability result, namely those such that $LR(S, R)$ has no cycle.

We say that a finitely generated monoid M is *atomic* if there exists a mapping $\nu : M \to \mathbf{N}$ satisfying $\nu(a) > 0$ for $a \neq 1$, and $\nu(ab) \geq \nu(a) + \nu(b)$ for a, b in M. As for the positive braid monoids, the existence of such a mapping implies that the left divisibility relation is a partial order on M. We say that M is *right Gaussian* if, in addition, it has left cancellation property and if any two elements of M have a lowest common right multiple. *Left Gaussian* monoids are defined symmetrically. A *Gaussian monoid* is a left and right Gaussian monoid. By Ore's criterion, such a monoid embeds in its group of fractions. A *Gaussian group* is the group of fractions of a Gaussian monoid.

An element a in a monoid M is an *atom* if it is indecomposable, namely, $a = bc$ implies $b = 1$ or $c = 1$. We prove in Section 2 that: if M is an atomic monoid, then the set of atoms of M is finite and generates M. Note that the atoms of B_+ are exactly the initial generators $x_1, \ldots, x_n$.

Let M be a Gaussian monoid. Let Δ_R denote the lowest common right multiple of the atoms, and let Δ_L denote the lowest common left multiple of the atoms. We say that M is a *Garside monoid* if the set of left divisors of Δ_R is equal to the set of right divisors of Δ_L. Positive braid monoids, and, more generally, finite Coxeter type Artin monoids are Garside monoids. A *Garside group* is the group of fractions of a Garside monoid.

Let S be a finite set, and let S^* denote the free monoid generated by S. A *complement* on S is simply a mapping $f : S \times S \to S^*$ that satisfies $f(x, x) = \varepsilon$ for all x in S, where ε denotes the empty word. The *monoid associated with f on the right* is the monoid $M_R(S, f)$ that admits the presentation

$$\langle S \mid xf(y, x) = yf(x, y) \text{ for } x, y \in S \rangle \ .$$

Similarly, $G_R(S, f)$ is the group that admits the same presentation. If S is $\{x_1, \ldots, x_n\}$ and f is defined by

$$f(x_i, x_j) = \begin{cases} \varepsilon & \text{for } i = j, \\ x_i x_j & \text{for } |i - j| = 1, \\ x_i & \text{for } |i - j| \geq 2, \end{cases}$$

then $M_R(S, f)$ is the positive braid monoid and $G_R(S, f)$ is the braid group on $n + 1$ strings. Artin monoids and groups have also the form $M_R(S, f)$ and $G_R(S, f)$ respectively. In [14], the first author shows that, under certain conditions described in Section 3, the monoid $M_R(S, f)$ is left Gaussian.

In Section 4 we prove that the converse is true, namely, if M is a right Gaussian monoid, then it has the form $M_R(S, f)$ for some S, f that satisfy the conditions mentioned above. Then we describe necessary, sufficient, and effective conditions for $M_R(S, f)$ to be a Garside monoid. This is applied in Section 5 to exhibit infinite families of Garside groups that include torus knot groups, fundamental groups of complements of complex lines through the origin, and some "braid groups" associated with complex reflection groups.

Our main tool in this paper is an algorithmic process, called the *word reversing process*. It is described in Section 3. It was first introduced in [11] and [12] in order to study a special group related to the self-distributive identity, and was developed in [14]. It is shown in [14] that this word reversing process gives rise to very simple algorithms which solve the word problem in a group of the form $G_R(S, f)$, whenever (S, f) satisfies the conditions mentioned before. In particular, they apply to the braid groups and have, in this case, a quadratic complexity. Tatsuoka uses in [29] a similar algorithmic process for showing that finite Coxeter type Artin groups have quadratic isoperimetric inequalities. We observe in Section 6 that the same ideas provide an algorithm which solves the word problem for general Gaussian groups, that this algorithm has a quadratic complexity in the case of Garside groups, and that Garside groups have quadratic isoperimetric inequalities—this result holds more generally for small Gaussian groups, a intermediate class between arbitrary Gaussian groups and Garside groups.

We construct normal forms for Gaussian groups in Section 7, and prove in Section 8 that, in the case of Garside groups, the language of normal forms is regular, geodesic, symmetric, has the 5-fellow traveller property, and has the uniqueness property. This shows in particular that Garside groups are geodesically fully biautomatic. These normal forms are nothing but those of [9] in the case of finite Coxeter type Artin groups, and our proof of Theorem 8.1 is inspired by the proof of [9, Theorem 0.1].

In the last section we apply the techniques developed in this paper to prove an original theorem on finite Coxeter type Artin groups. We consider an automorphism of a finite Coxeter type Artin group derived from an automorphism of its defining Coxeter graph. We prove that the subgroup of elements fixed by this automorphism is also a finite Coxeter type Artin group that can be explicitly determined.

2. Atomic, Gaussian, and Garside monoids and groups

Let S be a finite set (of letters). We write S^* for the free monoid generated by S, and $(S \cup S^{-1})^*$ for the free monoid generated by $S \cup S^{-1}$, where S^{-1} is a set in one-to-one correspondence with S whose elements represent the inverses of the elements of S. The elements of S^* will be called *positive words*, while the elements of $(S \cup S^{-1})^*$ will be simply called *words*. The general form of a monoid generated by S is $S^*/\equiv$, where $\equiv$ is a congruence relation on S^*. Similarly, the general form of a group generated by S is $(S \cup S^{-1})^*/\equiv$, where $\equiv$ is a congruence relation on $(S \cup S^{-1})^*$ that includes all pairs (xx^{-1}, ε) and $(x^{-1}x, \varepsilon)$, x in S, ε denoting the empty word. In general, we shall denote by $\overline{w}$ the class of the word w in a monoid $S^*/\equiv$ or in a group $(S \cup S^{-1})^*/\equiv$. If $\overline{w}$ is a, we say that w *represents* a or, equivalently, that w is an *expression* of a.

Proposition 2.1. *Let M be a monoid. The following conditions are equivalent:*

i) There exists a mapping $\nu : M \to \mathbf{N}$ satisfying $\nu(a) < \nu(ab)$ for all a, b in M, $b \neq 1$.

ii) There exists a mapping $\nu : M \to \mathbf{N}$ satisfying $\nu(b) < \nu(ab)$ for all a, b in M, $a \neq 1$.

iii) There exists a mapping $\nu : M \to \mathbf{N}$ satisfying $\nu(a) > 0$ for all a in M, $a \neq 1$, and satisfying

$$\nu(a) + \nu(b) \leq \nu(ab) \tag{2.1}$$

for all a, b in M.

iv) For any set S that generates M and for any a in M, the lengths of the expressions of a in S^* have a finite upper bound.

Proof. Let S be any set that generates the monoid M. Assume first (i). Considering the case $a = 1$ gives $\nu(b) \geq 1$ for all $b \neq 1$. It follows that, if the word w represents a, then $\lg(w) \leq \nu(a)$ holds. This gives (iv). Similarly, (ii) implies (iv), and so does (iii), as the latter clearly implies (i) and (ii).

Now, assume (iv). The mapping

$$\nu : a \mapsto \sup\{\lg(w)\ ;\ w \in S^* \text{ and } \overline{w} = a\} \tag{2.2}$$

satisfies (2.1), which establishes (iii). □

Definition. A finitely generated monoid M is *atomic* if it satisfies the equivalent conditions of Proposition 2.1. An element a of M is an *atom* if it is indecomposable, namely, $a = bc$ implies $b = 1$ or $c = 1$.

Proposition 2.2. *Let M be an atomic monoid. The subsets of M that generate M are exactly those subsets that include the set of all atoms. In particular, the set of atoms generates M and is finite.*

Proof. Let X be a generating set of M. Let a be an atom (if such an element exists). There exist $x_1, \ldots, x_r$ in X such that a is $x_1 \ldots x_r$. By definition, there exists an index i such that x_j is 1 if $j \neq i$. Then $a = x_i$ is in X. We prove now that the set of atoms generates M. We pick a in M and prove by induction on $\nu(a)$ that a is a finite product of atoms. If a is not an atom, then it is equal to a product bc, where b, c are in M and $\nu(b), \nu(c)$ are strictly less than $\nu(a)$. By induction hypothesis, b and c are both finite products of atoms, thus so is a. (In particular, atoms exist.) □

It follows that the mapping ν defined by (2.2) does not depend on the generating set S; for a in M, $\nu(a)$ is the maximal length of an expression of a as a product of atoms. We write $\|a\|$ for $\nu(a)$ and we call it the *norm* of a.

Although atomicity is a rather weak assumption, it implies strong properties for the divisibility relations of the involved monoids. We recall that a is a *left divisor* of b, or that b is a *right multiple* of a, if there exists c satisfying $b = ac$. If in addition we require $c \neq 1$, we say that a is a *proper left divisor* of b. Of course, *right divisors* and *left multiples* are defined symmetrically.

Proposition 2.3. *Let M be a finitely generated monoid. Then M is atomic if and only if the left divisibility relation is a partial order and every element of M admits only finitely many left divisors.*

Proof. Assume that M is atomic. If a is a proper left divisor of b, then $\|a\| < \|b\|$. So, the left divisibility relation is a partial order. The length of a word which represents an element a is at most $\|a\|$, thus there are only finitely many of them.

Assume now that the left divisibility relation is a partial order and that every element of M admits only finitely many left divisors. Let S be a generating set of M. Suppose that the element a can be represented by a word $x_1 \ldots x_\ell$ with $x_1, \ldots, x_\ell$ in S. Then the classes of $x_1 \ldots x_i$ are pairwise distinct, since the class of $x_1 \ldots x_i$ is a proper divisor of the class of $x_1 \ldots x_j$ for $i < j$. Hence ℓ must be bounded above by the number of left divisors of a. We conclude using Proposition 2.1.iv. □

In the context of atomic monoids, left and right divisibility are orderings. We consider now the possible existence of lowest upper bounds and greatest lower bounds in these orderings, namely, the existence of lowest common multiples and greatest common divisors. We use $a \vee_R b$ and $a \wedge_L b$ to denote respectively the right l.c.m. and the left g.c.d. of a and b. Similarly, we use $a \vee_L b$ and $a \wedge_R b$ to denote respectively the left l.c.m. and the right g.c.d. of a and b.

DEFINITION. A finitely generated monoid M is a *right Gaussian monoid* if:

i) M is a left cancellative atomic monoid;

ii) $a \vee_R b$ exists for all a, b in M.

In a right Gaussian monoid M, the element $a \wedge_L b$ exists for all a, b in M; it is the right l.c.m. of the common left divisors of a and b. In particular, left divisibility turns M into a lattice. *Left Gaussian monoids* are defined symmetrically. A *Gaussian monoid* is a right and left Gaussian monoid. Such a monoid satisfies Ore's conditions, and thus embeds in its group of (right) fractions. A *Gaussian group* is the group of (right) fractions of a Gaussian monoid.

As shown in the next proposition, weaker assumptions about right divisibility are sufficient to guarantee that a given monoid is a Gaussian monoid. A monoid M is *left regular* if any two elements of M have a common left multiple.

PROPOSITION 2.4. *Let M be a right Gaussian monoid. Then M is a left Gaussian monoid if and only if it is right cancellative and left regular.*

Proof. We assume that M is right cancellative and left regular and we prove that left l.c.m.'s always exist. Let a, b be elements of M. Choose c and d such that $da = cb$ holds and $\|da\|$ is minimal. We claim that da is the left l.c.m. of a and b in M. Consider a common left multiple of a and b, say $d'a = c'b$. By left regularity, there exist e, e' satisfying $ed = e'd'$. Let e'' be the right l.c.m. of e and e'. By hypothesis, e and e' are left divisors of ed, thus there exists d'' such that ed is equal to $e''d''$. Now, $ed = e'd'$ implies $ecb = eda = e'd'a = e'c'b$, therefore, by right cancellativity, $ec = e'c'$. Hence, e and e' are left divisors of ec as well, and so is e''. There exists c'' such that ec is equal to $e''c''$. This gives $e''d''a = eda = ecb = e''c''b$, hence $d''a = c''b$ by left cancellativity. Then $d''a$ is a common left multiple of a and b, and, by construction, $\|d''a\| \leq \|da\|$ and d is a left multiple of d''. The only possibility is d'' to be equal to d, thus $d'a$ is a left multiple of da. $\square$

We introduce now two special families of Gaussian monoids and groups.

If M is a right Gaussian monoid, and a, b belong to M, we use $a \setminus_R b$ to denote the unique element c that satisfies $bc = a \vee_R b$. Symmetrically, if M is a left Gaussian monoid, $a \setminus_L b$ denotes the element c that satisfies $ca = a \vee_L b$.

DEFINITION. A right Gaussian monoid is *right small* if there exists a finite subset of M that generates M and is closed under $\setminus_R$, i.e., $a \setminus_R b$ belongs to M whenever a and b

do. *Left small* left Gaussian monoids are defined symmetrically. A Gaussian monoid is *small* if it is both left and right small. A *small Gaussian group* is the group of fractions of a small Gaussian monoid.

DEFINITION. Let M be a Gaussian monoid. We denote by Δ_R the right l.c.m. of all atoms of M and call it the *right fundamental element* of M. The left divisors of Δ_R are called *right simple elements* of M. Similarly, we denote by Δ_L the left l.c.m. of all atoms and call it the *left fundamental element* of M. The right divisors of Δ_L are called *left simple elements*.

DEFINITION. A Gaussian monoid M is a *Garside monoid* if the set of right simple elements is equal to the set of left simple elements; these elements are then called *simple elements*. In that case, Δ_L is equal to Δ_R, it is denoted by Δ, and is called the *fundamental element* of M. A *Garside group* is the group of fractions of a Garside monoid.

PROPOSITION 2.5. *Every Garside monoid is a small Gaussian monoid—thus every Garside group is a small Gaussian group.*

Proof. Assume that M is a Garside monoid, and let a, b be simple elements of M. Then $a \vee_R b$ is right simple, and there exists c satisfying

$$\Delta = (a \vee_R b)c = b(a \setminus_R b)c.$$

So $(a \setminus_R b)c$ is left simple, hence right simple, and, therefore, $a \setminus_R b$ is (right) simple. This shows that the set of all simple elements of M, which is finite by Proposition 2.3, is closed under the operation $\setminus_R$. The argument is similar for the operation $\setminus_L$. □

PROPOSITION 2.6. *Let M be a Garside monoid, and let S be the set of its atoms. There exists a permutation $\delta : S \to S$ satisfying*

$$\Delta \cdot x = \delta(x) \cdot \Delta$$

for all x in S. In particular, if n is the order of δ, then Δ^n lies in the center of the Garside group defined by M.

Proof. Let a be a simple element of M. There exists a simple element a' satisfying $\Delta = a'a$. There exists another simple element $\delta(a)$ satisfying $\Delta = \delta(a)a'$. Then we have

$$\Delta \cdot a = \delta(a) \cdot a' \cdot a = \delta(a) \cdot \Delta \; . \tag{2.3}$$

By left and right cancellativity, the mapping δ is well-defined and injective. By Proposition 2.3, there are only finitely many simple elements, thus δ is a permutation of the simple elements. The value of $\delta(a)$ is completely determined by (2.3), thus, $a = bc$ implies $\delta(a) = \delta(b)\delta(c)$. So, δ maps non-atoms to non-atoms, therefore maps atoms to atoms, thus induces a permutation of S. □

Example #1 (*Artin groups*). Let S be a finite set. A *Coxeter matrix* over S is a matrix $M = (m_{s,t})_{s,t \in S}$ indexed by the elements of S and satisfying:

i) $m_{s,s} = 1$ for $s \in S$;

ii) $m_{s,t} = m_{t,s} \in \{2, 3, 4, \dots, \infty\}$ for $s, t \in S$, $s \neq t$.

The *Coxeter group* associated with M (or with Γ) is:

$$W = \langle S \mid s^2 = 1 \text{ (for } s \in S),\ (st)^{m_{s,t}} = 1 \text{ (for } s, t \in S,\ s \neq t,\ m_{s,t} < \infty) \rangle \ .$$

The *Artin monoid* and the *Artin group* associated with M (or with Γ) are respectively the monoid A_+ and the group A defined by the presentation

$$\langle S \mid \mathrm{prod}(s, t; m_{s,t}) = \mathrm{prod}(t, s; m_{s,t}) \text{ if } m_{s,t} < \infty \rangle \ ,$$

where $\mathrm{prod}(s, t; m)$ stands for $(st)^{m/2}$ if m is even, and for $(st)^{(m-1)/2}s$ if m is odd. The monoid A_+ (resp. the group A) is said to be of *finite Coxeter type* if W is finite.

The defining relations of A_+ are homogeneous, thus A_+ is atomic, the norm is equal to the word length, and the atoms are the elements of S.

By [5], A_+ is a Gaussian monoid if and only if it is of finite Coxeter type. In that case, A_+ embeds in A, and A is the Gaussian group defined by A_+.

Finite Coxeter type Artin groups are actually Garside groups. The set of simple elements is $\{\tau(w); w \in W\}$ and the fundamental element is $\Delta = \tau(w_0)$, where w_0 is the element of maximal length in W, and τ is the natural set-section of the canonical projection of A onto W defined as follows. Let w in W. We choose a reduced expression $w = s_1 \dots s_r$ of w and we map w to the element $s_1 \dots s_r$ of A_+. By Tits' solution of the word problem for Coxeter groups [30], this definition does not depend on the choice of the reduced expression of w.

We will see other examples of Garside groups in Section 5. However, we first need to introduce reversing processes in Section 3 and to give in Section 4 some criteria to check whether a given monoid is a Garside monoid.

Remark. In this paper, we only consider the case of finitely generated monoids and groups. However, most of the subsequent results about Gaussian groups and some of the results about Garside groups can be extended to more general cases provided atomicity remains satisfied, as is the case for the infinite braid group B_∞, or for the groups investigated in [13] and [14].

3. Reversing processes

We give in this section basic definitions on reversing processes and a summary of those results of [14] that we will need in this paper. We refer to [14] for the proofs. We recall from Section 1 the following definition.

Definition. Let S be a finite set. A *complement* on S is a mapping

$$f : S \times S \to S^*$$

such that $f(x, x)$ is the empty word for all x in S. The *monoid associated with f on the right* is the monoid $M_R(S, f)$ that admits the presentation

$$\langle S \mid xf(y, x) = yf(x, y) \text{ for } x, y \in S\rangle \ , \tag{3.1}$$

namely, the monoid $S^*/\equiv_R^f$, where $\equiv_R^f$ is the congruence relation on S^* generated by the pairs $(xf(y, x), yf(x, y))$, for x, y in S. Similarly, $G_R(S, f)$ is the group that admits the previous presentation. One can also *associate with f on the left* the monoid $M_L(S, f)$ and the group $G_L(S, f)$, both given by the presentation

$$\langle S \mid f(x, y)x = f(y, x)y \text{ for } x, y \in S\rangle \ .$$

Definition. A mapping $\nu : S^* \to \mathbf{N}$ is a *right norm* for the complement f if

$$\nu(u) < \nu(xu) \text{ and } \nu(uxf(y, x)v) = \nu(uyf(x, y)v) \tag{3.2}$$

holds for all x, y in S, and for all u, v in S^*. We say that (S, f) satisfies *Condition I_R* if S^* admits a right norm for the complement f.

Proposition 3.1. *The monoid $M_R(S, f)$ is atomic if and only if (S, f) satisfies Condition I_R.*

Proof. Assume that there exists a mapping ν satisfying (3.2). Using the definition of the congruence relation $\equiv_R^f$ and a trivial induction, we see that $u \equiv_R^f v$ implies $\nu(u) = \nu(v)$, so that ν induces a well-defined mapping on $M_R(S, f)$. This mapping satisfies Condition (i) of Proposition 2.1. Conversely, if M is atomic, then the mapping ν defined on S^* by $\nu(u) = \|\overline{u}\|$ satisfies (3.2). □

Definition. A word w in $(S \cup S^{-1})^*$ is *f-reversible (on the right) in one step* to a word w' if w' is obtained from w by replacing some subword $x^{-1}y$ (with x, y in S) with the corresponding word $f(y,x)f(x,y)^{-1}$. For $p \geq 0$, w is *f-reversible (on the right) in p steps* to w' if there exists a length $p+1$ sequence in $(S \cup S^{-1})^*$ from w to w' such that every term is f-reversible to the next one in one step.

The f-reversing process can continue as long as the current word contains a pair $x^{-1}y$. When no pair of this form remains, namely, when the word has the form uv^{-1} with u and v positive words, we say that the f-reversing process was *successful* for the initial word w. At this point, some ambiguity could occur in our definition as a given word may contain several reversing patterns of the form $x^{-1}y$ and we have not given a rule for choosing the order of the reversing steps. The next result shows that this does not matter.

PROPOSITION 3.2 [14, Lemma 1.1]. *Assume that there is at least one way to reverse the word w into some word uv^{-1}, where u, v are positive words. Then any sequence of reversing transformations starting from w leads to uv^{-1} in the same number of steps.* $\square$

DEFINITION. For w in $(S \cup S^{-1})^*$, $R_R^f(w)$ denotes the unique word of the form uv^{-1}, with u, v positive words, that is obtained from w by the right f-reversing process, if such a word exists. In that case, the *right f-numerator* of w, denoted by $N_R^f(w)$, is the word u, and the *right f-denominator* of w, denoted by $D_R^f(w)$, is the word v. For u, v in S^*, we denote by $C_R^f(u,v)$ the right f-numerator of $v^{-1}u$, if it exists.

If $R_R^f(w)$ exists, then $R_R^f(w^{-1})$ also exists and is equal to $R_R^f(w)^{-1}$, and we have $N_R^f(w^{-1}) = D_R^f(w)$ and $D_R^f(w^{-1}) = N_R^f(w)$. In particular, for u, v in S^*, if $C_R^f(u,v)$ exists, then $C_R^f(v,u)$ also exists and $R_R^f(v^{-1}u)$ is equal to $C_R^f(u,v)C_R^f(v,u)^{-1}$.

DEFINITION. We say that (S,f) satisfies *Condition II_R* if: for all x, y, z in S, either the words $C_R^f(z, xf(y,x))$ and $C_R^f(z, yf(x,y))$ both exist and are $\equiv_R^f$-equivalent, or neither of them exists.

DEFINITION. We say that (S,f) satisfies *Condition III_R* if $C_R^f(u,v)$ exists for all u, v in S^*. Note that (S,f) satisfies Condition III_R if and only if $R_R^f(w)$ exists for all w in $(S \cup S^{-1})^*$.

PROPOSITION 3.3 [14, Lemma 1.4]. *Assume that (S,f) satisfies Conditions I_R and II_R. Then, for u, v, u_1, v_1 in S^*, $uu_1 \equiv_R^f vv_1$ holds if and only if the words $C_R^f(u,v)$ and $C_R^f(v,u)$ exist and there exists a word w in S^* satisfying $u_1 \equiv_R^f C_R^f(v,u)w$ and $v_1 \equiv_R^f C_R^f(u,v)w$.* $\square$

(The proof of [14] uses the hypothesis that the elements of S have norm 1. This additional hypothesis can be dropped by resorting both to the length and the norm in the inductive argument.)

PROPOSITION 3.4 [14, Lemma 1.5(i)]. *Assume that (S, f) satisfies Conditions I_R and II_R. Let u, v be arbitrary words in S^*. The class of u in $M_R(S, f)$ is a left divisor of the class of v if and only if $C_R^f(u, v)$ exists and is empty. In particular, u and v represent the same element of $M_R(S, f)$ if and only if both $C_R^f(u, v)$ and $C_R^f(v, u)$ exist and are empty.* □

PROPOSITION 3.5 [14, Lemma 1.5(ii)]. *Assume that (S, f) satisfies Conditions I_R and II_R. Then the operation C_R^f is compatible with the congruence relation $\equiv_R^f$, namely, $u \equiv_R^f u'$ and $v \equiv_R^f v'$ hold, and $C_R^f(u, v)$ exists, then $C_R^f(u', v')$ also exists and is $\equiv_R^f$-equivalent to $C_R^f(u, v)$.* □

PROPOSITION 3.6 [14, Proposition 1.6]. *Assume that (S, f) satisfies Conditions I_R and II_R. Then the monoid $M_R(S, f)$ has the left cancellation property.* □

PROPOSITION 3.7 [14, Lemma 1.7]. *Assume that (S, f) satisfies Conditions I_R, II_R, and III_R. Let G be the group of fractions of $M_R(S, f)$. Two words w and w' in $(S \cup S^{-1})^*$ represent the same element of G if and only if there exist two positive words u and u' in S^* satisfying $N_R^f(w)u \equiv_R^f N_R^f(w')u'$ and $D_R^f(w)u \equiv_R^f D_R^f(w')u'$.* □

The following theorem is a direct consequence of the previous results.

THEOREM 3.8. *Let S be a finite set, and let f be a complement on S. If (S, f) satisfies Conditions I_R, II_R, and III_R, then $M_R(S, f)$ is a right Gaussian monoid.* □

DEFINITION. Assume that f is a complement on S. A set of positive words S' is *closed under C_R^f* if, for all u, v in S', $C_R^f(u, v)$ exists and belongs to S'. We say that (S, f) satisfies *Condition III_R^+* if there exists a finite subset S' of S^* that includes S and is closed under C_R^f. Note that Condition III_R^+ holds if and only if the closure of S under C_R^f exists and is finite.

LEMMA 3.9. *i) Assume that f is a complement on S, and S' is a subset of S^* that includes S and is closed under C_R^f. Then (S, f) satisfies Condition III_R.*

ii) Assume, in addition, that the length of every word in S' is bounded above by L, and that the number of steps needed to reverse a word of the form $u^{-1}v$ with u, v in S' is bounded above by N. Then the f-reversing of a word w of length ℓ in $(S \cup S^{-1})^*$ ends within at most $N\ell^2/4$ steps with a word of length at most $L\ell$.

Proof. Assume that w can be written

$$w = u_1^{e_1} \dots u_\ell^{e_\ell},$$

where each word u_i is a positive word belonging to S', and e_i is ± 1. Let p be the number of e_i's equal to 1. A simple inductive argument shows that $R_R^f(w)$ exists and has the form

$$R_R^f(w) = v_1 \dots v_p v_{p+1}^{-1} \dots v_\ell^{-1},$$

where, for each j, v_j is an element of S', and that the f-reversing of w decomposes into $p(\ell - p)$ f-reversings of words of the form $w_1^{-1} w_2$ with w_1, w_2 in S'. So f-reversing of w is always successful, and, in the case when L and N are finite, we obtain the bounds of Lemma 3.9.ii since $p(\ell - p) \le \ell^2/4$ always holds. □

In particular, Condition III_R^+ implies Condition III_R.

THEOREM 3.10. *Let S be a finite set, and let f be a complement on S. If (S, f) satisfies Conditions I_R, II_R, and III_R^+, then $M_R(S, f)$ is a right small right Gaussian monoid.*

Proof. Assume that (S, f) satisfies Conditions I_R, II_R and III_R^+, and that S' is a set of positive words that includes S and is closed under C_R^f. By Theorem 3.8, $M_R(S, f)$ is a right Gaussian monoid. By Proposition 3.3, for u, v in S^*, $vC_R^f(u, v)$ represents the right l.c.m. of the elements $\overline{u}$ and $\overline{v}$, so $C_R^f(u, v)$ represents the element $\overline{u} \backslash_R \overline{v}$. So the subset of $M_R(S, f)$ consisting of all elements represented by words in S' is closed under the operation $\backslash_R$. □

Everything we have said so far about left divisibility of course holds *mutatis mutandis* for right divisibility. We then speak about the left f-reversing process, about the functions R_L^f and C_L^f, and about Conditions I_L, II_L, III_L, and III_L^+.

COROLLARY 3.11. *Let M be a monoid, let S be a finite generating set of M, and let f, g be two complements on S such that M admits both presentations:*

$$\langle S \mid xf(y,x) = yf(x,y),\ x, y \in S \rangle \text{ and } \langle S \mid g(x,y)x = g(y,x)y,\ x, y \in S \rangle .$$

If (S, f) satisfies Conditions I_R, II_R, and III_R (resp. III_R^+), and (S, g) satisfies Conditions I_L, II_L, and III_L (resp. III_L^+), then M is a Gaussian monoid (resp. a small Gaussian monoid). □

Observe that, although reversing processes are quite effective, there is no general algorithmic method for establishing that a given pair (S, f) satisfies Condition III_R; a systematic verification would entail infinitely many reversings. On the other hand, the verification of Condition III_R^+ is easier: it suffices to start with the set S and to close it inductively under C_R^f. If the condition fails, we shall never know it, but, if it holds, we shall know it after a finite number of computation steps.

The situation is similar with Condition II_R: as it stands, it is not clear how to verify it systematically, for we have no way to decide whether two given words are or not $\equiv_R^f$-equivalent. However, we can replace Condition II_R with a nearly equivalent condition which does not resort to $\equiv_R^f$.

DEFINITION. We say that (S, f) satisfies *Condition* II_R^+ if: for all x, y, z in S, the word

$$C_R^f(C_R^f(z, xf(y,x)), C_R^f(z, yf(x,y))) \tag{3.3}$$

exists and is empty.

PROPOSITION 3.12. *Condition II_R^+ implies Condition II_R. Conversely, if (S, f) satisfies Conditions I_R, II_R and III_R, then it satisfies Condition II_R^+ as well.*

Proof. Assume that (S, f) satisfies II_R^+. The hypothesis that $C_R^f(u, v)$ and $C_R^f(v, u)$ exist and are empty always implies that u and v are $\equiv_R^f$-equivalent (without any assumption about f). So II_R^+ implies that, for every x, y, z in S, the words $C_R^f(z, xf(y,x))$ and $C_R^f(z, yf(x,y))$ exist and are $\equiv_R^f$-equivalent. Hence II_R holds.

Conversely, assume that (S, f) satisfies I_R, II_R and III_R. By III_R, the words $C_R^f(z, xf(y,x))$ and $C_R^f(z, yf(x,y))$ exist, and, by Proposition 3.5, they are $\equiv_R^f$-equivalent. Hence, by Proposition 3.4, the complement (3.3) is empty. □

4. PRESENTATIONS

We have stated in Theorems 3.8 and 3.10 sufficient conditions for a monoid given by a complemented presentation to be a (small) Gaussian monoid. In this section, we show that these conditions are also necessary. We also determine in terms of presentations necessary and sufficient conditions for a monoid to be a Garside monoid. This of course also applies to Gaussian groups and to Garside groups.

Our first step (Theorem 4.1) is to show that Gaussian monoids can always be presented using complements.

DEFINITION. Let M be a right Gaussian monoid, and let S be a finite generating set of M. A *right l.c.m. selector* on S in M is a complement f on S such that $xf(y,x)$ and

$yf(x,y)$ both represent $x \vee_R y$ in M for all x, y in S. *Left l.c.m. selectors* are defined symmetrically for left Gaussian monoids.

THEOREM 4.1. *Let M be a right Gaussian monoid, let S be a finite generating set of M, and let f be a right l.c.m. selector on S in M. Then M is isomorphic to the monoid $M_R(S,f)$.*

Proof. By hypothesis, there exists a congruence relation $\equiv$ on S^* such that M is $S^*/\equiv$. By construction, for every pair (x,y) in $S \times S$, the words $xf(y,x)$ and $yf(x,y)$ represent the left l.c.m. of x and y in M, so $xf(y,x) \equiv yf(x,y)$ holds. Since the pairs $(xf(y,x), yf(x,y))$ generate the congruence relation $\equiv_R^f$, we deduce that $u \equiv_R^f v$ implies $u \equiv v$, namely, that the monoid M is a quotient of the monoid $M_R(S,f)$.

We use now the hypothesis that M is atomic to prove that the surjective homomorphism associated with this quotient is actually an isomorphism. To this end, we define the norm of a positive word u as the norm of its class in M, and we prove inductively on n that: if u and v have norm at most n, then $u \equiv v$ implies $u \equiv_R^f v$. If n is 0, then u and v must be the empty word, and the result is obvious. Otherwise, due to the existence of the norm, neither u nor v may be the the empty word. So, write u as xu_1 and v as yv_1. By construction, the class of $xf(y,x)$ in M is the smallest common right multiple of x and y, and the class of xu_1 is a common right multiple of x and y as well. So, there must exist a positive word w satisfying $u_1 \equiv f(y,x)w$ and $v_1 \equiv f(x,y)w$. By induction hypothesis, $u_1 \equiv_R^f f(y,x)w$ and $v_1 \equiv_R^f f(x,y)w$ hold, thus we get

$$u = xu_1 \equiv_R^f xf(y,x)w \equiv_R^f yf(x,y)w \equiv_R^f yv_1 = v \ ,$$

as we wished. Note that the case $x = y$ is also covered in the previous argument. □

THEOREM 4.2. *Let M be a right Gaussian monoid, let S be an arbitrary finite generating set of M, and let f be an arbitrary right l.c.m. selector on S in M. Then (S,f) satisfies Conditions I_R, II_R, and III_R. If, in addition, M is left small, then (S,f) satisfies Condition III_R^+.*

The following lemma is a preliminary result to the proof of Theorem 4.2.

LEMMA 4.3. *Let M be a right Gaussian monoid, let S be a finite generating set of M, and let f be a right l.c.m. selector on S in M. Then $C_R^f(u,v)$ exists, $vC_R^f(u,v)$ represents $\overline{u} \vee_R \overline{v}$, and $C_R(u,v)$ represents $\overline{u} \setminus_R \overline{v}$, for all u, v in S^*.*

Proof. We prove inductively on n that: if $\|\overline{u} \vee_R \overline{v}\| \leq n$ holds, then $C_R^f(u,v)$ exists and $vC_R^f(u,v)$ represents $\overline{u} \vee_R \overline{v}$. If n is 0, the only possibility is that u and v are the empty word, and everything is obvious. Assume $n \geq 1$. If either u or v is the empty word, then everything is obvious again. So, assume $u = xu_1$ and $v = yv_1$, where x and y belong to S. By hypothesis, $\overline{u} \vee_R \overline{v}$ is a common right multiple of x and y, thus $x \vee_R y$ divides $\overline{u} \vee_R \overline{v}$. By hypothesis, $x \vee_R y$ is both the class of $xf(y,x)$ and the class of $yf(x,y)$. By construction, $\overline{u} \vee_R \overline{v}$ is a common multiple of $\overline{xu_1}$ and $\overline{xf(y,x)}$, so the l.c.m. of these elements is a left divisor of $\overline{u} \vee_R \overline{v}$. We have

$$\overline{xu_1} \vee_R \overline{xf(y,x)} = x(\overline{u_1} \vee_R \overline{f(y,x)}) \ .$$

This shows that the norm of $\overline{u_1} \vee_R \overline{f(y,x)}$ is at most $n-1$. So, the induction hypothesis shows that the words $C_R^f(u_1, f(y,x))$ and $C_R^f(f(y,x), u_1)$ exist, and that $uC_R^f(f(y,x), u_1)$ represents $\overline{u} \vee_R \overline{xf(y,x)} = \overline{u} \vee_R y$. A symmetric argument shows that the words $C_R^f(v_1, f(x,y))$ and $C_R^f(f(x,y), v_1)$ exist and that $vC_R^f(f(x,y), v_1)$ represents $x \vee_R \overline{v}$.

Let w be $xf(y,x)$, let u_2 be $C_R^f(u_1, f(y,x))$, and let v_2 be $C_R^f(v_1, f(x,y))$. By construction, $\overline{u} \vee_R \overline{v}$ is the right l.c.m. of $\overline{wu_2}$ and $\overline{wv_2}$ (which are $\overline{u} \vee_R y$ and $x \vee_R \overline{v}$ respectively). Again, the right l.c.m. of $\overline{u_2}$ and $\overline{v_2}$ has a norm strictly less than n. So, $C_R^f(u_2, v_2)$ and $C_R^f(v_2, u_2)$ exist and $v_2C_R^f(u_2, v_2)$ represents $\overline{u_2} \vee_R \overline{v_2}$.

The word $v^{-1}u$ is f-reversible to

$$v_1^{-1} \cdot f(x,y) \cdot f(y,x)^{-1} \cdot u_1 \ ,$$

and then to

$$C_R^f(f(x,y), v_1) \cdot C_R^f(v_1, f(x,y))^{-1} \cdot C_R^f(u_1, f(y,x)) \cdot C_R^f(f(y,x), u_1)^{-1},$$

which is $C_R^f(f(x,y), v_1) \cdot v_2^{-1} \cdot u_2 \cdot C_R^f(f(y,x), u_1)^{-1}$. The latter word in turn is f-reversible to

$$C_R^f(f(x,y), v_1) \cdot C_R^f(u_2, v_2) \cdot C_R^f(v_2, u_2)^{-1} \cdot C_R^f(f(y,x), u_1)^{-1} \ .$$

So, $C_R^f(u,v)$ exists and is equal to

$$C_R^f(f(x,y), v_1) \cdot C_R^f(u_2, v_2) \ .$$

Now, we have

$$\begin{aligned} \overline{v} \cdot \overline{C_R^f(u,v)} &= \overline{v} \cdot \overline{C_R^f(f(x,y), v_1)} \cdot \overline{C_R^f(u_2, v_2)} = (\overline{v} \vee_R y) \cdot \overline{C_R^f(u_2, v_2)} \\ &= \overline{w} \cdot \overline{v}_2 \cdot \overline{C_R^f(u_2, v_2)} = \overline{w} \cdot (\overline{u_2} \vee_R \overline{v_2}) = \overline{u} \vee_R \overline{v}. \end{aligned}$$

This completes the proof. □

Proof of Theorem 4.2. The pair (S, f) satisfies Condition I_R by Proposition 3.1. By the previous lemma, (S, f) satisfies Condition III_R. So, it remains to show that: if

x, y, z are elements of S, then $C_R^f(z, xf(y,x))$ and $C_R^f(z, yf(x,y))$ are $\equiv_R^f$-equivalent. Now, $xf(y,x)$ represents the right l.c.m. of x and y, and $xf(y,x)C_R^f(z, xf(y,x))$ represents the right l.c.m. of $x \vee_R y$ and z, namely, the right l.c.m. of x, y, and z. Similarly, $yf(x,y)C_R^f(z, yf(x,y))$ represents the right l.c.m. of x, y, and z. The words $xf(y,x)$ and $yf(x,y)$ are equivalent as well, so, by left cancellativity, we conclude that $C_R^f(z, xf(y,x))$ and $C_R^f(z, yf(x,y))$ are equivalent.

Assume now in addition that B is a finite subset of M that includes S and is closed under the operation $\backslash_R$. Let S' be the set of all positive words that represent elements of B. Because B is finite and, for every a in M, the lengths of the expressions of a are bounded by $\|a\|$, the set S' is finite. Now, for u, v in S', the word $C_R^f(v,u)$ represents $\overline{v} \backslash_R \overline{u}$, so it belongs to S'. Hence the set S' witnesses that Condition III_R^+ holds. □

Let us now consider the case of Garside monoids. We define below Conditions IV_{LR} and IV_{RL} which refine Conditions III_R^+ and III_L^+, and show that Garside monoids are characterized by the conjunction of Conditions I_R, II_R, II_L, IV_{LR}, and IV_{RL} (Theorems 4.4 and 4.9).

Definition. Assume that f is a complement on S. For $x_1, \ldots, x_k$ in S, let $J_R^f(x_1, \ldots, x_k)$ denote the word inductively defined (if it exists) by

$$J_R^f(x_1, \ldots, x_k) = \begin{cases} x_1 & \text{for } k = 1, \\ J_R^f(x_1, \ldots, x_{k-1}) C_R^f(x_k, J_R^f(x_1, \ldots, x_{k-1})) & \text{otherwise.} \end{cases}$$

The word $J_L^g(x_1, \ldots, x_k)$ is defined symmetrically in the same way.

Definition. We say that (S, f, g) satisfies *Condition* IV_{LR} if there is an enumeration $x_1, \ldots, x_n$ of the elements of S such that $J_R^f(x_1, \ldots, x_n)$ exists and such that

$$C_L^g(J_R^f(x_1, \ldots, x_n)\, x_i, J_R^f(x_1, \ldots, x_n))$$

exists and is the empty word for every x_i in S. *Condition* IV_{RL} is defined symmetrically.

So, if (S, f) satisfies Conditions I_R and II_R, then $J_R^f(x_1, \ldots, x_k)$ represents the right l.c.m. of $x_1, \ldots, x_k$ in $M_R(S, f)$, if it exists. If, in addition, $S = \{x_1, \ldots, x_n\}$ is the set of atoms of $M_R(S, f)$ and (S, f, g) satisfies Condition IV_{LR}, then the right l.c.m. Δ_L of the atoms exists and is represented by $J_R^f(x_1, \ldots, x_n)$.

Theorem 4.4. *Let S be a finite set, and let f, g be complements on S. Assume that*

i) The monoids $M_R(S, f)$ and $M_L(S, g)$ coincide;

ii) The set of atoms of $M_R(S,f)$ is S;
iii) The pair (S,f) satisfies Conditions I_R and II_R;
iv) The pair (S,g) satisfies Conditions (I_L and) II_L;
v) The triple (S,f,g) satisfies Conditions IV_{LR} and IV_{RL}.
Then $M_R(S,f)$ is a Garside monoid.

The following lemmas 4.5–4.8 are preliminary results to the proof of Theorem 4.4. We write M for the monoid both presented as $M_R(S,f)$ and $M_L(S,g)$, and we assume until the end of the proof of Theorem 4.4 that S is the set of atoms of M, that M is atomic—i.e., that (S,f) satisfies Condition I_R and, equivalently, that (S,g) satisfies Condition I_L—and that (S,f) and (S,g) satisfy respectively Condition II_R and II_L.

LEMMA 4.5. *Assume that (S,f,g) satisfies Condition IV_{LR}. Then there exists a permutation $\delta : S \to S$ such that*

$$\Delta_R \cdot x = \delta(x) \cdot \Delta_R$$

holds for all x in S.

Proof. Let x be an atom. Condition IV_{LR} says that $C_L^g(J_R^f(x_1,\ldots,x_n)x, J_R^f(x_1,\ldots,x_n))$ exists and is empty. By Proposition 3.4, this means that Δ_R is a right divisor of $\Delta_R x$. So, there exists $\delta(x)$ in M such that $\Delta_R x$ is equal to $\delta(x)\Delta_R$. By Proposition 3.6, the monoid M has the right cancellation property, thus $\delta(x)$ is well-defined. We immediately deduce, for every product of atoms, the equality

$$\Delta_R \cdot x_1 \ldots x_k = \delta(x_1) \ldots \delta(x_k) \cdot \Delta_R \ .$$

So, we can extend δ to an endomorphism of M such that

$$\Delta_R \cdot a = \delta(a) \cdot \Delta_R \tag{4.1}$$

always holds. The fact that M is left and right cancellative guarantees that δ is well-defined and injective. Note that (4.1) uniquely defines the value of $\delta(a)$. In particular, $\Delta_R\Delta_R = \Delta_R\Delta_R$ implies $\delta(\Delta_R) = \Delta_R$. Now, if a is a left divisor of Δ_R, then $\delta(a)$ is a left divisor of $\delta(\Delta_R) = \Delta_R$. So, right simple elements are globally preserved under δ, and, because δ is injective and there are finitely many left simple elements (Proposition 2.3), we conclude that δ induces a permutation of the right simple elements. Moreover, this permutation preserves left divisibility, hence maps non-atoms to non-atoms, therefore maps atoms to atoms. So, it induces a permutation of S. □

LEMMA 4.6. *Assume that (S,f,g) satisfies Conditions IV_{LR} and IV_{RL}. Then Δ_L is equal to Δ_R.*

Proof. Let x be an atom. By Lemma 4.5, there exists an atom $\delta(x)$ such that $\Delta_R x$ is equal to $\delta(x)\Delta_R$. Since Δ_R is the right l.c.m. of all atoms, there exists an element a in M satisfying $\Delta_R = \delta(x)a$. By left cancellativity, we have $ax = \Delta_R$, thus x divides Δ_R on the right. Since Δ_L is the left l.c.m. of all atoms, it follows that Δ_L divides Δ_R on the right, and, therefore, that $\|\Delta_L\| \leq \|\Delta_R\|$ holds. Similarly, Δ_R divides Δ_L on the left and $\|\Delta_R\| \leq \|\Delta_L\|$ holds, thus Δ_L is equal to Δ_R. □

Whenever (S, f, g) satisfies Conditions IV_{LR} and IV_{RL}, we use Δ to denote the common value of Δ_R and Δ_L in M.

LEMMA 4.7. *Assume that (S, f, g) satisfies Conditions IV_{LR} and IV_{RL}. Let a be an element of M. Then the following conditions are equivalent.*

i) a is a right simple element.

ii) a is a left simple element.

iii) There exists a' and a'' in M such that Δ is equal to $a'aa''$.

Proof. Let a be a right simple element. From the proof of Lemma 4.5, we know that there exists a right simple element $\delta(a)$ satisfying $\Delta a = \delta(a)\Delta$. By definition, there exists a' in M satisfying $\delta(a)a' = \Delta$. By left cancellativity, $\Delta = a'a$, thus a is a lrft simple element. This shows that (i) implies (ii). Similarly, (ii) implies (i). It is obvious that either (i) or (ii) implies (iii). It remains to show that (iii) implies (i). Assume $\Delta = a'aa''$. Then aa'' is a right divisor of Δ, thus it is a left divisor of Δ as well, therefore a is a left divisor of Δ. □

LEMMA 4.8. *Assume that (S, f, g) satisfies Conditions IV_{LR} and IV_{RL}. Then (S, f) satisfies Condition III_R^+.*

Proof. Assume that u, v are positive words that represent simple elements. There exist positive words u_1, v_1 satisfying

$$uu_1 \equiv_R^f vv_1 \equiv_R^f J_R^f(x_1, \ldots, x_n).$$

By Proposition 3.3, $C_R^f(u, v)$ exists and there is a positive word w satisfying

$$vC_R^f(u, v)w \equiv_R^f J_R^f(x_1, \ldots, x_n) \ . \tag{4.2}$$

By Lemma 4.7, the element a represented by $C_R^f(u, v)$ is simple, as (4.2) gives $\overline{v}\, a\, \overline{w} = \Delta$. Hence the set of all expressions of simple elements of M, which is finite by Proposition 2.3, is closed under C_R^f. □

Proof of Theorem 4.4. The pair (S, f) satisfies Condition III_R^+ by Lemma 4.8. Similarly, (S, g) satisfies Condition III_L^+. So, M is a small Gaussian monoid by Theorem 3.10. Finally, M is a Garside monoid by Lemma 4.7. □

THEOREM 4.9. *Let M be a Garside monoid, let S be the set of atoms of M, let f be a right l.c.m. selector on S in M, and let g be a left l.c.m. selector on S in M. Then (S, f, g) satisfies Conditions IV_{LR} and IV_{RL}.*

Proof. Let $x_1, \ldots, x_n$ be an enumeration of the atoms of M. Lemma 4.3 and an easy inductive argument show that $J_R^f(x_1, \ldots, x_k)$ exists and represents the right l.c.m. of $x_1, \ldots, x_k$. In particular, $J_R^f(x_1, \ldots, x_n)$ exists and represents $\Delta_R = \Delta$. Now, let x be an atom. Since $\Delta x = \delta(x)\Delta$ holds (Proposition 2.5), Δ divides Δx on the right, thus, by Proposition 3.4, $C_L^g(J_R^f(x_1, \ldots, x_n)x, J_R^f(x_1, \ldots, x_n))$ exists and is empty. □

5. Examples

We have seen that finite Coxeter type Artin groups are Garside groups. Although the definition in terms of l.c.m.'s seems to be rather natural, we have found only few examples of Gaussian groups and Garside groups in the literature. However, the criterions of Section 4 enable us to construct a number of new examples.

The first remark is:

LEMMA 5.1. *Assume that S is a two-element set, and that f is any complement on S. Then (S, f) satisfies Conditions II_R and II_L.*

Proof. Assume $S = \{x, y\}$. The only thing we have to verify for II_R is that the words $C_R^f(x, xf(y, x))$ and $C_R^f(x, yf(x, y))$ either both exist and are equivalent, or that neither of them exists. Now a direct computation gives

$$C_R^f(x, xf(y, x)) = C_R^f(\varepsilon, f(y, x)) = \varepsilon,$$
$$C_R^f(x, yf(x, y)) = C_R^f(f(x, y), f(x, y)) = \varepsilon.$$

The argument is similar for Condition II_L. □

EXAMPLE #2. For p, q positive integers, let $G_{p,q}$ be the group with presentation

$$\langle\ x, y \ \mid\ x^p = yx^q y\ \rangle\ . \tag{5.1}$$

We claim that, for $p > q$, $G_{p,q}$ is a small Gaussian group, but not a Garside group.

Let S be the set $\{x, y\}$, and let $M_{p,q}$ be the monoid that admits (5.1) as a presentation. Then $M_{p,q}$ is both $M_R(S, f)$ and $M_L(S, g)$ where the complements f and g are defined by

$$f(y, x) = x^{p-1}, \quad f(x, y) = x^q y, \quad g(x, y) = x^{p-1}, \quad g(y, x) = yx^q.$$

We shall verify that (S, f) satisfies Conditions I_R, II_R and III_R^+ when $p > q$ holds. Observe that, for $p \leq q$, $M_{p,q}$ is certainly not atomic, since we have

$$x^p = yx^q y = yyx^q yx^{q-p} y = \cdots = y^{k+1} x^q y (x^{q-p} y)^k$$

for every k. We henceforth assume $p > q$.

For I_R, unless $p = q + 2$, the relation is not homogeneous, and we cannot simply use the length as the mapping ν. However, it is clear that the mapping ν defined by $\nu(\varepsilon) = 0$, $\nu(x) = 2$, $\nu(y) = p - q$ and $\nu(uv) = \nu(u) + \nu(v)$ is a right norm for f.

Condition II_R is automatically verified by Lemma 5.1.

For Condition III_R^+, we claim that the closure of S under the complement C_R^f is the set

$$S' = \{x^i ; 0 \leq i < p\} \cup \{x^j yx^k ; 0 \leq j, k \leq q\}.$$

This results from the following explicit equalities, which are verified directly:

$$C_R^f(x^i, x^{i'}) = x^{\sup(i-i',0)},$$

$$C_R^f(x^i, x^j yx^k) = \begin{cases} \varepsilon & \text{for } i \leq j, \\ x^{q-k} y & \text{otherwise,} \end{cases}$$

$$C_R^f(x^j yx^k, x^{j'} yx^{k'}) = \begin{cases} x^{q-k'} yx^{\sup(j-j',0)} & \text{for } j \neq j', \\ x^{\sup(k-k',0)} & \text{for } j = j'. \end{cases}$$

Due to the symmetry in the defining relations, it is obvious that the complement g satisfies Conditions I_L, II_L and III_L^+. By Theorem 3.10, we conclude that $M_{p,q}$ is a small Gaussian monoid, and that $G_{p,q}$ is a Gaussian group.

This group is not a Garside group. Indeed, x and y are atoms in $M_{p,q}$, and we immediately find $\Delta_R = \Delta_L = x^p = yx^q y$, corresponding to $J_R^f(x, y) = x^p$. Now Condition IV_{LR} fails, for we find

$$C_L^g(x^p y, x^p) = x^q.$$

This failure corresponds to the fact that the element represented by yx^q is right simple in $M_{p,q}$, but it is not left simple.

Example #3. For p a positive integer, let M_p be the monoid with presentation

$$\langle\ x, y \ \mid\ xy^p = yx\ \rangle\ . \tag{5.2}$$

We claim that M_p embeds in its group of fractions, that M_p is a right Gaussian monoid, but, for $p \geq 2$, that M_p is neither a left Gaussian monoid, nor a right small right Gaussian monoid.

It is clear that the monoid M_p is both $M_R(S, f)$ and $M_L(S, g)$, where S is $\{x, y\}$, and f, g are the complements defined by

$$f(x, y) = x, \quad f(y, x) = y^p, \quad g(x, y) = y, \quad g(y, x) = xy^{p-1}.$$

We consider Conditions I_R, II_R and III_R for (S, f). For I_R, we cannot simply define a left norm ν by attributing fixed values to the letters as in Example #2, for the number of letters x is the same in both sides of (5.2). Now, defining inductively ν by $\nu(\varepsilon) = 0$ and

$$\nu(xw) = \nu(w) + 1, \qquad \nu(yw) = \nu(w) + p^{|w|_x},$$

where $|w|_x$ denotes the number of letters x in w, gives a right norm for (S, f). Indeed, we find for every word v

$$\nu(xy^p v) = \nu(v) + p^{|v|_x + 1} + 1 = \nu(yxv),$$

which is enough as $|xy^p v|_x$ and $|yxv|_x$ both are equal to $|v|_x + 1$. Hence (S, f) satisfies Condition I_R.

By Lemma 5.1, it satisfies Condition II_R.

Now, let S' be the set $\{x\} \cup \{y^j; j \geq 0\}$. It is easy to verify that S' is closed under C_R^f, due to the formulas

$$C_R^f(x, y^j) = x, \qquad C_R(y^j, x) = y^{pj}. \tag{5.3}$$

So, by Lemma 3.9, (S, f) satisfies Condition III_R, and, therefore, M_p is a right Gaussian monoid. Now, (5.3) shows that the closure of S under C_R^f contains the word y^{p^k} for every k, so it cannot be finite for $p \geq 2$. So M_p is not right small.

Because M_p is atomic, we know that (S, g) satisfies Condition I_L, and, by Lemma 5.1, it satisfies Condition II_L as well. Hence, by Proposition 3.6, the monoid M_L is left cancellative, and, by Ore's criterion, it embeds in its group of fractions. However (S, g) does not satisfy Condition III_L. Indeed, the word $w = xy^{p-1}x^{-1}$ is g-reversible on the left in two steps to the word $y^{-1}wy$, and, therefore, it is g-reversible in $2k$ steps to $y^{-k}wy^k$ for every k: thus the g-reversing of w cannot be successful.

We turn now to the construction of Garside groups. The following propositions 5.2 and 5.3 provide a machinery to produce infinite families of such groups.

Proposition 5.2. *Consider a finite set $S = \{x_1, \ldots, x_n\}$, n positive words $u_1, \ldots, u_n$ in S^*, and a permutation δ of $\{1, \ldots, n\}$. We assume that:*

i) There exists a mapping ν of S to the positive integers which, when extended to S^* by $\nu(\varepsilon) = 0$ and $\nu(uv) = \nu(u) + \nu(v)$, satisfies

$$\nu(x_1 u_1 x_{\delta(1)}) = \nu(x_2 u_2 x_{\delta(2)}) = \ldots = \nu(x_n u_n x_{\delta(n)}); \tag{5.4}$$

ii) For every index k, there exists an index j satisfying

$$x_k u_k = u_j x_{\delta(j)} \ . \tag{5.5}$$

Let M be the monoid defined by the presentation

$$\langle x_1, \ldots, x_n \mid x_1 u_1 x_{\delta(1)} = x_2 u_2 x_{\delta(2)} = \ldots = x_n u_n x_{\delta(n)} \rangle \ .$$

Then M is a Garside monoid.

Proof. Let f and g be the complements on S defined by

$$f(x_i, x_j) = u_j x_{\delta(j)} \quad \text{and} \quad g(x_i, x_j) = x_{\delta^{-1}(i)} u_{\delta^{-1}(i)}$$

for $i \neq j$. Then the monoid M is both $M_R(S, f)$ and $M_L(S, g)$. Hypothesis (i) guarantees that the mapping ν is a right norm for the complement f, thus, by Proposition 3.1, M is an atomic monoid. The congruence relation $\equiv_R^f$ is generated by the pairs $(x_i u_i x_{\delta(i)}, x_j u_j x_{\delta(j)})$ and the length of $x_i u_i x_{\delta(i)}$ is strictly greater than 1, thus, if x_i is in S, then there is no word besides x_i in S^* $\equiv_R^f$-equivalent to x_i. In particular, the elements of S are atoms. So, by Proposition 2.2, S is the set of atoms of M. A direct calculation gives:

$$C_R^f(x_k, x_i f(x_j, x_i)) = \begin{cases} u_i x_{\delta(i)} & \text{for } i = j \text{ and } i \neq k, \\ \varepsilon & \text{otherwise.} \end{cases}$$

So, $C_R^f(x_k, x_i f(x_j, x_i))$ and $C_R^f(x_k, x_j f(x_i, x_j))$ exist and are $\equiv_R^f$-equivalent in any case, thus (S, f) satisfies Condition II_R. Similarly, (S, g) satisfies Condition II_L. An easy inductive argument on k shows:

$$J_R^f(x_1, \ldots, x_k) = \begin{cases} x_1 & \text{for } k = 1, \\ x_1 u_1 x_{\delta(1)} & \text{for } k \geq 2. \end{cases}$$

In particular, $J_R^f(x_1, \ldots, x_n)$ exists and is equal to $x_1 u_1 x_{\delta(1)}$. Equality (5.5) and a direct calculation show that $C_L^g(x_1 u_1 x_{\delta(1)} x_k, x_1 u_1 x_{\delta(1)})$ exists and is the empty word for all x_k in S. So, (S, f, g) satisfies Condition IV_{LR}. Similarly, (S, f, g) satisfies Condition IV_{RL}. We conclude by Theorem 4.4 that M is a Garside monoid. □

Example #4. Consider a finite set $S = \{x_1, \dots, x_n\}$ and n positive integers $p_1, \dots, p_n$ strictly greater than 1. Then, by Proposition 5.2, the group

$$\langle x_1, \dots, x_n \mid x_1^{p_1} = x_2^{p_2} = \dots = x_n^{p_n} \rangle$$

is a Garside group. Here, $x_{\delta(i)} = x_i$, $u_i = x_i^{p_i - 2}$, and the mapping ν is defined as follows. We choose n positive integers $t_1, \dots, t_n$ satisfying $t_1 p_1 = t_2 p_2 = \dots = t_n p_n$, and we set

$$\nu(x_{i_1} x_{i_2} \dots x_{i_r}) = t_{i_1} + t_{i_2} + \dots + t_{i_r} \ .$$

Torus knot groups have the form

$$\langle x, y \mid x^p = y^q \rangle$$

(see [27, Chapter 3]), thus are among these examples.

Example #5. Let $x_1, \dots, x_p$ be p letters and let m be a positive integer. Then $\mathrm{prod}(x_1, \dots, x_p; m)$ denotes the word

$$\mathrm{prod}(x_1, \dots, x_p; m) = \underbrace{x_1 x_2 \dots x_p x_1 x_2 \dots}_{m \text{ factors}} \ .$$

Consider now a finite set $S = \{x_1, \dots, x_n\}$ and two positive integers p and m, $2 \le p \le n$ and $2 \le m$. By Proposition 5.2, the group

$$\begin{aligned}\langle x_1, \dots, x_n \mid \mathrm{prod}(x_1, \dots, x_p; m) = \mathrm{prod}(x_2, \dots, x_{p+1}; m) = \dots = \mathrm{prod}(x_{n-p+1}, \dots, x_n; m) \\ = \mathrm{prod}(x_{n-p+2}, \dots, x_n, x_1; m) = \dots = \mathrm{prod}(x_n, x_1, \dots, x_{p-1}; m)\rangle\end{aligned}$$

is a Garside group. The group

$$\langle x_1, \dots, x_n \mid x_1 x_2 \dots x_n = x_2 \dots x_n x_1 = \dots = x_n x_1 \dots x_{n-1} \rangle$$

is the fundamental group of the complement of n lines through the origin in $\mathbf{C}^2$ (see [25] or [28]). The group

$$\langle x_1, \dots, x_n \mid x_1 x_2 = x_2 x_3 = \dots = x_n x_1 \rangle$$

is the Artin group of type $I_2(n)$, however, the Garside monoid having the previous presentation is not an Artin monoid. According to [6], the group

$$\langle x, y, z \mid xyz = yzx = zxy \rangle$$

is the braid group associated with the complex reflection groups of type G_7, G_{11}, and G_{19}, and the group

$$\langle x, y, z \mid xyzxy = yzxyz = zxyzx \rangle$$

is the braid group associated with the complex reflection group of type G_{22}.

EXAMPLE #6. One can mix the presentations of Examples #4 and #5 to get new ones. For example,

$$\langle x_1, x_2, x_3, x_4, x_5 \mid x_1^2 = x_2^5 = x_3x_4x_5x_3 = x_4x_5x_3x_4 = x_5x_3x_4x_5 \rangle$$

is a Garside group.

PROPOSITION 5.3. *Consider n Garside monoids $M_1, \dots, M_n$, and n positive integers $p_1, \dots, p_n$. Let Δ_i denote the fundamental element of M_i. We assume that:*

i) There is a mapping $\nu_i : M_i \to \mathbf{N}$ satisfying $\nu_i(a) > 0$ for all a in M_i, $a \neq 1$, and $\nu_i(ab) = \nu_i(a) + \nu_i(b)$ for all a, b in M_i;

ii) If M_i has only one atom, namely, if M_i is isomorphic to $\mathbf{Z}_+$, then $p_i \geq 2$.

Let $\equiv$ be the congruence relation on $(M_1 * M_2 * \dots * M_n)$ generated by the pairs $(\Delta_i^{p_i}, \Delta_j^{p_j})$, and let M be the quotient

$$M = (M_1 * M_2 * \dots * M_n)/\equiv \ .$$

Then M is a Garside monoid.

Proof. Let S_i be the set of atoms of M_i, let f_i be a right l.c.m. selector on S_i in M_i, let g_i be a lrft l.c.m. selector on S_i in M_i, and let u_i be a positive word in S_i^* that represents Δ_i. Set

$$S = S_1 \cup S_2 \cup \dots \cup S_n \ .$$

We define a complement f on S by: for x in S_i and y in S_j,

$$f(x,y) = \begin{cases} f_i(x,y) & \text{for } i = j, \\ C_R^{f_j}(u_j, y) \cdot u_j^{p_j - 1} & \text{for } i \neq j. \end{cases}$$

Similarly, we define a complement g on S by: for x in S_i and y in S_j,

$$g(x,y) = \begin{cases} g_i(x,y) & \text{for } i = j, \\ u_i^{p_i - 1} \cdot C_L^{g_i}(x, u_i) & \text{for } i \neq j. \end{cases}$$

By construction, M admits both presentations:

$$\langle S \mid xf(y,x) = yf(x,y), \ x, y \in S \rangle \text{ and } \langle S \mid g(x,y)x = g(y,x)y, \ x, y \in S \rangle \ .$$

Let $\nu_i : S_i^* \to \mathbf{N}$ be the mapping defined by $\nu_i(v) = \nu_i(\overline{v})$. We choose n positive integers $t_1, \dots, t_n$ satisfying $t_1 p_1 \nu_1(u_1) = t_2 p_2 \nu_2(u_2) = \dots = t_n p_n \nu_n(u_n)$ and we define a mapping $\nu : S^* \to \mathbf{N}$ as follows. Let v be in S^*. We write $v = v_{i_1} v_{i_2} \dots v_{i_r}$, where v_{i_j} is in $S_{i_j}^*$. Then

$$\nu(v) = t_{i_1}\nu_{i_1}(v_{i_1}) + t_{i_2}\nu_{i_2}(v_{i_2}) + \dots + t_{i_r}\nu_{i_r}(v_{i_r}) \; .$$

By Assumption (i), this mapping is well-defined and is a right norm for the complement f, thus, by Proposition 3.1, M is an atomic monoid.

The congruence relation $\equiv_R^f$ is generated by the pairs $(xf_i(y,x), yf_i(x,y))$, x, y in S_i and i in $\{1, \dots, n\}$, and by the pairs $(u_i^{p_i}, u_j^{p_j})$, i, j in $\{1, \dots, n\}$. The lengths of both $xf_i(y,x)$ and $u_i^{p_i}$ are strictly greater than 1, thus, if x is in S, then there is no word besides x in S^* $\equiv_R^f$-equivalent to x. In particular, the elements of S are atoms. By Proposition 2.2, S is the set of atoms of M.

A direct calculation gives: for x in S_i, y in S_j, and z in S_k,

$$C_R^f(z, xf(y,x)) = \begin{cases} C_R^{f_i}(z, xf_i(y,x)) & \text{for } i = j = k, \\ C_R^{f_i}(C_R^{f_i}(u_i, x), f_i(y,x)) \cdot u_i^{p_i - 1} & \text{for } i = j \neq k, \\ \varepsilon & \text{for } i \neq j. \end{cases}$$

So, $C_R^f(z, xf(y,x))$ and $C_R^f(z, yf(x,y))$ exist and are $\equiv_R^f$-equivalent in any case, thus (S, f) satisfies Condition II_R. Similarly, (S, g) satisfies Condition II_L.

Without lost of generality, we may assume that there is an enumeration $x_1, \dots, x_r$ of the elements of S_1 such that $J_R^{f_1}(x_1, \dots, x_r)$ is u_1. A direct calculation gives: for y in $S_2 \cup \dots \cup S_n$,

$$C_R^f(y, u_1) = u_1^{p_1 - 1} \text{ and } C_R^f(y, u_1^{p_1}) = \varepsilon \; . \tag{5.6}$$

We extend the previous enumeration to an enumeration $x_1, \dots, x_r, x_{r+1}, \dots, x_m$ of S. By (5.6), $J_R^f(x_1, \dots, x_m)$ exists and is equal to $u_1^{p_1}$. Now, let x be in S_i. By Proposition 2.5, there is y in S_i such that $u_i^{p_i} x$ and $y u_i^{p_i}$ are $\equiv_R^f$-equivalent. Since $u_1^{p_1}$ is $\equiv_R^f$-equivalent to $u_i^{p_i}$, the word $u_1^{p_1} x$ is $\equiv_R^f$-equivalent to $y u_1^{p_1}$, thus, by Proposition 3.4, $C_L^g(u_1^{p_1} x, u_1^{p_1})$ exists and is the empty word. This shows that (S, f, g) satisfies Condition IV_{LR}. Similarly, (S, f, g) satisfies Condition IV_{RL}. We conclude by Theorem 4.4 that M is a Garside monoid. □

Example #7. Proposition 5.3 applied to the Artin groups of type B_3 and A_3 shows that the group

$$\langle x_1, x_2, x_3, y_1, y_2, y_3 \mid x_1x_2x_1x_2 = x_2x_1x_2x_1,\; x_1x_3 = x_3x_1,\; x_2x_3x_2 = x_3x_2x_3,$$
$$y_1y_2y_1 = y_2y_1y_2,\; y_1y_3 = y_3y_1,\; y_2y_3y_2 = y_3y_2y_3,\; (x_1x_2x_3)^6 = (y_1y_2y_3y_1y_2y_1)^3 \rangle$$

is a Garside group. (Expressions of the fundamental elements of the Artin groups of type A_n, B_n, and D_n can be found in [24].)

Example #8. It is proved in [3] that the braid group on n strings has a presentation with generators $\{a_{ts}; n \geq t > s \geq 1\}$ and with defining relations

$$a_{ts}a_{rq} = a_{rq}a_{ts} \quad \text{for } (t-r)(t-q)(s-r)(s-q) > 0,$$
$$a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr} \quad \text{for all } t,\, s,\, r \text{ with } n \geq t > s > r \geq 1.$$

These relations are complement relations, but they are incomplete as there is no complement for a_{ts} and a_{rq} in the cases $t > r > s > q$ and $r > t > q > s$. However, the above relations imply

$$a_{ts}a_{tr}a_{sq} = a_{rq}a_{tq}a_{rs} \quad \text{for } t > r > s > q,$$
$$a_{ts}a_{tq}a_{rs} = a_{rq}a_{rt}a_{qs} \quad \text{for } r > t > q > s,$$

and gathering the four series of relations gives a presentation of the type $G_R(S, f)$. The relations are homogeneous, so (S, f) satisfies Condition I_R. By a long verification, it is shown in [3] that (S, f) satisfies Condition II_R, and that the l.c.m. Δ of the generators exists and enjoys all desired properties, so that the monoid $M_R(S, f)$ is a Garside monoid. It follows in particular that the braid group equipped with this new presentation is eligible for the general algorithms and normal forms presented in the next sections.

6. Word problem and isoperimetric inequalities

Let G be a group given by a presentation $\langle S|R \rangle$, where R is some subset of $(S \cup S^{-1})^*$. The *word problem* in G consists in finding an algorithm which determines whether a word w in $(S \cup S^{-1})^*$ represents the identity in G.

Reversing processes give rise to algorithms which solve the word problem for Gaussian groups (Theorems 6.1 and 6.3). These algorithms were introduced in [14]. By Lemma 3.9, both have quadratic complexity in the case of a small Gaussian group—hence, in particular, in the case of a Garside group.

Theorem 6.1. *Let M be a right cancellative right Gaussian monoid, and let G be the group of (right) fractions of M. Let S be a finite generating set of M and let f be a right l.c.m. selector on S in M. Then a word w in $(S \cup S^{-1})^*$ represents the identity of G if and only if the word $R_R^f(D_R^f(w)^{-1}N_R^f(w))$ is empty.*

Proof. By construction, the words w and $R_R^f(w)$ represent the same element of G. The latter word is $N_R^f(w)D_R^f(w)^{-1}$. Hence it represents 1 in G if and only if the positive words $N_R^f(w)$ and $D_R^f(w)$ represent the same element of G. The hypotheses guarantee that M embeds in G, so the latter condition is equivalent to $N_R^f(w) \equiv_R^f D_R^f(w)$. By Proposition 3.4, this in turn is equivalent to the fact that both $C_R^f(N_R^f(w), D_R^f(w))$ and $C_R^f(D_R^f(w), N_R^f(w))$ are empty, i.e., that $R_R^f(D_R^f(w)^{-1}N_R^f(w))$ is the empty word. □

PROPOSITION 6.2. *Let M be a Gaussian monoid, and let G be the group of (right) fractions of M. Let S be a finite generating set of M, let f be a right l.c.m. selector on S in M, and let g be a left l.c.m. selector on S in M. Two words w and w' in $(S \cup S^{-1})^*$ represent the same element of G if and only if $N_L^g(R_R^f(w))$ is equivalent to $N_L^g(R_R^f(w'))$, and $D_L^g(R_R^f(w))$ is equivalent to $D_L^g(R_R^f(w'))$.*

Proof. Every word w in $(S \cup S^{-1})^*$ represents in G the same element as $R_L^g(R_R^f(w))$. In particular, if $N_L^g(R_R^f(w))$ is equivalent to $N_L^g(R_R^f(w'))$ and $D_L^g(R_R^f(w))$ is equivalent to $D_L^g(R_R^f(w'))$, then w and w' represent the same element of G.

We assume now that w and w' represent the same element of G. By Proposition 3.7, there exist positive words u, u' such that $N_R^f(w)u$ is equivalent to $N_R^f(w')u'$ and $D_R^f(w)u$ is equivalent to $D_R^f(w')u'$. By construction, the word $N_R^f(w)uu^{-1}D_R^f(w)^{-1}$ is g-reversible on the left to the word $N_R^f(w)D_R^f(w)^{-1}$, thus we have

$$N_L^g(R_R^f(w)) = C_L^g(D_R^f(w)u, N_R^f(w)u) .$$

Similarly, we have

$$N_L^g(R_R^f(w')) = C_L^g(D_R^f(w')u', N_R^f(w')u') .$$

It follows by Proposition 3.5 that $N_L^g(R_R^f(w))$ is equivalent to $N_L^g(R_R^f(w'))$. Similarly, $D_L^g(R_R^f(w))$ is equivalent to $D_L^g(R_R^f(w'))$. □

THEOREM 6.3. *Let M be a Gaussian monoid, and let G be the group of (right) fractions of M. Let S be a finite generating set of M, let f be a right l.c.m. selector on S in M, let g be a left l.c.m. selector on S in M. Then a word w in $(S \cup S^{-1})^*$ represents the identity of G if and only if the word $R_L^g(R_R^f(w))$ is empty.*

Proof. Obvious from Proposition 6.2: as it is a positive word, $N_L^g(R_R^f(w))$ is equivalent to ε (if and) only if it is empty. Similarly, $D_L^g(R_R^f(w))$ is equivalent to ε (if and) only if it is empty. □

DEFINITION. Let G be a group given by a finite presentation $\langle S|R\rangle$. Let $F(S)$ denote the free group generated by S, and let $R^{F(S)}$ denote the normal subgroup of $F(S)$

generated by R. Let α be an element of $R^{F(S)}$. Then α can be written in the form

$$\alpha = (\beta_1 r_1^{e_1} \beta_1^{-1})(\beta_2 r_2^{e_2} \beta_2^{-1}) \dots (\beta_n r_n^{e_n} \beta_n^{-1}) \tag{6.1}$$

where β_i is in $F(S)$, r_i is in R, and e_i is in $\{\pm 1\}$. The lowest n satisfying (6.1) is called the *combinatorial area* of α and is denoted by area(α). The group G has a *quadratic isoperimetric inequality* if there exists a constant $c > 0$ such that

$$\text{area}(\alpha) \leq c \cdot \text{lg}_S(\alpha)^2$$

holds for all α in $R^{F(S)}$. This definition depends neither on the choice of the (finite) generating set, nor on the choice of the (finite) set of relations.

We prove in Section 8 that Garside groups are biautomatic groups. By [17, Theorem 2.3.12], it follows that such groups have quadratic isoperimetric inequalities. However, as shown in the next theorem, reversing processes together with Lemma 3.9 give rise to the same result in a (strictly) larger framework. In [29], Tatsuoka proves this for finite Coxeter type Artin groups using similar techniques.

Theorem 6.4. *Let G be the group of (right) fractions of a right cancellative right small right Gaussian monoid. Then G has a quadratic isoperimetric inequality.*

Proof. Let M be the monoid considered, let S be the set of atoms of M, and let f be a right l.c.m. selector on S in M. We take S as generating set of G and

$$R = \{x f(y, x) f(x, y)^{-1} y^{-1};\ x, y \in S\}$$

as set of relations. For w in $(S \cup S^{-1})^*$, we denote by red(w) the element of $F(S)$ represented by w. One can easily verify that: if w in $(S \cup S^{-1})^*$ is f-reversible in one step to w', then red(w) can be written in the form

$$\text{red}(w) = (\beta r \beta^{-1}) \cdot \text{red}(w') \tag{6.2}$$

where β is in $F(S)$, and r belongs to R. Iterating (6.2) and using Lemma 3.9, we deduce that there exists a constant $K > 0$ such that: for all w in $(S \cup S^{-1})^*$ of length ℓ, red(w) can be written in the form

$$\text{red}(w) = (\beta_1 r_1 \beta_1^{-1}) \dots (\beta_n r_n \beta_n^{-1}) \cdot \text{red}(N_R^f(w) D_R^f(w)^{-1}) \tag{6.3}$$

where β_i is in $F(S)$, r_i is in R, and $n \leq K\ell^2/4$ holds. Similarly, we find that $\text{red}(D_R^f(w)^{-1} N_R^f(w))$ can be written in the form

$$\text{red}(D_R^f(w)^{-1} N_R^f(w)) = (\beta_1' r_1' {\beta_1'}^{-1}) \dots (\beta_{n'}' r_{n'}' {\beta_{n'}'}^{-1}) \cdot \text{red}(R_R^f(D_R^f(w)^{-1} N_R^f(w))) \tag{6.4}$$

where β'_i is in $F(S)$, r'_i is in R, and $n' \le K\ell^2/4$ holds.

Now, if $\mathrm{red}(w)$ is in $R^{F(S)}$, then, by Theorem 6.1, $R^f_R(D^f_R(w)^{-1}N^f_R(w))$ is empty. Conjugating by $\mathrm{red}(D^f_R(w))$ in (6.4), and introducing the hypothesis that $\mathrm{red}(w)$ belongs to $R^{F(S)}$, i.e., that the word $R^f_R(D^f_R(w)^{-1}N^f_R(w))$ is empty, we obtain an equality of the form

$$\mathrm{red}(N^f_R(w)D^f_R(w)^{-1}) = (\gamma_1 r'_1 \gamma_1^{-1}) \ldots (\gamma_{n'} r'_{n'} \gamma_{n'}^{-1}) \tag{6.5}$$

where γ_i is in $F(S)$. Finally (6.3) and (6.5) imply that the combinatorial area of $\mathrm{red}(w)$ is at most $K\ell^2/2$. □

The previous computation shows more generally that every upper bound for the number of elementary steps in a reversing process gives an isoperimetric inequality in the associated group. In the case of Example #3 the only upper bound on the length of the reversing process is exponential with respect to the length of the initial word, correponding to the fact that the group involved satisfies an exponential isoperimetric inequality. This raises two questions:

Question #1. For which functions T does there exist a right Gaussian monoid $M_R(S, f)$ such that $T(\ell)$ is the minimal upper bound on the number of steps of the f-reversing of all length ℓ words?

Let us mention that [12] gives an example where the only known upper bound about the number of steps for reversing a length ℓ word is a tower of exponentials of height 2^ℓ. This example however is not exactly relevant for the present question as it involves an infinite set of generators. Another related question involving the complexity of word reversing is:

Question #2. Assume that the monoid M admits two presentations $M_R(S, f)$, $M_L(S, g)$ and M is a right small right Gaussian monoid; is M necessarily a (small) Gaussian monoid?

7. Normal forms

Definition. Let M be a Gaussian monoid. For a in M, $\pi_R(a)$ denotes the left g.c.d. of a and Δ_R, and $\partial_R a$ denotes the element of M satisfying $a = \pi_R(a) \cdot \partial_R a$.

Lemma 7.1. *Let M be a Gaussian monoid. For a in M, there exists a non-negative integer k satisfying $\partial_R^k a = 1$.*

Proof. Since Δ_R is the right l.c.m. of all atoms, $a \neq 1$ implies $\pi_R(a) \neq 1$. This gives $\|\partial_R a\| < \|a\|$ for $a \neq 1$, thus there exists a non-negative integer k satisfying $\partial_R^k a = 1$. □

Definition. Let M be a Gaussian monoid. Let a be in M. The *degree* of a, denoted by $\deg(a)$, is the lowest k satisfying $\partial_R^k a = 1$. Then the expression

$$a = \pi_R(a) \cdot \pi_R(\partial_R a) \cdot \ldots \cdot \pi_R(\partial_R^{\deg(a)-1} a)$$

is called the *normal form* of a.

In order to define normal forms for Gaussian groups, we first need Proposition 7.4 and its corollary to guarantee that such forms exist and are unique.

From now on and till the end of this section, we fix the following assumptions: M is a Gaussian monoid, S is the set of atoms of M, f is a right l.c.m. selector on S in M, g is a left l.c.m. selector on S in M, and G is the group of (right) fractions of M.

Lemma 7.2. *Let x, y be in S, $x \neq y$. Then $C_L^g(f(y,x), f(x,y))$ is equal to x.*

Proof. Let a be the element of M represented by $f(y,x)$, and let b be the element of M represented by $f(x,y)$. If $C_L^g(f(y,x), f(x,y))$ is empty, then, by Proposition 3.4, b divides a on the right. Since $xa = yb$ holds, it follows that x divides y on the left, thus x is equal to y since both are atoms. This is a contradiction, thus $C_L^g(f(y,x), f(x,y))$ is non-empty. The word $C_L^g(f(y,x), f(x,y))f(y,x)$ represents the left l.c.m. of a and b. The equality $xa = yb$ shows that xa is a common left multiple of a and b. So, there exists a word v in S^* such that $vC_L^g(f(y,x), f(x,y))f(y,x)$ represents xa. By right cancellation, it follows that $vC_L^g(f(y,x), f(x,y))$ represents x, thus, since x is an atom, v is empty and $C_L^g(f(y,x), f(x,y))$ is equal to x. □

Taking Lemma 7.2 into account, the proof of the following lemma is the same as the proof of [14, Lemma 2.11]. So, we do not include it here.

Lemma 7.3 [14, Lemma 2.11]. *Let w, w' be two words in $(S \cup S^{-1})^*$. If w is f-reversible on the right to w', then there exists a positive word v in S^* such that $vN_L^g(w')$ is equivalent to $N_L^g(w)$ and $vD_L^g(w')$ is equivalent to $D_L^g(w)$.* □

PROPOSITION 7.4. *Let c be in G and let w be a word in $(S \cup S^{-1})^*$ which represents c. If a word of the form $u^{-1}v$, with u, v in S^*, also represents c, then there exists w' in S^* such that u is equivalent to $w' D_L^g(R_R^f(w))$ and v is equivalent to $w' N_L^g(R_R^f(w))$.*

Proof. By Lemma 7.3, there exists w' in S^* such that u is equivalent to $w' D_L^g(R_R^f(u^{-1}v))$ and v is equivalent to $w' N_L^g(R_R^f(u^{-1}v))$. By Theorem 6.1, $D_L^g(R_R^f(u^{-1}v))$ is equivalent to $D_L^g(R_R^f(w))$ and $N_L^g(R_R^f(u^{-1}v))$ is equivalent to $N_L^g(R_R^f(w))$. □

COROLLARY 7.5. *Let c be an element of G. There exists a unique pair (a, b) in $M \times M$ satisfying $c = a^{-1}b$ and $a \wedge_L b = 1$. Moreover, if w in $(S \cup S^{-1})^*$ represents c, then $D_L^g(R_R^f(w))$ represents a and $N_L^g(R_R^f(w))$ represents b.* □

DEFINITION. Let c be an element of G. Let a, b be elemnts of G such that c is $a^{-1}b$ and $a \wedge_L b$ is 1. Then the expression

$$c = \pi_R(\partial_R^{\deg(a)-1} a)^{-1} \cdot \ldots \cdot \pi_R(\partial_R a)^{-1} \cdot \pi_R(a)^{-1} \cdot \pi_R(b) \cdot \pi_R(\partial_R b) \cdot \ldots \cdot \pi_R(\partial_R^{\deg(b)-1} b)$$

is called the *normal form* of c. By Corollary 7.5, such a form always exists and is unique.

The normal forms defined above are nothing but those of [9] in the case of finite Coxeter type Artin groups. Because of the existence of the fundamental element Δ and of the permutation δ of Proposition 2.5, the normal forms of [5] and [18], and those of [15], [2], [8], [17] can also easily be extended to all Garside groups.

Let c be in G and let w be a word in $(S \cup S^{-1})^*$ which represents c. We now describe an algorithm that gives the normal form of c starting from w. Let a, b in M be satisfying $c = a^{-1}b$ and $a \wedge_L b = 1$. By Corollary 7.4, a is represented by $D_L^g(R_R^f(w))$ and b is represented by $N_L^g(R_R^f(w))$. So, it remains to describe how to find the normal form of an element of M. Let $x_1, \ldots, x_n$ be an enumeration of the atoms, and let $J_R^f(x_1, \ldots, x_n)$ be the word defined just before Theorem 4.4. As pointed out before, $J_R^f(x_1, \ldots, x_n)$ represents Δ_R and can be effectively computed. Now, Proposition 7.7 below gives an algorithm which determines an expression of $\overline{u} \wedge_L \overline{v}$ for all u, v in S^*. This ends our algorithm since: if u_0 represents $\pi_R(a)$ and u represents a, then, by Lemma 4.3, $C_R^f(u, u_0)$ represents $\partial_R a$.

LEMMA 7.6. *Let a, b, a', b' in M satisfy $aa' = bb' = a \vee_R b$. Then we have*

$$a \vee_R b = (a \wedge_L b)(a' \vee_L b') .$$

Proof. Let a'', b'' in M satisfy $a''a' = b''b' = a' \vee_L b'$. Because $aa' = bb'$ is a common left multiple of a' and b', there exists e satisfying $aa' = bb' = e(a' \vee_L b') = ea''a' = eb''b'$. We prove that e is $a \wedge_L b$. By right cancellation, $a = ea''$ and $b = eb''$ hold, thus e is a common left divisor of a and b. Let e_1 be a common left divisor of a and b. Let a_1, b_1 in M satisfy $a = e_1 a_1$ and $b = e_1 b_1$. By left cancellation, $a_1 a' = b_1 b'$ holds. So, there exists c in M satisfying $a_1 a' = b_1 b' = c(a' \vee_L b') = ca''a' = cb''b'$. By right cancellation, $a_1 = ca''$ and $b_1 = cb''$ hold, thus $a = e_1 ca'' = ea''$ and $b = e_1 cb'' = eb''$ holds as well. It follows, by right cancellation, that e_1 is a left divisor of e. □

Proposition 7.7. *Let u, v be in S^*. Then $\overline{u} \wedge_L \overline{v}$ is represented by $C_L^g(N_L^g(R_R^f(v^{-1}u)), u)$.*

Proof. Let a, b, a', b' in M satisfy $a = \overline{u}$, $b = \overline{v}$, and $aa' = bb' = a \vee_R b$. By Lemma 4.3, a' is represented by $C_R^f(v, u)$ and b' is represented by $C_R^f(u, v)$, thus $a' \vee_L b'$ is represented by $C_L^g(C_R^f(v, u), C_R^f(u, v))C_R^f(v, u)$. The element $a \vee_R b$ is represented by $uC_R^f(v, u)$. Finally, by Lemma 7.6 and Lemma 4.3, $a \wedge_L b$ is represented by

$$C_L^g(C_L^g(C_R^f(v, u), C_R^f(u, v))C_R^f(v, u), uC_R^f(v, u))C_L^g(N_L^g(R_R^f(v^{-1}u)), u) \ . \ \square$$

8. Automatic structure

We shall prove here that Garside groups are biautomatic groups. Roughly speaking, this means that there exists a finite state automaton that computes the normal forms of Section 7. The key point that explains automaticity is the fact that, if a, b are elements of a Garside monoid, then the value of the g.c.d. $(ab) \wedge_L \Delta$ depends only on a and on $b \wedge_L \Delta$, i.e., the 'state' of ab depends only on a and on the 'state' of b—but not on the whole of b. It is easy to see that such a result fails in the case of Example #2, and this makes it unlikely that a general automaticity result holds for small Gaussian groups even if they satisfy a quadratic isoperimetric inequality.

Our proof of Theorem 8.1 is inspired by the proof of [9, Theorem 0.1]. In particular, the proofs of Lemmas 8.6 and 8.7 are the same as the proofs of [8, Proposition 3.1] and [8, Proposition 3.3] respectively. We do not include them here.

Definition. A *finite state automaton* is a quintuple $\mathcal{F} = (Q, A, \mu, Y, q_0)$, where Q is a finite set, called the *state set*, A is a finite set, called the *alphabet*, $\mu : Q \times A \to Q$ is a function, called the *transition function*, Y is a subset of Q, whose elements are called the *accept states*, and q_0 is in Q, and is called the *start state*. For q in Q and $w = x_1 \dots x_n$ in A^*, we define the state $\mu(q, w)$ inductively on n by

$$\mu(q,w) = \begin{cases} q & \text{for } n = 0, \\ \mu(\mu(q, x_1 \dots x_{n-1}), x_n) & \text{for } n \geq 1. \end{cases}$$

Then

$$L_{\mathcal{F}} = \{w \in A^* \ ; \ \mu(q_0, w) \in Y\}$$

is called the *language recognized* by $\mathcal{F}$. A *regular language* is a language recognized by a finite state automaton.

DEFINITION. Let G be a group, and let S be a generating set of G. The *length* (with respect to S) of an element c of G, denoted by $\lg_S(c)$, is the shortest length of a word in $(S \cup S^{-1})^*$ representing c. The *distance* between two elements c and d in G, denoted by $d_S(c, d)$, is the length of $c^{-1}d$.

DEFINITION. Let G be a group, and let S be a finite generating set of G. A language L in $(S \cup S^{-1})^*$ *represents* G if all the elements of G are represented by elements of L. The language L has the *uniqueness property* if every element of G is represented by a unique element of L. It is *symmetric* if L is equal to L^{-1}, where L^{-1} is the language obtained by formally inverting the elements of L. It is *geodesic* if the length of w is equal to the length of $\overline{w}$ for all w in L. For $w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ in $(S \cup S^{-1})^*$ and for t in $\mathbf{N}$, we write

$$\overline{w}(t) = \begin{cases} 1 & \text{for } t = 0, \\ \overline{x_1^{\varepsilon_1} \dots x_t^{\varepsilon_t}} & \text{for } 1 \leq t \leq n, \\ \overline{w} & \text{for } t \geq n. \end{cases}$$

Let κ be a positive integer. We say that L has the *κ-fellow traveller property* if: for w, w' in L,

$$d_S(\overline{w}(t), \overline{w}'(t)) \leq \kappa \cdot d_S(\overline{w}, \overline{w}')$$

holds for all non-negative integers t.

DEFINITION. A group G is *automatic* if there exist a finite generating set S of G, a constant $\kappa > 0$, and a regular language L in $(S \cup S^{-1})^*$, such that L represents G and has the κ-fellow traveller property. If, in addition, L^{-1} also has the κ-fellow traveller property, then G is called *biautomatic*. If L is symmetric, G is called *fully biautomatic*. If L is geodesic, G is called *geodesically automatic*. We refer to [17] for a general exposition on automatic groups.

From now on and till the end of this section, we fix the following assumptions: M is a Garside monoid, S is the set of atoms of M, f is a right l.c.m. selector on S in M,

g is a left l.c.m. selector on S in M, Σ is the set of simple elements different from the identity, $\equiv$ is the congruence on Σ^* such that M is $\Sigma^*/\equiv$, and G is the group of fractions of M.

The goal of this section is to prove the following theorem.

THEOREM 8.1. *Let L be the language in $(\Sigma \cup \Sigma^{-1})^*$ of all normal forms. Then L is regular, represents G, has the uniqueness property, is symmetric, is geodesic, and has the 5-fellow traveller property.*

COROLLARY 8.2. *The group G is fully geodesically biautomatic.*

Note that, since L is regular, has the uniqueness property, and is geodesic, it can be used to compute with standard methods the growth series of G with respect to Σ.

By definition, the language L of normal forms represents G, has the uniqueness property, and is symmetric. So, it remains to prove that L is regular, has the 5-fellow traveller property, and is geodesic. This is the object of Propositions 8.3, 8.5, and 8.9 below.

PROPOSITION 8.3. *The language of normal forms is regular.*

The following lemma 8.4 is a preliminary result to the proof of Proposition 8.3. For a simple element σ, we denote by σ^* the simple element satisfying $\sigma\sigma^* = \Delta$.

LEMMA 8.4. *Let $\sigma_1, \ldots, \sigma_n$ be in Σ. Then the following conditions are equivalent.*

i) The word $\sigma_1\sigma_2\ldots\sigma_n$ is a normal form.

ii) The word $\sigma_i\sigma_{i+1}$ is a normal form for $i = 1, \ldots, n-1$.

iii) $\sigma_i^* \wedge_L \sigma_{i+1}$ is 1 for $i = 1, \ldots, n-1$.

Proof. Assume (i). By construction, $\sigma_i\sigma_{i+1}\ldots\sigma_n$ is a normal form. The element σ_i is a common left divisor of $\overline{\sigma_i\sigma_{i+1}}$ and Δ, thus σ_i divides $\pi_R(\overline{\sigma_i\sigma_{i+1}})$ on the left. The element $\pi_R(\overline{\sigma_i\sigma_{i+1}})$ divides $\overline{\sigma_i\sigma_{i+1}}$ on the left, and $\overline{\sigma_i\sigma_{i+1}}$ divides $\overline{\sigma_i\sigma_{i+1}\ldots\sigma_n}$ on the left, thus $\pi_R(\overline{\sigma_i\sigma_{i+1}})$ divides $\overline{\sigma_i\sigma_{i+1}\ldots\sigma_n}$ on the left. Since this element is simple, it follows that $\pi_R(\overline{\sigma_i\sigma_{i+1}})$ divides $\pi_R(\overline{\sigma_i\sigma_{i+1}\ldots\sigma_n}) = \sigma_i$ on the left, and, therefore, that $\pi_R(\overline{\sigma_i\sigma_{i+1}})$ is equal to σ_i. Then σ_{i+1} is $\partial_R(\overline{\sigma_i\sigma_{i+1}})$ and $\sigma_i\sigma_{i+1}$ is a normal form.

Conversely, assume (ii). We prove by induction on n that $\sigma_1\sigma_2\ldots\sigma_n$ is a normal form. The result is vacuously true if n is 1. We assume $n \geq 1$. Let a and a' in M be represented by $\sigma_1\sigma_2\ldots\sigma_n$ and $\sigma_2\ldots\sigma_n$ respectively. By induction hypothesis, $\sigma_2\ldots\sigma_n$ is the normal form of a'. The element σ_1 divides a on the left and is simple, thus it divides $\pi_R(a)$ on the left. Let α be the simple element of M satisfying $\sigma_1\alpha \equiv \pi_R(a)$. There exists b in M such that $\pi_R(a)b$ is a. By left cancellation, we deduce that αb is

a', thus, since α is a simple element, that α divides $\pi_R(a') = \sigma_2$ on the left. Let β be the simple element of M satisfying $\alpha\beta \equiv \sigma_2$. From the equivalence

$$\sigma_1\sigma_2 \equiv \sigma_1\alpha\beta \equiv \pi_R(a)\beta$$

we deduce that $\pi_R(a)$ divides $\overline{\sigma_1\sigma_2}$ on the left, thus divides σ_1 on the left since $\sigma_1\sigma_2$ is a normal form. This shows that $\pi_R(a)$ is σ_1, and, therefore, that $\sigma_1\sigma_2\ldots\sigma_n$ is a normal form.

Writing $\Delta = \sigma\sigma^*$, we obtain when σ, σ' are simple elements:

$$\sigma\sigma' \wedge_L \Delta = \sigma\sigma' \wedge_L \sigma\sigma^* = \sigma(\sigma' \wedge_L \sigma^*) \ .$$

So, $\sigma\sigma'$ is a normal form, namely, $\sigma\sigma' \wedge_L \Delta$ is σ, if and only if $\sigma' \wedge_L \sigma^*$ is 1. This gives the equivalence of (ii) and (iii). □

Proof of Proposition 8.3. We define V as $\Sigma \cup \Sigma^{-1} \cup \{v_0, v_1\}$, A as $\Sigma \cup \Sigma^{-1}$, and Y as $\Sigma \cup \Sigma^{-1} \cup \{v_0\}$. The function $\mu : V \times A \to V$ is defined by: for σ, τ in Σ,

$$\mu(v_0, \sigma) = \sigma, \quad \mu(v_0, \sigma^{-1}) = \sigma^{-1}$$
$$\mu(v_1, \sigma) = v_1, \quad \mu(v_1, \sigma^{-1}) = v_1$$
$$\mu(\sigma, \tau) = \begin{cases} \tau & \text{if } \sigma^* \wedge_L \tau = 1 \\ v_1 & \text{otherwise} \end{cases}, \quad \mu(\sigma, \tau^{-1}) = v_1$$
$$\mu(\sigma^{-1}, \tau) = \begin{cases} \tau & \text{if } \sigma \wedge_L \tau = 1 \\ v_1 & \text{otherwise} \end{cases}, \quad \mu(\sigma^{-1}, \tau^{-1}) = \begin{cases} \tau^{-1} & \text{if } \sigma \wedge_L \tau^* = 1 \\ v_1 & \text{otherwise} \end{cases}$$

By Lemma 8.4, the language of normal forms is recognized by $\mathcal{F} = (V, A, \mu, Y, v_0)$. □

PROPOSITION 8.5. *The language of normal forms has the 5-fellow traveller property.*

The following lemmas 8.6–8.8 are preliminary results to the proof of Proposition 8.5.

LEMMA 8.6 [8, Proposition 3.1]. *Let a be in M, and let σ be a simple element. Let $\sigma_1\sigma_2\ldots\sigma_p$ and $\tau_1\tau_2\ldots\tau_q$ be the normal forms of a and σa respectively. Then q is equal to p or to $p+1$, and there exist simple elements $\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_p$ (namely, elements of $\Sigma \cup \{1\}$) satisfying*

$$\tau_1 \equiv \sigma\alpha_1, \quad \tau_i \equiv \beta_{i-1}\alpha_i \ (i = 2, \ldots, p), \quad \tau_{p+1} = \beta_p,$$
$$\sigma_i \equiv \alpha_i\beta_i \ (i = 1, \ldots, p)$$

where τ_{p+1} is 1 if q is equal to p. □

LEMMA 8.7 [8, Proposition 3.3]. *Let a be in M, and let σ be a simple element. Let $\sigma_1\sigma_2\ldots\sigma_p$ and $\tau_1\tau_2\ldots\tau_q$ be the normal forms of a and $a\sigma$ respectively. Then q is equal to p or to $p+1$, and there exist simple elements $\gamma_1,\ldots,\gamma_p$ (namely, elements of $\Sigma\cup\{1\}$) satisfying*

$$\gamma_i\tau_{i+1}\ldots\tau_q \equiv \sigma_{i+1}\ldots\sigma_p\sigma \tag{8.1}$$

for $i=1,\ldots,p$. □

LEMMA 8.8. *Let a, b in M be such that $a\wedge_L b$ is 1, and let σ be a simple element. Then $a\sigma\wedge_L b$ is a simple element of M.*

Proof. Since $a\sigma\wedge_L b$ divides $a\Delta\wedge_L b$ on the left, it suffices to prove Lemma 8.8 for $\sigma=\Delta$. Let $\sigma_1\sigma_2\ldots\sigma_p$ and $\tau_1\tau_2\ldots\tau_q$ be the normal forms of a and b respectively. Let δ be the permutation of Proposition 2.5 extended to M. Then $\Delta\delta^{-1}(\sigma_1)\ldots\delta^{-1}(\sigma_p)$ is the normal form of $a\Delta=\Delta\delta^{-1}(a)$. Let a' and b' in M be represented by $\tau_1^*\delta^{-1}(\sigma_1)\ldots\delta^{-1}(\sigma_p)$ and $\tau_2\ldots\tau_q$ respectively. We have $a\Delta=\tau_1 a'$ and $b=\tau_1 b'$, thus

$$a\Delta\wedge_L b=\tau_1(a'\wedge_L b') \ .$$

We prove now that $a'\wedge_L b'$ is 1. From the equivalence

$$\tau_1\Delta\equiv\tau_1\tau_1^*(\tau_1^*)^*\equiv\Delta(\tau_1^*)^* \ ,$$

we deduce that $(\tau_1^*)^*$ is $\delta^{-1}(\tau_1)$, and, therefore,

$$(\tau_1^*)^*\wedge_L\delta^{-1}(\sigma_1)=\delta^{-1}(\tau_1)\wedge_L\delta^{-1}(\sigma_1)=\delta^{-1}(\tau_1\wedge_L\sigma_1)=1 \ .$$

By Lemma 8.4, it follows that $\tau_1^*\delta^{-1}(\sigma_1)\ldots\delta^{-1}(\sigma_p)$ is the normal form of a'. From Lemma 8.4, we also deduce that $\tau_1^*\wedge_L\tau_2$ is 1, and, $\tau_1^*=\pi_R(a')$ and $\tau_2=\pi_R(b')$ imply that this element is $a'\wedge_L b'\wedge_L\Delta$. So, $a'\wedge_L b'$ is 1, too. □

Proof of Proposition 8.5. Let c be in G, let σ be in Σ, and let ε be in $\{\pm1\}$. Let w and w' be the normal forms of c and $c\sigma^\varepsilon$ respectively. We prove

$$d_\Sigma(\overline{w}(t),\overline{w}'(t))\le 5 \tag{8.2}$$

for every non-negative integer t. Let u, v be normal forms. Then (8.2) together with an easy inductive argument on $d_\Sigma(\overline{u},\overline{v})$ shows

$$d_\Sigma(\overline{u}(t),\overline{v}(t))\le 5\cdot d_\Sigma(\overline{u},\overline{v})$$

for every non-negative integer t. Note that: if c' is $c\sigma^{-1}$, then c is $c'\sigma$. So, we may assume that ε is 1.

Let a, b in M satisfy $c = a^{-1}b$ and $a \wedge_L b = 1$. Let $\alpha_1 \dots \alpha_p$ and $\beta_1 \dots \beta_q$ be the normal forms of a and b respectively. The word w is $\alpha_p^{-1} \dots \alpha_1^{-1}\beta_1 \dots \beta_q$. Let $\gamma_1 \dots \gamma_\ell$ be the normal form of $b\sigma$, and let w_1 be $\alpha_p^{-1} \dots \alpha_1^{-1}\gamma_1 \dots \gamma_\ell$. By Lemma 8.7,

$$d_\Sigma(\overline{w}(t), \overline{w}_1(t)) \leq 1 \tag{8.3}$$

holds for every non-negative integer t. By Lemma 8.8, $a \wedge_L b\sigma$ is a simple element, say μ. Let α_1' and γ_1' be the simple elements satisfying $\alpha_1 \equiv \mu\alpha_1'$ and $\gamma_1 \equiv \mu\gamma_1'$, and let w_2 be $\alpha_p^{-1} \dots \alpha_2^{-1}(\alpha_1')^{-1}\gamma_1'\gamma_2 \dots \gamma_\ell$. Clearly,

$$d_\Sigma(\overline{w}_1(t), \overline{w}_2(t)) \leq 2 \tag{8.4}$$

holds for every non-negative integer t. Let a', b' in M satisfy $c\sigma = (a')^{-1}b'$ and $a' \wedge_L b' = 1$. Then a' and b' are represented by $\alpha_1'\alpha_2 \dots \alpha_p$ and $\gamma_1'\gamma_2 \dots \gamma_\ell$ respectively. Let $\sigma_1 \dots \sigma_r$ and $\tau_1 \dots \tau_s$ be the normal forms of a' and b' respectively. Then w' is $\sigma_r^{-1} \dots \sigma_1^{-1}\tau_1 \dots \tau_s$ and, by Lemma 8.6,

$$d_\Sigma(\overline{w}_2(t), \overline{w}'(t)) \leq 2 \tag{8.5}$$

holds for every non-negative integer t. The inequalities (8.3), (8.4), and (8.5) clearly give (8.2). □

PROPOSITION 8.9. *The language of normal forms is geodesic.*

Proof. Let c be in G, let w be an expression of c in $(\Sigma \cup \Sigma^{-1})^*$, and let w_0 be the normal form of c. We prove that the length of w is greater or equal to the length of w_0. We write w as $\gamma_1^{\varepsilon_1} \dots \gamma_n^{\varepsilon_n}$, γ_i in Σ and ε_i in $\{\pm 1\}$. We choose an expression u_i of γ_i in S^*. Then c is represented by $u_1^{\varepsilon_1} \dots u_n^{\varepsilon_n}$ in $(S \cup S^{-1})^*$. Let p be the number of ε_i's equal to 1. Following the proof of Lemma 3.9, one can establish:

$$R_L^g(R_R^f(u_1^{\varepsilon_1} \dots u_n^{\varepsilon_n})) = v_1^{-1} \dots v_{n-p}^{-1} v_{n-p+1} \dots v_n \ ,$$

where v_i is a word in S^* that represents a simple element, namely, an element of $\Sigma \cup \{1\}$. Let a, b in M satisfy $c = a^{-1}b$ and $a \wedge_L b = 1$. By Corollary 7.5, $v_{n-p} \dots v_1$ represents a, and $v_{n-p+1} \dots v_n$ represents b. This shows that there exist expressions $\alpha_1 \dots \alpha_k$ of a and $\beta_1 \dots \beta_\ell$ of b in Σ^* satisfying $k + l \leq n$.

So, it remains to prove that: if a is in M, w is an expression of a in Σ^*, and w_0 is the normal form of a, then the length of w is greater or equal to the length of w_0. This is a direct consequence of Lemma 8.6 together with an easy induction argument on the length of w. □

9. Automorphisms of a Gaussian monoid

In this section, we consider an automorphism of a Gaussian monoid and the induced automorphism of the associated Gaussian group, and we study the submonoid and subgroup of elements fixed by this automorphism. Then we state and prove Theorem 9.3 concerning the special case where the monoid is a finite Coxeter type Artin monoid.

We first remark that the group of automorphisms of a Gaussian monoid is finite since any of them permutes the atoms, and these generate the monoid.

Lemma 9.1. *Let M be a Gaussian monoid, and let ϕ be an automorphism of M. Let a, b be in M. Then*

$$\phi(a \vee_R b) = \phi(a) \vee_R \phi(b) \quad \text{and} \quad \phi(a \wedge_L b) = \phi(a) \wedge_L \phi(b) \ .$$

Proof. The element a divides $a \vee_R b$ on the left, thus $\phi(a)$ divides $\phi(a \vee_R b)$ on the left. Similarly, $\phi(b)$ divides $\phi(a \vee_R b)$ on the left, hence $\phi(a) \vee_R \phi(b)$ divides $\phi(a \vee_R b)$ on the left. The same argument applied to $\phi(a)$, $\phi(b)$, and ϕ^{-1}, shows that $a \vee_R b$ divides $\phi^{-1}(\phi(a) \vee_R \phi(b))$ on the left, and, therefore, that $\phi(a \vee_R b)$ divides $\phi(a) \vee_R \phi(b)$ on the left. So, $\phi(a \vee_R b)$ is equal to $\phi(a) \vee_R \phi(b)$. A similar argument gives the second equality (concerning g.c.d.'s). □

Definition. Let M be a monoid, and let ϕ be an automorphism of M. We set

$$M^\phi = \{a \in M \ ; \ \phi(a) = a\},$$

the *ϕ-trivial submonoid* of M. The *ϕ-orbit* of an element a in M is $\{\phi^k(a) \ ; \ k \in \mathbf{Z}\}$.

Theorem 9.2. *Let M be a Gaussian monoid, let S be the set of atoms of M, let G be the group of fractions of M, and let ϕ be an automorphism of M.*

i) The ϕ-trivial submonoid M^ϕ is a Gaussian monoid.

ii) Let $X_1, \dots, X_\ell$ be the ϕ-orbits in S. Let y_i denote the right l.c.m. of the elements of X_i. Then $y_1, \dots, y_\ell$ generate M^ϕ.

iii) The group of fractions of M^ϕ is equal to G^ϕ.

Proof. The restriction to M^ϕ of the norm of M satisfies the equivalent conditions of Proposition 2.1, thus M^ϕ is atomic. The monoid M^ϕ inherits the left and right cancellation properties from M. If a, b are in M^ϕ, then, by Lemma 9.1, we have

$$\phi(a \vee_R b) = \phi(a) \vee_R \phi(b) = a \vee_R b \ ,$$

thus $a \vee_R b$ is also in M^ϕ, and, therefore, is the right l.c.m. of a and b in M^ϕ. Similarly, left l.c.m.'s also exist in M^ϕ. This proves that M^ϕ is a Gaussian monoid.

We write X_i as $\{x_1, \dots, x_r\}$, where $\phi(x_j)$ is x_{j+1} for $j = 1, \dots, r-1$, and $\phi(x_r)$ is x_1. By Lemma 9.1, we have

$$\phi(y_i) = \phi(x_1 \vee_R \dots \vee_R x_r) = \phi(x_1) \vee_R \dots \vee_R \phi(x_r) = x_2 \vee_R \dots \vee_R x_r \vee_R x_1 = y_i \ ,$$

thus y_i is in M^ϕ. Now, let a be in M^ϕ. We prove by induction on the norm of a that a is in the submonoid generated by $y_1, \dots, y_\ell$. The result is obvious if the norm of a is 0. We assume that the norm of a is greater than 0. Let x_1 be an atom of M that divides a on the left. Let $X_i = \{x_1, \dots, x_r\}$ be the ϕ-orbit of x_1. We assume as before that $\phi(x_j)$ is x_{j+1} for $j = 1, \dots, r-1$, and $\phi(x_r)$ is x_1. If x_j divides a on the left, then $\phi(x_j) = x_{j+1}$ also divides $a = \phi(a)$ on the left. So, all the elements of X_i divides a on the left, and, therefore, y_i divides a on the left. Let a' in M be such that $y_i a'$ is a. From the equality

$$y_i a' = a = \phi(a) = \phi(y_i)\phi(a') = y_i \phi(a')$$

and from left cancellation, we deduce that a' is in M^ϕ. By induction hypothesis, it follows that a', and then also a, are in the submonoid generated by $y_1, \dots, y_\ell$.

The group of fractions of M^ϕ is obviously included in G^ϕ. It remains to show that: if c is in G^ϕ, then c is in the group of fractions of M^ϕ. By Corollary 7.5, c can be uniquely written as $a^{-1}b$, where a, b are in M, and $a \wedge_L b$ is 1. Now, $c = \phi(c)$ is also $\phi(a)^{-1}\phi(b)$, the elements $\phi(a)$ and $\phi(b)$ are in M, and $\phi(a) \wedge_L \phi(b) = \phi(a \wedge_L b)$ is 1. By uniqueness, it follows that $\phi(a)$ is a and $\phi(b)$ is b, thus a, b are both in M^ϕ. This proves that c is in the group of fractions of M^ϕ. □

Remark. The set $\{y_1, \dots, y_\ell\}$ of Proposition 9.2.ii is not necessarily the set of atoms of M^ϕ. For example, if M is given by the presentation

$$\langle x_1, x_2, x_3, x_4 \mid x_1x_2x_1 = x_2x_1x_2 = x_3x_4x_3 = x_4x_3x_4 \rangle \ ,$$

and ϕ is defined by

$$\phi(x_1) = x_2,\ \phi(x_2) = x_1,\ \phi(x_3) = x_3,\ \phi(x_4) = x_4 \ ,$$

then ℓ is 3, y_1 is $x_1x_2x_1$, y_2 is x_3, y_3 is x_4, and $y_2y_3y_2$ is equal to y_1.

We now consider a Coxeter graph Γ and an automorphism ϕ of Γ. This induces an automorphism of the associated Artin monoid A_+, and any automorphism of A_+ arises from an automorphism of Γ. We list below the pairs (Γ, ϕ), where Γ is a connected finite type Coxeter graph, and ϕ is a non-trivial automorphism of Γ. The vertices of Γ are numbered according to [19, page 58].

i) Γ is of type A_ℓ, and $\phi(x_i)$ is $x_{\ell-i+1}$ for $i = 1, \dots, \ell$.

ii) Γ is of type D_ℓ, $\phi(x_i)$ is x_i for $i = 1, \dots, \ell - 2$, $\phi(x_{\ell-1})$ is x_ℓ, and $\phi(x_\ell)$ is $x_{\ell-1}$.

iii) Γ is of type D_4, $\phi(x_1)$ is x_3, $\phi(x_2)$ is x_2, $\phi(x_3)$ is x_4, and $\phi(x_4)$ is x_1.

iv) Γ is of type E_6, $\phi(x_1)$ is x_6, $\phi(x_2)$ is x_2, $\phi(x_3)$ is x_5, $\phi(x_4)$ is x_4, $\phi(x_5)$ is x_3, and $\phi(x_6)$ is x_1.

v) Γ is of type F_4, $\phi(x_1)$ is x_4, $\phi(x_2)$ is x_3, $\phi(x_3)$ is x_2, and $\phi(x_4)$ is x_1.

vi) Γ is of type $I_2(p)$, $\phi(x_1)$ is x_2, and $\phi(x_2)$ is x_1.

THEOREM 9.3. *Let Γ be a finite type Coxeter graph, let ϕ be an automorphism of Γ, and let A be the Artin group associated with Γ. Then A^ϕ is also a finite Coxeter type Artin group.*

Theorem 9.3 is proved for Artin groups of type A_n in [21, Corollary 2.25] using topological methods where the Artin groups considered are viewed as groups of isotopy classes of diffeomorphisms of surfaces. Another proof for the Artin group of type E_6 is proposed in [21, Appendice]. This is due to J. Michel [22], is based on the fact that a similar result holds for finite Coxeter groups, and can be extended in a case by case proof for Artin groups associated with connected finite type Coxeter graphs. The proof given here is independent from the previous ones and works in the general case, even if Γ is not connected.

Proof. We start recalling some well-known definitions and results concerning finite Coxeter type Artin groups. We refer to [5] and [15] for the proofs. We also assume the reader to be familiar with the theory of Coxeter groups and refer to [4] and [20] for general expositions.

Let S be the set of atoms of A_+, let $M = (m_{s,t})_{s,t \in S}$ be the Coxeter matrix represented by Γ, and let W be the Coxeter group associated with Γ. For a subset X of S we write:

$M_X = (m_{s,t})_{s,t \in X}$,

Γ_X, the Coxeter graph which represents M_X,

W_X, the subgroup of W generated by X,

A_X, the subgroup of A generated by X.

Following the conventions of [23], we shall call the subgroup W_X a parabolic subgroup. It is the Coxeter group associated with Γ_X. Similarly, A_X is called parabolic subgroup and is the Artin group associated with Γ_X (see [31] and [23]). We denote by $\theta : A \to W$ the homomorphism which sends x to x for all x in S. This homomorphism has a natural set-section $\tau : W \to A_+$ defined in Section 2. The set of simple elements is $\{\tau(w); w \in W\}$ and the fundamental element is $\Delta = \tau(w_0)$, where w_0 is the element of maximal length in W. A direct consequence of the existence of τ is: if a is a simple element of A_+, then we have

$$\lg_S(a) = \lg_S(\theta(a)) \tag{9.1}$$

Now, let $X_1, \dots, X_\ell$ be the ϕ-orbits in S, and let y_i be the right l.c.m. of the elements of X_i.

Assertion. For i, j in $\{1, \dots, l\}$, $i \neq j$, there exists an integer $\tilde{m}_{i,j} \geq 2$ satisfying

$$y_i \vee_R y_j = \mathrm{prod}(y_i, y_j; \tilde{m}_{i,j}) = \mathrm{prod}(y_j, y_i; \tilde{m}_{i,j}) \ . \tag{9.2}$$

This assertion proves Theorem 9.3. Indeed, by Theorem 9.2, $(A_+)^\phi$ is generated by $y_1, \dots, y_\ell$ and is a Gaussian monoid. By Theorem 4.1 and (9.2), it follows that $(A_+)^\phi$ is the Artin monoid associated with the Coxeter matrix $\tilde{M} = (\tilde{m}_{i,j})$. Note that, by [5], an Artin monoid is Gaussian if and only if it is of finite Coxeter type. So, the Coxeter group associated with $\tilde{M}$ is finite. Finally, still by Theorem 9.2, A^ϕ is the group of fractions of $(A_+)^\phi$, hence is the Artin group associated with $\tilde{M}$.

Proof of the assertion. Let $X = X_i \cup X_j$. Then y_i is the right l.c.m. of the elements of X_i and is in $(A_{X_i})_+$, y_j is the right l.c.m. of the elements of X_j and is in $(A_{X_j})_+$, and $y_i \vee_R y_j$ is the right l.c.m. of the elements of X and is in $(A_X)_+$. In particular, $y_i \vee_R y_j$ is a simple element. Let w_i be the element of maximal length in W_{X_i}, and let w_j be the element of maximal length in W_{X_j}. Then y_i is $\tau(w_i)$ and y_j is $\tau(w_j)$.

Let a_1 in $(A_X)_+$ be such that $y_i a_1$ is $y_i \vee_R y_j$. If a_1 is the identity, then y_i is equal to $y_i \vee_R y_j$, thus w_i is also the element of maximal length of W_X. This is known not to be the case, therefore a_1 is not the identity. We choose x in X which divides a_1 on the left. The element $y_i x$ is simple since it divides $y_i \vee_R y_j$ on the left. The atom x is in X_j, otherwise, if x is in X_i, then

$$\lg_S(\theta(y_i x)) = \lg_S(w_i x) < \lg_S(w_i) + 1 = \lg_S(y_i x) \ ,$$

and this contradicts (9.1). Since both y_i and $y_i \vee_R y_j$ are in $(A_+)^\phi$, a_1 is also in $(A_+)^\phi$. From the same argument as that given in the proof of Theorem 9.2.ii, it follows that y_j divides a_1 on the left. Let a_2 in $(A_X)_+$ be such that $y_i y_j a_2$ is $y_i \vee_R y_j$. If a_2 is not the identity, then one may choose x in X which divides a_2 on the left, this element has to be in X_i (otherwise $y_i y_j x$ does not satisfy (9.1)), and then y_i divides a_2 on the left. An iteration of this argument finally shows that there exists an integer $m \geq 2$ satisfying

$$y_i \vee_R y_j = \mathrm{prod}(y_i, y_j; m) \ .$$

Similarly, there exists an integer $m' \geq 2$ satisfying

$$y_i \vee_R y_j = \text{prod}(y_j, y_i; m') \ .$$

We have $m = m'$, otherwise (say $m < m'$) there exists a in $(A_X)_+$ satisfying

$$y_i \vee_R y_j = \text{prod}(y_j, y_i; m') = y_j \text{prod}(y_i, y_j; m) a = y_j (y_i \vee_R y_j) a \ ,$$

and this is not possible. Setting $\tilde{m}_{i,j} = m = m'$, this finishes the proof of the assertion. □

A careful reading of the proof of Theorem 9.3 gives a method for finding the Coxeter matrix $\tilde{M} = (\tilde{m}_{i,j})$ that determines the Artin group A^ϕ. For a subset X of S, we denote by n_X the maximal length of an element of W_X. It is known to be equal to the sum of the exponents of W_X. The length of y_i is n_{X_i}, the length of y_j is n_{X_j}, and the length of $y_i \vee_R y_j$ is n_X. So, (9.2) gives:

$$\tilde{m}_{i,j}(n_{X_i} + n_{X_j}) = 2n_X \ . \tag{9.3}$$

Now, the following proposition is a direct consequence of (9.3).

Proposition 9.4. *Let Γ be a connected finite type Coxeter graph, let A be the Artin group associated with Γ, and let ϕ be a non-trivial automorphism of Γ.*

i) If A is of type A_ℓ, then A^ϕ is of type B_k, where k is $\ell/2$ if ℓ is even, and k is $(\ell+1)/2$ if ℓ is odd.

ii) If A is of type D_ℓ and ϕ has order 2, then A^ϕ is of type $B_{\ell-1}$.

iii) If A is of type D_4 and ϕ has order 3, then A^ϕ is of type $I_2(6) = G_2$.

iv) If A is of type E_6, then A^ϕ is of type F_4.

v) If A is of type F_4, then A^ϕ is of type $I_2(8)$.

vi) If A is of type $I_2(p)$, then A^ϕ is of type A_1. □

References

[1] S.I. Adjan, *Defining relations and algorithmic problems for groups and semigroups*, Proc. Steklov Inst. Math. **85** (1966).

[2] S.I. Adjan, *Fragments of the word Delta in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984) 25–34; translated Math. Notes of the Acad. Sci. USSR; 36-1 (1984) 505–510.

[3] J. Birman, K. H. Ko and S. J. Lee, *A new approach to the word problem in the braid groups*, to appear in Advances in Math.

[4]N. Bourbaki, "Groupes et algèbres de Lie, Chapitres 4, 5 et 6", Hermann, Paris, 1968.

[5] E. Brieskorn and K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972), 245–271.

[6] M. Broué, G. Malle, and R. Rouquier, *Complex reflection groups, braid groups, Hecke algebras*, preprint, 1997.

[7] M. Broué and J. Michel, *Sur certains éléments réguliers des groupes de Weyl et les variétés de Deligne-Lusztig associées*, in Finite reductive groupes, Progress in Mathematics, Birkhauser (1996).

[8] R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292** (1992), 671–683.

[9] —, *Geodesic automation and growth functions for Artin groups of finite type*, Math. Ann. **301** (1995), 307–324.

[10] A.H. Clifford and G.B. Preston, "The algebraic theory of semigroups", Math. Surveys, Vol. 7, Amer. Math. Soc., Providence, 1961.

[11] P. Dehornoy, *Deux propriétés des groupes de tresses*, C. R. Acad. Sci. Paris **315** (1992), 633–638.

[12] —, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345** (1994), 115–151.

[13] —, *The structure group for the associativity identity*, J. Pure Appl. Algebra **111** (1996), 59–82.

[14] —, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997), 115–137.

[15] P. Deligne, *Les immeubles des groupes de tresses généralisés*, Invent. Math. **17** (1972), 273–302.

[16] E.A. Elrifai and H.R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45** (1994), 479–497.

[17] D.B.A. Epstein and al., "Word processing in groups", Jones and Bartlett, Boston, 1992.

[18]F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20** (1969), 235–254.

[19] J.E. Humphreys, "Introduction to Lie algebras and representation theory", Springer-Verlag, New York, 1972.

[20] —, “Reflection groups and Coxeter groups”, Cambridge Studies in Advanced Mathematics, Vol. 29, Cambridge University Press, 1990.

[21] C. Labruère, “Groupes d’Artin et mapping class groups”, Ph. D. Thesis, Université de Bourgogne, 1997.

[22] J. Michel, Personal communication.

[23] L. Paris, *Parabolic subgroups of Artin groups*, to appear in J. Algebra.

[24] —, *Centralizers of parabolic subgroups of Artin groups of type A_ℓ, B_ℓ, and D_ℓ*, to appear in J. Algebra.

[25] R. Randell, *The fundamental group of the complement of a union of complex hyperplanes*, Invent. Math. **69** (1982), 103–108. *Correction*, Invent. Math. **80** (1985), 467–468.

[26] J.H. Remmers, *On the geometry of semigroup presentations*, Advances in Math. **36** (1980), 283–296.

[27] D. Rolfsen, “Knots and Links”, Math. Lecture Series, Vol. 7, Publish or Perish, Houston, 1976.

[28] M. Salvetti, *Topology of the complement of real hyperplanes in* $\mathbf{C}^N$, Invent. Math. **88** (1987), 603–618.

[29] K. Tatsuoka, *An isoperimetric inequality for Artin groups of finite type*, Trans. Amer. Math. Soc. **339** (1993), 537–551.

[30] J. Tits, *Le problème des mots dans les groupes de Coxeter*, Symposia Mathematica (INDAM, Rome, 1967–68), Academic Press, London, 1969, pp. 175–185.

[31] H. van der Lek, “The homotopy type of complex hyperplane complements”, Ph. D. Thesis, Nijmegen, 1983.

Authors addresses

Patrick Dehornoy
Université de Caen
Laboratoire SDAD ESA 6081
B.P. 5186, 14032 Caen cedex, FRANCE
dehornoy@math.unicaen.fr

Luis Paris

Université de Bourgogne
Laboratoire de Topologie, UMR 5584 du CNRS
B.P. 400, 21011 Dijon cedex, FRANCE
lparis@satie.u-bourgogne.fr