Garside monoids and groups

Thomas Gobet

October 1, 2023

Contents

Chapter 1

Garside monoids and groups

Throughout the whole chapter M will denote a monoid. Recall that a monoid always admits a unit 1.

1.1 Cancellative monoids

Definition 1.1.1. A monoid M is *left-cancellative* if for all $a, b, c \in M$,

$$ab = ac \ \Rightarrow b = c.$$

It is *right-cancellative* if for all $a, b, c \in M$,

$$ba = ca \ \Rightarrow \ b = c.$$

If M is both left- and right-cancellative, we say that M is *cancellative*.

Showing that a monoid is (left- or right-) cancellative is a difficult task in general.

Example 1.1.2. Every group G is in particular a cancellative monoid.

Example 1.1.3. Let $M = \langle\, x, y, z, t \mid xy = zt \,\rangle$. Then M is both left- and right-cancellative. To prove this, notice that there is no defining relation in M of the form $y \cdots = \cdots$, or $t \cdots = \cdots$. There is also no relation of the form $\cdots x = \cdots$, or $\cdots z = \cdots$. It follows that the positions in a word in which one can apply a relation stay the same after application of a defining relation. That is, if $x_1 x_2 \cdots x_k$ is a word in x, y, z, t, and $(i, i+1)$ are consecutive positions where a relation can be applied, i.e., $x_i x_{i+1}$ is the left or right hand side of the defining relation $xy = zt$, say $x_i = x$ and $x_{i+1} = y$, then one can neither apply a relation on $x_{i-1}x_i$ nor on $x_{i+1}x_{i+2}$, and the same stays true after replacing x_i by $x'_i = z$ and x_{i+1} by $x'_{i+1} = t$. Left-cancellativity easily follows from this observation, showing that $ab = ac$ implies $b = c$ by induction on the length of a, where the length $\ell(a)$ of an element $a \in M$ is defined by $\ell(a) = k$, where $a_1 a_2 \cdots a_k = a$, with $a_i \in \{x, y, z, t\}$ for all i. Note that this length is well-defined since the defining relation of M is homogeneous, hence all the words in M representing a have the same length. Right-cancellativity follows as the monoid is isomorphic to its opposite monoid.

Example 1.1.4. The monoid $M = \langle\, a, b, c \mid ab = ac \,\rangle$ is not left-cancellative. Indeed, as the defining relation is homogeneous, there is a well-defined length function on M which assigns to any element $m \in M$ the length of any word representing m. Then $ab = ac$ has length two and b has length one. But $b \neq c$ as no relation can be applied to the word b. However, we claim that M is right-cancellative (see Exercise 1.1.5 below).

Of course, one way to show that a monoid M is cancellative is to embed it into a group, but this is a difficult task in general, and many known criteria to embed a monoid M into a group G require one to first establish cancellativity of M.

Exercise 1.1.5. Show that $M = \langle\ a, b, c \mid ab = ac\ \rangle$ is right-cancellative.

Exercise 1.1.6. Let $M = \langle\ x, y \mid x^2 = y^2\ \rangle$. Show that M is left- and right-cancellative.

Cancellativity is obviously a necessary condition for embedding a monoid into a group. It turns out that it is not sufficient, as the next counterexample (guven by Maltsev [9] in 1937) shows.

Example 1.1.7. Let $M = \langle\ a, b, c, d, x, y, u, v \mid ax = by, cx = dy, au = bv\rangle$. Then M is both left- and right-cancellative, but does not embed into a group. To see this, consider any word $x_1x_2\cdots x_k$. Call a pair of successive positions $(i, i+1)$ *good* if one can apply a relation $x_ix_{i+1} = x'_ix'_{i+1}$. Note that any side of a relation ends with a letter in $S_1 = \{x, y, u, v\}$, while it begins with a letter in $S_2 = \{a, b, c, d\}$. Since we have $S_1 \cap S_2 = \emptyset$, it follows that the set of good positions in $x_1x_2\cdots x_k$ and $x_1x_2\cdots x_{i-1}x'_ix'_{i+1}x_{i+2}\cdots s_k$ are the same, and that if $(i, i+1)$ and $(j, j+1)$ are distinct good sets of positions, then $\{i, i+1, j, j+1\}$ has cardinal 4. As a consequence, the set of good positions is constant on words for any elements, and the order in which relations are applied to any word does not matter. Left- and right-cancellativity follows easily, arguing as in Example 1.1.3. Now assume that M embeds into a group G. Then in G we have

$$d^{-1}c = yx^{-1} = b^{-1}a = vu^{-1}$$

from what we deduce that $cu = dv$ in G. But $cu, dv \in M$, while in M we have $cu \neq dv$, a contradiction.

In Section 1.6 below, we shall establish a few criteria to check that a monoid is left- or right-cancellative.

Lemma 1.1.8. *If M is left-cancellative (respectively right-cancellative) and 1 is the only invertible element in M, then the left-divisibility (resp. right-divisibility) relation on M is a partial order.*

Proof. Reflexivity is clear as M has a unit 1 and transitivity is also clear (and both hold without the cancellativity assumption and without the assumption on invertible elements). Let $a, b \in M$ such that a left-divides b and b left-divides a. Then there are $c, c' \in M$ satisfying $ac = b$ and $bc' = a$. Hence we get $b = ac = bc'c$. By left-cancellativity this implies $c'c = 1$, hence $c = 1 = c'$ as 1 is the only invertible element in M. Hence $a = b$, and the left-divisibility relation is reflexive. The proof of the right counterparts is similar. □

We end up the section with a proof that the monoid $M = \langle a, b \mid aba = bab\rangle$ is both left- and right-cancellative. This is the braid monoid on three strands, one of the most basic examples of a Garside monoid, and we will use it as a running example along the way. The proof below is based on Garside's original proof of the cancellativity of the positive braid monoid B_n^+ [7].

Proposition 1.1.9. *The monoid $B_3^+ = \langle a, b \mid aba = bab\rangle$ is both left- and right-cancellative.*

Proof. Note that $M := B_3^+$ is isomorphic to the opposite monoid M^{op}. It therefore suffices to show that M is left-cancellative to also obtain right-cancellativity.

Since the defining relation $aba = bab$ is homogeneous, every element $x \in M$ has a well-defined length, given by the length of any word for x in the generating set $S := \{a, b\}$. We begin by showing the following property (P): let $X, Y \in M$ and $x, y \in S$ such that $xX = yY$. Then

1. If $x = y$, then $X = Y$.

2. If $x \neq y$, then there is $Z \in M$ such that $X = yxZ$ and $Y = xyZ$.

We argue by induction on the length of X. If $\ell(X) = 0$, then $X = 1 = Y$, but we also have $x = y$, hence 1 holds. The second situation cannot appear. If $\ell(X) = 1$, then the second situation also cannot appear, since we would have two word xX and yY of length two representing the same element of M but starting with a different letter, which is impossible since the single defining relation of M equates two words of length three.

Hence assume that the result holds for all X such that $\ell(X) \leq 1$. Assume that $\ell(X) > 1$. Consider a sequence of elements $x_0 = x, x_1, x_2, \ldots, x_k = y \in S$ and words $X_0, X_1, X_2, \cdots, X_k$ in S^* such that $x_0X_0 = x_1X_1 = \cdots = x_{k-1}X_{k-1} = x_kX_k$, (as elements of M) where X_0 is a word for X, X_k is a word for Y, and such that every two successive words x_iX_i and $x_{i+1}X_{i+1}$ in the sequence differ by a single application of the defining relation $aba = bab$. We then do a second induction, on k, to conclude the proof of (P). Assume that $k = 0$. Then $x = y, X = Y$, and there is nothing to prove. Assume that $k = 1$. Then one passes the word x_0X_0 to the word x_1X_1 by a single application of the relation $aba = bab$. If the relation is applied inside X_0, then $x = y$, and $X = Y$ since X_0 is a word for X, X_1 is a word for Y, and they differ by a single application of the relation $aba = bab$. If the relation is not applied inside X_0, it is then applied at the beginning of the word x_0X_0, hence $x_0 = a$ and X_0 begins with ba, or $x_0 = b$ and X_0 begins with ab. Assume that $x_0 = a$, the other case is similar. We then have the existence of a word W such that $X_0 = baW$, and $x_0X_0 = abaW$. The word x_1X_1 is then given by $babW$, hence we have $X_1 = abW$, which concludes the proof, taking for Z the element represented by the word W.

Now assume that $k \geq 2$. Let i be any integer such that $0 < i < k$. We can thus apply (P) to both the pairs of words (x_0X_0, x_iX_i), and (x_iX_i, x_kX_k), as in every couple, the second word is obtained from the first one by a number of applications of $aba = bab$ which is less than k. Hence we have three cases: if $x_0 = x_i = x_k$, then denoting by W the element represented by X_i we have $X = W$ and $W = Y$, hence $X = Y$, which concludes the proof. If $x_0 = x_i$ but $x_i \neq x_k$, say $x_0 = a$ and $x_k = b$ (the other case is similar), then there is an element $Z \in M$ such that $W = baZ$ and $Y = abZ$ and $X = baZ$. If $x_0 \neq x_i$ but $x_i = x_k$ we have a similar situation. Finally, assume that $x_0 \neq x_i$ and $x_i \neq x_k$, say $x_0 = a = x_k$ and $x_i = b$. Then there are $Z_1, Z_2 \in M$ such that $X = baZ_1$, $X_i = abZ_1$, $X_i = abZ_2$, $Y = baZ_2$. Now $\ell(X_i) < \ell(x_iX_i)$, hence by induction, applying the situation (1) twice we get that $abZ_1 = abZ_2$ implies that $bZ_1 = bZ_2$, which implies that $Z_1 = Z_2$. Setting $Z := Z_1 = Z_2$, we thus get $X = baZ_1 = baZ = baZ_2 = Y$, which concludes the proof of property (P).

We now show that M is left-cancellative. Assume that $x, y, z \in M$ are such that $xz = xy$. We argue by induction on $\ell(x)$. If $\ell(x) = 0$ then $x = 1$ and $z = y$. If $\ell(x) > 0$, then there is $u \in S$, $v \in M$ such that $x = uv$. We then have $uvz = uvy$. Since $\ell(u) = 1$, by property (P) we deduce that $vz = vy$. Since $\ell(v) = \ell(x) - 1$, by induction we deduce that $z = y$. This concludes the proof. □

The above proof gives an insight of how difficult it can be to show that a monoid defined by generators and relations is cancellative. There are very few general criteria to show such a property, which is a difficult task in general. In Section 1.6 below we will give some such criteria.

Exercise 1.1.10. Show that the monoid $M = \langle a, b \mid abab = baba \rangle$ is both left- and right-cancellative.

Exercise 1.1.11. Show that the monoid

$$M = \langle a, b, c \mid aba = bab, aca = cac, bcb = cbc, abca = bcab = cabc \rangle$$

is not cancellative.

1.2 Ore monoids

Definition 1.2.1 (Divisors and multiples)**.** Let $a, b, c \in M$. If $ab = c$ holds, we say that a is a *left-divisor* (respectively, that b is a *right-divisor*) of c and that c is a *right-multiple* of a (respectively a *left-multiple* of b).

Theorem 1.2.2 (Ore's Theorem)**.** *If M is cancellative, and if any two elements $a, b \in M$ admit a common left-multiple, that is, if there is $c \in M$ satisfying $a'a = c = b'b$ for some $a', b' \in M$, then M admits a group of (left-)fractions $G(M)$ in which it embeds.*

Proof. Set

$$G(M) := \{(a, b) \mid a, b \in M\}/\sim,$$

where $\sim$ is the equivalence relation generated by $(a, b) \sim (xa, xb)$, $x \in M$ for all $a, b, x \in M$. We will denote by $a^{-1}b$ the equivalence classe of the pair (a, b) in $G(M)$. We begin by defining the product of two fractions $a^{-1}b$ and $c^{-1}d$. To this end, consider a common left-multiple of b and c, that is, let b', c' such that $b'b = c'c$. We then set

$$(a^{-1}b) \cdot (c^{-1}d) := (b'a)^{-1}(c'd).$$

We have to check that this is independent of the choices we made. We first show that it is independent of the choice of common left-multiple of b and c. Hence let $b'', c'' \in M$ such that $b''b = c''c$. Then the two left-multiples $b''b = c''c$ and $b'b = c'c$ themselves have a common left-multiple, say there is $x, y \in M$ such that

$$xb''b = xc''c = yb'b = yc'c,$$

and by right-cancellativity we get that $xb'' = yb'$ and $xc'' = yc'$. We thus get

$$(b'a)^{-1}(c'd) = (yb'a)^{-1}(yc'd) = (xb''a)^{-1}(xc''d) = (b''a)^{-1}(c''d),$$

which shows the claim. We also need to show that the product $\cdot$ is independent of the choices of representatives (a, b) and (c, d) for the fractions $a^{-1}b$ and $c^{-1}d$. Hence let $x \in M$. We have

$$((xa)^{-1}xb) \cdot (c^{-1}d) = (\widetilde{b}xa)^{-1}\widetilde{c}d,$$

where $\widetilde{b}, \widetilde{c}$ are such that $\widetilde{c}c = \widetilde{b}xb$. Since this is a left-common multiple of b and c, we get by the already proved property that $(a^{-1}b) \cdot (c^{-1}d)$ does not depend on the chosen left-common multiple for b and c that

$$(\widetilde{b}xa)^{-1}\widetilde{c}d = (a^{-1}b) \cdot (c^{-1}d).$$

Similary we show that $(a^{-1}b) \cdot ((xc)^{-1}(xd)) = (a^{-1}b) \cdot (c^{-1}d)$. Hence the product is well-defined.

To prove associativity, let $x_i^{-1}y_i$, $i = 1, 2, 3$, be three fractions. Let a_1, a_2 such that $a_1y_1 = a_2x_2$. Let a_2', a_3' such that $a_2'y_2 = a_3'x_3$. And let a, a' such that $aa_2' = a'a_2$. We then have

$$(x_1^{-1}y_1) \cdot ((x_2^{-1}y_2) \cdot (x_3^{-1}y_3)) = (x_1^{-1}y_1) \cdot ((a_2'x_2)^{-1}a_3'y_3) = (a'a_1x_1)^{-1}(aa_3'y_3),$$

where the last equality holds true since $a'a_1y_1 = aa_2'x_2$. On the other hand we have

$$((x_1^{-1}y_1) \cdot (x_2^{-1}y_2)) \cdot (x_3^{-1}y_3) = ((a_1x_1)^{-1}a_2y_2) \cdot (x_3^{-1}y_3) = (a'a_1x_1)^{-1}(aa_3'y_3),$$

where the last equality holds true since $a'a_2y_2 = aa_3'x_3$. This shows associativity.

It is clear that the fraction $1^{-1}1$ is the neutral element, and that every fraction $a^{-1}b$ has an inverse $b^{-1}a$. □

Definition 1.2.3. A monoid satisfying the assumtions of Theorem 1.2.2 is a *(left) Ore monoid*.

Proposition 1.2.4. *Let M be a cancellative monoid in which any two pair of elements admit a common left-multiple and let $\iota_M : M \longrightarrow G(M)$ be the canonical embedding. Assume that G is a group and $f : M \longrightarrow G$ is an injective morphism of monoids. Then there is a unique injective group morphism $\varphi : G(M) \longrightarrow G$ such that $\varphi \circ \iota_M = f$.*

Proof. Let $(a, b) \in G(M)$ and define $\varphi((a, b))$ by $f(a)^{-1}f(b)$. It is clear that φ is well-defined. Let (a_1, b_1), $(a_2, b_2) \in G(M)$. Consider a left-multiple $b'b_1 = a'a_2$. We then have that $(a_1, b_1)(a_2, b_2) = (b'a_1, a'b_2)$. We thus have

$$\varphi((a_1, b_1)(a_2, b_2)) = f(b'a_1)^{-1}f(a'b_2).$$

On the other hand we have

$$\varphi((a_1, b_1))\varphi((a_2, b_2)) = f(a_1)^{-1}f(b_1)f(a_2)^{-1}f(b_2),$$

but since $b'b_1 = a'a_2$ we deduce that, in G, we have $f(b_1)f(a_2)^{-1} = f(b')^{-1}f(a')$, hence we have

$$\varphi((a_1, b_1)(a_2, b_2)) = f(a_1)f(b')^{-1}f(a')f(b_2) = f(a_1)^{-1}f(b_1)f(a_2)^{-1}f(b_2) = \varphi((a_1, b_1))\varphi((a_2, b_2)).$$

Since it is clear that $\varphi(1_{G(M)}) = 1_G$, we deduce that φ is a group morphism, and by construction it is clear that $\varphi \circ \iota_M = f$. Given $(a, b) \in G(M)$, we have

$$\varphi((a, b)) = 1 \;\Leftrightarrow\; f(a)^{-1}f(b) = 1 \;\Leftrightarrow f(a) = f(b),$$

which, as f is injective, happens if and only if $a = b$. Hence φ is injective.

Uniqueness follows from the fact that, if φ' is another group morphism such that $\varphi' \circ \iota_M = f$, then $\varphi'(a) = \varphi(a)$ for all $a \in M$, yielding $\varphi'(a, b) = \varphi'(a)^{-1}\varphi'(b)$ and hence

$$\varphi((a, b)) = f(a)^{-1}f(b) = \varphi'(a)^{-1}\varphi'(b) = \varphi'((a, b)),$$

which concludes the proof. □

Corollary 1.2.5. *Let M be a cancellative monoid in which any two pair of elements admit a common left-multiple and let $\langle \mathcal{S} \mid \mathcal{R} \rangle$ be a presentation of M. Then $\langle \mathcal{S} \mid \mathcal{R} \rangle$, viewed as a group presentation, is a presentation of $G(M)$.*

Proof. It is clear by construction that $\mathcal{S}$ generates $G(M)$ as a group, and since M embeds into $G(M)$, the defining relations $\mathcal{R}$ also hold in $G(M)$. It follows that $G(M)$ is a quotient of $\widetilde{G(M)} := \langle \mathcal{S} \mid \mathcal{R} \rangle$. Since M embeds into $G(M)$ and this map factors through $\widetilde{G(M)}$, the monoid M also embeds into $\widetilde{G(M)}$. by Proposition 1.2.4, there is a unique (injective) group morphism $\varphi : G(M) \longrightarrow \widetilde{G(M)}$ making the expected diagram commute. Both this morphism and the above quotient map send a generator $s \in \mathcal{S}$ to itself, hence the two maps are inverse to each other, and $G(M) \cong \widetilde{G(M)} = \langle \mathcal{S} \mid \mathcal{R} \rangle$. □

Remark 1.2.6. If M is a cancellative monoid in which any pair of elements admit a common left-multiple, one can similarly define a group of right-fractions of M in which M embeds. In particular, if M is cancellative and any pair of elements admit both a common left-multiple and a common right-multiple, then one gets two groups. By the universal property (Proposition 1.2.4), these groups are then isomorphic.

Example 1.2.7. Consider the monoid B_3^+ from Proposition 1.1.9. We already know from Proposition 1.1.9 that B_3^+ is cancellative. We show that any pair x, y of elements of B_3^+ admit a common left-multiple. To this end, consider the element $\Delta := aba = bab \in B_3^+$. We claim that Δ^2 is central in B_3^+. Indeed, we have

$$a\Delta^2 = a(aba)(aba) = a(bab)(aba) = (aba)(bab)a = \Delta^2 a,$$

and we similarly show that $b\Delta^2 = \Delta^2 b$. Since a and b generate B_3^+ we deduce that Δ^2 is central in B_3^+. Now a and b both right-divide Δ (hence Δ^2). It follows that, if x is any element and $x_1x_2\cdots x_k$ a word for x in S^* (recall that $S = \{a, b\}$), then considering $y_1, y_2, \ldots, y_k$ such that $y_ix_i = \Delta^2$ for all $i = 1, \ldots, k$, we have using that Δ^2 is central that

$$\begin{aligned} y_ky_{k-1}\cdots y_2y_1x_1x_2\cdots x_k &= y_ky_{k-1}\cdots y_2\Delta^2x_2\cdots x_k = \Delta^2 y_ky_{k-1}\cdots y_2x_2\cdots x_k \\ &= \Delta^2 y_ky_{k-1}\cdots y_2\Delta^2x_2\cdots x_k = \Delta^4 y_ky_{k-1}\cdots y_3x_3\cdots x_k \\ &= \cdots = (\Delta^2)^{i-1}y_k\cdots y_ix_i\cdots x_k = \cdots = \Delta^{2k}. \end{aligned}$$

This shows that, for any $x \in M$ such that $\ell(x) = k$, the element Δ^{2k} is a left-multiple of x. Hence setting $k := \max\{\ell(x), \ell(y)\}$, we get that Δ^{2k} is a left-multiple of both x and y. In fact this bound can be reduced to k, i.e., one can show that Δ^k is already a left-multiple of both x and y (see Exercise 1.2.8 below). Applying Ore's Theorem (Theorem 1.2.2 above), we get that B_3^+ embeds into its group of (left-)fractions $G(B_3^+)$, and by Corollary 1.2.5 this group has presentation $\langle a, b \mid aba = bab\rangle$.

Exercise 1.2.8. Let $B_3^+ = \langle a, b \mid aba = bab\rangle$. Let $x, y \in B_3^+$. Show that Δ^k is both a common left- and right-multiple of x and y, where $k := \max\{\ell(x), \ell(y)\}$.

Exercise 1.2.9. Let $B_3^+ = \langle a, b \mid aba = bab\rangle$ which, by Example 1.2.7 above, is an Ore monoid. Write the elements $ab^{-1}a$, a^2b^{-3} as fractions $x^{-1}y$ with $x, y \in B_3^+$.

1.3 Monoids with Noetherian divisibility

Definition 1.3.1 (Noetherian divisibility)**.** We say that the divisibility in M is *Noetherian* if there exists a function $\lambda : M \to \mathbb{Z}_{\geq 0}$ satisfying $\forall a, b \in M$, $\lambda(ab) \geq \lambda(a) + \lambda(b)$ and $a \neq 1 \Rightarrow \lambda(a) \neq 0$. We say that M is *right-Noetherian* (respectively *left-Noetherian*) if every strictly increasing sequence of divisors with respect to left-divisibility (resp. right-divisibility) is finite. Note that if the divisibility in M is Noetherian, then M is both left- and right-Noetherian.

Note that it implies that the only invertible element in M is 1 and that M is infinite for $M \neq \{1\}$. In particular, by Lemma 1.1.8, in a cancellative monoid M with Noetherian divisibility, both left-divisiblity and right-divisibility induce a partial order on M.

Example 1.3.2. Consider the monoid $M = \langle a, b \mid aba = bab\rangle$. Then M has Noetherian divisibility. Indeed, since its defining relation is homogeneous, the function λ defined on generators by $\lambda(a) = 1 = \lambda(b)$ uniquely extends to a length function $\lambda : M \longrightarrow \mathbb{Z}_{\geq 0}$ satisfying the assumtions of Definition 1.3.1. Note that in this case we have $\lambda(xy) = \lambda(x) + \lambda(y)$ for all $x, y \in M$. In fact M is the classical braid monoid on three strands.

Example 1.3.3. Consider the monoid $M = \langle a, b \mid aba = b^2\rangle$. Then M has Noetherian divisibility. Indeed, setting $\lambda(a) = 1$ and $\lambda(b) = 2$, we obtain that the defining relation is homogeneous. As in the previous case we thus have $\lambda(xy) = \lambda(x) + \lambda(y)$ for all $x, y \in M$.

Example 1.3.4. Consider the monoid $M = \langle a, b \mid aba = b \rangle$. Then M is neither left- nor right-Noetherian. Indeed we have

$$b = aba, ab = a^2ba, a^2b = a^3ba, \dots,$$

Hence denoting by $\leq$ the left-divisibility relation, we have

$$\cdots \leq a^{i+1}b \leq a^ib \leq \cdots \leq a^2b \leq ab \leq b,$$

and the above sequence is strictly decreasing as $a^{i+1}b \neq a^ib$ for all $i \geq 0$: indeed the parity of the number of a's appearing in a word is constant on words for a given element of M. Hence M is not right-Noetherian, and since M is symmetric we conclude that it is not left-Noetherian either.

Example 1.3.5. Consider the monoid $M = \langle a, b \mid ababa = b^2 \rangle$. Then for every $x \in M$, the number of b's appearing in any word for x is constant. It is clear that there is no length function $\lambda : M \longrightarrow \mathbb{Z}_{\geq 0}$ satisfying $\lambda(xy) = \lambda(x) + \lambda(y)$ for all $x, y \in M$ and $x \neq 1 \Rightarrow \lambda(x) \neq 0$, as because of the relation $ababa = b^2$ we would have $\lambda(a) = 0$, while $a \neq 1$ (there is an obvious morphism from M to $\mathbb{Z}/3\mathbb{Z}$ sending b to 0 and a to 1). But one can show there is one such fonction satisfying $\lambda(xy) \geq \lambda(x) + \lambda(y)$, given by

$$\lambda(x) = \sup\{k \mid x = a_1a_2 \cdots a_k, a_i \in \{a, b\}\}.$$

Exercise 1.3.6. Let $M = \langle a, b \mid aba = ba^2b \rangle$. Show that M does not have Noetherian divisibility.

Exercise 1.3.7. Show that the groups with the same presentations as the monoids M from Examples 1.3.2, 1.3.3 and Exercise 1.3.6 are all isomorphic.

1.4 Garside monoids

Definition 1.4.1. Assume that M is a monoid having 1 as only invertible element, so that left- and right-divisibility yield partial orders. Let $a, b \in M$. We say that $c \in M$ is a *left-lcm* of a and b if there are a', b' such that $c = a'a = b'b$, and if whenever c' is a common left-multiple of a and b, we have that c right-divides c'. We say that c is a *right-gcd* of a and b if it right-divides both a and b, and if any common right-divisor of a and b right-divides c.

Definition 1.4.2 (Garside monoid)**.** A *Garside monoid* is a pair (M, Δ) where M is a monoid with 1 and Δ is an element of M, satisfying the following five conditions

1. M is left- and right-cancellative,
2. The divisibility in M is Noetherian,
3. Any two elements in M admit a left- and right-lcm, and a left- and right-gcd,
4. the left- and right-divisors of the element Δ coincide and generate M,
5. The set of (left- or right-)divisors of Δ is finite.

Note that under these assumptions, the restrictions of left- and right-divisibility to the set of divisors of Δ yield two lattice structures on this set. We denote the set of divisors of Δ by $\mathrm{Div}(\Delta)$.

Definition 1.4.3. By Ore's Theorem 1.2.2, every Garside monoid (M, Δ) embeds into a group of left-fractions, or a group of right-fractions. By Remark 1.2.6, these two groups are isomorphic. We denote the resulting group by $G(M)$ and call it a *Garside group*. In other words, a Garside group is the group of (left- or right-) fractions of a Garside monoid. The element Δ is called a *Garside element* in M. More generally, an element Δ of a cancellative monoid M with Noetherian divisibility satisfying the conditions 4 and 5 above will be called a Garside element.

Note that, given a Garside monoid M, the element Δ is not uniquely determined in general. But we have:

Lemma 1.4.4. *Let M be a Garside monoid and Δ, Δ' two Garside elements in M. Then the left-gcd $\Delta \wedge_L \Delta'$ of Δ and Δ' is equal to the right-gcd $\Delta \wedge_R \Delta'$, and is a Garside element in M.*

Proof. Since $\Delta \wedge_L \Delta'$ is a left-divisor of both Δ and Δ', and Δ, Δ' are Garside elements in M, we have that $\Delta \wedge_L \Delta'$ is a right-divisor of both Δ and Δ'. Hence $\Delta \wedge_L \Delta' \leq_R \Delta \wedge_R \Delta'$. Hence there is an element $a \in M$ such that $\Delta \wedge_R \Delta' = a\Delta \wedge_L \Delta'$. Similarly, we have $\Delta \wedge_R \Delta' \leq_L \Delta \wedge_L \Delta'$, hence there is $b \in M$ such that $\Delta \wedge_L \Delta' = \Delta \wedge_R \Delta' b$. Combining both yields

$$a\Delta \wedge_R \Delta' b = \Delta \wedge_R \Delta',$$

hence by Noetherian divisibility we obtain that $\lambda(a) = 0 = \lambda(b)$, which forces $a = 1 = b$. Hence $\Delta \wedge_L \Delta' = \Delta \wedge_R \Delta'$.

Let $x \leq_L \Delta \wedge_L \Delta'$. Then $x \leq_L \Delta, \Delta'$, hence $x \leq_R \Delta, \Delta'$ since Δ, Δ' are Garside elements in M. Conversely, one similarly shows that every right-divisor of $\Delta \wedge_L \Delta' = \Delta \wedge_R \Delta'$ is also a left-divisor. Hence both sets coincide.

Every atom it both a left- and right- divisor of any Garside element, hence denoting by $\mathcal{S}$ the set of atoms of M, we have $s \leq_L \Delta, \Delta'$ and $s \leq_R \Delta, \Delta'$. It follows that the set S left- and -right divides $\Delta \wedge_L \Delta'$, hence that $\mathrm{Div}(\Delta \wedge_L \Delta')$ generates M.

It is finite since $\mathrm{Div}(\Delta)$ is finite, and $\Delta \wedge_L \Delta' \leq \Delta$. □

Proposition 1.4.5. *Let M be a Garside monoid with Garside element Δ. Let $k \geq 1$. Then Δ^k is a Garside element in M.*

Proof. TBD □

Example 1.4.6. Let $n \geq 1$ and let $M := ((\mathbb{N}_{\geq 0})^n, +)$. Then M is both left- and right-cancellative. We have $a = (a_1, a_2, \ldots, a_n) \leq b = (b_1, b_2, \ldots, b_n)$ if and only if $a_i \leq b_i$ for all $i = 1, \ldots, n$, where $\leq$ denotes either the left- or right-divisibility. In particular, one defines a length function $\lambda : M \longrightarrow \mathbb{Z}_{\geq 0}$ by $\lambda(a) = \sum_{i=1}^{n} a_i$ and we have $\lambda(ab) = \lambda(a) + \lambda(b)$ for all $a, b \in M$. This establishes that $\leq$ is Noetherian. Given $a, b \in M$, the element $a \vee b = (\max\{a_1, b_1\}, \max\{a_2, b_2\}, \ldots, \max\{a_n, b_n\})$ is both a left- and right-lcm of a and b, and $a \wedge b = (\min\{a_1, b_1\}, \min\{a_2, b_2\}, \ldots, \min\{a_n, b_n\})$ is both a left- and right-gcd of a and b. Finally, consider the element $\Delta := (1, 1, \ldots, 1) \in M$. The set of left- or right-divisors of Δ is given by the set of elements of the form $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$, where $\varepsilon_i \in \{0, 1\}$ for all $i = 1, \ldots, n$. It is thus finite, and contains the element e_i with zero entries except the i-th entry equal to 1, for all $i = 1, \ldots, n$, which generates M since $(a_1, a_2, \ldots, a_n) = e_1^{a_1} e_2^{a_2} \cdots e_n^{a_n}$. This shows that M is a Garside monoid, with group of fractions isomorphic to $(\mathbb{Z}^n, +)$.

Example 1.4.7. The monoid $B_3^+ = \langle a, b \mid aba = bab \rangle$ from Proposition 1.1.9 is a Garside monoid. We have seen in Proposition 1.1.9 that M is left- and right-cancellative. It has Noetherian divisibility since

the defining relation is homogeneous. We have seen in Example 1.2.7 that every pair of elements admits a common left- or right-multiple but the existence of lcm and gcd's has not been established yet: we will establish it in the next section. Finally, setting $\Delta := aba = bab$, the set of left- and right-divisors of Δ coincide, and is given by $\mathrm{Div}(\Delta) = \{1, a, b, ab, ba, aba\}$, which is finite and contains the generating set $\{a, b\}$ of M. Hence M is a Garside monoid, and by Corollary 1.2.5 we have $G(M) \cong \langle a, b \mid aba = bab \rangle$.

Proposition 1.4.8. *Let (M, Δ) be a Garside monoid. There is a power of Δ which is central in M (and hence in $G(M)$).*

Proof. Let $x \in \mathrm{Div}(\Delta)$. Then $y := \Delta x^{-1}$ is also in $\mathrm{Div}(\Delta)$. It follows that $\Delta y^{-1} \in \mathrm{Div}(\Delta)$. But $\Delta y^{-1} = \Delta x \Delta^{-1}$. Since $\mathrm{Div}(\Delta)$ is finite, we have $\Delta \mathrm{Div}(\Delta) \Delta^{-1} = \mathrm{Div}(\Delta)$, and there is a power $k \geq$ of Δ such that Δ^k acts by conjugation on $\mathrm{Div}(\Delta)$ as the identity. For such a k we thus have $\Delta^k x = x \Delta^k$ for all $s \in \mathrm{Div}(\Delta)$. Since $\mathrm{Div}(\Delta)$ generates M, we deduce that Δ^k is central in M. □

Proposition 1.4.9. *Every Garside group is torsion-free.*

Proof. We extend the partial order $\leq$ given by left-divisibility on M to $G(M)$ by setting $x \leq y$ if and only if $x^{-1}y \in M$. This yields a lattice order on $G(M)$.

Let $x \in G(M)$ and let $n \geq 1$ such that $x^n = 1$. Consider the element $y := 1 \wedge x \wedge x^2 \wedge \cdots \wedge x^{n-1}$. Then

$$xy = x(1 \wedge x \wedge x^2 \wedge \cdots \wedge x^{n-1}) = x \wedge x^2 \wedge \cdots \wedge x^{n-1} \wedge \underbrace{x^n}_{=1} = y,$$

hence $x = 1$. □

1.5 Word problem and normal forms

The aim of this section is to explain why Garside groups have a solvable word problem.

Throughout the whole section we will denote by (M, Δ) a Garside monoid.

1.5.1 Solution to the word problem: basic approach

Definition 1.5.1. An element s of M is an *atom* if whenever $x, y \in M$ are such that $s = xy$, then $x = 1$ or $y = 1$.

Proposition 1.5.2. *Let (M, Δ) be a Garside monoid. Then M admits the presentation*

$$\langle \underline{u}, u \in \mathrm{Div}(\Delta) \mid \underline{u} \cdot \underline{v} = \underline{w} \text{ if } uv = w \rangle. \tag{1.5.1}$$

Proof. Set $M' := \langle \underline{u}, u \in \mathrm{Div}(\Delta) \mid \underline{u} \cdot \underline{v} = \underline{w} \text{ if } uv = w \rangle$. It is clear that the defining relations of M' are satisfied in M under the map $\underline{u} \mapsto u$. We need to show that every relation in M is a consequence of those relations. Hence let $x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_\ell \in \mathrm{Div}(\Delta)$ such that

$$x_1 x_2 \cdots x_k = y_1 y_2 \cdots y_\ell. \tag{1.5.2}$$

We proceed by induction on $\ell(x_1 x_2 \cdots x_k)$. If $\ell(x_1 x_2 \cdots x_k) = 0$, then both sides of (1.5.2) are the identity. If $\ell(x_1 x_2 \cdots x_k) = 1$, then all factors but one in either side are equal to 1, in which case the result is also trivially true. Hence assume that $\ell(x_1 x_2 \cdots x_k) \geq 2$. Since M is a lattice for left-divisibility, let z be the least right-common multiple of x_1 and y_1. Then z must left-divide $x_1 x_2 \cdots x_k$, since it has a word beginning by x_1 and a word beginning by y_1. We thus have $x_1 x_2 \cdots x_k = zz'$

for some $z' \in M$. Let $a_1, b_1 \in M$ such that $z = x_1 a_1 = y_1 b_1$. Since Δ is a common right-multiple of x_1 and y_1, we must have $z \leq \Delta$, and hence $z, a_1, b_1 \in \mathrm{Div}(\Delta)$. By left-cancellativity we have $x_2 \cdots x_k = a_1 z'$ and $y_2 \cdots y_\ell = b_1 z'$. Now choose any word $u_1 u_2 \cdots u_p$ for z'. By induction, the relations $a_1 u_1 u_2 \cdots u_p = x_2 \cdots x_k$ and $b_1 u_1 u_2 \cdots u_p = y_2 \cdots y_\ell$ are consequences of the defining relations of M'. We can thus pass from $x_1 x_2 \cdots x_k$ to $x_1 a_1 u_1 u_2 \cdots u_p$ only using defining relations of M'. Now the relations $x_1 a_1 = z$ and $z = y_1 b_1$ are defining relations of M'. We can thus pass from $x_1 a_1 u_1 u_2 \cdots u_p$ to $y_1 b_1 u_1 u_2 \cdots u_p$ using defining relations of M'. Finally, as seen above we can pass from $y_1 b_1 u_1 u_2 \cdots u_p$ to $y_1 y_2 \cdots y_\ell$ using defining relations of M'. Hence the words $x_1 x_2 \cdots x_k$ and $y_1 y_2 \cdots y_\ell$ are related by defining relations of M', which concludes the proof. □

Corollary 1.5.3. *Every Garside monoid is finitely presented.*

Lemma 1.5.4. *Every Garside monoid has finitely many atoms.*

Proof. Every atom must be a generator of any presentation. Hence, by the above proposition, we have that the set of atoms is included in the set of divisors of Δ, which is finite. □

Lemma 1.5.5. *The lattice* $\mathrm{Div}(\Delta)$ *(for left- or right-divisibility) can be calculated in finite time.*

Proof. By Noetherian divisibility, the length of a word for Δ, defined as the maximal number of elements of $\mathrm{Div}(\Delta)\backslash\{1\}$ appearing in a word for Δ, is bounded. It follows that there are only finitely-many words for Δ, and these words can all be calculated starting from any word for Δ and applying defining relations whenever it is possible, and then iterating with new obtained words. This gives a finite set of prefixes of Δ, and prefixes representing the same elements can be identified since the graph of expressions of any element can be calculated using exactly the same procedure as the one used above for words for Δ. The poset of left divisors can thus be calculated. □

Theorem 1.5.6 (Solvability of the word problem in a Garside monoid, Brute force method)**.** *The word problem in a Garside group is solvable, that is, there is an algorithm allowing one to determine in finite time if a word in the elements of* $\mathrm{Div}(\Delta) \cup \mathrm{Div}(\Delta)^{-1}$ *represents the identity or not.*

Proof. Let $x, y \in \mathrm{Div}(\Delta)$. Consider the element $x^{-1}y$ of $G(M)$. Take any right-multiple z of x, y in $\mathrm{Div}(\Delta)$ (for instance, one can take $z = \Delta$!). There exist $x', y' \in \mathrm{Div}(\Delta)$ such that $xx' = yy'$. In $G(M)$, we then have $x^{-1}y = x'y'^{-1}$. We can thus "reverse" fractions in two elements of $\mathrm{Div}(\Delta)$. Is follows that any word $x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_k^{\epsilon_k}$, $x_i \in \mathrm{Div}(\Delta)$ and $\epsilon_i \in \{-1, 1\}$ for all $i = 1, \ldots, k$, can be transformed into a word $y_1 y_2 \cdots y_\ell y_{\ell+1}^{-1} \cdots y_k^{-1}$, still representing the same element of $G(M)$, and with $y_i \in \mathrm{Div}(\Delta)$ for all $i = 1, \ldots, k$. Since M embeds into $G(M)$ (by Ore's Theorem 1.2.2), determining whether the word $y_1 y_2 \cdots y_\ell y_{\ell+1}^{-1} \cdots y_k^{-1}$ represents the identity or not amounts to determining whether, in M, we have the equality $y_1 y_2 \cdots y_\ell = y_k y_{k-1} \cdots y_{\ell+1}$. But the number of words in $\mathrm{Div}(\Delta)$ for the element x represented by $y_1 y_2 \cdots y_k$ is finite, as seen in the proof of Lemma 1.5.5. The set of words for a given element can thus be calculated, hence it can be checked in finite time if $y_1 y_2 \cdots y_\ell = y_k \cdots y_{\ell+1}$ by calculating the graph of words for x starting from $y_1 y_2 \cdots y_\ell$, and verifying at the end if $y_k \cdots y_{\ell+1}$ appears in the obtained set of words or not. □

1.5.2 Solution to the word problem: normal forms

Lemma 1.5.7. *Let M be a Garside monoid. Let $g \in G(M)$. There is $m \geq 0$ such that $\Delta^m g \in M$.*

Proof. Recall that the action of Δ by conjugation preserves $\mathrm{Div}(\Delta)$. In other words, for every $x \in \mathrm{Div}(\Delta)$, there is $y \in \mathrm{Div}(\Delta)$ such that $x\Delta = \Delta y$. Let $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$, with $x_i \in \mathrm{Div}(\Delta)$ for all i, and $\varepsilon_i \in \{\pm 1\}$ for all i, be a word representing g. We claim that, taking $m = |\{i \mid \varepsilon_i = -1\}|$, we have $\Delta^m g \in M$. We argue by induction on m. If $m = 0$ then $g = \Delta^0 g \in M$. Assume that $m \geq 1$. Let i_1 be the smallest integer in $\{1, 2, \ldots, k\}$ such that $\varepsilon_i = -1$. Using the above observation, we have $\Delta^{m-1} x_1 x_2 \cdots x_{i_1-1} x_{i_1}^{-1} = y_1 y_2 \cdots y_{i_1-1} y_{i_1}^{-1} \Delta^{m-1}$, where we successively moved the $m-1$ copies of Δ to the right, and the y_i's are still divisors of Δ. We thus have

$$\begin{aligned} \Delta^m x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} &= \Delta y_1 y_2 \cdots y_{i_1-1} y_{i_1}^{-1} \Delta^{m-1} x_{i_1+1}^{\varepsilon_{i_1+1}} \cdots x_k^{\varepsilon_k} \\ &= \underbrace{z_1 z_2 \cdots z_{i_1-1}}_{\in M} \underbrace{\Delta y_{i_1-1}^{-1}}_{\in \mathrm{Div}(\Delta)} \underbrace{\Delta^{m-1} x_{i_1+1}^{\varepsilon_{i_1+1}} \cdots x_k^{\varepsilon_k}}_{\in M \text{ by induction}} \in M, \end{aligned}$$

which concludes the proof. □

Set $M^{-1} := \{x^{-1} \mid x \in M\} \subseteq G(M)$. Exactly the same proof as the one above (swapping the roles of positive and negative exponents) shows that there is $m' \geq 0$ such that $\Delta^{-m'} g \in M^{-1}$. In particular, since $M \cap M^{-1} = \{1\}$ because a Garside monoid has no intertible element distinct from 1, we get the existence of $m' \geq 0$ such that $\Delta^{m'} g \in M^{-1} \backslash \{1\}$ and hence $\Delta^k g \notin M$ for all $k \geq m' \geq 0$. Using this observation together with the lemma above, we conclude that, for all $g \in G(M)$, the set $\{i \in \mathbb{Z} \mid \Delta^i g \in M\}$ has a minimal element, denoted $-m(g)$. We thus have

$$g = \Delta^{m(g)} x,$$

with $x \in M$.

The proof of Lemma 1.5.7 gives an algorithm to write any word in $\mathrm{Div}(\Delta) \cup \mathrm{Div}(\Delta)^{-1}$ in the form $\Delta^{-m} x$ for some $x \in M$. The obtained m is not necessarily minimal, but we still kip this algorithm as first step, and will possibly get rid of superfluous copies of Δ afterwards.

Secondly, we define a normal form of $x \in M$ as follows. If $x \neq 1$, set $x_1 := \gcd(x, \Delta)$ (left-gcd). By cancellativity, there is a uniquely defined $x_1' \in M$ such that $x_1 x_1' = x$. If $y \neq 1$, then set $x_2 := \gcd(x_1', \Delta)$. There is then a uniquely defined $x_2' \in M$ such that $x_1 x_2 x_2' = x$. Iterating yields a normal form $x_1 x_2 \cdots x_k$ for x with all the factors in $\mathrm{Div}(\Delta)$. We call this the *left-greedy normal form* of $x \in M$.

Proposition 1.5.8 ((Charney) Local property of the normal form)**.** *Let $x \in M$ and $x = x_1 x_2 \cdots x_k$ be a decomposition of x as a product of elements of* $\mathrm{Div}(\Delta)$*. Then $x_1 x_2 \cdots x_k$ is the left-greedy normal form of x if and only if, for all $i = 1, \ldots, k-1$, we have* $\gcd(\Delta, x_i x_{i+1}) = x_i$*.*

Proof. For simplicity, given $x \in M$, we write $\alpha(x) := \gcd(x, \Delta)$ (left-gcd). We shall first show that for all $x, y \in M$, we have the (important) equality

$$\alpha(xy) = \alpha(x\alpha(y)). \tag{1.5.3}$$

Let $x = a_1 a_2 \cdots a_k$ be a decomposition of x as a product of simples (all distinct from 1). We proceed by induction on k. If $k = 0$ then we have $x = 1$ hence we simply get $\alpha(y) = \alpha(y)$ which holds true. Hence assume that $k \geq 1$. Since $a_1 \in \mathrm{Div}(\Delta)$, we have $a_1 \leq \alpha(xy)$. Let $u \in M$ such that $xy = \alpha(xy)u$ and $b \in \mathrm{Div}(\Delta)$ such that $\alpha(xy) = a_1 b$. We have

$$a_1 a_2 \cdots a_k y = \alpha(xy) u = a_1 b u$$

from what, by left-cancellativity, letting $x' := a_2 \cdots a_k$, we deduce that $x'y = a_2 \cdots a_k y = bu$. By induction we have that $\alpha(x'y) = \alpha(x'\alpha(y))$, hence $b \leq x'\alpha(y)$, hence

$$\alpha(xy) = a_1 b_1 \leq a_1 x' \alpha(y) = x\alpha(y),$$

yielding $\alpha(xy) \leq \alpha(x\alpha(y))$.

Since $xy = x\alpha(y)z$ for some $z \in M$, it is clear that $\alpha(x\alpha(y)) \leq \alpha(xy)$. This establishes (1.5.3).

We now prove the stated equivalence. Assume that $x = x_1 x_2 \cdots x_k$ is the left-greedy normal form of x. We have

$$x_i = \gcd(x_i x_{i+1} \cdots x_k, \Delta) = \alpha(x_i x_{i+1} \cdots x_k) \underbrace{=}_{(1.5.3)} \alpha(x_i \alpha(x_{i+1} \cdots x_k)) = \alpha(x_i x_{i+1}) = \gcd(x_i x_{i+1}, \Delta).$$

Conversely, assume that $x = x_1 x_2 \cdots x_k$ is a decomposition of x where all factors are nontrivial simple elements, and assume that $\gcd(x_i x_{i+1}, \Delta) = x_i$ for all $i = 1, 2, \ldots, k-1$. We show that $\alpha(x_i x_{i+1} \cdots x_k) = x_i$ by decreasing induction on i. We have $\alpha(x_k) = x_k$ and $\alpha(x_{k-1}x_k) = \gcd(x_{k-1}x_k, \Delta) = x_{k-1}$. Now assume that $i < k-1$. We have

$$\alpha(x_i x_{i+1} \cdots x_k) \underbrace{=}_{(1.5.3)} \alpha(x_i \alpha(x_{i+1} \cdots x_k)) = \alpha(x_i x_{i+1}) = \gcd(x_i x_{i+1}, \Delta) = x_i,$$

which concludes the proof. □

How to calculate the left-greedy normal form of an element of M

- **Step 1**: write $g \in G(M)$ in the form $\Delta^m x$ where $m \leq 0$ and $x \in M$: the algorithm is given in the proof of Lemma 1.5.7. Note that the obtained m is not necessarily $m(g)$.
- **Step 2**: calculate the left-greedy normal form of $x \in M$. Thanks to the equality (1.5.3), it is enough to be able to calculate $\alpha(xy)$ for $x, y \in \mathrm{Div}(\Delta)$. Indeed, given $x \in M$ and a decomposition $x = x_1 x_2 \cdots x_k$ into a product of simples, we wish to calculate $\alpha(x)$. By repeated applications of (1.5.3) we have

  $$\alpha(x_1 x_2 \cdots x_k) = \alpha(x_1 \alpha(x_2 \alpha(x_3 \alpha(\cdots \alpha(x_{k-2}\alpha(x_{k-1}\alpha(x_k))) \cdots))))$$

  and $\alpha(x_k) = x_k$. Thus we need to calculate $y := \alpha(x_{k-1}x_k) \in \mathrm{Div}(\Delta)$, then we need to calculate $\alpha(x_{k-2}y) \in \mathrm{Div}(\Delta)$, etc., and at each step we need to perform a calculation of the form $\alpha(uv)$ with $u, v \in \mathrm{Div}(\Delta)$.

  Lemma 1.5.9. *Let $x, y \in \mathrm{Div}(\Delta)$. Let $\overline{x} := x^{-1}\Delta \in \mathrm{Div}(\Delta)$. Let $z := \gcd(\overline{x}, y)$. Then $\alpha(xy) = xz$.*

  Proof. We have $x\overline{x} = \Delta$ and $z \leq \overline{x}$, hence $xz \in \mathrm{Div}(\Delta)$. Moreover, since $z \leq y$, we have $xz \leq xy$, hence $xz \leq \alpha(xy)$. Hence there is $z' \in \mathrm{Div}(\Delta)$ such that $xzz' = \alpha(xy)$. It follows that $zz' \in \mathrm{Div}(\Delta)$, and by cancellativity, $zz' \leq y$, forcing $z' = 1$ since $z = \gcd(y, \Delta)$. Hence $\alpha(xy) = xz$. □

  This allows one to calculate $\alpha(x)$. On then calculates $x' := \alpha(x)^{-1}x$, and goes on calculating $\alpha(x')$, and so on.

Definition 1.5.10. Let $x, y \in \mathrm{Div}(\Delta)$. We say that the product $x \cdot y$ is *left-weighted* if $\alpha(xy) = x$.

Remark 1.5.11. The above algorithm to calculate the left-greedy normal form can be optimized. Namely, given any decomposition $x = x_1 x_2 \cdots x_k$ as a product of simples, one can show that the following algorithm gives the left-greedy normal form: take any two successive pairs of factors, and make it left-weighted. If the second factor becomes trivial, remove it. Repeat until the process terminates.

- **Step 3**: With Steps 1 and 2, we can write any $g \in G(M)$ in the form $\Delta^m x_1 x_2 \cdots x_k$ for some $m \geq 0$ and $x \in M$, with x having a left-greedy normal form $x_1 x_2 \cdots x_k$. The exponent m may not be equal to $m(g)$. But powers of Δ may be cancelled by first factors of the left-greedy normal form equal to Δ. Namely, let i be the smallest positive integer such that $x_i \neq \Delta$. Then $g = \Delta^m x_1 x_2 \cdots x_k = \Delta^{m+i-1} x_i x_{i+1} \cdots x_k$. We then have $m - i + 1 = m(g)$, and $x_i x_{i+1} \cdots x_k$ is still in left-greedy normal form. Indeed, we then have $\Delta^{-m+i-1} g = x_i x_{i+1} \cdots x_k$, and if the exponent $-m + i - 1$ was not minimal, this would mean that $\Delta \leq x_i x_{i+1} \cdots x_k$, hence that $x_i = \gcd(\Delta, x_i x_{i+1} \cdots x_k) = \Delta$, contradicting $x_i \neq \Delta$.

We thus have another solution to the word problem:

Theorem 1.5.12 (Solution to the word problem in a Garside group using normal forms)**.** *Let M be a Garside monoid. Any $g \in G(M)$ can be written uniquely in the form $\Delta^m x_1 x_2 \cdots x_k$, where $m \in \mathbb{Z}$, $x_i \in \mathrm{Div}(\Delta) \backslash \{\Delta, 1\}$ and satisfy $\alpha(x_i x_{i+1}) = x_i$ for all $i = 1, \ldots, k-1$ (i.e., $x_1 x_2 \cdots x_k$ is not a right-multiple of Δ, and is a left-greedy normal form).*

It can be shown that this solution is much more efficient from an algorithmical point of view than the one given in Theorem 1.5.6; moreover, it yields a normal form for every element in $G(M)$, which is not the case with the aforementioned solution.

1.6 Criteria

Definition 1.6.1. Let $\langle\, \mathcal{S} \mid \mathcal{R} \,\rangle$ be a presentation of a monoid M. We say that the presentation $\langle\, \mathcal{S} \mid \mathcal{R} \,\rangle$ is *right-complemented* if in $\mathcal{R}$

- there is no relation of the form $u = 1$ for u a nonmepty word in $\mathcal{S}^*$,
- there is no relation of the form $sa = sb$ with $s \in \mathcal{S}$ and at least one word among a and b is nonempty,
- for $s, t \in \mathcal{S}$ with $s \neq t$, there is at most one relation of the form $s \cdots = t \cdots$. One similarly defines *left-complemented* presentations.

Example 1.6.2.

1. The presentation $\langle\, a, b \mid aba = bab \,\rangle$ of the monoid B_3^+ is both left- and right-complemented.
2. More generally, let $n \geq 2$ and consider the *positive braid monoid*

$$B_n^+ = \left\langle\, \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{c} \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \text{ for } 1 \leq i < n-1, \\ \sigma_i \sigma_j = \sigma_j \sigma_i \text{ for } |i-j| > 1. \end{array} \right\rangle. \tag{1.6.1}$$

The presentation above if both left- and right-complemented.

Given a right-complemented presentation, one can define a partial map $\theta : \mathcal{S}^2 \longrightarrow \mathcal{S}^*$ by setting $\theta(s,s) = 1$ for all $s \in \mathcal{S}$, $\theta(s,t) = a$ whenever $s \neq t$ and there is a relation of the form $sa = tb$ in $\mathcal{R}$, and $\theta(s,t) = \emptyset$ whenever $s \neq t$ and there is no relation of the form $s\cdots = t\cdots$ in $\mathcal{R}$. This partial map is the *syntactic right-complement* associated with the right-complemented presentation $\langle\, \mathcal{S} \mid \mathcal{R}\rangle$.

One can show the following (see [5, Lemma II.4.6]):

Lemma 1.6.3. *Let $\langle \mathcal{S} \mid \mathcal{R}\rangle$ be a right-complemented presentation with syntactic right-complement θ. There exists a unique (minimal) extension of θ to a partial map still denoted $\theta : (\mathcal{S}^*)^2 \longrightarrow \mathcal{S}^*$ such that*

$$\theta(s,s) = 1 \ \forall s \in \mathcal{S}, \tag{1.6.2}$$
$$\theta(bc,a) = \theta(c,\theta(b,a)) \ \forall a,b,c \in \mathcal{S}^*, \tag{1.6.3}$$
$$\theta(a,bc) = \theta(a,b)\theta(\theta(b,a),c) \ \forall a,b,c \in \mathcal{S}^*, \tag{1.6.4}$$
$$\theta(1,a) = a \ \forall a \in \mathcal{S}^*, \tag{1.6.5}$$
$$\theta(a,1) = 1 \ \forall a \in \mathcal{S}^*. \tag{1.6.6}$$

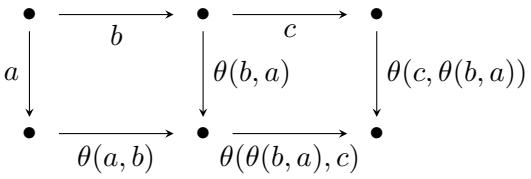

Figure 1.1: Commutative diagram illustrating the relations $\theta(bc,a) = \theta(c,\theta(b,a))$ and $\theta(a,bc) = \theta(a,b)\theta(\theta(b,a),c)$. Arrows represent elements of the monoid and composition of arrows corresponds to the product in M^{op}.

Definition 1.6.4. Let $\langle\, \mathcal{S} \mid \mathcal{R}\rangle$ be a right-complemented presentation of a monoid M with syntactic right-complement θ. We say that $\langle\, \mathcal{S} \mid \mathcal{R}\rangle$ satisfies the *θ-cube condition* holds for the triple $(a,b,c) \in \mathcal{S}^*$ if $\theta(\theta(a,b),\theta(a,c))$ and $\theta(\theta(b,a),\theta(b,c))$ exist and define words in $\mathcal{S}^*$ that are equivalent under $\mathcal{R}$ (if the two words are *equal*, we say that the *sharp* θ-cube condition holds).

Definition 1.6.5 (Conditional lcm)**.** We say that a left-cancellative (respectively right-cancellative) monoid M with no nontrivial invertible element *admits conditional right-lcms* (resp. *admits conditional left-lcms*) if any two elements of M that admit a common right-multiple (resp. left-multiple) admit a common right-lcm (resp. left-lcm).

The following proposition is useful to show that a monoid presentation defines a left-cancellative monoid:

Proposition 1.6.6 (see [5, Proposition II.4.16])**.** *If $\langle \mathcal{S}, \mathcal{R}\rangle$ is a right-complemented presentation of a monoid M with syntactic right-complement θ, and if M is right-Noetherian and the θ-cube condition holds for every triple of pairwise distinct elements of $\mathcal{S}$, then M is left-cancellative, and admits conditional right-lcms. More precisely, u and v admit a common right-multiple if and only if $\theta(u,v)$ exists and, then, $u\theta(u,v) = v\theta(v,u)$ represents the right-lcm of these elements.*

We also have the following:

Lemma 1.6.7 (see [5, Lemma II.2.22]). *If M is cancellative and admits conditional right-lcms (respectively left-lcms), then any two elements of M that admit a common left-multiple (resp. right-multiple) admit a right-gcd (resp. left-gcd).*

Proof. Let $a, b \in M$ admitting a common left-multiple, that is, let $a', b' \in M$ such that $a'a = b'b$. The elements a' and b' then admit a common right-multiple, hence they admit a right-lcm, say $a'u = b'v = c$, and c is a left-divisor of $a'a = b'b$. It follows that there is $d \in M$ such that $ud = a, vd = b$, hence d is a common right-divisor of a and b.

Now let d' be a common right-divisor of a and b. There are thus $a_1, b_1 \in M$ such that $a_1 d' = a$, $b_1 d' = b$. then $a'a_1 d' = a'a = b'b = b'b_1 d'$ hence $a'a_1 = b'b_1$. Hence $a'a_1$ is a common right-multiple of a' and b', hence a right-multiple of their right lcm, given by c. Hence there is $h' \in M$ satisfying $a'a_1 = ch' = a'uh'$, hence $a_1 = uh'$. We then obtain

$$ud = a = a_1 d' = uh'd'$$

implying that d' is a right-divisor of d. This shows that d is the right-gcd of a and b. □

Example 1.6.8. Let $B_3^+ = \langle\, a, b \mid aba = bab \,\rangle$. The presentation is right-complemented, with syntactic right-complement θ defined on pairs of distinct atoms by $\theta(a, b) = ba$, $\theta(b, a) = ab$. The sharp θ-cube condition is vacuously true, hence we obtain another proof that B_3^+ is left-cancellative. Moreover, we have already seen that B_3^+ is an Ore monoid, hence that every pair of distinct elements admits a common right-multiple. If follows that we have right-lcms in B_3^+, and since the presentation is symmetric we also have left-lcms. By the lemma above we thus also have left- and right-gcds. Proposition 1.6.6 is particularly useful to calculate the lcm of pairs of elements. Note that $\theta(a, b) = ba$ and $\theta(b, a) = ab$. For instance, we have

$$\theta(a^3, b) = \theta(a, \theta(a^2, b))$$

We then have

$$\theta(a^2, b) = \theta(a, \theta(a, b)) = \theta(a, ba) = \theta(a, b)\theta(\theta(b, a), a) = ba\theta(ab, a) = ba\theta(b, 1) = ba,$$

hence $\theta(a^2, b) = \theta(a, ba) = ba$. We thus have

$$\theta(a^3, b) = \theta(a, ba) = ba.$$

1.7 Examples

Exercise 1.7.1. Explain why the free group F_2 on two generators is not a Garside group. Show that $F_2 \times \mathbb{Z}$ is a Garside group.

Example 1.7.2. Consider the monoid $B(I_2(m))^*$, where $m \geq 2$, with m generators $x_1, x_2, \ldots, x_m$ satisfying the relations

$$x_1x_2 = x_2x_3 = \cdots = x_ix_{i+1} = \cdots = x_{m-1}x_m = x_mx_1.$$

We claim that it is a Garside monoid, with Garside element $\Delta = x_1x_2$. Since the defining relations are homogeneous, it has Noetherian divisibility. The above relation shows that the set of left- and right-divisors of Δ coincide, and are given by all the x_i's, 1, and Δ. The above presentation is right-complemented and up to reordering the indices, it is symmetric, hence it suffices to show that the

monoid is left-cancellative to obtain right-cancellativity for free. Hence let i, j, k be pairwise distinct integers in $\{1, 2, \dots, m\}$. Considering indices modulo m, we have

$$\theta(\theta(x_i, x_j), \theta(x_i, x_k)) = \theta(x_{i+1}, x_{i+1}) = 1 = \theta(x_{j+1}, x_{j+1}) = \theta(\theta(x_j, x_i), \theta(x_j, x_k)),$$

hence the sharp θ-cube condition holds true. It follows that the monoid is left-cancellative, and admits conditional right-lcms. But Δ acts on the x_i's via $\Delta x_i \Delta^{-1} = x_{i-2}$, hence every word in the x_i's with k elements is a left divisor of Δ^k. This shows that any pair of elements have a common right multiple, hence right-lcms exist. Since everything is symmetric we also get the existence of left-lcms, and of right- and left-gcds thanks to Lemma 1.6.7.

Exercise 1.7.3. Let $n, m \geq 2$. Consider the monoid

$$M = \langle\, x_1, x_2, \dots, x_n \mid x_1 x_2 \cdots x_m = x_2 x_3 \cdots x_m x_1 = \cdots = x_m x_1 x_2 \cdots x_{m-1} \,\rangle,$$

where the indices are taken modulo n if necessary. Show that M is a Garside monoid. (When n and m are coprime, the corresponding Garside group $G(M)$ is the knot group of the (n, m)-torus knot).

Example 1.7.4. Consider the monoid $M = \langle\, a, b \mid aba = b^2 \,\rangle$. The assignment $\lambda(a) = 1$, $\lambda(b) = 2$ extends to a function $\lambda : M \longrightarrow \mathbb{Z}_{\geq 0}$ such that $\lambda(xy) = \lambda(x) + \lambda(y)$ for all $x, y \in M$, hence M has Noetherian divisibility. The above presentation is right-complemented, and the sharp θ-cube condition is vacuously true. It is thus left- and right-cancellative, and admits conditional left- and right-lcms. The element $\Delta = b^3$ is a Garside element in b^3: its set of left- (or right-)divisors is given by $\{1, a, b, ab, b^2, ba, bab, b^3\}$. Every element which can be written as a product of k atoms is a left- and right-divisor of Δ. Note that Δ is central here. It follows that every par of elements admits a common left-multiple and a common right-multiple, hence that we have left- and right-lcms, and also left- and right-gcds.

Example 1.7.5. Consider the monoid $M = \langle\, a, b, c \mid acb = c^2, aca = bc \,\rangle$. We claim that M is a Garside monoid. First, setting $\lambda(a) = 1$, $\lambda(b) = 2$, $\lambda(c) = 3$, we get that the relations are homogeneous, hence that M has Noetherian divisibility. The presentation above is right-complemented. The problem here is that, working with this presentation, we see that the sharp θ-cube condition does not hold: indeed, we have $\theta(\theta(a, b), \theta(a, c)) = \theta(ca, cb) = \theta(a, b) = ca$, while $\theta(\theta(b, a), \theta(b, c))$ is not defined since $\theta(b, c)$ is not defined. We are typically in a situation where we must artificially enlarge the set of relations to be able to successfully check the θ-cube condition. Here we have no relation of the form $b \cdots = c \cdots$. Note that in M, we have

$$bcca = acaca = acbc = c^3,$$

hence we replace the above presentation by

$$M = \langle\, a, b, c \mid acb = c^2, aca = bc, bcca = c^3 \,\rangle.$$

We now check the θ-cube condition. We have

- $\theta(\theta(a, b), \theta(a, c)) = \theta(ca, cb) = \theta(a, b) = ca$,
- $\theta(\theta(b, a), \theta(b, c)) = \theta(c, cca) = \theta(1, ca) = ca$,
- $\theta(\theta(b, c), \theta(b, a)) = \theta(cca, c) = \theta(ca, 1) = 1$,
- $\theta(\theta(c, b), \theta(c, a)) = \theta(c^2, c) = \theta(c, 1) = 1$,

- $\theta(\theta(c,a),\theta(c,b)) = \theta(c,c^2) = \theta(1,c) = c$,
- $\theta(\theta(a,c),\theta(a,b)) = \theta(cb,ca) = \theta(b,a) = c$.

It follows that the sharp θ-cube condition holds, hence that M is left-cancellative, and admits conditional right-lcms. Note that the above presentations of M are not symmetric, hence we cannot deduce right-cancellativity without further effort. The enlarged presentation that we used to show left-cancellativity is unfortunately not left-complemented. Note that, in M, we have

$$acaca = acbc = c^3 = cacb,$$

hence we have

$$M = \langle\ a,b,c \mid acb = c^2, aca = bc, bcca = c^3, acaca = cacb\ \rangle. \tag{1.7.1}$$

The above presentation is now left-complemented, and can be used to check the sharp θ-cube condition, which we leave as an exercice. The monoid M is thus right-cancellative, and admits conditional left-lcms.

Consider the element $\Delta = c^4$. We claim that Δ is central in M. To show it, it suffices to show that $x\Delta = \Delta x$ for every $x \in \{a,b,c\}$. For c this is trivial and we have

$$ac^4 = acacbc = acacaca = acbcca = c^4a,$$

$$bc^4 = bc^2acb = c^4b.$$

The element c^4 is thus central, hence its set of left- and right-divisors coincide since if $\Delta = xy$, we have $\Delta = yx$ by cancellativity. Moreover, the defining relations show that every atoms left-divides Δ, hence it is a Garside element in M. Existence of common multiples (and hence lcms, and then gcds) then follow arguing as in the previous examples.

Exercise 1.7.6. Check that the monoid M from Example 1.7.5 is right-cancellative by checking the sharp θ-cube condition for the presentation (1.7.1). Identifify the left- and right-lcm of the set $\mathcal{S} = \{a,b,c\}$ of atoms.

In general it might be difficult to identify a Garside element and check that it satisfies the required properties. In the following chapter, we develop a method to "lift" an element of a quotient group of a candidate to be a Garside group with special properties.

Chapter 2

Interval groups

2.1 Balanced elements

Let G be a group and $A \subseteq G$ a family of elements such that $1 \notin A$ and A generates G as a monoid. For every $a \in A$, let $n_a \in \mathbb{Z}_{\geq 1}$ Consider the length function ℓ_A on G attached to this set of generators A and to the set of weights $(n_a)_{a \in A}$, that is, given $g \in G$ the integer $\ell_A(g)$ is defined by

$$\ell_A(g) = \min \left\{ \sum_{i=1}^{k} n_{a_i} \;\middle|\; g = a_1 a_2 \cdots a_k,\ a_i \in A \right\}.$$

If $n_a = 1$ for all $a \in A$, this is simply the length of g with respect to the generating set A (note that we abuse notation and omit the dependency on $(n_a)_{a \in A}$ to avoid too heavy notation). Define a partial order $\leq_A$ on G by

$$u \leq_A v \;\Leftrightarrow\; \ell_A(u) + \ell_A(u^{-1}v) = \ell_A(v).$$

In other word, we have $u \leq_A v$ if there is a word of shortest possible length for v (also called an A-reduced expression of v) which has an A-reduced expression of u as prefix. Similarly, one can define a partial order $\leq_{A,R}$ by

$$u \leq_A v \;\Leftrightarrow\; \ell_A(u) + \ell_A(vu^{-1}) = \ell_A(v).$$

Definition 2.1.1. Let G, A be as above. We say that an element $c \in G$ is *balanced* if

$$\{g \in G \mid g \leq_A c\} = \{g \in G \mid g \leq_{A,R} c\}.$$

We then denote by P_c the above set.

Example 2.1.2. If G is commutative, then any element $g \in G$ is balanced.

Example 2.1.3. More generally, if A is stable by conjugation in G, that is, if $gAg`-1 = A$ for all $g \in A$, then the partial orders $\leq_A$ and $\leq_{A,R}$ coincide, hence every element of G is balanced.

Example 2.1.4. Consider the symmetric group $G = \mathfrak{S}_3$, and take for A the set $S = \{(1,2),(2,3)\}$ of simple transpositions of G. The posets $(G, \leq_A)$ and $(G, \leq_{A,R})$ are given in the pictures below. The set of balanced elements of G is given by $\{1, s_1, s_2, s_1 s_2 s_1\}$.

2.2 Monoid attached to a balanced element

Let G, A be as in the previous section, and let $c \in G$ a balanced element. We define a monoid $M(P_c)$ generated by a copy $\{\underline{u} \mid u \in P_c\}$ of P_c by

$$M(P_c) = \langle \underline{u}, u \in P_c \mid \underline{u} \cdot \underline{v} = \underline{w} \text{ if } u, v, w \in P_c,\ uv = w \text{ and } u \leq_A w \}.$$

Note that the map $\varphi_c : M(P_c) \longrightarrow G$, $\underline{u} \mapsto u$ is a morphism of monoids. It follows that the subset $\mathbf{P_c} = \{\underline{u} \mid u \in P_c\} \subseteq M(P_c)$ is in one-to-one correspondence with P_c.

Lemma 2.2.1 (Cancellativity with rest in $\mathbf{P_c}$)**.** *Let $u, v \in P_c$ and $a \in M(P_c)$. Then*

$$(\underline{u}a = \underline{v}a \ \Rightarrow\ \underline{u} = \underline{v}) \quad \text{and} \quad (a\underline{u} = a\underline{v} \ \Rightarrow\ \underline{u} = \underline{v}).$$

Proof. It suffices to take the images of the equalities in G via the morphism $\varphi_c : M(P_c) \to G$, and then cancel the images of a. □

Lemma 2.2.2 (Extension of the length function ℓ_A to $M(P_c)$ and Noetherian divisibility)**.** *The length function ℓ_A on G extends to a length function ℓ on $M(P_c)$ via*

$$\ell(\underline{u_1} \cdot \underline{u_2} \cdot \cdots \cdot \underline{u_k}) = \sum_{i=1}^{k} \ell_A(u_i).$$

In particular, the monoid $M(P_c)$ has Noetherian divisibility.

Proof. This is immediate, as the defining relations of $M(P_c)$ are homogeneous with respect to the length function ℓ induced by ℓ_A on generators. □

Lemma 2.2.3. *1. Let $a \in M(P_c)$. Assume that $\ell(a) = \ell(\varphi_c(a))$ and $\varphi_c(a) \in P_c$. Then $a = \underline{\varphi_c(a)}$, i.e., $a \in \mathbf{P_c}$.*

2. If $a \in \mathbf{P_c}$ and b is a left- or right-divisor of a, then $b \in \mathbf{P_c}$.

Proof. First note that, for all $x \in M(P_c)$, we have $\ell_A(\varphi_c(x)) \leq \ell(x)$. It follows that, if $\ell(a) = \ell_A(\varphi_c(a))$, then for any divisor x of a, we also have $\ell(x) = \ell_A(\varphi_c(x))$.

For the first point, we argue by induction on $\ell(a)$. If $\ell(a) = 0$ then a is equal to 1 and the result is trivial. Hence assume that $\ell(a) > 1$. Consider a decomposition $a = bs$, where s is an atom (that is, a nontrivial element of $M(P_c)$ which cannot be written as a product of two nontrivial elements – such an element necessarily lies in $\mathbf{P_c}$). By the above observation we have $\ell(b) = \ell_A(\varphi_c(b))$, and $\varphi_c(b) \leq_A \varphi_c(a)$. Since $\varphi_c(a) \in P_c$, we have $\varphi_c(b) \in P_c$ as well, hence by induction we have $b = \underline{\varphi_c(b)}$. Now since $\varphi_c(a) = \varphi_c(b)\varphi_c(s)$ and $\ell_A(\varphi_c(a)) = \ell_A(\varphi_c(b)) + \ell_A(\varphi_c(s))$, we have that $\underline{\varphi_c(a)} = \underline{\varphi_c(b)} \cdot \underline{\varphi_c(s)}$ is a defining relation of $M(P_c)$, from what we derive that

$$a = bc = \underline{\varphi_c(b)} \cdot \underline{\varphi_c(s)} = \underline{\varphi_c(a)},$$

which concludes the proof of the first point.

Let us show the second point. For any decomposition $a = xy$, we have $\ell_A(\varphi_c(x)) = \ell(x)$ and $\ell_A(\varphi_c(y)) = \ell(y)$ by the observation made ad the beginning of the proof, and hence

$$\ell_A(\varphi_c(a)) = \ell(a) = \ell(xy) = \ell(x) + \ell(y) = \ell_A(\varphi_c(x)) + \ell_A(\varphi_c(y)),$$

from what since $\varphi_c(a) = \varphi_c(x)\varphi_c(y)$ we deduce that $\varphi_c(x), \varphi_c(y) \in P_c$. We conclude using the first point. □

Proposition 2.2.4 (Lifting the poset $(P_c, \leq)$)**.** *The bijection $P_c \longrightarrow \mathbf{P_c}$, $u \mapsto \underline{u}$ induces an isomorphism of posets between $(P_c, \leq_A)$ and $(\mathbf{P_c}, \leq)$.*

Proof. If $u \leq_A v$, then $w := u^{-1}v$ satisfies $\ell_A(u) + \ell_A(w) = \ell_A(v)$, hence w lies in P_c and we have a defining relation $\underline{u} \cdot \underline{w} = \underline{v}$ of $M(P_c)$; in particular, we have $\underline{u} \leq \underline{v}$.

Conversely, assume that $u, v \in P_c$ are such that $\underline{u} \leq \underline{v}$. Then there is $a \in M(P_c)$ such that $\underline{u}a = \underline{v}$. By Lemma 2.2.3, we have $a \in \mathbf{P}_c$, hence $a = \underline{w}$ for some $w \in P_c$. We thus have $\ell(x) = \ell(\varphi_c(x))$ for every $x \in \{\underline{u}, \underline{v}, \underline{w}\}$, and since $\ell(\underline{v}) = \ell(\underline{u}) + \ell(\underline{w})$ we deduce that $\ell_A(u) + \ell_A(w) = \ell_A(v)$, hence that $u \leq_A v$. □

Proposition 2.2.5. *We have*

1. *$(P_c, \leq_A)$ is a lattice if and only if $(P_c, \leq_{A,R})$ is a lattice,*
2. *If $(P_c, \leq_A)$ (and hence also $(P_c, \leq_{A,R})$) is a lattice, assume that $X \subseteq M(P_c)$ is a subset such that*
   (a) *The length function ℓ is bounded on X, that is, there is $M > 0$ such that $\ell(x) \leq M$ for all $x \in X$.*
   (b) *for all $x \in X$, every left-divisor of x also lies in X,*
   (c) *for every pair s, t of atoms of $M(P_c)$ and every $x \in X$ such that $xs, xt \in X$, we have $xz \in X$, where z is the unique element of $\mathbf{P_c}$ such that $\varphi_c(z)$ is the right lcm of $\varphi_c(s)$ and $\varphi_c(t)$.*

   Then there is $y \in M(P_c)$ such that $X = \{a \in M(P_c) \mid a \leq y\}$.

Proof. The first point follows from the observation that, for $x, y \in P_c$, we have $x \leq_A y$ if and only if $\overline{y} \leq_{A,R} \overline{x}$, where $\overline{x} = x^{-1}c$, $\overline{y} = y^{-1}c$.

For the second point, let $y \in X$ be an element of maximal length in X. Assume for contradiction that there is an element of X which is not a left-divisor of y. We can thus find $x \in X$ and s an atom of $M(P_c)$ such that $x \leq y$ but $xs \not\leq y$, $xs \in X$. Choose such an x of maximal length. Since y has maximal length among elements in X, we have $\ell(x) < \ell(y)$. In particular, we have $x < y$, hence there is an atom t such that $xt \leq y$. We have $xs, xt \in X$, hence by assumption we have $xz \in X$, where z is the lift in $\mathbf{P_c}$ of the right-lcm of $\varphi_c(s)$ and $\varphi_c(t)$ in P_c. Note that, since xz is a right-multiple of xs which does not left-divide y, it cannot be a left-divisor of y. But xt left-divides y, hence we can find $u \in [xt, xz]$ and s' an atom such that $us' \in [xt, xz]$, $u \leq y$, $us' \not\leq y$. We have $us' \in X$, $us' \not\leq y$, and $\ell(x) < \ell(us')$, contradicting the choice of x as being maximal in X and not dividing y. □

Corollary 2.2.6. *Assume that $(P_c, \leq_A)$ is a lattice. Let $x, y \in \mathbf{P_c}$. There is a unique $z \in \mathbf{P_c}$ such that $z \leq y$ and $xz \in \mathbf{P_c}$, and such that z is maximal with respect to $\leq$ for these properties.*

Proof. This is obtained by applying point (2) of Proposition 2.2.5 to the set X of elements $u \in M(P_c)$ such that $u \leq y$ and $xu \in \mathbf{P_c}$. The length function is bounded on X since $X \subseteq \mathbf{P_c}$ and $\ell(x) \leq \ell(c)$ for all $x \in P_c$. Hence condition (a) is fulfilled. If $u \in X$ and $v \leq u$, then $v \leq y$ and $xv \leq xu$, hence by point (2) of Lemma 2.2.3 we have $xv \in \mathbf{P}_c$. This yields condition (b). Condition (c) follows from the lattice property of $(P_c, \leq)$ and the isomorphism of posets $(P_c, \leq_A) \cong (\mathbf{P_c}, \leq)$: if s, t are atoms such that u, us, ut all lie in X, then $u, us, ut \leq y$ and $us, ut \in \mathbf{P_c}$. By cancellativity with rest in $\mathbf{P_c}$ (Lemma 2.2.1), we thus have that $u, us, ut \leq \overline{x}$, where $\overline{x}$ is the unique element of $\mathbf{P}_c$ such that $x\overline{x} = \underline{c}$. Writing $\overline{x} = uu'$, we obtain that $s, t \leq u'$. We thus obtain (see Proposition 2.2.4) that $\varphi_c(s), \varphi_c(t) \leq_A \varphi_c(u')$, hence $v \leq \varphi_c(u')$, where v is the right-lcm of $\varphi_c(s)$, $\varphi_c(t)$. We thus have $\underline{v} \leq u'$ again by Proposition 2.2.4, hence $u\underline{v} \leq uu' = \overline{x}$, which yields $u\underline{v} \in \mathbf{P_c}$ since divisors of elements of $\mathbf{P}_c$

are again in $\mathbf{P_c}$. But since $us, ut \leq y$, writing $y = uy'$ we have $s, t \leq y'$, from what we deduce that $\underline{v} \leq y'$. We thus have $u\underline{v} \leq uy' = y$, hence $u\underline{v} \in X$. □

Assume that $(P_c, \leq_A)$ is a lattice. We define two applications

$$\alpha_2, \omega_2 : \mathbf{P_c} \times \mathbf{P_c} \longrightarrow \mathbf{P_c}$$

as follows: we set $\alpha_2(x, y) = xz$, where z is as in Corollary 2.2.6. Since $z \leq y$, there is $a \in \mathbf{P_c}$ such that $za = y$. By cancellativity with rest in $\mathbf{P_c}$ (Lemma 2.2.1), the element a is well-defined. We set $\omega_2(x, y) = a$. Note that

$$xy = \alpha_2(x, y)\omega_2(x, y).$$

The aim now is to extend α_2, ω_2 into two applications

$$\alpha : M(P_c) \longrightarrow \mathbf{P_c},\ \omega : M(P_c) \longrightarrow M(P_c),$$

in such a way that, for $x, y \in \mathbf{P_c}$, we have $\alpha(xy) = \alpha_2(x, y)$ and $\omega(xy) = \omega_2(x, y)$. Roughly speaking, the element $\alpha(x)$ will be the greatest left-divisor of x lying in $\mathbf{P_c}$, and $\omega(x, y)$ will be the unique element in $M(P_c)$ such that $x = \alpha(x)\omega(x)$. It is not clear that $\alpha(x)$ is well-defined at this stage, and the same can be observed for $\omega(x, y)$: at this stage we only have cancellativity when the rest is in $\mathbf{P}_c$.

Lemma 2.2.7. *We begin by showing that, if $a, b, x, ab \in \mathbf{P_c}$, then*

1. $\alpha_2(ab, x) = \alpha_2(a, \alpha_2(b, x))$,
2. $\omega(ab, x) = \omega_2(a, \alpha_2(b, x))\omega_2(b, x)$.

Proof. We show 1. By definition of α_2, we have that $\alpha_2(ab, x) = abu$, where u is maximal such that $u \leq x$ and $abu \in \mathbf{P_c}$. In the same way $\alpha_2(b, x) = bv$, where v is maximal such that $v \leq x$ and $bv \in \mathbf{P_c}$. Since $u \leq x$ and $bu \in \mathbf{P_c}$, by maximality of v we have $u \leq v$, hence $bu \leq bv = \alpha_2(b, x)$. We thus have $abu \leq a\alpha_2(b, x)$, hence $abu \leq \alpha_2(a, \alpha_2(b, x))$. Hence there is $w \in \mathbf{P_c}$ such that $abuw = \alpha_2(a, \alpha_2(b, x))$. But since $\alpha_2(b, x) = bv$, we deduce that $abuw \leq abv$, hence by cancellativity with rest in $\mathbf{P_c}$ we obtain that $uw \leq v \leq x$. Since $uw \in \mathbf{P_c}$ we must have $w = 1$, otherwise it contradicts the maximality of u. We thus have

$$\alpha_2(a, \alpha_2(b, x)) = abu = \alpha_2(ab, x),$$

which concludes the proof of the first point.

We now show the second point. By the first point and the definition of ω_2, multiplying both sides of the equality in point (2) by $\alpha_2(ab, c)$ on the left yields abx. To conclude the proof, by cancellativity with rest in $\mathbf{P_c}$ it suffices to show that the right hand side of (2) is in $\mathbf{P_c}$. We have $\alpha_2(b, x) = bv$ with $v \in \mathbf{P_c}$, and $x = v\omega_2(b, x)$. Since ab lies in $\mathbf{P_c}$, we get that $\omega_2(a, bv)$ is a right-divisor of v, hence

$$x = v\omega_2(b, x) \geq_R \omega_2(a, bv)\omega_2(b, x) = \omega_2(a, \alpha_2(b, x))\omega_2(b, x),$$

which concludes the proof since a divisor of an element of $\mathbf{P_c}$ is also in $\mathbf{P_c}$. □

Proposition 2.2.8. *Assume that $(P_c, \leq)$ is a lattice. There are uniquely defined applications $\alpha : M(P_c) \longrightarrow \mathbf{P_c}$, $\omega : M(P_c) \longrightarrow M(P_c)$ such that*

1. *for $x, y \in \mathbf{P_c}$, we have $\alpha(xy) = \alpha_2(x, y)$ and $\omega(xy) = \omega_2(x, y)$,*

2. *for all* $x, y \in M(P_c)$, *we have* $\alpha(xy) = \alpha(x\alpha(y))$,[1]

3. *for all* $x, y \in M(P_c)$, *we have* $\omega(xy) = \omega(x\alpha(y))\omega(y)$.

Moreover, for $x \in M(P_c)$, *we have that* $\alpha(x)$ *is the greatest left-divisor of* x *lying in* $\mathbf{P_c}$.

Proof. We identify $M(P_c)$ with sequences $(a_1, a_2, \ldots, a_k)$ of elements of $\mathbf{P_c}$ modulo the relation

$$(a_1, \ldots, a_i, a_{i+1}, a_{i+2}, \ldots, a_k) \sim (a_1, \ldots, b, a_{i+2}, \ldots, a_k)$$

whenever $b = a_i a_{i+1}$ is a defining relation of $M(P_c)$.

We define α and ω inductively as follows: we set $\alpha(()) = 1$, $\alpha(a) = a$ whenever $a \in \mathbf{P_c}$, and whenever $k \geq 2$,

$$\alpha(a_1, a_2, \ldots, a_k) = \alpha_2(a_1, \alpha(a_2, \ldots, a_k)).$$

For ω, we set $\omega(()) = 1 = \omega(a)$ for all $a \in \mathbf{P_c}$, and

$$\omega(a_1, a_2, \ldots, a_k) = \omega(a_1, \alpha((a_2, \ldots, a_k))\omega((a_2, \ldots, a_k)).$$

First, we need to verify that these applications are well-defined on $M(P_c)$, that is, that these definitions are compatible with the equivalence relation $\sim$. This will be shown by induction on the number of terms in the sequence.

To see that the definition of ω and α is compatible with the equivalence relation $\sim$, by induction on the number of terms in a sequence we can assume that the relation is applied at the beginning of a sequence $(a_1, a_2, \ldots, a_k)$ of elements of $\mathbf{P_c}$. Hence assume that $a_1 a_2 = b$ is a defining relation of $M(P_c)$. On one hand we have

$$\alpha(a_1, a_2, \ldots, a_k) = \alpha_2(a_1, \alpha(a_2, \ldots, a_k)),$$

on the other hand we have

$$\alpha(b, a_3, \ldots, a_k) = \alpha_2(a_1 a_2, a_3, \ldots, a_k) = \alpha_2(a_1 a_2, \alpha(a_3, \ldots, a_k)$$

By point 1 of Lemma 2.2.7 above we thus have $\alpha(b, a_3, \ldots, a_k) = \alpha(a_1, a_2, \ldots, a_k)$.

Similarly, on one hand we have

$$\omega(a_1, a_2, \ldots, a_k) = \omega_2(a_1, \alpha(a_2, \ldots, a_k))\omega(a_2, \ldots, a_k) = \omega_2(a_1, \alpha(a_2, \ldots, a_k))\omega_2(a_2, \alpha(a_3, \ldots, a_k))\omega(a_3, \ldots, a_k),$$

and

$$\omega(b, a_3, \ldots, a_k) = \omega_2(a_1 a_2, a_3, \ldots, a_k) = \omega_2(a_1 a_2, \alpha(a_3, \ldots, a_k))\omega(a_3, \ldots, a_k).$$

It thus suffices to show that

$$\omega_2(a_1, \alpha(a_2, \ldots, a_k))\omega_2(a_2, \alpha(a_3, \ldots, a_k)) = \omega_2(a_1 a_2, \alpha(a_3, \ldots, a_k)),$$

while holds true by combining the definition of α and point 2 of Lemma 2.2.7 above.

We claim that $\alpha(x)$ is the greatest left-divisor of x lying in $\mathbf{P_c}$. We first show that $\alpha(x) \leq x$. This is achieved by induction on the length of a sequence $(x_1, x_2, \cdots, x_k)$ such that $x_i \in \mathbf{P_c}$ and $x_1 x_2 \cdots x_k = x$. If $k = 0$ or $k = 1$ then $\alpha(x) = x$. Assume that $k > 1$. We have

$$\alpha(x) = \alpha(x_1, x_2, \ldots, x_k) = \alpha_2(x_1, \alpha(x_2, \ldots, x_k)).$$

[1] Note that we recover (1.5.3).

But

$$\alpha_2(x_1, \alpha(x_2, \ldots, x_k)) \leq x_1\alpha(x_2, \ldots, x_k) \leq x_1x_2\cdots x_k,$$

where the first divisibility relation holds by definition of α_2, and the second one by induction. We now show that any element of $\mathbf{P_c}$ left-dividing x is also a left-divisor of $\alpha(x)$. Let $a \in \mathbf{P_c}$ be a left-divisor of x. Let $(a, a_2, \ldots, a_k)$ be a sequence of elements of $\mathbf{P_c}$ whose product is equal to x. Then by definition of α we have

$$\alpha(a, a_2, \ldots, a_k) = \alpha_2(a, \alpha_2(a_2, \ldots, a_k))$$

which is a right-multiple of a.

The fact that $\alpha(xy) = \alpha(x\alpha(y))$ follows from an iterated application of the definition of α on sequences, and the fact that $x = \alpha(x)\omega(x)$ is easy to show by induction on the number of terms in a sequence. The equality $\omega(xy) = \omega(x\alpha(y))\omega(y)$ is obtained by induction on the number of terms of a sequence for x. □

Proposition 2.2.9. *The following holds:*

1. *For all $x \in M(P_c)$, we have $x = \alpha(x)\omega(x)$,*
2. *The monoid $M(P_c)$ is cancellative.*

Proof. Let $x \in M(P_c)$. Then $\alpha(x) \leq y$ for some $y \in M(P_c)$. We claim that y is uniquely defined, equal to $\omega(x)$. We show it by induction on $\ell(x)$. If $\ell(x) = 0$ then $x = \alpha(x) = y = 1$. Hence assume that $\ell(x) > 0$. We have

$$\omega(x) = \omega(\alpha(x)y) = \omega(\alpha(x)\alpha(y))\omega(y),$$

but $\omega(\alpha(x)\alpha(y)) = \omega_2(\alpha(x), \alpha(y))$ and $\alpha(\alpha(x)\alpha(y)) = \alpha(\alpha(x)y) = \alpha(x)$, yielding $\omega(\alpha(x)\alpha(y)) = \alpha(y)$. We thus have $\omega(x) = \alpha(y)\omega(y)$ and by induction on length we have $y = \alpha(y)\omega(y)$. We deduce that $\omega(x) = y$.

We now show that $M(P_c)$ is left-cancellative (the proof of right-cancellativity is similar). Let $a, b, c \in M(P_c)$ such that $ab = ac$. It suffices to show it for $a \in \mathbf{P}_c$. We have $\alpha(ab) = ax$ for some $x \leq b$, $x \in \mathbf{P_c}$, hence there is $b' \in M(P_c)$ such that $b = xb'$. Similarly, we have $\alpha(ac) = ay$ for some $y \leq c$, $y \in \mathbf{P_c}$, hence there is $c' \in M(P_c)$ such that $yc' = c$. But by cancellativity with rest in $\mathbf{P_c}$ we have $y = x$. But we also have

$$\alpha(ab)b' = ab = \alpha(ab)c',$$

forwing $b' = c' = \omega(ab)$. We thus have $b = xb' = yc' = c$, which concludes the proof. □

Theorem 2.2.10. *Assume that $(P_c, \leq_A)$ is a lattice. Then the monoid $M(P_c)$ is a Garside monoid.*

Proof. We already know that $M(P_c)$ is left- and right-cancellative (Proposition 2.2.9), that it has Noetherian divisibility (Lemma 2.2.2), and that the lift $\Delta := \underline{c}$ of c in $M(P_c)$ is a Garside element (Proposition 2.2.4).

The only point which remains to be checked is that $M(P_c)$ has lcm's and gcd's. Let us show that $M(P_c)$ has gcd's. Hence let $x, y \in M(P_c)$. Let

$$X := \{a \in M(P_c) \mid a \leq x, a \leq y\}.$$

We show that X satisfies the assumtions of Proposition 2.2.5(2). If $z \in X$ and s, t at atoms such that $zs, zt \in X$, then we have $zs, zt \leq x$. Writing $x = zz'$, by cancellativity we have $s, t \leq z'$. We then have $s, t \leq \alpha(z')$ and we deduce that the lift u of the right lcm of s and t satisfies $u \leq \alpha(z') \leq z'$.

Hence $zu \in X$ (since the same property but with the roles of x and y swapped must be true), and we conclude using Proposition 2.2.5(2).

We now show the existence of lcm's. We first show that for every $x \in \mathbf{P_c}$, there is $x' \in \mathbf{P_c}$ such that $x\Delta = \Delta x'$. Indeed, let y such that $xy = \Delta$. Since y is also a left-divisor of Δ, there is x' such that $yx' = \Delta$. We then have $x\Delta = xyx' = \Delta x'$. It follows that Δ has a power Δ^n which is central in $M(P_c)$. It follows that every element from $M(P_c)$ is a left-divisor of a power of Δ, hence x and y have a common right-multiple. To conclude the proof, it suffices to take the gcd of the right-common multiples of x and y. □

Chapter 3

Examples

3.1 Artin groups of spherical type: classical Garside structure

3.1.1 Coxeter groups

Let S be a finite set. For $s,t \in S$, let $m_{s,t} \in \mathbb{Z}_{\geq 1} \cup \{+\infty\}$ such that

- $m_{s,s} = 1$, for all $s \in S$,
- $m_{s,t} = m_{t,s} \geq 2$ for all $s,t \in S$.

To this data, one attaches a group W defined by the presentation

$$W = \langle\ S \mid (st)^{m_{s,t}} = 1,\ \forall s,t \in S\ \rangle.$$

Note that the fact that $m_{s,s} = 1$ tells us that $s^2 = 1$ for all $s \in S$. We can thus rewrite the presentation as

$$W = \left\langle S \;\middle|\; \begin{array}{c} s^2 = 1,\ \forall s \in S, \\ \underbrace{sts\cdots}_{m_{s,t}\text{ factors}} = \underbrace{tst\cdots}_{m_{t,s}\text{ factors}},\ \forall s \neq t \in S. \end{array} \right\rangle$$

Definition 3.1.1. A data $(m_{s,t})_{s,t\in S}$ as above is a *Coxeter matrix*. A group W as above is a *Coxeter group*. A pair (W,S) as above is a *Coxeter system*.

Example 3.1.2. Let $W = \mathfrak{S}_n$, and let $S = \{s_1, s_2, \ldots, s_{n-1}\}$, where $s_i = (i, i+1)$ are the simple transpositions. They satisfy the relations

$$\begin{aligned} s_i^2 = 1\ \forall i = 1,\ldots,n-1, \\ s_i s_j = s_j s_i \text{ if } |i-j| > 1, \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}\ \forall i = 1,\ldots,n-2. \end{aligned}$$

These are the defining relations of a Coxeter group W' and since the simple transpositions generate $\mathfrak{S}_n$, there is a surjective group homomorphism $W' \twoheadrightarrow W$. One can show (see Exercise 3.1.3 below) that this homomorphism is an isomorphism, which shows that the symmetric group is a Coxeter group.

Exercise 3.1.3. Show that the map $W' \twoheadrightarrow \mathfrak{S}_n$ from Example 3.1.2 above is an isomorphism. Hint: show by induction on n that $|W'| \leq n!$.

Definition 3.1.4. Let (W, S) be a Coxeter system. The length function $\ell_S : W \longrightarrow \mathbb{Z}_{\geq 0}$ with respect to the generating set S is the *(classical) length function* on W. Given $s_1, s_2, \ldots, s_k \in S$, we say that the word $s_1 s_2 \cdots s_k \in S^*$ is a *reduced expression* for an element $w \in W$ if $k = \ell_S(w)$ and in W we have the equality $w = s_1 s_2 \cdots s_k$.

The following fundamental theorem gives various characterizations of Coxeter groups:

Theorem 3.1.5 (Characterizations of Coxeter groups)**.** *Let W be a group generated by a finite set S of involutions. Let $R := \bigcup_{w \in W} wSw^{-1}$ denote all the conjugates of the elements of S. The following are equivalent:*

1. *(W, S) is a Coxeter system,*
2. *(Exchange Lemma) if $s_1 s_2 \cdots s_k$ is a reduced expression of $w \in W$ and $s \in S$ is such that $\ell_S(sw) \leq \ell_S(w)$, then there is $i \in \{1, 2, \ldots, k\}$ such that $sw = s_1 \cdots s_{i-1} \widehat{s_i} s_{i+1} \cdots s_k$, where the hat denotes omission,*
3. *There exists a function $N : W \longrightarrow \mathcal{P}(R)$ satisfying the following two properties,*
   (a) *$N(s) = \{s\}$ for all $s \in S$,*
   (b) *$N(xy) = N(x) \dot{+} xN(y)x^{-1}$ for all $x, y \in W$, where $\dot{+}$ denotes symmetric difference,*
4. *(Mastumoto's Lemma) For $w \in W$, $s \in S$, we have $\ell_S(sw) \neq \ell_S(w)$, and any two reduced expressions for w can be transformed one into the other using a sequence of braid relations, that is, relations of the form*
$$\underbrace{st\cdots}_{m \text{ factors}} = \underbrace{ts\cdots}_{m \text{ factors}},$$
   where $s \neq t \in S$ and m denotes the order of st in W.

Proof. We do not give a full proof, but leave some implications as exercices.

(1) $\Rightarrow$ (3). Define a map $N : S^* \longrightarrow \mathcal{P}(R)$ as follows by induction on the length of a word. Set $N(s) = \{s\}$ for $s \in S$ and given any word $s_1 s_2 \cdots s_k \in S^*$, set $N(s_1 s_2 \cdots s_k) := \{s_1\} \dot{+} s_1 N(s_2 \cdots s_k) s_1$. We thus have

$$N(s_1 s_2 \cdots s_k) = \{s_1\} \dot{+} \{s_1 s_2 s_1\} \dot{+} \{s_1 s_2 s_3 s_2 s_1\} \dot{+} \ldots \dot{+} \{s_1 s_2 \cdots s_k s_{k-1} \cdots s_2 s_1\}.$$

If $x, y \in S^*$, it follows that $N(xy) = N(x) \dot{+} xN(y)x^{-1}$. It remains to show that N is invariant under the defining relations of W. Assume that $x = w_1 w_2 \in S^*$ and let $x' = w_1 s s w_2$. Then we have

$$N(x') = N(w_1) \dot{+} w_1 N(ssw_2) w_1^{-1} = N(w_1) \dot{+} w_1 (N(ss) + \overline{ss} N(w_2) \overline{ss}^{-1}) w_1^{-1}.$$

But $N(ss) = \{s\} \dot{+} \{s\} = \emptyset$ and $\overline{ss} = 1$, hence

$$N(x') = N(w_1) \dot{+} w_1 N(w_2) w_1^{-1} = N(w_1 w_2) = N(x).$$

Now assume that $st \cdots = ts \cdots$ is a defining relation of W, with $s \neq t \in S$. In particular both sides have $m_{s,t}$ factors. Let $x = w_1 st \cdots w_2$ and $x' = w_2 ts \cdots w_2$. We wish to show as above that $N(x) = N(x')$.

Decomposing $N(x')$ as above, we see that it suffices to show that $N(st\cdots) = N(ts\cdots)$. This holds true as, if $m_{s,t}$ is even, we have

$$N(st\cdots) = \{s\} \dot{+} \{sts\} \cdots \dot{+} \{st\cdots s\} \dot{+} \{ts\cdots t\} \dot{+} \cdots \dot{+} \{tst\} \dot{+} \{t\},$$

where the two middle terms have $m_{s,t} - 1$ factors. This is symmetric in s and t, hence $N(st\cdots) = N(ts\cdots)$. Now if $m_{s,t}$ is odd, we have

$$N(st\cdots) = \{s\} \dot{+} \{sts\} \cdots \dot{+} \{\underbrace{st\cdots s}_{=ts\cdots t}\} \dot{+} \cdots \dot{+} \{tst\} \dot{+} \{t\},$$

where the middle term has $m_{s,t}$ factors, hence is equal to either side of the defining relation. Again this is symmetric in s and t.

We lave the other implications as exercises (see Exercises 3.1.7 to 3.1.9 below). □

Exercise 3.1.6. Deduce from Theorem 3.1.5 that every Coxeter group has a solvable word problem.

Exercise 3.1.7. Show the implication (3) ⇒ (2) of Theorem 3.1.5. To this end

1. First show that $|N(w)| = \ell(w)$,
2. Then show that $\ell(sw) \leq (w) \Rightarrow \ell(sw) < \ell(w)$,
3. Conclude.

Exercise 3.1.8. Show the implication (2) ⇒ (4) of Theorem 3.1.5 by showing the following: let $f : S^* \longrightarrow M$ be a morphism of monoids, where M is a monoid. Show that if $f(st\cdots) = f(ts\cdots)$ for every defining relation of W, then f is constant on reduced expressions of elements of W. Show it by induction on the length of a reduced expression.

Exercise 3.1.9. Show the implication (4) ⇒ (1) of Theorem 3.1.5 by showing the following: if G is a group and $f : S^* \longrightarrow G$ is a morphism of monoids such that $f(s)^2 = 1$ for all $s \in S$ and f is constant on braid relations, then f factors through a group morphism $W \longrightarrow G$.

Exercise 3.1.10. Show that the symmetric group $\mathfrak{S}_n$ is a Coxeter group by considering the set S of simple transposition, the set R of transpositions, and showing that the function $N : W \longrightarrow \mathcal{P}(R)$ defined by

$$N(w) = \{(i,j) \mid i < j \text{ and } w^{-1}(i) > w^{-1}(j)\}$$

satisfies the properties from point (3) of Theorem 3.1.5.

Exercise 3.1.11. Let (W,S) be a Coxeter system and let $I \subseteq S$. Let W_I be the subgroup of W generated by I and let $\ell_I : W_I \longrightarrow \mathbb{Z}_{\geq 0}$ be the length function with respect to I.

1. Show that, for $w \in W_I$, we have $\ell_I(w) = \ell_S(w)$,
2. Show that (W_I, I) is a Coxeter system,
3. Show that if $w = s_1 s_2 \cdots s_k$ is a reduced expression of $w \in W_I$, then $s_i \in I$ for all $i = 1, \ldots, k$.

Proposition 3.1.12. *Let (W,S) be a Coxeter system. Let $w_0 \in W$. The following are equivalent*

1. *We have $\ell_S(sw_0) < \ell_S(w_0)$ for all $s \in S$,*

2. *We have* $\ell_S(w) + \ell_S(w^{-1}w_0) = \ell_S(w_0)$ *for all* $w \in W$,

3. w_0 *has maximal length among all elements of* W. *Moreover, if any of the above conditions is satisfies, then* w_0 *is unique and involutive, and* W *is finite.*

Proof. It is clear that (*ii*) implies (*iii*) and that (*iii*) implies (*i*).

Let us show that (*i*) implies (*ii*). We argue by induction on $\ell_s(w)$. For $w = 1$ the result is clear, hence assume that $\ell_S(w) > 1$. Let $s \in S$ such that $\ell_S(sw) < \ell_S(w)$. Setting $v = sw$ we then have $w = sv$ and $\ell_S(w) = \ell_S(s)+\ell_S(v) = \ell_S(v)+1$. By induction, we have $\ell_S(v)+\ell_S(v^{-1}w_0) = \ell_S(w_0)$. Let $s_1 s_2 \cdots s_\ell s_{\ell+1} \cdots s_k$ be a reduced expression of w_0, where $s_1 s_2 \cdots s_\ell$ is a reduced expression of v and $s_{\ell+1} \cdots s_k$ is a reduced expression of $v^{-1}w_0$. By (1) we have that $\ell_S(sw_0) < \ell_S(w_0)$. By the exchange lemma, there is $i \in \{1, 2, \ldots, k\}$ such that $sw_0 = s_1 \cdots \widehat{s_i} \cdots s_k$. If $i \leq \ell$, then $\ell_S(sv) = \ell_S(v) - 1$, a contradiction, since $sv = w$ and $\ell_S(w) = \ell_S(v) + 1$. Hence writing $v' = s_{\ell+1} \cdots \widehat{s_i} \cdots s_k$, we have that $ss_1 \cdots s_\ell s_{\ell+1} \cdots \widehat{s_i} \cdots s_k$ is a reduced expression of w_0, and it begins with a reduced expression $ss_1 \cdots s_k$ of $sv = w$. We thus have $\ell_S(w) + \ell_S(w^{-1}w_0) = \ell_S(w_0)$, as expected.

Let w_0 be an element satisfying condition (*ii*). Then $\ell_S(w_0^2) = \ell_S(w_0) - \ell_S(w_0) = 0$, hence $w_0^2 = 1$. If w_0' also satisfies condition (*ii*), then $\ell_S(w_0 w_0') = \ell_S(w_0) - \ell_S(w_0')$, which is zero by condition (*iii*). Hence $w_0 w_0' = 1$, hence $w_0' = w_0^{-1} = w_0$.

Finally, if (*i*) is satisfied, then $\ell_S(sw_0) < \ell_S(w_0)$ for all $s \in S$. It follows that $S \subseteq N(w_0)$ which is finite, hence S is finite, and by (*iii*) we get that W is finite. □

Corollary 3.1.13. *Let* (W, S) *be a finite Coxeter group and* w_0 *be its unique element of maximal length. Then*

$$W = \{w \in W \mid w \leq_S w_0\} = \{w \in W \mid w \leq_{S,R} w_0\}.$$

In particular, w_0 *is balanced.*

Proof. The fact that $W = \{w \in W \mid w \leq_S w_0\}$ is point (*ii*) of Proposition 3.1.12. Since $v \leq_S u$ if and only if $v^{-1} \leq_{S,R} u^{-1}$, and w_0 is involutive, we get that $\{w \in W \mid w \leq_{S,R} w_0\} = W^{-1} = W$, which concludes the proof. □

Proposition 3.1.14. *Let* (W, S) *be a Coxeter group partially order with the order* $\leq_S$ *(called the left weak order). Then any pair* x, y *or elements of* W *admits a meet, that is, an element* $z \in W$ *such that*

1. $z \leq_S x$ *and* $z \leq_S y$,

2. *if* $w \in W$ *satisfies* $w \leq_S x$ *and* $w \leq_S y$, *then* $w \leq z$.

Such an element is of course unique.

Proof. The proof is by induction on $\ell(x)$. If $\ell(x) = 0$, then $x = 1$, and $z = 1$ satisfies the two points above.

Hence assume that $\ell(x) > 0$. If there is no $w \in W \backslash \{1\}$ such that $w \leq_S x$ and $w \leq_S y$, then $z = 1$ satisfies the two assumptions. Otherwise, there is $w \neq 1$ such that $w \leq_S x$, $w \leq_S y$. Let z be such an element of maximal length, and let w be another element satisfying $w \leq_S y$ and $w \leq_S x$. We have to show that $w \leq_S z$.

Firstly, assume that $s \leq_S x$ and $s \leq_S y$. Then we claim that $s \leq_S z$. To this end, it suffices to consider two reduced decompositions $s_1 s_2 \cdots s_k s_1' \cdots s_\ell'$ and $s_1 s_2 \cdots s_k s_1'' \cdots s_m''$ of x and y respectively, such that $s_1 s_2 \cdots s_k$ is a reduced decomposition of z. If $s \not\leq_S z$, then by the exchange condition we have that $ss_1 \cdots s_k s_1' \cdots \widehat{s_i'} \cdots s_\ell'$ is a reduced expression of x and $ss_1 \cdots s_k s_1'' \cdots \widehat{s_j''} \cdots s_m''$ is a reduced

decomposition of y. But then $ss_1 \cdots s_k$ is reduced, hence $\ell_S(sz) = \ell_S(z)+1$ and $sz \leq x, y$, contradicting the maximality of the length of z. Hence $s \leq_S z$.

If $w = 1$ then $w \leq_S z$, hence assume that $w \neq 1$. There is $s \in S$ such that $\ell_S(sw) < \ell_S(w)$. We then have $sw \leq_S sx, sy$ and $\ell_S(sx) = \ell_S(x) - 1$. By induction, there is $u \in W$ such that $u \leq_S sx, sy$ and $v \leq_S u$ for all $v \in W$ such that $v \leq_S sx$ and $v \leq_S sy$. We thus have $sw \leq u$. Now by the previous paragraph, we also have $s \leq_S z$. Hence we also have $sz \leq_S sx, sy$, and hence $sz \leq_S u$. Now since $u \leq_S sx$, we have $su \leq_S x$, and similarly we have $su \leq_S y$. Hence $\ell_S(su) \leq \ell_S(z)$. But we also showed that $sz \leq_S u$. We hence have $\ell_S(sz) = \ell_S(z) - 1 \geq \ell_S(su) - 1 = \ell_S(u)$, forcing $sz = u$. Hence $sw \leq_S sz$, which implies that $w \leq_S z$. □

Corollary 3.1.15. *Assume that (W, S) is finite. Then $(W, \leq_S)$ is a lattice.*

Proof. By Proposition 3.1.14, we have the existence of meets. Using Proposition 3.1.12, we deduce the existence of joins: every pair x, y of elements of W admits at least one $z \in W$ such that $x \leq_S z$, $y \leq_S z$ (namely $z = w_0$), and for the join, just take the meet of all such z's. □

Corollary 3.1.16. *Let $G = W$, $A = S$, $c = w_0$. Then $M(P_c)$ is a Garside monoid.*

Proof. This is an immediate consequence of Corollaries 3.1.15, 3.1.13 and Theorem 2.2.10. □

We admit the following result:

Proposition 3.1.17. *Let (W, S) be a Coxeter system. Let $s, s' \in S$ with $s \neq s'$. Then in W we have $s \neq s'$ and the order of ss' is precisely $m_{s,s'}$.*

3.1.2 The classical Artin monoid of spherical type

Proposition 3.1.18 (Classical Garside structure on Artin groups of spherical type)**.** *The Garside group $G(M)$ where $M = M(P_c)$ is as in Corollary 3.1.16 is isomorphic to the Artin group B_W of type W, which has presentation*

$$B_W = \{\mathbf{s}, s \in S \mid \underbrace{\mathbf{st}\cdots}_{m_{s,t}\ factors} = \underbrace{\mathbf{ts}\cdots}_{m_{t,s}\ factors}\}.$$

Proof. Recall the presentation of $G(M(P_c))$ from Proposition 1.5.2 (combined with Corollary 1.2.5). We first show that the map $B_W \longrightarrow G(M(P_c))$, $\mathbf{s} \mapsto \underline{s}$ extends to a group homomorphism, which is therefore surjective as the set $\{\underline{s} \mid s \in S\}$ is precisely the set of atoms of $M(P_c)$. To this end, it suffices to show that $\ell_S(\underbrace{st\cdots}_{m_{s,t}\ \text{factors}}) = m_{s,t}$. This is a consequence of Proposition 3.1.17 above. Indeed, assume that $\ell_S(st\cdots) < m_{s,t}$. Then there is a reduced word for $w = st\cdots$ of length $m' < m_{s,t}$. Since $w \in W_I$ for $I = \{s, t\}$, this is still a word in s and t, and the parity of its length is the same as the parity of $m_{s,t}$. In both cases, using the fact that s and t are involutions, it yields a relation of the form $st\cdots = ts\cdots$, with $m'' < m_{s,t}$ on both sides, from what we deduce that $(st)^{m''} = 1$, a contradiction. This shows that we get a surjective group homomorphism $B_W \longrightarrow G(M(P_c))$.

Conversely, we need to construct a map $G(M(P_c)) \longrightarrow B_W$ which is an inverse to the one constructed above. Let $\underline{u} \in \mathbf{P_c}$. Let $s_1 s_2 \cdots s_k$ be a reduced decomposition of u, and define a map by $\underline{u} \mapsto \mathbf{s_1 s_2 \cdots s_k}$. We first need to show that this map is well-defined: this follows from Matsumoto's Lemma: if $s'_1 s'_2 \cdots s'_k$ is another reduced expression, then one passes from one decomposition to the other only using braid relations, which are the defining relations of B_W. Hence the map is well-defined.

Now, if $u, v \in P_c = W$ are such that $w = uv$ with $\ell_S(w) = \ell_S(u) + \ell_S(v)$, then choosing a reduced decomposition $s_1 \cdots s_\ell s'_1 \cdots s'_m$ of w where $s_1 \cdots s_\ell$ and $s'_1 \cdots s'_m$ are reduced decompositions of u and v respectively, we get that both $\underline{w}$ and $\underline{u} \cdot \underline{v}$ are sent to $\mathbf{s_1 s_2 \cdots s_\ell s'_1 \cdots s'_m}$, hence the map is a group morphism. It is clear that both maps are inverse to each other. □

Corollary 3.1.19. *Artin groups of spherical type have a solvable word problem, and are torsion free.*

Exercise 3.1.20. In the case where $W = \mathfrak{S}_n$, determine the center of B_W.

3.2 Artin groups of spherical type: dual Garside structure

In this subsection, we present an alternative Garside structure for the n-strand braid group. It is built as an interval group from $\mathfrak{S}_n$, using the set of generators T consisting of *all* the transpositions, instead of the set S of simple transpositions.

The results of this section generalize to Coxeter groups of spherical type, i.e., finite Coxeter groups, taking as set T the set of all the conjugates of elements of S. Since the general case is much more involve, we do not present it here. We mostly follow the treatment of Brady [1].

Consider the length function $\ell_T : \mathfrak{S}_n \longrightarrow \mathbb{Z}_{\geq 0}$. Denote by $\leq_T$ the partial order defined on $\mathfrak{S}_n$ by

$$u \leq_T v \;\Leftrightarrow\; \ell_T(u) + \ell_T(u^{-1}v) = \ell_T(v).$$

It is called the *absolute order* on $\mathfrak{S}_n$.

Proposition 3.2.1. *Let $w \in \mathfrak{S}_n$. Let k be the number of orbits of the action of w on $\{1, 2, \ldots, n\}$. Then*

1. $\ell_T(w) = n - k$,
2. *If $w = c_1 c_2 \cdots c_\ell$ is the cycle decomposition of w (without counting 1-cycles), then*

$$\ell_T(w) = \sum_{i=1}^{\ell} \ell_T(c_i)$$

.

Proof. Observe that the orbits of w correspond to the supports of the various cycles occurring in the decomposition of w as a product of disjoint cycles (including 1-cycles). When multiplying w by a transposition (i, j), two situations may appear: if i, j belong to the support of the same cycle c of w, then $(i, j)w$ has one more cycle than w, because c gets breaked into two cycles. If i belongs to the support of a cycle c_1 and j belongs to the support of a cycle c_2 with $c_1 \neq c_2$, then $(i, j)w$ has one cycle less than w since c_1 and c_2 get merged.

Now the identity has n orbits. It follows from the observation above that, if w has k orbits, then at least $n - k$ transpositions are needed to get w, hence $\ell_T(w) \geq n - k$.

Now let $w = c_1 c_2 \cdots c_\ell$ be the cycle decomposition of w, where we do *not* count 1-cycles. In particular, denoting m the number of fixed points of w, we have $m + \ell = k$. If c_i is a k_i-cycle, say $c_i = (j_1, j_2, \ldots, j_{k_i})$, then $c_i = (j_1, j_2)(j_2, j_3) \cdots (j_{k_i - 1}, j_{k_i})$, hence $\ell_T(c_i) \leq k_i - 1$. It follows that

$$\ell_T(w) \leq \sum_{i=1}^{\ell} \ell_T(c_i) \leq \sum_{i=1}^{\ell} (k_i - 1) = -\ell + \sum_{i=1}^{\ell} k_i = -\ell + n - m = n - k,$$

yielding the second inequality. Hence $\ell_T(w) = n - k$. This proves the first point, and in the above inequality we have equalities everywhere, which yields the second point. □

Lemma 3.2.2. *If $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, then $u := (i_1, i_2, \ldots, i_k) \leq_T (1, 2, \ldots, n) =: w$.*

Proof. The permutation $u^{-1}w$ is given by

$$(1, \ldots, i_1 - 1, i_k, i_k + 1, \ldots, n-1, n)(i_1, \ldots, i_2 - 1)(i_2, \ldots, i_3 - 1) \ldots (i_{k-1}, \ldots, i_k - 1).$$

By Proposition 3.2.1 above, we have $\ell(u^{-1}w) = n - k$, $\ell_T(u) = k - 1$, and $\ell_T(w) = n - 1$. This concludes the proof. □

Lemma 3.2.3. *Let $1 \leq i < j \leq n$ and $w \in \mathfrak{S}_n$. Then $(i, j) \leq_T w$ if and only if i and j belong to the support of the same cycle of w.*

Proof. If i and j belong to the same cycle of w, then $(i, j)w$ has one cycle more than w, hence $\ell_T((i, j)w) = \ell_T(w) - 1$ by Proposition 3.2.1. Conversely, if i and j belong to different cycles of w, then $(i, j)w$ has one cycle less than w, hence $\ell_T((i, j)w) = \ell_T(w) + 1$. □

Corollary 3.2.4. *Let $u, v \in \mathfrak{S}_n$ be such that $u \leq_T v$. Let c be a cycle of u. Then there is a cycle c' of v such that* $\mathrm{supp}(c) \subseteq \mathrm{supp}(c')$.

Proof. Assume not. Then there is a cycle c of u with two integers i,j in its support, belonging to different cycles of v. By the previous lemma we thus have $(i, j) \leq_T u$, $(i, j) \not\leq_T v$, contradicting $u \leq_T v$. □

Corollary 3.2.5. *Let Π_n denote the set of partitions of the set $\{1, 2, \ldots, n\}$. Define a map $p : \mathfrak{S}_n \longrightarrow \Pi_n$ by sending a permutation to the partition whose blocks are the supports of its cycles (including 1-cycles). Then p is a map of posets.*

Definition 3.2.6. Let u, v be two cycles in $\mathfrak{S}_n$ such that $\mathrm{supp}(u) \subseteq \mathrm{supp}(v)$. We say that u is *ordered consistently with v* if for all i, j, k, we have $(i, j, k) \leq_T u \Rightarrow (i, j, k) \leq_T v$.

Lemma 3.2.7. *Let $1 \leq i < j < k \leq n$. Then $(i, k, j) \not\leq_T (1, 2, \ldots, n)$.*

Proof. One checks that $(i, k, j)^{-1}(1, 2, \ldots, n)$ is again an n-cycle, hence has reflection length equal to $n - 1$. □

Lemma 3.2.8. *Let $u, v \in \mathfrak{S}_n$ be two cycles such that* $\mathrm{supp}(u) \subseteq \mathrm{supp}(v)$. *Then $u \leq_T v$ if and only if u is ordered consistently with v.*

Proof. If $u \leq_T v$, then by transitivity of $\leq_T$, we obtain that u is ordered consistently with v.

Assume that u is ordered consistently with v. Up to relabelling, we can assume that $v = (1, 2, \ldots, k)$ and that the support of u is given by integers $i_1, i_2, \ldots, i_\ell$ such that $1 = i_1 < i_2 < \cdots < i_\ell \leq k$. By Lemma 3.2.2, if $u = (1, i_2, \ldots, i_k)$, then we are done. If not, then u has the form $(1, i_2, \ldots, i_j, i_{j+1+p}, \ldots)$ for some $j \geq 1$ and $p \geq 1$. By Lemma 3.2.2 again, we have $w := (1, i_{j+1+p}, i_{j+1}) \leq_T u$, while $w \not\leq_T v$ by Lemma 3.2.7, contradicting the assumption. □

Proposition 3.2.9. *Let $w \in \mathfrak{S}_n$. Then w is T-balanced, and if we denote by P_w the set of prefixes of w, the restriction of the map p from Corollary 3.2.5 is injective.*

Proof. The fact that every permutation is balanced follows immediately from the fact that T is stable by conjugation.

The statement on the injectivity of the restriction of p is a corollary of Corollary 3.2.4 and Lemma 3.2.8. □

Definition 3.2.10. Let $u, v \in \mathfrak{S}_n$ with $u \leq_T v$ and $\mathrm{supp}(u) \subseteq \mathrm{supp}(v)$. We say that u has *crossing cycles with respect to v* if there are four distinct integers i, j, k, l in $\{1, 2, \ldots, n\}$ such that $(i, j, k, \ell) \leq_T v$, $(i, k), (j, \ell) \leq_T u$ but $(i, j, k, l) \not\leq_T u$.

Lemma 3.2.11. *Let $1 \leq i < j < k < \ell \leq m$. Then $(i, k)(j, \ell) \not\leq_T (1, 2, \ldots, m)$.*

Proof. One checks that $((i, k)(j, l))^{-1}(1, 2, \ldots, m)$ is again an m-cycle, hence has reflection length equal to $m - 1$. □

Proposition 3.2.12. *If $u, v \in \mathfrak{S}_n$ with $u \leq_T v$, then u has no crossing cycle with respect to v.*

Proof. Assume that there are four distinct integers i, j, k, ℓ in $\{1, 2, \ldots, n\}$ such that $(i, j, k, \ell) \leq_T v$ and $(i, k), (j, \ell) \leq_T u$. We know that i, j, k and ℓ are in the support of the same cycle of v, hence up to relabelling we can assume that this cycle is $(1, 2, \ldots, m)$ and that $1 \leq i < j < k < \ell \leq m$. Now since $(i, k) \leq_T u$, we have that i and k belong to the same cycle c_1 of u, and j, ℓ belong to the same cycle c_2 of u. If $c_1 = c_2$ then we are done. Hence assume that $c_1 \neq c_2$. Then $(i, k)(j, \ell) \leq c_1 c_2 \leq u$, a contradiction, since $(i, k)(j, \ell) \not\leq_T (1, 2, \ldots, m)$. □

Theorem 3.2.13. *Let $u, v \in \mathfrak{S}_n$. Then $u \leq_T v$ if and only if the three following conditions are satisfied:*

1. *Each cycle of u is contained in some cycle of v,*
2. *Each cycle of u is ordered consistently with the cycle of v which contains it,*
3. *u has no crossing cycles with respect to v.*

Proof. If $u \leq_T v$, then the three conditions given above hold true by Corollary 3.2.4, Lemma 3.2.8, and Proposition 3.2.12.

Conversely, assume that the above three conditions hold true. Using the fact that the reflection length is additive on the cycles and condition 1, we can assume that v consists of a single cycle. Hence let $u = c_1 c_2 \cdots c_k$ be the cycle decomposition of u, with each cycle c_i ordered consistently with respect to v. We argue by induction on k. If $k = 1$ then $c_1 \leq_T v$ by Lemma 3.2.8. Up to relabelling, we can assume that $v = (1, 2, \ldots, n)$, and since c_1 is ordered consistently with v, we can assume that $c_1 = (i_1, i_2, \ldots, i_\ell)$ where $1 = i_1 < i_2 < \cdots < i_\ell \leq n$. We thus have $c_1 \leq_T v$ and

$$c_1^{-1} v = (1, 2, \ldots, i_2 - 1)(i_2, \ldots, i_3 - 1) \cdots (i_\ell, \ldots, n).$$

Now, we show that each of the cycles $c_2, \ldots, c_k$ is contained in some cycle of $c_1^{-1} v$. If not, then there are i, j $(i < j)$ belonging to some cycle c_m of $c_1^{-1} v$, and belonging to different cycles of $c_1^{-1} v$ (they cannot be fixed by $c_1^{-1} v$ as they would be fixed by v, hence by u). Note that i and j cannot belong to $\{1, i_2, \ldots, i_\ell\}$. Inspecting the form of the cycle decomposition of $c_1^{-1} v$ which has been calculated above, we see that there are a, b with $a < b$ such that $1 \leq i_a < i < i_b < j$. But this yields $(i, j) \leq_T c_m$, $(i_a, i_b) \leq_T c_1$. This implies that u has crossing cycles with respect to v, a contradiction. Indeed, by Lemma 3.2.8 we would have $(i_a, i, i_b, j) \leq_T v$.

We can thus assume that $c_1^{-1} u = c_2 c_3 \cdots c_m$ is a product of disjoint cycles each of which is contained in a cycle of $c_1^{-1} v$. Moreover, it stays consistently ordered with respect to the cycle containing it, in view of the form of $c_1^{-1} v$. Furthermore, if $c_1^{-1} u$ had crossing cycles with respect to $c_1^{-1} v$, it would have crossing cycles with respect to v. Hence by induction, we deduce that $c_1^{-1} u \leq_T c_1^{-1} v$. We thus have

$$\ell_T(v) = \ell_T(c_1) + \ell_T(c_1^{-1} v) = \ell_T(c_1) + \ell_T(u^{-1} v) + \ell_T(c_1^{-1} v) = \ell_T(u) + \ell_T(u^{-1} v),$$

hence $u \leq_T v$, which concludes the proof. □

Corollary 3.2.14. *Let $u, v \in \mathfrak{S}_n$ such that $u, v \leq_T (1, 2, \ldots, n)$. Then*

$$u \leq_T v \;\Leftrightarrow\; p(u) \subseteq p(v).$$

Proof. The condition $p(u) \subseteq p(v)$ simply means that each cycle of u is contained in a cycle of v. Hence by Theorem 3.2.13 the implication " $\Rightarrow$ " holds true. Conversely, applying the same Theorem, using that $u, v \leq_T (1, 2, \ldots, n)$ implies that both Conditions 2 and 3 are fulfilled if $p(u) \subseteq p(v)$. □

Corollary 3.2.15. *The poset $P_c = \{u \in \mathfrak{S}_n \mid u \leq_T c = (1, 2, \ldots, n)\}$ endowed with the restriction of $\leq_T$ is a lattice.*

Proof. We have seen that the restriction of the map p to P_c is injective. By the corollary above, the partial order $\leq_T$ on P_c corresponds to the inclusion of partitions. The image of $p_{|P_c}$ is precisely the set of *noncrossing partitions*: a partition is said to be noncrossing if it does not contain distinct blocks B_1, B_2 and $i < j < k < \ell$ with $i, k \in B_1$ and $j, \ell \in B_2$. This is precisely saying that one has no crossing cycles with repect to $(1, 2, \ldots, n)$. The noncrossing partitions form a lattice, with meet operation given by inclusion. □

Corollary 3.2.16. *Let $c = (1, 2, \ldots, n)$. Let $\leq_T$ be as above. Then $M(P_c)$ is a Garside monoid.*

Proposition 3.2.17. *The n-strand braid group B_n is isomorphic to the group with generating set a_{ij}, $1 \leq i < j \leq n$ and relations*

$$a_{ij}a_{jk} = a_{jk}a_{ik} = a_{ik}a_{ij},$$

for all $1 \leq i < j < k \leq n$ and

$$a_{ij}a_{kl} = a_{kl}a_{ij}$$

for all $1 \leq i < j < k < l \leq n$ or $1 \leq i < k < l < j \leq n$.

Proof. The map $\varphi : G \longrightarrow B_n$, where G is the group defined by the presentation above, is defined on generators by $a_{ij} \mapsto \sigma_i\sigma_{i+1}\cdots\sigma_{j-1}\sigma_{j-2}^{-1}\cdots\sigma_i^{-1}$. On checks that these images satisfy the required relations, which defined a surjective homomorphism $G \longrightarrow B_n$, as the σ_i's are the images of $a_{i(i+1)}$. This is a technical check which we do not handle here.

We build the inverse map, sending σ_i to $a_{i(i+1)}$ for all i. We have

$$a_{i,i+1}a_{i+1,i+2}a_{i,i+1} = a_{i+1,i+2}a_{i,i+2}a_{i,i+1} = a_{i+1,i+2}a_{i,i+1}a_{i+1,i+2}$$

by applying twice the first relation. For i, j such that $i + 1 < j$ we have

$$a_{i,i+1}a_{j,j+1} = a_{j,j+1}a_{i,i+1}$$

by the second type of relations. We thus obtain a well-defined group homomorphism $\psi : B_n \longrightarrow G$. It is clear that $\varphi \circ \psi = \mathrm{Id}$ since it sends σ_i to σ_i. To show that ϕ is an isomorphism, it suffices to show that ψ is surjective. Let $1 \leq i < j$ with $j + 1 \leq n$. Using the first kind if relations we have that $a_{i,j+1} = a_{j,j+1}^{-1}a_{i,j}a_{j,j+1}$. Hence by induction on $|i - j|$ we seen that $a_{i,j}$ can be expressed as a product of $a_{k,k+1}$ and their inverses, which shows surjectivity of ψ. □

Lemma 3.2.18. *The map sending $a_{i,j}$ to $\underline{(i, j)}$ extends to a well-defined and surjective group homomorphism $B_n \longrightarrow G(P_c)$.*

Proof. For all $1 \leq i < j < k \leq n$, one has

$$\underline{(i,j,k)} = \underline{(i,j)}\ \underline{(j,k)} = \underline{(j,k)}\ \underline{(i,k)} = \underline{(i,k)}\ \underline{(i,j)}.$$

Similarly, for $1 \leq i < j < k < l \leq n$ or $1 \leq i < k < l < j \leq n$, the sets $\{i,j\}$ and $\{k,l\}$ are noncrossing, and hence

$$\underline{(i,j)}\ \underline{(k,l)} = \underline{(i,j)(k,l)} = \underline{(k,l)(i,j)} = \underline{(k,l)}\ \underline{(i,j)},$$

which shows that the map extends to a well-defined group homomorphism.

Surjectivity is clear since $M(P_c)$ is generated by lifts $\underline{(i,j)}$ of transpositions. □

Lemma 3.2.19. *The group $G(P_c)$ is isomorphic to the group with generators $[t]$, for t a transposition, and relations*

$$[t_1][t_2]\cdots[t_{n-1}] = [q_1][q_2]\cdots[q_{n-1}]$$

whenever $t_1 t_2 \cdots t_{n-1} = c = q_1 q_2 \cdots q_{n-1}$.

Proof. Let G be the group with the above presentation. We construct a map $G(M(P_c)) \longrightarrow G$, by sending each generator $\underline{u}$ to $[t_1]\cdots[t_k]$, where $t_1 t_2 \cdots t_k$ is a T-reduced expression of $u \in P_c$. We first show that the set-theoretic wap defined on generators. If $q_1 q_2 \cdots q_k$ is another T-reduced decomposition of u, then setting $v := u^{-1}c$, and choosing any T-reduced decomposition of w, say $r_1 \cdots r_{n-1-k}$, we have

$$[t_1]\cdots[t_k][r_1]\cdots[r_{n-1-k}] = [q_1]\cdots[q_k][r_1]\cdots[r_{n-1-k}]$$

since both $t_1 \cdots t_k r_1 \cdots r_{n-1-k}$ and $q_1 \cdots q_k r_1 \cdots r_{n-1-k}$ are T-reduced decompositions of c. Cancelling the k first factors in both sides of the above equality yields $[t_1]\cdots[t_k] = [q_1]\cdots[q_k]$, which is what we wanted to show.

Now assume that $\underline{u}\ \underline{v} = \underline{w}$ is a defining relation of $M(P_c)$. Choosing a T-reduced decomposition of w obtained by concatenating two reduced decompositions of u and v, and taking images by the above map, shows that images still satisfy the above relation.

We built the inverse map by sending each generator $[t]$ to $\underline{t}$. Given two reduced decompositions $t_1 t_2 \cdots t_{n-1}$ and $q_1 q_2 \cdots q_{n-1}$ of c, we have $\underline{t_1}\ \underline{t_2 \cdots t_{n-1}} = \underline{q_1}\ \underline{q_2 \cdots q_{n-1}}$ by construction of $M(P_c)$, hence we obtain a well-defined group homomorphism. It is clear that each $\underline{t}$ is sent to itself by the composition, and the same holds true for $[t]$, hence the two maps are inverse to each other.

□

We use the above Lemma to build a surjective map θ from $G(M(P_c))$ to B_n, as follows. We send every generator $[t] = [(i,j)]$ to $a_{i,j}$. To show that it is well-defined, it suffices to show that one can pass from any T-reduced decomposition $t_1 t_2 \cdots t_{n-1}$ of c to any other T-reduced decomposition $q_1 q_2 \cdots q_{n-1}$ of c by only using the defining relations of the presentation of Proposition 3.2.17. To this end, it is enough to show it by choosing for $q_1 q_2 \cdots q_{n-1}$ the T-reduced decomposition $s_1 s_2 \cdots s_{n-1}$ of c. This is done in the following Lemma:

Lemma 3.2.20. *For any set $t_1 = (i_1, j_1), \ldots, t_{n-1} = (i_{n-1}, j_{n-1})$ of $n-1$ transpositions satisfying $t_1 \cdots t_{n-1} = c$, one can transform the T-reduced decomposition $t_1 t_2 \cdots t_{n-1}$ into $s_1 s_2 \cdots s_{n-1}$ only by applying sequences of moves of the form*

$$(i,j)(j,k) \leftrightarrow (j,k)(i,k) \leftrightarrow (i,k)(i,j)$$

for $1 \leq i < j < k \leq n$ and

$$(i,j)(k,l) \leftrightarrow (k,l)(i,j)$$

for $1 \leq i < j < k < l \leq n$ or $1 \leq i < k << j \leq n$.

Proof. We argue by induction on n. If $n = 2$ then there is nothing to show since $c = (1, 2)$ which is a transposition. Hence assume that $n \geq 3$, and that any T-reduced word for $(2, 3, \ldots, n)$ can be transformed into $s_2 \cdots s_{n-1}$ by the substitutions in the statement.

Let k be maximal such that 1 occurs in the support of t_k. Note that such a k must exist since c has no fixed point. It suffices to show that we can transform $t_1 t_2 \cdots t_k$ into a sequence of the form $(1, 2)q_2 \cdots q_k$, only using the substitutions from the statement.

We want to show that the rightmost occurrence of 1 in transpositions can be moved to the very left, i.e., that we can assume that $k = 1$.

Hence assume that $k \neq 1$. Consider the sequence $t_{k-1}t_k$, which we write as $(a, b)(c, d)$, with $a < b, 1 = c < d$. If a, b, c, d are all distinct, then we know that $\{a, b\}$ and $\{c, d\}$ are noncrossing, hence $t_{k-1}t_k = t_k t_{k-1}$ and the leftmost occurrence of 1 can be moved to the left.

If a, b, c, d are not distinct, then we consider four cases separately.

If $a = c$, then $(1, b)(1, d) = (1, d, b)$ and $d < b$ otherwise $(1, d, b)$ is not in P_c. But we can use the transformation $(1, b)(1, d) = (1, d)(d, b)$ to move the rightmost occurrence of 1 to the left.

If $a = d$, then the product is $(d, b)(1, d) = (1, b, d)$, hence $b < d$, a contradiction since $d = a < b$.

If $b = c$, then $a < b = c = 1$, which cannot occur.

If $b = d$, then $(a, b)(1, b) = (1, a, b)$ hence $a < b$. But we can use a substitution $(a, b)(1, b) = (1, a)(a, b)$ and the rightmost occurrence of 1 has moved to the left.

Hence we can apply defining relations so that the rightmost occurrence of 1 lies in the first transposition. But since c send 1 to 2, we must have that this first transposition is $(1, 2)$, hence we have reached the situation which allows us to apply the induction hypothesis. □

3.3 Torus knot groups

Let $n, m \geq 2$ and consider the group

$$G(n, m) = \langle\ x, y\ |x^n = y^m\ \rangle.$$

Let $M(n, m)$ denote the monoid with the same presentation.

When n and m are coprime, the group $G(n, m)$ is the knot group of the torus knot $T_{n,m}$.

Proposition 3.3.1. *The monoid $M(n, m)$ is a Garside monoid.*

Proof. The fact that the divisibility is Noetherian is obtained by extending the assignment $x \mapsto m$, $y \mapsto n$ to a length function on $M = M(n, m)$. Since M has two generators and the presentation $x^n = y^m$ is both left- and right-complemented, we have that M is both left- and right-cancellative, since the sharp θ-cube condition is vacuously true. We also get the existence of conditional lcm's. It is clear that the set of left- and right-divisors of $\Delta = x^n = y^m$ is given by $\{x^i \mid i = 0, \ldots, n\} \cup \{y^i \mid i = 0, \ldots, m\}$, which is finite and contains the generating set $\{x, y\}$. Since Δ is central is a left- and right-multiple of both x and y, every pair of elements of M admits a power of Δ as common left- or right-multiple. The existence of lcm's follows since we have conditional lcm's, and the existence of gcd's follows as well (Lemma 1.6.7). □

Exercise 3.3.2. Let $n, m \geq 2$.

1. If n and m are coprime, show that the group $G(n, m)$ is isomorphic to the group $G(M)$ from Exercise 1.7.3.

2. Show that the statement of point 1 is false in general when n and m are not coprime.

Question 3.3.3. Do the groups $G(n, m)$ admit a (non-trivial) realization as interval groups ?

Chapter 4

An application in representation theory

The aim of this chapter is to show an example on how Garside-theoretic properties can be useful to show that a representation of a Garside group is faithful. We will show that the reduced Burau representation of a spherical and dihedral Artin-Tits group is faithful, following Lehrer and Xi [8].

Let (W, S) be a finite Coxeter system of rank two (that is, with $|S| = 2$). Denote $S = \{s, t\}$. Note that W is isomorphic to a dihedral group. One has $2\ell(w_0) = |W|$. Recall that the Artin group B_W attached to W is a Garside group. Note that

$$w_0 = st\cdots = ts\cdots,$$

where each product has $\ell(w_0)$ factors. This yields two reduced expressions of w_0.

Set $m = \ell(w_0)$. Let $\mathcal{A} = \mathbb{R}[v^{\pm 1}]$ and consider a free $\mathcal{A}$-module M of rank 2, with basis E_s, E_t. Define $\mathcal{A}$-linear operators T_s, T_t on M by their action on the basis elements as follows:

$$T_sE_s = qE_s,\ T_sE_t = -q^{-1}E_t + E_s,\ T_tE_s = -q^{-1}E_s + cE_t,\ T_tE_t = qE_t,$$

where $c = 4\cos^2(\pi/m)$. This yields the following matrices of the operators

$$M_s = \begin{bmatrix} q & 1 \\ 0 & -q^{-1} \end{bmatrix},\ M_t = \begin{bmatrix} -q^{-1} & 0 \\ c & q \end{bmatrix}.$$

The action of the elements T_tT_s and T_sT_t is represented by the matrices

$$\begin{bmatrix} -1 & -q^{-1} \\ cq & c-1 \end{bmatrix}, \begin{bmatrix} c-1 & q \\ -cq^{-1} & -1 \end{bmatrix},$$

Proposition 4.0.1. *The matrices M_s and M_t satisfy the defining relation of B_W. In other words, they define a representation $\rho : B_W \longrightarrow \mathrm{GL}_2(\mathcal{A})$.*

The proof will be derived from the following Lemma

Lemma 4.0.2. *Let $\zeta = e^{2i\pi/m}$. Let $k \geq 1$. Denote by $[k]$ the real number $\frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}}$. We have*

$$(M_tM_s)^k = \begin{bmatrix} -[k] - [k-1] & -q^{-1}[k] \\ cq[k] & [k] + [k+1] \end{bmatrix},\ M_s(M_tM_s)^k = \begin{bmatrix} q([k] + [k+1]) & [k+1] \\ -c[k] & -q^{-1}([k] + [k+1]) \end{bmatrix}$$

$$(M_sM_t)^k = \begin{bmatrix} [k] + [k+1] & q[k] \\ -cq^{-1}[k] & -[k] - [k-1] \end{bmatrix},\ M_t(M_sM_t)^k = \begin{bmatrix} -q^{-1}([k] + [k+1]) & -[k] \\ c[k+1] & q([k] + [k+1]) \end{bmatrix}$$

Proof. Note that $c = \zeta + \zeta^{-1} + 2$. We argue by induction on k. For $k = 1$ we recover the matrix which was calculated above. We have

$$(M_tM_s)^{k+1} = (M_tM_s)^k(M_tM_s) = \begin{bmatrix} -[k] - [k-1] & -q^{-1}[k] \\ cq[k] & [k] + [k+1] \end{bmatrix} \begin{bmatrix} -1 & -q^{-1} \\ cq & c-1 \end{bmatrix}$$
$$= \begin{bmatrix} [k] + [k-1] - c[k] & q^{-1}(2[k] + [k-1] - c[k]) \\ cq[k+1] & -[k] + c[k+1] - [k+1] \end{bmatrix},$$

Now using the eqality $[k] + [k-1] - c[k] = -[k] - [k+1]$, which is a straightforward computation using the equation $c = \zeta + \zeta^{-1} + 2$ and valid for all $k \geq 1$, we get that

$$(M_tM_s)^{k+1} = \begin{bmatrix} -[k] - [k+1] & -q^{-1}[k+1] \\ cq[k+1] & [k+1] + [k+2] \end{bmatrix}.$$

We then have

$$M_s(M_tM_s)^k = \begin{bmatrix} q & 1 \\ 0 & -q^{-1} \end{bmatrix} \begin{bmatrix} -[k] - [k-1] & -q^{-1}[k] \\ cq[k] & [k] + [k+1] \end{bmatrix}$$
$$= \begin{bmatrix} -q[k] - q[k-1] + cq[k] & [k+1] \\ -c[k] & -q^{-1}([k] + [k+1]) \end{bmatrix}$$
$$= \begin{bmatrix} q([k] + [k+1]) & [k+1] \\ -c[k] & -q^{-1}([k] + [k+1]) \end{bmatrix}.$$

The remaining calculations are performed similarly, and left to the reader. □

Note that, if $m = 2m'$, then

$$(M_tM_s)^{m'} = \begin{bmatrix} -[m'-1] & 0 \\ 0 & [m'+1] \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = (M_sM_t)^{m'},$$

which proves Proposition 4.0.1 in that case.

Now consider the case where $m = 2m' + 1$. In this case we have $[m'] + [m'+1] = 0$, and we get that

$$M_t(M_sM_t)^{m'} = \begin{pmatrix} 0 & -[m'] \\ c[m'+1] & 0 \end{pmatrix} = \begin{pmatrix} 0 & [m'+1] \\ -c[m'] & 0 \end{pmatrix} = M_s(M_tM_s)^{m'},$$

which also shows Proposition 4.0.1 in this case.

Write $A := W \backslash \{w_0, 1\}$. Note that, for every element $w \in A$, there is a single $s \in S$ such that $\ell(sw) = \ell(w) - 1$, which we denote $L(w)$. Similarly there is a single $s \in S$ such that $\ell(ws) = \ell(w) - 1$, which we denote by $R(w)$.

For $w \in W$, we denote by T_w the image of $\mathbf{w}$ by ρ.

Lemma 4.0.3. *Let $w \in A$. Let $r \in S$. Then*

$$T_wE_r = f_sE_s + f_tE_t,$$

where $f_s, f_t \in \mathcal{A}$ and for $r_1 \in S$, we have $\deg(f_{r_1}) \leq 0$ unless $r = R(w)$ and $r_1 = L(w)$, in which case we have $f_{r_1} = \lambda q +$ lower degree terms, where $\lambda > 0$.

Proof. This is an immediate consequence of Lemma 4.0.2. □

Corollary 4.0.4. *Let $w_1, \dots, w_p$ be elements of A. Then for $r \in S$ we have*

$$T_{w_1} T_{w_2} \cdots T_{w_p} E_r = h_s E_s + h_t E_t,$$

where $h_s, h_t \in \mathcal{A}$ and for $r_1 \in S$, we have $\deg(h_{r_1}) \leq p-1$ unless $r = R(w_p)$, $r_1 = L(w_1)$ and $L(w_i) = R(w_{i-1})$ for $i = 2, 3, \dots, p$. In the case where the three conditions are satisfied, we have $h_{r_1} = \alpha q^p +$ lower degree terms, where $\alpha > 0$.

Proof. This follows immediately from the previous lemma, applied repeteadly. □

Theorem 4.0.5 (Faithfulness of the Burau representation of dihedral type)**.** *Let (W, S) be a Coxeter system of dihedral type. Define a representation $\varphi : B_W \longrightarrow \mathrm{GL}_2(\mathcal{A})$ by $\mathbf{s} \mapsto qT_s$. Then φ is faithful.*

Proof. Recall that B_W is a Garside group (Corollary 3.1.16 and Proposition 3.1.18). In particular, every element of B_W can be written as a fraction $x^{-1}y$, where $x, y \in B_W^+$. To show that φ is faithful, it thus suffices to show that $\varphi_{|B_W^+}$ is faithful.

Recall the Garside normal form of elements of a Garside monoid. In our case, the simple elements of B_W are in bijection with W and are given by positively lifting any reduced expression of any element of W. Let $x \in B_W$ and denote $\alpha(x)$ the first term of the Garside normal form of x. If $x \neq 1$ and $\alpha(x) \neq \Delta$, then $\alpha(x)$ is the lift of some element of A. Elements of A have a unique reduced expression, hence $\alpha(x)$ has a unique atom among $\{\mathbf{s}, \mathbf{t}\}$ that right-divides it, say $\mathbf{s}$. Consider $y = \omega(x)$. If $y \neq 1$, then $\alpha(y) \neq \Delta$, hence the second term of the Garside normal form of x is again the lift of some element of Y. It thus has a single atom left-dividing it, and this atom must be $\mathbf{s}$: otherwise $\alpha(x)\mathbf{t}$ would be a simple element left-dividing x, contradicting the maximality of $\alpha(x)$.

We thus have that, if $x \in B_W$ and Δ is not a left-divisor of x, then the Garside normal form $x = x_1 x_2 \cdots x_k$ of x satisfies:

1. Every element x_1 is the positive lift of an element $y_i \in A$,
2. $L(x_i) = R(x_{i-1})$ for all $i = 2, \dots, k$.

Consider elements $x, y \in B_W^+$ such that $\varphi(x) = \varphi(y)$. We claim that either $x = y = 1$, or x and y have a non-trivial common left divisor.

To this end, consider the Garside normal forms $x = x_1 x_2 \cdots x_k$ and $y = y_1 y_2 \cdots y_\ell$. First suppose that $x_j = \Delta$ for some j. Then $x_1 = \Delta$, which yields the claim, unless $y = 1$. But note that $\det(\varphi(x)) = \pm q^{2\ell(x)}$, which forces $x = 1$ if $y = 1$. We can thus assume that for all $j = 1, \dots, k$, we have $x_j \neq \Delta$, and that for all $j = 1, \dots, \ell$, we have $y_j \neq \Delta$.

By the corollary above, the coefficient of E_r in $\varphi(x)(E_s + E_t)$ has greater degree if $r = L(x_1)$. Hence $L(x_1) = L(y_1)$. This proves the claim.

We deduce the theorem: if $\varphi(x) = \varphi(y)$, then writing $x = ax'$ and $y = ay'$ with $a = \gcd(x, y)$, we get that $\varphi(x') = \varphi(y')$, where x' and y' have no non trivial common left divisor, which yields $x' = y' = 1$, and thus $x = y$. □

Question 4.0.6. Do the torus knot groups $G(n, m)$ admit an analogue of Burau representation ? If yes, is it faithful ?

Bibliography

[1] T. Brady, *A partial order on the symmetric group and new $K(\pi, 1)$'s for the braid groups*, Adv. Math. **161** (2001), no. 1, 20–40.

[2] P. Dehornoy, *Groupes de Garside*, Ann. Sci. École Norm. Sup. (4) **35** (2002), no. 2, 267-306.

[3] P. Dehornoy, *The subword reversing method*, Internat. J. Algebra Comput. **21** (2011), no. 1-2, 71-118.

[4] P. Dehornoy, *A cancellativity criterion for presented monoids*, Semigroup Forum **99** (2019), no. 2, 368-390.

[5] P. Dehornoy, F. Digne, D. Krammer, E. Godelle, and J. Michel. *Foundations of Garside theory*, Tracts in Mathematics **22**, Europ. Math. Soc. (2015).

[6] P. Dehornoy and L. Paris, *Gaussian groups and Garside groups, two generalisations of Artin groups*, Proc. London Math. Soc. (3) **7**9 (1999), no. 3, 569-604.

[7] F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford Ser. **20** (1969), no. 2, 235–254.

[8] G.I. Lehrer, N. Xi, *On the injectivity of the braid group in the Hecke algebra*, Bull. Austral. Math. Soc. **64** (2001), no. 3, 487-493.

[9] A.I. Maltsev, *On the immersion of an algebraic ring into a field*, Mathematische Annalen **113** (1937), 686–691.