



ELSEVIER

Contents lists available at [SciVerse ScienceDirect](http://SciVerse.ScienceDirect.com)

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Algebra

Coxeter-like groups for set-theoretic solutions of the Yang–Baxter equation



Analogues des groupes de Coxeter pour les solutions ensemblistes de l'équation de Yang–Baxter

Patrick Dehornoy

Laboratoire de mathématiques Nicolas-Oresme, CNRS UMR 6139, université de Caen, 14032 Caen cedex, France

ARTICLE INFO

Article history:

Received 16 May 2013

Accepted after revision 3 July 2013

Available online 31 July 2013

Presented by the Editorial Board

ABSTRACT

We attach with every finite, involutive, nondegenerate set-theoretic solution of the Yang–Baxter equation a finite group that plays for the associated structure group the role that a finite Coxeter group plays for the associated Artin–Tits group.

© 2013 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

R É S U M É

On associe à chaque solution ensembliste involutive et non dégénérée de l'équation de Yang–Baxter un groupe fini qui joue, pour le groupe de structure associé, le rôle que joue un groupe de Coxeter fini pour le groupe d'Artin–Tits associé.

© 2013 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

Version française abrégée

Une solution ensembliste de l'équation de Yang–Baxter (YBE) est un couple (X, R) avec R bijection de X^2 dans X^2 satisfaisant $R^{12}R^{23}R^{12} = R^{23}R^{12}R^{23}$, où $R^{ij} : X^3 \rightarrow X^3$ correspond à R agissant en positions i et j . Une solution (X, R) est involutive si on a $R^2 = \text{id}$, et non dégénérée si, en écrivant $R(x, y) = (R_1(x, y), R_2(x, y))$, les applications $y \mapsto R_1(x, y)$ et $x \mapsto R_2(x, y)$ sont bijectives. Le groupe $\langle X \mid \{xy = zt \mid x, y, z, t \in X \text{ et } R(x, y) = (z, t)\} \rangle$ est appelé groupe de structure de (X, R) [5].

Les groupes de structure de solutions de YBE admettent diverses définitions alternatives et ont de riches propriétés ; en particulier, ce sont des groupes de Garside [1,3]. Dans le cas des groupes de tresses B_n , la structure de Garside est liée à la suite exacte $1 \rightarrow P_n \rightarrow B_n \rightarrow \mathfrak{S}_n \rightarrow 1$, où P_n est le groupe des tresses pures, le treillis des diviseurs de l'élément de Garside Δ_n est isomorphe à l'ordre faible sur \mathfrak{S}_n et son diagramme de Hasse est lié au graphe de Cayley de \mathfrak{S}_n : une présentation de \mathfrak{S}_n s'obtient en ajoutant des relations $s^2 = 1$ à celle de B_n , et \mathfrak{S}_n fournit un germe de Garside pour B_n [4].

Ces résultats s'étendent à tous les types de la classification de Cartan. Comme les groupes de Garside sont une extension des groupes d'Artin–Tits sphériques, il est naturel de poser ce qui suit.

Question 1.1. Supposons que G soit un groupe de Garside, avec structure de Garside (M, Δ) . Existe-t-il un quotient fini W de G fournissant un germe de Garside pour M dont le graphe de Cayley par rapport aux atomes de M soit isomorphe au treillis des diviseurs de Δ dans M ?

E-mail address: patrick.dehornoy@gmail.com.

En d'autres termes, tout groupe de Garside admet-il l'analogie d'un groupe de Coxeter associé? La question est ouverte. Le but de cette note est d'apporter une réponse positive dans le cas des groupes de structure de solutions de YBE. On associe à chaque solution un nombre appelé sa classe et on montre :

Théorème 1.2. *Supposons que G (resp. M) soit le groupe (resp. monoïde) de structure d'une solution ensembliste (X, R) de YBE involutive et non dégénérée de taille n et de classe p . Alors, il existe un élément de Garside Δ dans M et un groupe fini W d'ordre p^n avec une suite exacte $1 \rightarrow \mathbb{Z}^n \rightarrow G \rightarrow W \rightarrow 1$, tels que (W, X) fournit un germe pour M dont le graphe de Cayley est le diagramme de Hasse du treillis des diviseurs de Δ dans M . Une présentation de W s'obtient en ajoutant n relations de la forme $w_x = 1$ à celle de G , avec w_x mot de longueur p commençant par x .*

Le théorème 1.2 étend les résultats de [2], qui concernent les solutions de classe 2. Notre approche est disjointe et repose sur les RC-systèmes de [9] et l'existence d'une I -structure [6–8] permettant de transporter aux monoïdes de structure des résultats qui sont triviaux dans le cas de \mathbb{Z}^n .

La première étape consiste à passer des solutions de YBE aux RC-quasigroupes (Définition 2.1), qui sont les structures (X, \star) avec \star opération binaire sur X obéissant à la loi RC $(x \star y) \star (x \star z) = (y \star x) \star (y \star z)$ et où les translations $y \mapsto x \star y$ sont bijectives. Le groupe (resp. monoïde) associé est présenté par $\langle X \mid \{x(x \star y) = y(y \star x) \mid x, y \in X\} \rangle$. Les groupes de structure des solutions de YBE coïncident avec les groupes associés aux RC-quasigroupes [9], et on peut donc adopter ce point de vue.

Définition 2.2. Posons $\Pi_1(x_1) = x_1$ et $\Pi_n(x_1, \dots, x_n) = \Pi_{n-1}(x_1, \dots, x_{n-1}) \star \Pi_{n-1}(x_1, \dots, x_{n-2}, x_n)$. Un RC-quasigroupe (X, \star) est dit de classe p si on a $\Pi_{p+1}(x, \dots, x, y) = y$ pour tous x, y dans X .

Tout RC-quasigroupe fini est de classe finie (Lemme 2.3). À partir d'ici, supposons que G (resp. M) soit le groupe (resp. monoïde) associé à un RC-quasigroupe (X, \star) de taille n et de classe p . Le monoïde M est de type I , c'est-à-dire qu'il admet une I -structure [6,7] : il existe une bijection $\nu : \mathbb{N}^n \rightarrow M$ satisfaisant $\nu(1) = 1$ et $\{\nu(ux) \mid x \in X\} = \{\nu(u)x \mid x \in X\}$ pour tout u dans \mathbb{N}^n .

Lemme 3.1. *Pour tous x_1, \dots, x_r dans X , on a $\nu(x_1 \cdots x_r) = \Sigma_r(x_1, \dots, x_r)$, avec Σ_r inductivement défini par $\Sigma_1(x_1) = x_1$ et $\Sigma_r(x_1, \dots, x_r) = \Sigma_{r-1}(x_1, \dots, x_{r-1}) \cdot \Pi_r(x_1, \dots, x_r)$.*

Lemme 3.2. *Pour $x \in X$ et $r \geq 0$, soit $x^{[r]} = \nu(x^r)$. Pour $x \in X$ et $u \in \mathbb{N}^n$, on a $\nu(x^p u) = x^{[p]} \nu(u)$. En particulier, on a $\pi(x^p) = \text{id}$ et, pour tous x, y dans X , les éléments $x^{[p]}$ et $y^{[p]}$ commutent dans M .*

Lemme 3.3. *Supposons $p \geq 2$ et posons $\Delta = \nu(\prod_{x \in X} x^{p-1})$. Alors, Δ est un élément de Garside dans M , et la famille de ses diviseurs est $\nu(\{0, \dots, p-1\}^n)$, qui a p^n éléments. De plus, Δ^p est central.*

Pour $u \in \mathbb{N}^n$ et $x \in X$, notons $|u|_x$ le nombre (bien défini) de x dans une X -décomposition de u .

Lemme 3.4. *Pour u, u' dans \mathbb{N}^n , déclarons $u \equiv_p u'$ si, pour tout x dans X , on a $|u|_x = |u'|_x \pmod p$, et, pour g, g' dans M , déclarons $g \equiv g'$ pour $\nu^{-1}(g) \equiv_p \nu^{-1}(g')$. Alors, \equiv est une relation d'équivalence sur M qui est compatible avec la multiplication.*

Comme Δ est de Garside dans M , tout élément de G a une expression $\Delta^e h$ avec $e \in \mathbb{Z}$ et $h \in M$.

Lemme 3.5. *Pour $g = \Delta^{pe} h$, $g' = \Delta^{pe'} h'$ dans G avec $h, h' \in M$, déclarons $g \equiv g'$ pour $h \equiv h'$. Alors, \equiv est une congruence sur G avec p^n classes, et le noyau de $G \rightarrow G/\equiv$ est le sous-groupe abélien de G engendré par les éléments $x^{[p]}$ avec $x \in X$.*

On obtient alors le théorème 1.2. En effet, soit W le groupe-quotient G/\equiv . Le noyau de la projection de G sur W est le groupe abélien libre engendré par les n éléments $x^{[p]}$ avec $x \in X$, d'où la suite exacte $1 \rightarrow \mathbb{Z}^n \rightarrow G \rightarrow W \rightarrow 1$. Une présentation de W est obtenue à partir de celle de G en ajoutant les n relations $x^{[p]} = 1$. Du fait de sa présentation, (W, X) fournit un germe de Garside \underline{W} pour G . Le diagramme de Hasse du treillis des diviseurs de Δ est l'image par ν du sous-treillis de \mathbb{N}^n formé par les p^n diviseurs de $\prod_{x \in X} x^{p-1}$ dans \mathbb{N}^n , tandis que le graphe de Cayley de \underline{W} est l'image par ν du germe dérivé de \mathbb{Z}^n/\equiv_p : l'égalité dans le cas de \mathbb{N}^n donne l'égalité pour M .

1. Introduction

A set-theoretic solution of the Yang–Baxter equation (YBE) is a pair (X, R) , where R is a bijection from X^2 to itself satisfying $R^{12} R^{23} R^{12} = R^{23} R^{12} R^{23}$, in which $R^{ij} : X^3 \rightarrow X^3$ corresponds to R acting in positions i and j . Set-theoretic solutions of YBE provide particular solutions of the (quantum) Yang–Baxter equation, and received some attention in recent years.

A set-theoretic solution (X, R) of YBE is called *involutive* for $R^2 = \text{id}$, and *nondegenerate* if, writing $R(x, y) = (R_1(x, y), R_2(x, y))$, the maps $y \mapsto R_1(x, y)$ and $x \mapsto R_2(x, y)$ are one-to-one. In this case, the group (resp. monoid) presented by $\langle X \mid \{xy = z, t \mid x, y, z, t \in X \text{ and } R(x, y) = (z, t)\} \rangle$ is called the *structure group* (resp. *structure monoid*) of (X, R) [5].

Such structure groups of set-theoretic solutions of YBE admit a number of alternative definitions and make an interesting family. Among others, every structure group is a *Garside group* [1], meaning that there exists a pair (M, Δ) such that M is a cancellative monoid in which left-divisibility—defined by $g \preceq h \Leftrightarrow \exists h' \in M (h = gh')$ —is a lattice, Δ is a *Garside element* in M —meaning that the left and right divisors coincide, are finite in number, and generate M —and G is a group of fractions for M [3].

In the case of Artin’s braid group B_n , the seminal example of a Garside group, the Garside structure (B_n^+, Δ_n) is connected with the exact sequence $1 \rightarrow P_n \rightarrow B_n \rightarrow \mathfrak{S}_n \rightarrow 1$, where P_n is the pure braid group. In one direction, a presentation of \mathfrak{S}_n is obtained by adding $n - 1$ relations $\sigma_i^2 = 1$ to the standard presentation of B_n . In the other direction, call Σ the family of all transpositions $(i, i + 1)$ and, for f, g, h in \mathfrak{S}_n , say that $f \bullet g = h$ holds if we have $fg = h$ and the Σ -length of h is the sum of the Σ -lengths of f and g . Then $(\mathfrak{S}_n, \bullet)$ is a germ for the monoid B_n^+ that is bounded by Δ_n , meaning that \mathfrak{S}_n together with the family of relations $f \bullet g = fg$ makes a presentation of B_n^+ and, in addition, the Hasse diagram of the divisors of Δ_n in B_n^+ is isomorphic to the Cayley graph of $(\mathfrak{S}_n, \bullet)$ [4]. Similar results connect spherical Artin–Tits groups with the associated finite Coxeter group for all types in the Cartan classification.

As Garside groups extend spherical type Artin–Tits groups in many respects, it is natural to ask:

Question 1.1. Assume that G is a Garside group, with Garside structure (M, Δ) . Does there exist a finite quotient W of G such that W with the images of the atoms of M provides a Garside germ for M and the Cayley graph of this germ is isomorphic to the lattice of divisors of Δ in M ?

In other words, does every Garside group admit some Coxeter-like group? The general question remains open. The aim of this note is to establish a positive answer for structure groups of set-theoretic solutions of YBE. We attach with every such solution a number called its *class* and establish:

Theorem 1.2. Assume that G (resp. M) is the structure group (resp. monoid) of an involutive, nondegenerate solution (X, R) of YBE with X of size n and class p . Then there exist a Garside element Δ in M and a finite group W of order p^n entering a short exact sequence $1 \rightarrow \mathbb{Z}^n \rightarrow G \rightarrow W \rightarrow 1$ such that (W, X) provides a germ for M whose Cayley graph is the Hasse diagram of the divisors of Δ in M . A presentation of W is obtained by adding n relations $w_x = 1$ to that of G , with w_x an explicit length p word beginning with x .

Theorem 1.2 extends the results of [2], in which solutions of class 2 are addressed by a different method. Our approach relies on the connection with the *right-cyclic law* of [9] and on the existence of an *l-structure* [6–8], which enables one to carry to arbitrary structure monoids results that are trivial in the case of \mathbb{Z}^n .

2. The class of a finite RC-quasigroup

The first step consists in switching from solutions of YBE to RC-quasigroups.

Definition 2.1. An *RC-system* is a pair (X, \star) with \star a binary operation on X that obeys the *RC-law* $(x \star y) \star (x \star z) = (y \star x) \star (y \star z)$. An *RC-quasigroup* is an RC-system in which the maps $y \mapsto x \star y$ are bijections. An RC-quasigroup is *bijective* if the map $(x, y) \mapsto (x \star y, y \star x)$ from X^2 to X^2 is bijective. The *associated group* (resp. *monoid*) is presented by $\langle X \mid \{x(x \star y) = y(y \star x) \mid x, y \in X\} \rangle$.

As proved in [9], if (X, R) is an involutive, nondegenerate set-theoretic solution of YBE, then defining $x \star y$ to be the (unique) z satisfying $R_1(x, z) = y$ makes X into a bijective RC-quasigroup and the group and monoid associated with (X, \star) coincide with those of (X, R) . Conversely, every bijective RC-quasigroup (X, \star) comes associated with a set-theoretic solution of YBE. Thus investigating structure groups of set-theoretic solutions of YBE and groups of bijective RC-quasigroups are equivalent tasks.

Definition 2.2. Inductively define $\Pi_1(x_1) = x_1$ and

$$\Pi_n(x_1, \dots, x_n) = \Pi_{n-1}(x_1, \dots, x_{n-1}) \star \Pi_{n-1}(x_1, \dots, x_{n-2}, x_n). \tag{1}$$

An RC-quasigroup (X, \star) is said to be of *class* p if $\Pi_{p+1}(x, \dots, x, y) = y$ holds for all x, y in X .

Lemma 2.3. Every finite RC-quasigroup is of class p for some p .

Proof. Let (X, \star) be a finite RC-quasigroup. First, (X, \star) must be bijective [9] (or [8] for a different argument). Consider $\Phi : (x, y) \mapsto (x \star x, x \star y)$ on X^2 . Assume $(x, y) \neq (x', y')$. For $x \neq x'$, $\Psi(x, x) \neq \Psi(x', x')$ implies $x \star x \neq x' \star x'$; for $x = x'$, we

have $y \neq y'$, whence $x \star y \neq x \star y'$ since left-translations are injective; so $\Phi(x, y) \neq \Phi(x', y')$ always holds. So Φ is injective, hence bijective on X^2 , and $\Phi^{p+1} = \text{id}$ holds for some $p \geq 1$. An induction gives $\Phi^r(x, y) = (\Pi_r(x, \dots, x, x), \Pi_r(x, \dots, x, y))$. So $\Phi^{p+1} = \text{id}$ implies $\Pi_{p+1}(x, \dots, x, y) = y$ for all x, y , i.e., (X, \star) is of class p . \square

3. Using the I -structure

From now on, assume that M (resp. G) is the structure monoid (resp. group) of some finite RC-quasigroup (X, \star) of size n and class p . The form of the defining relations of M implies that the Cayley graph of M with respect to X is an n -dimensional lattice. Moreover M admits a (right) I -structure, i.e., a bijection $\nu: \mathbb{N}^n \rightarrow M$ satisfying $\nu(1) = 1$ and $\{\nu(ux) \mid x \in X\} = \{\nu(u)x \mid x \in X\}$ for every u in \mathbb{N}^n ; hence, equivalently, $\nu(ux) = \nu(u)\pi(u)(x)$ for some permutation $\pi(u)$ of X [6,7]. The monoid M is then called of right- I -type. Our point is that the I -structure (which is unique) is connected with \star . Without loss of generality, we assume that X is the standard basis of \mathbb{N}^n and that $\nu(x) = x$ holds for x in X .

Lemma 3.1. For all x_1, \dots, x_r in X , we have $\nu(x_1 \cdots x_r) = \Sigma_r(x_1, \dots, x_r)$, with Σ_r inductively defined by $\Sigma_1(x_1) = x_1$ and $\Sigma_r(x_1, \dots, x_r) = \Sigma_{r-1}(x_1, \dots, x_{r-1}) \cdot \Pi_r(x_1, \dots, x_r)$.

Proof. One can either check that $\Sigma_r(x_1, \dots, x_r)$ satisfies all properties required for an I -structure directly, or start from the existence of the I -structure ν and connect it with Σ_r . Writing $\pi[u]$ for the result of applying π to u componentwise, we have, for all u, v in \mathbb{N}^n , [6,7] (see also [8, Chapter 8]):

$$\nu(uv) = \nu(u)\nu(\pi(u)[v]) \quad \text{and} \quad \pi(uv) = \pi(\pi(u)[v]) \circ \pi(u). \tag{2}$$

We use induction on r . For $r = 1$, the result is obvious. Assume $r = 2$ and $x_1 \neq x_2$. The definition gives $\nu(x_1x_2) = x_1\pi(x_1)(x_2) = \nu(x_2x_1) = x_2\pi(x_2)(x_1)$, hence $\nu(x_1x_2)$ must be the right-lcm (least common right-multiple) of x_1 and x_2 in M . On the other hand, $x_1(x_1 \star x_2) = x_2(x_2 \star x_1)$ holds in M , and this must also be the right-lcm of x_1 and x_2 . By uniqueness and left-cancellativity, we deduce $\pi(x_1)(x_2) = x_1 \star x_2$. Next, for $x_1 = x_2$, the value of $\pi(x_1)(x_2)$, as well as that of $x_1 \star x_2$, must be the unique element of X that is not of the form $\pi(x_1)(x)$ or $x_1 \star x$ with $x \neq x_1$, respectively. This forces $\pi(x_1)(x_2) = x_1 \star x_2$ in this case, whence $\nu(x_1x_2) = x_1(x_1 \star x_2) = \Sigma_2(x_1, x_2)$ in every case. Assume now $r \geq 3$. We find:

$$\nu(x_1 \cdots x_r) = x_1\nu(\pi(x_1)[x_2 \cdots x_r]) = x_1\nu((x_1 \star x_2) \cdots (x_1 \star x_r)) = x_1\Sigma_{r-1}(x_1 \star x_2, \dots, x_1 \star x_r) = \Sigma_r(x_1, x_2, \dots, x_r),$$

the first equality by (2), the second by the case $r = 2$, the third by the induction hypothesis, and the last one by expanding the terms. \square

Lemma 3.2. For $x \in X$ and $r \geq 0$, let $x^{[r]} = \nu(x^r)$. For all $x \in X$ and $u \in \mathbb{N}^n$, we have $\nu(x^p u) = x^{[p]}\nu(u)$ in M . In particular, we have $\pi(x^p) = \text{id}$ and, for all x, y in X , the elements $x^{[p]}$ and $y^{[p]}$ commute in M .

Proof. Let $y_1 \cdots y_q$ be a decomposition of u in terms of elements of X . By Lemma 3.1, we have:

$$\begin{aligned} \nu(x^p u) &= \Sigma_{p+q}(x, \dots, x, y_1, \dots, y_q) = \Sigma_p(x, \dots, x)\Sigma_q(\Pi_{p+1}(x, \dots, x, y_1), \dots, \Pi_{p+1}(x, \dots, x, y_q)) \\ &= \Sigma_p(x, \dots, x)\Sigma_q(y_1, \dots, y_q) = \nu(x^p)\nu(y_1 \cdots y_q) = x^{[p]}\nu(u), \end{aligned}$$

in which the second equality comes from expanding the terms and the third one from the assumption that M is of class p . Applying with $u = y$ in X and merging with $\nu(x^p y) = \nu(x^p)\pi(x^p)(y)$, we deduce $\pi(x^p) = \text{id}$. On the other hand, applying with $u = y^{[p]}$, we find $x^{[p]}y^{[p]} = \nu(x^p y^p) = \nu(y^p x^p) = y^{[p]}x^{[p]}$. \square

Lemma 3.3. Assume $p \geq 2$ and define $\Delta = \nu(\prod_{x \in X} x^{p-1})$. Then Δ is a Garside element in M , and its family of divisors is $\nu(\{0, \dots, p-1\}^n)$, which has p^n elements. Moreover Δ^p is central in M .

Proof. The map ν is compatible with \preceq : for all u, v in \mathbb{N}^n , we have $u \preceq v$ in \mathbb{N}^n if and only if $\nu(u) \preceq \nu(v)$ holds in M . Indeed, by (2), $v = ux$ with x in X implies $\nu(v) = \nu(u)\pi(u)(x)$, whence $\nu(u) \preceq \nu(v)$ in M . Conversely, for $\nu(v) = \nu(u)x$ with x in X , as $\pi(u)$ is bijective, we have $\pi(u)(y) = x$ for some y in X , whence $\nu(uy) = \nu(u)\pi(u)(y) = \nu(u)x = \nu(v)$, and $v = uy$ since ν is injective, i.e., $u \preceq v$ in \mathbb{N}^n . Hence the left-divisors of Δ in M are the image under ν of the p^n divisors of δ^{p-1} in \mathbb{N}^n , with $\delta = \prod_{x \in X} x$. For right-divisors, the maps $\pi(u)$ are bijective, so every right-divisor of Δ must be a left-divisor of Δ . Then the duality map $g \mapsto h$ for $gh = \Delta$ is a bijection from the left- to the right-divisors of Δ . So the left and right divisors of Δ coincide, and they are p^n in number. Since every element of X divides Δ , the latter is a Garside element in M . Finally, by Lemma 3.1, Δ^p is the product of the elements $x^{[p]}$ repeated $p-1$ times; as $\sigma[\delta] = \delta$ holds for every permutation σ , we deduce $x\Delta^p = \Delta^p x$ for every x . \square

For $u \in \mathbb{N}^n$ and $x \in X$, write $|u|_x$ for the (well-defined) number of x in an X -decomposition of u .

Lemma 3.4. For u, u' in \mathbb{N}^n , say that $u \equiv_p u'$ holds if, for every x in X , we have $|u|_x = |u'|_x \pmod p$, and, for g, g' in M , say that $g \equiv g'$ holds for $v^{-1}(g) \equiv_p v^{-1}(g')$. Then \equiv is an equivalence relation on M that is compatible with left- and right-multiplication.

Proof. As v is bijective, carrying the equivalence relation \equiv_p of \mathbb{N}^n to M yields an equivalence relation. Assume $v(u) \equiv v(u')$. Without loss of generality, we may assume $u' = ux^p = x^p u$ with x in X . Applying (2) and Lemma 3.2, we deduce $\pi(u) = \pi(u')$ and, therefore, $v(u)\pi(u)(y) = v(uy) \equiv v(u'y) = v(u')\pi(u)(y)$. As $\pi(u)(y)$ takes every value in X when y varies, \equiv is compatible with right multiplication by X . On the other hand, $u \equiv_p u'$ implies $\sigma[u] \equiv_p \sigma[u']$ for every permutation σ , so we obtain $yv(u) = v(y\pi(y)^{-1}[u]) \equiv v(y\pi(y)^{-1}[u']) = yv(u')$, and \equiv is compatible with left multiplication by X . \square

Lemma 3.5. For $g = \Delta^{pe}h, g' = \Delta^{pe'}h'$ in G with e, e' in \mathbb{Z} and h, h' in M , say that $g \equiv g'$ holds if $h \equiv h'$ does. Then \equiv is a congruence on G with p^n classes, and the kernel of $G \rightarrow G/\equiv$ is the Abelian subgroup of G generated by the elements $x^{[p]}$ with $x \in X$.

Proof. As Δ is a Garside element in M , every element of G admits a (non-unique) expression $\Delta^{pe}h$ with $e \in \mathbb{Z}$ and $h \in M$. Assume $g = \Delta^{pe}h = \Delta^{pe_1}h_1$ with $e > e_1$. As M is left-cancellative, we find $h_1 = \Delta^{p(e-e_1)}h$, whence $h_1 \equiv h$. So, for every h' in M , we have $h \equiv h' \Leftrightarrow h_1 \equiv h'$ and \equiv is well defined on G . That \equiv is compatible with multiplication on G follows from the compatibility on M and the fact that Δ^p lies in the centre of G . Next, by definition, every element of G is \equiv -equivalent to some element of M , so the number of \equiv -classes in G is the number of \equiv -classes in M , hence the number p^n of \equiv_p -classes.

Finally, $u \equiv_p x^p u$ holds for all x in X and u in \mathbb{N}^n . This, together with Lemma 3.1, implies $x^{[p]} \equiv 1$. Conversely, assume $g \equiv 1$ in M . By definition, $v^{-1}(g)$ lies in the \equiv_p -class of 1, hence one can go from $v^{-1}(g)$ to 1 by multiplying or dividing by elements x^p . By Lemma 3.1, this means that one goes from g to 1 by multiplying or dividing by elements $x^{[p]}$. So these elements generate the kernel of $G \rightarrow G/\equiv$. \square

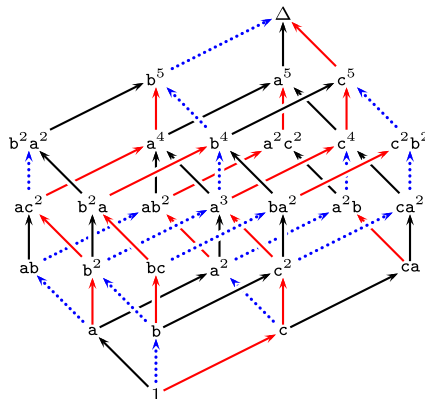
Theorem 1.2 follows. Define W to be G/\equiv . We saw that the kernel of the projection $G \rightarrow W$ is the free Abelian group generated by the n elements $x^{[p]}$ with $x \in X$, whence an exact sequence $1 \rightarrow \mathbb{Z}^n \rightarrow G \rightarrow W \rightarrow 1$. A presentation of W is obtained by adding to the presentation of G the n relations $x^{[p]} = 1$, i.e., $x(x \star x)((x \star x) \star (x \star x)) \dots = 1$. The Hasse diagram of the lattice made of the p^n divisors of Δ is the image under v of the sublattice of \mathbb{N}^n made of the p^n divisors of δ in \mathbb{N}^n , whereas the Cayley graph of the germ derived from (W, X) —i.e., W equipped with the partial product obtained by restricting to the cases when X -lengths add—is the image under v of the Cayley graph of the germ derived from the quotient group \mathbb{Z}^n/\equiv_p : the (obvious) equality in the case of \mathbb{N}^n implies the equality in the case of M .

4. An example

For an RC-quasigroup of class 1, i.e., satisfying $x \star y = y$ for all x, y , the group G is a free Abelian group, the group W is trivial, and the short exact sequence of Theorem 1.2 reduces to $1 \rightarrow \mathbb{Z}^n \rightarrow G \rightarrow 1$.

Class 2, i.e., when $(x \star x) \star (x \star y) = y$ holds for all x, y , is addressed in [2] (with no connection with RC-quasigroups). The element Δ is the right-lcm of X , it has 2^n divisors which are the right-lcms of subsets of X , and the group W is the order- 2^n quotient of G obtained by adding the relations $x(x \star x) = 1$.

For one example in class 3, consider $\{a, b, c\}$ with $x \star y = f(y)$, $f : a \mapsto b \mapsto c \mapsto a$. The associated presentation is $\langle a, b, c \mid ac = b^2, ba = c^2, cb = a^2 \rangle$. The smallest Garside element is a^3 , but, in view of Lemma 3.3, here with $p = 3$, we consider $\Delta = a^6$, which is the next Garside element after a^3 . Adding to the above presentation of G the three relations $x(x \star x)((x \star x) \star (x \star x)) = 1$, namely $abc = bca = cab = 1$, here reducing to $abc = 1$, one obtains for W the presentation $\langle a, b, c \mid ac = b^2, ba = c^2, cb = a^2, abc = 1 \rangle$. The lattice $\text{Div}(\Delta)$ has 27 elements, its diagram is the cube shown on the right. The latter is also the Cayley graph of the germ derived from (W, X) .



References

- [1] F. Chouraqui, Garside groups and Yang–Baxter equations, *Commun. Algebra* 38 (2010) 4441–4460.
- [2] F. Chouraqui, E. Godelle, Finite quotients of groups of I-type, arXiv:1301.3707.
- [3] P. Dehornoy, Groupes de Garside, *Ann. Sci. Éc. Norm. Super.* 35 (2002) 267–306.
- [4] P. Dehornoy, F. Digne, J. Michel, Garside families and Garside germs, *J. Algebra* 380 (2013) 109–145.
- [5] P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, *Duke Math. J.* 100 (1999) 169–209.
- [6] T. Gateva-Ivanova, M. Van den Bergh, Semigroups of I-type, *J. Algebra* 206 (1998) 97–112.
- [7] E. Jespers, J. Okninski, Monoids and groups of I-type, *Algebr. Represent. Theory* 8 (2005) 709–729.
- [8] E. Jespers, J. Okninski, Noetherian Semigroup Algebras, *Algebra Appl.*, vol. 7, Springer-Verlag, 2007.
- [9] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation, *Adv. Math.* 193 (2005) 4055.