Contemporary Mathematics

THIN GROUPS OF FRACTIONS

Patrick DEHORNOY

Abstract. A number of properties of spherical Artin–Tits groups extend to Garside groups, defined as the groups of fractions of monoids where least common multiples exist, there is no nontrivial unit, and some additional finiteness conditions are satisfied [**9**]. Here we investigate a wider class of groups of fractions, called *thin*, which are those associated with monoids where minimal common multiples exist, but they are not necessarily unique. Also, we allow units in the involved monoids. The main results are that all thin groups of fractions satisfy a quadratic isoperimetric inequality, and that, under some additional hypotheses, they admit an automatic structure.

1. Introduction

The algebraic theory of braids, as developed in [**15**] and [**14**], relies on the existence of Garside's fundamental elements Δ_n: for each n, the braid Δ_n is an element of the monoid B_n^+ which is a least common multiple of the standard generators σ_i, and the main technical point is that the left divisors of Δ_n in B_n^+ coincide with its right divisors. Most of the results established for Artin's braid groups B_n have been extended to more general groups: spherical Artin–Tits (or simply Artin) groups [**12, 4, 5**], Garside groups in the sense of [**11**], and, subsequently, of [**9**] (also called small or thin Gaussian groups in [**11**] and [**17**], respectively). All the considered groups are groups of fractions of monoids in which least common multiples exist, and, in each case, a key rôle is played by some element Δ of the associated monoid that satisfies most of the technical properties of Garside's braids Δ_n. In particular, it is proved in [**9**] that the greedy normal form of braids [**1, 14, 13**] extends to all Garside groups, and that it gives rise to a bi-automatic structure.

The aim of this paper is to consider groups of fractions of monoids where common multiples exist, but *least* common multiples need not exist. In this case, no counterpart of the element Δ need exist in general, but a number of properties involving the divisors of Δ can still be established when considering subsets of the monoid that are closed under convenient operations. In this way, one can define an extended notion of normal form, which coincides with the greedy normal form when

2000 *Mathematics Subject Classification.* 20M05, 20F36, 05C25.

Key words and phrases. Artin–Tits group, Gaussian group, Garside group, Garside element, normal form, automatic group.

least common multiples exist. The price to pay for the lack of lcm is a possible non-uniqueness. However, we shall see that, at least in good cases, this non necessarily unique normal form is still associated with an automatic structure. We shall be mainly interested in the *thin* case, defined as the case when a *finite* set of generators with good closure properties exists. The main results we prove are:

THEOREM 1.1 (Prop. 4.5). *Every thin group of fractions satisfies a quadratic isoperimetric inequality.*

THEOREM 1.2 (Prop. 9.10). *Assume that G is the group of fractions of a thin cancellative monoid M that admits a Garside element Δ such that all Δ-normal forms in M have the same length. Then G is an automatic group.*

These results apply to all thin Gaussian groups, which are the Garside groups of [**9**], hence in particular to all spherical Artin–Tits groups, for which the properties were already known, but they also apply to groups of a completely different flavour, as some simple examples will show.

The possible interest of our approach is double. On the one hand, as we mentioned, new groups are eligible. On the other hand, we hope that extending classical results may help to understand them better and to capture the really important hypotheses: studying Gaussian groups showed in [**9**] that the fact that Garside's element Δ_n is a least common multiple of the generators σ_i of B_n is useless, and, so, using such a fact gives slightly misleading arguments. Similarly, the approach developed in the current paper shows that a clear distinction should be made between the family of all divisors of Δ (the "simple" elements), and a smaller subfamily (the "primitive" elements) which contains the real information: the latter can be extended to the more general framework, while the former cannot, at least if we use the classical definition. This leads us here to an alternative, hopefully improved definition of a simple element. In the current framework, the proof that the Garside groups are automatic reduces to a small number of technical lemmas, each of which is specially easy when lcm's exist (Lemmas 7.8, 7.12, and 7.13).

The organization of the paper is as follows. In Sec. 2, we introduce the notion of a spanning subset of a monoid, which is a generating set satisfying some additional closure property. Then a thin monoid is defined to be a monoid that admits a finite spanning subset. In Sec. 3, we introduce the weaker notion of a quasi-spanning set so as to allow nontrivial units. In Sec. 4, we define thin groups of fractions as those associated with a thin Ore monoid, and we prove Theorem 1.1. In Sec. 5, we show that every thin monoid admits a minimal spanning subset. In Sec. 6, we introduce the notion of an S-simple element associated with a spanning subset S, which is a counterpart for the notion of divisor of Δ_n in braid monoids. In Sec. 7, we use S-simple elements to construct a counterpart to the greedy normal form of braids. In Sec. 8, we introduce Garside elements, which are convenient generalizations for the fundamental braids Δ_n. Finally, in Sec. 9, we prove Theorem 1.2.

2. Spanning subsets of a monoid

We consider in the sequel cancellative monoids. Most of the results until Sec. 4 are valid if we only assume left cancellativity. If M is a monoid, we say that an element of M is a left (right) unit if it admits a left (right) inverse; provided M is left or right cancellative, $uv = 1$ implies $uvu = u$ and $v = vuv$, hence $vu = 1$, so left and right units coincide, and they form a subgroup of M that will be denoted by M^*. For $u \in M^*$, we denote by u^{-1} the (unique) left and right inverse of u. As multiplying by a unit on the right is often considered in the sequel, we introduce a notation:

Definition 2.1. Assume that M is a (left) cancellative monoid. For $x, x' \in M$, we say that $x \simeq x'$ holds if we have $x' = xu$ for some u in M^*. We say that a subset S of M is *quasi-finite* if it contains finitely many $\simeq$-classes.

The relation $\simeq$ is an equivalence relation which is compatible with left multiplication. For $S \subseteq M$, the set SM^* is the smallest $\simeq$-saturated subset of M including S.

If M is a monoid, and x, y lie in M, we say that x is a left divisor of y, written $x \preceq y$, if $y = xz$ holds for some z. If, in addition, z is not a unit, we say that x is a proper left divisor of y, and write $x \prec y$. We have the symmetric notion of a right divisor, but, as left divisors play a distinguished rôle, we shall usually simply say "divisor" for "left divisor". The set of all (left) divisors of x is denoted $\mathrm{Div}(x)$. If x is a (left) divisor of y, we equivalently say that y is a (right) multiple of x. Notice that $\simeq$ is compatible with $\preceq$ and $\prec$ in the sense that $x \preceq y$ (resp. $x \prec y$) is equivalent to $x' \preceq y'$ (resp. $x' \prec y'$) whenever $x' \simeq x$ and $y' \simeq y$ hold.

The central notion of this paper is that of a spanning subset of a monoid; it is defined by means of some closure properties involving left divisors:

Definition 2.2. Assume that M is a (left) cancellative monoid, and S is a subset of M. We say that S *spans* M if S generates M, it contains 1, it is $\simeq$-saturated, *i.e.*, $SM^* \subseteq S$ holds, and

(2.1) If we have $x \preceq z$ and $y \preceq z$ with $x, y \in S$, then there exist x', y' in S satisfying $xy' = yx' \preceq z$.

We say that M is *thin* (resp. *quasi-thin*) if it admits a finite (resp. quasi-finite) spanning subset.

By definition, a thin monoid is finitely generated, but the converse need not be true, as a spanning subset is more than a generating subset. Note that the converse of Implication (2.1) always holds: $xy' = yx' \preceq z$ trivially implies $x \preceq z$ and $y \preceq z$. Spanning subsets always exist: if M is a monoid, then M is a spanning subset of itself. Actually, we shall be mainly interested in the case when small spanning subsets exist, so, typically, in the thin case. For a monoid with no nontrivial unit, or, more generally, with finitely many units, being quasi-thin is equivalent to being thin.

Example 2.3. Let M be a spherical Artin–Tits monoid, *i.e.*, one associated with a finite Coxeter group W. For $x, y \in M$, define $x\backslash y$ to be the unique element z such that xz is the least common multiple of x and y. Then the closure of the standard generators σ_i under the operation $\backslash$ is a finite spanning subset of M, in one-to-one correspondence with some subset of W [**11**]. So spherical Artin–Tits monoids are thin.

More generally, if M is a Gaussian monoid in the sense of [**11, 9**], *i.e.*, a cancellative monoid in which least common multiples exist and division has no infinite descending chain, then the closure of the set of atoms under operation $\backslash$ is a minimal spanning subset of M. Thus the monoid M is thin if and only if the

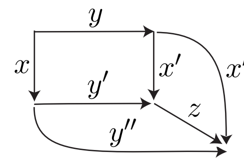

FIGURE 2.1. Spanning subset

latter closure is finite, *i.e.*, if M is thin in the sense of [**17**] (or small in the sense of [**11**]), so the terminologies are compatible.[1]

LEMMA 2.4. *Assume that M is a (left) cancellative monoid, and S is subset of M. Then Condition* (2.1) *for S is equivalent to*

(2.2) *If we have $xy'' = yx''$ with $x, y \in S$, then there exist x', y' in S and z in M satisfying $xy' = yx'$, $x'' = x'z$, and $y'' = y'z$ (Fig. 2.1).*

PROOF. It is clear that (2.2) implies (2.1); conversely, assuming $xy'' = yx''$, Condition (2.1) implies that there exist x', y' in S and z in M satisfying $xy' = yx'$, $xy'' = xy'z$, and $yx'' = yx'z$, hence $x'' = x'z$ and $y'' = y'z$ if we can cancel x and y on the left. □

If S, T are subsets of a monoid M, we put $ST = \{xy\,;\, x \in S, y \in T\}$. In particular, S^p is the set of all elements that can be written as $x_1 \cdots x_p$ with x_1, $\dots$, $x_p \in S$. Notice that $1 \in S$ implies $S \subseteq S^p$ for $p \geq 2$. We put $S^0 = \{1\}$.

LEMMA 2.5. *Assume that M is a monoid, and S is a subset of M satisfying Condition* (2.2). *Then, if we have $xy'' = yx''$ with $x \in S^p$ and $y \in S^q$, there exist an element z of M and two sequences $x_{i,j}$, $y_{i,j}$, $0 \leq i \leq p$, $0 \leq j \leq q$, of elements of S satisfying $x_{i,j-1}y_{i,j} = y_{i-1,j}x_{i,j}$ for all i, j, and $x = \prod x_{i,0}$, $y = \prod y_{0,j}$, $x'' = \prod x_{i,q}\, z$, and $y'' = \prod y_{p,j}\, z$. So, in particular, there exist x' in S^p, y' in S^q and z in M satisfying $xy' = yx'$, $x'' = x'z$, and $y'' = y'z$.*

PROOF. (Fig. 2.2) First, the condition is sufficient, as the local equalities $x_{i,j}y_{i,j+1} = y_{i,j}x_{i+1,j}$ imply $\prod_i x_{i,0} \prod_j y_{p,j} = \prod_j y_{0,j} \prod_i x_{i,q}$, hence $xy'' = yx''$ when x, y, x'', y'' have the above specified values.

We prove now that the condition is necessary. The result is trivial for $p = 0$ or $q = 0$. Indeed, $p = 0$ means $x = 1$: then the hypothesis $y \in S^q$ allows us to write $y = \prod_j y_{0,j}$ with $y_{0,1}$, $\dots$, $y_{0,q} \in S$, and the hypothesis $y'' = yx''$ then gives $y'' = \prod_j y_{0,j} z$ with $z = x''$. Then we use induction on $p + q$. By the remark above, the first nontrivial case is $p = q = 1$, and, then, the result is true by Condition (2.2). Assume now $p + q \geq 3$, with $p, q \geq 1$. Then at least one of p, q is greater than 1. Assume for instance $q \geq 2$. Write $y = y_1y_2$ with $y_1 \in S^{q_1}$, $y_2 \in S^{q_2}$ and $1 \leq q_1, q_2 < q$. Applying the induction hypothesis to $x \in S^p$, $y_1 \in S^{q_1}$ and $xy'' = y_1(y_2x'')$ gives z_1 in M and $x_{i,j}$, $y_{i,j}$, $0 \leq i \leq p$, $0 \leq j \leq q_1$ in S satisfying $x_{i,j-1}y_{i,j} = y_{i-1,j}x_{i,j}$, $y_2x'' = x_1z_1$, $y'' = y'_1z_1$ with

$$x = \prod_1^p x_{i,0}, \quad y_1 = \prod_1^{q_1} y_{0,j}, \quad x_1 = \prod_1^p x_{i,q_1}, \quad y'_1 = \prod_1^{q_1} y_{p,j}.$$

[1]In order to uniformize terminology with other authors, we use *Garside monoid* as a synonym for thin Gaussian monoid, and *Garside group* for the group of fractions of a Garside monoid [**9**].

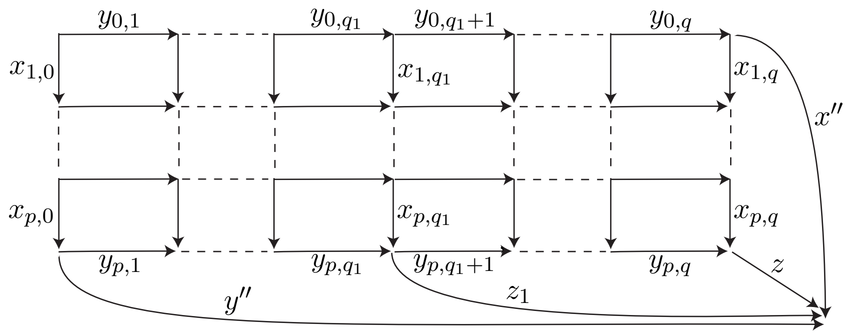

FIGURE 2.2. Power of a spanning subset

Applying the induction hypothesis to $x_1 \in S^p$, $y_2 \in S^{q_2}$ and $x_1 z_1 = y_2 x''$ gives z in M and $x_{i,j}$, $y_{i,j}$, $0 \le i \le p$, $q_1 < q_2$ in S satisfying $x_{i,j-1} y_{i,j} = y_{i-1,j} x_{i,j}$, $x'' = x'z$, $z_1 = y'_2 z$ with

$$x = \prod_1^p x_{i,0}, \quad y_2 = \prod_{q_1+1}^{q_2} y_{0,j}, \quad x' = \prod_1^p x_{i,q}, \quad y'_2 = \prod_{q_1+1}^{q_2} y_{p,j}.$$

Putting $y' = y'_1 y'_2$ gives the expected result.

Finally, with the previous notation, put $x' = \prod_i x_{i,q}$ and $y' = \prod_j y_{p,j}$. By construction, x' lies in S^p, y' lies in S^q, and we have $xy' = yx'$, $x'' = x'z$, and $y'' = y'z$. □

Applying Lemma 2.5 with $q = p$, we obtain

PROPOSITION 2.6. *Assume that M is a (left) cancellative monoid. If S spans M, so does S^p for every positive p.*

Cancellativity is not used in the proof of Lemma 2.5, so, at the expense of using (2.2) instead of (2.1) in the definition of a spanning subset, we could state Prop. 2.6 for a general monoid.

PROPOSITION 2.7. *Assume that M is a (left) cancellative monoid, and S spans M. Then every right divisor of an element of S lies in S, and we have $M^*S \subseteq S$.*

PROOF. Assume $y = xz \in S$. As S generates M, we have $x \in S^p$ for some p, so, applying Lemma 2.5 to the equality $x \cdot z = y \cdot 1$, we find x in S^p, y' in S, and z' in M satisfying $xy' = yx'$, $z = y'z'$, and $1 = x'z'$. The latter relation shows that x' and z' are units and $z = y'z'$ then implies $z \in SM^*$, hence $z \in S$ as S is supposed to be closed under right multiplication by a unit.

Assume $x \in S$ and $u \in M^*$. Then we have $x = u^{-1}(ux)$, so ux is a right divisor of x, and, by the previous result, it belongs to S. □

One of the interests of spanning subsets is that they completely determine the monoid in the sense below. In the sequel, if S is a set (of letters), and R is a set of relations over S, *i.e.*, of equalities of the form $x_1 \cdots x_p = y_1 \cdots y_q$ with $x_1, \ldots,$ $y_q \in S$, we denote by $\langle S; R \rangle^+$ the monoid so presented, and by $\langle S; R \rangle$ the group with the same presentation.

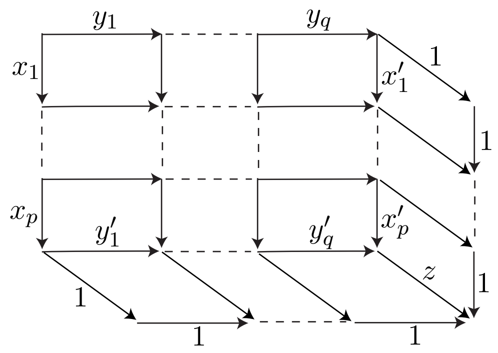

FIGURE 2.3. Quadratic isoperimetric inequality

DEFINITION 2.8. Assume that M is a (left) cancellative monoid, and S spans M. We denote by R_S the set of all relations $xy' = yx'$ with x, y, x', $y' \in S$.

PROPOSITION 2.9. *Assume that M is a (left) cancellative monoid, and S spans M. Then $\langle S; R_S\rangle^+$ is a presentation of M, and every equality $x_1 \cdots x_p = y_1 \cdots y_q$ with $x_1, \ldots, y_q \in S$ can be proved using $O((p+q)^2)$ relations of R_S.*

PROOF. (Fig. 2.3) The set S generates M by definition. Assume $x_1 \cdots x_p = y_1 \cdots y_q$ with $x_1, \ldots, y_q \in S$. By Lemma 2.5, there exist $x'_1, \ldots, x'_p, y'_1, \ldots, y'_q \in S$ and $z \in M$ satisfying

$$x_1 \cdots x_p y'_1 \cdots y'_q = y_1 \cdots y_q x'_1 \cdots x'_p, \quad x'_1 \cdots x'_p z = 1, \quad \text{and } y'_1 \cdots y'_q z = 1,$$

and, moreover, the first equality can be established using pq relations in R_S. As for the other ones, we know by Prop. 2.7 that each of the elements $x'_i \cdots x'_p z$ and $y'_j \cdots y'_q z$ belongs to S, and, therefore, the equality $x'_1 \cdots x'_p z = 1$ can be established using p relations of R_S (of the special form $xy = 1$), and, similarly, $y'_1 \cdots y'_q z = 1$ can be established using q relations of R_S. So, finally, the equality $x_1 \cdots x_p = y_1 \cdots y_q$ can be established using at most $(p+q)^2/4 + (p+q)$ relations of R_S. □

Applying the previous result to the case of a finite spanning subset, we obtain:

PROPOSITION 2.10. *Every thin cancellative monoid satisfies a quadratic isoperimetric inequality.*

In order to construct new examples of thin monoids, Prop. 2.9 suggests that we consider presentations where the relations are of the form $xy' = yx'$, *i.e.*, involve words of length at most 2. Every monoid admits a presentation of this type, and the question arises of recognizing spanning subsets. Typically, if $\langle S; R\rangle^+$ is a presentation of the type above for a monoid M, there is no obvious reason why S should span M, as some equalities in M may follow from the relations of R but not decompose into such relations using the scheme of Fig. 2.3. In particular, there is no reason why the equality $R = R_S$ should hold. Here, we shall refer to [**10**], where the notion of a complete presentation is defined. The idea is that a presentation is complete if enough relations have been displayed to avoid any hidden consequence.

Some definitions are necessary in order to describe the results precisely. The main notion is that of *word reversing*. Assuming that (S, R) is a semigroup presentation (*i.e.*, R consists of relations $u = v$ where u, v are nonempty words), we consider words over the symmetrized alphabet $S \cup S^{-1}$ where each letter x in S has a formal copy x^{-1} in S^{-1}; now, for w, w' words on $S \cup S^{-1}$, we say that w is *R-reversible* to w' if w' can be obtained from w by (iteratively) replacing some subwords of the form $u^{-1}v$ with new words $v'u'^{-1}$ provided u, v are nonempty words on S and $uv' = vu'$ is a relation in R (we allow in particular replacing $u^{-1}u$ with the empty word, *i.e.*, we assume that the trivial relation $u = u$ belongs to R).

It is not hard to see that word reversing produces R-equivalent words in the sense that, if u, v are words on S and $u^{-1}v$ is R-reversible to the empty word, then the words u and v are R-equivalent. We say that the presentation (S, R) is *complete* (on the right) when the converse implication is true, *i.e.*, if $u^{-1}v$ must be R-reversible to the empty word whenever u and v are R-equivalent words on S. In other words, the presentation is complete when word reversing detects every possible word equivalence.

Assume that u, v, w are three words on S. We say that the presentation (S, R) satisfies the *cube condition* for (u, v, w) if, for all words $u_1, u_2, v_1, v_2, w_1, w_2$ on S such that $u^{-1}w$ is R-reversible to $w_1u_1^{-1}$, $w^{-1}v$ is R-reversible to $v_1w_2^{-1}$, and $u_1^{-1}v_1$ is R-reversible to $v_2^{-1}u_2$, there exist three words u_0, v_0, w_0 on S such that $u^{-1}v$ is R-reversible to $v_0u_0^{-1}$, the word w_1v_2 is R-equivalent to v_0w_0, and the word w_2u_2 is R-equivalent to u_0w_0. Now the result is that, provided we consider a presentation (S, R) in which the relations preserve the length of the words—actually it is enough that they preserve some much weaker parameter, but this will not be needed for the examples we have in mind—then (S, R) is complete if and only if it satisfies the cube condition for each triple of letters. In good cases (essentially, when R-reversing admits no infinite sequence), we obtain in this way an effective criterion for recognizing complete presentations.

Now, the main advantage of complete presentations is that many properties of the defined monoid can be read from the presentation directly [**10**]. For instance, when (S, R) is a complete presentation, a sufficient condition for the monoid $\langle S, R\rangle^+$ to admit left cancellation is that R contains no relation of the form $xu = xv$ with $u \neq v$: if there is no obvious counter-example to cancellativity, then there is no hidden counter-example either. Also, a sufficient condition for S completed with 1 to span $\langle S, R\rangle^+$ is that all relations in R are of the form $u = v$ with u and v of length 1 or 2.

Example 2.11. With the previous method, we can exhibit thin monoids that do not resemble the Gaussian monoids of Example 2.3, namely monoids where least common multiples do not exist. The following three examples are typical, and they will be considered throughout the paper:

$$M_1 = \langle a, b\,;\, a^2 = b^2, ab = ba\rangle^+,$$
$$M_2 = \langle a, b, c\,;\, a^2 = b^2 = c^2, ab = bc = ca, ac = ba = cb\rangle^+,$$
$$M_3 = \langle a, b, c\,;\, ac = ca = b^2, ab = bc, cb = ba\rangle^+.$$

It is easy (although tedious) to check that the above presentations satisfy the cube condition for each triple of letters. So they are complete, and the above results apply. Firstly, in each case, the involved set of generators completed with 1 is a spanning subset, and, therefore, the monoid M_i is thin. Secondly, there is no relation $xu = xv$ with $u \neq v$ in the presentation, so the monoid M_i is (left) cancellative (the case of right cancellation is treated symmetrically, by introducing a convenient notion of left reversing and left completeness).

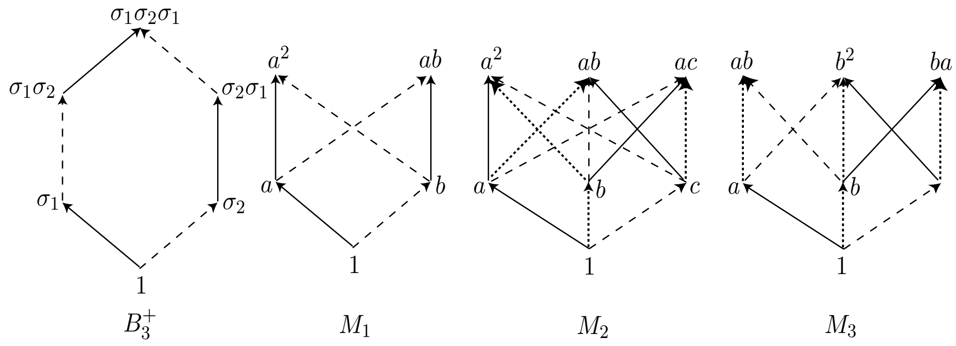

FIGURE 2.4. Characteristic graph associated with a spanning subset

If S spans a monoid M, then M is determined by S and R_S. Especially when the considered set S is finite, *i.e.*, in the thin case, it is natural to introduce the subgraph of the Cayley graph of M displaying the relations of R_S: by the remarks above, such a (finite) graph completely determines the monoid. In the Gaussian case, *i.e.*, when least common multiples exist, the graph is a lattice, in the sense that any two vertices admit a unique immediate common successor. In the general case, this need not be true. For instance, we display in Fig. 2.4 the graphs associated with the braid monoid B_3^+ and the spanning subset $\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1\}$, and with the thin monoids M_1, M_2, M_3 of Example 2.11.

3. Quasi-spanning subsets

Many results for the thin case extend to the quasi-thin case, and, to deal with the latter, it is convenient to introduce the notion of a quasi-spanning subset of a monoid, of which a typical example is a $\simeq$-selector through a spanning set, *i.e.*, a subset that picks one element in each equivalence class.

DEFINITION 3.1. Assume that M is a (left) cancellative monoid, and S is a subset of M. We say that S *quasi-spans* M if SM^* spans M.

By definition, a spanning subset is quasi-spanning, and both notions coincide if there is no nontrivial unit.

PROPOSITION 3.2. *Assume that M is a (left) cancellative monoid, and S spans M. Then every $\simeq$-selector through S quasi-spans M. Conversely, if S is a minimal quasi-spanning subset of M, then S is a $\simeq$-selector.*

PROOF. If Σ is a $\simeq$-selector through S, we have $\Sigma M^* = S$, so Σ is quasi-spanning. On the other hand, assume that S is a minimal quasi-spanning subset of M. Assume $y \simeq x$, with $x, y \in S$ and $x \neq y$. Then $(S - \{y\})M^*$ is equal to SM^*, and, therefore, $S - \{y\}$ quasi-spans M, contradicting the minimality of S. □

COROLLARY 3.3. *A cancellative monoid is quasi-thin if and only if it admits a finite quasi-spanning subset.*

LEMMA 3.4. *Assume that M is a (left) cancellative monoid, and S is a subset of M. Then S quasi-spans M if and only if SM^* generates M and contains* 1,

$M^*S \subseteq SM^*$ holds, and

$$\text{(3.1)} \qquad \begin{array}{l}\textit{If we have } x \preceq z \textit{ and } y \preceq z \textit{ with } x,\, y \in S,\\ \textit{then there exist } x',\, y' \textit{ in } S \textit{ satisfying } xy' \simeq yx' \preceq z.\end{array}$$

Proof. Assume that S satisfies the above conditions. Then SM^* contains 1, it generates M by hypothesis, and it is $\simeq$-saturated by construction. Assume $xu \preceq z$ and $yv \preceq z$ with x, $y \in S$, and u, $v \in M^*$. Then we have $x \preceq z$ and $y \preceq z$, so, by (3.1), there exist x', y' in S satisfying $xy' \simeq yx' \preceq z$, say $xy' = yx'w \preceq z$ with $w \in M^*$. Then we have also $(xu)(u^{-1}y') = (yv)(v^{-1}x'w) \preceq z$, and the elements $u^{-1}y'$ and $v^{-1}x'w$ belong to M^*SM^*, hence to SM^*, which therefore satisfies Condition (2.1), and spans M.

Conversely, assume that S quasi-spans M. Then $1 \in M^*$ implies $S \subseteq SM^*$, and restricting Condition (2.1) for SM^* to S yields Condition (3.1). Moreover, we have $M^*SM^* \subseteq SM^*$ by Prop. 2.7, hence, a fortiori, $M^*S \subseteq SM^*$. So all conditions of Lemma 3.4 are satisfied. □

If S quasi-spans a monoid M, then we have $M^*S \subseteq SM^*$ by Lemma 3.4, hence $M^*SM^* = SM^*$, and a straightforward induction then implies

$$\text{(3.2)} \qquad (SM^*)^n = S^nM^*$$

for every positive n. As SM^* is supposed to generate M, it follows that every element of M admits a decomposition of the form $x = x_1 \cdots x_n u$ with $x_1, \ldots,$ $x_n \in S$ and $u \in M^*$.

Proposition 3.5. *Assume that M is a (left) cancellative monoid and S quasi-spans M.*
(i) The subset S^p quasi-spans M for every positive p.
(ii) If we have $x \preceq z$ and $y \preceq z$ with $x \in S^p$ and $y \in S^q$, then there exist $x' \in S^p$ and $y' \in S^q$ satisfying $xy' \simeq yx' \preceq z$.
(iii) If we have $x_i \preceq z$ with $x_i \in S$ for $1 \leq i \leq n$, then there exists x in S^n satisfying $x_i \preceq x \preceq z$ for $1 \leq i \leq n$.

Proof. (i) By definition, SM^* spans M, so, by Prop. 2.6, $(SM^*)^p$ spans M as well for every positive p. By (3.2), the latter is S^pM^*, and, by Lemma 3.4 again, S^pM^* spanning M implies S^p quasi-spanning M.

(ii) Applying Lemma 2.5 to the spanning subset SM^* of M, we obtain x'' in $(SM^*)^p$ and y'' in $(SM^*)^q$ satisfying $xy'' = yx'' \preceq z$. By (3.2), we have $(SM^*)^p = S^pM^*$ and $(SM^*)^q = S^qM^*$, so we deduce that there exist x' in S^p, y' in S^q, and u, v in M^* satisfying $x'' = x'u$ and $y'' = y'v$, hence $xy' \simeq yx' \preceq z$.

(iii) We use induction on $n \geq 1$. For $n = 1$, we take $x = x_1$. Assume $n \geq 2$. By induction hypothesis, some y in S^{n-1} satisfies $x_i \preceq y \preceq z$ for $i \leq n-1$. Applying (ii) to x_n and y, we obtain x' in S and y' in S^{n-1} satisfying $x_ny' \simeq yx' \preceq z$. Putting $x = yx'$ gives the result. □

Proposition 3.6. *Assume that M is a (left) cancellative monoid and S is a minimal quasi-spanning subset of M. Then, for every pair (x, u) in $S \times M^*$, there exists a unique pair (x', u') in $S \times M^*$ satisfying $ux = x'u'$. The mapping $x \mapsto x'$ defines an action of the group M^* on S. If x is fixed under this action, the mapping $u \mapsto u'$ is an endomorphism of M^* for every x.*

Proof. By Lemma 3.4, we have $M^*S \subseteq SM^*$, so $ux \in SM^*$, *i.e.*, there exist x' in S and u' in M^* satisfying $ux = x'u'$. The uniqueness of x' follows from Prop. 3.2,

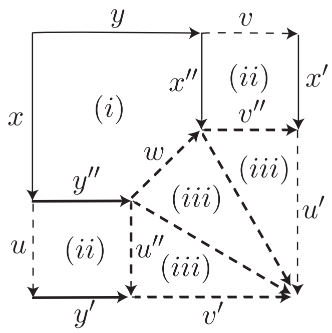

Figure 3.1. Decomposition of a relation

and that of u' then follows from left cancellativity. Writing ${}^{u}x$ for x', we have $1x \simeq x$ for every x in S, and, therefore ${}^{1}x = x$, and $uvx \simeq u{}^{v}x \simeq {}^{u}({}^{v}x)$, hence ${}^{uv}x = {}^{u}({}^{v}x)$.

Assume now ${}^{u}x = x$. Writing u^x for u', we find $(uv)x = uxv^x = xu^xv^x$, hence $(uv)^x = u^xv^x$. □

The previous result gives a way for constructing quasi-thin monoids with a prescribed group of units. Assume that M is a cancellative monoid with no non-trivial unit, S spans M, and G is a group with a left action on M that preserves S globally. Consider the semi-direct product $M \rtimes G$ where $(x, u)(y, v)$ is defined to be $(xu(y), uv)$. The set of units in $M \rtimes G$ is $\{1\} \times G$, and the set $S \times \{1\}$ is a quasi-spanning subset of $M \rtimes G$. More generally, instead of a semidirect product, we could also use a crossed product as in [**17**].

In the same way as a spanning subset determines a monoid, a quasi-spanning subset together with the units determine a monoid.

Definition 3.7. Assume that M is a (left) cancellative monoid, and S quasi-spans M. We denote by R^*_S the set consisting of

(i) all relations $xy' = yx'u$ with x, y, x', $y' \in S$ and $u \in M^*$,
(ii) all relations $ux = x'u'$ with x, $x' \in S$ and u, $u' \in M^*$,
(iii) all relations $uv = w$ with u, v, $w \in M^*$.

Proposition 3.8. *Assume that M is a (left) cancellative monoid, and S quasi-spans M. Then $\langle S{\cup}M^*; R^*_S\rangle^+$ is a presentation of M, and every equality $x_1 \cdots x_p = y_1 \cdots y_q$ with $x_1, \ldots, y_q \in S$ can be proved using $O((p + q)^2)$ relations of R^*_S.*

Proof. By Lemma 3.4, the set SM^* spans M, so, by Prop. 2.9, $\langle SM^*; R_{SM^*}\rangle^+$ is a presentation of M, and every equality $x_1 \cdots x_p = y_1 \cdots y_q$ with $x_1, \ldots, y_q \in SM^*$ can be established using at most $O((p+q)^2)$ relations in R_{SM^*}. So, it suffices to prove that every relation in R_{SM^*} can be decomposed into a uniformly bounded number of relations in R^*_S. By construction, every element in SM^* can be expressed as xu with $x \in S$ and $u \in M^*$. So assume $xuy'v' = yvx'u'$ with x, y, x', $y' \in S$ and u, v, u', $v' \in M^*$. There exist x'', y'' in S and u'', v'' in M^* satisfying the type (ii) relations $uy' = y''u''$ and $vx' = x''v''$: then $xuy'v' = yvx'u'$ implies the type (i) relation $xy''w = yx''$ with $w = u''v'u'^{-1}v''^{-1}$, and the latter equality follows from three type (iii) relations (Fig. 3.1). Thus every relation of R_{SM^*} can be decomposed into at most six relations in R^*_S. □

Instead of using all units in the presentation, we can replace M^* with any set that generates it (as a monoid). We obtain:

Corollary 3.9. *Assume that M is a (left) cancellative monoid, S quasi-spans M, and $\langle S'; R'\rangle^+$ is a presentation of M^* as a monoid. Let R consist of*
(i) all relations $xy' = yx'u_1 \cdots u_p$ with $x, y, x', y' \in S$, $u_1, \dots, u_p \in S'$,
(ii) all relations $ux = x'u'_1 \cdots u'_p$ with $x, x' \in S$, $u, u'_1, \dots, u'_p \in S'$.
Then $\langle S \cup S'; R \cup R'\rangle^+$ is a presentation of M.

The question of whether an isoperimetric inequality is satisfied when the previous presentation is finite is open: even if we assume that the presentation of the group M^* satisfies such a condition, there is no easy way to conclude for M as we know nothing about the elements denoted u'', v'', and w in Fig. 3.1.

4. Thin groups of fractions

By a well known result of Ore [**7**], a cancellative monoid M embeds in a group of (right) fractions if and only if any two elements of M admit at least one common multiple. A monoid satisfying such conditions will be called a *Ore monoid* in the sequel. It is then natural to consider those groups of fractions that are associated with thin monoids:

Definition 4.1. We say that a group G is a *thin* (resp. *quasi-thin*) group of fractions if there exists a thin (resp. quasi-thin) Ore monoid M such that G is the group of fractions of M.

Thus, the braid groups B_n, the spherical Artin–Tits groups, and, more generally, the Garside groups of [**9**] are thin groups of fractions. We shall give more examples below.

A nice point is that, when a quasi-spanning subset is known in a monoid M, then it is easy to study the possible existence of common multiples in M. Indeed, we have the following criterion:

Proposition 4.2. *Assume that M is a (left) cancellative monoid, and S is a quasi-spanning subset in M. Then any two elements of M admit a common multiple if and only the following condition holds:*

(4.1) *For all x, y in S, there exist x', y' in S satisfying $xy' \simeq yx'$.*

Proof. Assume $x, y \in S$. If common multiples always exist in M, there exists z satisfying $x \preceq z$ and $y \preceq z$, and, therefore, since S is quasi-spanning, there exist x', y' in S satisfying $xy' \simeq yx'(\preceq z)$. So (4.1) holds.

Conversely, assume (4.1). First, we claim that, for all x, y in SM^*, there exist x', y' in SM^* satisfying $xy' = yx'$. Indeed, assume $x \simeq x_0$, $y \simeq y_0$ with $x_0, y_0 \in S$. By hypothesis, there exists z satisfying $x_0 \preceq z$ and $y_0 \preceq z$. Then $x \preceq z$ and $y \preceq z$ hold as well. As SM^* spans M, we deduce that there exist x', y' in SM^* satisfying $xy' = yx'(\preceq z)$.

We prove now that, if x belongs to $(SM^*)^p$ and y belongs to $(SM^*)^q$, then x and y admit a common multiple in M. The result is trivial for $p = 0$ and $q = 0$, and the case $p = q = 1$ has been treated above. Then we use a recurrence on $p + q$: the principle is to construct a diagram like the one in Fig. 2.2 starting from the left and the top edges. By hypothesis, each small square can be closed, so, inductively, the full diagram can be completed. □

It follows that, if M is a cancellative monoid and S is a quasi-spanning subset in M that satisfies (4.1), then M is a Ore monoid, and it embeds in a group of right fractions. Moreover, the latter admits the presentation $\langle S; R_S\rangle$, where R_S is as in Prop. 2.9. In particular, we can state:

Corollary 4.3. *Assume that M is a thin cancellative monoid and S spans M and satisfies* (4.1). *Then the group $\langle S; R_S\rangle$ is a thin group of fractions.*

Example 4.4. For $i = 1, \dots, 3$, the monoid M_i of Example 2.11 satisfies Condition (4.1), as we can check on the graph of Fig. 2.4. Thus, any two elements in M_i admit a common multiple, and, therefore, M_i embeds in a group of fractions. So the groups

$$G_1 = \langle a, b\,;\, a^2 = b^2, ab = ba\rangle$$
$$G_2 = \langle a, b, c\,;\, a^2 = b^2 = c^2, ab = bc = ca, ac = ba = cb\rangle$$
$$G_3 = \langle a, b, c\,;\, ac = ca = b^2, ab = bc, cb = ba\rangle$$

are thin groups of fractions.

Observe that the monoid $\langle a, b, c\,;\, ab = bc = ca\rangle^+$ is the Birman-Ko-Lee monoid for the braid group B_3 [**2**]; then M_2 is the quotient of the latter monoid under the additional relation $a^2 = b^2$, and, therefore, the group G_2 is the quotient of B_3 obtained by adding the relation $\sigma_1^2 = \sigma_2^2$, thus an intermediate group between B_3 and the symmetric group S_3.

We can now state our first general result about thin groups of fractions:

Proposition 4.5. *Every thin group of fractions satisfies a quadratic isoperimetric inequality.*

Proof. Assume that G is the group of fractions of the Ore monoid M, and S is a finite spanning subset of M. By Prop. 2.9, $\langle S; R_S\rangle^+$ is a presentation of M, and, therefore, $\langle S; R_S\rangle$ is a presentation of G, which is finite by construction. Assume that $x_1^{e_1} \cdots x_n^{e_n} = 1$ holds in G, with $x_1, \dots, x_n \in S$ and $e_1, \dots, e_n = \pm 1$. First, an easy induction on m shows that, if the sequence $(e_1, \dots, e_n)$ contains p times $+1$, q times -1, and m subpairs $(-1, +1)$, then there exist $y_1, \dots, y_p$ and $z_1, \dots, z_q$ in M such that $x_1^{e_1} \cdots x_n^{e_n} = y_1 \cdots y_p z_q^{-1} \cdots z_1^{-1}$ holds in G, and the equality can be established using m relations of R_S. Then $x_1^{e_1} \cdots x_n^{e_n} = 1$ in G implies $y_1 \cdots y_p = z_1 \cdots z_q$ in G, hence in M. By Prop. 2.9 again, the latter equality, if true, can be established using at most $(p + q)^2$ relations of R_S. We have $m \le pq \le (p + q)^2/4$ and $p + q = n$, so, alltogether, we need $5n^2/4$ relations of R_S at most to establish $x_1^{e_1} \cdots x_n^{e_n} = 1$. □

So, for instance, all Garside groups satisfy a quadratic isoperimetric inequality—as was already proved in [**11**]—and so do the groups G_i of Example 4.4.

If we consider a Ore monoid M which is quasi-thin only, there is no clear result, as the complexity of the group of units is involved. If the group M^* is finite, then the presentation of Prop. 3.8 is finite, and it gives rise to a quadratic isoperimetric inequality: however, in this case, M is thin, and Prop. 4.5 applies.

5. Primitive elements

The rest of the paper is centered on the possible existence of an automatic structure for a thin group of fractions, a strengthening of the existence of a quadratic isoperimetric inequality. In this section, we show that every thin monoid admits a minimal spanning subset, whose elements will be called primitive. Such primitive elements are themselves connected with atoms, and we begin with some observations about such elements which extend earlier results of [**11, 9**] so as to allow the existence of nontrivial units.

DEFINITION 5.1. Assume that M is a cancellative monoid. We say that an element x of M is an *atom* if x is not a unit but $x = yz$ implies that either y or z is a unit. The set of all atoms in M is denoted by A_M.

LEMMA 5.2. *If M is a cancellative monoid, then the atoms of M are closed under left and right multiplication by a unit, and, therefore, $\simeq$-saturated.*

PROOF. Assume $x \in A_M$ and $u \in M^*$. First, $xu \in M^*$ would imply $x \in M^*$, so we have $xu \notin M^*$. Then assume $xu = yz$. We have $x = y(zu^{-1})$, hence either y or zu^{-1} is a unit, and, in the latter case, so z. So xu is an atom. The case of left multiplication by a unit is similar. □

DEFINITION 5.3. Assume that M is a monoid. For $x \in M$, we put $\|x\| = 0$ if x is a unit, and

$$\|x\| = \sup\{n\,;\,(\exists x_1, \dots, x_n \in A_M)(x = x_1 \cdots x_n)\}$$

otherwise, if such a decomposition exists and the involved supremum is finite. Then we say that M is *quasi-atomic* if $\|x\|$ exists for each x in M.

Thus, M is quasi-atomic if and only if it is generated by its atoms and its units, and, moreover, for each x in M, the maximal number of atoms occurring in a decomposition of x is finite. If there is no nontrivial unit in the monoid M, then M is quasi-atomic if and only if it is atomic in the sense of [**11, 9**].

LEMMA 5.4. *Assume that M is a quasi-atomic monoid. Then we have*

$$\|x\| = 0 \Leftrightarrow x \in M^*, \tag{5.1}$$

$$\|xy\| \geq \|x\| + \|y\|, \tag{5.2}$$

$$u \in M^* \Rightarrow \|xu\| = \|ux\| = \|x\|, \tag{5.3}$$

for all x, y in M. So $x \simeq x'$ implies $\|x\| = \|x'\|$.

PROOF. For (5.1), $x \in M^*$ implies $\|x\| = 0$ by definition. Conversely, for $x \notin M^*$, the hypothesis that $\|x\|$ exists means that x can be expressed as a finite product of atoms, so, by definition, $\|x\| \geq 1$ holds in this case.

Assume now $\|x\| = p$ and $\|y\| = q$. For $p = q = 0$, both x and y are units, so is xy, and we have $\|xy\| = 0 = p + q$. For $p > 0$ and $q = 0$, y is a unit, while x admits a decomposition $x = x_1 \cdots x_p$ with $x_1, \dots, x_p \in A_M$. Then $x_p y$ is an atom, and we obtain $xy = x_1 \cdots x_{p-1}(x_p y)$, hence $\|xy\| \geq p = p + q$. The argument is similar for $p = 0$ and $q > 0$. Assume now $p > 0$ and $q > 0$. Then x and y admit decompositions $x = x_1 \cdots x_p$, $y = y_1 \cdots y_q$ with $x_1, \dots, y_q \in A_M$, and we deduce $xy = x_1 \cdots x_p y_1 \cdots y_q$, hence $\|xy\| \geq p + q$. This shows (5.2).

Assume $u \in M^*$. Then (5.2) gives $\|xu\| \geq \|x\|$. Applying this with xu instead of x and u^{-1} instead of u, we obtain $\|(xu)u^{-1}\| \geq \|xu\|$, *i.e.*, $\|x\| \geq \|xu\|$, whence $\|xu\| = \|x\|$. The argument is similar for ux. □

Proposition 5.5. *A monoid M is quasi-atomic if and only if there exists a mapping $l : M \to \mathbb{N}$ satisfying, for all x, y in M,*

$$l(x) = 0 \Rightarrow x \in M^*, \tag{5.4}$$

$$l(xy) \geq l(x) + l(y). \tag{5.5}$$

Proof. Lemma 5.4 shows that the mapping $\|\|$ satisfies (5.4) and (5.5) when M is quasi-atomic, so the condition is necessary.

Conversely, assume that l is a mapping satisfying (5.4) and (5.5). Assume $x \in M - M^*$, and let $x = x_1 \cdots x_p$ be a decomposition of x into non-invertible elements. By (5.4), we have $l(x_i) \geq 1$ for each i, and, by (5.5), $l(x) \geq l(x_1) + \cdots + l(x_p)$, hence $l(x) \geq p$. So, the supremum n of the lengths of the decompositions of x into a product of non-invertible elements satisfies $n \leq l(x)$, and, therefore, it is finite. Now, let $x = x_1 \cdots x_n$ be such a decomposition with maximal length. We claim that $x_1, \ldots, x_n$ are atoms. Indeed, if x_i is not an atom, it can be decomposed as $x_i = x_i' x_i''$ with neither x_i' nor x_i'' in M^*, and replacing x_i with $x_i' x_i''$ gives a decomposition of x of length $n + 1$. Hence every non-invertible element x of M is a product of at most $l(x)$ atoms. This shows that M is quasi-atomic, and that $\|x\| \leq l(x)$ holds for every x in M. □

Example 5.6. The monoids M_i of Example 2.11 all are quasi-atomic, and even atomic as they contain no nontrivial unit: as the defining relations preserve the length, the latter induces a well defined mapping l of M_i to $\mathbb{N}$ that satisfies (5.4) and (5.5).

The previous situation is general, as we have:

Proposition 5.7. *Every thin cancellative monoid is quasi-atomic.*

Proof. Assume that M is a thin cancellative monoid, and S is a finite spanning subset of M. Let $x \in M$. As S generates M, x belongs to S^p for some p. Now, let $x = x_1 \cdots x_n$ be an arbitrary decomposition of x with $x_1, \ldots, x_n \in S - M^*$. By Prop. 2.7, S^p spans M, so the element $x_i \cdots x_n$, which is a right divisor of x, belongs to S^p as well. Assume $n \geq \mathrm{card}(S^p)$. Then there exist i, j with $0 \leq i < j \leq n$ satisfying $x_i \cdots x_n = x_j \cdots x_n$, which implies $x_i \cdots x_{j-1} = 1$ and contradicts the assumption $x_i \notin M^*$. Thus we must have $n \leq \mathrm{card}(S^p) \leq \mathrm{card}(S)^p$. Let us define $l(x)$ to be the maximal possible value of n in a decomposition as above. It is clear that $l(x) = 0$ implies $x \in M^*$, and that $l(xy) \geq l(x) + l(y)$ always holds, as concatenating a maximal decomposition for x and a maximal decomposition for y shows. So the mapping l satisfies the conditions (5.4) and (5.5), and, by Prop. 5.5, M is quasi-atomic. □

When we only assume that a finite quasi-spanning set exists, the situation is more complicated. However, we can still recognize quasi-atomicity as follows:

Proposition 5.8. *Assume that M is a quasi-thin cancellative monoid. Then M is quasi-atomic if and only if the group M^* is closed under conjugation in M, in the sense that, if $xu = u'x$ holds, then $u \in M^*$ implies $u' \in M^*$.*

Proof. Assume that M is quasi-atomic and we have $xu = u'x$ with $u \in M^*$. By Lemma 5.4, we have $\|x\| = \|xu\| = \|u'x\| \geq \|u'\| + \|x\|$, hence $\|u'\| = 0$, and $u' \in M^*$ by (5.1). So the condition is necessary.

Conversely, assume that M^* is closed under conjugation, and S is a finite quasi-spanning set in M. We adapt the argument of the proof of Prop. 5.7. Let $x \in M$.

Then x belongs to S^pM^* for some p. Let $x = x_1 \cdots x_n u$ be any decomposition of x with with $x_1, \ldots, x_n \in S - M^*$ and $u \in M^*$. The set S^pM^* spans M, so, by Prop. 2.7, $x_i \cdots x_n$, which is a right divisor of x, belongs to S^pM^* for each i. If $n \geq \mathrm{card}(S^p)$ holds, there exist i, j with $0 \leq i < j \leq n$ satisfying $x_i \cdots x_n \simeq x_j \cdots x_n$, so we have $(x_i \cdots x_{j-1})(x_j \cdots x_n) = (x_j \cdots x_n)u$ for some unit u. This, by hypothesis, implies $x_i \cdots x_{j-1} \in M^*$, contradicting the hypothesis $x_i \notin M^*$. So we must have $n \leq \mathrm{card}(S^p) \leq \mathrm{card}(S)^p$. If we define $l(x)$ to be the maximal possible value of n in a decomposition as above, then l satisfies (5.4) and (5.5), and M is quasi-atomic. □

If M is a quasi-atomic cancellative monoid, then the relation $\prec$ is a strict partial ordering with no infinite descending chain (and so is its right counterpart). Indeed, by (5.2), $x \prec y$ implies $\|x\| < \|y\|$, so $\prec$ may admit no cycle, hence it is a strict partial ordering, and it admits no infinite descending chain since $(\mathbb{N}, <)$ does not. In such a framework, we can introduce the notion of a minimal common (right) multiple ("mcm"), which extends the notion of a least common multiple ("lcm"):

Definition 5.9. Assume that M is a monoid. For x, $y \in M$, we say that z is an *mcm* of x and y if both $x \preceq z$ and $y \preceq z$ hold, but $x \preceq z'$ and $y \preceq z'$ hold for no proper divisor z' of z. We denote by $C(x, y)$ the set of all elements y' such that xy' is an mcm of x and y (if any).

An mcm is like a lcm, except that we require no uniqueness. For instance, in the monoid M_1 of Example 2.11, the elements a and b admit two mcm's, namely a^2 and ab, but they admit no lcm, as we have neither $a^2 \preceq ab$ nor $ab \preceq a^2$.

Lemma 5.10. *Assume that M is a quasi-atomic cancellative monoid. Then, for all x, y in M, every common multiple of x and y (if any) is a multiple of some mcm of x and y.*

Proof. Assume $x \preceq z$ and $y \preceq z$. Let $Z = \{z' \preceq z \,;\, x \preceq z', y \preceq z'\}$. Then any element z' of Z such that $\|z'\|$ has the least possible value is an mcm of x and y. □

We are now ready to introduce the notion of a primitive element:

Definition 5.11. Assume that M is a quasi-atomic cancellative monoid. We say that an element x of M is *primitive* if x belongs to the smallest subset S of M that contains the atoms and is such that, if x and y belong to S, so does y' whenever xy' is an mcm of x and y. The set of all primitive elements of M is denoted by P_M.

In other words, P_M is the closure of A_M under operation C.

Example 5.12. If any two elements admitting a common multiple admit a lcm, the set $C(x, y)$ is either empty, or it consists of a single element $x\backslash y$, so the primitive elements are the closure of the atoms under operation $\backslash$.

Consider now the monoid M_1 of Example 2.11. There are two atoms, namely a and b. We observed above that a and b admit two right mcm's, namely a^2 and ab, so $C(a, b)$ consist of the two elements a and b, and so does $C(b, a)$. It follows that the closure of A_M under C is the set $\{1, a, b\}$, *i.e.*, there are three primitive elements in M_1.

The reader can easily check that there are four primitive elements in the monoids M_2 and M_3, namely 1 and the atoms a, b, and c.

Lemma 5.13. *Assume that M is a quasi-atomic cancellative monoid. Then the set P_M is closed under right multiplication by a unit, and, therefore, it is $\simeq$-saturated.*

Proof. Assume $x \in P_M$, and $u \in M^*$. If x is an atom, then xu is an atom as well, so it is primitive. Otherwise, there exist y, z in P_M such that yx is an mcm of y and z. In this case, yxu is also an mcm of y and z, so xu also belongs to $C(y, z)$, and, therefore, it is primitive. So, we have $P_M M^* \subseteq P_M$, and, therefore, P_M is $\simeq$-saturated. □

We can now prove:

Proposition 5.14. *Assume that M is a quasi-atomic cancellative monoid. Then P_M spans M, and every spanning subset of M includes P_M.*

Proof. First, P_M is $\simeq$-saturated by Lemma 5.13. Then, if x is an atom of M and u is a unit, xu is an mcm of x and x, and, therefore, u is primitive. Thus P_M includes A_M and M^*, and, therefore, it generates M. Next, assume $x \preceq z$ and $y \preceq z$ with x, $y \in P_M$. By Lemma 5.10, there exist x', y' such that $xy' = yx' \preceq z$ holds and xy' is an mcm of x and y. This implies $x' \in P_M$ and $y' \in P_M$ by definition. Hence P_M satisfies Condition (2.1), *i.e.*, it spans M.

Let S be an arbitrary spanning subset of M. As S generates M, it necessarily includes A_M. Then, S has to be closed under C. Indeed, assume that x, y lie in S, and xy'' is an mcm of x and y, say $xy'' = yx''$. As S spans M, there exist y' in S and z satisfying $y'' = y'z$. The hypothesis that xy'' is an mcm implies $\|xy'\| = \|xy''\|$, hence $\|z\| = 0$, and $y' \simeq y''$. As S is $\simeq$-saturated by definition, we deduce $y'' \in S$. So, S includes A_M and it is closed under C, hence it includes the closure P_M of A_M under C. □

Corollary 5.15. *Assume that M is a quasi-atomic cancellative monoid. Then M is thin (resp. quasi-thin) if and only the set P_M is finite (resp. quasi-finite).*

Once we know that primitive elements span M, we can apply Prop. 2.7 and we deduce that, if M is a quasi-atomic cancellative monoid, then the set P_M is closed under left multiplication by a unit, and every right divisor of a primitive element is primitive.

Another consequence of Prop. 5.14 is that, if M is a quasi-atomic cancellative monoid, and S is a $\simeq$-selector through P_M, then S is a minimal quasi-spanning subset of M, and $S \cap A_M$ is a $\simeq$-selector through A_M. Indeed, by construction, SM^* is equal to P_M, so S quasi-spans M. If S' is a proper subset of S, $S'M^*$ is a proper subset of P_M, so it cannot span M, and S' cannot quasi-span M. Finally, every atom x is primitive, so it belongs to SM^*, and, therefore, x is $\simeq$-equivalent to one element of S.

6. Simple elements

A crucial feature in Garside's and Thurston's analysis of the braid monoids and its subsequent extensions is the existence of a finite subset that is closed both under lcm and right divisor: in the current framework, this means that there exists a finite spanning subset S that is closed under lcm, *i.e.*, the lcm of two elements of S belongs to S. The least such set S happens to be the closure of primitive elements under lcm, and its elements, called minimal in [**5, 6**], or simple in [**9**], play a prominent rôle. In particular, there exists a maximal simple element Δ which enjoys most of the properties of Garside's fundamental braids Δ_n [**15**].

So, in the current approach, a natural idea would be to look for finite spanning subsets closed under mcm. Unfortunately, when least common multiples do not exist, more precisely when common multiples exist but some elements admit at least two non $\simeq$-equivalent mcm's, no such set may exist:

Proposition 6.1. *Assume that M is a quasi-atomic cancellative monoid, any two elements of M admit a common multiple, and S is a finite spanning subset of M that is closed under mcm. Assume in addition that $x \preceq y \in S$ implies $x \in S$. Then any two elements of M admit a lcm.*

Proof. As S is finite and closed under right mcm, there exists Δ in S such that $x \preceq \Delta$ holds for every x in S, *i.e.*, there exists x^* satisfying $xx^* = \Delta$; as M is left cancellative, x^* is unique, and, as S spans M, every right divisor of an element of S belongs to S, so x^* belongs to S. The mapping $x \mapsto x^*$ is injective, and, therefore, it is a permutation of S. Assume x, $y \in S$, and let xy' and xy'' be two right mcm's of x and y. By hypothesis, xy' belongs to S, so, by the previous remark, there exists z in S satisfying $xy' = z^*$, *i.e.*, $zxy' = \Delta$. By hypothesis, S is closed under left divisors, so zx and, similarly, zy belong to S, and so does their right mcm zxy''. So we must have $zxy'' \preceq \Delta$, hence $y'' \preceq y'$. In other words, xy' is a lcm of x and y. Finally, as S generates M, the existence of a lcm for each pair of elements of S inductively implies the existence of a lcm for each pair of elements of M. □

Thus, we must find a more subtle definition. The following one is convenient, in the sense that it will prove appropriate for the construction of a normal form.

Definition 6.2. Assume that M is a cancellative monoid, and S quasi-spans M. We say that an element x of M is S*-simple* if $y \prec x$ implies $\mathrm{Div}(y) \cap S \neq \mathrm{Div}(x) \cap S$. If M is quasi-atomic, we say *simple* for P_M-simple.

The elements of S always are S-simple. Indeed, for $x \in S$, we have $x \in \mathrm{Div}(x) \cap S$, but $y \prec x$ implies $x \not\preceq y$, *i.e.*, $x \notin \mathrm{Div}(y) \cap S$. So, in particular, a primitive element is always simple. By definition, an element is S-simple if and only if it is an mcm of its divisors lying in S. In particular, in the Gaussian case, an element is S-simple if and only if it is the lcm of its divisors lying in S, and, therefore, a S-simple element x is completely determined by the set $\mathrm{Div}(x) \cap S$. This need not be true in the general case.

Example 6.3. Let M be a free commutative monoid based on $\{a_1, \dots, a_n\}$. Then the atoms of M are $a_1, \dots, a_n$, there are $n+1$ primitive elements, namely 1 and the atoms, and there are 2^n simple elements, namely the elements $a_I = \prod_{i \in I} a_i$ for $I \subseteq \{1, \dots, n\}$. Indeed, $a_i \preceq a_I$ is equivalent to $i \in I$ in this case, and, for every x, the element a_I with $I = \{i\,; a_i \preceq x\}$ is a divisor of x with the same divisors in P_M, so no element not of the form a_I may be simple.

On the other hand, there are three primitive elements, namely 1, a, and b in the monoid M_1 of Example 2.11. These elements are simple, and there are two more simple elements, namely a^2 and ab. Here, we have $\mathrm{Div}(a^2) \cap P_M = \mathrm{Div}(ab) \cap P_M = P_M$, which gives an example where a simple element is not determined by the family of its primitive divisors.

Similarly, there are seven simple elements in M_3, namely the four primitive elements 1, a, b, c, and, in addition, the three elements ab, ba, and b^2: the sets of primitive divisors of the latter elements are $\{a, b\}$, $\{b, c\}$, and $\{a, b, c\}$ respectively, so, here, a simple element happens to be determined by its primitive divisors (although the monoid admits no lcm).

In the Gaussian case, *i.e.*, when least common multiples exist, the current definition of a simple element is equivalent to that of [**9**]. In particular, in the thin case, the simple elements of M have a natural characterization extending that given for a free commutative monoid in Example 6.3.

PROPOSITION 6.4. *Assume that M is a thin Gaussian monoid, i.e., a Garside monoid. Then the simple elements of M are finite in number, and they coincide with the divisors of the lcm Δ of P_M.*

PROOF. Let $\{x_i\,;\, i = 1, \ldots, n\}$ be an enumeration of P_M. For $I \subseteq \{1, \ldots, n\}$, let x_I be the lcm of the x_i's with $i \in I$. Then x_I is simple, and, conversely, every simple element must be of this form. Let Δ be the lcm of P_M. Then, by construction, every simple element x_I is a divisor of Δ. The computation rules for lcm's then imply that simple elements span M [**9**], and, as a consequence, that every divisor of Δ is simple. □

It is well known that, if M is a spherical Artin–Tits monoid, then the simple elements are in one-to-one correspondence with the elements of the associated finite Coxeter group [**4, 12**]: for instance, the $n!$ simple elements in the braid monoid B_n^+ are in one-to-one correspondence with the permutations of n objects. More generally, it is shown in [**9**] that the simple elements of a Garside monoid make a finite lattice with a unique maximal element, the lcm Δ of the primitive element. As shows the case of the monoid M_1, such a property need not be true in the general case.

For future use, we gather now some general results about S-simple elements.

LEMMA 6.5. *Assume that M is a cancellative monoid, and S quasi-spans M.*
(i) An element of M is S-simple if and only if it is SM^*-simple.
(ii) The set of all S-simple elements is closed under left and right multiplication by a unit, and, therefore, it is $\simeq$-saturated.

PROOF. (i) Assume that x is S-simple, and $y \prec x$ holds. By definition, we have $\mathrm{Div}(y) \cap S \neq \mathrm{Div}(x) \cap S$, so, a fortiori, $\mathrm{Div}(y) \cap SM^* \neq \mathrm{Div}(x) \cap SM^*$, and x is SM^*-simple. Conversely, assume that x is SM^*-simple, and $y \prec x$ holds. Then we have $z \preceq x$ and $z \not\preceq y$ for some z in SM^*. By definition, we have $z = z'u$ for some z' in S and u in M^*. Then $z' \preceq x$ and $z' \not\preceq y$ hold, and x is S-simple.

(ii) Assume that x is S-simple and u is a unit. Then we have $\mathrm{Div}(xu) = \mathrm{Div}(x)$, and $y \prec xu$ is equivalent to $y \prec x$. Hence $y \prec x$ implies $\mathrm{Div}(y) \cap S \neq \mathrm{Div}(xu) \cap S$, and xu is S-simple. The argument is similar for left multiplication by u, as $\mathrm{Div}(ux) = \mathrm{Div}(x)$ holds. □

In the general case, as shows the example of M_1, simple elements need not span the monoid. However, we still have the following closure property:

LEMMA 6.6. *Assume that M is a cancellative monoid, and S quasi-spans M. Then every right divisor of a S-simple element of M is S-simple.*

PROOF. Assume that xy is S-simple. We wish to show that y is S-simple. Assume $y' \prec y$. Then we have $xy' \prec xy$, so, by definition, there exists z in S satisfying $z \preceq xy$ and $z \not\preceq xy'$. As SM^* spans M, there exists z' in SM^* and x' in M satisfying $xz' = zx' \preceq xy$, hence $z' \preceq y$. Thus, z' belongs to $\mathrm{Div}(y) \cap SM^*$. On the other hand, $z' \preceq y'$ would imply $zx' = xz' \preceq xy'$, hence $z \preceq xy'$, contradicting the hypothesis. So $z' \preceq y'$ is impossible. We have $\mathrm{Div}(y') \cap SM^* \neq \mathrm{Div}(y) \cap SM^*$, so y is SM^*-simple, hence S-simple. □

Proposition 6.4 implies that, in the Gaussian case, there exist at most 2^n simple elements when there are n primitive elements, a bound which we have seen is nearly reached in the case of a free commutative monoid. The result extends to the general case as follows:

PROPOSITION 6.7. *Assume that M is a cancellative monoid, and S is a quasi-spanning subset of M with n elements. Then every S-simple element belongs to $S^n M^*$, and, therefore, there are at most n^n $\simeq$-equivalence classes of S-simple elements in M.*

PROOF. Assume that x is S-simple, and let $x_1, \ldots, x_p$ be an enumeration of $\mathrm{Div}(x) \cap S$. By Proposition 3.5(iii), there exists x' in S^p such that $x_i \preceq x'$ holds for $1 \leq i \leq p$. Then, we have $\mathrm{Div}(x') \cap S \supseteq \mathrm{Div}(x) \cap S$, hence $\mathrm{Div}(x') \cap S = \mathrm{Div}(x) \cap S$. By definition of a S-simple element, $x' \prec x$ is impossible, so $x' \simeq x$ is the only possibility, which shows that x belongs to $S^p M^*$, and, therefore, to $S^n M^*$ since 1 is primitive and $p \leq n$ holds. □

COROLLARY 6.8. *If M is a thin cancellative monoid, then the simple elements of M are finite in number. More precisely, if M contains n primitive elements, it contains at most n^n simple elements.*

If M is a quasi-atomic cancellative monoid and S is a $\simeq$-selector through simple elements, then $S \cap P_M$ is a $\simeq$-selector through P_M, and $S \cap A_M$ is a $\simeq$-selector through A_M. Conversely, every $\simeq$-selector through A_M can be extended into a selector through P_M, and, then, through simple elements.

Finally, let us observe that simple elements, as atoms and primitive elements, are defined intrinsically, and, therefore, they are preserved by automorphisms:

PROPOSITION 6.9. *Assume that M is a quasi-atomic cancellative monoid, and ϕ is an automorphism of M. Then ϕ globally preserves A_M, P_M, and the set of all simple elements in M.*

PROOF. As ϕ maps units to units, then it maps non-atoms to non-atoms, and, therefore, it maps atoms to atoms. Then, it maps every mcm of two elements to an mcm of their images, and, therefore, it maps every primitive element to a primitive element. Finally, ϕ preserves the relations $\preceq$ and $\prec$, so it maps simple elements to simple elements. □

7. Normal forms

The main interest of simple elements in the Gaussian case, *i.e.*, when least common multiples exist, is that they can be used to construct good normal forms. In particular, the greedy normal form originally defined for the braid monoids [**12, 1, 18, 13, 14**] extends to every Gaussian monoid, and, subsequently, to the corresponding group of fractions [**9**]. The principle is that, for $x \neq 1$ in the considered monoid M, there exists a maximal simple divisor x_1 of x, namely the gcd of x and the maximal simple element Δ, so we can write $x = x_1 x'$, and, applying the process to x', we inductively obtain a decomposition $x = x_1 x_2 \cdots$ in terms of simple elements. This decomposition enjoys good properties, and, in particular, it gives rise to a bi-automatic structure on the associated group of fractions.

A crucial technical point in the above construction is that simple elements happen to span the monoid, in the Gaussian case. We shall see now that a similar construction is still possible in the general case when we start with an arbitrary spanning set S and use the derived notion of a S-simple element. The price to pay for the generalization is that a given element possibly may have more than one normal decomposition, but, this fact excepted, the results remain similar, and the proofs are extremely easy.

As in the Gaussian case, we start from the fact that, for every element x, there exists a maximal S-simple divisor of x:

Lemma 7.1. *Assume that M is a quasi-atomic cancellative monoid, S quasi-spans M, and x_0 is a S-simple element. Then, for every x in M, there exists a S-simple divisor x_1 of x satisfying* $\mathrm{Div}(x) \cap S = \mathrm{Div}(x_1) \cap S$*; moreover, we may assume $x_0 \preceq x_1$ whenever $x_0 \preceq x$ holds.*

If M is Gaussian, then x_1 is a lcm of $\mathrm{Div}(x) \cap S$*, and, so, it is unique.*

Proof. Assume $x_0 \preceq x$. Let Y be the set of all S-simple elements y satisfying $x_0 \preceq y \preceq x$, and let x_1 be an element of Y such that $\|x_1\|$ has the maximal possible value: such an element exists since $y \in Y$ implies $\|y\| \leq \|x\|$. Write $x = x_1 x''$. Assume $z \in \mathrm{Div}(x) \cap S$. As S quasi-spans M, there must exist z' in S, and x'_1 in M satisfying $x_1 z' = x'_1 z' \preceq x$. So we have $x_0 \preceq x_1 \preceq x_1 z' \preceq x$. Moreover, provided z' has been chosen so that $\|x_1 z'\|$ has the least possible value, no proper divisor of $x_1 z'$ is a multiple of z, which implies that $x_1 z'$ is S-simple, and, therefore, it belongs to Y. The definition of x_1 then implies $\|x_1 z'\| = \|x_1\|$, hence $z' \in M^*$, and then $z \preceq x_1$. So we have $\mathrm{Div}(x_1) \cap S = \mathrm{Div}(x) \cap S$. Take $x_0 = 1$ for the general result.

In the Gaussian case, the lcm of $\mathrm{Div}(x) \cap S$ is a S-simple element satisfying the requirements, and it divides every other element satisfying them, so it must be the only solution. □

Definition 7.2. Assume that M is a cancellative monoid, and S quasi-spans M. We say that a sequence $(x_1, \ldots, x_n)$ in M is *S-prenormal* if, for each i, we have $\mathrm{Div}(x_i) \cap S = \mathrm{Div}(x_i \cdots x_n) \cap S$. We say that $(x_1, \ldots, x_n)$ is *S-normal* if it is S-prenormal, and, in addition, each factor x_i is S-simple. If M is quasi-atomic, we say (pre)normal for P_M-(pre)normal.

Say that a sequence $(x_1, \ldots, x_n)$ is a decomposition for x if $x = x_1 \cdots x_n$ holds. Iterating Lemma 7.1, we find:

Proposition 7.3. *Assume that M is a quasi-atomic cancellative monoid, S quasi-spans M, and x_0 is a S-simple element. Then every element x of M satisfying $x_0 \preceq x$ admits a S-normal decomposition $(x_1, \ldots, x_n)$ with $x_0 \preceq x_1$.*

Proof. Lemma 7.1 gives a S-simple element x_1 satisfying both $x_0 \preceq x_1$ and $\mathrm{Div}(x_1) \cap S = \mathrm{Div}(x) \cap S$. Write $x = x_1 x'$. If x' is a unit, then x is S-simple by Lemma 6.5(ii), and we are done. Otherwise, we have $\|x'\| < \|x\|$: inductively, we find a S-normal decomposition $(x_2, \dots, x_n)$ of x', and concatenating x_1 with the latter gives a S-normal decomposition of x. □

By Lemma 7.1, the normal form of Prop. 7.3 is unique in the Gaussian case, and it coincides with the greedy normal form of [**14, 9**]. More generally, the S-normal form is unique whenever distinct S-normal elements never admit the same divisors in S. Now, the latter condition need not be true, and the normal form need not be unique in general.

EXAMPLE 7.4. Consider once again the monoid M_1 of Example 2.11. Then a^2 and ab are simple elements, and (a^2, a^2) and (ab, ab) are two normal decompositions for a^4 in M. On the other hand, we observed that, in the case of M_3, the simple elements are uniquely determined by their primitive divisors. So, in this case, the normal decomposition is unique.

When nontrivial units exist, we can replace the family of all S-simple elements by a $\simeq$-selector, at the expense of keeping a unit at the end of the decomposition.

PROPOSITION 7.5. *Assume that M is a quasi-atomic cancellative monoid, S quasi-spans M, and Σ is a $\simeq$-selector through S-simple elements in M. Then every element x of M admits a decomposition $(x_1, \dots, x_n, u)$ with $x_1, \dots, x_n \in \Sigma$, $u \in M^*$ and $(x_1, \dots, x_n)$ a S-normal sequence.*

PROOF. We can refine Lemma 7.1 so as to require that the element x_1 be chosen in the $\simeq$-selector Σ. Then the inductive argument is the same as for Prop. 7.3. For the last S-simple factor, say x'_n, we can find x_n in Σ and u in M^* satisfying $x'_n = x_n u$, and we finally obtain $x = x_1 \dots x_n u$. □

The interest of the current construction lies in that S-normal sequences admit a purely *local* characterization. To state the results easily, we introduce one more notation.

DEFINITION 7.6. Assume that M is a monoid and S is a subset of M. For x, $y \in M$, we say that x *covers* y w.r.t. S, denoted $x \triangleright_S y$, if $\mathrm{Div}(xy) \cap S = \mathrm{Div}(x) \cap S$ holds, *i.e.*, if every element of S dividing xy already divides x. If M is quasi-atomic, we write $\triangleright$ for $\triangleright_{P_M}$.

Thus, by definition, a sequence $(x_1, \dots, x_n)$ is S-prenormal if and only if $x_i \triangleright_S x_{i+1} \cdots x_n$ is true for every i. We begin with an obvious observation.

LEMMA 7.7. *Assume that M is a cancellative monoid and S is a subset of M. Then the relations $\triangleright_S$ and $\triangleright_{SM^*}$ coincide.*

PROOF. It is obvious that $x \triangleright_{SM^*} y$ implies $x \triangleright_S y$. Conversely, assume $x \triangleright_S y$ and $z' \simeq z \in S$. Then $z' \preceq xy$ (resp. $z' \preceq x$) is equivalent to $z \preceq xy$ (resp. $z \preceq x$). So $z' \preceq xy$ implies $z \preceq xy$, hence $z \preceq x$, hence $z' \preceq x$, and we have $x \triangleright_{SM^*} y$. □

It turns out that all subsequent properties of the normal form rely on the following basic observations:

LEMMA 7.8. *Assume that M is a cancellative monoid, and S quasi-spans M. Then, for x, y, z in M:*
(i) The relation $y \triangleright_S z$ implies $xy \triangleright_S z$;
(ii) The conjunction of $x \triangleright_S y$ and $y \triangleright_S z$ implies $x \triangleright_S yz$.

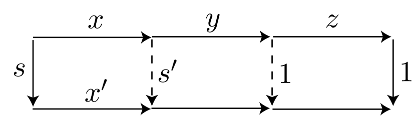

Figure 7.1. Covering relation

Proof. (i) (Fig. 7.1) Assume $s \in S$ and $s \preceq xyz$. As SM^* spans M, there exist s' in SM^*, and x' in M satisfying $sx' = xs' \preceq xyz$, hence $s' \preceq yz$. By Lemma 7.7, $y \rhd_S z$ implies $y \rhd_{SM^*} z$, so $s' \preceq yz$ implies $s' \preceq y$, and, therefore, we have $s \preceq xs' \preceq xy$.

(ii) Assume $s \in S$ and $s \preceq xyz$. By (i), $y \rhd_S z$ implies $xy \rhd_S z$, so we deduce $s \preceq xy$. Then the hypothesis $x \rhd_S y$ implies $s \preceq x$. □

We can now establish the expected local characterization of normal sequences, a necessary first step toward a possible automatic structure:

Proposition 7.9. *Assume that M is a cancellative monoid, and S quasi-spans M. Then a sequence $(x_1, \ldots, x_n)$ in M^n is S-prenormal if and only if $x_i \rhd_S x_{i+1}$ holds for each i.*

Proof. By definition, the sequence $(x_1, \ldots, x_n)$ is S-prenormal if and only if $x_i \rhd_S x_{i+1} \cdots x_n$ holds for each i. By definition, the latter relation always implies $x_i \rhd_S x_{i+1}$. By Lemma 7.8(ii), the converse implication is also true: a descending induction on j shows that $(\forall i \geq j)(x_i \rhd_S x_{i+1})$ implies $x_i \rhd_S x_{i+1} \cdots x_p$. Indeed, the conjunction of $x_j \rhd_S x_{j+1}$ and $x_{j+1} \rhd_S x_{j+2} \cdots x_n$ implies $x_j \rhd_S x_{j+1} \cdots x_n$. □

Remark 7.10. Instead of using S-simple elements, we could think of simply considering elements of S, and constructing a normal form of x starting with a maximal divisor of x in S. But, then, the normal sequences would not necessarily admit the local characterization of Prop. 7.9. For instance, in the monoid M_1, if we take $S = \mathrm{Div}(a^2)$ (a spanning subset that we shall consider in Sec. 8 below), the two sequences (a, b) and (b, a) would be S-normal, as a is a maximal divisor of ab in S, and b is a maximal divisor of ab in S, but the concatenated sequence (a, b, a) would not, as we have $a^2 \preceq aba$, and therefore a is not a maximal divisor of aba in S.

We have seen that the normal form of Prop. 7.3 need not be unique in general. We shall need in Sec. 9 below the following refinement of Prop. 7.3 that connects the various normal decompositions of an element:

Proposition 7.11. *Assume that M is a quasi-atomic cancellative monoid, S quasi-spans M, and $x_1, \ldots, x_n$ are S-simple elements of M. Then $x_1 \cdots x_n$ admits a S-normal decomposition $(x'_1, \ldots, x'_m)$ such that $m \leq n$ holds and, for each i, we have $x_1 \cdots x_{f(i)} \preceq x'_1 \cdots x'_i$ for some increasing mapping f of $\{1, \ldots, m\}$ into $\{1, \ldots, n\}$ with $f(m) = n$.*

Proof. The result is trivial for $n = 1$. Assume $n = 2$. Applying Prop. 7.3 to x_1x_2, we find a S-normal decomposition of x_1x_2 that begins with some multiple x'_1 of x_1. Two cases may happen. Either x_1x_2 is S-simple, and (x'_1) is the expected decomposition. Or we have $x'_1 = x_1y$ with $y \prec x_2$, and, therefore, $x_1x_2 = x'_1x'_2$ with $x_2 = yx'_2$. By Lemma 6.6, the latter relation forces x'_2 to be S-simple, and, therefore, (x'_1, x'_2) is a S-normal decomposition of the expected form.

For $n \geq 3$, we use induction on n. Applying the induction hypothesis, we find a S-normal decomposition $(y_2, \dots, y_p)$ for $x_2 \cdots x_n$ and an increasing mapping g of $\{2, \dots, p\}$ into $\{2, \dots, n\}$ satisfying $x_2 \cdots x_{g(i)} \preceq y_2 \cdots y_i$ for $2 \leq i \leq p$. If $p < n$ holds, we can apply the induction hypothesis to x_1, y_2, ... , y_p, and get the result directly. So, assume $p = n$. Then g must be the identity mapping. Applying the result with $n = 2$ to $x_1 y_2$, we obtain a S-normal decomposition of length 2 or 1. In the latter case, we resort to the induction hypothesis directly. So, assume that we have obtained (x'_1, y'_2) with $x_1 \preceq x'_1$ and $x'_1 y'_2 = x_1 y_2$. We apply the induction hypothesis another time to $y'_2 y_3 \cdots y_n$, obtaining a S-normal decomposition $(x'_2, \dots, x'_m)$. Then $(x'_1, x'_2, \dots, x'_m)$ satisfies our requirements. Indeed, by construction, we have $y_2 \rhd_S y_3 \cdots y_n$, hence, by Lemma 7.8, $x'_1 y'_2 = x_1 y_2 \rhd_S y_3 \cdots y_n$, and, as $x'_1 \rhd_S y'_2$ holds by construction, $x'_1 \rhd_S y'_2 y_3 \cdots y_n$, hence $x'_1 \rhd_S x'_2$. So the sequence $(x'_1, \dots, x'_m)$ is S-normal. The relations $x_1 \cdots x_{f(i)} \preceq x'_1 \cdots x'_i$ follow from the induction hypothesis. □

Although natural, the previous result was not obvious: putting in normal form a product of two simple elements might have required say three simple elements, since the conditions for being normal discard some decompositions.

We consider now the effect of multiplication on normal forms, *i.e.*, we try to connect the normal form(s) of an element x with those of yx and xy, especially when y is S-simple. As one can expect, such results will be crucial for constructing an automatic structure.

LEMMA 7.12. *Assume that M is a quasi-atomic cancellative monoid, and S quasi-spans M. Let x, y be arbitrary elements of M, and $(x_1, \dots, x_n)$ be a S-prenormal decomposition of x. Put $y_0 = y$, and, inductively, let (x'_i, y_i) be any S-prenormal decomposition of $y_{i-1} x_i$. Then $(x'_1, \dots, x'_n, y_n)$ is a S-prenormal decomposition of yx.*

If, in addition, y is S-simple and $(x_1, \dots, x_n)$ is S-normal, then we may assume that each element y_i is S-simple, and then $(x'_1, \dots, x'_n, y_n)$ is a S-normal decomposition of yx.

PROOF. (Fig. 7.2) We have $x'_n \rhd_S y_n$ by construction, so the point is to show $x'_i \rhd_S x'_{i+1}$ for each i. Assume $z \in S$ and $z \preceq x'_i x'_{i+1}$. This implies $z \preceq x'_i x'_{i+1} y_{i+1}$, *i.e.*, $z \preceq y_{i-1} x_i x_{i+1}$. By hypothesis, we have $x_i \rhd_S x_{i+1}$, hence, by Lemma 7.8(i), $y_{i-1} x_i \rhd_S x_{i+1}$. So $z \preceq y_{i-1} x_i x_{i+1}$ implies $z \preceq y_{i-1} x_i$, *i.e.*, $z \preceq x'_i y_i$. Now, by hypothesis, we have $x'_i \rhd_S y_i$, so we deduce $z \preceq x'_i$, hence $x'_i \rhd_S x'_{i+1}$, and the sequence $(x'_1, \dots, x'_n, y_n)$ is S-prenormal.

If y and each x_i are S-simple, we can inductively assume that y_{i-1} and x'_i are S-simple: indeed, in this case, Prop. 7.11 guarantees that $y_{i-1} x_i$ admits a S-normal form of length 2 at most, and, if we define (x'_i, y_i) to be such a S-normal sequence (with possibly $y_i = 1$), then induction continues. □

Let us finally consider multiplication on the right. A similar argument is possible, but it works in the Gaussian case only.

LEMMA 7.13. *Assume that M is a Gaussian monoid, S quasi-spans M. Let x, y be arbitrary elements of M, and $(x_1, \dots, x_n)$ be a S-prenormal decomposition of xy. Put $y_n = y$, and, inductively, define x'_i and y_{i-1} so that $y_{i-1} x_i = x'_i y_i$*

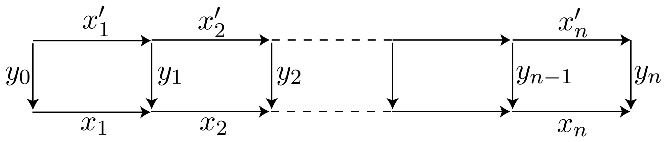

FIGURE 7.2. Comparing normal forms of x and yx

holds and the latter is a left lcm of x_i and y_i. Then $(x'_1, \dots, x'_n)$ is a S-prenormal decomposition of x.

PROOF. (Fig. 7.2 again) Let us show that $x_i \triangleright_S x_{i+1}$ implies $x'_i \triangleright_S x'_{i+1}$. Assume $z \in S$ and $z \preceq x'_i x'_{i+1}$. As in the proof of Lemma 7.12, we deduce $z \preceq y_{i-1} x_i x_{i+1}$, hence, as $x_i \triangleright_S x_{i+1}$ implies $y_{i-1} x_i \triangleright_S x_{i+1}$, $z \preceq y_{i-1} x_i$, *i.e.*, $z \preceq x'_i y_i$. By construction, y_i and x'_{i+1} have no common divisor; *in the Gaussian case*, this implies that every common divisor of $x'_i y_i$ and $x'_i x'_{i+1}$ is a divisor of x'_i. So, we have $z \preceq x'_i$, and $x'_i \triangleright_S x'_{i+1}$.

Finally, we observe that $y_0 = 1$ necessarily holds, as, by the results of [**9**], $y_0 x_1 \cdots x_n$ has to be a left lcm of $x_1 \cdots x_n$ and y, hence to equal $x_1 \cdots x_n$. □

EXAMPLE 7.14. When lcm's need not exist, the previous argument fails, and so does the result itself. For instance, let us consider M_1 again. Choose $x = a^3$, $y = b$. Then (a^2, a) is a normal decomposition of x. One possibility according to Lemma 7.13 is to define $y_0 = 1$, $y_1 = b$, $x'_1 = b$, $x'_2 = a$. Indeed, $ab = ba$ is a left mcm of a and b, and $1a^2 = bb$ is a left mcm of a^2 and b. Now, (b, a) is not a (pre)normal sequence, as we have $a \in S$, $a \preceq ba$, and $a \not\preceq b$, hence $b \not\triangleright_S a$.

8. Garside elements

As was recalled above, if M is a thin Gaussian monoid, *i.e.*, a Garside monoid, then the lcm Δ of all primitive elements plays an important rôle. Technically, the point is that the left divisors of Δ coincide with its right divisors, which implies in particular that conjugation by Δ gives an automorphism of M, and that some power of Δ belongs to the center of M. Conversely, it is proved in [**9**] that, if M is a Gaussian monoid and Δ is an element of M such that the left divisors of Δ coincide with its right divisors and they generate M, then these divisors of Δ span M, and, therefore, M is thin, and, therefore, it is a Garside monoid.

In the general case, there seems to be no reason why the existence of a finite spanning set should imply the existence of an element Δ with similar properties. Even worse, Prop. 6.1 shows that the existence of such an element is impossible in the non-Gaussian case if we require both closure under mcm and left divisors.

However, we shall see now how to define an appropriate notion of a Garside element which may exist in the non-Gaussian case, and extends the usual notion in the Gaussian case. We shall then prove in the general case a large part of the results established in the Gaussian case.

DEFINITION 8.1. Assume that M is a cancellative monoid. We say that an element Δ of M is a *Garside* element if $\mathrm{Div}(\Delta)$ is a finite spanning subset of M.

Notice that, if Δ is a Garside element in M, then M must be thin by definition, hence quasi-atomic by Prop. 5.7, and every primitive element of M must divide Δ, since, by Prop. 5.14, the family P_M is the least spanning subset of M, and, therefore, it must be included in $\mathrm{Div}(\Delta)$. Let us mention that most of the subsequent results could be extended to a *quasi-Garside* element, the latter being defined as an element Δ such that $\mathrm{Div}(\Delta)$ spans M and is quasi-finite.

LEMMA 8.2. *Assume that M is a thin cancellative monoid, and Δ is a Garside element in M. Then, for every element x in $\mathrm{Div}(\Delta)$, there exists a unique element x^* in $\mathrm{Div}(\Delta)$ satisfying $xx^* = \Delta$; the mapping $x \mapsto x^*$ is a permutation of $\mathrm{Div}(\Delta)$; for x, $y \in \mathrm{Div}(\Delta)$, x being a left divisor of y is equivalent to y^* being a right divisor of x^*.*

PROOF. (The argument was already used for Prop. 6.1.) By definition $x \preceq \Delta$ means that $xx^* = \Delta$ holds for some right divisor x^* of Δ, which is unique as M is assumed to be (left) cancellative. By hypothesis, the family $\mathrm{Div}(\Delta)$ spans M which contains Δ, so, by Prop. 2.7, it also contains every right divisor of Δ, so, in particular, x^* belongs to $\mathrm{Div}(\Delta)$. Then $x^* = y^*$ implies $xx^* = \Delta = yy^* = yx^*$, hence $x = y$, as M is cancellative. This proves that $x \mapsto x^*$ is an injection of $\mathrm{Div}(\Delta)$ into itself, hence a bijection as $\mathrm{Div}(\Delta)$ is assumed to be finite. Finally $y = xz$ implies $xx^* = \Delta = yy^* = xzy^*$, hence $x^* = zy^*$. □

We deduce that, in the Gaussian case, our current notion of a Garside element coincides with that considered in [**9**]:

LEMMA 8.3. *Assume that M is a thin cancellative monoid.*
(i) If Δ is a Garside element in M, then the left and the right divisors of Δ coincide and they generate M.
(ii) Conversely, if M is Gaussian and Δ is an element of M such that the left and the right divisors of Δ coincide and they generate M, then Δ is a Garside element in M.

PROOF. (i) Assume that Δ is Garside. By Prop. 2.7, every right divisor of Δ belongs to $\mathrm{Div}(\Delta)$, hence is a left divisor of Δ, while, by Lemma 8.2, every element of $\mathrm{Div}(\Delta)$ belongs to the range of the mapping $x \mapsto x^*$, hence it is a right divisor of Δ: so the left and the right divisors of Δ coincide.

(ii) Assume now that M is Gaussian and the left and the right divisors of Δ coincide and they generate M. Assume $x, y \preceq \Delta$ and $xy'' = yx''$. Let $xy' = yx'$ be the lcm of x and y. By definition, we have $x' \preceq x''$ and $y' \preceq y''$. Moreover, $x, y \preceq \Delta$ implies $xy' \preceq \Delta$. So xy' and yx' are left divisors of Δ, hence they are right divisors of Δ as well, and so are y' and x'. Finally, x' and y' belong to $\mathrm{Div}(\Delta)$, and the latter spans M. So Δ is a Garside element. □

In the thin Gaussian case, *i.e.*, in a Garside monoid, there always exists a unique minimal Garside element, namely the lcm of all primitive elements. In the general case, we have no such result, but the following examples show that Garside elements may still exist.

EXAMPLE 8.4. Consider again the monoid M_1 of Example 2.11. Let $\Delta_1 = a^2$ and $\Delta_2 = ab$. Then Δ_1 and Δ_2 both are minimal Garside elements. For instance, we have $\mathrm{Div}(\Delta_1) = \{1, a, b, a^2\}$, a spanning subset of M_1, and the left and the right divisors of Δ_1 coincide. Observe that, in this case, the divisors of Δ_1 properly include the primitive elements.

The reader can check similarly that the monoid M_2 contains three minimal Garside elements, namely a^2, ab, and ac, while M_3 contains one minimal Garside element only, namely b^2.

Proposition 8.5. *Assume that M is a thin cancellative monoid, and Δ is a Garside element in M. The mapping $x \mapsto x^{**}$ extends into an automorphism ϕ_Δ of M and we have*

$$x\Delta = \Delta\phi_\Delta(x) \tag{8.1}$$

for every x in M. The automorphism ϕ_Δ globally preserves $\mathrm{Div}(\Delta)$*, the units, the atoms, the primitive elements, and the simple elements of M. The order of ϕ_Δ is a finite integer e, and the element Δ^e belongs to the center of M, which therefore is not trivial.*

Proof. By Lemma 8.2, the mapping $x \mapsto x^{**}$ is a permutation of $\mathrm{Div}(\Delta)$, and it has a finite order say e. By definition, we have $x\Delta = x(x^*x^{**}) = (xx^*)x^{**} = \Delta x^{**}$ for every x in $\mathrm{Div}(\Delta)$. Assume $x_1 \cdots x_p = y_1 \cdots y_q$ with $x_1, \ldots, y_q \in \mathrm{Div}(\Delta)$. Using the previous remark, we obtain

$$\Delta x_1^{**} \cdots x_p^{**} = x_1 \cdots x_p\Delta = y_1 \cdots y_q\Delta = \Delta y_1^{**} \cdots y_q^{**},$$

hence $x_1^{**} \cdots x_p^{**} = y_1^{**} \cdots y_q^{**}$ by cancelling Δ. Thus putting $\phi_\Delta(x_1 \cdots x_p) = x_1^{**} \cdots x_p^{**}$ yields a well defined mapping. As $\mathrm{Div}(\Delta)$ generates M, the mapping ϕ_Δ is defined everywhere on M, and, by construction, it is an endomorphism and (8.1) is satisfied. Then, ϕ_Δ^e is also an endomorphism, and it is the identity on $\mathrm{Div}(\Delta)$, so it is the identity everywhere. Hence ϕ_Δ must be an automorphism. Moreover, (8.1) inductively implies $x\Delta^k = \Delta^k\phi_\Delta^k(x)$ for every positive k and every x, so, in particular, $x\Delta^e = \Delta^e x$ for every x, *i.e.*, Δ^e commutes with every element of M. Finally, we apply Prop. 6.9. □

Example 8.6. Different Garside elements may give rise to different automorphisms. For instance, in M_2, the automorphism ϕ_{a^2} is the identity, while ϕ_{ab} and ϕ_{ac} have order 3, and they correspond to the cyclic permutations (a, c, b) and (a, b, c) of the atoms respectively.

Proposition 8.7. *Assume that M is a thin cancellative monoid, and Δ is a Garside element in M. Then any two elements of M admit a common multiple; more precisely, for $x \in \mathrm{Div}(\Delta)^p$ and $y \in \mathrm{Div}(\Delta)^q$, we have $xy' = yx'$ for some x' in $\mathrm{Div}(\Delta)^p$ and y' in $\mathrm{Div}(\Delta)^q$.*

Proof. The proof of Prop. 4.2 shows that, if S spans M and any two elements of S admit a common multiple, then two elements x of S^p and y of S^q admit a common multiple $xy' = yx'$ with $x' \in S^p$ and $y' \in S^q$. Here we apply the result to the spanning subset $\mathrm{Div}(\Delta)$. The only point to check is the result in the case $p = q = 1$. Now, for $x \preceq \Delta$ and $y \preceq \Delta$, we can take $x' = y^*$ and $y' = x^*$. □

For a while let us write $\mathrm{Div}_r(x)$ for the set of all right divisors of x.

Lemma 8.8. *Assume that M is a thin cancellative monoid, and Δ is a Garside element in M. Then, for every positive integer k, we have $\mathrm{Div}(\Delta^k) = \mathrm{Div}_r(\Delta^k) = \mathrm{Div}(\Delta)^k$, and, therefore, Δ^k is a Garside element.*

Proof. We prove the three relations $\mathrm{Div}_r(\Delta^k) \subseteq \mathrm{Div}(\Delta)^k \subseteq \mathrm{Div}(\Delta^k) \subseteq \mathrm{Div}_r(\Delta^k)$. First, by Prop. 2.6, the set $\mathrm{Div}(\Delta)^k$ spans M, and it contains Δ^k, so, by Prop. 2.7, it also contains every right divisor of Δ^k.

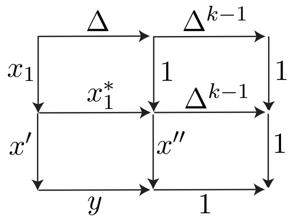

FIGURE 8.1. Divisors of Δ^k

The second inclusion is proved using induction on k. The result is trivial for $k = 1$. Assume $k \geq 2$, and let $x \in \mathrm{Div}(\Delta)^k$, say $x = x_1x'$ with $x_1 \preceq \Delta$ and $x' \in \mathrm{Div}(\Delta)^{k-1}$ (Fig. 8.1). By construction, x_1^* belongs to $\mathrm{Div}(\Delta)$, so, by Proposition 8.7, we have $x'y = x_1^*x''$ for some $y \in \mathrm{Div}(\Delta)$ and $x'' \in \mathrm{Div}(\Delta)^{k-1}$. By induction hypothesis, we have $x'' \preceq \Delta^{k-1}$, and, therefore,

$$x \preceq xy = x_1x'y = x_1x_1^*x'' = \Delta x'' \preceq \Delta\Delta^{k-1} = \Delta^k.$$

For the third inclusion, assume $x \preceq \Delta^k$, say $xy = \Delta^k$. We find

$$\phi_\Delta^{-k}(y)xy = \phi_\Delta^{-k}(y)\Delta^k = \Delta^k\phi_\Delta^k(\phi_\Delta^{-k}(y)) = \Delta^k y,$$

hence $\phi_\Delta^{-k}(y)x = \Delta^k$, which shows that x is a right divisor of Δ^k. □

PROPOSITION 8.9. *Assume that M is a thin cancellative monoid, and Δ is a Garside element in M. Then any two elements of M admit a common left multiple.*

PROOF. Assume x, $y \in M$. Then both x and y belong to $\mathrm{Div}(\Delta)^k$ for k large enough. By Lemma 8.8, this implies that Δ^k is both a common right multiple, and a common left multiple of x and y. □

If a thin cancellative monoid M contains a Garside element, then, by Proposition 8.7, it is a Ore monoid, and, therefore, it embeds in a thin group of (right) fractions G. Using the Garside element, we can also express every element of G as a left fraction whose denominator is a power of Δ.

PROPOSITION 8.10. *Assume that M is a thin cancellative monoid, and Δ is a Garside element in M. Then M embeds in a group of fractions G; every element of G admits a unique decomposition $\Delta^{-k}x$ with $k \in \mathbb{Z}$ and $x \in M$ satisfying $\Delta \not\preceq x$.*

PROOF. Let $z = xy^{-1}$ be an element of G. As y belongs to $\mathrm{Div}(\Delta)^\ell$ for some positive ℓ, we have $y \preceq \Delta^\ell$ by Lemma 8.8, say $yx' = \Delta^\ell$. Then we find

$$z = xx'x'^{-1}y^{-1} = xx'\Delta^{-\ell} = \Delta^{-\ell}\phi_\Delta^{-\ell}(xx'),$$

i.e., $z = \Delta^{-\ell}z_0$ for some z_0 in M. Assume $p \leq \ell$ and $y = \Delta^p z \in M$. Then, in M, we have $z_0 = \Delta^{\ell-p}y$, hence $\ell - p \leq \|z_0\|$. Thus the set $\{p \in \mathbb{Z}\,;\, \Delta^p z \in M\}$ must have a least element, say k. Then, by construction, z can be expressed as $\Delta^{-k}x$ for some x in M. As any relation $x = \Delta x'$ in M would imply $z = \Delta^{-k+1}x'$ and contradict the definition of k, we have $\Delta \not\preceq x$. Finally, $\Delta^{-k}x = \Delta^{-k'}x'$ with $k' > k$ implies $\Delta^{-k+k'}x = x'$ in M, hence $\Delta \preceq x'$, showing the uniqueness of the decomposition $\Delta^{-k}x$ when $\Delta \not\preceq x$ is required. □

If Δ is a Garside element in a monoid M, then, by hypothesis, the set $\mathrm{Div}(\Delta)$ spans M, and, therefore, there exist the associated notions of a $\mathrm{Div}(\Delta)$-simple element and a $\mathrm{Div}(\Delta)$-normal sequence. For simplicity, we call them Δ-simple and Δ-normal respectively, and we write $\triangleright_\Delta$ for $\triangleright_{\mathrm{Div}(\Delta)}$. Using Prop. 8.10 and the results of Sec. 7, we obtain:

Proposition 8.11. *Assume that M is a thin cancellative monoid, Δ is a Garside element in M, and G is the group of fractions of M. Then every element of G admits a decomposition $\Delta^{-k}x_1 \cdots x_p$ where k is a uniquely determined integer and $(x_1, \dots, x_p)$ is a Δ-normal sequence with $x_1 \not\simeq \Delta$.*

Proof. The only point to establish is that, if $(x_1, \dots, x_p)$ is a Δ-normal sequence, then $\Delta \not\preceq x_1 \cdots x_p$ is equivalent to $x_1 \not\simeq \Delta$. The condition is obviously necessary. Conversely, as Δ belongs to $\mathrm{Div}(\Delta)$, the relation $\Delta \preceq x_1 \cdots x_p$ implies $\Delta \preceq x_1$ by definition of a Δ-normal sequence. Now, as Δ is divisible by every element of $\mathrm{Div}(\Delta)$, no proper multiple of Δ may be Δ-simple, and $\Delta \preceq x_1$ implies $\Delta \simeq x_1$ when x_1 is Δ-simple. □

Example 8.12. Even if we use a minimal Garside element, the Δ-normal form need not coincide with the (P_M)-normal form in general. For instance, consider once more the monoid M_1 of Example 2.11. We have seen that $\Delta_1 = a^2$ is a minimal Garside element in M_1. Then the Δ_1-simple elements coincide with the simple elements: there are five of them, namely 1, a, b, a^2, and ab. Now, the relations $\triangleright$ and $\triangleright_{\Delta_1}$ do not coincide, because we have $\mathrm{Div}(\Delta_1) = P_{M_1} \cup \{\Delta_1\}$. It follows that the Δ_1-simple elements are determined by their divisors in $\mathrm{Div}(\Delta_1)$, while they are not determined by their primitive divisors: both a^2 and ab are divisible by 1, a, b, but only a^2 is divisible by a^2. As a consequence, the Δ_1-normal form is unique, while we have seen the normal form is not.

9. Automatic structure

In the Gaussian case, *i.e.*, when lcm exist, thinness implies the existence of a Garside element, and the latter implies the existence of an automatic structure for the associated group of fractions. We shall show now that the latter result extends to more general cases: indeed, we shall prove that, under suitable hypotheses, the normal form of Prop. 8.11 is associated with an automatic structure.

The first steps, namely proving that the normal decompositions make a regular language, are easy.

Proposition 9.1. *Assume that M is a thin cancellative monoid, Δ is a Garside element in M, and G is the group of fractions of M. Let Σ_Δ denote the set of all Δ-simple elements in M. Then the language consisting of all normal sequences in the sense of Prop. 8.11 is regular.*

Proof. By Prop. 6.7, there are finitely many Δ-simple elements, *i.e.*, the set Σ_Δ is finite. Put $A = \Sigma_\Delta \cup \{\Delta^{-1}\}$. A word over A, *i.e.*, a finite sequence $(x_1, \dots, x_n)$ of letters, is a normal form if and only if the following requirements are obeyed:

- a letter Δ^{-1} or Δ cannot follow any other letter;
- a letter x in $\Sigma_\Delta - \{\Delta\}$ may follow only Δ^{-1} or one of those (finitely many) letters y in Σ_Δ that satisfy $y \triangleright_\Delta x$.

Define a state set Q to be $A \cup \{1, \bot\}$, where 1 is an initial state and $\bot$ is a failure state, and a transition function $F : Q \times A \to Q$ by

Q ↓ A →	$x \neq \Delta, \Delta^{-1}$	Δ	Δ^{-1}
$y \neq \Delta, \Delta^{-1}$	$\perp$ for $y \not\rhd_\Delta x$ x for $y \rhd_\Delta x$	$\perp$	$\perp$
Δ	x	Δ	$\perp$
Δ^{-1}	x	$\perp$	Δ^{-1}
1	x	Δ	Δ^{-1}
$\perp$	$\perp$	$\perp$	$\perp$

Then the finite state automaton $(Q, A, F, 1, Q - \{\perp\})$ recognizes the language of Δ-normal forms (see for instance [**14**] for definitions). □

Provided all Δ-normal forms have the same length, we can readily apply the method of [**3**] or [**19**], and deduce:

Corollary 9.2. *Assume that G is the group of fractions of a cancellative monoid M that admits a Garside element Δ such that all Δ-normal forms of an element have the same length. Then G has rational growth, i.e., the number of elements of G with a Δ-normal form of length n is a rational function of n.*

If G is a group generated by a family A, we denote by $\Gamma_A(G)$ the Cayley graph of G with respect to A, *i.e.*, the labelled graph whose vertices are the elements of G and there exists a z-labelled edge from x to y if $y = xz$ holds in G. For x, $y \in G$, the distance $\mathrm{dist}_{A,G}(x, y)$ between x and y in $\Gamma_A(G)$ is the minimal length of an unoriented path from x to y.

Definition 9.3. Assume that G is a group generated by A. The *synchronous distance* between two words on A, *i.e.*, two sequences of letters in A, say $(x_1, \ldots, x_p)$ and $(y_1, \ldots, y_q)$, is defined to be the supremum of the numbers

$$\mathrm{dist}_{A,G}(x_1 \cdots x_{\inf(i,p)}, y_1 \cdots y_{\inf(i,q)})$$

for $1 \leq i \leq \sup(p, q)$.

By the results of [**14**], the Δ-normal form of Prop. 8.11 is associated with a (left) automatic structure if and only if the fellow traveller property (FTP) is satisfied, *i.e.*, for every x in the group and every y in $\Sigma_\Delta \cup \{\Delta^{-1}\}$,

- the synchronous distance between any two Δ-normal decompositions of x is uniformly bounded, and
- the synchronous distance between a Δ-normal decomposition of x and one of yx is uniformly bounded.

We shall see that such conditions are satisfied in good cases. To this end, we shall first establish a bound for the distance between the various normal forms of an element in the monoid. (The notion of the synchronous distance is extended to the case of the monoid in the obvious way.)

Lemma 9.4. *Assume that M is a quasi-atomic cancellative monoid, S is a quasi-spanning subset of M of cardinality k and, for every x in M, the following condition holds:*

(9.1) *All S-normal decompositions of x have the same length.*

Then the synchronous distance between any two S-normal decompositions of an element of M is uniformly bounded by $2(k-1)$.

We begin with two auxiliary results.

Lemma 9.5. *Assume that M is a (left) cancellative monoid, and S quasi-spans M. Then $x_1 \triangleright_S \cdots \triangleright_S x_k \triangleright_S x$ implies $x_1 \cdots x_k \triangleright_{S^k} x$.*

Proof. We use induction on $k \geq 0$. Assume $z \in S^k$ and $z \preceq x_1 \cdots x_k x$. For $k = 0$, *i.e.*, for $z = 1$, the result is vacuously true. Otherwise, write $z = z_1 z'$, with $z_1 \in S$ and $z' \in S^{k-1}$. By Lemma 7.8(ii), $x_1 \triangleright_S \cdots \triangleright_S x_k \triangleright_S x$ implies $x_1 \triangleright_S x_2 \cdots x_k x$. By hypothesis, we have $z_1 \preceq x_1 \cdots x_k x$, hence $z_1 \preceq x_1$, say $x_1 = z_1 x'_1$. Then, by Lemma 7.8(i), we have $x'_1 x_2 \triangleright_S x_3 \triangleright_S \cdots \triangleright_S x_k \triangleright_S x$, and, as M is (left) cancellative, $z' \preceq (x'_1 x_2) x_3 \cdots x_k x$. By induction hypothesis, this implies $z' \preceq (x'_1 x_2) x_3 \cdots x_k$, hence $z = z_1 z' \preceq z_1 (x'_1 x_2) x_3 \cdots x_k$, *i.e.*, $z \preceq x_1 \cdots x_k$. □

Lemma 9.6. *Under the hypotheses of Lemma 9.4, if $(x_1, \dots, x_n)$ is a S-normal decomposition for x, and x'_1 is a maximal S-simple divisor of x, then there exist $x'_2, \dots, x'_k$ such that $(x'_1, \dots, x'_k, x_{k+1}, \dots, x_n)$ is another S-normal decomposition of x.*

Proof. As x'_1 is S-simple, it belongs to S^k by Prop. 6.7. By Lemma 9.5, we have $x_1 \cdots x_k \triangleright_{S^k} x_{k+1} \cdots x_n$, so $x'_1 \preceq x$ implies $x'_1 \preceq x_1 \cdots x_k$, say $x_1 \cdots x_k = x'_1 y$. Let $(x'_2, \dots, x'_{k'})$ be a S-normal decomposition of y. By hypothesis, we have $\mathrm{Div}(x'_1) \cap S = \mathrm{Div}(x) \cap S$, hence $x'_1 \triangleright_S x'_2 \cdots x'_{k'}$, so $(x'_1, \dots, x'_{k'})$ is a S-normal sequence, hence another S-normal decomposition for $x_1 \cdots x_k$. Then Condition (9.1) implies $k' = k$.

Let us now consider the S-covering relation between x'_k and x_{k+1}. As in the proof of Prop. 7.11, let x' be a maximal S-simple divisor of $x'_k x_{k+1}$ satisfying $x'_k \preceq x'$. Write $x' = x'_k z$. Then $x'_1 \cdots x'_k z$ equals $x'_1 \cdots x'_{k-1} x'$, so it belongs to S^k, and, therefore, by Prop. 7.11, it must admit at least one normal form of length at most k. On the other hand, we have $x_k \triangleright_S x_{k+1}$ and $z \preceq x_{k+1}$, hence $x_k \triangleright_S z$, so, if z is not invertible, $(x_1, \dots, x_k, z)$ is another S-normal decomposition of $x'_1 \cdots x'_{k-1} x'$. Condition (9.1) discards this possibility. Hence, z must be invertible, *i.e.*, we must have $x'_k \triangleright_S x_{k+1}$. So the sequence $(x'_1, \dots, x'_k, x_{k+1})$ is S-normal, and, trivially, so is $(x'_1, \dots, x'_k, x_{k+1}, \dots, x_n)$. □

Proof of Lemma 9.4. Let $(x_1, \dots, x_n)$ and $(x'_1, \dots, x'_n)$ be two S-normal decomposition of an element x of M. Applying Lemma 9.6 to $(x_1, \dots, x_n)$ and to x'_1, we find $x_{2,1}, \dots, x_{k,1}$ so that $(x'_1, x_{2,1}, \dots, x_{k,1}, x_{k+1}, \dots, x_n)$ is another S-normal decomposition of x. Then, applying Lemma 9.6 to the latter sequence and to x'_2, we find $x_{3,2}, \dots, x_{k+1,2}$ so that $(x'_1, x'_2, x_{3,2}, \dots, x_{k+1,2}, x_{k+2}, \dots, x_n)$ is a S-normal decomposition of x. Similarly, having found a S-normal form $(x'_1, \dots, x'_i, x_{i+1,i}, \dots, x_{i+k-1,i}, x_{i+k}, \dots, x_n)$ for x, applying Lemma 9.6 to this sequence and to x'_{i+1} yields a new S-normal decomposition $(x'_1, \dots, x'_{i+1}, x_{i+2,i+1}, \dots, x_{i+k,i+1}, x_{i+k+1}, \dots, x_n)$. Now, we read on Fig. 9.1 that, for each i, the distance between $x_1 \cdots x_i$ and $x'_1 \cdots x'_i$ is bounded above by $2(k-1)$, as $x_1 \cdots x_{i+k-1}$ is a common multiple of these elements. □

Applying the previous result to the case of monoids with a Garside element, we deduce:

Proposition 9.7. *Assume that M is a thin cancellative monoid, Δ is a Garside element in M with k divisors, and G is the group of fractions of M. Assume moreover that, for every x in M, the following condition holds:*

(9.2) *All Δ-normal decompositions of x have the same length.*

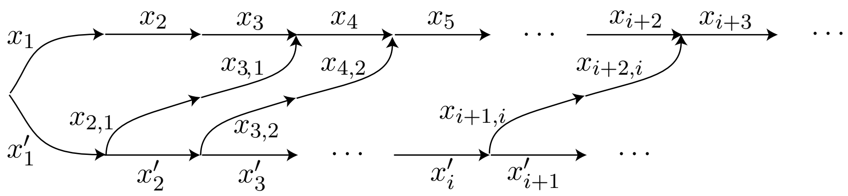

FIGURE 9.1. Comparing two normal forms of x (here $k = 3$)

Then the synchronous distance between any two Δ-normal decompositions of an element of G is uniformly bounded by $2(k-1)$.

PROOF. We have seen that, if $(\Delta^{-1}, \dots, \Delta^{-1}, x_1, \dots, x_n)$, k times Δ^{-1}, and $(\Delta^{-1}, \dots, \Delta^{-1}, x'_1, \dots, x'_{n'})$, k' times Δ^{-1}, are two Δ-normal decompositions for some element z of G, then, necessarily, $k = k'$ holds, and, therefore, $(x_1, \dots, x_n)$ and $(x'_1, \dots, x'_{n'})$ are two Δ-normal decompositions for some element of M. Then we apply Lemma 9.4 with $S = \mathrm{Div}(\Delta)$. □

The case of left multiplication in the monoid has already been treated in Lemma 7.12, which gives:

LEMMA 9.8. *Assume that M is a quasi-atomic cancellative monoid, S quasi-spans M, and y is a S-simple element of M. Then, for every element x of M, and every S-normal decomposition of x, there exists a S-normal decomposition of yx at synchronous distance at most* 1.

It remains to extend the result to the group of fractions.

PROPOSITION 9.9. *Assume that M is a thin cancellative monoid, Δ is a Garside element in M with k divisors, G is the group of fractions of M, and y is a Δ-simple element of M. Then, for every element z of G, and every Δ-normal decomposition of z, there exists a Δ-normal decomposition of yz at synchronous distance at most* $3k$.

PROOF. Assume first $y \in \mathrm{Div}(\Delta)$. Assume $z = \Delta^{-k}x$, with $x \in M$ and $\Delta \not\preceq x$. Then we have $yz = \Delta^{-k}y'x$ with $y' = \phi_\Delta^{-k}(y)$. By Prop. 8.5, we have $y' \preceq \Delta$, so, in particular, y' is Δ-simple, and we can apply Lemma 9.8 to y' and any Δ-normal decomposition $(x_1, \dots, x_n)$ of x to obtain a Δ-normal decomposition $(x'_1, \dots, x'_n, y'_n)$ of $y'x$. There remains one point to check: if it contains at least one Δ^{-1}, the sequence $(\Delta^{-1}, \dots, \Delta^{-1}, x'_1, \dots, x'_n, y'_n)$ is Δ-normal only if x'_1 is not Δ: if $x'_1 = \Delta$ holds, we must cancel x'_1 with the last Δ^{-1}, and repeat the reduction until we possibly find $x'_i \neq \Delta$. As each such reduction increases the synchronous distance by 2, there could be a problem here. Actually, we shall prove that $x'_1 \simeq x'_2 \simeq \Delta$ implies $\Delta \preceq x_1$, hence $x_1 \simeq \Delta$. Here we use the hypothesis that y' is not only Δ-simple, but also it is a divisor of Δ. First, $x'_1 \simeq x'_2 \simeq \Delta$ implies $x'_1x'_2 \simeq \Delta^2$. Indeed, for $u \in M^*$, we have $u\Delta = xv$ for some x and v satisfying $x \in \mathrm{Div}(\Delta)$ and $v \in M^*$, and $\|x\| = \|\Delta\|$ implies $x \simeq \Delta$. So we deduce $\Delta^2 \preceq y'x_1x_2$, *i.e.*, $y'y'^*\Delta \preceq y'x_1x_2$, hence $y'^*\Delta \preceq x_1x_2$, *i.e.*, $\Delta\phi_\Delta(y'^*) \preceq x_1x_2$ which implies $\Delta \preceq x_1x_2$, and, finally, $\Delta \preceq x_1$ as $x_1 \triangleright_\Delta x_2$ holds by hypothesis. So, at most one reduction $\Delta^{-1}\Delta$ may occur, and the synchronous distance between the Δ-normal form of x and that of yx is at most 3.

The result for an arbitrary Δ-simple element y follows, as, by Prop. 6.7, any such element is the product of at most k elements of $\mathrm{Div}(\Delta)$. □

Putting Propositions 9.1, 9.7, and 9.9 together, we deduce

PROPOSITION 9.10. *Assume that G is the group of fractions of a cancellative monoid M that admits a Garside element Δ such that all Δ-normal forms of an element have the same length. Then G is an automatic group.*

The previous result applies in particular to every thin Gaussian group, *i.e.*, to every Garside group—hence in particular to every spherical Artin–Tits group. But non-Gaussian groups are also eligible:

EXAMPLE 9.11. Consider once more the groups G_1 and G_3 of Example 4.4. We have seen in Example 8.12 that the monoid M_1 contains a Garside element Δ such that the Δ-simple elements are determined by their divisors in $\mathrm{Div}(\Delta)$. So the associated Δ-normal form is unique, and, therefore, the length requirement is satisfied. The argument is similar for M_3. So the groups G_1 and G_3 are automatic.

The case of G_2 is slightly different. Indeed, in the monoid M_2, a^2 is a Garside element, but ab and ac are a^2-simple elements with the same divisors in $\mathrm{Div}(a^2)$, namely 1, a, b, c. Now, we have the following sufficient condition:

PROPOSITION 9.12. *Assume that M is a thin cancellative monoid with no non-trivial unit, Δ is a Garside element in M, and the following condition holds in M: If x and x' are distinct Δ-simple elements with the same divisors in* $\mathrm{Div}(\Delta)$*, then every common multiple of x and x' is a multiple of some Δ-simple common multiple of x and x'. Then the Δ-normal form is unique, and, therefore, the group of fractions of M is automatic.*

PROOF. It suffices to show that, for every x in M, there exists a unique Δ-simple element x_1 with the same divisors as x in $\mathrm{Div}(\Delta)$. Now, assume that x_1 and x'_1 satisfy these conditions and are distinct. Then, by hypothesis, there exists a Δ-simple element x''_1 satisfying $x_1 \preceq x''_1 \preceq x$ and $x'_1 \preceq x''_1 \preceq x$. Then $x'_1 = x''_1$ would imply $x_1 \prec x'_1$, contradicting the Δ-simplicity of x'_1. So we must have $x_1 \prec x''_1$, and, therefore, $\mathrm{Div}(x_1) \cap \mathrm{Div}(\Delta) \neq \mathrm{Div}(x'_1) \cap \mathrm{Div}(\Delta) \subseteq \mathrm{Div}(x) \cap \mathrm{Div}(\Delta)$, which contradicts $\mathrm{Div}(x_1) \cap \mathrm{Div}(\Delta) = \mathrm{Div}(x) \cap \mathrm{Div}(\Delta)$. □

EXAMPLE 9.13. The previous criterion applies to the monoid M_2: indeed, for $\Delta_1 = a^2$, the only problem with Δ_1 occurs with the Δ_1-simple elements ab and ac. Now, every common multiple of ab and ac is a multiple of a^2, *i.e.*, of Δ_1. We deduce that G_2 is automatic.

Let us conclude with some open questions.

QUESTION 9.14. If Δ is a Garside element in a thin cancellative monoid M, do all Δ-normal decompositions of a given element of M necessarily have the same length, *i.e.*, is the additional assumption of Prop. 9.10 superfluous?

In the Gaussian case, Lemma 7.13 gives a uniform bound for the synchronous distance between the normal form of x and that of xy when y is simple. It is then easy to deduce that the Δ-normal form of Prop. 9.10 gives rise to a bi-automatic structure—alternatively, we can also replace in this case the asymmetric form $\Delta^{-k}x_1 \cdots y_n$ with a symmetric one $y_p^{-1} \cdots y_1^{-1} x_1 \cdots x_n$ [**18, 9**]. In the general case, the argument fails, the behaviour of Δ-normal form with respect to right multiplication remains unknown, and so does the existence of an automatic structure involving a symmetric fractionary decomposition (defining the latter in the non-Gaussian case seems to require a uniform bound for the distance between the possible various mcm's of two elements in the monoid).

Question 9.15. Under the hypotheses of Prop. 9.10, is the group G bi-automatic?

(In the case of the groups G_1, G_2, G_3 of Example 4.4, a simple specific argument gives a positive answer.)

By Prop. 8.7, common multiples must exist in every thin cancellative monoid admitting a Garside element. In the Gaussian case, *i.e.*, when we assume not only that common multiples exist, but even that least common multiples exist, then the lcm of all primitive elements is a Garside element.

Question 9.16. Does every thin cancellative monoid admitting common multiples contain a Garside element? More precisely, need every mcm of the primitive elements be a Garside element?

Finally, let us mention an open problem dealing with the Gaussian case:

Question 9.17. Is every finitely generated Gaussian group thin, *i.e.*, is every finitely generated Gaussian group necessarily a Garside group?

References

[1] S.I. Adyan, *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.

[2] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.

[3] M. Brazil, *Monoid growth functions for braid groups*, Int. J. Algebra & Comput. **1-2** (1991) 201–205.

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

[5] R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292-4** (1992) 671–683.

[6] R. Charney, *Geodesic automation and growth functions for Artin groups of finite type*, Math. Ann. **301-2** (1995) 307–324.

[7] A.H. Clifford & G.B. Preston, *The Algebraic Theory of Semigroups, vol. 1*, Amer. Math. Soc. Surveys **7**, (1961).

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

[9] P. Dehornoy, *Groupes de Garside*, Ann. Sci. Ec. Norm. Sup., to appear; ArXiv math.GR/0111157.

[10] P. Dehornoy, *Complete positive group presentations*, Preprint; ArXiv math.GR/0111275.

[11] P. Dehornoy & L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. **79-3** (1999) 569–604.

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

[13] E. A. Elrifai & H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.

[14] D. Epstein & *al.*, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).

[15] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20** No.78 (1969) 235–254.

[16] R. C. Lyndon & P. E. Schupp, *Combinatorial group theory*, Springer (1977).

[17] M. Picantin, *The center of thin Gaussian groups*, J. of Algebra **245-1** (2001) 92–122.

[18] W. Thurston, *Finite state algorithms for the braid group*, Circulated notes (1988).

[19] P. Xu, *Growth of the positive braid groups*, J. Pure Appl. Algebra **80** (1992) 197–215.

Laboratoire SDAD, Mathématiques, Université de Caen BP 5186, 14032 Caen, France
E-mail address: dehornoy@math.unicaen.fr
URL: //www.math.unicaen.fr/∼dehornoy