GAUSSIAN GROUPS ARE TORSION FREE

Patrick DEHORNOY

Abstract. Assume that G is a group of fractions of a cancellative monoid where lower common multiples exist and divisibility has no infinite descending chain. Then G is torsion free. The result applies in particular to all finite Coxeter type Artin groups.

Finding an elementary proof for the fact that Artin's braid groups are torsion free has been reported to be a longstanding open question [9]. The existence of a linear ordering of the braids that is left compatible with product [4] has provided such a proof—see also [10]. The argument applies to Artin groups of type B_n as well, but it remains rather specific, and there seems to be little hope to extend it to a much larger family of groups. On the other hand, we have observed in [5] and [6] that Garside's analysis of the braids [8] applies to a large family of groups, namely all groups of fractions associated with certain monoids where divisibility has a lattice structure or, equivalently, all groups that admit a presentation of a certain syntactic form. Such groups have been called Gaussian in [6]. It is shown in the latter paper that all finite Coxeter type Artin groups, as well as a number of other groups like torus knot groups or some complex reflection groups, are Gaussian. In the present paper, we give an extremely simple argument proving that all Gaussian groups are torsion-free. However, the argument applies to an even larger family of groups of fractions.

Assume that M is a monoid. For a, b in M, we say that b is a *proper right divisor* of a—or that a is a proper left multiple of b—if there exist $c \neq 1$ such that a is cb. We say that M is *right Noetherian* if the relation of being a proper right divisor has no infinite descending chain. By standard arguments, this is equivalent to the existence of a mapping ρ of M to the ordinals such that $\rho(cb) > \rho(b)$ holds whenever c is not 1.

We say that the monoid M is *right Gaussian* if it is right Noetherian, left cancellative, and every pair of elements (a, b) in M admits a right lower common multiple, *i.e.*, there exists an element c that is a right multiple both of a and b and every common right multiple of a and b is a right multiple of c. The present notion of a right Gaussian monoid is slightly more general than the one considered in [6], which essentially corresponds to the special case where the rank function ρ mentioned above has integer values. *Left Gaussian* monoids are defined symmetrically. A *Gaussian* monoid is a monoid that is both left and right Gaussian. If M is a Gaussian monoid—or, simply, a right cancellative right Gaussian monoid—it satisfies Ore's conditions [2], and therefore it embeds in a group of (right) fractions (every element of the group is a fraction ab^{-1} with a, b in the corresponding monoid). We say that a group is *Gaussian* if it is a group of fractions of a Gaussian monoid.

By [1] or [7], all finite Coxeter type Artin groups are Gaussian. Proposition 2 below gives an effective criterion for recognizing Gaussian groups from presentations. This, in particular, allows us to construct a number of examples in [6].

The result we shall prove here is:

THEOREM 1. *Assume that G is the group of right fractions of a right cancellative right Gaussian monoid. Then G is torsion-free.*

The main idea in the proof is to use words for representing the elements of the groups and to work directly at the level of words rather than in the associated groups. More specifically, we resort to the word reversing process of [3] and [5]—also considered in [11]—that expresses every element of the considered group as a fraction, and we compute the numerators and denominators of the successive powers of an arbitrary element of the group.

DEFINITION. Let S be a nonempty set. A *complement* on S is a mapping f of $S \times S$ into the free monoid S^* generated by S such that $f(x,x)$ is the empty word ε for every x in S.

Assume that f is a complement on S. We denote by M_f the monoid with presentation

$$\langle S \ ; \ \{xf(y,x) = yf(x,y) \ ; \ x, y \in S\}\rangle, \tag{1}$$

i.e., the monoid $S^*/\equiv_f$, where $\equiv_f$ is the congruence on S^* generated by all pairs of the form $(xf(y,x), yf(x,y))$ with x, y in S. Similarly, we denote by G_f the group that admits (1) as a presentation. The elements of G_f will be represented by words in $(S \cup S^{-1})^*$, where S^{-1} is a disjoint copy of S.

By definition, the words $y^{-1}x$ and $f(x,y)f(y,x)^{-1}$ represent the same element of G_f for all x, y in S. The key idea is to give an orientation to this equivalence, *i.e.*, to use it as a rewriting rule that switches the negative and the positive letters in a word.

DEFINITION. Assume that f is a complement on S. We denote by $\vdash_f$ the least reflexive transitive relation on $(S \cup S^{-1})^*$ that is compatible with the product on both sides and that contains all pairs of the form $(y^{-1}x, f(x,y)f(y,x)^{-1})$ for x, y in S.

One easily verifies that, for every word w in $(S \cup S^{-1})^*$, there exists at most one pair (u, v) in $S^* \times S^*$ such that $w \vdash_f uv^{-1}$ holds. Since $w \vdash_f w'$ always implies that w and w' represent the same element of G_f, the relation above gives a decomposition of the element represented by w as a fraction, and it is natural to call u and v the numerator and the denominator of w. We shall denote them respectively by $N(w)$ and $D(w)$.

Finally, for u and v in S^*, we define $C(u, v)$ to be $D(u^{-1}v)$, if it exists. The mapping C is an extension of the mapping f: by definition, for x, y in S, $C(x, y)$ exists and it is equal to $f(x, y)$. An easy induction shows that, if u and v are words in S^* and $C(u, v)$ and $C(v, u)$ exist, then the equivalence

$$u\, C(v, u) \equiv_f v\, C(u, v) \tag{2}$$

holds.

Proposition 2. [6] *Right Gaussian monoids are exactly those monoids of the form M_f where f is a complement on a set S that satisfies the following conditions:*

I: there exists a mapping ρ of S^* to the ordinals that is compatible with $\equiv_f$ and that satisfies $\rho(xu) > \rho(u)$ for every x in S and every u in S^*;

II: for all x, y, z in S, either the words $C(f(x, y), f(z, y))$ and $C(f(x, z), f(y, z))$ do not exist, or both exist and they are $\equiv_f$-equivalent;

III: for every word w in $(S \cup S^{-1})^*$, the words $N(w)$ and $D(w)$ exist.

(The result of [6] deals only with the case where the rank mapping ρ takes integer values, which amounts to considering a more restricted notion of Noetherianity. However, the argument remains the same in the general case, and the latter appears as more natural.)

It follows that we can study Gaussian monoids by using complements and the derived notions, *i.e.*, we can resort to the techniques of [5]. The basic technical result is the following lemma.

Lemma 3. *Assume that f is a complement on S that satisfies Conditions I and II. Let u, v, u', v' be arbitrary words in S^*. Then the following are equivalent:*

(i) The equivalence $uv' \equiv_f vu'$ holds;

(ii) The words $C(v, u)$ and $C(u, v)$ exist, and there exists a word w in S^* such that both $v' \equiv_f C(v, u)w$ and $u' \equiv_f C(u, v)w$ hold.

In the previous statement, it is clear that (ii) implies (i), so the point is to show that (i) implies (ii): this is made by using an induction on the ordinal $\rho(uv')$, where ρ is a rank function witnessing that the complement f satisfies Condition I, and this is a rather direct extension of the corresponding result in [5].

Two important corollaries of the previous lemma are:

Lemma 4. *Assume that f is a complement on S that satisfies Conditions I and II. Let u, v be arbitrary word in S^*. Then $u \equiv_f v$ holds if and only if the words $C(u, v)$ and $C(v, u)$ both exist and are empty.*

Proof. If $u \equiv_f v$ holds, Lemma 3 guarantees that the words $C(v, u)$ and $C(u, v)$ exist, and that there exists a word w in S^* that satisfies $\varepsilon \equiv_f C(v, u)w \equiv_f C(u, v)w$. Now, by construction, the latter equivalences imply $C(v, u) = C(u, v) = \varepsilon$. ■

Thus, under the previous hypotheses, two words u, v in S^* are $\equiv_f$-equivalent if and only if $u^{-1}v \vdash_f \varepsilon$ holds, *i.e.*, if iteratively replacing patterns $x^{-1}y$ with the corresponding pattern $f(x, y)f(y, x)^{-1}$ in the word $u^{-1}v$ leads eventually to an empty word.

Lemma 5. [5] *Assume that f is a complement on S that satisfies Conditions I, II, and III. Let w, w' be arbitrary words in $(S \cup S^{-1})^*$. Then w and w' represent the same element of G_f if and only if there exist words u, u' in S^* satisfying both $N(w)\ u \equiv_f N(w')\ u'$ and $D(w)\ u \equiv_f D(w')\ u'$.*

We turn now to the specific argument that is relevant for studying torsion in G_f. Though nearly trivial, the next result is the core of the argument.

Lemma 6. *Assume that f is a complement on S that satisfies Conditions I and II. Assume in addition that the monoid M_f is right cancellative. Assume that u, v are words in S^* such that $C(C(u, v), C(v, u))$ and $C(C(v, u), C(u, v))$ exist and are empty. Then $C(u, v)$ and $C(v, u)$ are empty as well.*

Proof. By Lemma 4, the hypothesis implies $C(u, v) \equiv_f C(v, u)$. By Formula (2), we have $uC(v, u) \equiv_f vC(u, v)$, hence $uC(v, u) \equiv_f vC(v, u)$. Using the hypothesis that M_f is right cancellative, we deduce $u \equiv_f v$, which, by Lemma 4, implies that $C(u, v)$ and $C(v, u)$ are empty. ■

Lemma 7. *Assume that f is a complement on S that satisfies Condition III. Let w be an arbitrary word in $(S \cup S^{-1})^*$. For, for every positive integer n, we have*

$$N(w^n) = u_1 u_2 \dots u_n, \quad D(w^n) = v_1 v_2 \dots v_n \tag{3}$$

where u_1, …, v_n are defined inductively by $u_1 = N(w)$, $v_1 = D(w)$, $u_{i+1} = C(u_i, v_i)$, and $v_{i+1} = C(v_i, u_i)$.

Proof. We use induction on n. If n is 1, the result is obvious. Otherwise, using the induction hypothesis and the relations $v_i^{-1}u_i \vdash_f u_{i+1}v_{i+1}^{-1}$, $i = 1, \ldots, n-1$, which follow from the definition of u_{i+1} and v_{i+1}, we find

$$\begin{aligned} w^n = w^{n-1}w &\vdash_f u_1u_2\ldots u_{n-1}v_{n-1}^{-1}\ldots v_2^{-1}v_1^{-1}u_1v_1^{-1} \\ &\vdash_f u_1u_2\ldots u_{n-1}v_{n-1}^{-1}\ldots v_2^{-1}u_2v_2^{-1}v_1^{-1} \\ &\ldots \\ &\vdash_f u_1u_2\ldots u_{n-1}v_{n-1}^{-1}u_{n-1}v_{n-1}^{-1}\ldots v_2^{-1}v_1^{-1}, \\ &\vdash_f u_1u_2\ldots u_{n-1}u_nv_n^{-1}v_{n-1}^{-1}\ldots v_2^{-1}v_1^{-1}, \end{aligned}$$

which gives (3) by definition of the numerator and denominator. ■

LEMMA 8. *Assume that f is a complement on S that satisfies Conditions I, II, and III. Assume in addition that the monoid M_f is right cancellative. Let w be an arbitrary word in $(S \cup S^{-1})^*$. Then w represents 1 in G_f if and only if the equalities*

$$N(w^2) = N(w) \qquad \text{and} \qquad D(w^2) = D(w) \tag{4}$$

hold.

Proof. By construction, the words w and $N(w)D(w)^{-1}$ represent the same element of G_f. So (4) implies that w and w^2 represent the same element of G_f, and, therefore, that w represents 1.

Conversely, let us first observe that the hypotheses of the lemma imply that the monoid M_f embeds in the group G_f. Indeed, assume that w, w' are words in S^* that represent the same element of G_f. By Lemma 5, there exist words u, u' in S^* that satisfy $N(w)\ u \equiv_f N(w')\ u'$ and $D(w)\ u \equiv_f D(w')\ u'$. By construction, $N(w)$ is w, and $D(w)$ is the empty word ε, and the same holds for w', so the equivalences become $wu \equiv_f w'u'$ and $u \equiv_f u'$. We deduce $wu \equiv_f w'u$, and $w \equiv_f w'$ whenever M_f is right cancellative.

Assume now that w is a word in $(S \cup S^{-1})^*$ that represents 1. So does $N(w)D(w)^{-1}$. Hence $N(w)$ and $D(w)$ represent the same element of G_f. By the previous result, $N(w) \equiv_f D(w)$ holds. By Lemma 4, this implies

$$C(N(w), D(w)) = C(D(w), N(w)) = \varepsilon. \tag{5}$$

Now, by Lemma 7, we have the following *equalities* of words

$$N(w^2) = N(w)C(N(w), D(w)), \text{ and } D(w^2) = D(w)C(D(w), N(w)).$$

So (5) gives the result. ■

We can now prove Theorem 1. Let w be an arbitrary word in $(S \cup S^{-1})^*$. As in Lemma 7, we define inductively two sequences of positive words u_1, u_2, ..., v_1, v_2, ... by $u_1 = N(w)$, $v_1 = D(w)$, $u_{i+1} = C(u_i, v_i)$, $v_{i+1} = C(v_i, u_i)$. By Formula (3), we have

$$N(w^n) = u_1 u_2 \ldots u_n, \quad D(w^n) = v_1 v_2 \ldots v_n,$$
$$N(w^{2n}) = u_1 u_2 \ldots u_{2n}, \quad D(w^{2n}) = v_1 v_2 \ldots v_{2n}.$$

Assume that w^n represents 1 in G_f. Then, by Lemma 8, the words $N(w^n)$ and $N(w^{2n})$ on the one hand, and $D(w^n)$ and $D(w^{2n})$ on the other hand, are equal, which means that each of the words u_{n+1}, ..., u_{2n} and v_{n+1}, ..., v_{2n} is empty. Now Lemma 6 tells us that $u_{i+2} = v_{i+2} = \varepsilon$ implies $u_{i+1} = v_{i+1} = \varepsilon$ provided that i is at least 1. So the assumption $u_{n+1} = v_{n+1} = \varepsilon$ implies $u_2 = v_2 = \varepsilon$, *i.e.*,

$$N(w^2) = N(w) \quad \text{and} \quad D(w^2) = D(w).$$

By Lemma 8, this means that w represents 1 in G_f. ■

Remark 9. Most of the results about word reversing can be extended to the case where the complement is not unique, which corresponds to monoids where common multiples exist, but not necessarily lower common multiples. In this case, convenient versions of Proposition 2 and Lemmas 3, 4, 5 hold, but the lack of uniqueness for the numerators and denominators causes Lemma 8 to fail. However, it is easy to see that Theorem 1 cannot hold in general in this framework. Indeed, a typical example of a group eligible for the previous approach is the group

$$\langle x, y \ ; \ xy = yx, x^2 = y^2 \rangle,$$

where we have two ways of completing the pair (x, y). Now, in this group, we have $xy^{-1} \neq 1$, but $(xy^{-1})^2 = 1$.

References

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

[2] A.H. Clifford & G.B. Preston, *The algebraic theory of semigroups, vol. 1*, AMS Surveys **7**, (1961).

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

[4] —, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.

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

[6] P. Dehornoy & L. Paris, *Gaussian groups and Garside groups: two generalizations of Artin groups*, Preprint (1997).

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

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

[9] W. Magnus, *Braid groups: a survey*, Proc. Second Int. Conf. Theory of Groups, Camberra 1973, 463–487.

[10] D. Rolfsen & J. Zhu, *Braids, orderings and zero divisors*, Proc. Amer. Math. Soc., to appear.

[11] K. Tatsuoka, *An isoperimetric inequality for Artin groups of finite type*, Trans. Amer. Math. Soc. **339–2** (1993) 537–551.

SDAD ESA 6081
Département de mathématiques,
Université, 14 032 Caen, France
dehornoy@math.unicaen.fr