GROUPES DE GARSIDE

Patrick DEHORNOY

Abstract. Define a Garside monoid to be a cancellative monoid where right and left lcm's exist and that satisfy additional finiteness assumptions, and a Garside group to be the group of fractions of a Garside monoid. The family of Garside groups contains the braid groups, all spherical Artin groups, and various generalizations previously considered[1]. Here we prove that Garside groups are biautomatic, and that being a Garside group is a recursively enumerable property, i.e., there exists an algorithm constructing the (infinite) list of all small Gaussian groups. The latter result relies on an effective, tractable method for recognizing those presentations that define a Garside monoid.

Résumé. Les monoïdes de Garside sont introduits comme monoïdes simplifiables où existent ppcm et pgcd et où sont satisfaites des conditions convenables de finitude, et les groupes de Garside comme groupes de fractions de monoïdes de Garside. La famille des groupes de Garside contient les groupes de tresses, les groupes d'Artin sphériques, et diverses généralisations considérées antérieurement[2]. Dans cet article, nous montrons que les groupes de Garside sont bi-automatiques, et qu'être un groupe de Garside est une propriété récursivement énumérable, c'est-à-dire qu'il existe un algorithme énumérant la liste infinie de tous ces groupes. Ce résultat repose sur une méthode effective pour reconnaître les présentations des monoïdes de Garside.

Key words : Presentations of monoids and groups; word problem; rewriting systems; Cayley graph; braid groups; Artin groups.

MSC 2000 : 20M05, 20F36, 05C25, 68Q42.

L'objet de cet article est l'étude par des méthodes algébriques et combinatoires d'une classe de groupes, appelés groupes de Garside, qui contient en particulier les groupes de tresses classiques, tous les groupes d'Artin sphériques, et diverses extensions de ces groupes précédemment introduites. Les groupes de Garside sont définis comme groupes de fractions des monoïdes de Garside, ces derniers étant définis par l'existence de notions convenables de plus petit commun multiple (ppcm) et de plus

[1] In particular, the Garside groups considered in [17] are special cases of those considered here; the latter had been called "small Gaussian" in earlier works; the name has been changed in order to uniformize the terminology with works by Bessis, Charney, Michel, and other authors

[2] En particulier, les groupes de Garside introduits dans [17] sont un cas particulier de ceux considérés ici, qui, eux, avaient été appelés petits groupes gaussiens; ce changement de nom a été décidé afin d'uniformiser la terminologie avec d'autres travaux récents de Bessis, Charney, Michel, entre autres.

grand commun diviseur (pgcd), et la satisfaction de conditions de noethérianité et de génération finie. On démontre ici :

Théorème A. *Tout groupe de Garside est bi-automatique.*

Théorème B. *Etre un groupe de Garside et un monoïde de Garside sont des propriétés Σ_1^0, c'est-à-dire récursivement énumérables.*

Le théorème A, qui résout positivement une conjecture de [17] (énoncée en termes de petit groupe gaussien), implique en particulier que tout groupe de Garside a un problème de mot et un problème de conjugaison décidables, et qu'il satisfait une inégalité isopérimétrique quadratique.

Le théorème B signifie qu'il existe un algorithme (théorique) qui énumère systématiquement toutes les présentations de groupes de Garside et de monoïdes de Garside. Il repose sur l'existence d'un critère effectif caractérisant certaines présentations des monoïdes de Garside. Plus précisément, il existe des conditions explicites $(**)$ de complexité Σ_1^0 telle qu'on ait les résultats suivants, dont les termes seront définis plus bas :

Théorème B'. *(i) Si M est un monoïde de Garside, et si f est un sélecteur de ppcm sur une partie génératrice Σ de M, alors M admet la présentation complémentée $\langle \Sigma; R_f \rangle^+$, et celle-ci satisfait aux conditions $(**)$.*

(ii) Inversement, si $\langle \Sigma; R_f \rangle^+$ est une présentation complémentée satisfaisant aux conditions $(**)$, alors le monoïde qu'elle définit est un monoïde de Garside, et f est un sélecteur de ppcm sur Σ.

Si la démonstration du théorème B', qui occupe la plus grande partie de l'article, est assez délicate, les conditions $(**)$ qu'il met en jeu sont simples, et, en particulier, leur implantation sur ordinateur est aisée. La conjonction des théorèmes A et B' permet donc de construire de nombreux exemples de groupes automatiques.

Les propriétés algébriques des groupes de tresses et de leurs extensions ont fait l'objet de nombreux travaux. Dans le cas des groupes de tresses, la plupart des résultats classiques sur les problèmes de mots et de conjugaison, les formes normales, et l'automaticité sont présents ou implicites dans les travaux de Garside [21] et Thurston [27] — voir aussi [2] [19]. On sait que les méthodes et les résultats s'étendent à des classes de groupes plus vastes : groupes d'Artin sphériques [5] [18] [8] [9], groupes des tresses des groupes de réflexions complexes [6], groupes de Garside au sens de [17] et [4] — qu'on appellera ici «groupes de Garside au sens restreint» . La classe des groupes de Garside considérés ici, et introduits dans [17] sous l'appellation «petits groupes gaussiens» , inclut strictement toutes les classes précédentes. Par exemple, les groupes $\langle a, b\,;\, ab^p a = b^q \rangle$ sont pour $q \geq p \geq 1$ des groupes de Garside n'appartenant à aucune des familles précédentes.

Un groupe de Garside est le groupe de fractions d'un monoïde dans lequel existe une bonne théorie de la divisibilité et des ppcm (la définition précise sera donnée au début de la section 1). Déjà relevée chez Garside et Deligne, l'importance des ppcm dans les monoïdes de tresses a été dégagée explicitement par Thurston dans la construction de formes normales et, de là, de structures automatiques [27] [20], et

elle est au centre de l'étude développée dans [17] pour les groupes dits de Garside. En un sens, le théorème A n'est qu'une extension naturelle du résultat analogue établi dans [17] pour les groupes de Garside au sens restreint, lequel ne fait que reprendre l'argument de [9] pour les groupes d'Artin sphériques, qui, à son tour, n'est qu'une adaptation de l'argument original de [27]. Le point nouveau consiste ici à s'affranchir d'une hypothèse technique superflue incluse dans la définition des groupes de Garside au sens restreint, à savoir la propriété (vérifiée dans le cas des tresses et des groupes d'Artin) que l'élément fondamental Δ est le ppcm des générateurs minimaux. L'intérêt de la présente approche ne tient pas tant à l'affaiblissement des hypothèses obtenu qu'à l'argument utilisé pour établir le résultat, à savoir l'utilisation systématique des compléments : si M est un monoïde admettant la simplification à gauche, et où deux éléments quelconques admettent un unique ppcm à droite, nous appellerons *complément* (à droite) de x dans y, et noterons $x\backslash y$, l'unique élément z tel que xz est le ppcm à droite de x et y. L'étude pour elles-mêmes de l'opération $\backslash$ et de sa contrepartie à gauche / semble nouvelle. Nous montrons ici comment construire à l'aide de ces opérations des formes normales explicites et des structures automatiques. De telles constructions sont déjà présentes dans [27] et [20] dans le cas des tresses, et le passage aux groupes de Garside serait une extension facile si toutes les hypothèses avaient été conservées. La tâche en fait n'est pas si aisée, car les constructions initiales utilisaient au moins trois conditions que nous éliminons ici : préservation de la longueur dans les relations définissant le groupe, existence d'une structure de groupe de Coxeter sous-jacente (le groupe symétrique et ses opérations de treillis dans le cas des tresses), centralité de l'élément Δ^2. S'affranchir de telles hypothèses exige de reprendre l'étude du début, avec des arguments et un enchaînement différents, tout en aboutissant à des démonstrations plus simples et naturelles que celles de [8] et [17]. Il semble donc que les groupes de Garside constituent un cadre bien adapté, ce que confirment d'autres travaux récents : [14], où il est montré que les groupes de Garside, et, plus généralement, les groupes gaussiens sont sans torsion, [23], où est adaptée la solution du problème de conjugaison décrite par Morton et ElRifai [19] dans le cas des tresses, [24], où il est montré que tout groupe de Garside se décompose en produit croisé de groupes de Garside avec centre monogène.

Sauf dans des cas triviaux, il est très difficile de reconnaître les propriétés combinatoires d'un groupe à partir d'une présentation, et de nombreux résultats d'indécidabilité sont connus [3]. Il existe en particulier très peu de critères permettant de reconnaître qu'un monoïde se plonge dans le groupe de même présentation [1] [25], et on sait que la preuve d'un tel résultat par Garside dans le cas des groupes de tresses est à l'origine de la plupart des développements algébriques ultérieurs sur ces groupes. Le théorème B repose sur une nouvelle méthode dans cette direction. L'outil essentiel utilisé ici est une opération combinatoire sur les mots appelée *redressement*. Introduite dans [11], et considérée sous une forme similaire dans [26], puis étudiée sytématiquement dans [13], cette opération est une contrepartie syntaxique à l'opération de complément : à partir d'une certaine fonction f déterminée par la présentation lorsque celle-ci est d'un certain type dit complémenté, le redressement permet de définir une opération binaire $\backslash_f$ sur les mots de sorte que, si M est un monoïde engendré par un ensemble Σ, et si u, v sont des mots sur Σ représentant respectivement les éléments x et y de M, alors le mot $u\backslash_f v$ représente

l'élément $x\backslash y$, sous la condition que la fonction f, c'est-à-dire la présentation considérée, vérifie une certaine condition dite propriété du cube, déjà implicite dans le théorème H de [21]. Il a été montré dans [17] que tous les groupes de Garside admettent une présentation complémentée, et, réciproquement, on y a donné des conditions suffisantes pour qu'une présentation complémentée définisse un groupe de Garside. Ces conditions au demeurant sont d'intérêt pratique limité, car elles nécessitent d'une part d'établir la noethérianité d'une relation et, d'autre part, de vérifier la propriété du cube pour une infinité de mots : dans les deux cas, il s'agit de conditions de type infinitaire (conditions respectivement Π^1_1 et Π^0_1 dans le langage de la théorie de la récursivité, c'est-à-dire mettant en jeu une quantification universelle portant respectivement sur les suites de mots et les mots). Dans certains cas particuliers, comme celui des tresses et, plus généralement, lorsque les relations de la présentation considérée préservent la longueur, la condition de noethérianité est triviale, et la propriété du cube se réduit à une vérification finie, qui constitue le travail de Garside dans [21]. Notre travail ici consiste à montrer que, dans le cas général, la condition de noethérianité peut être déduite de conditions effectives plus faibles, et qu'il est suffisant de vérifier la propriété du cube pour des triplets de mots pris dans un certain ensemble fini. De la sorte, et comme énoncé dans le théorème B', nous obtenons un critère algorithmique — et simple : si, par exemple, nous entrons la présentation standard d'un monoïde de tresses dans l'algorithme, celui-ci répondra en un temps fini qu'il s'agit d'un monoïde de Garside, et il fournira une description explicite d'une structure automatique. Le prix à payer pour ces résultats est une analyse fine du processus de redressement des mots — lequel jouait déjà un rôle technique essentiel dans la construction d'un ordre total sur les tresses [16].

Le plan de l'article est le suivant. Dans la section 1, nous définissons les notions de monoïde de Garside et de groupe de Garside; nous établissons des propriétés de base des opérations de complément, et nous décrivons un treillis fini attaché à chaque monoïde de Garside et qui le caractérise. Dans la section 2, on établit des formules de dualité reliant les opérations de ppcm, pgcd, et complément à gauche et à droite dans tout monoïde de Garside. En fait, on travaille ici dans un cadre plus général : ainsi, on obtient à la fois des formules de dualité utiles pour la preuve du théorème A, et une caractérisation des monoïdes de Garside par des hypothèses plus faibles (mais moins naturelles) que celles de la définition initiale, lesquelles seront prises comme point de départ pour la preuve du théorème B'. Dans la section 3, on démontre le théorème A. Grâce au pgcd, on définit une forme normale unique pour les éléments de tout groupe de Garside : cette forme, la «mixed canonical form» de [20], est bien connue dans le cas des tresses, le point spécifique ici étant la simplicité de la preuve d'automaticité, ainsi que la possibilité de construire effectivement des automates (ou des transducteurs) calculant les formes normales. En particulier, on montre comment calculer le pgcd à gauche *et* le pgcd à droite avec l'élément Δ au moyen d'un automate dont les états sont des fonctions sur la clôture des atomes par complément (et non des diviseurs de Δ ainsi qu'il est classique pour le pgcd à gauche). Dans la section 4, on montre que tout groupe de Garside admet une présentation de forme syntactique particulière, dite complémentée, et que toutes les opérations du monoïde, ppcm, pgcd, compléments,

peuvent se calculer à partir de l'opération de redressement des mots déduite de la présentation. Ceci donne en particulier une solution effective au problème de mot (du monoïde et du groupe). Dans la section 5, et grâce à la caractérisation de la section 2, on montre que les présentations complémentées de groupes de Garside satisfont à certaines conditions nécessaires et suffisantes, dont la propriété du cube. A ce stade, le théorème B' n'est pas établi, car le critère obtenu requiert de vérifier la propriété du cube pour tous les triplets de mots : l'objet de la section 6 est alors de montrer qu'il suffit d'effectuer cette vérification pour un ensemble fini de mots, à savoir la clôture des générateurs par l'opération $\backslash_f$. Ceci établit le résultat cherché, et fournit un critère pratique, ainsi que l'illustre un exemple.

Si Σ est un alphabet, et R une famille de relations sur Σ, c'est-à-dire une famille de paires de mots sur Σ, nous noterons $\langle \Sigma\,;\, R\rangle^+$ le monoïde engendré par Σ et présenté par les relations R, et $\langle \Sigma\,;\, R\rangle$ le groupe correspondant.

L'auteur remercie Matthieu Picantin pour ses remarques judicieuses.

1. Calcul des compléments

Si M est un monoïde, et x, y des éléments de M, on dira que x est diviseur à gauche de y, ou, de façon équivalente, que y est multiple à droite de x, s'il existe z vérifiant $xz = y$; on parlera de diviseur ou de multiple propre si, en outre, on a $z \neq 1$. De là une notion naturelle de plus petit multiple commun (ppcm) à droite : z est un ppcm à droite de x et y si z est un multiple à droite de x et de y, et un diviseur à gauche de tout multiple à droite commun à x et y. De la même façon, z est un plus grand commun diviseur à gauche, ou pgcd à gauche, de x et y si z est un diviseur à gauche de x et y, et un multiple à droite de tout diviseur à gauche commun à x et y.

Il n'y a en général aucune raison pour qu'un ppcm z de x et y, s'il existe, soit unique, non plus que l'élément y' vérifiant $z = xy'$. Cependant, des conditions assez faibles garantissent cette unicité.

Lemme 1.1. *Soit M un monoïde simplifiable à gauche où 1 est le seul élément inversible. Alors la relation «être un diviseur à gauche propre» est un ordre partiel sur M, et les ppcm à droite et pgcd à gauche de deux éléments sont uniques quand ils existent.*

Démonstration. Par hypothèse, la conjonction de $x \neq 1$ et $y \neq 1$ implique $xy \neq 1$ dans M, donc la relation «être un diviseur à gauche propre» est transitive; que M soit simplifiable à gauche entraîne que cette relation est irréflexive, et c'est donc un ordre (strict). Quand ils existent, le ppcm à droite et le pgcd à gauche de deux éléments x, y sont la borne supérieure et la borne inférieure de x et y dans l'ordre ci-dessus. ∎

Définition 1.2. Sous les hypothèses du lemme précédent, nous noterons $x \vee y$ le ppcm à droite de x et y, quand il existe; dans ce cas, l'unique élément z vérifiant $x \vee y = xz$ sera noté $x\backslash y$, lu «x sous y» , et appelé *complément à droite* de y sur x.

On a donc

$$x \vee y = x(x\backslash y) = y(y\backslash x) \tag{1.1}$$

dès que $x \vee y$ est défini. De façon symétrique (donc sous l'hypothèse que le monoïde est simplifiable à droite), nous notons $x \mathbin{\widetilde{\vee}} y$ le ppcm à gauche de x et y quand il existe, et x/y l'unique élément z vérifiant $x \mathbin{\widetilde{\vee}} y = zx$. La contrepartie de (1.1) est alors

$$x \mathbin{\widetilde{\vee}} y = (x/y)y = (y/x)x \tag{1.2}$$

(Figure 1.1). Noter que x est un diviseur à gauche de y si et seulement si $y\backslash x$ est défini et égal à 1 : dans ce cas, $x\backslash y$ est le quotient «$x^{-1}y$» et, de même, x/y est le quotient «xy^{-1}» dans le cas où y est un diviseur à droite de x — ce qui explique et justifie nos notations.

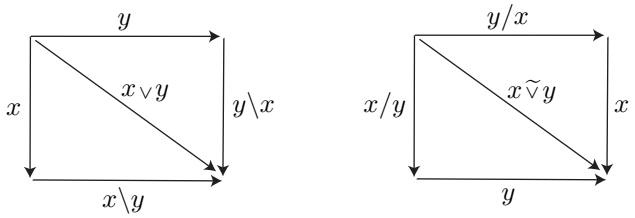


Figure 1.1. Complément à droite et à gauche

L'objet de notre étude est la famille des monoïdes appelés gaussiens dans [17] et [14]. Ceux-ci sont définis en termes de ppcm et de pgcd : essentiellement, un monoïde gaussien est un monoïde avec uniques ppcm et pgcd à droite et à gauche, et un monoïde de Garside est un monoïde gaussien satisfaisant une condition forte de génération finie. Pour une définition précise, nous aurons besoin d'une notion supplémentaire :

Définition 1.3. Soit M un monoïde. On dit qu'un élément x de M est un *atome* si x est distinct de 1 et que $x = yz$ entraîne $y = 1$ ou $z = 1$. On dit que M est *atomique* si M est engendré par ses atomes et si, de plus, pour tout x dans M, la *norme* $\|x\|$ de x, définie comme la borne supérieure des longueurs des décompositions de x en produit d'atomes, est finie.

On remarquera que 1 est nécessairement le seul élément inversible dans un monoïde atomique, puisque, par définition, on a $\|xy\| \geq \|x\| + \|y\|$ pour tous x, y, et $\|x\| \geq 1$ pour $x \neq 1$.

La définition suivante d'un monoïde gaussien apparaît dans [17] :

Définition 1.4. (i) On dit qu'un monoïde M est *gaussien* si M est atomique, simplifiable, et si deux éléments quelconques de M admettent un ppcm à droite et à gauche, et un pgcd à droite et à gauche.

(ii) On dit qu'un monoïde gaussien M est un *monoïde de Garside* s'il contient un *élément de Garside*, ce dernier étant défini comme un élément Δ tel que les diviseurs à gauche de Δ coïncident avec les diviseurs à droite de Δ, ils soient en nombre fini, et ils engendrent M.

(iii) Tout monoïde gaussien satisfait aux conditions de Ore, et admet donc un groupe de fractions. On dit qu'un groupe G est un *groupe gaussien* (*resp.* un *groupe de Garside*) s'il existe un monoïde gaussien M (*resp.* un monoïde de Garside M) tel que G soit le groupe de fractions de M.

Exemple 1.5. Les groupes de tresses [21] et, plus généralement, tous les groupes d'Artin sphériques, c'est-à-dire associés à un groupe de Coxeter fini, sont des groupes de Garside [5] [18], l'élément dit fondamental étant un élément de Garside. Plus généralement, tous les groupes de Garside au sens de [17] sont des groupes de Garside au sens ci-dessus, mais la réciproque est fausse : un groupe de Garside au sens restreint de [17] est un groupe de Garside dans lequel, de surcroît, le ppcm à droite des atomes est un élément de Garside. Un contre-exemple typique est $\langle a, b\,;\, aba = b^2\rangle^+$: il y a ici deux atomes, à savoir a et b, dont le ppcm est b^2, qui n'est pas un élément de Garside, puisque ab est un diviseur à gauche mais pas à droite de b^2; par contre, l'élément $\Delta = b^3$ est un élément de Garside.

Nous allons dans la suite établir divers résultats sur les monoïdes de Garside, en particulier l'équivalence de la définition originale avec plusieurs définitions alternatives. Tous ces résultats reposent sur les propriétés algébriques des opérations de ppcm et de complément, que nous allons établir maintenant. Il sera utile de disposer de telles propriétés dans un cadre plus général que celui des monoïdes de Garside. En particulier, nous considérerons le cas où l'opération de ppcm (à droite) n'est pas nécessairement partout définie. Pour ce faire, nous utiliserons un symbole $\perp$ signifiant «non défini» : de la sorte, $x \vee y = \perp$ signifie que x et y n'ont pas de ppcm, et une égalité telle que $x \vee y = x' \vee y'$ signifie que soit $x \vee y$ et $x' \vee y'$ sont définis et ils sont égaux, soit ni $x \vee y$, ni $x' \vee y'$ ne sont définis. On convient qu'on a toujours $x\perp = \perp x = \perp$. Ainsi les égalités (1.1) et (1.2) sont toujours satisfaites, que les ppcm et compléments mentionnés soient définis ou non.

Pour formuler de façon compacte nos hypothèses, nous utiliserons les abréviations suivantes :

Définition 1.6. On dira qu'un monoïde M satisfait la condition
- (C_0) si l'élément 1 est le seul inversible de M;
- (C_0^+) si M est atomique;
- (C_1) si M admet la simplification à gauche;
- $(\widetilde{C}_1)$ si M admet la simplification à droite;
- (C_2) si deux éléments de M admettant un multiple à droite commun admettent un ppcm à droite;
- (C_2^+) si deux éléments quelconques de M admettent un ppcm à droite;
- (C_3) si M possède une partie génératrice finie P close par $\backslash$, c'est-à-dire telle que $x, y \in P$ entraîne $x\backslash y \in P$;
- (C_3^+) si M possède une partie génératrice finie S close par $\backslash$ et $\vee$, c'est-à-dire telle que $x, y \in S$ entraîne $x\backslash y \in S$ et $x \vee y \in S$.

Noter que (C_0^+) entraîne (C_0), et, de même, (C_2^+) entraîne (C_2), et (C_3^+) entraîne (C_3). La conjonction de (C_0), (C_1) et (C_2) est le cadre naturel pour que les opérations de ppcm et de complément à droite soient bien définies — donc, en

particulier, pour que (C_3) et (C_3^+) aient un sens — et (C_2^+) est la condition additionnelle garantissant que ces opérations soient partout définies. Sous l'hypothèse que (C_0), (C_1) et (C_2) sont satisfaites, l'égalité (1.1) est toujours valable, de même que $x \vee y = y \vee x$, et

$$(xy) \vee (xz) = x(y \vee z). \tag{1.3}$$

Lemme 1.7. *Soit M un monoïde satisfaisant (C_0), (C_1) et (C_2). Pour tous x, y, z dans M, on a :*

$$(xy)\backslash z = y\backslash(x\backslash z), \qquad z\backslash(xy) = (z\backslash x) \cdot ((x\backslash z)\backslash y) \tag{1.4}$$

$$(x \vee y)\backslash z = (x\backslash y)\backslash(x\backslash z) = (y\backslash x)\backslash(y\backslash z), \qquad z\backslash(x \vee y) = (z\backslash x) \vee (z\backslash y) \tag{1.5}$$

Démonstration. Pour (1.4), on a, en utilisant (1.1) et (1.3),

$$xy((xy)\backslash z) = (xy)\vee z = (xy)\vee(x\vee z) = (xy)\vee(x(x\backslash z)) = x(y\vee(x\backslash z)) = xy(y\backslash(x\backslash z)),$$
$$z((xy)\backslash z) = (xy) \vee z = xy((z\backslash x)\backslash y) = x(z\backslash x)(y\backslash(z\backslash x)) = z(x\backslash z)(y\backslash(z\backslash x)),$$

et on simplifie à gauche par xy dans le premier cas, et par z dans le second. Pour (1.5), appliquer (1.4) à $x \vee y = x(x\backslash y)$ donne directement $(x \vee y)\backslash z = (x\backslash y)\backslash(x\backslash z)$. Comme $\vee$ est symétrique, cette expression est aussi $(y\backslash x)\backslash(y\backslash z)$. Enfin, on trouve, en appliquant (1.4), l'égalité précédente, et (1.1),

$$z\backslash(x\vee y) = z\backslash(x(x\backslash y)) = (z\backslash x)((x\backslash z)\backslash(x\backslash y)) = (z\backslash x)((z\backslash x)\backslash(z\backslash y)) = (z\backslash x)\vee(z\backslash y).$$

(Figure 1.2). Remarquer que les formules sont valides lorsqu'un des ppcm n'est pas défini, chacune des expressions ayant alors la valeur $\perp$, c'est-à-dire étant non définie. ■

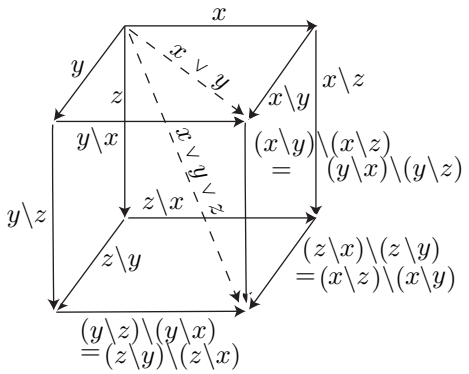


Figure 1.2. Complément itéré

Dans le contexte précédent, pour $X, Y \subseteq M$ et $k \geq 1$, on pose $X\backslash Y = \{x\backslash y\,;\, x \in X, y \in Y\}$, $X^k = \{x_1 \cdots x_k\,;\, x_1, \ldots, x_k \in X\}$, et $X^0 = \{1\}$.

Lemme 1.8. *Soit M un monoïde satisfaisant aux conditions (C_0), (C_1) et (C_2), et P une partie génératrice de M close par $\backslash$. Alors, pour tout k, on a $M\backslash P^k \subseteq P^k$, P^k est close par $\backslash$ et par diviseur à droite, et M satisfait à la condition (C_2^+).*

Démonstration. On montre par induction sur $i+k$ que la conjonction de $x \in P^i$ et $y \in P^k$ entraîne $x\backslash y \in P^k$. Pour $k = 0$, c'est-à-dire pour $y = 1$, on a $x\backslash y = 1$, et le résultat est vrai. Supposons $k = 1$. Pour $i = 0$, soit $x = 1$, le résultat est vrai. Pour $i = 1$, le résultat est l'hypothèse que P est clos par $\backslash$. Pour $i \geq 2$, écrivons $x = x_1x'$ avec $x_1 \in P$ et $x' \in P^{i-1}$. Par (1.4), on a $x\backslash y = x'\backslash(x_1\backslash y)$. L'hypothèse d'induction donne $x_1\backslash y \in P$, d'où $x'\backslash(x_1\backslash y) \in P$. Supposons enfin $k \geq 2$. On écrit $y = y_1y'$ avec $y' \in P$ et $y' \in P^{k-1}$. Par (1.4), on a $x\backslash y = (x\backslash y_1)((y_1\backslash x)\backslash y')$. L'hypothèse d'induction donne $x\backslash y_1 \in P$ et $y_1\backslash x \in P^i$. On déduit $(y_1\backslash x)\backslash y' \in P^{k-1}$, d'où $x\backslash y \in P^k$.

On a ainsi montré $P^i\backslash P^k \subseteq P^k$ pour tout i, d'où $M\backslash P^k \subseteq P^k$ si P engendre M, c'est-à-dire que M est la réunion des ensembles P^i. On a aussi $P^k\backslash P^k \subseteq P^k$, donc P^k est clos par l'opération $\backslash$. De plus, supposons $y \in P^k$ et $y = zx$. On a alors $x = z\backslash y$, donc $x \in P^k$.

Les calculs précédents montrent que $x\backslash y$, donc aussi $x \vee y$, existent pour tout x dans M et tout y dans P^k, pour tout k. Comme P engendre M, on déduit que $x\backslash y$ et $x \vee y$ existent pour tous x, y dans M, et M satisfait donc à la condition (C_2^+). ■

Lemme 1.9. *Soit M un monoïde satisfaisant (C_0), (C_1) et (C_2), et P un sous-ensemble de M clos par $\backslash$. Soit S la clôture de P par $\vee$.*

(i) L'ensemble S est clos par $\backslash$ et $\vee$. Si P est fini, alors S est fini, on a $\mathrm{card}(S) \leq 2^{\mathrm{card}(P)}$; par conséquent, la condition (C_3) entraîne la condition (C_3^+).

(ii) Pour tous i, k, on a $S^i\backslash S^k \subseteq S^k$ et $S^i \vee S^k \subseteq S^{\sup(i,k)}$; en particulier, S^k est clos par $\backslash$ et $\vee$ pour tout k.

Démonstration. (i) Par construction, tout élément de S peut être exprimé comme ppcm à droite d'un sous-ensemble fini de P, donc, si P a n éléments, S a au plus 2^n éléments. Par construction, S est clos par $\vee$, et il s'agit de montrer qu'il est également clos par $\backslash$. Supposons $x = x_1 \vee \cdots \vee x_p$, $y = y_1 \vee \cdots \vee y_q$ avec $x_1, \ldots, y_q \in P$. Nous voulons établir $x\backslash y \in S$. D'abord, (1.5) entraîne $x\backslash y = (x\backslash y_1) \vee \cdots \vee (x\backslash y_q)$, donc il suffit de montrer $x\backslash y_j \in P$ pour tout j. On utilise une induction sur $p \geq 1$. Pour $p = 1$, le résultat est l'hypothèse que P est clos par ppcm à droite. Sinon, posons $x' = x_1 \vee \cdots \vee x_{p-1}$. Par (1.5), nous obtenons

$$x\backslash y_j = (x' \vee x_p)\backslash y_j = (x'\backslash x_p)\backslash(x'\backslash y_j);$$

L'hypothèse d'induction entraîne $x'\backslash x_p \in P$ et $x'\backslash y_j \in P$, d'où $(x'\backslash x_p)\backslash(x'\backslash y_j) \in P$ puisque P est clos par $\backslash$.

(ii) L'ensemble S étant clos par $\backslash$, le lemme 1.8 donne $S^i\backslash S^k \subseteq S^k$ directement. On établit la relation $S^i \vee S^k \subseteq S^{\sup(i,k)}$ par récurrence sur $\inf(i,k)$. Le résultat est trivial pour $\inf(i,k) = 0$. Pour $\inf(i,k) = 1$, soit par exemple $k = 1$, on utilise une récurrence sur i : supposant $x \in S^i$ et $y \in S$, on pose $x = x_1x'$ avec $x_1 \in S$ et $x' \in S^{i-1}$. Par les formules du lemme 1.7, on trouve

$$x \vee y = (x_1 \vee y)((x_1\backslash y)\backslash x') \in S \cdot S^{i-1} = S^i.$$

Supposons enfin $\inf(i,k) \geq 2$. On écrit $x = x_1x'$, $y = y_1y'$ avec $x_1, y_1 \in S$, $x_1 \in S^{u-1}$, et $y' \in S^{k-1}$. Les règles du lemme 1.7 donnent

$$x \vee y = (x_1 \vee y_1)\,(((x_1\backslash y_1)\backslash x') \vee ((y_1\backslash x_1)\backslash y')).$$

On a alors $x_1 \vee y_1 \in S$, puis, d'après ce qui précède, $(x_1\backslash y_1)\backslash x' \in S^{i-1}$, et $(y_1\backslash x_1)\backslash y' \in S^{k-1}$, d'où $((x_1\backslash y_1)\backslash x') \vee ((y_1\backslash x_1)\backslash y') \in S^{\inf(i-1,k-1)}$ par hypothèse de récurrence, et, finalement, $x \vee y \in S^{\sup(i,,)}$. ■

Sous les hypothèses précédentes, tout élément de S qui s'exprime comme le ppcm à droite de k éléments de P peut aussi s'exprimer comme produit de k éléments de P. En effet, on peut établir par récurrence une formule générale du type

$$x \vee y \vee z \vee \cdots = x \cdot (x\backslash y) \cdot ((x\backslash y)\backslash(x\backslash z)) \cdot \cdots.$$

Nous allons dans la suite donner plusieurs définitions équivalentes des monoïdes de Garside. La première provient de la remarque que, si M est un monoïde de Garside et que Δ est un élément de Garside dans M, alors l'ensemble S des diviseurs de Δ est clos par les opérations de ppcm, pgcd et complément à droite et à gauche. L'existence d'un tel ensemble peut en fait être prise comme définition :

Proposition 1.10. *Soit M un monoïde gaussien, Δ est élément de M, et S une partie de M. Alors il y a équivalence entre*

(i) Δ est élément de Garside, et S est l'ensemble des diviseurs (à gauche ou à droite) de Δ;

(ii) S est une partie génératrice finie de M qui est close par diviseur, ppcm, complément et pgcd à droite et à gauche, et Δ est le ppcm à droite de S.

Démonstration. Supposons (i). Supposons $x \in S$ et $x = yz$: alors il existe x' vérifiant $xx' = \Delta$, d'où $y(zx') = \Delta$, et y est dans S. Ainsi, S est clos par diviseur à gauche, et, par un argument symétrique, par diviseur à droite.

Soient maintenant x, y dans S. Par hypothèse, Δ est multiple à droite de x et y, donc de $x \vee y$. Par conséquent, $x \vee y$ est dans S, et il en est de même de $x\backslash y$, qui en est un diviseur à droite. Le cas du ppcm et du complément à gauche est symétrique; le cas des pgcd est trivial. Enfin, Δ, étant élément de S, en est nécessairement ppcm à droite et à gauche puisque S est clos par ces opérations.

Réciproquement, supposons (ii). Le premier problème est de montrer que l'ensemble $\widetilde{S}$ des diviseurs à gauche de Δ coïncide avec S. D'abord, par construction, tout élément de S est diviseur à gauche de Δ, et S est donc inclus dans $\widetilde{S}$. Soit x un élément quelconque de $\widetilde{S}$. Il existe donc x' vérifiant $xx' = \Delta$, d'où $x = \Delta/x'$. Par le lemme 1.9, on a $M\backslash S \subseteq S$, et donc, symétriquement, $S/M \subseteq S$, d'où en particulier $x = \Delta/x' \in S$. Donc S est l'ensemble des diviseurs à gauche de Δ.

Le second problème est de montrer de même que S coïncide avec l'ensemble des diviseurs à droite de Δ. Ce point résultera du calcul précédent (renversé par symétrie) pourvu qu'on montre que Δ est le ppcm à gauche de S. Comme Δ est dans S, il s'agit de montrer que tout élément x de S est un diviseur à droite de Δ. Soit x un tel élément. Par hypothèse, $x \mathbin{\widetilde{\vee}} \Delta$ existe et est dans S : il existe y vérifiant $x \mathbin{\widetilde{\vee}} \Delta = y\Delta$, et, puisque $y\Delta$ est dans S, il existe z vérifiant $y\Delta z = \Delta$. Comme

Δ est dans S, et que S est clos par diviseur à gauche et à droite, y et z sont dans S. Il existe donc y' dans S, à savoir $y' = y\backslash\Delta$, vérifiant $yy' = \Delta$, et, puisque la simplification à gauche est possible, on déduit $y' = \Delta z$. Puisque y' est dans S, il existe ensuite y'' dans S, à savoir $y'' = y'\backslash\Delta$, vérifiant $y'y'' = \Delta$, d'où $\Delta = \Delta zy''$. Ceci entraîne $zy'' = 1$, d'où $z = y'' = 1$, donc $y\Delta = \Delta$, et, finalement, $y = 1$, ce qui montre que x est diviseur à droite de Δ. ■

On notera que l'argument précédent utilise seulement (C_0), et non (C_0^+).

Définition 1.11. Si M est un monoïde de Garside, on appelle *primitifs à droite* les éléments de la clôture des atomes de M par l'opération $\backslash$, et *simples* les éléments de la clôture des éléments primitifs par l'opération $\vee$ — qui est aussi la clôture des atomes par $\backslash$ et $\vee$.

Si M est un monoïde de Garside, alors l'ensemble des atomes de M est la partie génératrice minimale de M, l'ensemble des éléments primitifs à droite est la partie génératrice close par $\backslash$ minimale, l'ensemble S des éléments simples est la partie génératrice close par $\backslash$ et $\vee$ minimale, et son ppcm est l'élément de Garside de norme minimale[1]. Avec les notations précédentes, la structure $(S, \vee, \wedge)$ est un treillis (fini), et il en est de même de la structure symétrique $(S, \widetilde{\vee}, \widetilde{\wedge})$.

Proposition 1.12. *Un monoïde de Garside est déterminé par l'ensemble de ses éléments primitifs à droite et la restriction de l'opération $\backslash$ à ces éléments.*

Démonstration. Soit M un monoïde de Garside, et P l'ensemble de ses éléments primitifs à droite. Par hypothèse, P engendre M, donc il suffit de montrer que, pour tous $x_1, \dots, x_p$, $y_1, \dots, y_q$ dans P, la condition $x_1 \cdots x_p = y_1 \cdots y_q$ peut s'exprimer en terme de la restriction de $\backslash$ à P. Or $x_1 \cdots x_p = y_1 \cdots y_q$ équivaut à $(x_1 \cdots x_p)\backslash(y_1 \cdots y_q) = (y_1 \cdots y_q)\backslash(x_1 \cdots x_p) = 1$, et les règles de calcul du lemme 1.7 montrent que $(x_1 \cdots x_p)\backslash(y_1 \cdots y_q)$ s'exprime comme produit de q éléments de P déterminés de proche en proche à partir de $x_1, \dots, y_q$ à l'aide de l'opération $\backslash$. Par exemple, pour $p = q = 2$, on trouve

$$(x_1x_2)\backslash(y_1y_2) = (x_2\backslash(x_1\backslash y_1))\cdot(((x_1\backslash y_1)\backslash x_2)\backslash((y_1\backslash x_1)\backslash y_2)).$$

En vertu de la condition (C_0), le produit de ces q éléments vaut 1 si et seulement chacun d'eux vaut 1, ce qui donne une condition du type requis. Par exemple, $x_1x_2 = y_1y_2$ est équivalent à la conjonction des quatre égalités

$$\begin{aligned} x_2\backslash(x_1\backslash y_1) = 1, \quad & ((x_1\backslash y_1)\backslash x_2)\backslash((y_1\backslash x_1)\backslash y_2) = 1, \\ y_2\backslash(y_1\backslash x_1) = 1, \quad & ((y_1\backslash x_1)\backslash y_2)\backslash((x_1\backslash y_1)\backslash x_2) = 1. \end{aligned}$$ ■

Proposition 1.13. *Un monoïde de Garside M est déterminé par son graphe caractéristique, défini comme la restriction aux éléments simples du graphe de Cayley atomique, c'est-à-dire la famille des triplets (x, a, y) où x et y sont simples et a est un atome vérifiant $xa = y$.*

[1] dans le cas des groupes d'Artin, les éléments simples sont aussi appelés *réduits* dans la littérature

Démonstration. Notons S l'ensemble des éléments simples de M, et Γ son graphe caractéristique. D'après la proposition précédente, il suffit de montrer que, pour x, y dans S, la valeur de $x\backslash y$ est déterminée par Γ. Soient x, y des éléments de S, donc des sommets de Γ. Le ppcm à droite de x et y est la borne supérieure de x et y dans Γ, c'est-à-dire l'unique sommet z accessible depuis x et y dans Γ tel que, pour tout sommet z' accessible depuis x et y, z' soit accessible depuis z. Alors $x\backslash y$ est l'unique sommet y' de Γ tel qu'il existe un chemin de 1 à y' qui porte les mêmes étiquettes que le chemin de x à z. En effet, si $a_1, \ldots, a_k$ est la suite des étiquettes du chemin de x à z dans Γ, on a $x\backslash y = a_1 \cdots a_k$ dans M. Le seul point à justifier est l'existence d'un chemin étiqueté $a_1, \ldots, a_k$ depuis 1 dans Γ : or, pour $i \leq k$, $a_1 \cdots a_i$ est un diviseur à gauche de $x\backslash y$, donc un élément de S, et donc l'arête $(a_1 \cdots a_{i-1}, a_i, a_1 \cdots a_i)$ appartient bien à Γ. ■

Exemple 1.14. La figure 1.3 montre le graphe caractéristique dans le cas du monoïde $\langle a, b\,;\, aba = b^2\rangle^+$, dont les critères de la section 6 montreront qu'il est un monoïde de Garside : il y a ici 8 éléments simples. Noter que le ppcm à droite des atomes, à savoir b^2, n'est pas l'élément Δ, qui est b^3.

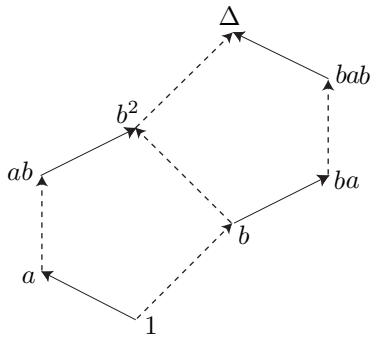
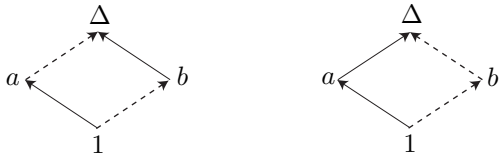


Figure 1.3. Graphe caractéristique du monoïde $\langle a, b\,;\, aba = b^2\rangle^+$
(Les arêtes pleines représentent a, les tiretées b)

En effaçant les étiquettes du graphe caractéristique, on obtient le diagramme de Hasse du treillis des éléments simples. Ce graphe ne détermine pas le monoïde à isomorphisme près. Par exemple, les monoïdes $\langle a, b\,;\, ab = ba\rangle^+$ et $\langle a, b\,;\, a^2 = b^2\rangle^+$ sont tous deux des monoïdes de Garside; les graphes de Cayley associés sont respectivement



Les graphes non étiquetés sous-jacents sont identiques, alors que les monoïdes ne sont pas isomorphes, puisque les graphes étiquetés ne le sont pas.

Lorsque M est le monoïde d'Artin associé à un groupe de Coxeter fini W, les éléments simples de M sont en bijection avec les éléments de W, et le graphe

caractéristique de M s'obtient à partir du graphe de Cayley de W en orientant les flèches, c'est-à-dire en supprimant les relations de torsion $x^2 = 1$. Cette propriété ne s'étend pas au cas d'un monoïde de Garside général, puisque, dans l'exemple 1.14, tous les sommets du graphe n'ont pas le même degré, ce qui exclut que ce dernier soit la projection du graphe de Cayley d'un groupe.

Question 1.15. Le graphe caractéristique d'un monoïde de Garside est-il la projection du graphe de Cayley d'un monoïde quotient de M obtenu en ajoutant des relations de torsion ?

Le réponse est positive dans le cas de l'exemple 1.14 : si W est le monoïde obtenu en ajoutant à la présentation les relations de torsion $a^2 = 1$ et $b^4 = b$ (la seconde est en fait conséquence de la première), alors le graphe caractéristique de M s'obtient à partir du graphe de Cayley de W en supprimant des arêtes de torsion (Figure 1.4). Le groupe $\langle a, b\,;\, aba = b^2\rangle$ est le groupe de tresses B_3, présenté à partir des générateurs $a = \sigma_1$ et $b = \sigma_2\sigma_1$. Le groupe B_3 est également le groupe de fractions du monoïde de Garside B_3^+, dont le groupe de Coxeter associé est le groupe symétrique $\mathfrak{S}_3$. Remarquer que ce dernier admet la présentation $\langle a, b\,;\, aba = b^2, a^2 = 1, b^3 = 1\rangle$, et qu'il s'obtient donc à partir du monoïde $\langle a, b\,;\, aba = b^2, a^2 = 1, b^4 = b\rangle^+$ en quotientant par la relation $b^3 = 1$.

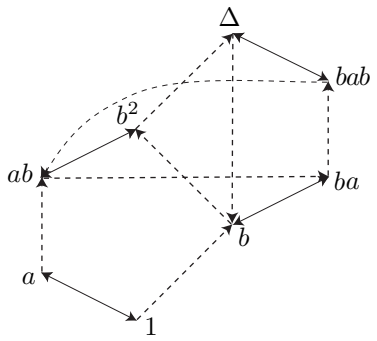


Figure 1.4. Graphe de Cayley du monoïde $\langle a, b\,;\, aba = b^2, a^2 = 1, b^4 = b\rangle^+$
(Les arêtes pleines représentent a, les tiretées b)

2. Dualité dans les monoïdes de Garside

L'objet de cette section est à la fois d'établir des formules de calcul valables dans tout monoïde de Garside (lemmes 2.5 et 2.6), et de donner une nouvelle caractérisation de ceux-ci par des conditions plus faibles que celles de la définition initiale qui seront utilisées dans la section 5. Le résultat est le suivant :

Proposition 2.1. *Un monoïde est un monoïde de Garside si, et seulement si, il vérifie les conditions* (C_0), (C_1), (C_2), (C_3), *et* $(\widetilde{C}_1)$.

Tout monoïde gaussien satisfait par définition aux conditions (C_0), (C_1), (C_2) et $(\widetilde{C}_1)$, et tout monoïde de Garside satisfait en outre la condition (C_3) d'après la proposition 1.10, donc les conditions de la proposition 2.1 sont nécessaires. Le problème est de montrer que ces conditions sont aussi suffisantes, et, en particulier, de montrer qu'elles entraînent l'existence des ppcm à gauche qui n'y sont pas mentionnés, non plus que l'atomicité. La démonstration comporte plusieurs résultats intermédiaires, et repose sur l'existence d'une dualité échangeant division à gauche et à droite pour les éléments simples.

Lemme 2.2. *Soit* M *un monoïde satisfaisant aux conditions* (C_0), (C_1) *et* (C_2^+), S *une partie génératrice de* M *close par* $\backslash$ *et* $\vee$, *et admettant un ppcm à droite* Δ.

(i) Pour tout entier k, *l'ensemble* S^k *est clos par* $\backslash$ *et* $\vee$, *tout diviseur à droite de* Δ^k *appartient à* S^k, *et tout élément de* S^k *est un diviseur à gauche de* Δ^k.

(ii) Posons $x^* = x\backslash\Delta$ *pour* $x \in S$. *Alors, on a* $x^* \in S$ *et* $xx^* = \Delta$. *Pour* x, y *dans* S, y^* *est un diviseur à droite de* x^* *si* x *est un diviseur à gauche de* y, *et l'implication réciproque est vraie si* M *admet la simplification à droite.*

(iii) La fonction $x \mapsto x^{**}$ *s'étend en un endomorphisme* ϕ *de* M *qui envoie* S^k *dans lui-même pour tout* k, *et, pour tout* x *dans* M, *on a*

$$x\Delta = \Delta\phi(x). \tag{2.1}$$

Démonstration. (i) Le lemme 1.9(iii) affirme que S^k est clos par $\backslash$ et $\vee$, et le lemme 1.8 que tout diviseur à droite de Δ^k appartient à S^k, puisque Δ^k est élément de S^k par construction.

Supposons $x \in S^k$. On démontre par récurrence sur k que x est un diviseur à gauche de Δ^k. Pour $k = 0$, on a $x = 1$, et le résultat est trivial. Pour $k = 1$, le résultat découle de la définition de Δ. Supposons $x \in S^k$ avec $k \geq 2$. On écrit $x = x_1x'$ avec $x_1 \in S$ et $x' \in S^{k-1}$. Par (1.4), on a

$$\Delta^k\backslash x = (\Delta^k\backslash x_1) \cdot ((x_1\backslash\Delta^k)\backslash x').$$

Puisque x_1 est dans S, il est diviseur à gauche de Δ, donc de Δ^k, donc on a $\Delta^k\backslash x_1 = 1$, et, d'autre part, toujours par (1.4),

$$x_1\backslash\Delta^k = (x_1\backslash\Delta)\cdot((\Delta\backslash x_1)\backslash\Delta^{k-1}) = (x_1\backslash\Delta)\cdot(1\backslash\Delta^{k-1}) = (x_1\backslash\Delta)\cdot\Delta^{k-1}.$$

On déduit

$$\Delta^k\backslash x = ((x_1\backslash\Delta)\Delta^{k-1})\backslash x' = \Delta^{k-1}\backslash((x_1\backslash\Delta)\backslash x').$$

Par le lemme 1.8, $(x_1\backslash\Delta)\backslash x'$ est dans S^{k-1}, donc, par hypothèse de récurrence, cet élément est un diviseur à gauche de Δ^{k-1}. On déduit $\Delta^{k-1}\backslash((x_1\backslash\Delta)\backslash x') = 1$, soit finalement $\Delta^k\backslash x = 1$, et x est diviseur à gauche de Δ^k.

(ii) Supposons $x \in S$. Comme Δ est dans S, on a $x^* = x\backslash\Delta \in S$ puisque, par hypothèse, S est clos par $\backslash$. Par définition, x est diviseur à gauche de Δ, donc on a $xx^* = x \vee \Delta = \Delta$. Supposons que x et y soient dans S et x est un diviseur à gauche de y, disons $y = xz$. On a alors $xx^* = \Delta = yy^* = xzy^*$, d'où $x^* = zy^*$, et y^* est diviseur à droite de x^*. Inversement, $x^* = zy^*$ entraîne $yy^* = xzy^*$, donc $xz = y$ si la simplification à droite par y^* est permise.

(iii) Supposons $x \in S$. Alors x^* est dans S, donc x^{**} est défini, et on obtient

$$x\Delta = x(x^*x^{**}) = (xx^*)x^{**} = \Delta x^{**}. \tag{2.2}$$

Soit x un élément quelconque de M. Puisque S engendre M, il existe une décomposition, en général non unique, de x comme produit d'éléments de S. Supposons $x = x_1 \cdots x_p = y_1 \cdots y_q$, avec $x_1, \ldots, x_p, y_1, \ldots, y_q \in S$. Par (2.2), on obtient

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

et, puisque Δ est simplifiable à gauche, il n'y a pas d'ambiguïté à définir ϕ par $\phi(x) = x_1^{**} \cdots x_k^{**}$. Alors, par construction, ϕ est un endomorphisme de M, et (2.1) est vérifiée pour tout x dans M. Enfin, $x \in S^k$ entraîne $\phi(x) \in S^k$ par construction. ■

Nous introduisons désormais la condition de finitude (C_3) dans les hypothèses. Notons que, même si M est un monoïde de type fini, les conditions (C_0), (C_1) et (C_2^+) ne garantissent pas (C_3), c'est-à-dire l'existence d'une partie génératrice finie close par $\backslash$: le monoïde de Baumslag–Solitar $\langle a, b\,;\, ab^2 = ba\rangle^+$ est un contre-exemple, car on a alors $a\backslash b^n = b^{2n}$ pour tout n, et la clôture par $\backslash$ de l'ensemble des atomes $\{a, b\}$ est infinie.

D'après le lemme 1.9, si M est un monoïde vérifiant les conditions (C_0), (C_1), (C_2) et (C_3), il existe une partie finie S close par $\backslash$ et $\vee$. En particulier, S admet un ppcm à droite Δ, qui est élément de S, et M vérifie les hypothèses du lemme 2.2.

Lemme 2.3. *Soit M un monoïde vérifiant les conditions (C_0), (C_1), (C_2) et (C_3), et S une partie génératrice finie de M close par $\backslash$ et $\vee$. Soient *, ϕ comme dans le lemme 2.2. Alors les conditions suivantes sont équivalentes :*

(i) Le monoïde M satisfait $(\widetilde{C}_1)$, c'est-à-dire admet la simplification à droite;

(ii) L'application $x \mapsto x^*$ est une permutation de S;

(iii) Il existe m tel que $\phi^m(x) = x$ soit vérifié pour tout x dans S;

(iv) L'application ϕ est un automorphisme de M, et une permutation de S^k pour tout k.

Démonstration. Notons Δ le ppcm à droite de S. Puisque S est fini, (ii) et (iii) sont équivalents, et, puisque ϕ est un endomorphisme, que S engendre M, et que ϕ envoie S^k dans lui-même pour tout k, il en est de même de (ii) et (iv).

Supposons $x, y \in S$ et $x^* = y^*$. On a alors $xx^* = \Delta = yy^* = yx^*$, d'où $x = y$ si M admet la simplification à droite. Donc (i) entraîne l'injectivité de * sur S, donc (ii) puisque S est fini.

Inversement, supposons $xz = yz$. Pour k assez grand, x, y et z sont dans S^k, donc z est un diviseur à gauche de Δ^k, et $xz = yz$ entraîne $x\Delta^k = y\Delta^k$. Par (2.1), on trouve

$$\Delta^k \phi^k(x) = x\Delta^k = y\Delta^k = \Delta^k \phi^k(y),$$

d'où $\phi^k(x) = \phi^k(y)$, et $x = y$ si (iv) est vérifiée. Donc (iv) entraîne (i). ■

Nous supposons désormais, jusqu'à la fin de cette section, que M est un monoïde satisfaisant aux conditions (C_0), (C_1), (C_2), (C_3), et $(\widetilde{C}_1)$, et que S est une partie génératrice finie de M close par $\backslash$ et $\vee$. Gardant les conventions précédentes, nous notons Δ le ppcm à droite de S, et, pour x dans S, nous posons $x^* = x\backslash\Delta$, et nous notons ϕ l'automorphisme de M induit par $x \mapsto x^{**}$.

Lemme 2.4. *(i) Les implications du lemme 2.2(i) sont des équivalences : pour tout k, il y a équivalence entre être diviseur à gauche de Δ^k, être diviseur à droite de Δ^k, et appartenir à S^k.*

(ii) Tout élément de S^k admet au plus $\mathrm{card}(S)^k$ diviseurs à gauche.

(iii) Le monoïde M est atomique, et $x \in S^k$ entraîne $\|x\| \leq \mathrm{card}(S)^k$; en particulier, on a $\|\Delta\| \leq \mathrm{card}(S)$.

(iv) Deux éléments quelconques de M ont un pgcd à gauche. La structure $(M, \vee, \wedge)$ est un treillis, et $(S, \vee, \wedge)$ est un treillis fini de minimum 1 et de maximum Δ.

Démonstration. (i) Par le lemme 2.3, ϕ est un automorphisme de M. Supposons que x divise à gauche Δ^k, soit $xz = \Delta^k$. On a alors

$$\phi^{-k}(z)xz = \phi^{-k}(z)\Delta^k = \Delta^k z,$$

d'où, en simplifiant à droite, $\Delta^k = \phi^{-k}(z)x$, et x divise à droite Δ^k.

(ii) D'après (i), tout diviseur à gauche d'un élément de S^k est lui-même élément de S^k, d'où le résultat puisqu'on a $\mathrm{card}(S^k) \leq \mathrm{card}(S)^k$.

(iii) Supposons $x \in S^k$, et $x = x_1 \cdots x_n$ avec $x_1, \ldots, x_n \neq 1$. Par construction, $x_1 \cdots x_i$ est un diviseur à gauche de x, donc de Δ^k, pour tout i, ce qui entraîne $x_1 \cdots x_i \in S^k$. Les conditions (C_0) et (C_1) entraînent $x_1 \cdots x_i \neq x_1 \cdots x_j$ pour $i \neq j$. On a donc $n \leq \mathrm{card}(S^k) \leq \mathrm{card}(S)^k$, soit $\|x\| \leq \mathrm{card}(S)^k$.

(iv) D'après le lemme 2.4(ii), l'ensemble des diviseurs à gauche de tout élément de M est fini. Donc, pour x, y quelconques dans M, l'ensemble des diviseurs à gauche communs de x et y est fini, et il admet un ppcm à droite, lequel est un pgcd à gauche de x et y par construction. Que $(M, \vee, \wedge)$ soit un treillis est alors standard. Pour S, nous remarquons que, pour $x, y \in S$, l'ensemble des diviseurs à gauche de x et y est inclus dans S et donc que le ppcm à droite de cet ensemble, qui est $x \wedge y$, appartient à S. ■

L'étape suivante consiste à utiliser la dualité $x \mapsto x^*$ pour montrer la symétrie de la structure. Par le lemme 2.3, nous savons que l'application $x \mapsto x^*$ est une permutation de S. Pour x dans S, nous noterons ${}^*x$ l'unique élément de S vérifiant $({}^*x)^* = x$. Alors, pour tout x dans S, nous avons

$$\Delta = x \cdot x^* = {}^*x \cdot x, \tag{2.3}$$

et, donc, ${}^*(x^*) = x$. D'après le lemme 2.2(ii), si x et y sont dans S, x est diviseur à gauche de y si et seulement si y^* est diviseur à droite de x^*, et, par conséquent, x est diviseur à droite de y si et seulement si ${}^*y$ est diviseur à gauche de ${}^*x$.

Lemme 2.5. *(i) Deux éléments quelconques de M admettent un ppcm à gauche et un pgcd à droite.*

(ii) L'ensemble S est clos par les opérations $/$, $\widetilde{\vee}$ et $\widetilde{\wedge}$, et, pour $x, y \in S$, on a

$$x/y = ({}^*x \wedge {}^*y)\backslash {}^*y, \qquad x \mathbin{\widetilde{\vee}} y = ({}^*x \wedge {}^*y)^*, \qquad x \mathbin{\widetilde{\wedge}} y = ({}^*x \vee {}^*y)^*. \tag{2.4}$$

(iii) L'élément Δ est ppcm à gauche de S, et, pour tout x dans S, on a ${}^*x = \Delta/x$.

Démonstration. (i) Soient x, y quelconques dans M. Alors il existe k tel que x et y appartiennent à S^k, ce qui, par le lemme 2.4, entraîne que Δ^k est un multiple à gauche de x et de y. D'après [17, Proposition 2.4], ceci est suffisant pour assurer l'existence d'un ppcm à gauche et d'un pgcd à droite pour x et y

(ii) Par définition, ${}^*x \wedge {}^*y$ est un diviseur à gauche de ${}^*x$ et ${}^*y$, donc $({}^*x \wedge {}^*y)^*$ est un multiple à gauche de x et y, et donc de $x \mathbin{\widetilde{\vee}} y$. Donc, en particulier, $x \mathbin{\widetilde{\vee}} y$ est dans S, et ${}^*(x \vee y)$ est défini. Ensuite, x et y sont des diviseurs à droite de $x \mathbin{\widetilde{\vee}} y$, donc ${}^*(x \mathbin{\widetilde{\vee}} y)$ est un diviseur à gauche de ${}^*x$ et de ${}^*y$, donc de ${}^*x \wedge {}^*y$. Par conséquent, $({}^*x \wedge {}^*y)^*$ est un diviseur à droite de $x \mathbin{\widetilde{\vee}} y$, et nous déduisons $x \mathbin{\widetilde{\vee}} y = ({}^*x \wedge {}^*y)^*$.

On trouve ensuite

$${}^*yy = \Delta = {}^*(x \mathbin{\widetilde{\vee}} y)(x \mathbin{\widetilde{\vee}} y) = ({}^*x \wedge {}^*y)(x/y)y,$$

d'où ${}^*y = ({}^*x \wedge {}^*y)(x/y)$, qui donne $x/y = ({}^*x \wedge {}^*y)\backslash {}^*y$.

L'argument est semblable pour le pgcd à droite. Comme ${}^*x$ et ${}^*y$ sont des diviseurs à gauche de ${}^*x \vee {}^*y$, $({}^*x \vee {}^*y)^*$ est diviseur à droite de x et de y, donc de $x \mathbin{\widetilde{\wedge}} y$. D'un autre côté, $x \mathbin{\widetilde{\wedge}} y$ est un diviseur à droite d'un élément de S, donc il est élément de S. Puisque $x \mathbin{\widetilde{\wedge}} y$ est diviseur à droite de x et y, ${}^*x$ et ${}^*y$ sont diviseurs à gauche de ${}^*(x \mathbin{\widetilde{\wedge}} y)$, donc ${}^*x \vee {}^*y$ est diviseur à gauche de ${}^*(x \mathbin{\widetilde{\wedge}} y)$, et $x \mathbin{\widetilde{\wedge}} y$ est diviseur à droite de $({}^*x \vee {}^*y)^*$.

(iii) On a déjà noté que Δ est multiple à gauche de tout élément de S. Puisque Δ appartient à S, ceci entraîne que Δ est ppcm à gauche de S. Soit x quelconque dans S : on a alors ${}^*xx = {}^*x({}^*x)^* = \Delta = \Delta \mathbin{\widetilde{\vee}} x = (\Delta/x)x$, d'où ${}^*x = \Delta/x$. ■

Nous avons ainsi complété la démonstration de la proposition 2.1. En effet, il s'agissait de montrer qu'un monoïde M comme ci-dessus est un monoïde de Garside. Or, d'après le lemme 2.4(iii), M est atomique; par définition, deux éléments quelconques de M admettent un ppcm à droite; ils admettent un pgcd à gauche par le lemme 2.4(iii), et un ppcm à gauche et un pgcd à droite par le lemme 2.5, donc M est un monoïde gaussien. Enfin, la partie S considérée ci-dessus est finie, elle engendre M, et on a vu qu'elle est close par chacune des opérations $\backslash$, $/$, $\vee$ et $\widetilde{\vee}$. Par la proposition 1.10, on déduit que M est un monoïde de Garside. ■

Les formules de dualité (2.4) sont valables dans tout monoïde de Garside, et elles déterminent les opérations $/$, $\widetilde{\vee}$ et $\widetilde{\wedge}$ en termes de leurs contreparties $\backslash$, $\vee$ et $\wedge$. Ces formules ne s'appliquent qu'aux éléments de l'ensemble S considéré, ce

qui n'est pas une restriction véritable : pour des éléments x, y arbitraires, on peut déterminer les valeurs de x/y, $x \mathbin{\widetilde{\vee}} y$ et $x \mathbin{\widetilde{\wedge}} y$ soit en utilisant une décomposition de x et y en produit d'éléments de S, soit — ce qui est essentiellement équivalent — en remplaçant S par une puissance S^k telle que x et y appartiennent à S^k; on sait alors que l'ensemble S^k a la mêmes propriétés de clôture que S. Nous terminerons cette section par une formule générale exprimant le pgcd de deux éléments arbitraires en termes des opérations de complément $\backslash$ et $/$.

Lemme 2.6. *Soit M un monoïde gaussien. Alors, pour tous x, y dans M, on a*

$$x \vee y = (x \wedge y)\cdot((x\backslash y) \mathbin{\widetilde{\vee}} (y\backslash x)), \tag{2.5}$$

et, donc, $x \wedge y = (x \vee y)/((x\backslash y) \mathbin{\widetilde{\vee}} (y\backslash x))$.

Démonstration. Posons $x' = y\backslash x$, $y' = x\backslash y$, $x'' = x'/y'$, et $y'' = y'/x'$. Par définition, nous avons

$$x \vee y = xy' = yx' \quad \text{et} \quad x' \mathbin{\widetilde{\vee}} y' = x''y' = y''x'.$$

D'après la première égalité, $x \vee y$ est un multiple à gauche de x' et y', donc il existe z vérifiant $x \vee y = z(x' \mathbin{\widetilde{\vee}} y')$. On déduit $xy' = zx''y'$, donc $x = zx''$, et, de même, $y = zy''$. Donc z est un diviseur à gauche de x et y, donc de $x \wedge y$.

Réciproquement, supposons $x = z_1x_1$ et $y = z_1y_1$. On a $z_1x_1y' = z_1y_1x' = x \vee y$, donc $x_1y' = y_1x'$. Il existe donc z'' vérifiant $x_1 = z''x''$ et $y_1 = z''y''$. On déduit $z_1z''x''y' = z_1z''y''x' = x \vee y$, d'où $z_1z'' = z$. Par conséquent, z_1 est un diviseur à gauche de z, et on conclut que z est le pgcd à gauche de x et y. ∎

3. Structure automatique

Nous établissons ici que tout groupe de Garside est bi-automatique (Théorème A de l'introduction), et, de surcroît, que cette structure automatique s'explicite très simplement en termes des opérations de complément.

Dans un premier temps, nous allons construire une forme normale dans tout groupe gaussien (de Garside ou non). Soit M un monoïde quelconque, et S une partie génératrice de M. Alors tout élément de M s'écrit comme produit fini d'éléments de S. L'idée pour obtenir une décomposition distinguée, classique pour les groupes de tresses depuis [18] [2] [20] [19], consiste à pousser les éléments de S par exemple vers la gauche, de sorte que le premier élément soit maximal.

Définition 3.1. Soit M un monoïde, et S une partie de M. Pour $x, y \in M$, on dira que $x \perp_S y$ est vérifié si, pour tout diviseur à gauche s de y appartenant à $S \setminus \{1\}$, on a $xs \notin S$.

Le point crucial de la construction est le résultat suivant, qui est une conséquence immédiate des règles du calcul des compléments :

Lemme 3.2. *Soit M un monoïde vérifiant les conditions (C_0), (C_1) et (C_2), et S une partie de M close par $\backslash$ et $\vee$. Soit $(x_1, \ldots, x_p)$ une suite d'éléments de S vérifiant $x_i \perp_S x_{i+1}$ pour tout i. Alors on a $x_1 \perp_S x_2 \cdots x_p$.*

Démonstration. (Figure 3.1) Supposons $x_1 s_1 \in S$, avec $s_1 \in S$ et $s_1 \neq 1$. Il s'agit de montrer que s_1 n'est pas un diviseur à gauche de $x_2 \cdots x_p$. Posons de proche en proche $s_i = x_i \backslash s_{i-1}$ pour $2 \leq i \leq p$, et montrons par récurrence sur i qu'on a $x_i s_i \in S$, $s_i \in S$ et $s_i \neq 1$. Pour $i = 1$, ce sont les hypothèses posées plus haut. Pour $i \geq 2$, on a $s_i = x_i \backslash s_{i-1}$ et $x_i s_i = x_i \vee s_{i-1}$, d'où $s_i \in S$ et $x_i s_i \in S$, puisque x_i est dans S, s_{i-1} aussi par hypothèse de récurrence, et S est clos par $\backslash$ et $\vee$; par ailleurs, la conjonction de $x_{i-1} s_{i-1} \in S$ et $x_{i-1} \perp_S x_i$ entraîne que s_{i-1} n'est pas un diviseur à gauche de x_i, c'est-à-dire que $x_i \backslash s_{i-1}$, qui est s_i, ne vaut pas 1. On a donc $s_p \neq 1$. Or, par les règles du lemme 1.7, on a $s_p = (x_2 \cdots x_p) \backslash s_1$, et $s_p \neq 1$ signifie donc que s_1 n'est pas un diviseur à gauche de $x_2 \cdots x_p$. ■

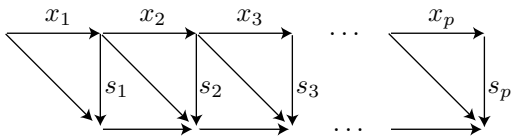


Figure 3.1. Décomposition normale

Proposition 3.3. *Soit M un monoïde gaussien — ou, plus généralement, un monoïde vérifiant (C_0^+), (C_1), et (C_2^+) — et S une partie génératrice de M close par $\backslash$ et $\vee$. Alors tout élément de M possède une unique décomposition $x_1 \cdots x_p$ avec $x_1, \ldots, x_p \in S$ et $x_i \perp_S x_{i+1}$ pour tout i.*

Démonstration. On prouve d'abord l'existence d'une décomposition comme ci-dessus pour tout élément x de M par récurrence sur la norme $\|x\|$. Pour $\|x\| = 0$, on a $x = 1$, et le résultat est vrai. Supposons $x \neq 1$. Notons $\mathrm{Div}(x)$ l'ensemble des diviseurs à gauche de x. Soit x_1 un élément de norme maximale dans $\mathrm{Div}(x)$. Comme $y \in \mathrm{Div}(x)$ entraîne $\|y\| \leq \|x\|$, un tel élément x_1 existe, et, comme $\mathrm{Div}(x)$ contient au moins un atome, on a $x_1 \neq 1$. Ecrivons $x = x_1 x'$. On a alors $\|x'\| \leq \|x\| - \|x_1\| < \|x\|$, donc, par hypothèse de récurrence, x' possède une décomposition $x' = x_2 \cdots x_p$ avec $x_i \in S$ et $x_i \perp_S x_{i+1}$ pour $i \geq 2$. On a alors $x = x_1 x_2 \cdots x_p$, et il s'agit de montrer $x_1 \perp_S x_2$. Soit x un diviseur à gauche propre de x_2 appartenant à S. Alors $x_1 x$ est un diviseur à gauche de $x_1 x_2$, donc de x, et on a $\|x_1 x\| \geq \|x_1\| + \|x\| > \|x_1\|$, ce qui, par définition de x_1, entraîne $x_1 x \notin S$.

Pour l'unicité, il suffit de montrer que, si $(x_1, \ldots, x_p)$ est une suite d'éléments de S vérifiant $x_i \perp_S x_{i+1}$ pour $1 \leq i < p$, alors x_1 est déterminé par le produit $x_1 \cdots x_p$. En effet, puisque M est simplifiable à gauche, une récurrence montre ensuite que x_2, …, x_p sont déterminés de même. Posons $x = x_1 \cdots x_p$. Par construction, x_1 appartient à $\mathrm{Div}(x) \cap S$. Supposons que $x_1 s$ soit un diviseur à gauche de x : alors s est un diviseur à gauche de $x_2 \cdots x_p$, par le lemme 3.2, on a $x_1 \perp_S x_2 \ldots x_p$, et donc on déduit $x_1 s \notin S$. Ceci signifie que x_1 est un élément de norme maximale dans $\mathrm{Div}(x) \cap S$, ce qui détermine x_1 de façon unique, car

$\mathrm{Div}(x) \cap S$ est clos par ppcm à droite et, si x_1 et x_1' étaient deux éléments distincts de norme maximale dans $\mathrm{Div}(x) \cap S$, l'élément $x_1 \vee x_1'$ contredirait cette maximalité. ■

On considère maintenant le cas des monoïdes de Garside. Supposons que M soit un monoïde de Garside. Nous savons que M admet une unique partie génératrice minimale, à savoir l'ensemble A de ses atomes, et que la clôture S de A par $\backslash$ et $\vee$ est la plus petite partie génératrice de M qui soit close par ces opérations. Notons que S est également la clôture de A par les opérations à gauche $/$ et $\widetilde{\vee}$. En effet, d'après le lemme 2.5(ii), l'ensemble S est clos par $/$ et $\widetilde{\vee}$, donc, si $\widetilde{S}$ désigne la clôture de A par $/$ et $\widetilde{\vee}$, nous avons $\widetilde{S} \subseteq S$. Comme les hypothèses sont symétriques, un argument similaire donne $S \subseteq \widetilde{S}$, d'où $S = \widetilde{S}$. On note Δ le ppcm de S, et les opérations de dualité réfèrent au complément dans Δ : pour x dans S, on pose $x^* = x\backslash\Delta$, et ${}^*x = \Delta/x$.

Nous allons appliquer la proposition 3.3 en prenant pour S l'ensemble des éléments simples. En fait, la minimalité n'est requise nulle part, et nous pourrions aussi bien utiliser à la place de S une partie génératrice quelconque qui soit close pour $\backslash$ et $\vee$, en particulier toute partie S^k avec $k \geq 1$.

La condition d'orthogonalité mentionnée dans la construction s'exprime simplement en termes de pgcd.

Lemme 3.4. *Soit M un monoïde de Garside, et S l'ensemble de ses éléments simples. Pour x, y dans S, $x \perp_S y$ équivaut à $x^* \wedge y = 1$.*

Démonstration. On a $x \perp_S y$ si et seulement si, pour tout diviseur à gauche simple s de y distinct de 1, xs n'est pas simple, c'est-à-dire que xs n'est pas un diviseur à gauche de Δ de S, soit encore que s n'est pas un diviseur à gauche de $x\backslash\Delta$, qui est x^*. ■

Proposition 3.5. *Soit M un monoïde de Garside. Tout élément x de M admet une unique décomposition de la forme $x_1 \cdots x_p$ avec $x_1, \ldots, x_p$ simples distincts de 1 et $x_i^* \wedge x_{i+1} = 1$ pour tout i. Pour $x \neq 1$, le premier facteur de la décomposition est $x \wedge \Delta$.*

Démonstration. D'après la proposition 3.3 et le lemme 3.4, seule la dernière assertion reste à démontrer. Supposons $x \neq 1$, et soit $x_1 \cdots x_p$ la décomposition de x donnée par la proposition. Par construction, x_1 est un diviseur à gauche simple de x de norme maximale. Puisqu'il est simple, x_1 est un diviseur à gauche de Δ, donc de $x \wedge \Delta$, et, de là, nous avons $\|x_1\| \leq \|x \wedge \Delta\|$. D'un autre côté, $x \wedge \Delta$ est un diviseur à gauche simple de x, donc, par définition de x_1, on doit avoir $\|x_1\| = \|x \wedge \Delta\|$, d'où $x_1 = x \wedge \Delta$ puisque x_1 est un diviseur à gauche de $x \wedge \Delta$. ■

La forme normale précédente sera appelée forme normale à gauche pour M. De façon symétrique, nous avons une forme normale à droite :

Proposition 3.6. *Soit M un monoïde de Garside. Tout élément x de M admet une unique décomposition de la forme $x_q \cdots x_1$ avec $x_1, \ldots, x_q$ simples et ${}^*x_i \mathbin{\widetilde{\wedge}} x_{i+1} = 1$ pour tout i. Pour $x \neq 1$, le dernier facteur de la décomposition est $x \mathbin{\widetilde{\wedge}} \Delta$.*

Considérons maintenant le cas des groupes de Garside. Il se ramène à celui des monoïdes grâce à l'existence de fractions irréductibles.

Lemme 3.7. *Soit M un monoïde de Garside, et G son groupe de fractions. Alors tout élément z de G admet une unique décomposition $z = x^{-1}y$ avec $x, y \in M$ et $x \wedge y = 1$, et, symétriquement, une unique décomposition $z = x'y'^{-1}$ avec $x', y' \in M$ et $x' \mathbin{\widetilde{\wedge}} y' = 1$.*

Démonstration. Par définition, tout élément z de G admet une décomposition $z = x'^{-1}y'$ avec $x', y' \in M$. Posant $x' = z'x$ et $y' = z'y$ avec $z' = x' \wedge y'$, on a $x \wedge y = 1$ et $z = x^{-1}y$ par construction. Par le lemme 2.6, on obtient $x \vee y = x(x\backslash y) = y(y\backslash x) = (x\backslash y) \mathbin{\widetilde{\vee}} (y\backslash x)$. Supposons alors $z = x''^{-1}y''$ avec $x'', y'' \in M$. De $x^{-1}y = (x\backslash y)(y\backslash x)^{-1}$ on déduit $x''(x\backslash y) = y''(y\backslash x)$, donc, puisque $x(x\backslash y)$ est le ppcm à gauche de $x\backslash y$ et $y\backslash x$, l'existence de z'' vérifiant $x'' = z''x$ et $y'' = z''y$. Alors $x'' \wedge y'' = 1$ entraîne $z'' = 1$, soit $x'' = x$ et $y'' = y$. ■

Définition 3.8. Dans le contexte du lemme précédent, les éléments x et y seront appelés le *dénominateur* et le *numérateur gauches* de z, et notés $D(z)$ et $N(z)$; symétriquement, x' et y' seront appelés numérateurs et dénominateurs à droite, et notés $\widetilde{N}(z)$ et $\widetilde{D}(z)$. Ainsi, pour tout z dans G, on a

$$z = D(z)^{-1}N(z) = \widetilde{N}(z)\widetilde{D}(z)^{-1},$$

avec $D(z) \wedge N(z) = \widetilde{N}(z) \mathbin{\widetilde{\wedge}} \widetilde{D}(z) = 1$.

En rassemblant les éléments, nous obtenons l'existence des formes normales appelées «mixed canonical forms» dans [20, Chap. 9] :

Proposition 3.9. *Soit G le groupe de fractions d'un monoïde de Garside M.*
(i) Tout élément de G admet une unique décomposition de la forme $x_p^{-1} \cdots x_1^{-1} y_1 \cdots y_q$, avec $x_1, \ldots, x_p, y_1, \ldots, y_q$ éléments simples de M vérifiant $x_1 \wedge y_1 = 1$, et, pour tout k, $x_k^* \wedge x_{k+1} = 1$, et $y_k^* \wedge y_{k+1} = 1$.
(ii) Tout élément de G admet une unique décomposition de la forme $x_p \cdots x_1 y_1^{-1} \cdots y_q^{-1}$, avec $x_1, \ldots, x_p, y_1, \ldots, y_q$ éléments simples de M vérifiant $x_1 \mathbin{\widetilde{\wedge}} y_1 = 1$, et, pour tout k, ${}^*x_k \mathbin{\widetilde{\wedge}} x_{k+1} = 1$, et ${}^*y_k \mathbin{\widetilde{\wedge}} y_{k+1} = 1$.

Dans le contexte précédent, nous dirons que la suite $(x_p^{-1}, \ldots, x_1^{-1}, y_1, \ldots, y_q)$ est la forme normale à gauche de l'élément z, et que $(x_p, \ldots, x_1, y_1^{-1}, \ldots, y_q^{-1})$ en est la forme normale à droite.

Nous allons montrer que les formes normales précédentes sont associées à une structure (bi)-automatique. La démonstration est extrêmement simple, qui contraste avec les calculs de [9], repris dans [17]. Les seuls résultats dont nous aurons besoin sont les suivants :

Lemme 3.10. *Soit M un monoïde gaussien.*

(i) Supposons que x' divise à gauche zx, et y' divise à gauche zy. Alors $x' \wedge y'$ divise à gauche $z(x \wedge y)$; donc, en particulier, $x \wedge y = 1$ entraîne $x' \wedge y' = x' \wedge y' \wedge z$.

(ii) Si Δ est un élément de Garside de M, on a $(xy) \wedge \Delta = (x(y \wedge \Delta)) \wedge \Delta$ pour tous x, y dans M.

Démonstration. (i) Par définition, $x' \wedge y'$ divise à gauche zx et zy, donc il divise leur pgcd à gauche, qui est $z(x \wedge y)$. Pour $x \wedge y = 1$, on déduit que $x' \wedge y'$ divise à gauche z, donc $x' \wedge y' \wedge z$.

(ii) Posons $y' = y \wedge \Delta$. Alors $(xy) \wedge \Delta$ est le ppcm à droite des diviseurs de Δ qui divisent à gauche xy, soit $(xy) \wedge \Delta = \bigvee\{s\,;\, \Delta\backslash s = (xy)\backslash s = 1\}$. On a $(xy)\backslash s = y\backslash(x\backslash s)$; or, pour s divisant Δ, $x\backslash s$ divise Δ, donc la condition $y\backslash(x\backslash s) = 1$ dans la formule précédente est équivalente à $y'\backslash(x\backslash s) = 1$, d'où

$$xy \wedge \Delta = \bigvee\{s\,;\, \Delta\backslash s = y\backslash(x\backslash s) = 1\} = \bigvee\{s\,;\, \Delta\backslash s = y'\backslash(x\backslash s) = 1\} = xy' \wedge \Delta. \blacksquare$$

Il est alors très facile de calculer, pour s simple, la forme normale d'un élément $zs^{\pm 1}$ à partir de celle de z. Dans le cas de la forme normale à gauche, il est commode de décrire le passage de la forme normale de z à celle de zs^{-1}, et à celle de $z\Delta$: le passage de z à zs s'en déduit en écrivant $zs = z\Delta(s^*)^{-1}$.

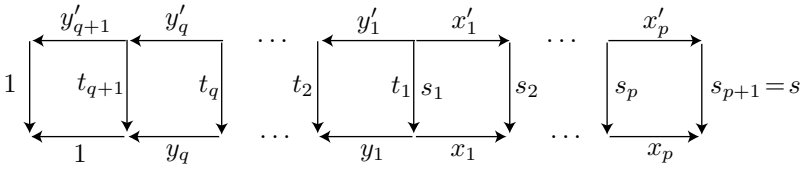
Lemme 3.11. *Soit G le groupe de fractions d'un monoïde de Garside M, et $(y_q^{-1}, \dots, y_1^{-1}, x_1, \dots, x_p)$ la forme normale à gauche d'un élément z de G.*

(i) Pour s simple, la forme normale à gauche de zs^{-1} est $(y'^{-1}_{q+1}, \dots, y'^{-1}_1, x'_1, \dots, x'_p)$, avec $s_{p+1} = s$, puis $x'_i = x_i/s_{i+1}$ et $s_i = s_{i+1}/x_i$ pour $p \geq i \geq 1$, ensuite $t_1 = s_1$, $y'_j = t_j y_j \wedge \Delta$ et $t_{j+1} = y_j\backslash(t_j y_j)$ pour $1 \leq j \leq q$, et, enfin, $y'_{q+1} = t_{q+1}$.

(ii) La forme normale à gauche de $z\Delta$ est $(y_q^{-1}, \dots, y_2^{-1}, y_1^*, x_1^{**}, \dots, x_p^{**})$.

(iii) La forme normale à gauche de $z\Delta^{-1}$ est $(y_q^{-1}, \dots, y_1^{-1}, ({}^*x_1)^{-1}, {}^{**}x_2, \dots, {}^{**}x_p)$.

Démonstration. (i) Par construction, on a $x'_i s_{i+1} = s_i x_i$ pour tout i, et $y'_j t_{j+1} = t_j y_j$ pour tout j, donc le diagramme



commute, et on obtient $y'^{-1}_{q+1} \cdots y'^{-1}_1 x'_1 \cdots x'_p = y_q^{-1} \cdots y_1^{-1} x_1 \cdots x_p s^{-1} = zs^{-1}$. La seule question est de montrer que la suite $(y'^{-1}_{q+1}, \dots, y'^{-1}_1, x'_1, \dots, x'_p)$ est bien une forme normale à gauche. Par construction, tous les facteurs sont simples, et il s'agit de vérifier les conditions de pgcd.

Considérons d'abord le cas de x'_i et x'_{i+1}. Par définition, on a

$$x'_i x'^*_i s_i^{**} = \Delta s_i^{**} = s_i \Delta = s_i x_i x_i^* = x'_i s_{i+1} x_i^*,$$

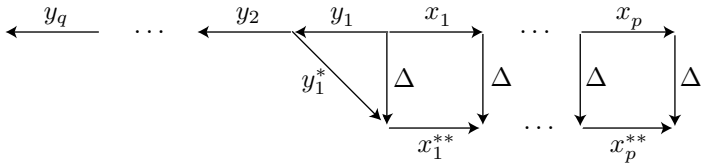
donc $x'^*_i s_i^{**} = s_{i+1} x_i^*$, ce qui montre que x'^*_i est un diviseur à gauche de $s_{i+1} x_i^*$. Par ailleurs, on a $x'_{i+1} s_{i+2} = s_{i+1} x_i$, donc x'_{i+1} est un diviseur à gauche de $s_{i+1} x_{i+1}$.

Comme on a $s_{i+1} \wedge x'_{i+1} = 1$ par construction, et $x_i^* \wedge x_{i+1} = 1$ par hypothèse, le lemme 3.10(i) donne $x_i'^* \wedge x'_{i+1} = 1$, comme souhaité.

Considérons maintenant le cas de y'_1 et x'_1. A nouveau, x'_1 est diviseur à gauche de $s_1 x_1$, et, de même, y'_1 est diviseur à gauche de $s_1 y_1$. On a $s_1 \wedge x'_1 = 1$ par construction, et $x_1 \wedge y_1 = 1$ par hypothèse, d'où $x'_1 \wedge y'_1 = 1$ par le lemme 3.10(i).

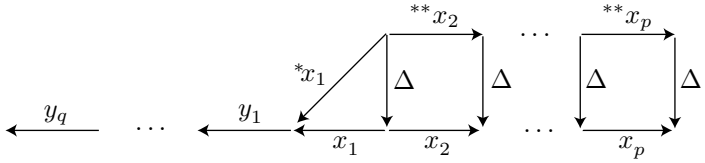
Considérons finalement le cas de y'_j et y'_{j+1}. Par définition, on a $y'_j = t_j y_j \wedge \Delta$. Or, par hypothèse, on a aussi $y_j = (y_j \cdots y_q) \wedge \Delta$. Par le lemme 3.10(ii), on déduit $y'_j = (t_j y_j \cdots y_q) \wedge \Delta = (y'_j y'_{j+1} \cdots y'_{q+1}) \wedge \Delta$, donc, en particulier, $y_j'^* \wedge (y'_{j+1} \cdots y'_{q+1}) = 1$, et, a fortiori, $y_j'^* \wedge y'_{j+1} = 1$.

(ii) On a $x_i \Delta = \Delta x_i^{**}$ pour tout i, et, par ailleurs, $y_1 y_1^* = \Delta$, donc le diagramme



est commutatif, et on obtient $y_q^{-1} \cdots y_2^{-1} y_1^* x_1^{**} \cdots x_p^{**} = z\Delta$. La seule question est à nouveau de montrer que la suite $(y_q^{-1}, \ldots, y_2^{-1}, y_1^*, x_1^{**}, \ldots, x_p^{**})$ est une forme normale à gauche, soit, les facteurs étant clairement simples, de montrer que les conditions de pgcd entre deux termes consécutifs sont vérifiées. Or, pour tout i, on a $(x_i^{**})^* \wedge x_{i+1}^{**} = (x_i^* \wedge x_{i+1})^{**} = 1^{**} = 1$, puisque l'application $x \mapsto x^{**}$ induit un automorphisme de M. Ensuite, on a $y_1^* \wedge y_2 = 1$ par hypothèse, puis, pour $j \geq 2$, $y_j^* \wedge y_{j+1} = 1$, toujours par hypothèse.

(iii) L'argument est similaire. On a cette fois ${}^{**}x_i \Delta = \Delta x_i$ pour tout i, et ${}^*x_1 x_1 = \Delta$, d'où le diagramme commutatif



qui donne $y_q^{-1} \cdots y_1^{-1} ({}^*x_1)^{-1} {}^{**}x_2 \cdots {}^{**}x_p = z\Delta^{-1}$. Il s'agit encore de vérifier les conditions de pgcd entre termes voisins : pour tout i, on a $({}^{**}x_i)^* \wedge {}^{**}x_{i+1} = {}^{**}(x_i^* \wedge x_{i+1}) = {}^{**}1 = 1$, et, enfin, $({}^*x_1)^* \wedge y_1 = x_1 \wedge y_1 = 1$. ■

Proposition 3.12. *Tout groupe de Garside est bi-automatique.*

Démonstration. Soit M un monoïde de Garside, et G son groupe de fractions. Soit S l'ensemble des éléments simples de M. Considérons le langage L formé par les formes normales à gauche, considérées comme mots sur l'alphabet $S \cup S^{-1}$. D'abord L est un langage régulier, car l'appartenance d'un mot à L est définie par des conditions locales consistant en une liste (finie) de lettres permises après chaque lettre : après une lettre négative y^{-1}, les lettres autorisées sont les lettres positives x vérifiant $x \wedge y = 1$, et les lettres négatives y'^{-1} vérifiant $y'^* \wedge y = 1$; après une lettre positive x, les lettres autorisées sont les lettres positives x' vérifiant $x^* \wedge x' = 1$.

Ensuite la formule explicite du lemme 3.11(i) montre que la distance entre la forme normale d'un élément z et celle de zs^{-1} est uniformément bornée par 2 (en

termes de l'alphabet S), ce qui établit la propriété du 2-compagnon de route — ou «2-fellow traveller property» . On déduit que le langage des formes normales à gauche est associé à une structure automatique.

Enfin, la symétrie de la forme normale entraîne une propriété de compagnon de route similaire pour la multiplication à gauche, et donc le langage L est associé à une structure bi-automatique. ■

A côté du résultat d'existence précédent, qui ne décrit pas explicitement les automates mis en jeu, nous allons maintenant construire des automates très simples calculant les formes normales. Nous considérerons ici seulement le cas des monoïdes. Le cas des groupes n'est pas directement couvert par cette approche, mais les algorithmes décrits à la section 4 montrent comment se ramener à des fractions irréductibles, et, de là, du groupe au monoïde.

Le cas de la forme normale à droite est le plus facile, et la solution est une extension naturelle de celle décrite dans [20, chapitre 9] pour les groupes de tresses. Nous allons décrire un automate fini d'alphabet A et d'ensemble d'états S calculant le dernier facteur de la forme normale à droite, au sens où l'état final obtenu après lecture d'un mot u par l'automate est $\overline{u} \mathbin{\widetilde{\wedge}} \Delta$, où $\overline{u}$ désigne la classe du mot u dans le monoïde. On rappelle qu'un tel automate est la donnée d'une fonction $T : S \times A \to S$ et d'un état initial q; l'état final de l'automate après lecture du mot u est, par définition, l'état $T(q, u)$ défini inductivement, en notant ε le mot vide, par $T(q, \varepsilon) = q$ et $T(q, ux) = T(T(q, u), x)$. On part de formules de calcul de pgcd.

Lemme 3.13. *Soit M un monoïde de Garside. Pour s, t simples, on a*

$$st \wedge \Delta = {}^{*}(t^{*}/s^{**}), \qquad \text{et} \qquad st \mathbin{\widetilde{\wedge}} \Delta = ({}^{**}t \backslash {}^{*}s)^{*}. \tag{3.1}$$

Démonstration. La forme normale à gauche de s est (s), donc, par le lemme 3.11(ii), celle de $s\Delta$ est (Δ, s^{**}), et celle de st, qui est $s\Delta(t^{*})^{-1}$, est $({}^{*}(t^{*}/s^{**}), s^{**}/t^{*})$. Or, par définition, le premier terme de cette suite est $st \wedge \Delta$.

Un argument symétrique montre que la forme normale à droite de Δt est $({}^{**}t, \Delta)$, et que celle de st est $({}^{*}s \backslash {}^{**}t, ({}^{**}t \backslash {}^{*}s)^{*})$. Par définition, le dernier terme de cette dernière suite est $st \mathbin{\widetilde{\wedge}} \Delta$. ■

Proposition 3.14. *Soit M un monoïde de Garside, A l'ensemble de ses atomes, S l'ensemble de ses simples, et Δ l'élément simple maximal. Définissons $T : S \times A \to S$ par $T(s, a) = ({}^{**}a \backslash {}^{*}s)^{*}$. Alors, pour tout mot u sur A, on a $\overline{u} \mathbin{\widetilde{\wedge}} \Delta = T(1, u)$, c'est-à-dire que le résultat de la lecture de u par l'automate $(T, 1)$ est le dernier terme de la forme normale à droite de $\overline{u}$.*

Démonstration. On a trivialement $\overline{\varepsilon} \mathbin{\widetilde{\wedge}} \Delta = 1 = T(1, \varepsilon)$, donc, pour montrer le résultat inductivement, il suffit de démontrer l'égalité

$$xa \mathbin{\widetilde{\wedge}} \Delta = T(x \mathbin{\widetilde{\wedge}} \Delta, a)$$

pour x dans M et a dans A. Par le lemme 3.10(ii) (en fait, sa contrepartie pour le pgcd à droite), on a $(xa) \mathbin{\widetilde{\wedge}} \Delta = ((x \mathbin{\widetilde{\wedge}} \Delta)a) \mathbin{\widetilde{\wedge}} \Delta$. Comme $x \mathbin{\widetilde{\wedge}} \Delta$ et a sont simples, le résultat découle alors immédiatement de la formule (3.1). ■

Remarque. Comme dans [20], nous pouvons considérer un transducteur, défini comme un automate muni d'une fonction de sortie O envoyant $S \times A$ dans l'ensemble des mots sur A. On définit alors la sortie produite par la lecture du mot u comme le mot $O(q,u)$ inductivement défini par $O(q,\varepsilon) = \varepsilon$ et $O(q,ua) = O(q,u)O(T(q,u),a)$. La démonstration précédente montre que, si nous posons $O(s,a) = {}^*s\backslash^{**}a$, alors, pour tout mot u sur A, on a $\overline{u} = \overline{O(1,u)}\cdot T(1,u)$: c'est dire que le mot $O(1,u)$ représente le reste du mot u lorsque le dernier terme de la forme normale à droite a été retiré. En faisant lire par le transducteur le mot $O(1,u)$, on obtiendra de même l'avant-dernier terme de la forme normale à droite de $\overline{u}$, et ainsi de suite. Cette itération fournit un algorithme de complexité quadratique déterminant la forme normale à droite.

Exemple 3.15. La figure 3.1 représente le transducteur calculant la forme normale à droite pour le monoïde $\langle a,b\,;\, aba = b^2\rangle^+$. Les états (domaines cerclés) correspondent aux éléments simples. Les flèches pleines représentent la lecture de a, les tiretées la lecture de b; la présence d'une étiquette u sur une flèche x entre les états s et t signifie qu'on a $T(s,x) = t$ et $O(s,x) = u$, c'est-à-dire que, partant de l'état s et lisant la lettre x, on passe dans l'état t en produisant le mot u.

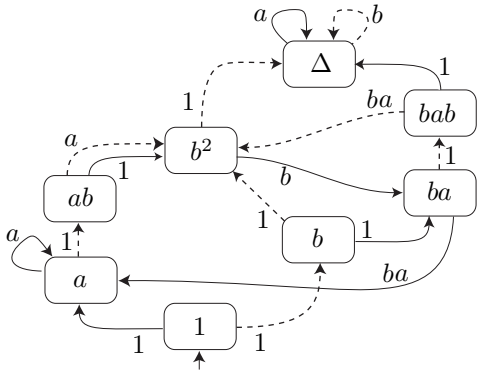


Figure 3.2. Transducteur pour $\langle a,b\,;\, aba = b^2\rangle^+$

Pour la forme normale à gauche, nous pouvons trivialement obtenir des résultats analogues en considérant des pseudo-automates lisant les mots de droite à gauche, mais la véritable question est l'existence d'automates standard lisant de gauche à droite. L'approche précédente échoue, car il est en général faux que la valeur de $(xa)\wedge\Delta$ ne dépende que des valeurs de $x\wedge\Delta$ et de a : dans le groupe de tresses B_3, on a $\sigma_1\sigma_2 \wedge \Delta = \sigma_1\sigma_2^2 \wedge \Delta = \sigma_1\sigma_2$, mais $\sigma_1\sigma_2\sigma_1 \wedge \Delta = \Delta \neq \sigma_1\sigma_2^2\sigma_1 \wedge \Delta = \sigma_1\sigma_2$. Par contre, la construction est encore possible en prenant comme ensemble d'états l'ensemble P^P, où P est l'ensemble des éléments primitifs à droite de M, c'est-à-dire la clôture des atomes par l'opération $\backslash$.

Proposition 3.16. *Soit M un monoïde de Garside, A l'ensemble de ses atomes, et P l'ensemble de ses éléments primitifs à droite. Définissons $T : P^P \times A \to P^P$ par*

$$T(f,a) = r_a \circ f \tag{3.2}$$

où r_a est définie pour $a \in A$ et $p \in P$ par $r_a(p) = a\backslash p$. Alors, pour tout mot u sur A, on a

$$\overline{u} \wedge \Delta = \bigvee \{p \in P\,;\, T(\mathrm{id}, u)(p) = 1\}$$

— et donc l'automate (T, id) détermine le premier facteur de la forme normale à gauche de $\overline{u}$.

Démonstration. Pour x dans M, notons f_x l'application de P dans P définie par $f_x(p) = x\backslash p$. On a $f_1 = \mathrm{id}$ par définition, et, d'après les formules des compléments, il vient, pour $x \in M$, $a \in A$ et $p \in P$,

$$f_{xa}(p) = (xa)\backslash p = a\backslash(x\backslash p) = a\backslash f_x(p) = r_a(f_x(p)),$$

soit $f_{xa} = r_a \circ f_x$, et, inductivement, $f_{\overline{u}} = T(\mathrm{id}, u)$ pour tout mot u sur A. Or, pour p primitif, p est un diviseur à gauche de x si et seulement si on a $x\backslash p = 1$, soit $f_x(p) = 1$. Le seul point à montrer est donc que $x \wedge \Delta$ est égal au ppcm à droite x' des éléments primitifs divisant x à gauche. Or, tout élément primitif est simple, donc x' est un diviseur à gauche de $x \wedge \Delta$. Inversement, $x \wedge \Delta$ est simple, donc, d'après les résultats de la section 1, il est un ppcm à droite d'élements primitifs, lesquels sont nécessairement des diviseurs à gauche de x. ■

Remarque. L'approche précédente s'applique également à la forme normale à droite. Introduisons l'ensemble $\widetilde{P}$ des éléments *primitifs à gauche* comme la clôture des atomes par l'opération $/$. Pour $x \in M$, définissons $\widetilde{f}_x : \widetilde{P} \to \widetilde{P}$ par $\widetilde{f}_x(p) = p/x$. Alors la fonction $\widetilde{f}_x$ est calculée inductivement par la règle $\widetilde{f}_{xa}(p) = \widetilde{f}_x(p/a)$. On obtient donc $\widetilde{f}_{\overline{u}} = \widetilde{T}(\mathrm{id}, u)$, où $\widetilde{T} = \widetilde{P}^{\widetilde{P}} \times A \to \widetilde{P}^{\widetilde{P}}$ est déterminée par

$$\widetilde{T}(f, a) = f \circ \widetilde{r}_a, \tag{3.3}$$

avec $r_a : p \mapsto p/a$, formule qui est la contre-partie exacte de (3.2). On obtient alors, pour tout mot u sur A,

$$\overline{u} \mathbin{\widetilde{\wedge}} \Delta = \widetilde{\bigvee} \{p \in \widetilde{P}\,;\, \widetilde{T}(\mathrm{id}, u)(p) = 1\} :$$

l'automate $(\widetilde{T}, \mathrm{id})$ détermine le dernier facteur de la forme normale à droite de $\overline{u}$. Ces résultats montrent à nouveau le rôle central des opérations $\backslash$ et $/$: les automates précédents sont essentiellement la table de ces opérations sur les clôtures des atomes.

Exemple 3.17. La figure 3.2 montre l'automate calculant le pgcd à gauche avec Δ dans le cas du monoïde de tresses B_3^+, de présentation $\langle a, b\,;\, aba = bab\rangle^+$. Il y a deux atomes, à savoir a et b, et cinq éléments primitifs à droite (et à gauche), à savoir $1, a, b, ab, ba$. On obtient un automate à 20 états, représenté sur la figure 3.2 (les flèches en plein représentent a, les flèches en tireté représentent b).

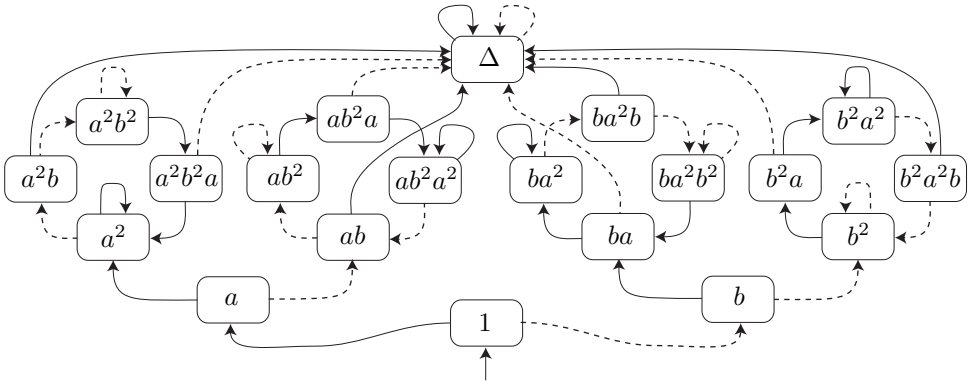


Figure 3.2. Automate pour le pgcd à gauche dans B_3

4. Présentations

On montre ici que tout groupe de Garside admet une présentation d'un certain type, dit complémenté, et que toutes les opérations du monoïde se calculent à partir d'une telle présentation au moyen d'une opération combinatoire appelée redressement de mots. Les résultats du début de la section figurent, avec des notations différentes, dans [17], auquel nous renvoyons pour d'autres détails et les démonstrations manquantes.

Pour tout ensemble Σ, nous noterons $\mathrm{Mo}(\Sigma)$ l'ensemble des mots sur Σ, c'est-à-dire le monoïde libre de base Σ; le mot vide est noté ε. Si Σ est une partie génératrice d'un monoïde M, alors, par définition, tout élément x de M admet des décompositions comme produit d'éléments de Σ : pour w dans $\mathrm{Mo}(\Sigma)$, on notera comme précédemment $\overline{w}$ l'image x de w dans M; on dira alors que w est une expression de x, et que x est l'évaluation de w dans M.

Définition 4.1. Soit M un monoïde vérifiant les conditions (C_0), (C_1) et (C_2), et Σ est une partie génératrice de M. On appelle *sélecteur de ppcm* sur Σ toute application (partielle) f de $\Sigma \times \Sigma$ dans $\mathrm{Mo}(\Sigma)$ tel que, pour $a, b \in \Sigma$, $f(a, b)$ est une expression de $a\backslash b$ lorsque ce dernier existe.

Par définition, on a $a\backslash a = 1$ pour tout a dans Σ, donc, si f est un sélecteur de ppcm sur Σ, et si M satisfait à la condition (C_0), c'est-à-dire n'admet pas d'inversible autre que 1, alors, nécessairement, $f(a, a)$ est le mot vide ε. Par ailleurs, par définition, $a\backslash b$ existe si et seulement si $b\backslash a$ existe, et, par conséquent, le domaine de tout sélecteur de ppcm est un sous-ensemble symétrique de $\Sigma \times \Sigma$.

Définition 4.2. Soit Σ un ensemble non vide. On appelle *fonction de redressement* sur Σ une application partielle de $\Sigma\times\Sigma$ dans $\mathrm{Mo}(\Sigma)$ vérifiant $f(a, a) = \varepsilon$ pour tout a, et telle que le domaine de f est symétrique. On note alors R_f la famille des relations $af(a, b) = bf(b, a)$ pour $(a, b) \in \mathrm{Dom}(f)$, et $\equiv_f^+$ la congruence sur $\mathrm{Mo}(\Sigma)$ engendrée par R_f. On dit qu'une présentation de monoïde est *complémentée* si elle est associée à une (nécessairement unique) fonction de redressement.

Proposition 4.3. [17] *Soit M un monoïde gaussien — ou, plus généralement, un monoïde vérifiant les conditions (C_0^+), (C_1) et (C_2). Soit Σ une partie génératrice quelconque de M, et f un sélecteur de ppcm sur Σ. Alors f est une fonction de redressement sur Σ et $\langle \Sigma\,;\, R_f\rangle^+$ est une présentation complémentée de M.*

Démonstration. Notons $\sim$ la congruence sur $\mathrm{Mo}(\Sigma)$ telle que M est $\mathrm{Mo}(\Sigma)/\sim$. Par définition d'un sélecteur de ppcm, on a $af(a,b) \sim bf(b,a)$ pour $a, b \in \mathrm{Dom}(f)$, donc $u \equiv_f^+ v$ entraîne $u \sim v$ puisque les paires $\{af(a,b), bf(b,a)\}$ engendrent $\equiv_f^+$.

Réciproquement, nous montrons que $u \sim v$ entraîne $u \equiv_f^+ v$ par récurrence sur $\|\overline{u}\|$. Pour $\|\overline{u}\| = 0$, on a $\overline{u} = \overline{v} = 1$, donc, par (C_0), $u = v = \varepsilon$, et $u \equiv_f^+ v$. Supposons $u, v \neq \varepsilon$. On écrit $u = au_1$, $v = bv_1$, avec $a, b \in \Sigma$. L'hypothèse $\overline{u} = \overline{v}$ signifie que $\overline{u}$ est un multiple commun à droite de a et b. Par (C_2), il existe un mot w vérifiant $\overline{u} = \overline{v} = (a \vee b)\overline{w}$, d'où $u = au_1 \sim af(a,b)w \sim bf(b,a)w \sim bv_1 = v$. Par (C_1), on déduit $u_1 \sim f(a,b)w$ et $v_1 \sim f(b,a)w$. Or, par (C_0^+), on a $\|\overline{f(a,b)w}\| \leq \|\overline{u}\| - \|a\| < \|\overline{u}\|$, et, de même, $\|\overline{f(b,a)w}\| < \|\overline{u}\|$. Appliquant l'hypothèse de récurrence, on déduit $u_1 \equiv_f^+ f(a,b)w$, et $v_1 \equiv_f^+ f(b,a)w$, d'où $u = au_1 \equiv_f^+ af(a,b)w \equiv_f^+ bf(b,a)w \equiv_f^+ bv_1 = v$, et donc $u \equiv_f^+ v$. ∎

Question 4.4. *Le résultat précédent reste-t-il valable lorsque la condition (C_0^+) (atomicité) est affaiblie en (C_0) (pas d'inversible autre que 1) ?*

Si M est un monoïde gaussien, Σ une partie génératrice de M, et f un sélecteur de ppcm sur Σ, alors toutes les opérations de M se calculent à partir de f de façon effective. Pour le démontrer, nous introduisons une opération combinatoire sur les mots appelée *redressement* («reversing» en anglais).

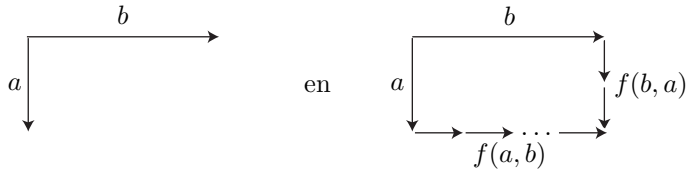
Par définition, si f est un sélecteur de ppcm sur Σ, le mot $f(a,b)$ est une expression de l'élément $a\backslash b$ de M pour tous a, b dans Σ. L'idée est d'étendre l'application f en une opération binaire partielle notée $\backslash_f$ sur $\mathrm{Mo}(\Sigma)$ de sorte que, pour tous mots u, v sur Σ, le mot $u\backslash_f v$ soit une expression du complément $\overline{u}\backslash\overline{v}$, quand ce dernier existe.

Dans toute la suite, lorsque Σ est un alphabet, nous introduirons une copie disjointe notée a^{-1} pour chaque lettre a de Σ, et nous noterons Σ^{-1} l'ensemble des lettres a^{-1}. Pour tout mot w sur $\Sigma \cup \Sigma^{-1}$, on note w^{-1} le mot obtenu en échangeant chaque lettre a avec la lettre a^{-1} correspondante, et en renversant l'ordre des lettres. Ainsi, si G est un groupe engendré par Σ et si le mot w représente l'élément x de G, alors w^{-1} représente x^{-1}.

Définition 4.5. [13] [17] Soit f une fonction de redressement sur Σ. Pour w, w' mots sur $\Sigma \cup \Sigma^{-1}$, on dit que w est *f-redressable* en w', noté $w \to_f w'$, si on peut passer de w à w' en un nombre fini d'étapes consistant à remplacer un sous-mot de la forme $a^{-1}b$ avec $a, b \in \Sigma$ par le mot $f(a,b)f(b,a)^{-1}$ correspondant. Pour u, v mots sur Σ, on définit $u\backslash_f v$ comme l'unique mot u' sur Σ tel qu'il existe un mot v' sur Σ vérifiant $u^{-1}v \to_f v'u'^{-1}$, s'il existe, et $u \vee_f v$ comme $u{\cdot}(u\backslash_f v)$.

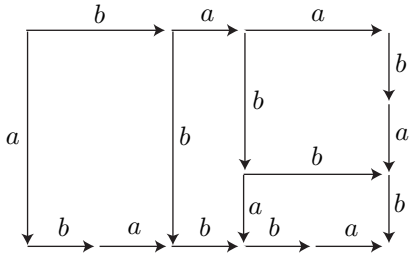
On associe à chaque redressement de mot un graphe planaire (voisin d'un diagramme de Dehn) composé de flèches verticales et horizontales étiquetées par des

éléments de Σ, et tel que le redressement du mot $a^{-1}b$ en $f(a,b)f(b,a)^{-1}$ se traduit par la fermeture du motif



Nous renvoyons à [16, chapitre II], et considérons ici simplement un exemple.

Exemple 4.6. Soit $\Sigma = \{a, b\}$, et soit f l'application de Σ^2 dans $\mathrm{Mo}(\Sigma)$ définie par $f(a,b) = ba$, $f(b,a) = b$, $f(a,a) = f(b,b) = \varepsilon$. Le monoïde $\langle \Sigma\,;\, R_f\rangle^+$ est ici $\langle a, b\,;\, aba = b^2\rangle^+$. La figure ci-dessous illustre le redressement du mot $a^{-1}ba^2$ en le mot $bab^2ab^{-1}a^{-1}b^{-1}$, qui donne donc $a\backslash_f ba^2 = bab^2a$ et $ba^2\backslash_f a = bab$.



L'opération $\backslash_f$ est en général une opération partielle sur $\mathrm{Mo}(\Sigma)$, non nécessairement définie pour tous les mots : comme $\backslash_f$ coïncide avec f sur $\Sigma \times \Sigma$, c'est le cas si f n'est pas partout définie sur $\Sigma \times \Sigma$, mais, même si f est partout définie, il se peut que le redressement d'un mot ne se termine pas en un nombre fini d'étapes. Comme dans la section 1, nous noterons $u\backslash_f v = \perp$ quand $u\backslash_f v$ n'existe pas, et nous étendons $\backslash_f$ en une opération partout définie sur $\mathrm{Mo}(\Sigma) \cup \{\perp\}$ en posant $u\backslash_f \perp = \perp\backslash_f u = \perp\backslash_f \perp = \perp$ pour tout u, et de même pour le produit des mots. De même, nous étendons $\equiv_f^+$ en une congruence sur $\mathrm{Mo}(\Sigma) \cup \{\perp\}$ en déclarant $\perp \equiv_f^+ \perp$ vrai, et $u \equiv_f^+ \perp$ faux pour tout u dans $\mathrm{Mo}(\Sigma)$.

Lemme 4.7. [13] *Soit f une fonction de redressement sur Σ. Alors, pour tous mots u, v sur Σ, on a $u(u\backslash_f v) \equiv_f^+ v(v\backslash_f u)$.*

D'après nos conventions, le résultat précédent signifie que soit $u\backslash_f v$ et $v\backslash_f u$ sont définis et on a l'équivalence annoncée, soit ni l'un ni l'autre n'est défini. La démonstration est une induction facile sur le nombre d'étapes élémentaires de redressement.

Proposition 4.8. [17] *Soit M un monoïde gaussien — ou, plus généralement, un monoïde vérifiant les conditions (C_0^+), (C_1) et (C_2) —, Σ une partie génératrice de M, et f un sélecteur de ppcm sur Σ. Alors, pour tous mots u, v dans $\mathrm{Mo}(\Sigma)$, le mot $u\backslash_f v$ existe dans $\mathrm{Mo}(\Sigma)$ si et seulement si l'élément $\overline{u}\backslash\overline{v}$ existe dans M, et, dans ce cas, $u\backslash_f v$ est une expression de $\overline{u}\backslash\overline{v}$, et $u \vee_f v$ est une expression de $\overline{u} \vee \overline{v}$.*

Démonstration. Le lemme 4.7 montre que, si $u\backslash_f v$ est défini, alors la classe de $u \vee_f v$ est un multiple à droite commun des classes de u et v, donc, par (C_2), le ppcm à droite de ces classes existe.

Inversement, montrons par induction sur n que, si u et v sont deux mots tels que $\overline{u} \vee \overline{v}$ existe et qu'on ait $\|\overline{u} \vee \overline{v}\| = n$, alors $u\backslash_f v$ existe et représente $\overline{u}\backslash\overline{v}$. Pour $n = 0$, on a $u = v = \varepsilon$, et les résultats ont triviaux. Supposons $n \geq 1$. Pour $u = \varepsilon$ ou $v = \varepsilon$, les résultats sont à nouveau triviaux. Supposons $u = au_1$ et $v = bv_1$ avec $a, b \in \Sigma$, et soit $z = \overline{u} \vee \overline{v}$. Par hypothèse, z est multiple à droite commun à a et b, donc $f(a,b)$ et $f(b,a)$ sont définis. Ensuite z est multiple à droite commum de $\overline{au_1}$ et $\overline{af(a,b)}$, donc $\overline{u_1}$ et $\overline{f(a,b)}$ ont un multiple à droite commun, donc un ppcm à droite. Or, par construction, on a $\|\overline{u_1} \vee \overline{f(a,b)}\| \leq \|z\| - \|\overline{a}\| = n - 1$, donc, par hypothèse de récurrence, $u_1\backslash_f f(a,b)$ existe et il représente $\overline{u_1}\backslash\overline{f(a,b)}$. De même, $v_1\backslash_f f(b,a)$ existe et représente $\overline{v_1}\backslash\overline{f(b,a)}$; finalement, en posant $u_2 = f(a,b)\backslash_f u_1$ et $v_2 = f(xy,a)\backslash_f v_1$, on a de même que $u_2\backslash_f v_2$ existe et représente $\overline{u_2}\backslash\overline{v_2}$. Donc $u\backslash_f v$ est défini, et il représente

$$(\overline{v_1}\backslash\overline{f(b,a)})\cdot((\overline{f(b,a)}\backslash\overline{v_1})\backslash(\overline{f(a,b)}\backslash\overline{u_1})),$$

lequel est, d'après les formules de complément, $\overline{u}\backslash\overline{v}$. ■

Définition 4.9. Soit f une fonction de redressement sur Σ. Pour u, v mots sur Σ, on dit que $u \equiv_f^{++} v$ est vérifié si on a $u\backslash_f v = v\backslash_f u = \varepsilon$, c'est-à-dire $u^{-1}v \to_f \varepsilon$. On étend $\equiv_f^{++}$ de sorte que $\bot \equiv_f^{++} \bot$ soit vrai, et $u \equiv_f^{++} \bot$ et $\bot \equiv_f^{++} u$ faux pour tout mot u.

Par le lemme 4.7, $u \equiv_f^{++} v$ entraîne $u \equiv_f^{+} v$. Dans le cas d'un monoïde gaussien, la proposition 4.8 affirme que cette implication est une équivalence. Nous allons en déduire une solution pour le problème de mot du monoïde par redressement, et, pour celui du groupe associé, par double redressement. On notera $\equiv_f$ la congruence sur $\mathrm{Mo}(\Sigma \cup \Sigma^{-1})$ engendrée par $\equiv_f^{+}$ et les paires $\{aa^{-1}, \varepsilon\}$ et $\{a^{-1}a, \varepsilon\}$ pour a dans Σ, de sorte que le groupe $\langle \Sigma\,;\, R_f\rangle$ est $\mathrm{Mo}(\Sigma \cup \Sigma^{-1})/\equiv_f$. Remarquons que, par construction, $w \to_f w'$ entraîne $w \equiv_f w'$ pour tous w, w' mots sur $\Sigma \cup \Sigma^{-1}$.

Proposition 4.10. *Soit M un monoïde gaussien — ou, plus généralement, un monoïde vérifiant les conditions (C_0^+), (C_1) et (C_2) —, Σ une partie génératrice de M, et f un sélecteur de ppcm sur Σ.*

(i) Deux mots u, v sur Σ représentent le même élément de M si et seulement on a $u \equiv_f^{++} v$, c'est-à-dire $u^{-1}v \to_f \varepsilon$.

(ii) Supposons que M vérifie de surcroît la condition (C_2^+), et soit G le groupe de fractions de M. Alors un mot w sur $\Sigma \cup \Sigma^{-1}$ représente 1 dans G si et seulement si il existe deux mots u, v sur Σ vérifiant $w \to_f uv^{-1}$ et $u^{-1}v \to_f \varepsilon$.

Démonstration. (i) Par le lemme 4.7, la condition est suffisante. Inversement, $\overline{u} = \overline{v}$ entraîne $\overline{u}\backslash\overline{v} = \overline{v}\backslash\overline{u} = 1$, d'où $u\backslash_f v = v\backslash_f u = \varepsilon$ par la proposion 4.8.

(ii) La condition est suffisante, car $w \to_f w'$ entraîne $w \equiv_f w'$. Inversement, supposons $w \to_f uv^{-1}$. Alors $w \equiv_f \varepsilon$ entraîne $u \equiv_f v$, donc $u \equiv_f^{+} v$ puisque M se plonge dans G, d'où $u^{-1}v \to_f \varepsilon$ par (i). ■

Si M est un monoïde gaussien, les opérations $\backslash$ et $\vee$ de M se déterminent par redressement à partir de tout sélecteur de ppcm. Le pgcd, ainsi que les opérations symétriques de ppcm à gauche et de pgcd à droite, peuvent également être calculées à l'aide de redressements, à condition d'introduire, à côté d'un sélecteur à droite associé au ppcm à droite comme ci-dessus, une notion symétrique de sélecteur à gauche et de redressement à gauche : supposant Σ partie génératrice de M, on appellera *sélecteur de ppcm à gauche* sur Σ une application $\widetilde{f}$ de $\Sigma \times \Sigma$ dans $\mathrm{Mo}(\Sigma)$ telle que, pour tous a, b dans Σ, $\widetilde{f}(a,b)$ représente l'élément a/b, s'il existe. Si $\widetilde{f}$ est une fonction de redressement sur Σ, et si w, w' sont deux mots sur $\Sigma \cup \Sigma^{-1}$, on dira que w est $\widetilde{f}$-redressable à gauche en w', noté $w \mathrel{\widetilde{\rightarrow}_{\widetilde{f}}} w'$, si on peut passer de w à w' en un nombre fini d'étapes consistant à remplacer un factuer du type ab^{-1} avec $a, b \in \Sigma$ par le facteur $\widetilde{f}(b,a)^{-1}\widetilde{f}(a,b)$ correspondant. Les résultats sont alors symétriques : introduisant $u /\!\!_{\widetilde{f}}\, v$ comme l'unique mot u' tel qu'il existe v' vérifiant $uv^{-1} \mathrel{\widetilde{\rightarrow}_{\widetilde{f}}} v'^{-1}u'$, et $u \mathbin{\widetilde{\vee}_{\widetilde{f}}} v$ comme $(u /\!\!_{\widetilde{f}}\, v)\cdot v$, on obtient que $u /\!\!_{\widetilde{f}}\, v$ représente l'élément $\overline{u}/\overline{v}$, et $u \mathbin{\widetilde{\vee}_{\widetilde{f}}} v$ l'élément $\overline{u} \mathbin{\widetilde{\vee}} \overline{v}$. On déduit alors du lemme 2.6 :

Proposition 4.11. *Soit M un monoïde gaussien, Σ une partie génératrice de M, et f et $\widetilde{f}$ respectivement un sélecteur de ppcm à droite et à gauche sur Σ. Alors, pour tous mots u, v sur Σ, le mot $(u \vee_f v) /\!\!_{\widetilde{f}}\, ((u\backslash_f v) \mathbin{\widetilde{\vee}_{\widetilde{f}}} (v\backslash_f u))$ représente $\overline{u} \wedge \overline{v}$.*

On obtient donc le pgcd à gauche de $\overline{u}$ et $\overline{v}$ par un triple redressement : on redresse à droite $u^{-1}v$ en $v'u'^{-1}$, qu'on redresse à gauche en $u''^{-1}v''$, et un représentant du pgcd à gauche de $\overline{u}$ et $\overline{v}$ est obtenu en redressant à gauche le mot uu''^{-1}. Les opérations du groupe de fractions se calculent de façon semblable. En particulier, dénominateurs et numérateurs se déterminent par double redressement.

Proposition 4.12. *Soit G le groupe de fractions d'un monoïde gaussien M, Σ une partie génératrice de M, et f et $\widetilde{f}$ respectivement un sélecteur de ppcm à droite et à gauche sur Σ. Soit z un élément quelconque de G, et w un mot sur $\Sigma \cup \Sigma^{-1}$ représentant z. Soient u, v, u', v' les mots sur Σ vérifiant $w \rightarrow_f vu^{-1} \mathrel{\widetilde{\rightarrow}_{\widetilde{f}}} u'^{-1}v'$. Alors u' représente $D(z)$, et v' représente $N(z)$.*

Démonstration. Par construction, on a $z = \overline{u'}^{-1}\overline{v'}$, donc, d'après le lemme 3.7, il suffit de montrer $\overline{u'} \wedge \overline{v'} = 1$. Or, par construction, on a $u' = u /\!\!_{\widetilde{f}}\, v$ et $v' = v /\!\!_{\widetilde{f}}\, u$: si $\overline{u'}$ et $\overline{v'}$ avaient un diviseur à gauche non trivial commun, $u'v$ et $v'u$ ne pourraient représenter un ppcm à gauche de $\overline{u}$ et $\overline{v}$. ∎

Comme $z = 1$ équivaut à $D(z) = N(z) = 1$, nous en déduisons une solution alternative du problème de mot.

Corollaire 4.13. *Sous les mêmes hypothèses, un mot w sur $\Sigma \cup \Sigma^{-1}$ représente 1 dans G si, et seulement si, il existe deux mots u, v sur Σ vérifiant $w \rightarrow_f uv^{-1} \mathrel{\widetilde{\rightarrow}_{\widetilde{f}}} \varepsilon$.*

Enfin, le lemme 3.11 montre comment calculer par redressement la forme normale (à gauche) de tout élément d'un groupe de Garside : supposant que $(\overline{v_q}^{-1}, \ldots, \overline{v_1}^{-1}, \overline{u_1}, \ldots, \overline{u_p})$ soit la forme normale de z, on obtient la forme normale de $z\Delta$ en déterminant les éléments $\overline{u_i}^{**}$, donc par double redressement

face à un mot représentant Δ. Pour w représentant un élément simple, on obtient le numérateur de la forme normale de $z\overline{w}^{-1}$ en redressant à gauche le mot $u_1 \cdots u_p w^{-1}$; le dénominateur s'obtient alors par une succession de calculs de pgcd, donc également par redressement. Noter que le lemme 3.13 permet de déterminer successivement chaque facteur du dénominateur à l'aide d'un unique redressement.

5. Reconnaître les monoïdes de Garside

Nous avons vu dans la section précédente que tout monoïde de Garside admet une présentation complémentée $\langle \Sigma; R_f \rangle^+$, où f est une fonction de redressement sur Σ, et qu'alors toutes les opérations du monoïde et celles de son groupe de fractions se déterminent par f-redressement. Nous abordons ici la question réciproque de reconnaître quand une présentation complémentée définit un monoïde de Garside.

Le fait d'admettre une présentation complémentée est une hypothèse faible, et des conditions sur la fonction de redressement considérée doivent être ajoutées pour que le monoïde associé ait de bonnes propriétés. Nous allons établir une liste de conditions nécessaires vérifiées par tout sélecteur de ppcm dans un monoïde de Garside, puis montrer que ces conditions sont suffisantes. Nous partirons (une fois encore) des propriétés de l'opération $\backslash$.

Lemme 5.1. *Soit M un monoïde gaussien — ou, plus généralement, un monoïde vérifiant les conditions (C_0), (C_1) et (C_2). Alors, pour tous x, y, z dans M, on a*

$$(x\backslash y)\backslash(x\backslash z) = (y\backslash x)\backslash(y\backslash z). \tag{5.1}$$

Démonstration. D'après le lemme 1.7, le membre de gauche dans (5.1) est égal à $(x \vee y)\backslash z$, et celui de droite à $(y \vee x)\backslash z$: comme $\vee$ est une opération commutative, les deux sont égaux. Par ailleurs, si l'une des expressions n'est pas définie, il en est de même de l'autre. ■

Lemme 5.2. *Soit M un monoïde gaussien — ou, plus généralement, un monoïde vérifiant les conditions (C_0^+), (C_1) et (C_2) —, Σ une partie génératrice quelconque de M, et f un sélecteur de ppcm sur Σ. Alors, pour tous mots u, v, w dans $\mathrm{Mo}(\Sigma)$, on a*

$$(u\backslash_f v)\backslash_f(u\backslash_f w) \ \equiv_f^{++} \ (v\backslash_f u)\backslash_f(v\backslash_f w). \tag{5.2}$$

Démonstration. Compte tenu de la proposition 4.8, la formule (5.2) est la traduction directe de la formule (5.1). ■

Définition 5.3. Soit f une fonction de redressement sur Σ.

(i) Pour $X \subseteq \mathrm{Mo}(\Sigma) \cup \{\perp\}$, on dit que f a la *propriété du cube* (*resp.* la *propriété du cube faible*) sur X si la relation (5.2) (*resp.* la relation

$$(u\backslash_f v)\backslash_f(u\backslash_f w) \ \equiv_f^{+} \ (v\backslash_f u)\backslash_f(v\backslash_f w) \ ) \tag{5.3}$$

est vérifiée pour tous u, v, w dans X.

(ii) On dit que f vérifie la condition $(*)$ s'il existe une partie finie X de $\mathrm{Mo}(\Sigma)$ qui est close par $\backslash_f$, c'est-à-dire telle que, pour tous u, v dans X, $u\backslash_f v$ existe et appartient à X, et si, de plus, la clôture $X^\vee$ de X par $\vee_f$ est finie et il existe Ω dans $X^\vee$ tel que, pour tout u dans $X^\vee$, on ait $\Omega\backslash_f u = \varepsilon$ et il existe v dans $X^\vee$ vérifiant $v\backslash_f\Omega \equiv_f^{++} u$.

Affirmer que f a la propriété du cube sur un triplet $\{u, v, w\}$ signifie, lorsque tous les mots mis en jeu sont définis, que le cube représenté sur la figure 5.1 se ferme au sens où, partant des trois arêtes étiquetées u, v, w et utilisant le redressement de mots pour construire les six faces, le redressement des trois petites faces triangulaires restantes se termine avec des mots vides.

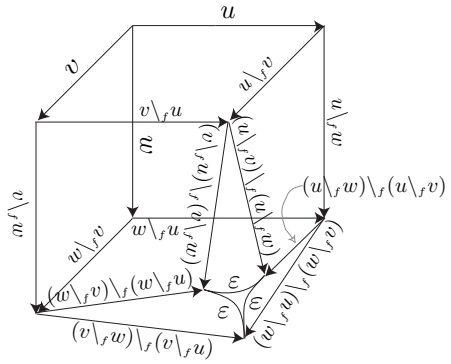


Figure 5.1. Propriété du cube

Proposition 5.4. *Soit M un monoïde de Garside, Σ une partie génératrice finie de M, et f un sélecteur de ppcm sur Σ. Alors la fonction f a la propriété du cube sur* $\mathrm{Mo}(\Sigma)$ *et elle vérifie la condition* $(*)$.

Démonstration. Le lemme 5.2 exprime que f a la propriété du cube sur $\mathrm{Mo}(\Sigma)$. Notons X l'ensemble des expressions des éléments primitifs à droite de M. Comme Σ est fini, et que la longueur des expressions dans $\mathrm{Mo}(\Sigma)$ de chaque élément x de M est bornée supérieurement par $\|x\|$, l'ensemble X est fini. Supposons $u, v \in X$. Par la proposition 4.8, le mot $u\backslash_f v$ est une expression de $\overline{u}\backslash\overline{v}$: comme $\overline{u}$ et $\overline{v}$ sont primitifs à droite, il en est de même de $\overline{u}\backslash\overline{v}$, et $u\backslash_f v$ appartient à X. Donc X est clos par $\backslash_f$.

Par le même raisonnement, l'ensemble Y des expressions des éléments simples de M est un ensemble fini de mots qui est clos par les opérations $\backslash_f$ et $\vee_f$, et qui inclut X. Par conséquent, la clôture $X^\vee$ de X par $\vee_f$ est finie, et elle contient au moins une expression pour chaque élément simple de M. Soit Ω une expression quelconque de l'élément Δ dans $X^\vee$. Pour tout mot u dans $X^\vee$, le mot $\Omega\backslash_f u$ représente $\Delta\backslash\overline{u}$, qui est 1, et on a donc nécessairement $\Omega\backslash_f u = \varepsilon$. Inversement, si Ω vérifie $\Omega\backslash_f u = \varepsilon$ pour tout u dans $X^\vee$, Ω représente nécesairement Δ, puisqu'il représente un élément qui est un multiple de tous les éléments simples.

D'après la proposition 2.1, l'application $s \mapsto s\backslash\Delta$ est surjective sur les simples de M. Donc, pour tout mot u dans $X^\vee$, il doit exister un élément simple s vérifiant

$\overline{u} = s\backslash\Delta$. Cet élément s a au moins une expression v dans $X^\vee$, et la condition $\overline{u} = \overline{v}\backslash\Delta$ entraîne $u \equiv_f^{++} v\backslash_f\Omega$. Par conséquent, la condition $(*)$ est vérifiée. ■

Nous allons maintenant montrer que les conditions nécessaires de la proposition 5.4 sont aussi suffisantes, et, pour cela, utiliser la caractérisation de la proposition 2.1 en termes des conditions (C_i). La condition (C_0) est gratuite.

Lemme 5.5. *Soit f une fonction de redressement sur Σ. Alors le monoïde $\langle\Sigma\,;\,R_f\rangle^+$ satisfait à la condition (C_0), c'est-à-dire n'a d'autre inversible que* 1.

Démonstration. Par construction, $u \equiv_f^+ \varepsilon$ n'est possible que pour $u = \varepsilon$. ■

Le point crucial est le résultat suivant, qui montre l'importance de la propriété du cube.

Proposition 5.6. *Soit f une fonction de redressement sur Σ. Alors les conditions suivantes sont équivalentes :*

(i) La fonction f a la propriété du cube sur $\mathrm{Mo}(\Sigma)$*;*

(ii) Les relations $\equiv_f^+$ et $\equiv_f^{++}$ coïncident;

(iii) La relation $\equiv_f^+$ est compatible avec l'opération $\backslash_f$, au sens où la conjonction de $u' \equiv_f^+ u$ et $v' \equiv_f^+ v$ entraîne $u'\backslash_f v' \equiv_f^+ u\backslash_f v$.

Démonstration. Supposons (i), et montrons (ii). Par le lemme 4.7, la relation $\equiv_f^{++}$ est toujours incluse dans la relation $\equiv_f^+$. Pour prouver l'inclusion réciproque, puisque, par définition, $\equiv_f^+$ est la relation d'équivalence engendrée par les paires $(uaf(a,b)v, ubf(b,a)v)$ avec $a, b \in \Sigma$ et $u, v \in \mathrm{Mo}(\Sigma)$, il suffit de montrer qu'on a $uaf(a,b)v \equiv_f^{++} ubf(b,a)v$, soit

$$v^{-1}f(b,a)^{-1}b^{-1}u^{-1}uaf(a,b)v \to_f \varepsilon,$$

ce qui est trivial, et que $\equiv_f^{++}$ est une relation d'équivalence. Réflexivité et symétrie sont claires, et seule la transitivité fait problème. Supposons $u \equiv_f^{++} v \equiv_f^{++} w$. Par hypothèse, les mots $v\backslash_f u$, $u\backslash_f v$, $v\backslash_f w$ et $w\backslash_f v$ existent et sont vides. Donc $(v\backslash_f u)\backslash_f(v\backslash_f w)$ existe, et il est vide. Comme f a la propriété du cube sur $\{v, u, w\}$, ceci entraîne $(u\backslash_f v)\backslash_f(u\backslash_f w) \equiv_f^+ \varepsilon$, donc $(u\backslash_f v)\backslash_f(u\backslash_f w) = \varepsilon$. L'existence du mot $(u\backslash_f v)\backslash_f(u\backslash_f w)$ entraîne en particulier celle de $u\backslash_f w$. De plus, $u\backslash_f v = \varepsilon$ entraîne $(u\backslash_f v)\backslash_f(u\backslash_f w) = u\backslash_f w$. Nous avons donc $u\backslash_f w = \varepsilon$. Un argument symétrique donne $w\backslash_f u = \varepsilon$, donc $u \equiv_f^{++} w$. Donc $\equiv_f^{++}$ est transitive, et (i) entraîne (ii).

Supposons maintenant (ii), et montrons (iii). Puisque la relation $\equiv_f^+$ est symétrique et transitive, il suffit de montrer que, si $u\backslash_f v$ existe et qu'on a $v' \equiv_f^+ v$, alors $u\backslash_f v'$ existe aussi et on a $u\backslash_f v' \equiv_f^+ u\backslash_f v$ et $v'\backslash_f u \equiv_f^+ v\backslash_f u$. Or, sous ces hypothèse, le lemme 4.7 entraîne $u(u\backslash_f v) \equiv_f^+ v(v\backslash_f u)$, donc $u(u\backslash_f v) \equiv_f^+ v'(v\backslash_f u)$, soit, par (ii), $u(u\backslash_f v) \equiv_f^{++} v'(v\backslash_f u)$, et donc $(v'(v\backslash_f u))\backslash_f(u(u\backslash_f v)) = \varepsilon$. Ceci entraîne en particulier $(v'(v\backslash_f u))\backslash_f u = \varepsilon$, soit, par (1.4),

$$(v\backslash_f u)\backslash_f(v'\backslash_f u) = \varepsilon. \tag{5.4}$$

Nous déduisons que $v'\backslash_f u$, et, par conséquent, $u\backslash_f v'$, existent. Comme v et v' jouent maintenant des rôles symétriques, le calcul précédent donne $(v'\backslash_f u)\backslash_f(v\backslash_f u) = \varepsilon$, ce qui, conjugué à (5.4), démontre $v'\backslash_f u \equiv_f^{++} v\backslash_f u$, donc $v'\backslash_f u \equiv_f^{+} v\backslash_f u$. Un calcul semblable donne $(u\backslash_f v)\backslash_f(u\backslash_f v') = \varepsilon$ et $(u\backslash_f v')\backslash_f(u\backslash_f v) = \varepsilon$, d'où $u\backslash_f v \equiv_f^{++} u'\backslash_f v$, et, finalement $u\backslash_f v \equiv_f^{+} u'\backslash_f v$. Donc (ii) implique (iii).

On sait que $u' \equiv_f^{++} u$ entraîne $u' \equiv_f^{+} u$. Inversement, supposons $u' \equiv_f^{+} u$. Par construction, on a $u^{-1}u \to_f \varepsilon$, c'est-à-dire $u\backslash_f u = \varepsilon$. Si (iii) est vraie, on déduit que $u' \equiv_f^{+} u$ entraîne l'existence de $u\backslash_f u'$ et $u'\backslash_f u$, et qu'on a $u'\backslash_f u \equiv_f^{+} u\backslash_f u = \varepsilon$, et $u\backslash_f u' \equiv_f^{+} u\backslash_f u = \varepsilon$, soit $u' \equiv_f^{++} u$. Ceci montre que (iii) entraîne (ii).

Finalement, supposons (ii) et (iii), et soient u, v, w des mots quelconques sur Σ. Si $u\backslash_f v$ n'est pas défini, $v\backslash_f u$ ne l'est pas non plus, et $(u\backslash_f v)\backslash_f(u\backslash_f w)$ et $(v\backslash_f u)\backslash_f(v\backslash_f w)$ sont tous deux $\perp$, donc (5.2) est vraie. Supposons que $u\backslash_f v$ et $v\backslash_f u$ soient définis. Par (1.4), on a $(u\backslash_f v)\backslash_f(u\backslash_f w) = (u(u\backslash_f v))\backslash_f w$ et $(v\backslash_f u)\backslash_f(v\backslash_f w) = (v(v\backslash_f u))\backslash_f w$. Supposons $(u(u\backslash_f v))\backslash_f w$ défini. Par le lemme 4.7, on a $u(u\backslash_f v) \equiv_f^{+} v(v\backslash_f u)$, donc $u\,(u\backslash_f v) \equiv_f^{+} v\,(v\backslash_f u)$. Alors (iii) entraîne que $(v(v\backslash_f u))\backslash_f w$ est également défini, et qu'on a $(v(v\backslash_f u))\backslash_f w \equiv_f^{+} (u(u\backslash_f v))\backslash_f w$. Par (ii), on déduit $(v(v\backslash_f u))\backslash_f w \equiv_f^{++} (u(u\backslash_f v))\backslash_f w$, donc en particulier $((u(u\backslash_f v))\backslash_f w)\backslash_f((v(v\backslash_f u))\backslash_f w) = \varepsilon$. Un calcul symétrique donne $((v(v\backslash_f u))\backslash_f w)\backslash_f((u(u\backslash_f vu))\backslash_f w) = \varepsilon$, d'où $(u(u\backslash_f v))\backslash_f w \equiv_f^{++} (v(v\backslash_f u))\backslash_f w$, qui est la condition (5.2) pour u, v, w. Donc (ii) et (iii) entraînent (i). ■

Il est alors facile d'établir les conditions (C_1) et (C_2).

Lemme 5.7. *Soit f une fonction de redressement sur Σ ayant la propriété du cube sur* $\mathrm{Mo}(\Sigma)$. *Alors le monoïde $\langle \Sigma\,;\, R_f\rangle^+$ satisfait à la condition (C_1), c'est-à-dire admet la simplification à gauche.*

Démonstration. Soit M le monoïde $\langle \Sigma\,;\, R_f\rangle^+$. Supposons $\overline{u}\,\overline{v} = \overline{u}\,\overline{v'}$ dans M, soit $uv \equiv_f^{+} uv'$. Par la proposition 5.6, on a $uv \equiv_f^{++} uv'$, c'est-à-dire $(uv)^{-1}(uv') \to_f \varepsilon$. Par construction, on a $(uv)^{-1}(uv') \to_f v^{-1}v'$, donc, par unicité du résultat du redressement, $v^{-1}v' \to_f \varepsilon$, soit $v \equiv_f^{++} v'$, qui entraîne $v \equiv_f^{+} v'$, et $\overline{v} = \overline{v'}$. ■

Lemme 5.8. *Soit f une fonction de redressement sur Σ ayant la propriété du cube sur* $\mathrm{Mo}(\Sigma)$. *Alors, quels que soient les mots u, v sur Σ, il y a équivalence entre*

(i) les mots $u\backslash_f v$ et $v\backslash_f u$ sont définis;

(ii) les éléments $\overline{u}$ et $\overline{v}$ admettent un multiple à droite commun dans le monoïde $\langle \Sigma; R_f\rangle^+$.

Dans ce cas, $\overline{u}$ et $\overline{v}$ admettent un ppcm à droite, à savoir $\overline{u \vee_f v}$, et $u\backslash_f v$ représente $\overline{u}\backslash\overline{v}$.

Démonstration. Supposons (i). Par le lemme 4.7, on a $u(u\backslash_f v) \equiv_f^{+} v(v\backslash_f u)$, et la classe commune de ces deux mots est un multiple à droite commun pour les classes de u et v. Donc (ii) est vérifiée.

Inversement, supposons (ii). Il existe des mots u' et v' vérifiant $uv' \equiv_f^{+} vu'$. Puisque f a la propriété du cube, ceci implique $uv' \equiv_f^{++} vu'$ par la proposition 5.6,

soit ${v'}^{-1}u^{-1}vu' \to_f \varepsilon$. Ainsi, le redressement du mot ${v'}^{-1}u^{-1}vu'$ converge, et, *a fortiori*, celui du sous-mot $u^{-1}v$ converge aussi, ce qui est dire que les mots $u\backslash_f v$ et $v\backslash_f u$ existent, et on a (i). De plus, l'hypothèse ${v'}^{-1}u^{-1}vu' \to_f \varepsilon$ implique l'existence de mots u'', v'' satisfaisant

$$ {v'}^{-1}(u\backslash_f v) \to_f {v''}^{-1}, \quad (v\backslash_f u)^{-1}u' \to_f u'', \quad {v''}^{-1}u'' \to_f \varepsilon. $$

Ainsi, $\overline{u}'$ est un multiple à droite de la classe de $v\backslash_f u$, et, donc, $\overline{vu'}$ est un multiple à droite de la classe de $v \vee_f u$: cette dernière est donc ppcm à droite de $\overline{u}$ et $\overline{v}$. ■

Lemme 5.9. *Soit f une fonction de redressement sur Σ ayant la propriété du cube sur* $\mathrm{Mo}(\Sigma)$. *Alors le monoïde $\langle \Sigma ; R_f \rangle^+$ satisfait à la condition (C_2) : toute paire d'éléments ayant un multiple à droite commun admet un ppcm à droite.*

Démonstration. Supposons que $\overline{u}$ et $\overline{v}$ admettent un multiple à droite commun dans M. Par le lemme 5.8, les mots $u\backslash_f v$ et $v\backslash_f u$ sont définis, et $u \vee_f v$ et $v \vee_f u$ représentent un ppcm à droite de $\overline{u}$ et $\overline{v}$. ■

Nous passons à la condition (C_3).

Lemme 5.10. *Soit f une fonction de redressement sur Σ, telle qu'il existe une partie X de* $\mathrm{Mo}(\Sigma)$ *close par $\backslash_f$. Alors le f-redressement converge toujours, et donc l'opération $\backslash_f$ est partout définie sur* $\mathrm{Mo}(\Sigma)$. *De plus, si le redressement de tout mot $u^{-1}v$ avec $u, v \in X$ requiert au plus k étapes et se termine avec un mot de longueur au plus ℓ, alors le redressement d'un mot quelconque sur $\Sigma \cup \Sigma^{-1}$ requiert au plus $\frac{1}{4}k \cdot \lg(w)^2$ étapes, et il se termine avec un mot de longueur au plus $\ell \cdot \lg(w)$.*

Démonstration. Soit w un mot sur $\Sigma \cup \Sigma^{-1}$. Ecrivons $w = u_1^{e_1} \cdots u_r^{e_r}$ avec $u_i \in X$, $e_i = \pm 1$ pour chaque i, et $r \leq \lg(w)$. Soit p le nombre d'exposants e_i positifs. Un argument inductif illustré sur la figure 5.2 montre qu'il existe des mots v_1, ..., v_r dans X tels que w soit f-redressable en $v_1 \cdots v_p v_{p+1}^{-1} \cdots v_r^{-1}$, et que le redressement se décompose en $p(r-p)$ redressements de mots de la forme $w_1^{-1}w_2$ avec w_1, w_2 dans X. Les bornes en résultent, puisqu'on a toujours $p(r-p) \leq r^2/4$. ■

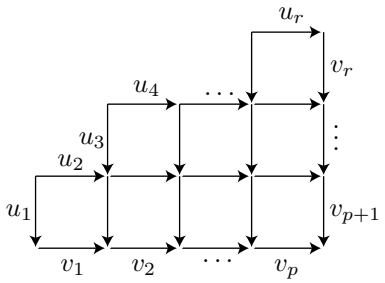


Figure 5.2. Convergence du redressement

Lemme 5.11. *Soit f une fonction de redressement sur Σ, ayant la propriété du cube sur* $\mathrm{Mo}(\Sigma)$*, et telle que f satisfasse à la condition* $(*)$*. Alors le monoïde $\langle \Sigma\,;\, R_f\rangle^+$ satisfait à la condition* (C_3)*.*

Démonstration. Soit X la clôture de Σ par l'opération $\backslash_f$. D'après le lemme 5.10, l'opération $\backslash_f$ est partout définie sur $\langle \Sigma\,;\, R_f\rangle^+$. Il résulte du lemme 5.8 que l'ensemble des éléments du monoïde représentés par un mot de X est clos par l'opération $\backslash$, et qu'il engendre le monoïde puisqu'il inclut Σ. ■

Finalement, nous déduisons la réciproque de la proposition 5.4 :

Proposition 5.12. *Soit f une fonction de redressement sur Σ, ayant la propriété du cube sur* $\mathrm{Mo}(\Sigma)$*, et satisfaisant à la condition* $(*)$*. Alors le monoïde $\langle \Sigma\,;\, R_f\rangle^+$ est un monoïde de Garside, et, donc, le groupe $\langle \Sigma\,;\, R_f\rangle$ est un groupe de Garside.*

Démonstration. Par la proposition 2.1, il suffit d'établir que le monoïde $\langle \Sigma\,;\, R_f\rangle^+$ satisfait aux conditions (C_0), (C_1), (C_2), (C_3) et $(\widetilde{C}_1)$. Les quatre premières conditions résultent des lemmes 5.5, 5.7, 5.9 et 5.11. Enfin, pour $(\widetilde{C}_1)$, d'après le lemme 2.3, il suffit d'établir la surjectivité de l'application $x \mapsto x^*$ sur les éléments simples; compte tenu de la correspondance entre opération $\backslash$ sur M et opération $\backslash_f$ sur $\mathrm{Mo}(\Sigma)$, et entre égalité dans M et $\equiv_f^{++}$-equivalence dans $\mathrm{Mo}(\Sigma)$ due à la satisfaction par f de la prioriété du cube, la condition $(*)$ donne le résultat. ■

6. Critères pour la propriété du cube

La propriété du cube pour la fonction f est primordiale pour l'étude du monoïde $\langle \Sigma\,;\, R_f\rangle^+$: si elle n'est pas satisfaite, on ne sait essentiellement rien dire, alors que, si elle l'est, on peut contrôler la divisibilité et l'égalité à l'aide de redressements de mots et, en particulier, établir assez simplement l'éventuel caractère petit gaussien du monoïde. Il est donc crucial de savoir reconnaître si une fonction de redressement donnée satisfait ou non la propriété du cube.

Si f est une fonction de redressement sur un ensemble (fini) Σ, et u, v, w des mots sur Σ, établir la propriété du cube en u, v, w se fait de façon effective à l'aide de redressements. Plus précisément, il existe un processus consistant en une suite finie de redressements tel que, si la condition est vérifiée, alors le processus se termine en un nombre fini d'étapes et il donne une preuve de la condition cherchée. Cette situation, plus faible que la décidabilité puisqu'il se peut, si la condition n'est pas vérifiée, qu'on n'obtienne pas de réponse en un temps fini, est typique d'une condition récursivement énumérable — ou semi-décidable, ou Σ_1^0 [3].

Considérons maintenant la propriété du cube sur l'ensemble $\mathrm{Mo}(\Sigma)$ entier : comme il existe une infinité de triplets de mots dans $\mathrm{Mo}(\Sigma)$, énumérer ceux-ci systématiquement et vérifier la condition pour chacun d'eux ne permet pas d'établir, même de façon théorique, la propriété en un nombre fini d'étapes. On ne peut obtenir un critère effectif que si on sait par avance que la propriété du cube sur un certain sous-ensemble fini de $\mathrm{Mo}(\Sigma)$ entraîne la propriété du cube partout.

Nous rappellons d'abord deux résultats partiels dans cette direction obtenus antérieurement. Le premier est implicite dans la preuve de Garside que le monoïde des tresses B_n^+ satisfait aux conditions (C_1) et (C_2).

Proposition 6.1. [13] [15] *Soit f une fonction de redressement sur Σ telle que le monoïde $\langle \Sigma\,;\, R_f\rangle^+$ satisfasse (C_0^+). Alors f a la propriété du cube sur* $\mathrm{Mo}(\Sigma)$ *si et seulement si elle a la propriété du cube sur Σ, si et seulement si elle a la propriété du cube faible sur Σ.*

Le critère précédent s'applique aux présentations standards des groupes d'Artin, la condition (C_0^+) étant vérifiée puisque les relations préservent la longueur : les résultats de [5] montrent alors la propriété du cube sur les générateurs. Il en est de même pour les présentations de groupe considérés dans [7] : elles sont associées à des fonctions de redressement f telles que $f(a,b)$ n'est défini que pour a dans A et b dans B, $\{A,B\}$ étant une partition de l'ensemble des générateurs : la propriété du cube sur les lettres est triviale car tout triplet contient nécessairement deux lettres de A, ou deux lettres de B, pour lesquelles aucun redressement n'est possible; les groupes ainsi présentés ne sont pas gaussiens, puisque, dans le monoïde associé, deux éléments de A, ou de B, n'ont pas de multiple commun.

Mis à part de tels cas, il est en général difficile d'établir la condition (C_0^+), et aucune méthode uniforme n'est connue — voir [23] pour un exemple mettant en jeu l'algorithme de Knuth-Bendix.

Un autre critère pour la propriété du cube est établi dans [15], à partir d'une définition alternative de celle-ci :

Lemme 6.2. *Soit f une fonction de redressement sur Σ, et X une partie de* $\mathrm{Mo}(\Sigma)$. *Alors f a la propriété du cube sur X si et seulement si on a*

$$w\backslash_f(u(u\backslash_f v)) \equiv_f^+ w\backslash_f(v(v\backslash_f u)), \quad \text{et} \quad (u(u\backslash_f v))\backslash_f w \equiv_f^+ (v(v\backslash_f u))\backslash_f w \tag{6.1}$$

pour tous u, v, w dans X.

Démonstration. La relation (1.4) donne $(u\backslash_f v)\backslash_f(u\backslash_f w) = (u(u\backslash_f v))\backslash_f w$ et $(v\backslash_f u)\backslash_f(v\backslash_f w) = (v(v\backslash_f u))\backslash_f w$, donc (5.2) est équivalente à la seconde des relations (6.1). Pour la première, en utilisant (1.4) et le lemme 4.7, et en supposant (5.2) satisfaite pour (u,w,v) et pour (w,v,u), on obtient

$$\begin{aligned} w\backslash_f(u(u\backslash_f v)) &= (w\backslash_f u)\cdot((u\backslash_f w)\backslash_f(u\backslash_f v)) \\ &\equiv_f^+ (w\backslash_f u)\cdot((w\backslash_f u)\backslash_f(w\backslash_f v)) \\ &\equiv_f^+ (w\backslash_f v)\cdot((w\backslash_f v)\backslash_f(w\backslash_f u)) \\ &\equiv_f^+ (w\backslash_f v)\cdot((v\backslash_f w)\backslash_f(v\backslash_f u)) = w\backslash_f(v(v\backslash_f u)). \end{aligned}$$

■

Définition 6.3. Soit f une fonction de redressement sur Σ, et X une partie de $\mathrm{Mo}(\Sigma)$. Pour $u \equiv_f^+ v$, définissons $d_f(u,v)$ comme le nombre minimal de R_f-relations nécessaires pour transformer u en v. On dit alors que f est *k-cohérente* sur X si, pour tous u,v,w dans X, on a

$$d_f(w\backslash_f u(u\backslash_f v), w\backslash_f v(v\backslash_f u)) + d_f((u(u\backslash_f v))\backslash_f w, (v(v\backslash_f u))\backslash_f w) \le k \tag{6.2}$$

Par définition, si X est fini, et si f a la propriété du cube (faible) sur X, alors elle est k-cohérente pour un certain k. Un critère suffisant mais non nécessaire est :

Proposition 6.4. [15] *Si f est une fonction de redressement sur Σ qui est* 1*-cohérente sur Σ, alors f a la propriété du cube sur* $\mathrm{Mo}(\Sigma)$.

Le critère de la proposition 6.4 est automatiquement vérifié dans le cas de deux générateurs, mais il l'est rarement dans le cas général.

Nous allons maintenant établir un nouveau critère, qui s'applique dans tous les cas et ne nécessite aucune vérification préalable.

Proposition 6.5. *Soit f une fonction de redressement sur Σ, et X une partie de* $\mathrm{Mo}(\Sigma) \cup \{\perp\}$ *qui inclut Σ et est close par $\backslash_f$. Alors f a la propriété du cube sur* $\mathrm{Mo}(\Sigma)$ *si, et seulement si, elle a la propriété du cube sur X.*

Il est évident que la condition est nécessaire, et tout le travail consiste à montrer qu'elle est suffisante. La démonstration est décomposée en plusieurs étapes. Jusqu'à la fin de la section, nous supposons que f est une fonction de redressement fixé sur Σ, que X est une partie de $\mathrm{Mo}(\Sigma) \cup \{\perp\}$ qui inclut Σ et est close par $\backslash_f$, et que f a la propriété du cube sur X. D'après la proposition 5.6, il suffit que nous montrions la compatibilité de l'opération $\backslash_f$ et de la relation $\equiv_f^+$.

Lemme 6.6. *Pour $u, v, v' \in X$, la relation $v' \equiv_f^{++} v$ entraîne $v'\backslash_f u \equiv_f^{++} v\backslash_f u$ et $u\backslash_f v' \equiv_f^{++} u\backslash_f v$.*

Démonstration. Suppsons que $v\backslash_f u$ existe. Par hypothèse, nous avons $v'\backslash_f v = v\backslash_f v' = \varepsilon$. Comme f a la propriété du cube sur $\{v, v', u\}$, nous déduisons

$$v'\backslash_f u = \varepsilon\backslash_f(v'\backslash_f u) = (v'\backslash_f v)\backslash_f(v'\backslash_f u) \equiv_f^{++} (v\backslash_f v')\backslash_f(v\backslash_f u) = \varepsilon\backslash_f(v\backslash_f u) = v\backslash_f u.$$

Ceci entraîne en particulier que $v'\backslash_f u$ et donc $u\backslash_f v'$ existent. Utilisant la propriété du cube en $\{u, v, v'\}$, nous trouvons

$$(u\backslash_f v)\backslash_f(u\backslash_f v') \equiv_f^{++} (v\backslash_f u)\backslash_f(v\backslash_f v') = (v\backslash_f u)\backslash_f \varepsilon = \varepsilon,$$

qui entraîne $(u\backslash_f v)\backslash_f(u\backslash_f v') = \varepsilon$. On obtient $(u\backslash_f v')\backslash_f(u\backslash_f v) = \varepsilon$ symétriquement, d'où on déduit $u\backslash_f v' \equiv_f^{++} u\backslash_f v$. ■

Lemme 6.7. *(i) La relation $\equiv_f^{++}$ est transitive sur X.*

(ii) Pour u, v, u', v' dans X, la conjonction de $u' \equiv_f^{++} u$ et $v' \equiv_f^{++} v$ entraîne $v'\backslash_f u' \equiv_f^{++} v\backslash_f u$.

Démonstration. (i) Supposons $u, v, w \in X$ et $u \equiv_f^{++} v \equiv_f^{++} w$. Par hypothèse, on a $u\backslash_f v = v\backslash_f u = \varepsilon$. Appliquant le lemme 6.6 à $v \equiv_f^{++} w$, on obtient $u\backslash_f w \equiv_f^{++} \varepsilon$ et $w\backslash_f u \equiv_f^{++} \varepsilon$, donc $u\backslash_f w = w\backslash_f u = \varepsilon$, soit $u \equiv_f^{++} w$.

(ii) Supposons que $v\backslash_f u$ existe. En appliquant le lemma 6.6, on obtient

$$v'\backslash_f u' \equiv_f^{++} v'\backslash_f u \equiv_f^{++} v\backslash_f u,$$

qui entraîne $v'\backslash_f u' \equiv_f^{++} v\backslash_f u$ par (i), puisque $v'\backslash_f u'$, $v'\backslash_f u$ et $v\backslash_f u$ appartiennent à X, ce dernier étant supposé clos par $\backslash_f$. ■

Nous introduisons maintenant des raffinements de la relation $\equiv_f^{++}$.

Définition 6.8. Pour u, u' dans $\mathrm{Mo}(\Sigma) \cup \{\perp\}$, on dira que $u \equiv^{(0)}_{f,Y} u'$ est vérifié si on a $u = u' = \varepsilon$, et, pour $p \geq 1$, que $u \equiv^{(p)}_{f,Y} u'$ est vérifié s'il existe deux décompositions $u = u_1 \cdots u_p$, $u' = u'_1 \cdots u'_p$ telles qu'on ait u_1, …, $u'_p \in X$ et $u'_j \equiv^{++}_f u_j$ pour tout j.

Ainsi, $u' \equiv^{(1)}_{f,Y} u$ est la conjonction de $u' \equiv^{++}_f u$ et de $u, u' \in X$.

Lemme 6.9. *(i) Toute relation $u \equiv^{(p)}_{f,Y} u'$ entraîne $u \equiv^{++}_f u'$.*
(ii) La conjonction des relations $u' \equiv^{(p)}_{f,Y} u$ et $v' \equiv^{(q)}_{f,Y} v$ entraîne $u'\backslash_f v' \equiv^{(q)}_{f,Y} u\backslash_f v$ et $v'\backslash_f u' \equiv^{(p)}_{f,Y} v\backslash_f u$.

Démonstration. (i) Le résultat est clair par récurrence sur p (noter que, même pour $u, u' \in X$, il n'y a en général aucune raison pour que, réciproquement, $u \equiv^{++}_f u'$ entraîne $u \equiv^{(p)}_{f,Y} u'$).
(ii) Observons d'abord que le résultat est vrai pour $p = 0$ et pour $q = 0$. En effet, pour $p = 0$, on a $u' = u = \varepsilon$, donc $u'\backslash_f v' = \varepsilon = u\backslash_f v$, et, pour $q = 0$, on a $v' = v = \varepsilon$, donc $v'\backslash_f u' = u'$ et $v\backslash_f u = u$.

Ensuite, nous utilisons une récurrence sur $p+q$. Supposons $u' \equiv^{(p)}_{f,Y} u$ et $v' \equiv^{(q)}_{f,Y} v$. D'après ce qui précède, nous pouvons supposer $p \geq 1$ et $q \geq 1$. Alors, on peut écrire $u = u_1 u_2$, $u' = u'_1 u'_2$ avec $u'_1 \equiv^{++}_f u_1$ et $u'_2 \equiv^{(p-1)}_{f,Y} u_2$, et, de même, $v = v_1 v_2$, $v' = v'_1 v'_2$ avec $v'_1 \equiv^{++}_f v_1$ et $v'_2 \equiv^{(q-1)}_{f,Y} v_2$. Posons $u_{0,j} = u_j$ et $v_{i,0} = v_i$, puis $u_{i,j} = v_{i-1,j}\backslash_f u_{i,j-1}$ et $v_{i,j} = u_{i,j-1}\backslash_f v_{i-1,j}$ (Figure 6.1). L'hypothèse que X est close par $\backslash_f$ entraîne inductivement que tous les mots $u_{i,1}$, $u'_{i,1}$, v_i, et v'_i sont dans $X \cup \{\perp\}$. Le lemme 6.7(ii) donne $u'_{1,1} \equiv^{++}_f u_{1,1}$ et $v'_{1,1} \equiv^{++}_f v_{1,1}$. Ensuite, l'hypothèse de récurrence donne $u'_{1,2} \equiv^{(p-1)}_{f,Y} u_{1,2}$ et $v'_{1,2} \equiv^{++}_f v_{1,2}$. Elle donne de même $u'_{2,1} \equiv^{++}_f u_{2,1}$ et $v'_{2,1} \equiv^{(q-1)}_{f,Y} v_{2,1}$, et, finalement, $u'_{2,2} \equiv^{(p-1)}_{f,Y} u_{2,2}$ et $v'_{2,2} \equiv^{(q-1)}_{f,Y} v_{2,2}$. Réunissant les relations, on déduit $u'\backslash_f v' = u'_{2,1}u'_{2,2} \equiv^{(p)}_{f,Y} u_{2,1}u_{2,2} = u\backslash_f v$, et $v'\backslash_f u' = v'_{1,2}v'_{2,2} \equiv^{(q)}_{f,Y} v_{1,2}v_{2,2} = v\backslash_f u$. ∎

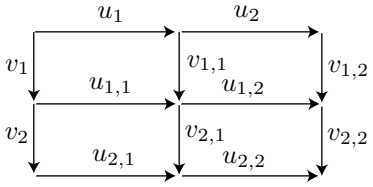


Figure 6.1. Démonstration du lemme 6.9

Définition 6.10. Pour v, v' dans $\mathrm{Mo}(\Sigma)\cup\{\perp\}$, on dira que $v \equiv^{+++}_{f,Y} v'$ est vérifié s'il existe deux décompositions $v = v_0v_1v_2v_3$, $v' = v'_0v'_1v'_2v'_3$ et deux entiers q, r vérifiant
(i) $v'_0 \equiv^{(q)}_{f,Y} v_0$, et $v'_3 \equiv^{(r)}_{f,Y} v_3$,
(ii) $v_1, v_2, v'_1, v'_2 \in X$, et $v'_2 \equiv^{++}_f v_1\backslash_f v'_1$, et $v_2 \equiv^{++}_f v'_1\backslash_f v_1$.

Lemme 6.11. *La relation $v \equiv^{+++}_{f,Y} v'$ entraîne $v \equiv^{++}_f v'$.*

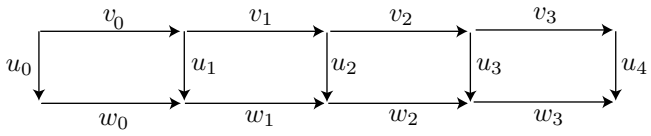
Démonstration. Avec les notations de la définition, on a d'abord $v_0' \equiv_f^{++} v_0$ et $v_3' \equiv_f^{++} v_3$ par le lemme 6.9(i), soit $v_0^{-1}v_0' \to_f \varepsilon$ et $v_3^{-1}v_3' \to_f \varepsilon$. De même, par hypothèse, on a $v_2 \equiv_f^{++} v_1'\backslash_f v_1$, soit $v_2^{-1}(v_1'\backslash_f v_1) \to_f \varepsilon$, et, symétriquement, ${v_2'}^{-1}(v_1'\backslash_f v_1) \to_f \varepsilon$. On trouve alors

$$\begin{aligned} v^{-1}v' &= v_3^{-1}v_2^{-1}v_1^{-1}v_0^{-1}v_0'v_1'v_2'v_3' \\ &\to_f v_3^{-1}v_2^{-1}v_1^{-1}v_1'v_2'v_3' \to_f v_3^{-1}v_2^{-1}(v_1\backslash_f v_1')(v_1'\backslash_f v_1)^{-1}v_2'v_3' \to_f v_3^{-1}v_3' \to_f \varepsilon, \end{aligned}$$

lorsque tous les mots v_i, v_i' sont dans $\mathrm{Mo}(\Sigma)$, et on conclut que $v \equiv_f^{++} v'$ est vrai. D'un autre côté, si au moins un des mots v_i est $\perp$, le mot v_i' correspondant est également $\perp$, et on a $v = v' = \perp$, donc $v \equiv_f^{++} v'$. ■

Lemme 6.12. *La conjonction de $u' \equiv_{f,Y}^{(p)} u$ et $v' \equiv_{f,Y}^{+++} v$ entraîne $u'\backslash_f v' \equiv_{f,Y}^{+++} u\backslash_f v$ et $v'\backslash_f u' \equiv_{f,Y}^{(p)} v\backslash_f u$.*

Démonstration. Nous raisonnons par récurrence sur p. Supposons $u' \equiv_{f,Y}^{(p)} u$ et $v' \equiv_{f,Y}^{+++} v$. Pour $p = 0$, la seule possibilité est $u' = u = \varepsilon$, donc $u'\backslash_f v' = v' \equiv_{f,Y}^{+++} v = u\backslash_f u$, et le résultat est vrai. Supposons $p = 1$. Fixons des décompositions $v = v_0v_1v_2v_3$, $v' = v_0'v_1'v_2'v_3'$ comme dans la définition 6.10. On pose $u_0 = u$ et $u_0' = u'$, et on définit de proche en proche $u_j = v_{j-1}\backslash_f u_{j-1}$ et $w_j = u_j\backslash_f v_j$, et, de même, $u_j' = v_{j-1}'\backslash_f u_{j-1}'$ et $w_j' = u_j'\backslash_f v_j'$.



Par hypothèse, nous avons $u' \equiv_{f,Y}^{(1)} u$ et $v_0' \equiv_{f,Y}^{(q)} v_0$, donc le lemme 6.9 donne

$$u_1' \equiv_{f,Y}^{(1)} u_1, \tag{6.3}$$
$$w_0' \equiv_{f,Y}^{(q)} w_0. \tag{6.4}$$

Par hypothèse, v_1 et v_1' sont dans X, donc il en est de même de $v_1\backslash_f v_1'$ et $v_1'\backslash_f v_1$. Toujours par hypothèse, nous avons $v_2 \equiv_f^{++} v_1\backslash_f v_1'$ et $v_2' \equiv_f^{++} v_1'\backslash_f v_1$, donc, par le lemme 6.6, nous obtenons

$$u_3 = v_2\backslash_f u_2 \equiv_f^{++} (v_1\backslash_f v_1')\backslash_f u_2 = (v_1\backslash_f v_1')\backslash_f (v_1\backslash_f u_1), \tag{6.5}$$
$$w_2 = u_2\backslash_f v_2 \equiv_f^{++} u_2\backslash_f (v_1\backslash_f v_1') = (v_1\backslash_f u_1)\backslash_f (v_1\backslash_f v_1'), \tag{6.6}$$

et, *mutatis mutandis*,

$$u_3' \equiv_f^{++} = (v_1'\backslash_f v_1)\backslash_f (v_1'\backslash_f u_1'), \tag{6.7}$$
$$w_2' \equiv_f^{++} (v_1'\backslash_f u_1')\backslash_f (v_1'\backslash_f v_1), \tag{6.8}$$

Comme f a la propriété du cube sur X, le mot de droite dans (6.5) est $\equiv_f^{++}$-équivalent à $(v_1'\backslash_f v_1)\backslash_f(v_1'\backslash_f u_1)$, et, comme tous les mots concernés sont dans X et que $\equiv_f^{++}$ est transitive sur X d'après le lemme 6.7(ii), nous déduisons

$$u_3 \equiv_f^{++} (v_1'\backslash_f v_1)\backslash_f(v_1'\backslash_f u_1). \tag{6.9}$$

Nous avons vu que $u_1' \equiv_f^{++} u_1$ est vrai, et u_1, u_1', v_1' et $v_1'\backslash_f v_1$ sont dans X, donc, en appliquant le lemme 6.6 deux fois en partant de (6.7) et de (6.9), nous obtenons $u_3' \equiv_f^{++} u_3$, et même $u_3' \equiv_{f,Y}^{(1)} u_3$ puisque u_3 et u_3' sont dans X par construction.

En appliquant de même la propriété du cube et la transitivité de $\equiv_f^{++}$ sur X, nous obtenons à partir de (6.6) et (6.8) les relations

$$w_2 \equiv_f^{++} (u_1\backslash_f v_1)\backslash_f(u_1\backslash_f v_1') = w_1\backslash_f(u_1\backslash_f v_1'), \tag{6.10}$$

$$w_2' \equiv_f^{++} (u_1'\backslash_f v_1')\backslash_f(u_1'\backslash_f v_1) = w_1'\backslash_f(u_1'\backslash_f v_1). \tag{6.11}$$

Comme on a $u_1' \equiv_f^{++} u_1$, le lemme 6.6 donne d'abord $u_1\backslash_f v_1' \equiv_f^{++} u_1'\backslash_f v_1' = w_1'$, d'où, en utilisant (6.10), le lemme 6.6 à nouveau, et la transitivité de $\equiv_f^{++}$ sur X,

$$w_2 \equiv_f^{++} w_1\backslash_f w_1', \tag{6.12}$$

et, par un argument symétrique en partant de (6.11),

$$w_2' \equiv_f^{++} w_1'\backslash_f w_1. \tag{6.13}$$

Maintenant, nous avons vu que $u_3' \equiv_{f,Y}^{(1)} u_3$ est vérifiée, et, par hypothèse, nous avons $v_3' \equiv_{f,Y}^{(r)} v_3$. En appliquant le lemme 6.9, nous déduisons

$$u_4' \equiv_{f,Y}^{(1)} u_4, \tag{6.14}$$

$$w_3' \equiv_{f,Y}^{(r)} w_3. \tag{6.15}$$

Par construction, on a $u\backslash_f v = w_0w_1w_2w_3$ et $v\backslash_f u = u_4$, et, de même, $u'\backslash_f v' = w_0'w_1'w_2'w_3'$ et $v'\backslash_f u' = u_4'$. Alors, la conjonction de (6.3), (6.12), (6.13) et (6.15) donne $u'\backslash_f v' \equiv_{f,Y}^{+++} u\backslash_f v$, et (6.14) donne $v'\backslash_f u' \equiv_{f,Y}^{(1)} v\backslash_f u$, ce qui est le résultat escompté.

Supposons finalement $p \geq 2$. On écrit $u = u_1u_2$, $u' = u_1'u_2'$ avec $u_1' \equiv_{f,Y}^{(1)} u_1$ et $u_2' \equiv_{f,Y}^{(p-1)} u_2$. En appliquant l'hypothèse de récurrence à u_1, u_1', v et v', nous obtenons

$$u_1'\backslash_f v' \equiv_{f,Y}^{+++} u_1\backslash_f v \tag{6.16}$$

$$v'\backslash_f u_1' \equiv_{f,Y}^{(1)} v\backslash_f u_1. \tag{6.17}$$

Ensuite, en utilisant (6.16) et en appliquant l'hypothèse de récurrence à u_2, u_2', $u_1\backslash_f v$ et $u_1'\backslash_f v'$, nous obtenons

$$u_2'\backslash_f(u_1'\backslash_f v') \equiv_{f,Y}^{+++} u_2\backslash_f(u_1\backslash_f v) \tag{6.18}$$

$$(u_1'\backslash_f v')\backslash_f u_2' \equiv_{f,Y}^{(p)} (u_1\backslash_f v)\backslash_f u_2. \tag{6.19}$$

La relation (6.18) est $u'\backslash_f v' \equiv_{f,Y}^{+++} u\backslash_f v$, tandis que la concaténation de (6.17) et (6.19) donne $v'\backslash_f u' \equiv_{f,Y}^{(p)} v\backslash_f u$. La démonstration est donc complète. ■

Nous pouvons maintenant compléter la démonstration de la Proposition 6.5.

Démonstration. Soit f une fonction de redressement sur Σ, X une partie de $\mathrm{Mo}(\Sigma)\cup\{\perp\}$ close par $\backslash_f$, et telle que f ait la propriété du cube sur X. D'après la proposition 5.6, il suffit que nous montrions que la conjonction de $u' \equiv_f^+ u$ et $v' \equiv_f^+ v$ entraîne $u'\backslash_f v' \equiv_f^+ u\backslash_f v$ et $v'\backslash_f u' \equiv_f^+ v\backslash_f u$. Comme $\equiv_f^+$ est une relation transitive, il suffit de prouver l'implication dans le cas où on a utilisé exactement une relation de R_f pour transformer uv en $u'v'$. Supposons donc, sans perte de généralité puisque la conclusion cherchée est symétrique, $u' = u$ et que v' soit obtenu à partir de v en utilisant une relation de la présentation, c'est-à-dire en remplaçant un facteur $af(a,b)$ par le facteur $bf(b,a)$ correspondant. On a donc des décompositions $v = v_0af(a,b)v_3$ et $v' = v_0bf(b,a)v_3$. Soient p, q, r les longueurs des mots u, v_0 et v_3. Par hypothèse, Σ est inclus dans X, donc $u' = u$ entraîne $u' \equiv_{f,Y}^{(p)} u$, et, de même, on a $v_0 \equiv_{f,Y}^{(q)} v_0$ et $v_3 \equiv_{f,Y}^{(r)} v_3$, et, par conséquent, on a $v' \equiv_{f,Y}^{+++} v$ par définition. Par le lemme 6.12, on déduit $u\backslash_f v' \equiv_{f,Y}^{+++} u\backslash_f v'$ et $v'\backslash_f u \equiv_{f,Y}^{(p)} v\backslash_f u$, et, de là, en particulier, $u\backslash_f v' \equiv_f^+ u\backslash_f v'$ et $v'\backslash_f u \equiv_f^+ v\backslash_f u$, ce qui est exactement ce que nous voulions démontrer. ∎

Remarque. Au lieu d'utiliser la relation $\equiv_f^{++}$, et ses raffinements $\equiv_{f,Y}^{(p)}$ et $\equiv_{f,Y}^{+++}$, nous pourrions espérer n'utiliser partout que la relation $\equiv_f^+$, ce qui simplifierait la démonstration, notamment parce que $\equiv_f^+$ est partout transitive. Il est douteux qu'une telle approche naïve puisse aboutir, car la contrepartie du lemme 6.6 n'a aucune raison d'être vraie : *a priori*, l'hypothèse $u' \equiv_f^+ u$ n'implique aucune conséquence directe pour les mots $u\backslash_f u'$ et $u'\backslash_f u$.

Question 6.13. *Soit f une fonction de redressement sur Σ, et X une partie de $\mathrm{Mo}(\Sigma)\cup\{\perp\}$ close par $\backslash_f$. Que peut-on déduire de l'hypothèse que f a la propriété du cube faible sur X — en particulier dans le cas $X = \mathrm{Mo}(\Sigma)$?*

Cette question, qui est ouverte, est de peu d'intérêt algorithmique car la seule méthode systématique connue pour établir la propriété du cube faible (5.3) est d'établir la propriété du cube forte (5.2).

En rapprochant les propositions 5.4, 5.12, et 6.5, nous obtenons une version explicite du théorème B' de l'introduction :

Proposition 6.14. *Pour f fonction de redressement sur Σ, notons $(**)$ la conjonction des conditions suivantes :*

(i) la clôture $\widetilde{\Sigma}$ de Σ pour $\backslash_f$ existe et elle est finie;

(ii) la fonction f a la propriété du cube sur $\widetilde{\Sigma}$;

(iii) notant $\widetilde{\Sigma}^\vee$ la clôture de $\widetilde{\Sigma}$ par $\vee_f$ — qui nécessairement existe et est finie si (i) et (ii) sont vérifiées — il existe un mot Ω dans $\widetilde{\Sigma}^\vee$ tel que, pour tout u dans $\widetilde{\Sigma}^\vee$, on ait $\Omega\backslash_f u = \varepsilon$ et il existe v dans $\widetilde{\Sigma}^\vee$ vérifiant $v\backslash_f\Omega \equiv_f^{++} u$.

Si M est un monoïde de Garside, et si f est un sélecteur de ppcm sur une partie génératrice Σ de M, alors f est une fonction de redressement sur Σ, elle satisfait aux conditions $(**)$ et M admet la présentation $\langle\Sigma; R_f\rangle^+$. Inversement, si f est une fonction de redressement sur Σ satisfaisant aux conditions $(**)$, alors le monoïde $\langle\Sigma; R_f\rangle^+$ est un monoïde de Garside, et f est un sélecteur de ppcm sur Σ.

Les conditions mises en jeu dans la proposition précédente sont de type Σ_1^0 : si le monoïde $\langle \Sigma\,;\, R_f\rangle^+$ est un monoïde de Garside, alors les conditions (i), (ii) et (iii) sont vérifiées, donc, partant de l'ensemble fini Σ, on déterminera en un nombre fini d'étapes la clôture de Σ pour $\backslash_f$, puis on établira la propriété du cube pour f sur cette clôture, et, enfin, la condition (iii), toujours par un nombre fini de redressements qui, par hypothèse, convergent tous en un nombre fini d'étapes.

Exemple 6.15. Considérons la présentation $\langle a, b\,;\, aba = b^2\rangle^+$, associée au complément f défini par $f(a, b) = ba$ et $f(b, a) = b$. La clôture de $\{a, b\}$ par $\backslash_f$ est l'ensemble $\{a, b, ba, bab, \varepsilon, ab\}$. Que f ait la propriété du cube sur cet ensemble se vérifie directement — en fait, on peut aussi appliquer ici le critère de la proposition 6.4 car l'alphabet est réduit à deux lettres. Enfin, la clôture de $\{a, b, ba, bab, \varepsilon, ab\}$ par $\vee_f$ est l'ensemble $\{a, b, ba, bab, \varepsilon, ab, aba, bb, abab, baba\}$, et il est immédiat de vérifier que les choix$\Omega = abab$ et $\Omega = baba$ conviennent pour la condition (iii). (Noter que le groupe $\langle a, b\,;\, aba = b^2\rangle$ est le groupe de tresses B_3 rapporté aux générateurs $a = \sigma_1$ et $b = \sigma_2\sigma_1$.)

Il est alors facile de déduire le théorème B de l'introduction. Partant d'une présentation supposée finie d'un groupe G (*resp.* d'un monoïde M), nous pouvons énumérer systématiquement toutes les présentations de G (*resp.* de M) en appliquant les transformations de Tietze, et, pour chacune d'elles, tester si elle est complémentée, c'est-à-dire associée à une fonction de redressement, et si cette dernière satisfait aux conditions de la proposition 6.14. Alors G est un groupe de Garside (*resp.* M est un monoïde de Garside) si et seulement si la réponse est positive pour au moins une des présentationss, ce qui se trouvera établi en un nombre fini d'étapes pour autant que les tests des diverses présentations soient menés en parallèle, c'est-à-dire sans attendre l'hypothétique fin d'un test pour passer au suivant.

Remarque. Un groupe de Garside peut s'exprimer comme groupe de fractions de plusieurs monoïdes : par définition, au moins un de ceux-ci est un monoïde de Garside, mais ce n'est pas nécessairement le cas des autres. Par exemple, le groupe de tresses B_3 est à la fois le groupe de fractions des monoïdes $\langle a, b\,;\, aba = bab\rangle^+$ et $\langle a, b\,;\, aba = b^2\rangle^+$, qui sont petits gaussiens, et du monoïde $\langle a, b\,;\, aba = baab\rangle^+$, qui n'est pas atomique. De la même façon, un monoïde de Garside peut admettre plusieurs présentations associées à des compléments différents, et les conditions de la proposition 6.14 ne valent que pour ceux de ces compléments qui sont des sélecteurs de ppcm : ainsi, le monoïde de Garside $\langle a, b, c; ab = bc = ca\rangle^+$ admet aussi la présentation $\langle a, b, c; ab = bc = ca, aba = caa\rangle^+$, pour laquelle le redressement n'est pas toujours convergent. Il serait donc incorrect d'énoncer la proposition 6.14 sous la forme «Le monoïde $\langle \Sigma; R_f\rangle^+$ est un monoïde de Garside si et seulement si f satisfait aux conditions $(**)$» .

Références

[1] S.I. Adjan, *On the embeddability of semigroups* , Soviet. Math. Dokl., 1-4; 1960; 819–820.

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

[3] G. Baumslag & C.F. Miller III (eds), Algorithms and Classification in Combinatorial Group Theory, MSRI Publications 23, Springer Verlag (1992).

[4] D. Bessis, F. Digne, & J. Michel, *Springer theory in braid groups and the Birman-Ko-Lee monoid*, prépublication (2000).

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

[6] M. Broué, G. Malle & R. Rouquier, *Complex reflection groups, braid groups, Hecke algebras*, J. Reine Angew. Math. **500** (1998) 127–190.

[7] M. Burger & S. Mozes, *Finitely presented simple groups and product of trees*, C. R. Acad. Sci. Paris **324–1** (1997) 747–752.

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

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

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

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

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

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

[14] —, *Gaussian groups are torsion free*, J. of Algebra **210** (1998) 291–297.

[15] —, *On completeness of word reversing*, Discrete Math. **225** (2000) 93–119.

[16] —, Braids and Self-Distributivity, Progress in Math. vol. 192, Birkhäuser (2000).

[17] P. Dehornoy & L. Paris, *Garside groups, a generalization of Artin groups*, Proc. London Math. Soc. **79-3** (1999) 569–604.

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

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

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

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

[22] J. Michel, *A note on words in braid monoids*, J. of Algebra **215** (1999) 366–377.

[23] M. Picantin, *The conjugacy problem in small Gaussian groups*, Comm. in Algebra, à paraître.

[24] —, *The center of small Gaussian groups*, J. of Algebra, à paraître.

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

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

[27] W. Thurston, *Finite state algorithms for the braid group*, notes en circulation (1988).

SDAD FRE 2271 CNRS, Mathématiques
Université de Caen, 14 032 Caen, France
dehornoy@math.unicaen.fr
http ://www.math.unicaen.fr/∼dehornoy/