Garside Groups And The Yang-Baxter Equation

Author:
Raúl Sastriques Guardiola

PhD Advisors:
Adolfo Ballester Bolinches,
José Sergio Camp Mora

VNIVERSITAT DE VALÈNCIA

Programa de Doctorado en Matématicas
Enero 2024

Agradecimientos

Esta tesis doctoral es el resultado de estos últimos años de trabajo y solo ha sido posible a muchas personas a las cuales quiero agradecer aquí.

Primero que todo, quiero agradecer a mis directores de tesis Adolfo Ballester Bolinches por la confianza que me brindó al aceptar dirigir esta tesis, dirección y labor administrativa, así como a José Sergio Camp Mora por todo el tiempo y dedicación invertidos a lo largo de la tesis doctoral.

Quiero agradecer también agradecer a mis padres, por el tiempo y paciencia invertidos durante todos estos años, así como a mi familia más amplia, por su apoyo, comprensión y cariño.

Además, quiero agradecer y recordar, a todas aquellas personas con las que me he encontrado en el camino, como el profesor Ramón Esteban o mis compañeros del departamento de Álgebra; a Leandro Vendramin por acogerme en Bruselas durante mi mes de estancia y por la magnifica compañía de la cual pude disfrutar lejos de casa; a mis compañeros de carrera y amigos Roberto Giménez, Irene Creus, Gabriel Calvo y Paula Segura, por su amistad, templanza y por aquello vivido y sufrido juntos. Por último quiero agradecer a aquellos, que si ser su obligación me prestaron su ayuda como los profesores del Máster en Matemática Avanzada de la UMU, y en particular, a Juan Jacobo Simón Pinero.

Resúmen

En 1998 Patrick Dehornoy y Luis Paris introdujeron en [33] la noción de grupos Garside, como una generalización de los grupos Artin-Tits de tipo esférico, o tipo Coxeter finito. Desde entonces, muchos autores han desarrollado la teoría de dichos Grupos, desde sus propiedades computacionales ([56, 58, 57, 41, 73, 63]...) así como propiedades más abstractas ([32, 62, 65, 19, 50, 49]....). Hoy en día, la teoría de Garside todavía está en desarrollo, de hecho, se podría decir que todavía está en sus primeros días de desarrollo, así pues, los grupos Garside no se han clasificado en diferentes familias de manera completa, y como veremos, algunas familias de Grupos Garside están lejos de ser completamente entendidas, de hecho, carecen de una clasificación/descripción adecuada en términos de grupos. Además, existen numerosas generalizaciones de los grupos de Garside en la literatura: pre-Garside [50], sistemas cuasi-Garside [49], gérmenes de Garside [31], l-grupos a derecha [70]. Sin embargo, en esta tesis no desarrollaremos ninguna de estas generalizaciones, así pues, nos quedaremos con la definición clásica de grupos de Garside introducida por P. Dehornoy y L. Paris, para más tarde, centrarnos en el estudio de una familia de Grupos de Garside en particular: la familia de las soluciones conjuntistas finitas, no degeneradas e involutivas de la ecuación de Yang-Baxter.

En el capítulo 1 de la presente tesis, veremos los conceptos básicos y necesarios sobre los grupos de Garside para el desarrollo de nuestros nuevos resultados acerca de este tema.

Empezaremos en la primera sección con una discusión histórica acerca de los grupos de Garside, esto es, que los motivó, exponiendo brevemente los grupos de trenzas y los grupos de Artin-Tits de tipo esférico, los cuales constituyen los primeros ejemplos de grupos de Garside, y que a su vez, suscitan un gran interés académico. En la siguiente sección, veremos la definición formal de monoide de Garside así como algunas de las propiedades básicas acerca de dichos monoides. Aún sin entrar en la definición rigurosa, la cual veremos más adelante, tenemos que un monoide M es de Garside si es un monoide Gaussiano (cancelativo, atómico y la divisibilidad a izquierda y derecha forma un retículo) y tiene un elemento de Garside $\Delta \in M$ (esto es, el conjunto de divisores a izquierda y derecha de Δ coinciden, es finito y genera el monoide M). Cabe destacar que pese a la artificialidad de dicha definición, son muchos los monoides que la cumplen, así como infinitos los elementos de Garside para un monoide de Garside M. Así pues, es fácil ver que tanto el mínimo común múltiplo como el máximo común divisor entre dos elementos de Garside, es también de Garside, así como cualquier potencia de un elemento de Garside es también de Garside. Sin embargo, como veremos en la presente tesis, existe un (único) elemento de Garside mínimo, el máximo común divisor de todos ellos, el cual es de especial relevancia, y el cual denotaremos por δ. Si M es un monoide de Garside, tenemos que M satisface el criterio de Ore, por lo que es posible definir el grupo de fracciones de M, al cual llamamos grupo de Garside y solemos denotar por G. Por

último, destacaremos en esta breve introducción, la estructura introducida por M. Picantin en [62] denominada cuasi-centro del monoide, $QZ(M)$, el cual es un monoide libre abeliano finitamente generado, cuyos elementos tienen todos la propiedad de ser equilibrados, esto es, el conjunto de divisores a izquierda y a derecha coinciden, como en el caso de los elementos de Garside, los cuales pertenecen a dicha estructura. Es gracias al cuasi-centro que podemos clasificar un monoide de Garside como indescomponible, si su cuasi-centro es un monoide cíclico infinito (generado por el elemento de Garside minimal δ).

Antes de entrar en mayor profundidad, tras ver algunas propiedad elementales en la sección segunda, veremos algunos ejemplos notables en la tercera sección, para así dar pie al estudio de los submonoides y de Garside en siguiente sección. Cabe destacar que como es frecuente en el estudio de cualquier estructura algebraica, los monoides de Garside contenidos a su vez dentro de un monoide de Garside son de especial interés. Sin embargo, dichos submonoides, de no guardar una especial relación con el monoide en el cual se encuentran contenidos puede no facilitar ninguna información acerca de este último, razón por la cual, la definición de submonoides parabólicos resulta imprescindible al tiempo que constituye una generalización de los subgrupos parabólicos usados en el estudio de los grupos de Artin-Tits. Destacamos el hecho de que la intersección de dos subgrupos parabólicos estándar es de nuevo un subgrupo parabólico estándar, lo cual permite a su vez definir la unión de dos subgrupos parabólico estándar a partir de la intersección de todos los subgrupos parabólicos estándar que los contienen. Con respecto a estos subgrupos parabólicos, esta aún por ver si las propiedades de dichos subgrupos en el caso de grupos de Artin se pueden trasladar en su totalidad a los grupos de Garside en general. Así mismo, dar una descripción completa de dichos subgrupos, es todavía, una labor pendiente de los investigadores de los grupos de Garside.

En la quinta y sexta sección, abordamos el producto Zappa-Szép de monoides, una generalización del producto semidirecto el cual nos permite expresar un monoide de Garside como producto de submonoides de Garside "más simples", esto es, indescomponibles en el sentido introducido pon M. Picantin. Los resultados de esta sección son un compendio de algunos de los resultados de V. Gebhardt y S. Tawn en [48], los cuales demuestran la equivalencia entre producto Zappa-Szép y el "producto cruzado" introducido por M. Picantin por el cual es posible escribir todo monoide de Garside como producto Zappa-Szép/producto de submonoides con cuasi-centro cíclico infinito. De hecho, aún cuando los autores de dichos artículos no lo mencionan, es fácil ver que el cuasi-centro de un monoide de Garside es cíclico si y solamente si el centro del monoide es cíclico. Como veremos más adelante, en el capítulo segundo, es posible descomponer un monoide de Garside como producto Zappa-Szép de submonoides cuyos elemento de Garside minimales forman una base para el cuasi-centro del monoide.

En la penúltima sección veremos como construir nuevos monoides de Garside a partir de dos monoides de Garside, esta vez, usando el producto libre amalgamado en lugar del Zappa-Szép, siendo este otro método para la construcción de ejemplos y familias de grupos de Garside. Finalmente, en la última sección expondremos de forma breve algunas de las buenas propiedades computacionales que exhiben los monoides de Garside, no siendo la finalidad de esta tesis la construcción de nuevos algoritmos, sin embargo, parece pues relevante tener en cuenta la posibilidad que ofrecen los monoides con la vista en futuras aplicaciones, como puede ser la criptografía, entre otras.

En el capítulo 2, expondremos algunos de nuestros resultados sobre los monoides de Garside en términos del producto Zappa-Szép. Entre estos resultados, cabe destacar nuestros hallazgos relacionando la descomposición del grupo de Garside G en términos Zappa-Szép, y factorización de los elementos de Garside del grupo G en términos de los elementos de Garside de los factores Zappa-Szép.

THEOREM 1. *Si G es un monoide de Garside tal que $G = H \bowtie K$ y denotamos por δ_G, δ_H y δ_K a los elementos de Garside minimales de G, H y K respectivamente, entonces $\delta_G = \delta_H \delta_K$.*

De forma más general, tenemos:

THEOREM 2. *Sea G un monoide de Garside el cual se descompone como el producto Zappa-Szép de ciertos monoides de Garside indescomponibles $H_1, H_2, ..., H_n$. Si δ_G denota el elemento de Garside minimal de G, entonces $\delta_G = \delta_1 \cdot \delta_2 \cdot ... \cdot \delta_n$ donde δ_i es el elemento de Garside minimal de H_i para $i = 1, ..., n$. Adicionalmente, $\delta_G^k = \delta_1^k \cdot \delta_2^k \cdot ... \cdot \delta_n^k$ para todo $k \in \mathbb{Z}$.*

Otro resultado a destacar, es la descripción de todos los elementos de Garside de un grupo de Garside. Cuando el grupo de Garside G es indescomponible, entonces todo elemento de Garside es una potencia positiva del elemento de Garside minimal de G. Para el caso descomponible, tenemos lo siguiente:

THEOREM 3. *Si G es un monoide de Garside tal que $G = H \bowtie K$ con H, K dos monoides de Garside indescomponible, entonces $\left\{\delta_H^a \delta_K^b \mid a, b \geq 1\right\}$ es el conjunto de todos los elementos de Garside de G.*

Motivados por el resultado anterior y teniendo por finalidad una descripción detallada de los elementos de Garside de G, demostramos el resultado siguiente:

THEOREM 4. *Sea G un monoide de Garside y sea $\{x_1, x_2, ..., x_r\}$ una base del cuasi-centro de G. Si A_i el es conjunto de átomos dividiendo a x_i, y llamamos N_i al submonoide generado por A_i, entonces G se descompone como el producto Zappa-Szép de los monoides $N_1, ..., N_r$, de modo que $N_i N_j = N_j N_i$ dados $i, j \in \{1, ..., r\}$, y tal que el producto Zappa-Szép es asociativo.*

Así pues, somo capaces de un grupo de Garside como producto de subgrupos parabólicos cuyos elementos de Garside conmutan entre sí formando una base para el cuasi-centro de G. Llamamos a los términos $N_1, ..., N_r$ anteriores, factores cuasi-centrales de G. Gracias al anterior resultado, tenemos ahora:

COROLLARY 5. *Sea G un monoide de Garside, y sea $N_1, N_2, ..., N_r$ su descomposición en términos cuasi-centrales. Si denotamos por δ_{N_i} al elemento de Garside minimal de N_i para $i = 1, ..., r$, entonces $\left\{\delta_{N_1}^{e_1} \cdot ... \cdot \delta_{N_r}^{e_r} | e_i \geq 1 \text{ for } i = 1, ..., r\right\}$ es el conjunto de todos los elementos de Garside de G.*

Finalmente, destacaremos un último resultado del capítulo segundo, el cual responde a la cuestión acerca de como podemos describir los submonoides parabólicos en términos de una descomposición Zappa-Szép, al tiempo que suscita la cuestión acerca de la relación que guardan los factores de una descomposición con respecto a la totalidad de los submonoides parabólicos.

THEOREM 6. *Sea G un monoide de Garside el cual admite una descomposición $M_1, M_2, ..., M_r$ en términos Zappa-Szép. Si S es un submonoide parabólico de G, entonces S es el producto Zappa-Szép de los submonoides $S_i = S \cap M_i$.*

En el capítulo 3, cambiamos de manera aparente el tema de estudio para centrarnos en la ecuación cuántica de Yang-Baxter, la cual bajo condiciones específicas, tal y como veremos, nos provee de una familia de grupos de Garside, de gran interés en la literatura académica.

Finalmente, remarcamos aquí que si bien todo lo expuesto en estos dos capítulos posee una gran relevancia para el estudio de los grupos de Garside, no todo aquello que posee una gran relevancia para dicho estudio esta presente en estos capítulos. Así mismo, pese a resultar posible el extenderse más en las cuestiones expuestas, resulta necesario poner fin a dicho desarrollo aún cuando con ello se dejen de explorar otras cuestiones. Así pues, quedan abiertas al estudio cuestiones ya abiertas con anterioridad, tales como si la existencia de un plegamiento fuerte de una solución implica necesariamente la descomponibilidad de dicha solución (véase [22]). Al mismo tiempo, resulta de interés razonar bajo que condiciones el producto de subgrupos parabólicos estándar sea de nuevo parabólico estándar, así como que relación guardan los factores principales con respecto a este tipo de subgrupos. Otra cuestión, sería si dichos subgrupos parabólicos forman un retículo, al igual los divisores del elemento de Garside Δ. Por último, destacar que dichos subgrupos en el caso de Artin-Tits han sido extensamente estudiados, razón por la cual, resulta de interés que propiedades de dichos grupos son generalizables al caso de Garside en general y cuales son particulares de dichos grupos.

Con el propósito de estudiar una familia en concreto de grupos de Garside, empezamos el capítulo tercero de esta tesis. Dicha familia resulta de gran interés, más allá de la teoría de Garside, pues aparece en el ámbito del estudio de la ecuación cuántica de Yang-Baxter (ECYB), la cual a suscitado un gran interés en el ámbito del álgebra en las últimas dos décadas. Esta ecuación, con origen en la física teórica, fue introducida por primera vez por C.N. Yang [81] y posteriormente en [5] de R. Baxter. Una solución de ECYB es un aplicación lineal $R : V \otimes V \longrightarrow V \otimes V$ donde V es un espacio vectorial que satisface una ecuación particular:

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}, \tag{0.0.1}$$

donde $R^{ij} : V \otimes V \otimes V \longrightarrow V \otimes V \otimes V$, viene dada por R en las componentes i, j y actuá como la identidad en el otra componente. El problema de construir y clasificar estas soluciones sigue siendo un área activa de investigación. Si bien el estudio del ECYB condujo a la fundación de grupos cuánticos en la física matemática, el estudio de las soluciones no degeneradas e involutivas se han relacionado en muchos áreas matemáticas, tales como: álgebras binomiales cuánticas [43, 44], semigrupos de tipo I y grupos de Bieberbach [47, 78, 54], coloraciones de curvas planas y 1-cociclos biyectivos [38], álgebras de Hopf triangulares, mínimas y semisimples [37], sistemas dinámicos [80], cristales geométricos [36], llaves y anillos radicales [68, 3], subgrupos regulares de las extensiones holomorfas y Hopf-Galois [39, 9], grupos de tipo central [26], "racks" y álgebras de Hopf [35, 66, 71], grupos trifactorizados ([77, 42]), grupos Garside, gérmenes de Garside y RC cálculos [19], y "cycle sets" [69], por el momento...

En la primera sección de este capítulo, veremos la definición de solución (conjuntista) de la ecuación de Yang-Baxter (EYB) siendo nuestro objeto exclusivo de estudio las dichas soluciones bajo las condiciones de no degeneradas, involutivas y estar definidas sobre un conjunto finito. Es para este tipo de soluciones, las cuales denotamos mediante el par (X, S) con X un conjunto finito y $S : X^2 \to X^2$, donde podemos definir otras estructuras algebraicas, tales como el grupo de estructura de la solución:

$$G(X, S) = \langle X \mid xy = tz \text{ dado } S(x, y) = (t, z) \rangle .$$

Así mismo, dado que cada una de las componentes de S define una permutación de X, si escribimos $S(x, y) = \big(g_x(y), f_y(x)\big)$ para x, y en X, entonces podemos definir el grupo de permutación asociado a la solución (X, S) como el subgrupo de $\mathrm{Sym}_{|X|}$ generado por $\{g_x \mid x \in X\}$. Además, existe una permutación T de X, tal que la identidad $f_x^{-1} T = T g_x$ se cumple para todo $x \in X$. Así pues, el subgrupo generado por $\{f_x \mid x \in X\}$ es isomorfo al grupo de permutación anteriormente definido. Dichos objetos matemáticos, fueron definidos por primera vez por P. Etingof, A. Soloviev y T. Schedler en [38], en donde, entre otras cosas, se clasificaron y construyen todas las soluciones finitas, no degeneradas e involutivas de la EYB, definidas sobre un conjunto X con a lo sumo 8 elementos. Así mismo, también cabe destacar otras aportaciones realizadas por lo autores del artículo anteriormente señalado a la clasificación y estudio de las soluciones, en particular, los conceptos de solución retractable y multipermutacional. Decimos que una solución (X, S) es retractable cuando $g_x = g_y$ para distintos $x, y \in X$. En tal caso, la relación $x \sim y$ establece una relación binaria de equivalencia compatible con S, tal que es posible definir una nueva solución sobre $X/\!\sim$, denominada solución retractada de (X, S). En los casos en que es posible retractar una solución y su solución retractada, reiteradamente hasta obtener la solución definida sobre un conjunto con un solo elemento, llamamos a dicha solución multipermutacional. Es con estas nociones, entre otras, que podemos entrar a desarrollar y profundizar acerca de las soluciones de la EYB en la cuarta sección del capítulo.

En la segunda sección, introducimos los grupos IYB y el concepto de I-estructura, el cual nos permite describir el grupo de estructura con mayor facilidad y claridad. Un grupo finito es un grupo IYB , si es el grupo de permutaciones de una solución finita no degenerada e involutiva de la EYB. En dicha sección exploramos algunos de los resultados sobre la IYB ya conocidos, de los cuales destacamos el hecho de que todo subgrupo de Hall de un grupo IYB es de nuevo un grupo IYB, además, el producto directo de grupos IYB es de nuevo IYB y todo grupo finito resoluble es isomorfo a un subgrupo de un grupo IYB. Si bien existen métodos para la construcción de grupos IYB a partir de otros grupos IYB, buena parte de estos resultados tan solo haremos referencia a los respectivos artículos, dada la complejidad de dichos resultados.

En la tercera sección, introducimos de forma breve la estructura algebraica conocida como Braza a izquierda, la cual también resulta de utilidad por tal de estudiar dichas soluciones, aún cuando no desarrollaremos nuestros resultados por esta vía, si bien nos resultará de utilidad a la hora de exponer ciertos resultados. Dicho de forma gruesa, una braza izquierda, es el resultado de definir sobre el grupo de permutaciones de una solución, una operación suma $+$, la cual proviene de considerar la permutación asociada a un elemento z del grupo de estructura asociado a la solución. Es por ello, que a partir de la terna $(\mathcal{G}, +, \cdot)$ definiendo la braza, tenemos una estructura que encapsula suficiente información sobre la solución,

como para resultar equivalente el estudio de brazas a izquierda con el estudio de soluciones finitas, no degeneradas e involutivas. Cabe destacar, que el concepto de braza a izquierda es un elemento que ha sido generalizado a través de las brazas a izquierda "retorcidas" ("skew left braces" en inglés), las cuales guardan a su vez relación con soluciones de la EYB en condiciones más generales de las señaladas con anterioridad.

En la sección cuarta, encontramos un compendio acerca de los principales resultados sobre las soluciones de la EYB para el caso de la presente tesis, esto es: no degeneradas, finitas e involutivas. Así, por ejemplo, sabemos que si (X, S) es una solución finita, no degenerada e involutiva, entonces es indescomponible si y solamente si el grupo de permutaciones $\mathcal{G}$ actúa transitivamente sobre X. Si $\mathcal{G}$ es abeliano, entonces la solución es retractable, y si es cíclico, entonces es multipermutacional. Tal y como estos resultados sugieren, existe una íntima relación entre propiedades de los grupos asociados y propiedades de las soluciones de la EYB. Dichos resultados, suscitaron nuestro interés por tal de incorporar técnicas de teoría de grupos al estudio de la EYB.

En la quinta sección, exponemos la relación entre las soluciones de la EYB y los grupos de Garside. Tal y como probó F. Chouraqui en [19], todo grupo de estructura de una solución finita, no degenerada e involutiva, es un grupo de Garside satisfaciendo ciertas propiedades adicionales (H), y recíprocamente, todo grupo de Garside satisfaciendo (H), es el grupo de estructura de una solución finita no degenerada e involutiva. Además, los conceptos de descomposición de una solución de la EYB y la descomposición en mediante el producto Zappa-Szép del grupo de Garside resultan ser equivalentes. Consecuentemente, los grupos de Garside satisfaciendo (H) constituyen una familia cerrada para la descomposición, sobre la cual disertaremos en lo restante de tesis.

Finalmente, en la última sección exploramos una nueva vía para la clasificación de los grupos de Garside relacionados con la EYB, haciendo uso de los hallazgos de P. Dehornoy en [29] y [30]. Tal y como el autor demostró, si G es el grupo de estructura de una solución finita, no degenerada e involutiva de la EYB (X, S), entonces existe un entero positivo d, el cual llamamos clase de Dehornoy, tal que G tiene un cociente W de orden $d^{|X|}$, el cual caracteriza a la solución. Además, dicho resultado es explicito, esto es, es posible construir el cociente W, incluso es posible representar de manera lineal tanto el grupo de estructura como su cociente. Este resultado, constituye una generalización a los grupos de Garside de las propiedades de los grupos de trenzas y de Artin-Tits de tipo esférico, y en particular, es una versión de los grupos de Coxeter para los grupos Garside asociados con la EYB. Es con todo lo expuesto hasta ahora, que estamos es disposición de exponer nuestros nuevos resultados acerca de la EYB, los cuales presentamos en los dos subsiguientes capítulos de la tesis.

En el capítulo 4 reproducimos los resultados publicados en nuestro artículo [7], siendo nuestro resultado principal el siguiente:

THEOREM 7. [7, A] *Sea (X, S) una solución finita no degenerada e involutiva de la EYB, y sea T su permutación diagonal. Si el orden de T y el cardinal de X son coprimos, entonces la solución (X, S) es descomponible o bien X tiene solo un elemento.*

Nuestro resultado, constituye una generalización de previos resultados de [67], así como de W. Rump en [69], el cual utilizamos para nuestra demostración:

THEOREM 8 (W. Rump). *Sea (X, S) una solución finita no degenerada e involutiva de la EYB. Si la permutación diagonal T es la identidad, entonces (X, S) es descomponible o bien X consta de un único elemento.*

Además, vemos durante la demostración de dicho resultado como podemos construir de forma natural los subgrupos de Hall del grupo de permutaciones, así como el hecho de que dichos subgrupos de Hall sean grupos IYB, esto es, el grupo de permutaciones de otra solución de la EYB, la cual podemos construir con facilidad.

Finalmente, en el capítulo 5, último de la tesis, exponemos nuestro últimos hallazgos acerca de la soluciones finitas, no degeneradas e involutivas de la EYB. Entre dichos resultados, cabe destacar el siguiente teorema y su corolario:

THEOREM 9. *Sea (X, S) una solución finita, no degenerada, involutiva e indescomponible de la EYB. Si su grupo de permutaciones $\mathcal{G}$ tiene tiene un elemento de orden primo q, entonces:*

- *q divide $|X|$, o bien*
- *q divide $p^n - 1$, con p primo y p^n dividiendo $|X|$.*

En particular, si $|X| = p^m$ y $p \neq q$, entonce q divide a $p^r - 1$, para algún $r \leq m - 1$.

COROLLARY 10. *Sea $\mathcal{G}$ el grupo de permutaciones de una solución finita, no degenerada e involutiva de la EYB (X, S). Denotamos $|X| = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, con p_i primos para $i = 1, \ldots, k$. Si G tiene un elemento de orden primo q, tal que q no divide a $|X|$, ni a ningún $p_i^n - 1$ con $n \leq n_i$, $i = 1, \ldots, k$, entonces (X, S) es una solución descomponible.*

Los resultados anteriores, pendientes de publicación, extienden algunos resultados ya conocidos en la literatura académica (véase [16] o [55]). Sin embargo, nuestro resultado, de carácter más general, profundiza en los posibles primos del grupo de permutaciones, lo cual resulta de gran relevancia por tal de clasificar dichas soluciones de la EYB. De forma resumida, si (X, S) es una solución de la EYB satisfaciendo las hipótesis del resultado anterior, sabemos existe un un subgrupo A normal abeliano del grupo de estructura G, tal que $G/A \cong \mathcal{G}$. Además, tal y como demostró P. Dehornoy, existe N normal en G tal que $G/N = W$ es un subgrupo de orden d^n, donde n es el cardinal de X, el cual caracteriza a la solución y tiene a $\mathcal{G}$ como cociente. Es fácil ver que si T es la permutación diagonal asociada a (X, S), entonces el orden de T divide a d, y n divide al orden de $\mathcal{G}$. Es por ello que los primos de T y n son primos de la clase de Dehornoy d. Pese a que el recíproco es un problema todavía abierto, nuestro resultado restringe los posibles primos para W, de tal forma que esperamos sea útil en un futuro por tal de clasificar dichos subgrupos, y en consecuencia, clasificar las soluciones de la EYB para el caso finito, no degenerado e involutivo. Así mismo, al igual que en capítulo anterior, es notorio que el orden de la permutación diagonal T juega un papel fundamental en el estudio de las soluciones de la EYB, sin embargo, su implicación no resulta para nada intuitiva. Al mismo tiempo, la clase de Dehornoy, determina los primos del grupo W en cuestión, y si bien son pocos los ejemplos de los que disponemos, la cuota $n!$ donde n es el cardinal de X, parece lejos de ser ajustada, pues sabemos que se cumple $d \leq n$ para toda solución con $n \leq 10$. Así mismo, cabe destacar que la aproximación establecida por F. Cedó y J. Okniński en [16], donde estudian soluciones tal que ninguna potencia de primo

divide a $n = |X|$, si bien resulta restrictivo, resulta lógico dada la conexión tan estrecha entre los primos dividiendo a X y al orden de W, así como la complejidad añadida al considerar potencias de primos, tal y como ilustra nuestro resultado. Cabe pues esperar, que sea el tiempo quien decida el papel de los números primos en el estudio de la EYB...

Resum

El 1998 Patrick Dehornoy i Luis Paris van introduir a [33] la noció de grups de Garside, com una generalització dels grups Artin-Tits de tipus esfèric, o tipus Coxeter finit. Des de llavors, molts autors han desenvolupat la teoria dels grups esmentats, des de les seves propietats computacionals ([56, 58, 57, 41, 73, 63]...) així com propietats més abstractes ([32, 62, 65, 19, 50, 49]....). Avui dia, la teoria de Garside encara està en desenvolupament, de fet, es podria dir que encara està en els primers dies de desenvolupament, així doncs, els grups de Garside no s'han classificat en diferents famílies de manera completa, i com veurem, algunes famílies de grups Garside estan lluny de ser completament enteses, de fet, no tenen una classificació/descripció adequada en termes de grups. A més, existeixen nombroses generalitzacions dels grups de Garside a la literatura: pre-Garside [50], sistemes quasi-Garside [49], gèrmens de Garside [31], l-grups a dreta [70]. No obstant això, en aquesta tesi no desenvoluparem cap d'aquestes generalitzacions, així doncs, ens quedarem amb la definició clàssica de grups de Garside introduïda per P. Dehornoy i L. Paris, per més tard, centrar-nos en l'estudi d'una família de Grups de Garside en particular: la família de les solucions conjuntistes finites, no degenerades i involutives de la equació de Yang-Baxter.

Al capítol 1 de la present tesi, veurem els conceptes bàsics i necessaris sobre els grups de Garside per al desenvolupament dels nostres nous resultats apropa aquest tema.

Començarem a la primera secció amb una discussió històrica sobre dels grups de Garside, és a dir, que els va motivar, exposant breument els grups de trenes i els grups d'Artin-Tits de tipus esfèric, els quals constitueixen els primers exemples de grups de Garside, i que alhora susciten un gran interès acadèmic. A la següent secció, veurem la definició formal de monoide de Garside així com algunes de les propietats bàsiques sobre aquests monoides. Encara sense entrar a la definició rigorosa, la qual veurem més endavant, tenim que un monoide M és de Garside si és un monoide Gaussià (cancel·latiu, atòmic i la divisibilitat a esquerra i dreta forma un reticle) i té un element de Garside $\Delta \in M$ (és a dir, el conjunt de divisors a esquerra i dreta de Δ coincideixen, és finit i genera el monoide M). Cal destacar que malgrat l'artificialitat d'aquesta definició són molts els monoides que la compleixen, així com infinits els elements de Garside per a un monoide de Garside M. Així doncs, és fàcil veure que tant el mínim comú múltiple com el màxim comú divisor entre dos elements de Garside, és també de Garside, així com qualsevol potència d'un element de Garside és també de Garside. Tanmateix, com veurem en aquesta tesi, existeix un (únic) element de Garside mínim, el màxim comú divisor de tots ells, el qual és d'especial rellevància, i el qual denotarem per δ. Si M és un monoide de Garside, M satisfà el criteri d'Ore, per la qual cosa és possible definir el grup de fraccions de M, al qual anomenem grup de Garside i solem denotar per G. Finalment, destacarem en aquesta breu introducció, l'estructura introduïda per M. Picantin a [62], anomenada quasi-centre del monoide, $QZ(M)$, el qual és un monoide lliure abelià

finitament generat, els elements del qual tenen tots la propietat de ser equilibrats, és a dir, el conjunt de divisors a esquerra i a dreta coincideixen, com en el cas de els elements de Garside, els quals pertanyen a aquesta estructura. És gràcies al quasi-centre que podem classificar un monoide de Garside com a indescomponible, si el seu quasi-centre és un monoide cíclic infinit (generat per l'element de Garside minimal δ).

Abans d'entrar en més profunditat, després de veure algunes propietats elementals a la secció segona, veurem alguns exemples notables a la tercera secció, per donar així peu a l'estudi dels submonoides de Garside a la següent secció. Cal destacar que com és freqüent a l'estudi de qualsevol estructura algebraica, els monoides de Garside continguts alhora dins d'un monoide de Garside són d'especial interès. No obstant això, aquests submonoides, de no guardar una relació especial amb el monoide en el qual es troben continguts, pot no facilitar cap informació sobre aquest darrer, raó per la qual, la definició de submonoides parabòlics resulta imprescindible alhora que constitueix una generalització dels subgrups parabòlics usats a l'estudi dels grups d'Artin-Tits. Destaquem el fet que la intersecció de dos subgrups parabòlics estàndard és de nou un subgrup parabòlic estàndard, la qual cosa permet definir la unió de dos subgrups parabòlic estàndard a partir de la intersecció de tots els subgrups parabòlics estàndard que els contenen. Pel que fa a aquests subgrups parabòlics, encara està per veure si les propietats dels dits subgrups en el cas de grups d'Artin es poden traslladar íntegrament als grups de Garside en general. Així mateix, donar una descripció completa d'aquests subgrups, és encara, una tasca pendent dels investigadors dels grups de Garside.

A la cinquena i sisena secció, abordem el producte Zappa-Szép de monoides, una generalització del producte semidirecte el qual ens permet expressar un monoide de Garside com a producte de submonoides de Garside "més simples", és a dir, indescomponibles en el sentit introduït per M. Picantin. Els resultats d'aquesta secció són un compendi d'alguns dels resultats de V. Gebhardt i S. Tawn a [48], els quals demostren l'equivalència entre producte Zappa-Szép i el "producte creuat" introduït per M. Picantin, pel qual és possible escriure tot monoide de Garside com producte Zappa-Szép de submonoides amb quasi-centre cíclic infinit. De fet, encara que els autors d'aquests articles no ho esmenten, és fàcil veure que el quasi centre d'un monoide de Garside és cíclic si i només si el centre del monoide és cíclic. Com veurem més endavant, al capítol segon, és possible descompondre un monoide de Garside com a producte Zappa-Szép de submonoides els element de Garside minimals formen una base per al quasi-centre del monoide.

A la penúltima secció veurem com construir nous monoides de Garside a partir de dos monoides de Garside, aquesta vegada, usant el producte lliure amalgamat en lloc del Zappa-Szép, sent aquest altre mètode per a la construcció d'exemples i famílies de grups de Garside. Finalment, a la darrera secció exposarem de forma breu algunes de les bones propietats computacionals que exhibeixen els monoides de Garside, no sent la finalitat d'aquesta tesi la construcció de nous algorismes, però, sembla doncs rellevant tenir en compte la possibilitat que ofereixen els monoides amb la vista en futures aplicacions, com pot ser la criptografia, entre d'altres.

Al Capítol 2, exposarem alguns dels nostres resultats sobre els monoides de Garside en termes del producte Zappa-Szép. Entre aquests resultats, cal destacar les nostres troballes relacionant la descomposició del grup de Garside G en termes Zappa-Szép, i la factorització

dels elements de Garside del grup G en termes dels elements de Garside dels factors Zappa-Szép.

THEOREM 11. *Si G és un monoide de Garside tal que $G = H \bowtie K$ i denotem per δ_G, δ_H i δ_K als elements de Garside minimals de G, H i K respectivament, llavors $\delta_G = \delta_H \delta_K$.*

De manera més general, tenim:

THEOREM 12. *Sigui G un monoide de Garside el qual es descompon com el producte Zappa-Szép de certs monoides de Garside indescomponibles $H_1, H_2, ..., H_n$. Si δ_G denota l'element de Garside minimal de G, llavors $\delta_G = \delta_1 \cdot \delta_2 \cdot ... \cdot \delta_n$ on δ_i és el element de Garside minimal de H_i per a $i = 1, ..., n$. Addicionalment, $\delta_G^k = \delta_1^k \cdot \delta_2^k \cdot ... \cdot \delta_n^k$ per a tot $k \in \mathbb{Z}$.*

Un altre resultat a destacar, és la descripció de tots els elements de Garside d'un grup de Garside. Quan el grup de Garside G és indescomponible, aleshores tot element de Garside és una potència positiva de l'element de Garside minimal de G. Per al cas descomponible, tenim el següent:

THEOREM 13. *Si G és un monoide de Garside tal que $G = H \bowtie K$ amb H, K dos monoides de Garside indescomponible, llavors $\left\{\delta_H^a \delta_K^b \mid a, b \geq 1\right\}$ és el conjunt de tots els elements de Garside de G.*

Motivats pel resultat anterior i tenint per finalitat una descripció detallada dels elements de Garside de G, demostrem el resultat següent:

THEOREM 14. *Sigui G un monoide de Garside i sigui $\{x_1, x_2, ..., x_r\}$ una base del quasi-centre de G. Si A_i és el conjunt d'àtoms dividint a x_i, i anomenem N_i al submonoide generat per A_i, aleshores G es descompon com el producte Zappa-Szép dels monoides $N_1, ..., N_r$, de manera que $N_i N_j = N_j N_i$ donats $i, j \in \{1, ..., r\}$, i tal que el producte Zappa-Szép és associatiu.*

Així doncs, som capaços d'un grup de Garside com a producte de subgrups parabòlica els elements del qual Garside commuten entre si formant una base per al quasicentre de G. Anomenem els termes $N_1, ..., N_r$ anteriors, factors quasi centrals de G. Gràcies a això resultat, ara tenim:

COROLLARY 15. *Sigui G un monoide de Garside i sigui $N_1, N_2, ..., N_r$ la seva descomposició. en termes gairebé centrals. Si denotem per δ_{N_i} al element mínim de Garside de N_i per a $i = 1, ..., r$, llavors $\left\{\delta_{N_1}^{e_1} \cdot ... \cdot \delta_{N_r}^{e_r} | e_i \geq 1 \text{ per } i = 1, ..., r\right\}$ és el conjunt de tots els elements de Garside de G.*

Finalment, destacarem un darrer resultat del capítol segon, el qual respon a la qüestió sobre com podem descriure els submonoides parabòlics en termes d'una descomposició Zappa-Szép, alhora que suscita la qüestió sobre la relació que guarden els factors d'una descomposició respecte a la totalitat de els submonoides parabòlics.

THEOREM 16. *Sigui G un monoide de Garside el qual admet una descomposició $M_1, M_2, ..., M_r$ en termes Zappa-Szép. Si S és un submonoide parabòlic de G, llavors S és el producte Zappa-Szép dels submonoides $S_i = S \cap M_i$.*

Al Capítol 3, canviem de manera aparent el tema d'estudi per centrar-nos en l'equació quàntica de Yang-Baxter, la qual sota condicions específiques, tal com veurem, ens proveeix d'una família de grups de Garside, de gran interès en la literatura acadèmica.

Finalment, remarquem aquí que si bé tot allò exposat en aquests dos capítols té una gran rellevància per a l'estudi dels grups de Garside, no tot allò que posseeix una gran rellevància per a dit estudio aquesta present en aquests capítols. Així mateix, malgrat resultar possible estendre's més en les qüestions exposades, és necessari posar fi a aquest desenvolupament encara que amb això es deixin d'explorar altres qüestions. Queden, doncs, obertes a l'estudi qüestions ja obertes amb anterioritat, com si l'existència d'un plegament fort d'una solució implica necessàriament la descomponibilitat d'aquesta solució (vegeu [22]). Al mateix temps, resulta d'interès raonar sota quines condicions el producte de subgrups parabòlics estàndard sigui de nou parabòlic estàndard, així com quina relació guarden els factors principals respecte a aquest tipus de subgrups. Una altra qüestió seria si aquests subgrups parabòlics formen un reticle, igual que els divisors de l'element de Garside Δ. Finalment, cal destacar que aquests subgrups a el cas d'Artin-Tits han estat extensament estudiats, raó per la qual cosa resulta d'interès que propietats d'aquests grups són generalitzables al cas de Garside en general i quins són particulars d'aquests grups.

Amb el propòsit d'estudiar una família en concret de grups de Garside, comencem el capítol tercer d'aquesta tesi. Aquesta família resulta de gran interès, més enllà de la teoria de Garside, ja que apareix a l'àmbit de l'estudi de l'equació quàntica de Yang-Baxter (ECYB), la qual ha suscitat un gran interès en l'àmbit de l'àlgebra a les darreres dues dècades. Aquesta equació, amb origen en la física teòrica, va ser introduïda per primera vegada per CN Yang [81] i posteriorment a [5] de R. Baxter. Una solució d'ECYB és una aplicació lineal $R : V \otimes V \longrightarrow V \otimes V$ on V és un espai vectorial que satisfà una equació particular:

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}, \tag{0.0.2}$$

on $R^{ij} : V \otimes V \otimes V \longrightarrow V \otimes V \otimes V$, ve donada per R en els components i, j i actua com la identitat a l'altra component. El problema de construir i classificar aquestes solucions segueix sent una àrea activa de recerca. Si bé el estudi de l'ECYB va conduir a la fundació de grups quàntics a la física matemàtica, l'estudi de les solucions no degenerades i involutives s'han relacionat en moltes àrees matemàtiques, com ara: àlgebres binomials quàntiques [43, 44], semigrups de tipus I i grups de Bieberbach [47, 78, 54], coloracions de corbes planes i 1-cocicles bijectius [38], àlgebres de Hopf triangulars, mínimes i semisimples [37], sistemes dinàmics [80], vidres geomètrics [36], claus i anells radicals [68, 3], subgrups regulars de les extensions holomorfes i Hopf-Galois [39, 9], grups de tipus central [26], "racks" i àlgebres de Hopf [35, 66, 71], grups trifactoritzats ([77, 42]), grups Garside, gèrmens de Garside i RC càlculs [19], i "cycle sets" [69], de moment...

A la primera secció d'aquest capítol, veurem la definició de solució (conjuntista) de l'equació de Yang-Baxter (EYB) essent el nostre objecte exclusiu d'estudi les dites solucions sota les condicions de no degenerades, involutives i estar definides sobre un conjunt finit. És per a aquest tipus de solucions, les quals denotem mitjançant el per a (X, S) amb X un conjunt finit i $S : X^2 \to X^2$, on podem definir altres estructures algebraiques, tals com

el grup d'estructura de la solució:

$$G(X,S) = \langle X \mid xy = tz \text{ donat } S(x,y) = (t,z) \rangle .$$

Així mateix, atès que cadascuna de les components de S defineix una permutació de X, si escrivim $S(x,y) = \big(g_x(y), f_y(x)\big)$ per a x, y a X, llavors podem definir el grup de permutació associat a la solució (X,S) com el subgrup de $\mathrm{Sym}_{|X|}$ generat per $\{g_x \mid x \in X\}$. A més, existeix una permutació T de X, tal que la identitat $f_x^{-1}T = Tg_x$ es compleix per a tot $x \in X$. Així doncs, el subgrup generat per $\{f_x \mid x \in X\}$ és isomorf al grup de permutació anteriorment definit. Aquests objectes matemàtics, van ser definits per primera vegada per P. Etingof, A. Soloviev i T. Schedler a [38], on, entre altres coses, es van classificar i construir totes les solucions finites, no degenerades e involutives de l'EYB, definides sobre un conjunt X amb com a màxim 8 elements. Així mateix, també cal destacar altres aportacions realitzades pels autors de l'article anteriorment assenyalat a la classificació i estudi de les solucions, en particular, els conceptes de solució retractable i multipermutacional. Diem que una solució (X,S) és retractable quan $g_x = g_y$ per a diferents $x, i \in X$. En aquest cas, la relació $x \sim i$ estableix una relació binària d'equivalència compatible amb S, tal que és possible definir una nova solució sobre $X/\!\sim$, anomenada solució retractada de (X,S). En els casos en què és possible retractar una solució i la seva solució retractada, reiteradament fins a obtenir la solució definida sobre un conjunt amb un sol element, anomenem aquesta solució multipermutacional. És amb aquestes nocions, entre d'altres, que podem entrar a desenvolupar i aprofundir sobre les solucions de l'EYB a la quarta secció del capítol.

A la segona secció, introduïm els grups IYB i el concepte de I-estructura, que ens permet descriure el grup d'estructura amb més facilitat i claredat. Un grup finit és un grup IYB , si és el grup de permutacions d'una solució finita no degenerada e involutiva de l'EYB. En aquesta secció explorem alguns dels resultats sobre la IYB ja coneguts, dels quals destaquem el fet que tot subgrup de Hall d'un grup IYB és de nou un grup IYB, a més, el producte directe de grups IYB és de nou IYB i tot grup finit resoluble és isomorf a un subgrup d'un grup IYB. Si bé hi ha mètodes per a la construcció de grups IYB a partir d'altres grups IYB, bona part d'aquests resultats tan sols farem referència als respectius articles, atesa la complexitat d'aquests resultats.

A la tercera secció, introduïm de forma breu l'estructura algebraica coneguda com a Braza a esquerra, la qual també resulta d'utilitat per estudiar aquestes solucions, encara que no desenvoluparem els nostres resultats per aquesta via, si bé ens resultarà útil alhora d'exposar certs resultats. Dit de forma gruixuda, una braça esquerra, és el resultat de definir sobre el grup de permutacions d'una solució, una operació suma $+$, la qual prové de considerar la permutació associada a un element z del grup d'estructura associat a la solució. És per això que a partir de la terna $(\mathcal{G}, +, \cdot)$ definint la braça, tenim una estructura que encapsula suficient informació sobre la solució, com per resultar equivalent l'estudi de braces a esquerra amb l'estudi de solucions finites, no degenerades i involutives. Cal destacar que el concepte de braça a esquerra és un element que ha estat generalitzat a través de les braces a esquerra "retorçades" ("skew left braces" en anglès), les quals guarden alhora relació amb solucions de l'EYB en condicions més generals de les assenyalades amb anterioritat.

A la secció quarta, trobem un compendi sobre els principals resultats sobre les solucions de l'EYB per al cas de la present tesi, és a dir: no degenerades, finites i involutives. Així, per exemple, sabem que si (X,S) és una solució finita, no degenerada e involutiva, llavors és

indescomponible si i només si el grup de permutacions $\mathcal{G}$ actua transitivament sobre X. Si $\mathcal{G}$ és abelià, llavors la solució és retractable, i si és cíclic, aleshores és multipermutacional. Tal com aquests resultats suggereixen, hi ha una íntima relació entre propietats dels grups associats i propietats de les solucions de l'EYB. Aquests resultats van suscitar el nostre interès per incorporar tècniques de teoria de grups a l'estudi de l'EYB.

A la cinquena secció, exposem la relació entre les solucions de l'EYB i els grups de Garside. Tal com va provar F. Chouraqui a [19], tot grup d'estructura d'una solució finita, no degenerada e involutiva, és un grup de Garside satisfent certes propietats addicionals (H), i recíprocament, tot grup de Garside satisfent (H), és el grup d'estructura d'una solució finita no degenerada e involutiva. A més, els conceptes de descomposició d'una solució de l'EYB i la descomposició a través del producte Zappa-Szép del grup de Garside resulten ser equivalents. Conseqüentment, els grups de Garside satisfent (H) constitueixen una família tancada per a la descomposició, sobre la qual dissertarem en la resta de tesis.

Finalment, a la darrera secció explorem una nova via per a la classificació dels grups de Garside relacionats amb l'EYB, fent ús de les troballes de P. Dehornoy a [29] i [30]. Tal com va demostrar l'autor, si G és el grup d'estructura d'una solució finita, no degenerada e involutiva de l'EYB (X, S), llavors hi ha un sencer positiu d, el qual anomenem classe de Dehornoy, tal que G té un quocient W d'ordre $d^{|X|}$, el qual caracteritza a la solució. A més, aquest resultat és explícit, és a dir, és possible construir el quocient W, fins i tot és possible representar de manera lineal tant el grup d'estructura com el quocient. Aquest resultat, constitueix una generalització als grups de Garside de les propietats dels grups de trenes i d'Artin-Tits de tipus esfèric, i en particular, és una versió dels grups de Coxeter per als grups Garside associats amb l'EYB. És amb tot allò exposat fins ara, que estem és disposició d'exposar els nostres nous resultats sobre l'EYB, els quals presentem en els dos subsegüents capítols de la tesi.

Al capítol 4 reproduïm els resultats publicats al nostre article [7], sent el nostre resultat principal el següent:

THEOREM 17. [7, A] *Sigui (X, S) una solució finita no degenerada e involutiva de l'EYB, i sigui T la seva permutació diagonal. Si l'ordre de T i el cardinal de X són coprims, aleshores la solució (X, S) és descomponible o bé X té sol un element.*

El nostre resultat, constitueix una generalització de resultats previs de [67], així com de W. Rump a [69], el qual utilitzem per a la nostra demostració:

THEOREM 18 (W. Rump). *Sigui (X, S) una solució finita no degenerada e involutiva de l'EYB. Si la permutació diagonal T és la identitat, llavors (X, S) és descomponible o bé X consta d'un únic element.*

A més, veiem durant la demostració del resultat com podem construir de forma natural els subgrups de Hall del grup de permutacions, així com el fet que aquests subgrups de Hall siguin grups IYB, és a dir, el grup de permutacions d'una altra solució de l'EYB, la qual podem construir amb facilitat.

Finalment, al capítol 5, últim de la tesi, exposem les nostres últimes troballes sobre la solucions finites, no degenerades i involutives de l'EYB. Entre aquests resultats, cal destacar el següent teorema i el seu corol·lari:

THEOREM 19. *Sigui (X,S) una solució finita, no degenerada, involutiva i indescomponible de l'EYB. Si el vostre grup de permutacions $\mathcal{G}$ té un element d'ordre primer q, llavors:*

- *q divideix $|X|$, o bé*
- *q divideix p^n-1, amb p primer i p^n dividint $|X|$.*

En particular, si $|X|=p^m$ i $p\neq q$, aleshores q divideix p^r-1, per a algun $r\leq m-1$.

COROLLARY 20. *Sigui $\mathcal{G}$ el grup de permutacions d'una solució finita, no degenerada e involutiva de l'EYB (X,S). Denotem $|X|=p_1^{n_1}\cdot\ldots\cdot p_k^{n_k}$, amb p_i primers per a $i=1,\ldots,k$. Si G té un element d'ordre primer q, tal que q no divideix $|X|$, ni cap p_i^n-1 amb $n\leq n_i$, $i=1,\ldots,k$, aleshores (X,S) és una solució descomponible.*

Els resultats anteriors, pendents de publicació, n'estenen alguns resultats ja coneguts en la literatura acadèmica (vegeu [16] o [55]). Tot i això, el nostre resultat, de caràcter més general, aprofundeix en els possibles cosins del grup de permutacions, la qual cosa resulta de gran rellevància per tal de classificar aquestes solucions de l'EYB. De manera resumida, si (X,S) és una solució de l'EYB satisfent les hipòtesis del resultat anterior, sabem existeix un subgrup A normal abelià del grup d'estructura G, de manera que $G/A\cong\mathcal{G}$. A més, tal i com va demostrar P. Dehornoy, existeix N normal a G tal que $G/N=W$ és un subgrup d'ordre d^n, on n és el cardinal de X, el qual caracteritza a la solució i té a $\mathcal{G}$ com a quocient. És fàcil veure que si T és la permutació diagonal associada a (X,S), llavors l'ordre de T divideix d, i n divideix l'ordre de $\mathcal{G}$. És per això que els primers de T i n són primers de la classe de Dehornoy d. Tot i que el recíproc és un problema encara obert, el nostre resultat restringeix els possibles primers per W, de manera que esperem sigui útil en un futur per tal de classificar aquests subgrups, i en conseqüència, classificar les solucions de l'EYB per al cas finit, no degenerat i involutiu. Així mateix, igual que en el capítol anterior, és notori que l'ordre de la permutació diagonal T juga un paper fonamental en l'estudi de les solucions de l'EYB, però, la seva implicació no resulta gens intuïtiva. Alhora, la classe de Dehornoy, determina els cosins del grup W en qüestió, i si bé són pocs els exemples de què disposem, la quota $n!$ on n és el cardinal de X, sembla lluny de ser ajustada, ja que sabem que es compleix $d\leq n$ per a tota solució amb $n\leq 10$. Així mateix, cal destacar que l'aproximació establerta per F. Cedó i J. Okniński a [16], on estudien solucions tals que cap potència de primer divideix a $n=|X|$, si bé resulta restrictiu, resulta lògic donada la connexió tan estreta entre els cosins dividint a X i a l'ordre de W, així com la complexitat afegida en considerar potències de cosins, tal com il·lustra el nostre resultat. Cal doncs esperar, que sigui el temps qui decideixi el paper dels nombres primers a l'estudi de l'EYB...

Summary

In 1998 Patrick Dehornoy and Luis Paris introduced the notion of Garside groups as a generalization of Artin-Tits groups of spherical type, or finite Coxeter type, in [33]. Since then, many authors have developed the theory of such Groups, from computational properties ([56, 58, 57, 41, 73, 63]...) to more abstract ones ([32, 62, 65, 49, 50, 19]...). Nowadays, Garside theory is still in development, in fact, one could say it is still on its early days of development, as one such example, Garside groups have not been classified into different families, and as we shall see, some families of Garside Groups are far from being completely understood, in fact, they lack of a proper classification/description in terms of groups. Additionally, generalizations of the Garside groups we shall deal with are also common in literature: pre-Garside [50], quasy-Garside systems [49], Garside families and germs [31], right l-groups [70]. It is the aim of the thesis to gain depth about such topics, in particular in Chapter 1, we shall see an introduction to Garside groups and monoids, starting with the historical motivation for such groups and discovering the main, and latest results, regarding Garside monoids and groups. In Chapter 2, we shall expose some of our work regarding Garside monoids in terms of Zappa-Szép product, a special kind of product generalizing the semidirect product, which allows us to decompose every Garside monoid in terms of a product of smaller ones, in fact, every Garside monoid can be written as a Zappa-Szép product of Garside monoids with cyclic center, or in Garside terminology, irreducible Garside submonoids. Beyond this, we decided to study a particular Garside family, related with the so called Yang-Baxter equation (YBE), with the aim of describing the groups related with such family.

The quantum Yang-Baxter equation (QYBE) is a significant equation in theoretical physics, first introduced by C.N. Yang [81] and later in [5] by R. Baxter. A solution of QYBE is a linear map $R : V \otimes V \longrightarrow V \otimes V$ where V is a vector space, satisfying a particular equation. The problem of constructing and classifying these solutions remains an active area of research. While the study of the QYBE lead to the foundation of quantum groups if mathematical physics, the study of non-degenerate, braided involutive solutions has been related with many different mathematical areas, such as: quantum binomial algebras [43, 44], semigroups of I-type and Bieberbach groups [47, 78, 54], coloring's of plane curves and bijective 1-cocycles [38], semisimple minimal triangular Hopf algebras [37], dynamical systems [80], geometric crystals [36], braces and radical rings [68, 3], regular subgroups of the holomorf and Hopf-Galois extensions [39, 9], groups of central type [26], racks and Hopf algebras [71, 35, 66], trifactorized groups ([77, 42]), Garside groups, Garside germs and RC-calculus [19], and cycle sets [69], for the moment...

In Chapter 3, we review the Yang-Baxter equation, in particular, we specialize for the non-degenerate, finite and involutive case, since those are the necessary and sufficient conditions for the YBE to relate with Garside monoids. In Chapter 4, we expose our first new results with regard to the YBE, which consist of a generalization of a previous result of Wolfgang Rump. Finally, in Chapter 5 we expose the new results of our second article, which describes the possible primes dividing a group that characterizes a solution of the YBE.

Contents

CHAPTER 1

Introduction to Garside groups

1.1. Historical discussion

Before to introduce Garside groups, we shall digress a little bit and discuss Braid groups and Artin-Tits groups in a shallow manner. Since these groups have a very rich literature and are a topic of active research in the present times, to condense such knowledge into the present text becomes unreasonable. However, to include them seems necessary since they constitute the first examples of a family of Garside groups; more precisely, Garside groups where introduced in [33] by Patrick Dehornoy and Luis Paris in the following terms: "It is known that a number of algebraic properties of the braid groups extend to arbitrary finite Coxeter type Artin groups. Here we show how to extend the results to more general groups that we call Garside groups".

The braid group on n strands (denoted B_n), also known as the Artin braid group, is the group whose elements are equivalence classes of n-braids (e.g. under ambient isotopy), and whose group operation is composition of braids.

Definition 21. The **Braid group** with n strands B_n can be presented by:

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \text{and } \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| \neq 1 \right\rangle.$$

Braid groups can be geometrically represented by strands between two sets with n points, and in particular, braid groups are related with knot theory.

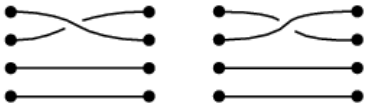

Figure 1.1.1. Two different braids from B_4.

It is easy to see that B_n embeds as a subgroup into B_{n+1}. Additionally, if we add σ_i^2 for all $i = 1, ..., n$ in the relations defining B_n, we obtain Σ_n, the permutation group of n symbols. In particular, Σ_n is a finite quotient which characterizes the infinite group B_n.

Generalizing braid groups we find Artin-Tits groups, named after Emil Artin, due to his early work on braid groups in the 1920s to 1940s, and Jacques Tits who developed the theory of a more general class of groups in the 1960s. Formally speaking:

Definition 22. An **Artin–Tits group** A is a finitely presented group with presentation:

$$A = \left\langle X \mid \left\langle x_i, x_j \right\rangle^{m_{ij}} = \left\langle x_j, x_i \right\rangle^{m_{ji}} \text{ for all } x_i \neq x_j \text{ in } X \right\rangle,$$

where $m_{ij} \geq 2$ are positive integers such that $m_{ij} = m_{ji}$ and $\langle s,t\rangle^k = ststst...$ with k terms in total.

In particular, one says that an Artin–Tits group is of spherical type when the associated **Coxeter group** (obtained by adding the relation x_i^2 for all $x_i \in X$, to the presentation) is finite. This particular case, represents a generalization of Braid groups, and a particular family of Garside groups.

REMARK 23. As the reader may notice, if $X = \{x_1, x_2, ..., x_n\}$, $m_{i,j} = 3$ for $|i-j| = 1$ and $m_{ij} = 2$ otherwise, then presentation above A is the classical presentation of the braid group on $n+1$ strings.

Within the study of Artin-Tits groups, the notions of reducible and irreducible, soon appeared in literature. Without going into the details, every reducible Artin-Tits groups decomposes in terms of irreducible ones. Consequently, to describe the irreducible Artin-Tits groups was one of the main goals of research. This task, for the special case of Artin-Tits groups of spherical type, was finally achieved by H.S.M. Coxeter in [24]. More precisely, every irreducible Artin-Tits groups of spherical type belongs to one of the infinite families $A_n, B_n, D_n, I_2(n)$ or is one of the six exceptional groups E_6, E_7, E_8, F_4, H_3 and H_4.

The classification of indecomposable Artin-Tits groups spherical type, as implied by the existence of the 6 sporadic groups, presents a challenging endeavor. Similarly, extending this classification to Garside groups, which can be viewed as a broader category, also presents a formidable open problem in the current research landscape.

1.2. Garside monoids and groups

Various equivalent representations of Garside groups exist, and numerous generalizations have been developed since their inception. However, in this text, we will focus solely on one particular presentation. To understand this, we'll first need to cover some basic definitions.

DEFINITION 24. A monoid M is said to be **right cancellative** if for every $a, b, c \in M$ $a \cdot c = b \cdot c$ implies $a = b$. Similarly, it is said to be **left cancellative** if for every $a, b, c \in M$ $c \cdot a = c \cdot b$ implies $a = b$. A monoid M is said to be **cancellative** if it is both left and right cancellative.

DEFINITION 25. An element a in a monoid M is an **atom** if for all b, c in M so that $a = b \cdot c$ then either $b = 1$ or $c = 1$.

For any element x in the monoid M, $\| x \|$ denotes the **norm of the element** x, supremum of the lengths of all expressions of x in terms of atoms of M.

DEFINITION 26. A monoid M is said an **atomic monoid** if M is generated by its atoms and $\| x \|$ is finite for all $x \in M$.

DEFINITION 27. If M is a monoid, and the equality $a \cdot c = b$ holds for some $a, b, c \in M$, then we say that: a is a **left divisor** of b; b is a **right multiple** of a; c is a **right divisor** of b; and b is a **left multiple** of c.

Given a monoid M we may consider two associated partial orders:

$$a \leq_L b \text{ if } a \text{ left divides } b,$$

$$a \leq_R b \text{ if } a \text{ right divides } b.$$

for $a, b \in M$. When every pair of elements have a supremum and a infimum, then the partial order is said to be a lattice. For the above partial orders, being a lattice implies that for each pair of elements $a, b \in M$, there exist a unique **least common multiple**, to the left and to the right, denoted by $a \vee_L b$ and $a \vee_R b$, and also a unique **greatest common divisor**, to the left and to the right, denoted by $a \wedge_L b$ and $a \wedge_R b$. If $a \vee_R b$ is the right least common multiple of a, b then $a \vee_R b = ac = bd$ for some elements $c, d \in M$; we will denote this "right complements" c and d by $a\backslash b$ and $b\backslash a$ respectively, so that $a \vee_R b = a(a\backslash b) = b(b\backslash a)$.

Definition 28. An element Δ in M is said **balanced** if the sets of left divisors and right divisors coincide, and the **set of divisors** is denoted by $\mathrm{Div}(\Delta)$.

Definition 29. A monoid M is a **Garside monoid** when:

1. M is cancellative.
2. M is atomic.
3. $\leq_R$ and $\leq_L$ are both lattices in M.
4. There exists a balanced element $\Delta \in M$, called **Garside element** of M, such that:
   a) For each $a \in M$, $a \leq_R \Delta$ iff $a \leq_L \Delta$.
   b) The set of divisors of Δ is finite and generates M.

Remark 30. Conditions 1,2 and 3 define the so called **Gaussian monoids**, thus a Garside group is a Gaussian monoid with a Garside element. Underlying

Because Garside groups satisfy Ore's condition, every Garside monoid M satisfies embeds in its group of fractions, see [33] or alternatively [23, 1.23].

Definition 31. A **Garside group** is the group of fractions of a Garside monoid.

When there is no ambiguity,G^+ will represent the underlying Garside monoid of a given Garside group G, and in some occasions, the elements of G^+ are referred to as positive elements. It is a simple fact that G^+ is a **conical** monoid, that is, if $a, b \in G^+$ are so that $a \cdot b = 1$ then $a = b = 1$, i.e., no non-trivial element in G^+ has an inverse. This turns out to be a good property and Garside groups work as expected with respect its underlying Garside monoid.

Lemma 32. [49, 1.11] *Let G be a Garside group. For every element g in the group G there exists a unique pair (a, b) of elements in the monoid G^+ such that $g = a^{-1}b$ and the elements a and b are coprime for left divisibility. Furthermore if cg lies in $G^+$for some c in G^+then a right divides c.*

Lemma 33. [63, 3.1] *Let G be a Garside group. Let a, b be conjugate elements in G, then a, b are also conjugated by an element in G^+.*

Before we conclude this section, it's worth noting that alternative definitions of Garside groups can be found in the literature (see [33, 27, 49, 62]), however we followed the lines of [19] instead. Additionally, a definition regarding other structures can also be made:

Theorem 34. [64]

1. *A divisibility monoid is a Garside monoid if and only if every pair of atoms admits common multiples.*

2. *A Garside monoid is a divisibility monoid if and only if the lattice of its simple elements is a hypercube.*

A simple fact about Garside elements is that if Δ is a Garside element, then so is Δ^n for every natural number $n \geq 1$. Another simple fact is that if Δ_1, Δ_2 are Garside elements so is its greater common divisor, and so, every Garside monoid has a minimal Garside element with respect to divisibility.

It is known that the Garside element of a Garside monoid M, induces a permutation on the set of atoms of M, that is, given an atom a we have $a\Delta = \Delta b$ for some atom b (see [33, 2.6]). Hence, since the set of atoms is finite, there exists a positive integer e so that Δ^e in a central element. This power e is usually referred to as the **exponent of the monoid**.

THEOREM 35. [58, 3.17] *Let G be a Garside group with Garside element Δ and exponent e. Then every finite subgroup of $G/\langle\Delta^e\rangle$ is cyclic.*

Next result shows that Garside groups have finite abelian subgroup rank.

PROPOSITION 36. [56, 3.5] *If H is an abelian subgroup of a Garside group G then $|N_G(H) : C_G(H)| < \infty$.*

PROPOSITION 37. [18] *Every Garside group has finite virtual cohomological dimension, hence every abelian subgroup of a Garside group is finitely generated.*

The above result is generalized by Corollary 86, which states that every solvable subgroup of a Garside group is finitely generated and virtually abelian. Since the structure group of a solution is both solvable and a Garside group, it is virtually abelian. Actually, in section 2.5 of [38], an abelian group with finite index is defined. Additionally, with regard of groups of I-type, which also provide solutions of the YBE, authors in [47] also proved that this groups are abelian-by-finite.

DEFINITION 38. Two elements x, y in a monoid are said **commensurable** if there exist positive integers k, r so that x^k and y^r are conjugated.

THEOREM 39. [58, 3.1] *Let G be a Garside group. Then $Z(G)$ is cyclic if and only if for every pair of Garside elements Δ_1, Δ_2 of G are commensurable.*

Garside groups with cyclic center play a central role in Garside group theory, as we shall see later on.

1.3. Some examples of Garside groups

We already know that all Braid groups and Artin-Tits groups of spherical type are Garside Groups.

EXAMPLE 40. [33, Example #4] Given n positive integers $p_1, ..., p_n$, the group defined by

$$\left\langle x_1, x_2, ..., x_n | x_1^{p_1} = x_2^{p_2} = ... = x_n^{p_n} \right\rangle,$$

is a Garside group with Garside element $\Delta = x_1^{p_1}$. In particular, pq-Torus knot groups presented by $\langle x, y | x^p = y^q \rangle$ is a family of Garside groups.

EXAMPLE 41. The group $G = \langle a, b | aba = b^2 \rangle$ is a Garside group with minimal Garside element $\Delta = abab = b^3$. Notice that aba is the least common multiple to the left and to the right for the atoms a, b, but is not a Garside element since ab is a left divisor but not a right divisor.

In example above, if $x = ab$ and $y = b$, then x, y generate the group and satisfy the relation $x^2y^{-1} = y^2$, that is $x^2 = y^3$, and so it is a $2,3$-Torus knot group. Thus, one Garside group can have different presentations.

EXAMPLE 42. Another simple example is the Garside group (see [72, p 228] or [61, 4.2])

$$G = \langle a, b \mid ababa = b^2 \rangle,$$

its minimal Garside element is $\Delta = b^3$. In this case, we see that relations defining the group are not length preserving. However, if we take $x = ab$ and $y = b$, then $x^3y^{-1} = ababa = b^2 = y^2$ and $x^3 = y^3$. Thus we can provide, in this case, a different presentation that is length preserving.

REMARK 43. In the present text we won't deal with problems regarding different presentations and shall always consider a fixed presentation for a Garside group.

EXAMPLE 44. The Artin-Tits Group $G = \langle a, b \mid aba = bab \rangle$ has $\Delta = aba$ as non central Garside element and $Z(G) = \langle \Delta^2 \rangle$. That is, it has exponent 2.

1.4. Garside subgroups and parabolic subgroups

The notions of parabolic and Garside subgroups was introduced by E. Godelle in [49]. In that article the notion of quasi-Garside is used, which allows to the set of divisors of the Garside element, $\mathrm{Div}(\Delta)$, to be infinite. However, since we only deal with the finite case, we have omitted the term quasi-Garside in the statement of the results.

DEFINITION 45. Given a Garside group G with Garside element Δ, if δ is balanced element of G^+, the **support** of δ is the set $\mathrm{Supp}_{G^+}(\delta)$ of atoms of G^+ that are in $\mathrm{Div}(\delta)$.

[49, 1.6] Let G be a Garside group with Garside element Δ, and H be a subgroup of G. Set $H^+ = H \cap G^+$. We say that the subgroup H is a **Garside subgroup** of the group G if:

1. the submonoid H^+ is a closed sublattice of the monoid G^+;
2. for every $x \in H^+$, the elements of G^+ $x \wedge_L \Delta$,$x \wedge_R \Delta$ are also in H^+;
3. the subgroup H is generated by the submonoid H^+.

REMARK 46. Definition above implies that the Garside subgroup structure is related with the structure within it exits. Additionally, notation above for H^+ is coherent with the fact that H is the group generated by H^+.

PROPOSITION 47. [49, 1.15] *Let G be a Garside group with Garside element Δ. Let H be a Garside subgroup of G. Then, we have*

$$\mathrm{N}_G(H) = H^+ \cdot \mathrm{N}_G\left(H^+\right).$$

PROPOSITION 48. [49, 1.14] *Let G be a Garside group and let H and K be two Garside subgroups of G. Then, the subgroup $H \cap K$ is a Garside subgroup of the group G and the submonoid $(H \cap K) \cap G^+$ is equal to the submonoid $H^+ \cap K^+$.*

THEOREM 49. [49, 1.10] *Let G be a Garside group with Garside element Δ, and let H be a Garside subgroup of G. Set $H^+ = H \cap G^+$.*

1. *The subset $H^+ \cap Div(\Delta)$ is a closed sublattice of G^+. In particular, there exists an element δ in H^+ that is balanced in H^+ and such that $H^+ \cap Div(\Delta) = Div_{H^+}(\delta)$.*
2. *H is a Garside group with Garside element δ and H^+ as underlying Garside monoid.*

DEFINITION 50. [49, 2.2] Let G be a Garside group with Garside element Δ.

1. Let δ be a balanced element of $\mathrm{Div}(\Delta)$. Denote by G_δ the subgroup of G generated by $\mathrm{Supp}_{G^+}(\delta)$. We say that G_δ is a **standard parabolic subgroup** of the group G if $\mathrm{Div}(\delta) = \mathrm{Div}(\Delta) \cap G_\delta^+$. In that case, the monoid G_δ^+ is called a **parabolic submonoid** of the monoid G^+.
2. Let H be a subgroup of G. We say that H is a **parabolic subgroup** of G if it is conjugated to a standard parabolic subgroup of G.

REMARK 51. Notice that in theorem above, unlike in the previous definition, the element δ is balanced in the Garside submonoid, but not necessarily balanced in G^+. The significance of this will be highlighted in subsequent discussions.

LEMMA 52. [49, 2.1] *Let G be a Garside group with Garside element Δ. Let δ be a balanced element of $Div(\Delta)$; we denote by H the subgroup of G generated by $Supp_{G^+}(\delta)$, and we set $H^+ = H \cap G^+$. Then H is a Garside group with Garside element δ and $Supp_{G^+}(\delta)$ as set of atoms. Furthermore, the subgroup H is a Garside subgroup with δ as Garside element if and only if the equality $Div(\delta) = Div(\Delta) \cap H^+$ holds in G^+.*

We can derive two consequences of theorem above:

1. Standard parabolic subgroups are indeed Garside subgroups.
2. Garside groups within a Garside group may not necessarily be related with the group's overall structure. Therefore, a subgroup being Garside is not the same as being a Garside subgroup.

In the same article, [49, 3.4,3.5.3.5,3.8], many questions are asked and answered, in all cases with a negative answer. The following is a compilation of them:

Let G be a Garside group with Garside element Δ. Let X denote the set of atoms of G^+ and for $Y \subseteq X$ a set of atoms of the monoid G^+, denote by G_Y^+ the submonoid generated by Y. Additionally, let δ be a balanced element of $\mathrm{Div}(\Delta)$.

1. Is the subgroup G_Y^+ necessarily a Garside subgroup?
   a) If the subgroup G_Y^+ is a Garside group, is it necessarily a Garside subgroup?
   b) If the subgroup G_Y^+ is a Garside subgroup, is it necessarily a (standard) parabolic subgroup?
   c) Are $\mathrm{Div}(\Delta) \cap G_\delta^+$ and $\mathrm{Div}(\delta)$ necessarily equal?
   d) Do we have necessarily a one-to-one correspondence between the balanced elements in $\mathrm{Div}(\Delta)$ and the standard parabolic subgroups?
   e) Is the intersection of two Garside subgroups generated by sets of atoms necessarily (a Garside subgroup) generated by a set of atoms?

In so far, we have seen that the class of Garside groups strictly contains the class of Garside subgroups, which also strictly contains the class of (standard) parabolic subgroups. Therefore, since these notions differ, one should inquire about the special properties associated with each of them. The following can be taken as an approximation to the this problem.

LEMMA 53. [49, 1.9] *Let G be a Garside group with Garside element Δ, and H be a Garside subgroup of G. Set $H^+ = H \cap G^+$. Let h_1, h_2 belong to H^+. Then the element h_1 is a left (right) divisor of h_2 in H^+ if and only if h_1 is a left (right) divisor of h_2 in G^+.*

While one implication is trivial, the non-trivial part is far from trivial since, in Garside monoids, one element can have many possible words in terms of atoms, even of different lengths. One intuitive way, and likely easy, to approach this property relates with its Garside element: since the Garside subgroup H satisfies, by definition, that every common divisor of an arbitrary element of $H^+$and the Garside element $\Delta \in G^+$ belongs to H^+, this properties extends from the Garside element Δ to the whole Garside monoid G^+. One way to rephrase the previous is: "from the Garside element to the Garside monoid". Although this is not a rigorous mathematical claim, it feels intuitive and will be repeated later on.

Now is the turn of parabolic submonoids:

PROPOSITION 54. [49, 2.5] *Let G_δ^+ be a parabolic submonoid of a Garside monoid G^+. Then G_δ^+ is closed under left divisibility and under right divisibility. That is, if $g \in G^+$ is such that g left divides, or right divides, some $x \in G_\delta^+$, then $g \in G_\delta^+$.*

Result above is an strong version of the previous result for Garside subgroups. Now, for the case of parabolic subgroups, not only the divisibility relation is inherited, but also the element dividing. Similarly as before, we see from its definition, if G_δ^+ is a parabolic submonoid, the relation $\mathrm{Div}(\delta) = \mathrm{Div}(\Delta) \cap G_\delta^+$ is satisfied, and thus, the divisors of δ and Δ are shared in G_δ^+. In some sense, the sentence "from the Garside element to the whole monoid", applies again for the previous proposition.

PROPOSITION 55. [49, 2.7] *Let G be a Garside group, and G_δ, G_τ be two standard parabolic subgroups of G. Then $G_{\delta\wedge\tau}$ is a standard parabolic subgroup of G, which is equal to the subgroup $G_\delta \cap G_\tau$.*

Unfortunately, for the join of two standard parabolic subgroups no similar result is known. In the next sections we shall see a way to create bigger Garside groups starting with two Garside, so that they become standard parabolic subgroups of the new structure.

In [25] the following is said: "We show that, in an Artin–Tits group of spherical type, the intersection of two parabolic subgroups is a parabolic subgroup. Moreover, we show that the set of parabolic subgroups forms a lattice with respect to inclusion. This extends to all Artin–Tits groups of spherical type a result that was previously known for braid groups".

Question. Can the previous mentioned be generalized to the context of Garside groups?

1.5. Irreducible Garside monoids

Concerning parabolic subgroups and Artin-Tits groups, there exists the concept of irreducible Garside monoids, which serve as a natural extension of irreducibility in Artin-Tits

monoids to the realm of Garside groups. This accomplishment was made by Matthieu Picantin in [62, Theorem B], where he successfully described all Garside monoids as a sequence of "crossed products" of Garside parabolic submonoids. However, we will forgo detailing the crossed product concept due to its high level of complexity and technicality. It was later shown to be equivalent to the Zappa-Szép product, which we will introduce later in the text.

Based on the fact the every Garside element Δ acts on the monoid, that is, given $a \in G^+$ there exists $b \in G^+$ so that $a\Delta = \Delta b$, M. Picantin introduced the quasi-center of a Garside monoid, which comprises the set elements behaving like Δ. Formally:

DEFINITION 56. [62, B] Assume that M is a Garside monoid, X is its set of atoms, and G is its group of fractions. Then the **quasi-center** of M (resp. the **quasi-centralizer** of X in G) is the submonoid $QZ(M) = \{x \in M | \text{given } a \in X, \text{exists } b \in X \text{ so that } xa = bx\}$ (resp. the subgroup $QZ(G) = \{x \in G | \text{given } a \in X, \text{exists } b \in X \text{ so that } xa = bx\}$).

LEMMA 57. [62, 1.8] *Assume that M is a thin Gaussian monoid, X is the set of its atoms, and G is its group of fractions. Then:*

1. *the quasi-centralizer of X in G is the group of fractions of the quasi-center of M;*
2. *the center of G is the group of fractions of the center of M.*

DEFINITION 58. Assume that M is a Garside monoid. For every a in M, we define

$$\Delta_a = \vee_R \{b \backslash a; b \in M\}.$$

Notice that a similar definition can be made by means of the left least common multiple $\vee_L$, however, they turn out to be equivalent by [62, 2.13].

Moving forward, we will explore a number of key findings and definitions from the same article, which will prove to be significant later on.

PROPOSITION 59. [62, 2.2,2.6,2.7,2.8,2.9] *Let M be a Garside monoid and a an element of M. Then:*

1. *The element Δ_a is quasi-central. More precisely, the application $a \mapsto \Delta_a$ is a surjection from M onto the quasi-center of M.*
2. *If $\Delta_a = a$ then a is quasi-central.*
3. *If a divides a quasi-central element b in M, then Δ_a and divides b.*
4. *The set $\{\Delta_x \mid x \text{ atom of } M\}$ is basis for the quasi-center of M.*
5. *Either $\Delta_a = \Delta_b$ or $\Delta_a \wedge \Delta_b = 1$ for b in M.*
6. *The quasi-center is closed under $\vee$ and $\wedge$.*
7. $\Delta_a \vee \Delta_b = \Delta_{a \vee b}$.

REMARK 60. Although $\vee$ and $\wedge$ should have been considered also to the left and to the right, for elements in the quasi-center this notions turn out tho be equivalent by definition.

Different characterizations of irreducible Garside monoids exists, but from a chronological point of view, the first definition of irreducible Garside monoid is the following one: a Garside monoid is **irreducible** if $\Delta_a = \Delta_b$ for every atom a, b of G^+.

PROPOSITION 61. [62, 4.1] *Let G^+ be an irreducible Garside monoid with minimal Garside element Δ. Denote by e is its exponent, and G is its group of fractions. Then:*

1. *The quasi-center of G^+ is the infinite cyclic submonoid generated Δ.*
2. *The center of G^+ (resp. of G) is the infinite cyclic submonoid (resp. subgroup) generated by Δ^e.*

1.6. Zappa-Szép decompositions

In order to solve some problems regarding Picantin's crossed-product, in [48] the authors study the Zappa-Szép product of monoids for the case of Garside monoids, showing that in this case they are equivalent.

DEFINITION 62. A monoid M is the (internal) **Zappa-Szép product** of two submonoids A and B, $M = A \bowtie B$, if every element $x \in M$ can be uniquely written as $x = a \cdot b = b' \cdot a'$, with $a, a' \in A$, $b, b' \in B$.

It is easy to see that Zappa-Szép product generalized direct and semidirect product for monoids. If $G^+ = H^+ \bowtie K^+$ is a Garside monoid, then the Garside group G can be presented as

$$G = \left\{ h_1 k_1 k_2^{-1} h_2^{-1} \mid h_i \in H, k_i \in K,\ i = 1, 2 \right\}.$$

DEFINITION 63. A Garside monoid is an **indecomposable Garside monoid**, if it cannot be written as a Zappa-Szép product of two non-trivial submonoids.

Next results allow us to avoid Picantin's crossed product.

THEOREM 64. [48, 39] *A Garside monoid M is irreducible if and only if it is (Zappa-Szép) indecomposable.*

Actually, the notion of crossed product introduced by Picantin, is equivalent, for Garside monoids, to the notion of Zappa-Szép product as the following result shows.

THEOREM 65. [48, 33] *If G^+ is a Garside monoid with submonoids H^+ and K^+, one has $G^+ = H^+ \bowtie K^+$ if and only if G^+ can be written as a crossed product of the monoids H^+ and K^+.*

REMARK 66. It is a easy fact that the set of atoms of G^+ is the disjoint union of the sets of atoms of H^+ and K^+. For that, take a an atom of G^+ and write $a = hk$ for some $h \in H^+$, $k \in K^+$, then being an atom implies either $h = 1$ or $k = 1$, and so a is a atom of H^+ or K^+. So far we know that if G^+ is not an indecomposable monoid, it can be written as the product of two Garside submonoids H^+ and K^+. Now we can repeat the same argument for H^+,K^+ if they are not indecomposable and continue applying this argument recursively. Because the set of atoms of G^+ is finite, we are ensured that this process terminates, and we obtain a decomposition in terms of finitely many indecomposable Garside submonoids. Unfortunately, this Zappa-Szép decomposition is not associative, and so, not necessarily unique.

Usually, we will denote this indecomposable Garside submonoids by $H_1, ..., H_n$, and will consider them in order from left to right on the (recursive) decomposition of G^+, which we shall not specify.

REMARK 67. We know that a Garside monoid is by definition generated by the set of divisors of the Garside element Δ. Thus, Δ can be written as the product of atoms (irreducible elements). Similarly, by results above we have that the whole Garside monoid can be written

as the product of some irreducible Garside submonoids generated by some disjoint subsets of atoms of G. Thus, the analogy: "from the Garside element to the Garside monoid" is again satisfied.

LEMMA 68. [57, 4.5] *If δ_H and δ_K are the minimal Garside elements of H^+ and K^+, respectively, then $\delta_H \cdot \delta_K$ is the minimal Garside element of $H^+ \bowtie K^+$.*

THEOREM 69. [48, 34] *If $G^+ = H^+ \bowtie K^+$ is a Garside monoid, then H^+ and K^+ are parabolic submonoids of G^+. In particular, H^+ and K^+ are Garside monoids. Additionally, factorization of a Garside element Δ of G^+, $\Delta = \Delta_H \Delta_K$, produces Garside elements of Δ_H of H^+ and Δ_K of K^+.*

It is not always true that the product of Garside elements of the monoids H^+ and K^+ produces a Garside element of G^+ (see [48, 36]).

LEMMA 70. [48, 17] *Suppose that $G^+ = H^+ \bowtie K^+$ and that H^+ is conical. Then, for all $x, y \in G^+$, $xy \in K^+$ implies that $x \in K^+$ and $y \in K^+$. Consequently, if $h \in H^+$, every divisor of h belongs to H^+.*

LEMMA 71. [48, 18] *Suppose that $G^+ = H^+ \bowtie K^+$ and that H^+ is conical. Let $g \in G^+$ and write its factorization as $g = ha = bh'$ with $h, h' \in H^+$ and $a, b \in K^+$. If a is an atom of K^+,then so is b.*

REMARK 72. By definition, every Garside monoid G^+ is conical, thus so are H^+ and K^+. Thus, there is not additional hypothesis when G^+ is a Garside monoid.

PROPOSITION 73. [48, 35] *Let $G^+ = H^+ \bowtie K^+$ be a Garside monoid and let $k \in K^+$. Then $\Delta_k^{G^+} = \bigvee \{x \backslash k : x \in G^+\} \in K^+$.*

THEOREM 74. [48, 37] *Suppose that $G^+ = H^+ \bowtie K^+$ and that H^+ and K^+ are Garside monoids. Then G^+ is a Garside monoid.*

Before to proceed, we shall recall some results from previous chapter in order to facilitate the reader the understanding of some proofs.

PROPOSITION 75. [62] *Let G be a monoid, then:*

1. *If $ab = ba$ and $a \wedge_R b = 1$, then $ab = a \vee b$.*
2. *If $b \in QZ(G)$ and $a \in G$ divides b, then Δ_a divides b.*
3. *$QZ(G)$ is closed under $\vee$ and $\wedge$.*

1.7. Free groups and HNN extensions

In this section we shall see a different kind of product of Garside monoids. They were introduce by Matthieu Picantin in [65] and remarkably, the class of Garside groups is closed under this product (alternatively, extensions).

DEFINITION 76. Let M_1, M_2, H be monoids with morphisms $\phi_1 : H \hookrightarrow M_1$ and $\phi_2 : H \hookrightarrow M_2$. The **amalgamated free product** of M_1 and M_2 with respect to H, ϕ_1, and ϕ_2 is the monoid

$$\langle M_1 \star M_2 : \phi_1(h) = \phi_2(h), h \in H \rangle^+,$$

where $M_1 \star M_2$ stands for the free product of M_1 and M_2. When $H = \langle h \rangle^+$is cyclic, we denote $\phi_1(h) = h_1, \phi_2(h) = h_2$, and the **cyclic amalgamated free product** $M_1 \star_{h_1 = h_2} M_2$.

For the first result regarding such product, we recall that a root of an element x is an element h so that there exists a positive integer k so that $h^k = x$.

THEOREM 77. [65, 16] *Let M_1 and M_2 be some Garside monoids. Then, for any root h_1 of any Garside element in M_1 and any root h_2 of any Garside element in M_2, the cyclic amalgamated free product $M_1 \star_{h_1=h_2} M_2$ is a Garside monoid.*

Actually, a necessary assumption is that $\phi_i(H)$ has to contain a Garside element of M_i for $i \in \{1,2\}$. When restricted to cyclic amalgamated submonoids, the latter naturally expresses in terms of roots of Garside elements.

COROLLARY 78. [65, 23] *Let M_1 and M_2 be some Garside monoids. The (enveloping group of) the cyclic amalgamated free product $M_1 \star_{h_1=h_2} M_2$ is Garside if and only if h_1 is a root of some Garside element in M_1 and h_2 is a root of some Garside element in M_2.*

DEFINITION 79. Let M and H be two monoids with morphisms $\phi_1 : H \hookrightarrow M$ and $\phi_2 : H \hookrightarrow M$. The **HNN extension** of M with respect to H, ϕ_1, and ϕ_2 is the monoid

$$\langle M, t : \phi_1(h)t = t\phi_2(h), h \in H\rangle^+ .$$

For the following result, we recall that if x is an element in a Garside monoid G^+, then $\|x\|$ is the supremum of the lengths of every possible word for x.

THEOREM 80. [65, 26] *Let M be a Garside monoid and H be the infinite cyclic monoid $\langle h\rangle^+$ with a morphism $\phi_i : H \hookrightarrow M$ for $i \in \{1,2\}$ satisfying $\|\phi_1(h)\| = \|\phi_2(h)\|$. Then the enveloping group of the HNN extension $\langle M, t : \phi_1(h)t = t\phi_2(h)\rangle^+$ is a Garside group if and only if $\phi_1(h)$ and $\phi_2(h)$ are two n-th roots of the same Garside element in M for some $n > 0$.*

Here again, a necessary assumption is actually that $\phi_1(H)$ and $\phi_2(H)$ have to contain the same Garside element of M. When restricted to cyclic HNN extensions, the case when H is cyclic, the latter naturally expresses in terms of roots of Garside elements.

Despite the great results achieved by Picantin, as the reader may know, free products are quite difficult to deal with and few properties can be easily derived from results above. In particular, this thesis does not contain any new results following this line. Finally, we end this section with two remarkable results proven by means of the HNN extensions.

PROPOSITION 81. [65, 35] *A non-cyclic one-relator group is Garside if and only if its center is non-trivial.*

1.8. Computational properties

This section is devoted to summarize some of the literature regarding Garside monoids "good monoids", in particular, some of the common computational problems can be achieved and besides some other properties regarding monoids. The reader is expected to be already familiarized with Garside monoids, and no formal definitions are included in this section since a reference is always provided.

In [33] is proved for Garside groups: "the language of normal forms is regular, symmetric, and geodesic, has the 5-fellow traveler property, and has the uniqueness property, implying that Garside groups are geodesically fully biautomatic".

In [27] is proved that all Garside Groups are biautomatic meaning that normal forms can be computed by means of a finite automaton.

THEOREM 82. [63, 3.4] *The conjugacy problem in Garside groups is solvable.*

PROPOSITION 83. [73, 2.5] *If G is the group of fractions of a tame Garside monoid, then the problem of existence of n-th roots in G is decidable.*

PROPOSITION 84. [56] *Every abelian subgroup of a Garside group is torsion-free and finitely generated.*

PROPOSITION 85. [28] *Every Garside group is torsion-free.*

COROLLARY 86. [57, 7.3] *Let G be a Garside group.*

1. *Every solvable subgroup of G is finitely generated and virtually abelian.*
2. *G cannot contain subgroups isomorphic to the additive group of rational numbers or the group of p-adic fractions $\mathbb{Q}_p = \left\{k/p^l \mid k \in \mathbb{Z}, l \in \mathbb{N}\right\}$.*
3. *For any finite set X, of semigroup generators for $G, t_X(G)$ is a closed discrete set.*

THEOREM 87. [57, 8.1] *Let G be a Garside group and $g \in G$.*

1. *There are only finitely many $n \in \mathbb{N}$ such that g has an n-th root.*
2. *For each $n \in \mathbb{N}$, there are only finitely many conjugacy classes of n-th roots of g.*

The following is claimed in [57] section 5: "Because Garside groups are torsion-free and have solvable word problem, the order problem is trivial and the intersection problem for cyclic subgroups is equivalent to the generalized power problem."

THEOREM 88. [57, 5.2] *The power problem and the power conjugacy problem are solvable in Garside groups.*

As a final claim, the reader is advised that not every computational problem regarding Garside groups is easy, indeed, encryption algorithms using Garside monoids have been developed. For more computation properties the reader is referred to articles above mentioned and also to [73, 59, 6].

CHAPTER 2

On Zappa-Szép decompositions

In order to simplify notation and improve readability, in this chapter we will omit the super index + in order to refer to a monoid, that is, we will write G for both the Garside monoid and the Garside group. In case such a difference becomes relevant it will be explicitly specified. Additionally, whenever we have a quasi-central element δ of the monoid, and $a \in G$ also in the monoid, $a\delta = \delta b$ for some element $b \in G^+$. Thus, δ defines a morphism in the monoid and we will consider the conjugated element $a^\delta = \delta^{-1}a\delta = b$, despite no inverse can be taken in the monoid.

DEFINITION 89. [48] The tuple $(\Delta_G, \Delta_H, \Delta_K)$ is a **Zappa-Szép Garside structure** for the Zappa-Szép product $G = H \bowtie K$, if:

1. G is a Garside monoid (and hence H and K are also Garside monoids);
2. $\Delta_G, \Delta_H, \Delta_K$ are Garside elements for G, H, K, respectively; and
3. $\Delta_G = \Delta_H\Delta_K$ holds.

THEOREM 90. *If $(\Delta_G, \Delta_H, \Delta_K)$ is a Garside tuple, then Δ_H and Δ_K are quasi-central elements of G.*

PROOF. From symmetry of Zappa-Szép product, it suffices to show that Δ_K is quasi-central in G. If we denote by A_G, A_H, A_K to the set of atoms of G, H, K, then it is a trivial fact that $A_G = A_H \dot\cup A_K$. Because Δ_K permutes the atoms in A_K, given $a \in A_H$, we shall prove that $a^{\Delta_K} \in A_H$. Given that Δ_H is a Garside element of H, there is c in A_H, so that $c^{\Delta_H} = a$ and since Δ_G is a Garside element of G, $c^{\Delta_G} \in A_G$. Now notice that c^{Δ_G} cannot belong to A_K, otherwise, $\left(c^{\Delta_G}\right)^{\Delta_K^{-1}} \in A_K$ and since $\Delta_G = \Delta_H\Delta_K$, we get $\left(c^{\Delta_G}\right)^{\Delta_K^{-1}} = c^{\Delta_H} = a \in A_H \cap A_K$, a contradiction. Thus, $a^{\Delta_K} = \left(c^{\Delta_H}\right)^{\Delta_K} = c^{\Delta_G} \in A_H$, as desired. □

A Garside monoid is by definition indecomposable if and only if its quasi-center is infinite cyclic. However, the following easy result provides a similar characterization in terms of its center.

COROLLARY 91. *Let G be a non-trivial Garside monoid. Then $Z(G)$ is cyclic in and only if G is a indecomposable Garside monoid.*

PROOF. By way of contradiction suppose G is decomposable and write $G = H \bowtie K$ with H, K parabolic submonoids. If Δ_G is a central Garside element of G, we write $\Delta_G = \Delta_H\Delta_K$ with Δ_H, Δ_K Garside elements of H and K. Because Δ_H, Δ_K are quasi-central elements of G and there exists an integer $n \geq 1$ so that $\Delta_H^n, \Delta_K^n \in Z(G)$. If δ is the generator of the center of G, then $\delta \in G$ divides both $\Delta_H^n \in H$ and $\Delta_K^n \in K$ and so by Proposition 54, δ belongs to $H \cap K = 1$, a contradiction. □

REMARK 92. We can recover Theorem 39 using result above. With notation above, let $\Delta_1 = \Delta_H^2\Delta_K$ and $\Delta_2 = \Delta_H\Delta_K^2$. Because Δ_H, Δ_K are in the quasi-center of G, they commute and $\Delta_1 = \Delta_H^2\Delta_K = \Delta_K\Delta_H^2$ and $\Delta_2 = \Delta_H\Delta_K^2 = \Delta_K^2\Delta_H$ are the unique ways of writing those elements. Thus they are different elements, and similarly, every power of Δ_1 and Δ_2 are different elements of G. Since Δ_1, Δ_2 are Garside elements, there exist positive integers r, s so that Δ_1^r, Δ_2^s are central Garside elements of G. Thus Δ_1^r and Δ_2^s are two different Garside elements that are not commensurable. Conversely, if we assume G has cyclic center, then it is indecomposable and every Garside element is a power of the Garside element δ generating the quasi-center of G, thus every pair of Garside elements are commensurable.

REMARK 93. In Definition 58, the quasi-central elements Δ_a where defined as the l.c.m. of the complements of a. Because we are dealing with different Garside monoids at the same time, we will write $\Delta_a^G = \vee_R \{b \backslash a | b \in G\}$ in order to specificy that the element is constructed in the Garside monoid G.

PROPOSITION 94. *Let G be a Garside monoid with $G = H \bowtie K$ and let $x \in QZ(G)$. If we write $x = x_H x_K$ where $x_H \in H$ and $x_K \in K$ then $x_H \in QZ(H) \cap QZ(G)$ and $x_K \in QZ(K) \cap QZ(G)$.*

PROOF. Let A_G, A_H be the set of atoms of G and H. We know that $x \in QZ(G) = \left\langle \Delta_a^G \mid a \in A_G \right\rangle$. By Proposition 73, if $a \in A_H$, then $\Delta_a^G \in H$ and thus, since the quasi-center of G is abelian, we can write $x = \left(\prod_{a\in A_H} \Delta_a^{e_a}\right)\left(\prod_{b\in A_K} \Delta_b^{e_b}\right)$ for some integers e_c for $c \in A_G$. Now, by the uniqueness of the Zappa-Szép product $x_H = \left(\prod_{a\in A_H} \Delta_a^{e_a}\right) \in QZ(G)$ and $x_K = \left(\prod_{b\in A_K} \Delta_b^{e_b}\right) \in QZ(G)$. If $d \in A_H$, then $d^{x_H} \in H \cap A_G$, that is, $x_H \in QZ(H)$. Similarly $x_K \in QZ(G) \cap QZ(K)$. □

REMARK 95. Result above generalizes Theorem 90, with a different prove involving Picantin results about the generators of the quasi-center of G and some divisibility properties given by Gebhardt and Tawn. Additionally, following reasoning above, if Δ_G is a Garside element of G, then given an atom $a \in A_G$,then Δ_a^G divides Δ_G,and so $e_a \geq 1$ for every a. In particular, Δ_a divides x_H for all $a \in A_H$ and Δ_b divides x_K for all $b \in A_K$,and so Δ_H, Δ_K are Garside elements of H and K.

PROPOSITION 96. *Let G be a Garside monoid with set of atoms X, and let $\delta = \vee_{a\in X}\Delta_a$. Then δ is a Garside element dividing every Garside element of G.*

PROOF. By definition $\delta \in QZ(G)$ (see Proposition 75), and so, it is a balanced element. Since every atom a divides Δ_a which divides δ by definition, δ is a Garside element of G. If Δ is a Garside element of G and $a \in X$, a divides $\Delta \in QZ(G)$, and so Δ_a divides Δ by Proposition 75. The result follows by the definition of δ. □

REMARK 97. The element δ above is also referred as the **minimal Garside element** of the Garside group G. The fact that such an element exists is an easy consequence from the fact that the quasi-center is lattice l.c.m. and g.c.d., however the explicit version given above, makes use of Picantin's notation and definition of the quasi-center, which will be relevant in the following. Additionally, if x denotes the least common multiple of the atoms of G, then x is not necessarily a Garside element, however Δ_x is always the minimal Garside element G.

In case x is a Garside element, then $\Delta_x = x$ is the minimal Garside element of G, which we will denote by δ_G or simply δ.

COROLLARY 98. *Let G be a decomposable Garside monoid with decomposition $G = H \bowtie K$. Then $\delta_G = \delta_H \delta_K$, that is, the minimal Garside element of G is the product of the minimal Garside elements of H and K.*

PROOF. We denote by A_G, A_H, A_K the set of atoms of the monoids G, H, K, and recall that A_G is the disjoint union of A_H, A_K. By proposition above, $\delta_G = \vee_{a \in A_G} \Delta_a = \left(\vee_{a \in A_H} \Delta_a\right) \vee \left(\vee_{b \in A_K} \Delta_b\right) = \delta_H \vee \delta_K$. In addition, $\delta_H \delta_K = \delta_K \delta_H$ since the quasi-center is a free abelian group, and $\delta_H \wedge \delta_K = 1$ given that $H \cap K = 1$, thus $\delta_H \vee \delta_K = \delta_H \delta_K$ by Proposition 75. □

COROLLARY 99. *Let G be a Garside monoid and suppose that G decomposes as the Zappa-Szép product of some irreducible Garside monoids $H_1, H_2, ..., H_n$. If δ_G denotes the minimal Garside element of G, then $\delta_G = \delta_1 \cdot \delta_2 \cdot ... \cdot \delta_n$ where each δ_i is the minimal Garside element of H_i, $i = 1, ..., n$. Additionally, $\delta_G^k = \delta_1^k \cdot \delta_2^k \cdot ... \cdot \delta_n^k$ for all $k \in \mathbb{Z}$.*

PROOF. By hypothesis, G in not indecomposable and we can write $G = H \bowtie K$ for some Garside submonoids H, K which factorize in terms of $H_1, ..., H_r$ and $H_{r+1}, ..., H_n$ respectively. Thus the result follows by induction on the number n of irreducible factors, being result above the prove for the base case $n = 2$. □

REMARK 100. Notice that product of the δ_i^k may not be commutative since they are not necessarily quasi-central elements of G. Additionally, if we change the decomposition of the group we get a different product for the minimal Garside element.

PROPOSITION 101. *Let $G = H \bowtie K$ where H, K are irreducible, then $QZ(G) = \langle \delta_H \rangle \times \langle \delta_K \rangle$.*

PROOF. Let x be a quasi-central element of G dividing δ_H, then $x \in H$ and $x = x_H$ is a quasi-central element of H. Since H is indecomposable, its quasi-center is generated by δ_H and thus δ_H divides x. A similar argument for K holds, proving the result. □

COROLLARY 102. *If $G = H \bowtie K$ with H, K two irreducible Garside monoids, then $\left\{\delta_H^a \delta_K^b \mid a, b \geq 1\right\}$ are all the Garside elements of G.*

PROOF. Let us write $\Delta = \delta_H^a \delta_K^b$ for some fixed integers $a, b \geq 1$. We know that $\delta_H, \delta_K \in QZ(G)$, thus $\Delta \in QZ(G)$. Because $\delta_G = \delta_H \delta_K$ divides Δ, every atom of G divides Δ and it is a Garside element of G. Reciprocally, if Δ is a Garside element of G, then $\Delta \in QZ(G) = \langle \delta_H, \delta_K \rangle$, which finishes the proof. □

EXAMPLE 103. The Garside monoid

$$G^+ = \left\{a, b, c, d \mid ab = ba, ac = ca, bc = cb, a^d = a, b^d = c, c^d = b\right\},$$

admits two different decompositions

$$G = (A \times B \times C) \rtimes D,$$

where the action is given by $a^d = a, b^d = c, c^d = b$, and

$$G = (B \times C) \rtimes (A \times D),$$

with action $b^a = b, c^a = c, b^d = c, c^d = b$. Although the irreducible factors A, B, C, D are the same for both decompositions of G, if we write $G = H \bowtie K$ then for the first decomposition

we get $H = A \times B \times C$ and $K = D$ and minimal Garside element $\delta = abcd$ while in the second one we get $H = B \times C$ and $K = A \times D$ and $\delta = bcad$.

THEOREM 104. *Let G be a Garside monoid and let $\{x_1, x_2, ..., x_r\}$ be the basis of $QZ(G)$. If A_i is the set of atoms dividing x_i, and $N_i = \langle A_i \rangle$ as a monoid, then G decomposes as the Zappa-Szép product of the monoids $N_1, N_2, ..., N_r$ with $N_i N_j = N_j N_i$ whenever $1 \leq i, j \leq r$, and the Zappa-Szép product is associative in this case.*

PROOF. We argue by induction on the number of atoms of G, and assume that G is not irreducible Garside and has more than one atom. Additionally, we also set integers i, j to belong to the set $\{1, ..., r\}$. We write $G = H \bowtie K$ for some parabolic submonoids H, K of G and denote by A_G, A_H, A_K to the set of atoms of G, H and K. Remark that for every $s \in \{1, ..., r\}$, there exists an atom $a_s \in A_G$ so that $x_s = \Delta^G_{a_s}$. Moreover if $a_s \in A_H$ then $x_s \in H$, and if $a_s \in A_K$, then $x_s \in K$, and thus either $N_i \subseteq H$ or $N_j \subseteq K$. If both N_i, N_j are contained in H, by induction hypothesis H is the Zappa-Szép product of some $M_1, M_2, ..., M_d$ so that $M_i M_j = M_j M_i$ for $1 \leq i, j \leq d$.

If for some $k \in \{1, ..., d\}$ the Garside element of M_k divides x_i, then the set of atoms of M_k is contained in N_i, and so $M_k \subseteq N_i$. Reciprocally, if a is an atom of N_i, then a is an atom of H, and so $a \in M_k$ for some $k \in \{1, ..., s\}$, and N_i is the product of some of the monoids $M_1, M_2, ..., M_s$.

Now, the same applies to N_j, and $N_i N_j = N_j N_i$ since both are product of some of the $M_1, M_2, ..., M_s$ and they permute. Moreover, if $N_i \cap N_j \neq 1$, then N_i and N_j have some factor M_k is common. Thus, if a is an atom of M_k, $a \in A_i \cap A_j$, and so $x_i = \Delta^G_a = x_j$ a contradiction.

In case both N_i, N_j are contained in K a similar argument shows that $N_i N_j = N_j N_i$ and we may assume that N_i is in H while N_j is in K. Trivially $N_i \cap N_j \subseteq H \cap K = 1$ and by way of contradiction suppose that $N_i N_j \neq N_j N_i$; then there exists atoms $a \in A_i, b \in A_j$ so that if $ab = b'a'$ with $a' \in H$ and $b' \in K$ then either $a' \notin A_i$ or $b' \notin A_j$. Furthermore, a', b' are atoms of G, in particular $a' \in A_H$ and $b' \in A_K$ by Proposition 71, and without lost of generality we assume $a' \notin A_i$. Because $x_i = da$ for some $d \in N_i$, $x_i b = dab = db'a' = b''d'a'$ for some $b'' \in K$ and $d' \in H$. On the other hand, since $x_i \in QZ(G) \cap H$ we have $x_i b = c x_i$ for some $c \in K$, and by the uniqueness of the Zappa-Szép product we have $c = b''$ and $x_i = d'a'$, a contradiction with $a' \notin A_i$.

Finally, since $N_i N_j = N_j N_i$ and $N_i \cap N_j = 1$, the Zappa-Szép product $N_1 \bowtie N_2 \bowtie ... \bowtie N_r = \prod_{i=1}^r N_i$ is well defined, is associative and coincides with G since every atom of G is an atom of some N_i. □

DEFINITION 105. We call the decomposition $N_1, N_2, ..., N_r$ above, the **quasi-central decomposition** of G, and each N_i with $i \in \{1, ..., r\}$ a **quasi-central factor of** G.

REMARK 106. We knew that every Garside element is quasi-central, and so it can be written as the product of the generators of the quasi-center. Theorem above proves the equivalent version for the Garside monoid, thus, once again, we extend a property "from the Garside element to the whole Garside monoid".

Additionally, it will be interesting to write a Garside element of G as the product of the Garside elements of the submonoids; although we have already proven the result when the Garside monoid decomposes as the product of two irreducible Garside submonoids and

for the minimal Garside element, we can now generalize this by means of the quasi-central decomposition.

COROLLARY 107. *Let G be a Garside monoid and $N_1, N_2, ..., N_r$ its quasi-central decomposition, then $\Delta \in G$ is a Garside element of G if and only if $\Delta = \delta_{N_1}^{e_1} \cdot ... \cdot \delta_{N_r}^{e_r}$ for some integers $e_i \geq 1$ for $i = 1, ..., r$.*

PROOF. An element Δ is a Garside element if and only if Δ is quasi-central and every atom divides Δ, that is, if and only if every generator of the quasi-center divides Δ. Since $\left\{\delta_{N_i}\right\}_{i=1}^{r}$ form a basis for $QZ(G)$, the result follows. □

REMARK 108. We know that if $G = H \bowtie K$, then any decomposition of the Garside element $\Delta = \Delta_H \Delta_K$ produces Garside elements Δ_H, Δ_K for H, K. However the converse is not always true, and result above explains why: Garside elements of the factors must also be quasi-central elements of G.

PROPOSITION 109. *Let G be a Garside monoid and $N_1, N_2, ..., N_r$ be its quasi-central factors, then $Z(G) = \cap_{i=1}^{r} C_G(N_i)$ and $QZ(G^+) = \cap_{i=1}^{r} N_{G^+}\left(N_i^+\right)$.*

PROOF. Write $C = \cap_{i=1}^{r} C_G(N_i)$ and let $x \in C$. If $g \in G$, then $g = n_1 \cdot n_2 \cdot ... \cdot n_r$ with $n_i \in N_i$, and so $xg = gx$, that is $x \in Z(G)$. Conversely, if $x \in Z(G)$, then $xn = nx$ for all $n \in G$, in particular, for all $n \in N_i$ with $i \in \{1, ..., r\}$ and $x \in C_G(N_i)$.

We now show that if $x \in N_{G^+}\left(N_i^+\right)$ for some fixed $i \in \{1, ..., r\}$, then conjugation by x permutes the set of atoms of N_i^+. If $g_1, g_2 \in G$ are so that $g_1^x = g_2^x$, then $xg_1x = xg_2x$ holds in the monoid; since G is cancellative, relation before implies $g_1 = g_2$ and conjugation by x is an injective map. By definition, $(N_i)^x = N_i$ and if a is an atom of N_i, then so is a^x, otherwise $a^x = n_1 n_2$ with $1 \neq n_i \in N_i = N_i$, and so we can write $n_i = m_i^x$ with $m_i \in N_i$ for $i = 1, 2$ and $a^x = (m_1 m_2)^x$. Thus, since conjugation by x is injective, $a = m_1 m_2$ which implies $m_1 = 1$ or $m_2 = 1$ and so $n_1 = 1$ or $n_2 = 1$, a contradiction. Hence, conjugation by x sends A_{N_i}, the set of atoms of N_i^+, to A_{N_i}, and since A_{N_i} is finite and conjugation is injective, it defines a permutation over A_{N_i}. Finally, if $x \in \cap_{i=1}^{r} N_{G^+}\left(N_i^+\right)$ and $a \in A_G$, then $a \in A_{N_i}$ for some $i \in \{1, ..., r\}$ and $a^x \in A_{N_i} \subseteq A_G$, that is $x \in QZ(G^+)$.

Conversely, write $G = H \bowtie K$, and let $x \in QZ(G)$. If $x = x_H x_K$ where $x_H \in H$ and $x_K \in K$, we take $h \in H$, we know that thus $h^x = (h^{x_H})^{x_K} \in H$. Thus if $x \in QZ(G)$ then $x \in N_G(H) \cap N_G(K)$. For a fixed $i \in \{1, ..., r\}$, because the product of the quasi-central factors are permutable, we can arrange the product so that $H = N_i$ and K is product of all quasi-central factor different from N_i, and so $x \in N_{G^+}\left(N_i^+\right)$. Because we can do this for every $i \in \{1, ..., r\}$ the result follows.

□

REMARK 110. Formula $Z(G) = \cap_{i=1}^{r} C_G(N_i)$ also holds for both in the monoid and its group of fractions. It is also true for a Garside group G that $QZ(G) \subseteq \cap_{i=1}^{r} N_G(N_i)$, however the reverse inclusion may not hold in the group.

PROPOSITION 111. *Let G be a Garside group with $G = H \bowtie K$ and let $x \in C_G(QZ(G))$, and write $x = x_H x_K$ with $x_H \in H$, $x_K \in K$. Then $x_H, x_K \in C_G(QZ(G))$.*

PROOF. Let $g \in QZ(G)$, then $x_H x_K = x = x^g = x_H^g x_K^g$. But $x_H^g \in H$ and $x_K^g \in K$, therefore by the uniqueness of the Zappa-Szép product $x_H = x_H^g$ and $x_K = x_K^g$.

□

PROPOSITION 112. *A Garside group G is abelian if and only if its quasi-central factors are all cyclic.*

PROOF. If G is abelian and a, b are atoms of G, then $ab = ba$, which implies $a, b \in QZ(G)$. Thus the quasi-central factors of G are the infinite cyclic generated by one atom.

Conversely, if the quasi-central factors $N_1, N_2, ..., N_r$ are all cyclic, we write $N_i = \langle x_i \rangle$ for $i = 1, ..., r$. Notice that if a is an atom of G, then $a \in N_i$ for some $i \in \{1, ..., r\}$ and so $a = x_i^s$. Consequently, $a = x_i$ and every generator of a quasi-central factor, x_i, is an atom of G for all i. Then, since the Zappa-Szép product $N_i \bowtie N_j$ is well defined for $i \neq j$, $x_i x_j = x_j x_i$ for all $i, j \in \{1, ..., r\}$. Therefore G is an abelian group. □

REMARK 113. Cyclicness of the indecomposable factors of a Garside group G is a necessary condition for G to be abelian, but it is not sufficient; let $G = (\langle a \rangle \times \langle b \rangle) \rtimes \langle c \rangle$ where the action of c is given by $a^c = b$ and $b^c = a$. Then G has indecomposable factors cyclic but it is not abelian.

REMARK 114. From [2, Corollary 7.6.5.], if all the quasi-central factors of a Garside group G are abelian, then G is poly-cyclic.

THEOREM 115. *Let G be a Garside monoid and $M_1, M_2, ..., M_r$ some decomposition of G. If S is a parabolic submonoid of G, then S is the Zappa-Szép product of $S_i = S \cap M_i$.*

PROOF. Since G decomposes as the Zappa-Szép product of $M_1, ..., M_r$, then exists $i \in \{1, ..., r\}$ so that $G = H \bowtie K$ where H and K factorize as Zappa-Szép product of $M_1, ..., M_i$ and $M_{i+1}, ..., M_r$ respectively. Additionally, H, K are parabolic submonoids and so are $S \cap H$ and $S \cap K$ by Proposition 55. Given $s \in S$, we know that $s = hk$ for uniques $h \in H$, $k \in K$; given that h, k are left and right divisors of s, we conclude by Proposition 54 that $h, k \in S$, and thus $S = (S \cap H) \bowtie (S \cap K)$. Therefore it suffices to show that $S \cap H$ and $S \cap K$ factorize as the Zappa-Szép product of $\{S_j\}_{j=1}^{i}$ and $\{S_j\}_{j=i+1}^{r}$ respectively. If $r = 2$, then: $i = 1$, $H = M_1$, $K = M_2$ and $S = S_1 \bowtie S_2$. If $r > 2$ then we can apply induction hypothesis to H and K so that the standards parabolic submonoid $S \cap H$ and $S \cap K$ decompose as the Zappa-Szép product of $\{(S \cap H) \cap M_j\}_{j=1}^{i} = \{S_j\}_{j=1}^{i}$ and $\{(S \cap K) \cap M_j\}_{j=i+1}^{r} = \{S_j\}_{j=i+1}^{r}$, as claimed. □

CHAPTER 3

Introduction to the Yang-Baxter equation

3.1. Basic definitions and results

The quantum Yang-Baxter equation (**QYBE** or **YBE**) is a significant equation in theoretical physics, first introduced by C.N. Yang [81] and later in [5] by R. Baxter. A solution of QYBE is a linear map $R : V \otimes V \longrightarrow V \otimes V$ where V is a vector space, satisfying the equation:

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}. \tag{3.1.1}$$

Here R^{ij} denotes the map $V \otimes V \otimes V \longrightarrow V \otimes V \otimes V$, acting as R on the (i, j) tensor factor and as the identity on the remaining factor.

Let $\alpha : V \otimes V \longrightarrow V \otimes V$ be the **permutation map**, that is, the linear map such that $\alpha(u \otimes v) = v \otimes u$ for all $u, v \in V$. Then, R is a solution of QYBE if and only if $\overline{R} = \alpha \circ R$ satisfies the equation:

$$\overline{R}^{12}\overline{R}^{23}\overline{R}^{12} = \overline{R}^{23}\overline{R}^{12}\overline{R}^{23}. \tag{3.1.2}$$

In this case, $\overline{R}$ is a **solution** of the Yang-Baxter equation (YBE). A central open problem is to construct and classify solutions of this equation.

In [34], V. Drinfeld suggested studying solutions of the Yang-Baxter equation induced by a map $S : X \times X \to X \times X$ where X is a basis of the vector space V. Such solutions are referred to as **set-theoretic solution** of the Yang-Baxter equation. When the map S is the permutation map of X^2, then (X, S) is called **trivial solution**.

Definition 116. Given a nonempty set X and a map S from $X \times X$ to itself, we write $S(x, y) = \big(g_x(y), f_y(x)\big)$ for x, y in X. Additionally, we denote by S^{ij} to the map from X^3 to itself acting as S on the i-th and j-th components and as the identity on the remaining one.

1. The pair (X, S) is called **non-degenerate** if the maps $g_x, f_x : X \to X$ are bijections for every x in X.
2. The pair (X, S) is called **involutive** if $S^2 = \mathrm{Id}_X$.
3. The pair (X, S) is said to be a **braided** set if S satisfies the braid relation:

$$S^{12}S^{23}S^{12} = S^{23}S^{12}S^{23}. \tag{3.1.3}$$

Alternatively, we can write conditions above in terms of the associated permutations.

Theorem 117. [19, 3.1] *Given a pair (X, S) as above, write $|X| = n$. Then:*

1. *(X, S) is non-degenerate if and only if f_i, g_i are bijective, $1 \le i \le n$.*
2. *(X, S) is involutive if and only if $g_{g_i(j)}f_j(i) = i$ and $f_{f_j(i)}g_i(j) = j, 1 \le i, j \le n$.*
3. *(X, S) is braided if and only if $g_ig_j = g_{g_i(j)}g_{f_j(i)}, f_jf_i = f_{f_j(i)}f_{g_i(j)}$, and $f_{g_{f_j(i)}(k)}g_i(j) = g_{f_{g_j(k)}(i)}f_k(j), 1 \le i, j, k \le n$.*

If α is the permutation map, then the map $R = \alpha \circ S$ is called the R-matrix corresponding to S. Etingof, Soloviev, and Schedler show in [38] that (X, S) is a braided set if and only if the R-matrix satisfies the quantum Yang-Baxter, and that (X, S) is a braided and involutive if and only if in addition the R-matrix satisfies the unitary condition $R^{21}R = 1$ (of special interest in physics). They also defined the **structure group of a solution**, for the involutive case, given by

$$G(X, S) = \langle X \mid xy = tz \text{ where } S(x, y) = (t, z) \rangle ,$$

that is: the group generated by the elements of X and with defining relations given by S, and show that if (X, S) is non-degenerate and braided, the assignment $x \to f_x$ is a **right action** of G on X, which allows to define the **permutation group** of a solution $\mathcal{G}_{(X,S)}$, as the subgroup of Sym_X generated by $\{f_x \mid x \text{ in } X\}$. For the involutive case , the **diagonal map** T of a solution is defined as $T(x) = f_x^{-1}(x)$, which happens to be a permutation of Sym_X such that $f_x^{-1}T = Tg_x$, consequently $\mathcal{G}_{(X,S)}$ is isomorphic to the group $\langle g_x \mid x \in X \rangle$.

Remark 118. From now on, along the entire thesis and unless it is specified, all pairs (X, S) considered will be braided, non-degenerate, involutive with X a finite set. Since such pairs produce solutions of the YBE naturally by the above mentioned, in order to remark this, we shall refer to (X, S) as a solution of YBE marked in red.

Definition 119. Two solutions (X, S) and (X', S') are **isomorphic** if there exists a bijection $\varphi : X \to X'$ which maps S to S'.

Definition 120. [38, 2.5] Given a non-degenerate involutive solution (X, S), then:

1. A subset Y of X is said to be an **invariant subset** if $S(Y \times Y) \subset Y \times Y$.
2. An invariant subset $Y \subset X$ is said to be **non-degenerate subset** if $(Y, S|_{Y\times Y})$ is a non-degenerate involutive set-theoretical solution.
3. A solution (X, S) is said to be **decomposable solution** if it is a union of two nonempty disjoint non-degenerate invariant subsets. Otherwise, (X, S) is said to be **indecomposable solution**.

Example 121. Consider the solution (X, S) where $X = \{1, 2, 3, 4\}$, and $S : X^2 \to X^2$ given by $S(i, j) = (g_i(j), f_j(i))$ with

$$\begin{array}{llll} g_1 = (3, 4), & g_2 = (3, 4), & g_3 = (1, 2), & g_4 = (1, 2), \\ f_1 = (3, 4), & f_2 = (3, 4), & f_3 = (1, 2), & f_4 = (1, 2). \end{array}$$

The structure group of the solution is

$$G(X, S) = \left\langle x_1, x_2, x_3, x_4 \middle| \begin{array}{lll} x_1x_2 = x_2x_1, & x_1x_3 = x_4x_2, & x_1x_4 = x_3x_2 \\ x_2x_3 = x_4x_1, & x_2x_4 = x_3x_1, & x_3x_4 = x_4x_3 \end{array} \right\rangle .$$

It is easy to see that if we write $Y = \{x_1, x_2\}$ and $Z = \{x_3, x_4\}$ then $X = Y \cup Z$ and Y, Z are non-degenerate invariant subsets, and so, the solution (X, S) is decomposable.

Example 122. There are only 5 indecomposable solutions of the Yang-Baxter equation on a set of 4 elements up to isomorphism. The following is one of them; for the set $X = \{1, 2, 3, 4\}$, consider map $S : X^2 \to X^2$ given by $S(i, j) = (g_i(j), f_j(i))$ where

$$\begin{array}{llll} g_1 = (1, 4), & g_2 = (1, 2, 4, 3), & g_3 = (2, 3), & g_4 = (1, 3, 4, 2), \\ f_1 = (1, 2), & f_2 = (1, 3, 2, 4), & f_3 = (3, 4), & f_4 = (1, 4, 2, 3). \end{array}$$

Additionally, the structure group of the solution is

$$G(X,S)=\left\langle x_1,x_2,x_3,x_4 \middle| \begin{array}{lll} x_1x_1=x_4x_2, & x_1x_2=x_2x_3, & x_1x_3=x_3x_1 \\ x_2x_2=x_4x_4, & x_2x_3=x_1x_2, & x_2x_4=x_3x_3 \end{array} \right\rangle,$$

and its permutational group $\mathcal{G}_{(X,S)}$ is the group of size 8 generated by $\langle g_1,g_2,g_3,g_4\rangle$.

REMARK 123. Notice that the generators $x_1,...,x_4$, of the structure group we used in examples above, are different from the elements of $X=\{1,2,3,4\}$. This is actually an abuse of notation, since generators of $G(X,S)$ are by definition the elements of X. However in order to write the permutations g_1,g_2,g_3,g_4 notation gets simplified this way. We will also write $x_i\in X$ in some occasions, that is, the reader is expected to identify x_i with i and its associated permutation with g_{x_i} or g_i for short. The reader is advised that this abuse of notation will be common from now on.

THEOREM 124. [38, 2.14] *Given a solution (X,S), its structure group $G(X,S)$ is solvable.*

THEOREM 125. [38, 2.11] *A solution (X,S) is indecomposable if and only if $\mathcal{G}_{(X,S)}$ acts transitively on X.*

Among the first solutions studied, we found the so called **square-free solutions**, such named is given by the fact that all relations defining the structure group are square-free, that is, no relation involves x^2 for $x\in X$. Equivalently, if T denotes the diagonal map, then a solution is square-free if and only if $T=\mathrm{Id}$.

Wolfgang Rump proved the following result, which is key in the study of square-free solutions, and will play a fundamental role in the proof of our main result in the next chapter of the thesis.

THEOREM 126. [69, 1] *Every square-free solution of the YBE with more than one element is decomposable. However an indecomposable square-free solution is possible when $|X|$ is infinite.*

THEOREM 127. [38, 2.12] *Let (X,S) be an indecomposable solution, and $|X|=p$, where p is a prime. Then (X,S) is isomorphic to the cyclic permutation solution $(\mathbb{Z}/p\mathbb{Z},S_c)$, where $S_c(x,y)=(y-1,x+1)$.*

DEFINITION 128. Solution $S_c(x,y)=(y-1,x+1)$ is called the **cyclic solution** and is a indecomposable solution of the YBE for every finite set X (not necessarily prime).

Now, let (X,S) be a solution of the YBE. For $x,y\in X$ let $x\sim y$ if and only if $g_x=g_y$ and denote by $[x]$ to the class of $x\in X$. Then $\sim$ is an equivalence relation on X and we will prove it is compatible with S (or see [54, 38] alternatively). Because the map S can be written in terms of g exclusively, $S(x,y)=\left(g_x(y),g^{-1}_{g_x(y)}(x)\right)$, it suffices to show that g is compatible with $\sim$, that is, we need to prove that $g_i([x_j])=[g_i(x_j)]$ is well defined for every $i,j\in X$. Let $x_j\sim x_k$, then $g_j=g_k$ and we claim that $f_j=f_k$ too. To see this, let T be the diagonal map, then $f_r^{-1}T=Tg_r$ for every $r\in X$, and thus, $f_k=\left(g_k^{-1}\right)^T=\left(g_j^{-1}\right)^T=f_j$ as claimed. Now,

we make use of Theorem 117, in particular, we know that $g_i g_j = g_{g_i(j)} g_{f_j(i)}$ for every $i, j \in X$, and so $g_i g_k = g_{g_i(k)} g_{f_k(i)}$. Given that $g_j = g_k$, we get $g_{g_i(j)} g_{f_j(i)} = g_{g_i(k)} g_{f_k(i)}$, but $f_j = f_k$, hence $g_{g_i(j)} = g_{g_i(k)}$, i.e. $x_{g_i(j)} \sim x_{g_i(k)}$, and $[g_i(x_j)] = [g_i(x_k)]$, as desired. Consequently, if we define $\widetilde{S} : X^2 \to X^2$ given by $\widetilde{S}([x],[y]) = \left([g_x(y)], \left[f_y(x)\right]\right)$, then $\widetilde{S}$ is well defined and $\left(X/\sim, \widetilde{S}\right)$ is also a solution of the YBE.

This solution, first introduced in [38] and also studied in [54, Section 4], is known as the **retracted solution** of (X,S) and is usually denoted by $\mathrm{Ret}(X,S)$. In case $\mathrm{Ret}(X,S) = (X,S)$ we say that (X,S) is **irretractable solution**, otherwise, we say (X,S) is a **retractable solution**. If we define inductively, $\mathrm{Ret}^{k+1}(X,S)$ as the retracted solution of $\mathrm{Ret}^k(X,S)$, then we say that a solution (X,S) is a **multipermutation solution** if there exists $s \geq 1$ so that $\mathrm{Ret}^s(X,S)$ has cardinality 1.

3.2. I-structure and IYB groups

As mentioned before, Gateva-Ivanova and Van den Bergh introduced the notion of monoids and groups of left and right I-type. Such groups are related with the structure group of solutions of the YBE. Since this groups are Garside groups, it is clear that these groups share their properties. In this section, we shall see some results adapted to the content of this thesis, but first we shall fix some notation: given a positive integer n we denote by Fa_n to the free-abelian monoid of rank n and by FA_n to the free-abelian group of rank n.

Definition 129. A group $\mathcal{G}$ is an **IYB group** if there exists a map $\phi : \mathrm{FA}_n \to \mathrm{Sym}_n$ such that $G = \{(a, \phi(a)) : a \in \mathrm{FA}_n\}$ is a subgroup of $\mathrm{FA}_n \rtimes \mathrm{Sym}_n$ and $\mathcal{G}$ is isomorphic to $\phi(\mathrm{FA}_n)$.

The reader is referred to [11, 2.1], where many equivalent definitions of and IYB group can be found. However, the idea behind this groups can be found in [38], where the subgroups Γ and A play the role of FA_n.

Let us now see how the groups G and $\mathcal{G}$ are related with the Yang-Baxter equation. Let (X,S) be a solution of the YBE with $X = \{x_1, ..., x_n\}$, and for $x_i, x_j \in X$ write $S(x_i, x_j) = (x_t, x_z)$, then $x_i x_j = x_t x_z$ is a defining relation of the structure group $G(X,S)$. For simplicity, we write $g_i(j) = t$ and $g_t(z) = i$. Now, write $\mathrm{FA}_n = \langle u_1, ..., u_n \rangle$ and let $y_i = \left(u_i, g_i^{-1}\right)$ for $i = 1, ..., n$, where g_i are the permutations associated with $x_i \in X$. Then, if we call $G = \langle y_1, ..., y_n \rangle$, we have:

$$\begin{aligned} y_i y_j &= \left(u_i, g_i^{-1}\right)\left(u_j, g_j^{-1}\right) = \left(u_i u_j^{g_i}, g_i^{-1} g_j^{-1}\right) = \left(u_i u_t, g_i^{-1} g_j^{-1}\right) = \left(u_t, g_t^{-1}\right)\left(u_i^{g_t^{-1}}, \phi\left(u_i^{g_t^{-1}}\right)\right) \\ &= y_t y_z. \end{aligned}$$

Thus, the group G is isomorphic to the structure group $G(X,S)$, and the IYB group $\mathcal{G}$ is isomorphic to the permutation group $\mathcal{G}_{(X,S)}$.

As claimed in [11], a natural way towards classification of solutions of the YBE starts with the classification of finite groups, that are of the type $\phi(Fa_n)$ for some structure group G. And then describe all structure groups that have a fixed IYB group as permutation group, but notice that $\langle 1 \rangle \times \mathcal{G} \cong \mathcal{G}$, and so we can associate with each IYB group, infinitely many

solutions of the Yang-Baxter equation. Consequently, this task is not an easy one and it is still in progress.

THEOREM 130. [11, 3.1] *If $\mathcal{G}$ is an IYB group then its* Hall *subgroups are also IYB groups.*

Recall that the permutation group of a solution is always solvable. Thus Sym_n is not an IYB group for $n \geq 5$, however...

THEOREM 131. [11, 3.6] *Let n be a positive integer. Then the Sylow subgroups of Sym_n are IYB groups.*

THEOREM 132. [11, 3.2] *The class of IYB groups is closed under direct products. That is, the direct product of IYB groups is an IYB group.*

COROLLARY 133. [11, 3.7] *Any finite nilpotent group is isomorphic to a subgroup of an IYB nilpotent group.*

Similarly, for solvable groups we have:

PROPOSITION 134. [13, 9.1] *The wreath product of IYB groups is an IYB group. In particular, every finite solvable group is isomorphic to a subgroup of an IYB group.*

Motivated by this result, authors from [12, p. 3] raised the following question: Let G be a finite solvable group, is G the permutation group of an IYB group? The answer was shown negative by Bachiller, who provided a nilpotent counterexample (see [3, section 4.3]). As a final claim, we remark that many results constructing IYB groups under special conditions can be found in [11], and as a consequence, more classical groups are related with IYB. For instance, it is shown that every finite nilpotent group of class 2 is IYB group. Additionally, an infinite family of solutions of the Yang-Baxter equation with the same IYB group is constructed. However, the strongest result regarding the semidirect product of IYB groups under extra hypothesis can be found in [51, A], where the notions of equivariant and IYB-structure are introduced. Given the difficulty of such result, the reader is refereed to the previous article.

3.3. Finite left braces

In this section we shall see a brief introduction to finite left braces, and some results regarding such structure. Despite we shall not develop any result regarding left braces, introduction of such notation will be helpful in next sections.

DEFINITION 135. A **left brace** is a set B with two operations $+$ and $\cdot$ such that $(B, +)$ is an abelian group, $(B, \cdot)$ is a group and

$$a(b + c) + a = ab + ac,$$

for all $a, b, c \in B$. The group $(B, +)$ is called the additive group and $(B, \cdot)$ the multiplicative group of the left brace. A **right brace** is defined in a similar way, subject to

$$(a + b)c + c = ac + bc.$$

In a left/right brace, the identity element for $+$ and $\cdot$ coincide.

The subsequent outcome serves as the rationale for incorporating left braces in this text presentation.

THEOREM 136. [13, 4.6] *A finite group G is an IYB group if and only if it is the multiplicative group of a finite left brace.*

From result above we see that the study IYB groups can be achieved by means of finite left braces. Actually, left braces and other generalizations such as: skew left braces; relate with the study of solutions of the YBE, not necessarily finite non-degenerate and involutive. However, we have not followed this path in the study of the YBE and we will make use of group theory instead. However, in some cases, we shall make use of the left brace structure. Additionally, some interesting properties have been enunciated in terms of left braces.

DEFINITION 137. [71, 74] Given a left brace B, the **right powers** of B are defined by $B^{(n+1)} = B^{(n)} \cdot B$, which are a left ideals of B. The **left powers** are B^n are defined by $B^{n+1} = B \cdot B^n$, which are right ideals. Additionally, the **chain of ideals** defined by $B^{[n+1]} = \sum_{i=1}^{n} B^{[i]} B^{[n+1-i]}$, where $B^{[1]} = B$ is a chain of two-sided ideals.

THEOREM 138. [74, 13] *Let $(B, +, \cdot)$ be either a left brace or a right brace. If $B^n = B^{(m)} = 0$ for some natural numbers m, n, then the multiplicative group of B is a nilpotent group.*

THEOREM 139. [74, 14] *Let B be a left brace such that $B^{(n)} = 0$ for some n. If the multiplicative group of B is nilpotent then $B^m = 0$ for some m, and hence $B^{[s]} = 0$ for some s.*

DEFINITION 140. Given a left brace $(B, +, \cdot)$, the operation $\circ$ defined by $a \circ b = ab + a + b$ makes $(B, \circ)$ a group, called the **adjoint group**.

THEOREM 141. [71, 3] *Let B be a brace of multipermutation level 2. The adjoint group of B is nilpotent if and only if $B^{(n)} = 0$ for some n.*

THEOREM 142. [75, 28] *Let B be a finite left brace, let $x \in B$ and let $B(x)$ be the smallest left brace containing x. Denote $X = \{x + ax : a \in B(x)\}$, and let $S : X \times X \to X \times X$ be a restriction to X of the Yang-Baxter map associated with B. Then (X, S) is an indecomposable solution of the YBE.*

LEMMA 143. [75, 31] *Let (X, S) be a finite solution and let B be a finite left brace such that $X \subseteq B$ and S is a restriction of the Yang-Baxter map associated to B. Assume that every element of B is a sum of some elements from X. If (X, S) has finite multipermutation level, then B is a right nilpotent brace and $B^{(m+2)} = 0$ where $m = mpl(X, S)$.*

Finally, the reader is referred to [10], where braces and the Yang-Baxter equation are studied in great detail.

3.4. About solutions

Next, we provide a list of results that together provide an in depth approach to the study of solutions of the YBE.

PROPOSITION 144. [54, 4.2] *The structure group of a retractable solution is poly-infinite cyclic.*

PROPOSITION 145. [38, 3.8] *Given a retractable solution (X,S), if $Ret(X,S)$ is indecomposable, then (X,S) is also indecomposable.*

LEMMA 146. [75, 36] *Let (X,S) be a finite multipermutation solution with $|X|>1$. If for every $x\in X$ there is $y\in X$ such that $S(x,y)=(y,x)$, then the solution (X,S) is decomposable.*

THEOREM 147. [38, Section 3.2] *Let (X,S) be a solution of the YBE. If the permutation group $\mathcal{G}_{(X,S)}$ is finite and cyclic, then (X,S) is a multipermutation solution.*

THEOREM 148. [67, 3.3] *Let (X,S) be a solution of the YBE. If $\mathcal{G}_{(X,S)}$ acts regularly on X, then (X,S) is retractable.*

COROLLARY 149. [67, 3.4] [69, 1] *If (X,S) is a indecomposable solution of the YBE such that $\mathcal{G}_{(X,S)}$ is abelian, then (X,S) is retractable.*

Notice that because we are dealing with finite solutions of the YBE, being retractable in theorem above being a multipermutation solution (see [13, 6.5] for an alternative proof). However, for the case where $\mathcal{G}_{(X,S)}$ is a nilpotent group, as example 122 shows, the solution (X,S) is not even retractable.

THEOREM 150. [68, Example 2] *There is a solution (X,S) to the Yang-Baxter equation, which is not a multipermutation solution, and whose permutation group $\mathcal{G}_{(X,S)}$ is nilpotent.*

CONJECTURE 151. [13, 7.1][45, 2.28] *(Gateva-Ivanova) Every square-free solution (X,S) of the Yang-Baxter equation of cardinality $n\geq 2$ is retractable. Furthermore, it is a multipermutation solution of level $m<n$.*

In the general scenario, this statement is incorrect, as demonstrated in [79], [13, 7.4]. Actually, the multipermutation level of a solution cannot be bounded in terms of n, even when the permutation group is abelian.

THEOREM 152. [13, 7.3] *Let n be a positive integer. Then there exists a finite multipermutation square-free solution of the Yang-Baxter equation of multipermutation level n such that its associated permutation group is an elementary abelian 2-group.*

However, there are specific classes where this question yields an affirmative result. For instance, this holds true when the structure group is abelian and also, as we shall see later, for the so called solutions of **square-free cardinality**, i.e., $|X|$ is not divisible by any power of a prime (see [12, 13, 16]).

LEMMA 153. [16, 3.5] *Let (X,S) be a solution of the YBE. Suppose that $\mathcal{G}_{(X,S)}$ has an abelian normal Sylow p-subgroup for some prime divisor p of $\left|\mathcal{G}_{(X,S)}\right|$. Then (X,S) is retractable.*

THEOREM 154. [16, 4.2] *Let (X,S) be an indecomposable solution of the YBE with $|X|=p_1\cdot\ldots\cdot p_n$ for different primes $p_1,\ldots,p_n$. Then (X,S) have multipermutation level $\leq n$.*

Indeed, a method to construct indecomposable solutions of size $|X|=p_1\cdot\ldots\cdot p_n$ and multipermutation level exactly n is provided given different primes $p_1,\ldots,p_n$ (see [16, 5.1]).

LEMMA 155. [75, 34] *Let (X,S) be a multipermutation solution and $Y \subseteq X$ be such that $S(Y,Y) \subseteq (Y,Y)$. Denote by $S_{|Y}$ to the restriction of S to $Y \times Y$. Then $(Y, S_{|Y})$ is also a solution of a finite multipermutation level and $mpl(Y, S_{|Y}) \leq mpl(X,S)$.*

The first part of Lemma above was proved in [13, 6.4] under the additional assumption that $(Y, S_{|Y})$ is invariant under the permutation group of $\mathcal{G}_{(X,S)}$.

DEFINITION 156. [38, 3.3,3.4] Let (Z, S_Z) be a decomposable solution, and write $Z = X \cup Y$ for some invariant non-degenerate subsets X, Y. Then (Z, S_Z) is called **twisted union** if $S_Z(x,y) = (g(y), f(x))$ for some permutations $g : Y \to Y$ and $f : X \to X$.

A solution (Z, S_Z) which is the union of solutions (X, S_X) and (Y, S_Y), is called a **generalized twisted union** of X and Y if the map $S_Z : X \times Y \to Y \times X$ is given by

$$S_Z(x,y) = \left(g_x(y), f_y(x)\right),$$

where $g_x : Y \to Y, f_y : X \to X$ are permutations, such that the permutation $g_{f_y(x)} : Y \to Y, x \in X$, is independent of $y \in Y$, and the permutation $f_{g_x(y)} : X \to X$, $y \in Y$, is independent of $x \in X$.

EXAMPLE 157. [38] If (X,S) is a solution so that $S(x,y) = \left(g(y), g^{-1}(x)\right)$, that is, a **permutation solution** (see [34]), then it is a twisted union of cyclic permutation solutions. Likewise, any multipermutation solution of level 2 is a generalized twisted union of indecomposable multipermutation solutions of level ≤ 2.

THEOREM 158. [12, 3.1] *There exists a multipermutation square-free solution of level 3 that it is not a generalized twisted union. Furthermore, the associated IYB group is abelian.*

THEOREM 159. [12, 4.2] *Let (X,S) be an square-free solution of the YBE. If every permutation is cyclic then (X,S) is a multipermutation solution. Moreover, if $|X| > 1$ then (X,S) is a generalized twisted union.*

Another approach to the study of solutions of the YBE also given in [38], is to consider those solutions for which the set X is an abelian group and the map S an affine transformation of X^2. Such solutions are called **affine solutions**. Extending the list of examples given in [38], more solutions where found in [1]. However, the previous approach towards classification by means of the affine solutions and generalized twisted unions used by Etingof, Soloviev and Schedler has been rarely continued (see [76]).

So far, solutions up to size 10 have been computed.

n	2	3	4	5	6	7	8	9	10
solutions	2	5	23	88	595	3456	34530	321931	4895272
square-free	1	2	5	17	68	336	2041	15534	150957
indecomposable	1	1	5	1	10	1	100	16	36
multipermutation	2	5	21	84	554	3295	32155	305916	4606440
irretractable	0	0	2	4	9	13	191	685	3590

FIGURE 3.4.1. Involutive non-degenerate solutions of the YBE

Another approach to the study of solutions was given in a talk during a workshop in Oberwolfach ([4]), where Ballester-Bolinches stated the question of describing all solutions with primitive permutation group. Such result, was achieved in [14].

THEOREM 160. [14, 3.1] *Let (X,S) be a finite primitive solution of the YBE with $|X|>1$. Then $|X|$ is prime. Thus, for each prime number p, there is only one primitive solution up to isomorphism: the cyclic solution.*

More recently, a more general class of solutions has been proposed for further research.

DEFINITION 161. [16] An indecomposable solution (X,S) of the YBE is called of **primitive level k** if k is the biggest positive integer such that there exist solutions $(X,S)=(X_1,S_1),(X_2,S_2),...,(X_k,S_k)$ with $|X_i|>|X_{i+1}|>1$ for $1\leq i\leq k-1$ and epimorphisms p_{i+1}: $(X_i,S_i)\rightarrow(X_{i+1},S-i+1)$ so that (X_k,S_k) is primitive.

Simple solutions where introduced by Vendramin [79, 2.9], but later studied by Cedó and Okniński in [15]... they are different definitions but coincide for the indecomposable case.

DEFINITION 162. [16, 3.1] A solution (X,S) of the YBE is a **simple solution** if $|X|>1$ and for every epimorphism $f:(X,S)\longrightarrow(Y,S')$ of solutions either f is an isomorphism or $|Y|=1$.

It is shown in [15, 4.13] that if $p_1,...,p_k$ are distinct primes and $m_1,...,m_k$ are positive integers and $m_1>1$, then there is a simple solution (X,S) of the YBE of cardinality $p_1^{m_1}\cdot...\cdot p_k^{m_k}$. However, there is no simple solution of a non-prime square-free cardinality, as it is asked in [15, 7.5]. Actually, several questions regarding simple solutions are asked in [15] and some of them remain unanswered. To name a few, it is unknown whether all indecomposable and irretractable solutions of size p^2, for p a prime, are also simple solutions. It is also asked whether there is a finite simple solution (X,S) of the YBE such that $G(X,S)$ is a non-trivial simple left brace. Another question, wonders if there exist a finite simple solution (X,S) with $X=Y\times Z$, so that the sets $O_y=\{(y,z)\mid z\in Z\}$ for $y\in Y$, are blocks of imprimitivity for the action of $\mathcal{G}_{(X,S)}$ on X, and $|Z|$ is not a divisor of $|Y|$. This last question is motivated by the construction of simple solutions so that $|Z|$ is a divisor of $|Y|$. With respect to such solutions, the reader is advised to check [17], where same authors proved some questions from article above and generalized other results. As a final comment about simple solutions, the following consists of a composition of [15, 4.1] and [17, 3.4].

LEMMA 163. [16, 3.2] *Assume that (X,S) is a simple solution of the YBE. Then it is indecomposable if $|X|>2$ and it is irretractable if $|X|$ is not a prime number.*

THEOREM 164. [16] *Given a solution (X,S) of square-free cardinality with $|X|=p_1\cdot...\cdot p_k$, the following hold:*

1. *$p_1,...,p_n$ are the only primes dividing the order of $\mathcal{G}_{(X,S)}$.*
2. *The Sylow p_i-subgroups of $\mathcal{G}_{(X,S)}$ are elementary abelian.*
3. *If P_i is a p_i-Sylow subgroup of the additive left brace $\mathcal{G}_{(X,S)}$, then $\mathcal{G}_{(X,S)}=P_1\cdot...\cdot P_n$.*
4. *$Soc\left(\mathcal{G}_{(X,S)}\right)$ is a Hall π-subgroup of the additive group $\mathcal{G}_{(X,S)}$ for some subset π of $\{p_1,...,p_n\}$.*

The reader is referred to the article to see more results regarding the brace structure of such solutions, which are described in great detail. In [8, 16], M. Castelli, G. Pinto and W. Rump prove that in the special case where $|X|=pq$ and the permutation group is cyclic then the multipermutation level equals 1. Additionally, a list of indecomposable solutions is given for size pq and abelian permutation group. Another approach for the classification

of solutions of the YBE is taken by P. Jedlička, A. Pilitowska, and A. Zamojska-Dzienio in [52], where solutions of multipermutation level 2 are studied, and later characterized for the indecomposable case with abelian permutation group in [53], by same authors.

So far, we have exposed most of results regarding non-degenerate and involutive solutions of the YBE. Now, we are ready to connect such solution with the main topic of earlier chapters, that is, with Garside groups.

3.5. Garside and the Yang-Baxter

Relationship between Garside groups with no squares on its presentation and square-free solutions of the Yang-Baxter equation was first proved in [46, 1.16]. Later, F. Chouraqui proved the result without the square-free hypothesis. Additionally, more precursors of such result can be found in literature, in words of F. Chouraqui in [19]: "Gateva-Ivanova and Van den Bergh define in [47] monoids and groups of left and right I-type, and they show that they yield solutions to the quantum Yang–Baxter equation. They show also that a monoid of left I-type is cancellative and has a group of fractions that is torsion-free and Abelian-by-finite. Jespers and Okniński extend their results in [54], and establish a correspondence between groups of I-type and the structure group of a non-degenerate, involutive, and braided set-theoretic solution". Relationship between Garside groups and the Yang-Baxter equation is provided by the following result.

THEOREM 165. [19, 1]

1. *Let X be a finite set, and (X,S) be solution of the YBE. Then the structure group $G(X,S)$ is a Garside group.*
2. *Conversely, assume that $Mon\langle X \mid Rel\rangle$ is a Garside monoid such that:*
   a) *The cardinality of Rel is $n(n-1)/2$, where n is the cardinality of X and each side of a relation in Rel has length 2; and*
   b) *If the word x_ix_j appears in Rel, then it appears only once.*

   Then there exists a function $S : X \times X \to X \times X$ such that (X,S) is a solution and $\langle X \mid Rel\rangle$ is its structure group.

Additionally, some new properties about this Garside family were also found in the same article.

THEOREM 166. [19, 2] *Let (X,S) be a solution of the YBE. Let $G(X,S)$ be its structure group and M the monoid with the same presentation. Then:*

1. *The right least common multiple of the elements in X is a Garside element in M;*
2. *The (co)homological dimension of $G(X,S)$ is equal to the cardinality of X;*
3. *The Garside group $G(X,S)$ is irreducible if and only if (X,S) is indecomposable.*

REMARK 167. Notice that on the last sentence, by indecomposable we mean as a solution, that is, X is not the disjoint union of two non-degenerate subsets (see [19, 5.3]). Actually, it is fairly easy to see how Zappa-Szép decomposition of the structure group relates with the decomposability of a solution in terms of disjoint non-degenerate subsets. However, the reader is referred to the previous reference to see a proof involving the original definition of irreducible Garside monoid, introduced by M. Picantin in terms of the quasi-center.

PROPOSITION 168. [21, 2.3] *For the structure monoid of a solution of the YBE. The following is satisfied:*

1. *If a is in $\mathrm{D}(\Delta)$ then it has $\ell(a)!$ representative words.*
2. *The number of divisors or Δ of length k is $\frac{n!}{(n-k)!k!}$ and so $|\mathrm{D}(\Delta)| = 2^n$.*

Actually similar results to the following ones were stated for the square-free case in [46].

PROPOSITION 169. [22, 4.2] [19] *Let M be the structure monoid of a solution (X,S), then:*

1. *The Garside element Δ is the l.c.m. of X for both left and right divisibility.*
2. *Let s belong to M. Then: s belongs to Div (Δ) if and only if exists $X_\ell \subseteq X$ such that s is the left l.c.m. of X_ℓ, if and only if, $X_r \subseteq X$ such that s is the right l.c.m. of X_r.*
3. *If s belongs to Div(Δ) then the subsets X_ℓ and X_r above are unique and have the same cardinality.*

Results above where obtained using the definition of Garside and dealing with the monoid. Actually, similar results from [46] where stated for monoids of I-type, and by that time, neither such monoids where fully related with the YBE nor the YBE was matches with Garside monoids. In the following, we shall give a different approach to the previous results. Despite we shall not provide a careful and in depth proof, it should be clear that by means of the I-structure such results can be more easily obtained.

As usual, let (X,S) be a solution of the YBE with $|X| = n$ and $S\left(x_i, x_j\right) = \left(x_t, x_z\right)$ where $t = g_i\left(j\right)$ and $z = f_j\left(i\right) = g_t^{-1}\left(i\right)$. We know that the structure group $G\left(X,S\right)$ can be seen as a subgroup of $\mathrm{FA}_n \rtimes \mathrm{Sym}_n$ where FA_n is the free abelian group with n generators, say $u_1, ..., u_n$. The set of atoms generating the Garside group $G\left(X,S\right)$ are $\{x_1, ..., x_n\}$, and we can identify x_i with $\left(u_i, g_i^{-1}\right)$. Actually, we already know that the expression $x_i x_j = x_t x_z$ can be derived from $\left(u_i u_t, \phi\left(u_i u_t\right)\right)$ in $\mathrm{FA}_n \rtimes \mathrm{Sym}_n$, in particular, such element represents the l.c.m. to the left for x_i and x_j (by letting Sym_n to act on the left we get the right l.c.m). Actually, we can compute the l.c.m. of any two elements of the monoid this way, despite not being atoms, by merging the elements of Fa_n.

On the other hand, if we consider the element $\left(u_i^2, \phi\left(u_i\right)\right) = \left(u_i, g_i^{-1}\right)\left(u_*, \phi\left(u_*\right)\right)$, then it cannot be written in other different way, has x_i as divisor on the left. Moreover, relation $g_i\left(*\right) = i$, is satisfied, and so $* = g_i^{-1}\left(i\right) = T^{-1}\left(i\right)$ where T is the diagonal map. Hence, $\left(u_i^2, \phi\left(u_i\right)\right) = x_i T^{-1}\left(x_i\right)$ and this expression is unique. Such elements, are called **frozen pairs**, and is clear that there are n different frozen pairs in $G\left(X,S\right)$. Elements of the form $\left(u_i^k, \phi\left(u_i^k\right)\right)$ fall under the similar conditions given $k \geq 2$ is a positive integer, and following [20], we call these **frozen element** of length k associated with x_i, and we denote them by $x_i^{[k]}$. More specifically, we see that $\left(u_i^k, \phi\left(u_i^k\right)\right) = \left(u_i, g_i^{-1}\right)\left(u_s^{k-1}, \phi\left(u_s^{k-1}\right)\right)$ where $s = T^{-1}\left(i\right)$, and so the frozen element of length k is a continuation of the frozen pair starting with x_i by concatenation of frozen pairs; because such continuation is unique, it should be clear that:

$$x_i^{[k]} = \left(u_i^k, \phi\left(u_i^k\right)\right) = x_i \cdot T^{-1}\left(x_i\right) \cdot T^{-2}\left(x_i\right) \cdot ... \cdot T^{-(k-1)}\left(x_i\right).$$

Additionally, if we write the semidirect action on the left, $\mathrm{Sym}_n \ltimes \mathrm{FA}_n$, then the natural way to describe the atoms is $x_i = \left(f_i, u_i\right)$ for $i = 1, ..., n$, and the frozen chain of length k for x_i ends with x_i, that is, $x_i^{[k]} = T^{k-1}\left(x_i\right) \cdot ... \cdot T^2\left(x_i\right) T\left(x_i\right) x_i$.

For the Garside element, we can make use of the fact that it is the l.c.m. of the atoms, and so $\delta = (u_1 \cdot u_2 \cdot ... \cdot u_n, \phi(u_1 \cdot u_2 \cdot ... \cdot u_n))$ (indeed, it is easy to prove by means of this presentation that δ is the minimal Garside element of G). In particular, we see that an element $\left(u_{s_1}^{e_1} \cdot ... \cdot u_{s_r}^{e_r}, \tau\right)$ where $\tau \in \mathcal{G}_{(X,S)}$ is a divisor of the Garside element if and only if the indices $s_1, ..., s_r$ are all different and $e_1, ..., e_r$ are either 0 or 1, that is, no frozen pair divides δ. Additionally, there are as many divisors of length k, as subsets of k different elements taken from a set with n elements. Thus δ has $\binom{n}{k}$ divisors of length k and a total of 2^n divisors in the monoid. Finally, if we consider an element of length k in the monoid, then the sum of the exponents in FA_n equals k, for instance, the elements $\left(u_i u_j u_t, \phi\right)$ and $\left(u_i^2 u_j, \phi\right)$ are elements of length 3, and a simple induction gives us that every element of length k has at most $k!$ different possible expressions in terms of atoms. In particular, the minimal Garside element can be written in $n!$ different ways in terms of atoms.

So far we know that Garside groups relate with non-degenerate involutive set-theoretical solutions of the YBE and vice versa. Additionally, if X is a finite set, and $S : X \times X \to X \times X$ is given by $S(x, y) = (g(x), f(y))$, that is, all elements in X have the same associated permutation, then one can substitute being involutive (i.e. $g = f^{-1}$) with $fg = gf$ in order to obtain that $G(X, S)$ is a Garside monoid. This result is achieved by constructing a new solution that is in fact braided, involutive and non-degenerate and have structure group isomorphic to $G(X, S)$. Form more details the reader is referred to [19].

PROPOSITION 170. [22, 5.3] *Let (X, S) be solution of the YBE. Assume $H^+$is a Garside submonoid of structure monoid $G^+(X, S)$ such that its atoms set X_H is closed under right complement in $G^+(X, S)$. Denote by H the (Garside) subgroup of $G(X, S)$ generated by H^+. Then there exists a uniquely well defined involutive bijective map $S_H : X_H \times X_H \to X_H \times X_H$ such that the pair (X_H, S_H) is a solution of the YBE so that $G(X_H, S_H)$ is isomorphic to H.*

By results above, we can now provide a nice characterization of Garside groups arising from solutions of the YBE.

COROLLARY 171. *If G^+, H^+, K^+ are monoids so that $G^+ = H^+ \bowtie K^+$, then G^+ is the structure monoid of a solution of the YBE if and only if H^+, K^+ are the structure monoids of solutions of the YBE.*

DEFINITION 172. We say that a partition $X_1, ..., X_k$ of a set X is **proper partition** if each X_i is not empty, they are disjoint, $X = \dot{\cup}_{i=1}^{k} X_i$ and $1 < k < |X|$.

DEFINITION 173. [22, 5.6] Let X be a finite set, and (X, S) be a solution of the YBE.

1. We say that (X, S) is **foldable** if X has a proper partition $X_1, ..., X_k$ such that:
   1. Every set X_i generates an atomic Garside submonoid of $M(X, S)$ with Garside element Δ_i.
   2. The set $X' = \{\Delta_1, ..., \Delta_k\}$ is closed by right and left complements in $G^+(X, S)$ and is the atom set of a Garside subgroup of $G(X, S)$.
2. In this case, let $S' : X' \times X' \to X' \times X'$ be the involutive bijective map provided by result above. We say that (X', S') is a folding of (X, S), or equivalently that $G(X', S')$ is a folding of $G(X, S)$.

3. We say that (X,S) is **strongly foldable** when furthermore each X_i generates a standard parabolic subgroup of $G(X,S)$. In this case, we say that (X',S') is a strong folding of (X,S).

THEOREM 174. [22, 2] *Let X be a finite set, and (X,S) be a solution of the YBE. The pair (X,S) is decomposable if and only if it has a strong folding (X',S) which is a trivial solution and such that $|X'|=2$.*

THEOREM 175. [22, 1] *Let X be a finite set, and (X,S) be a solution of the YBE. Let $G(X,S)$ be the structure group of (X,S). For $Y\subseteq X$, denote by G_Y the subgroup of $G(X,S)$ generated by Y. The map $Y\to G_Y$ induces a one-to-one correspondence between the set of invariant non-degenerate subsets of (X,S) and the set of standard parabolic subgroups of $G(X,S)$.*

LEMMA 176. [22, 4.3] *Given a solution (X,S) of the YBE. Denote by $G=G(X,S)$ its structure group, which is a Garside group, and given an invariant subset of atoms $Y\subseteq X$, denote by G_Y^+ to the submonoid of G^+ generated by Y. Then:*

1. *If s belongs to G_Y^+, then all the letters in a word that represents s belong to Y. In particular, every left or right divisor of s lies in G_Y^+.*
2. *Let s belong to $Div(\Delta)$. Then $s\in G_Y^+$ if and only if $X_\ell(s)\subseteq Y$ if and only if $X_r(s)\subseteq Y$. In particular, δ belongs to G_Y^+.*
3. *The monoid G_Y^+ is equal to $G^+\cap G_Y$.*

3.6. Coxeter-like quotient

In so far, we know that the structure group $G(X,S)$ of a non-degenerate involutive finite solution of the YBE (X,S), is a Garside group. Moreover, we know that braid groups and Artin-Tits groups of spherical type, can be characterized by means of short exact sequences, that is, there is a canonical way of constructing a normal subgroup so that the quotient group characterizes the group. In this section, we present an equivalent version of the Coxeter subgroup for our concerning case, first studied by F. Chouraqui in [21] under additional hypothesis, and later fully developed by P. Dehornoy in [29] and [30].

We remind the reader that for each atom $x_i\in X=\{x_1,...,x_n\}$, we have a frozen chain starting at x_i of arbitrary length. In particular, for x_i and length k we write the frozen chain as

$$x_i^{[k]}=\left(u_i^k,\phi\left(u_i^k\right)\right)=x_i\cdot T^{-1}(x_i)\cdot T^2(x_i)\cdot\ldots\cdot T^{k-1}(x_i).$$

Additionally, notice that because the diagonal map has finite order, say $o(T)=t$, if we let s be the order of $\phi\left(u_i^t\right)$, the associated permutation to u_i^t, then

$$\left(u_i^t,\phi\left(u_i^t\right)\right)^s=\left(u_i^{ts},\phi\left(u_i^t\right)^s\right),$$

since $\phi\left(u_i^t\right)$ fixes i, whence, $\phi\left(u_i^{ts}\right)=\phi\left(u_i^t\right)^s=1$. Thus, if $|X|=n$ and we take r as the l.c.m. of the orders of $\phi\left(u_i^t\right)$ for all $i=1,...,n$, then $\phi\left(u_i^{tr}\right)=1$ for all $i\in\{1,...,n\}$.

DEFINITION 177. Given a solution (X,S) of the YBE with $|X|=n$, the **Dehornoy class** of the solution is the least positive integer d so that $\phi\left(u_i^d\right)=1$ for all $i\in\{1,...,n\}$.

Before to explore more about the Dehornoy class we shall discuss several things. Firstly, we named the class after P. Dehornoy, who first introduced the class using other terms that shall omit in this text. Secondly, by the above commented it is clear that such element exists, however, this is dependent of our definition and the reader is referred to [30]. Thirdly, we borrowed the terms frozen chain from F. Chouraqui in [20], who also noticed the fact that every frozen chain can be written in terms of the diagonal permutation, and defined the Dehornoy class is a similar way. However, and unlike both authors, we shall make use of the I-structure for this particular Garside groups. Finally, the reader is pointed out that different definitions of the Dehornoy class can be made, in particular, we can provide two alternative definitions:

1. If we call $\Gamma=\{(u,1)\mid u\in \mathrm{FA}_n\}$, and let $A=\Gamma\cap G(X,S)$, then d is the least positive integer so that for every $(u,\phi(u))\in G(X,S)$ we have $\left(u^d,\phi\left(u^d\right)\right)\in A$. The group A is the unique **maximal normal abelian** subgroup of $G(X,S)$.
2. Equivalently, if we regard the structure group as a finite left brace, then addition on the brace is given by $\left(u_i,g_i^{-1}\right)+\left(u_j,g_j^{-1}\right)=\left(u_iu_j,\phi\left(u_iu_j\right)\right)$, and thus, d is exponent of the additive group of the left brace. In particular, the Dehornoy class is a divisor of the order of the finite group $\mathcal{G}_{(X,S)}$. In fact, this can be found as a theorem.

THEOREM 178. [55, G] *The Dehornoy class d of a solution (X,S) is the least common multiple of the orders (for the sum $+$) of the generators g_x for $x\in X$ of the group $\mathcal{G}_{(X,S)}$. If the solution is indecomposable, d is the additive order of g_x.*

In [30, 5.4] it is proven that d is a divisor of $n^2!$. However, the fact that d divides $n!$ seems somewhat implicit in P. Dehornoy's article, but more surprisingly, we see in [47, 5.2], a precursor of the Dehornoy class and this property. Additionally, for the indecomposable case, it was also proven by F. Chouraqui in [20], that all permutations have the same additive order, although this is an straightforward argument:

Consider the group A defined above, let $x_j^{[s]}\in A$, and take x_k an atom of $G(X,S)$. If we write $g_k^{-1}(j)=i$, then $x_j^{[s]}x_k=\left(u_j^su_k,1\cdot g_k^{-1}\right)=\left(u_k,g_k^{-1}\right)\left(u_i^s,\phi\left(u_i^s\right)\right)=x_kx_i^{[s]}$. Thus, $\phi(u_i^s)=1$ and conjugation by an atom sends $x_j^{[s]}$ to $x_i^{[s]}$. More generally, since every element can be written as a product of atoms, if $y\in G(X,S)$ and τ is its associated permutation, then conjugation by y sends $x_j^{[s]}$ to $x_{\tau(x_j)}^{[s]}$. When the solution is indecomposable, $\mathcal{G}_{(X,S)}$ acts transitively on X, thus $\left\{x_i^{[s]}\right\}_{i=1}^n$ are all conjugated in $G(X,S)$, and so, they all belong to A. In fact, same argument shows that the subgroup A normal in $G(X,S)$, and also the following result:

LEMMA 179. [55, 6.1] *For all elements x from the same $\mathcal{G}_{(X,S)}$-orbit of a solution (X,S), the order of g_x in the finite abelian group $(\mathcal{G}_{(X,S)},+)$ is the same.*

So far, we are ready to introduce the seminal result from P. Dehornoy in [29], which was later enhanced in [30].

THEOREM 180. [29, 1.2] *Let G is the structure group of solution (X,S) of YBE with X of size n and class d. Then there exist a Garside element Δ in M and a finite group W of order d^n entering a short exact sequence $1 \to \mathbb{Z}^n \to G(X,S) \to W \to 1$ such that (W,X) provides a germ for G^+ whose Cayley graph is the Hasse diagram of the divisors of a Garside element Δ. A presentation of W is obtained by adding n relations $x_i^{[d]} = 1$ to that of G, with $x_i^{[d]}$ the frozen chain starting at x_i.*

Using the I-structure, we can write result above in the following way:

THEOREM 181. *Let (X,S) be a solution of the Yang-Baxter equation and write $G(X,S) = \langle (u_i,\varphi_i) \mid i = 1,...,n\rangle$. If d is its Dehornoy class and we denote by $N = \left\langle x_i^{[d]} = (u_i^d, 1) \mid i = 1,...,n \right\rangle$, then the quotient group $W = G(X,S)/N$ is a finite group of size d^n. Additionally, there exists a bijection between the elements of W and the set of divisors of some Garside element Δ.*

REMARK 182. Notice that the unique maximal normal abelian subgroup A contains N, and so $W/(A/N) \cong G(X,S)/A$ which is also isomorphic to the permutation group $\mathcal{G}_{(X,S)}$. Thus, the order of $\mathcal{G}_{(X,S)}$ is a divisor of d^n (and as we know, divisible by d).

Moreover, as it is proven in [30], the quotient W characterizes the solution (X,S). From such a remarkable fact, and following P. Dehornoy's terminology, we have the following definition.

DEFINITION 183. Given a solution (X,S), we call the associated quotient group W the **Coxeter-like quotient** associated with (X,S).

THEOREM 184. [30, 5.11] *Given an solution (X,S) with Dehornoy class d and $|X| = n$, the Coxeter-like quotient W embeds into the wreath product $(\mathbb{Z}/d\mathbb{Z}) \wr Sym_n$ so that the first component is a bijection.*

Additionally, a linear representation of the structure group $G(X,S)$ and W is provided in the same article.

PROPOSITION 185. [30, 5.13] *Let (X,S) be a solution of the YBE of cardinal $|X| = n$ y Dehornoy class d. For $x_i \in X$ consider the matrix:*

$$\Theta_{x_i} = Q_i P_{g_i},$$

where Q_i is the diagonal $n \times n$-matrix with diagonal entries $(1,\ldots,1,q,1,\ldots,1)$ with q at position i, and P_{g_i} is the permutation matrix associated with g_i, that is, the matrix obtained by permuting the rows of the identity matrix by g_i. Then $\Theta_{x_1},...,\Theta_{x_n}$ provides a faithful representation of $G(X,S)$ into $\mathrm{GL}\left(n, \mathbb{Q}\left[q,q^{-1}\right]\right)$. In particular, specializing at $q = e^{2i\pi/d}$ gives a faithful representation of the Coxeter-like quotient W.

EXAMPLE 186. Consider the cyclic solution of three elements, that is, let $X = \{x_1,x_2,x_3\}$ and $g_1 = g_2 = g_3 = (123)$. Then

$$Q_1 = \begin{pmatrix} q & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Q_2 = \begin{pmatrix} q & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Q_3 = \begin{pmatrix} q & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{and } P_{g_i} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\Theta_{x_1} = \begin{pmatrix} 0 & q & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \Theta_{x_2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & q \\ 1 & 0 & 0 \end{pmatrix}, \Theta_{x_3} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ q & 0 & 0 \end{pmatrix}.$$

The Dehornoy class is 3, and thus the Coxeter-like quotient group W has cardinal $3^3 = 27$ and we can represent it by $\langle \Theta_{x_1}, \Theta_{x_2}, \Theta_{x_3} | q = e^{2\pi i/3} \rangle$. Remark that we obtained this example from [40, 2.14], where the matrix representation is extensively used and some results regarding the Dehornoy class are proven.

Ultimately, we enunciate a result which presents a connection between the group W and geometry, thus allowing for geometric interpretations for Garside groups related with the YBE, just like with Braid groups and Artin-Tits groups of spherical type.

PROPOSITION 187. [30, 5.15] *Every finite group that is the Dehornoy quotient group associated with a solution of size n, can be realized as a group of isometries in an n-dimensional Hermitian space.*

Finally, we end this section with an outstanding idea set in [30] by P. Dehornoy's: To extend the notion of I-structure by replacing the free abelian group FA_n with some other group and to characterize those Garside groups that admit such structure.

CHAPTER 4

A decomposition criteria for the Yang-Baxter equation

In this chapter, we shall present the content of our first article with the same title as above, but firstly we shall digress a little bit with some notation and results, so that the our goal can be better understood.

Given a solution (X,S) of the YBE, as usual, let $|X|=n$ and be means of the I-structure we identify $G(X,S)$ with the subgroup of $\mathrm{FA}_n \rtimes \mathrm{Sym}_n$ given by $\left\langle \left(u_i, g_i^{-1}\right)\right\rangle$. Moreover, given a positive integer $k \geq 1$, the subgroup $\left\langle x_i^{[k]}\right\rangle_{i=1}^{n}$ generated by the frozen elements of length k, is also the structure group of a solution of the YBE, since it is also a subgroup of $\mathrm{FA}_n \rtimes \mathrm{Sym}_n$ satisfying the necessary conditions for $\left\langle \phi\left(u_i^k\right)\right\rangle$ to be an IYB group. Actually, a simple proof can also be achieved by means of the Garside structure and Chouraqui's characterization given in Theorem 165 (actually, a simple proof can be made by means of cycle sets). In any case, given a solution (X,S) we can obtain new solutions by means of the frozen elements of arbitrary length k, which we denote by $\left(X^{[k]}, S^{[k]}\right)$, and so that

$$\mathcal{G}_{\left(X^{[k]},S^{[k]}\right)} = \left\langle \phi\left(u_i^k\right)\right\rangle_{i=1}^{k} \text{ and } G\left(X^{[k]},S^{[k]}\right) = \left\langle \left(u_i^k, \phi\left(u_i^k\right)\right)\right\rangle_{i=1}^{k},$$

in particular, $\mathcal{G}_{\left(X^{[k]},S^{[k]}\right)} \leq \mathcal{G}_{(X,S)}$ and $G\left(X^{[k]},S^{[k]}\right) \leq G(X,S)$. In particular, if (X,S) is retractable, the so is $\left(X^{[k]},S^{[k]}\right)$, and if (X,S) is has m.p.l r then the multipermutation level of $\left(X^{[k]},S^{[k]}\right)$ is lower equal than r (a formal proof for this result can be found in [55, 3.2]).

In the following, we shall see some results motivating our main theorem of this chapter.

THEOREM 188. [67] *Let (X,S) be a solution of the YBE of size $|X|=n$, and diagonal map T. If one of the following holds:*

1. *Some permutation $g_x \in \mathcal{G}_{(X,S)}$ is a cycle of length at least $|X|/2$ and is coprime with $|X|$.*
2. *Some permutation $g_x \in \mathcal{G}_{(X,S)}$ is the identity.*
3. *T is a cycle of length $n-1$.*
4. *T is an $(n-2)$-cycle and n is odd.*
5. *T is an $(n-3)$-cycle and g.c.d.$(3,n)=1$.*

Then (X,S) is decomposable.

Additionally, an indecomposable criteria is also proven in same article.

THEOREM 189. [67, 3.5] *Let (X,S) be a solution of the YBE of size n. If T is a cycle of length n, then X is indecomposable.*

Inspired by results above, we started looking for a general criteria for deciding whether a given solution is indecomposable or not. In particular, we found a simple sufficient condition for a solution to be decomposable, in particular, we require that the order of T and n are coprime. But in order to proof our main result, first, we need a couple of lemmas.

LEMMA 190. *Let G be a solvable group acting transitively on a set X of m elements, and let π be the set of primes dividing m. Then any Hall π-subgroup of G is transitive, as well.*

PROOF. First, recall that, since G is solvable, we know that there exists some Hall π-subgroup of G. Also these subgroups form a conjugacy class of subgroups of G. Moreover, if P is any Hall π-subgroup of G, there is some π'-Hall subgroup Q of G such that $G = PQ$.

Now, since G is transitive, the index in G of $\mathrm{Stab}(x)$ is equal to m, for every $x \in X$. If H is a π'-Hall subgroup of $\mathrm{Stab}(x)$, then it is a π'-Hall subgroup of G as well, and $Q = H^g$, for some $g \in G$. It follows that Q stabilizes some $y \in X$. Then $G = P\mathrm{Stab}(y)$. By the modular law, the index in P of $P \cap \mathrm{Stab}(y) = \mathrm{Stab}(y)$ is exactly m. Then the action of P on X is transitive. □

REMARK 191. Despite the fact that the next result is well known, we decided to state it here for convenience.

LEMMA 192. *Let (X, S) be an involutive solution of the YBE of class d. Let us denote by T the diagonal permutation. Then $T^d = Id_X$.*

PROOF. Denote by $G(X, S)$ the structure group, and by A its maximal normal abelian subgroup. By the definition of d, we know that the element $x_i^{[d]} = x_i T^{-1}(x_i) \cdot \ldots \cdot T^{-(d-1)}(x_i)$ is in A, for every $x_i \in X$. In particular if $T^{-1}(x_i) = x_j$ then $x_j^{[d]} = T^{-1}(x_i) \cdot T^{-2}(x_i) \ldots \cdot T^{-d}(x_i)$ is in A. Moreover, the swapping of an element $y \in G(X, S)$, with some element in A, fixes y, since every element of A acts trivially. Therefore, the first and last factors in the product $x_i T^{-1}(x_i) \cdot \ldots \cdot T^{-(d-1)}(x_i) T^{-d}(x_i)$, i.e. $x_i x_j^{[d]} = x_i^{[d]} T^{-d}(x_i)$, must coincide. Hence, we conclude $x_i = T^{-d}(x_i)$ for any $x_i \in X$, as desired. □

Notice that the order of T has to be a divisor of the class of the solution, but these two could be different.

EXAMPLE 193. Let (X, S) be the solution of the YBE where $X = \{x_1, \ldots, x_6\}$ and $S(x, y) = (g_y(x), f_x(y))$ given by:

$$g_{x_1} = (1,2,4,3,6,5), \quad g_{x_2} = (1,5,4,2,6,3), \quad g_{x_3} = (1,5,4,2,6,3),$$
$$g_{x_4} = (1,2,4,3,6,5), \quad g_{x_5} = (1,5,4,2,6,3), \quad g_{x_6} = (1,2,4,3,6,5),$$

and $f_{x_i} = T^{-1} g_{x_i}^{-1} T$ with diagonal permutation $T = (1,5)(2,4)(3,6)$. Despite the fact that T is of order 2, we see that the frozen pair $x_1 x_5$ has associated permutation $g_{x_1} g_{x_5} = (2,5,3) \neq \mathrm{Id}$, that is (X, S) has class different from 2 (actually, it has class 6).

Finally, before to enunciate our main result, we shall recall a Theorem of Wolfgang Rump, which we shall now make use of it in order to generalize it.

THEOREM 194. [69, 1] *Every square-free solution of the YBE with more than one element is decomposable. However an indecomposable square-free solution is possible when $|X|$ is infinite.*

THEOREM 195. [7, A] *Let (X,S) be a solution of the YBE, and denote by T its diagonal permutation. If the order of T and the cardinality of X are coprime, the solution is either decomposable or X has only one element.*

PROOF. First, we write $|X| = n$, and denote by d the Dehornoy class of the solution. Now, let π be the set of primes dividing n, and let also π' denote the set of primes not in π. As usual, let $G(X,S)$ be the structure group of the solution and A its maximal normal abelian subgroup. Additionally, we factorize $d = rs$, where r is a π-number and s is a π'-number.

We know that the subgroup of $G(X,S)$ generated by frozen elements of length s, is the structure group the solution $\left(X^{[s]}, S^{[s]}\right)$, i.e. $G\left(X^{[s]}, S^{[s]}\right) = \left\langle x_i^{[s]} \right\rangle_{i=1}^{n}$, and such solution has Dehornoy class $d/s = r$. Thus, as shown in Remark 182, the cardinality of the permutation group $\mathcal{G}_{\left(X^{[s]},S^{[s]}\right)}$ divides r^n. Additionally, from the left brace structure, $\left(\mathcal{G}_{(X,S)}, +\right)$ is an abelian group, where addition is given by $\phi(u) + \phi(v) = \phi(uv)$, in particular $k\phi(u) = \phi\left(u^k\right) \in \mathcal{G}_{\left(X^{[k]},S^{[k]}\right)}$, and so the exponent of the group $\mathcal{G}_{(X,S)}/\mathcal{G}_{\left(X^{[s]},S^{[s]}\right)}$ equals s. Therefore, $\mathcal{G}_{\left(X^{[s]},S^{[s]}\right)}$ is a Hall π-subgroup of $\mathcal{G}_{(X,S)}$.

Now notice that the product $x_i^{[s]}x_j^{[s]}$, is a frozen pair in $G\left(X^{[s]}, S^{[s]}\right)$ if and only if $x_i^{[s]}x_j^{[s]}$ is a frozen element of length $2s$ in $G(X,S)$ (which is trivial using the I-structure), in particular, the diagonal map of $\left(X^{[s]}, S^{[s]}\right)$ equals T^s, whose order is a π'-number by hypothesis.

Finally, assume that (X,S) is indecomposable. Then, by Lemma 190 , $\left(X^{[s]}, S^{[s]}\right)$ is also indecomposable. The cardinality of $X^{[s]}$ is n, so it is coprime with the order of T^s. Moreover, by Lemma 192, the order of T^s is a divisor of the Dehornoy class r, a π-number, and thus $T^s = \mathrm{Id}_X$. That means that $\left(X^{[s]}, S^{[s]}\right)$ is an square-free solution, and being indecomposable, we deduce form Theorem 126 that $n = 1$, concluding the proof. □

REMARK 196. If (X,S) is a solution of the IYB with diagonal permutation T, $|X| = n$ and Dehornoy class d, if we take is a positive integer s, then $\left(X^{[s]}, S^{[s]}\right)$ is a solution of the IYB with diagonal permutation T^s. Moreover if k equals the g.c.d. of s and d then its Dehornoy class is d/k, thus, if s is coprime with d then its Dehornoy equals d. In particular, if s is not coprime with d then $\left(X^{[s]}, S^{[s]}\right)$ and (X,S) are not isomorphic solutions. Additionally, in case we choose s to be the g.c.d. between n and the order of T, then $\left(X^{[s]}, S^{[s]}\right)$ is an indecomposable solution.

CHAPTER 5

About the primes dividing an IYB group

We start this chapter revisiting some basic results from group theory, which shall facilitate the introduction of our notation. Given an action of G into X, we say that $\mathcal{B}$ is a **block system** to any partition of X preserved by the action of G, i.e. $\mathcal{B} = \{B_1, ..., B_k\}$ where $X = \cup_{i=1}^{k} B_i$ and $B_i \cdot g = B_j \in \mathcal{B}$ for all $B_i \in \mathcal{B}$ and all $g \in G$. In general, whenever an element $x \in X$ belongs to B_i, we shall write B_x instead of B_1.

THEOREM 197 (Maschke's Theorem). *Every representation of a finite group G over a field $\mathbb{F}$ with characteristic not dividing the order of G is a direct sum of irreducible representations.*

Motivated by many examples of the YBE, we decided to study the primes dividing $\left|\mathcal{G}_{(X,S)}\right|$, that is, the primes dividing the Dehornoy class d of a solution, which also coincide with the primed dividing the order of the Coxeter-like quotient W associated with the solution (X, S). For the indecomposable case, we know that both $|X|$ and the order of T divide d, and so primes in $|X|, o(T)$ are primes dividing d, although the converse relation is still open. So far, we thought that all primes involved in d where primes dividing $|X|$, however, as we shall see, that is not always the case. Our main result of this chapter provides a characterization of primes involved in the order of the permutation group, and can be easily related with some recent results such as Theorem 164 (1), and

THEOREM 198. [55, F] *Take an indecomposable solution (X, S) of size pq, with $p < q$ prime and diagonal permutation T. Then the cycles in T have all order a multiple of q, with at most one exception of order a multiple of p.*

Recall that, in a finite solvable group G, any Hall π-subgroup P of G has a complement. This is to say, there is Q subgroup of G such that $G = PQ = QP$ and $P \cap Q = 1$.

DEFINITION 199. Let Q be an IYB-group with solution $\left(X, S_Q\right)$. Denote by w_x the element of Q associated to the right action of $x \in X$. Assume Q is a π-group for some set of primes π. We define the class of groups $\mathcal{S}(Q)$ as the class of finite solvable groups G such that Q is a Hall π-subgroup of G, and G has a faithful right action f on X such that:

- The restriction of f to Q yields the right action of S_Q, which we will sometimes write as f^Q.
- If P is a π'-complement of Q in G, and we have any two $p \in P$, $w_x \in Q$, then $w_x p = p' w'$ for some uniques $w' \in Q$, $p' \in P$. In this case $w' = w_{f_p(x)}$.

PROPOSITION 200. *Using the above notation:*

1. *If $G \in \mathcal{S}(Q)$ and $Q \leq H \leq G$, then $H \in \mathcal{S}(Q)$.*
2. *Assume G is an IYB-group with solution (X, S) and let Q be a Hall π-subgroup of G. Then $G \in \mathcal{S}(Q)$.*

PROOF.

1. Since Q is a Hall π-subgroup of H, it suffices to take the restriction to H of the right action of G.
2. Denote by f the right action of G on X. Since Q is a Hall π-subgroup of G, then Q is an IYB group with solution (X, S_Q). Then the right action of S_Q on X associated to the element $x \in X$ is $f_x^Q = f_{w_x}$ for some element $w_x \in Q$, and Q is generated by the elements w_x with $x \in X$. Moreover, for every $h \in G$, $w_x h = h' w_{f_h(x)}$. In particular, if P is a π'-complement of Q in G, and $p \in P$, we have $w_x p = p' w_{f_p(x)}$. We just need to prove that $p' \in P$. Since P is a Hall π'-subgroup, P is also an IYB-group with solution (X, S_P). If p_y is some generator of P, with $y \in X$, then $w_x p = p' w_{f_{p_y}(x)}$,and $p w_{f_{p_y}(x)}^{-1} = w_x^{-1} p'$. It follows that $p' = p_{f_{w_{f_p(x)}}^{-1}(y)} \in P$, and so, $p' \in P$ for every $p \in P$.

□

DEFINITION 201. If H is any subgroup of a group G, the largest normal subgroup of G contained in H is the subgroup

$$\mathrm{Core}_G(H) = \bigcap_{g \in G} H^g,$$

Consider G a transitive group of permutations of X, and N a normal subgroup of G. Then $N\mathrm{Stab}_G(x)$ is the stabilizer of the block B_x in some block system $\mathcal{B}$. Since G is transitive, every block stabilizer is conjugate to $N\mathrm{Stab}_G(x)$. Therefore, N stabilizes every block in $\mathcal{B}$. As a consequence, the block system $\mathcal{B}$ consists exactly of the N-orbits in X. Thus G/N acts transitively on $\mathcal{B}$ and N acts transitively on every block B_x. However, the action of G/N on $\mathcal{B}$ could be non-faithful. The induced group of permutations on $\mathcal{B}$ is $G/N_{\mathcal{B}}$, where $N_{\mathcal{B}} = \mathrm{Core}_G(\mathrm{Stab}_G(B_x))$, for any block $B_x \in \mathcal{B}$.

Assume also that G is an IYB-group with indecomposable solution (X, S), and $\mathcal{B}$ is a block system for the right action of S. We define an equivalence relation $\sim$ in X that has $\mathcal{B}$ as equivalence classes. Then $G/N_{\mathcal{B}}$ is the induced group of permutations on $X/\sim$. However, this is not necessarily an IYB-group. But we can give sufficient conditions. Similarly to retractability (see Section 3.4) if we impose $f_x = f_y$ whenever x, y are in the same block, $G/N_{\mathcal{B}}$ is an IYB-group in case S is compatible with $\sim$. Since $\mathcal{B}$ is a block system for the right action of S, this is compatible with $\sim$. Therefore, only the left action of S has to be checked. Notice that unlike in [54, Section 3], we are not interested in the blocks of $\mathcal{B}$, but in the permutation of such blocks induced by $G/N_{\mathcal{B}}$.

We will also need a theorem regarding the intersection of a family of maximal subgroups of a finite group.

DEFINITION 202. The Frattini subgroup of a finite group G is the subgroup

$$\Phi(G) = \cap\{M : M \text{ is a maximal subgroup of } G\}.$$

If p is a prime dividing $|G|$, then

$$\Phi_p(G) = \cap\{M : M \text{ is a maximal subgroup of } G \text{ with } (p, |G : M|) = 1\}.$$

THEOREM 203. [60, Theorem 7 (iii)] *If G is a finite group, then $\Phi_p(G) = PT$, where P is a normal Sylow p-subgroup of $\Phi_p(G)$ and T is a nilpotent complement of P.*

Notice that since P char $\Phi_p(G) \trianglelefteq G$, we have $P \trianglelefteq G$ as well.

LEMMA 204. *Let Q be an IYB-group with solution (X,S), and let G be a transitive group in $\mathcal{S}(Q)$. Denote by f the right action of G on X and write $|X| = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$, with p_i primes. If Q is a non-trivial q-group for some prime q not dividing $|X|$, then q divides $p_i^n - 1$ for some $i \in \{1,\ldots,r\}$ and $1 \leq n \leq n_i$. In particular, if f is not a primitive permutation and $|X| = p^m$, then q divides $p^l - 1$ for some $1 \leq l \leq m-1$.*

PROOF. We use induction on $|G|$. Since $G \in \mathcal{S}(Q)$, we may denote by $f_x^Q \in Q$ to the permutation induced by the right action of S for $x \in X$, and w_x the associated element of Q. Let P be a q'-complement of Q in G. Since q does not divide $|X|$, P has to be transitive on X. Now, since every stabilizer $\mathrm{Stab}(x)$ contains a Sylow q-subgroup of G, and these stabilizers are conjugate in G, it follows that G cannot have any non-trivial normal q-subgroup. Then $F = \mathrm{Fitt}(G)$, the Fitting subgroup of G, is a q'-subgroup, which is non trivial because G is solvable. Consider M any maximal subgroup of G containing Q. As noted above, $M \in \mathcal{S}(Q)$. If M is transitive on X, then we may use induction hypothesis and conclude $Q = 1$. Now, since G is solvable, $F/\Phi(G)$ is abelian and $F \cap M \trianglelefteq G$. Then the $F \cap M$-orbits in X form a block system $\mathcal{B}$ whose stabilizers are $\{(F \cap M)\mathrm{Stab}_G(x) : x \in X\}$. Consider the subgroup $N_{\mathcal{B}} = \mathrm{Core}((F \cap M)\mathrm{Stab}(x))$. This is independent of the choice of x. If $G = N_{\mathcal{B}}M$, then $G = (F \cap M)\mathrm{Stab}(x)M = \mathrm{Stab}(x)M$. It follows that M is transitive and $Q = 1$. As a consequence, we may assume $N_{\mathcal{B}} \leq M$, so that $N_{\mathcal{B}} \leq \mathrm{Core}(M)$.

Now, $G/N_{\mathcal{B}}$ is a transitive group of permutations of $\mathcal{B}$, and we aim to prove that the the equivalence relation $\sim$ in X which has $\mathcal{B}$ as equivalence classes and $f_x^Q = f_y^Q$ for all $y \in B_x$, is compatible with S, and that $Q/(Q \cap N_{\mathcal{B}})$ is isomorphic to an IYB-group with solution $(X/\sim, S/\sim)$. As noted before, it suffices to show the compatibility of the left action in S with $\sim$, but first we shall see that $\sim$ is well defined. If $h \in F \cap M$ and $w_x \in Q$, then since $G \in \mathcal{S}(Q)$,

$$h^{w_x^{-1}} = w_x h w_x^{-1} = h' w_{f_h(x)} w_x^{-1},$$

for some $h' \in F \cap M$, and because $h^{w_x^{-1}} \in F \cap M$, $w_{f_h(x)} w_x^{-1} = h'^{-1} h^{w_x^{-1}}$ belong to $P \cap Q = 1$, that is, $w_x = w_{f_h(x)}$. Consequently, $w_x = w_y$ when x, y belong to the same block $B \in \mathcal{B}$. Now, consider the diagonal permutation of (X,S), denoted by T, and defined as $T(x) = f_x^{Q-1}(x)$ (see [38, 69] for more details). Since $f_x^Q = f_y^Q$, when x, y are in the same block, $T(x), T(y)$ are in the same block, too. By [38], the left action in S is equal to $g_x^Q = T^{-1}\left(f_x^Q\right)^{-1} T$. Thus, it has to send elements in the same block to elements in the same block. And we conclude $\sim$ is compatible with S. Then the quotient $Q/\sim = Q/(Q \cap N_{\mathcal{B}}) \simeq QN_{\mathcal{B}}/N_{\mathcal{B}}$ is an IYB-group with solution $(X/\sim, S/\sim)$. Also $G/N_{\mathcal{B}} \in \mathcal{S}(Q/\sim)$. Moreover, $|X/\sim|$ is a divisor of $|X|$. Therefore, if $N_{\mathcal{B}} \neq 1$, we may use induction hypothesis and conclude that $G/N_{\mathcal{B}}$ has a trivial Sylow q-subgroup. It follows that $Q \leq N_{\mathcal{B}}$ and $Q \leq \mathrm{Core}_G(M)$. If this holds for every maximal subgroup M of G containing Q, then $\mathrm{Core}_G(M)$ contains Q, for every M maximal subgroup of G with index coprime with q. This is to say, $Q \leq \Phi_q(G)$, and Q is normal in G by the theorem above. Since G has no normal q-subgroup, we conclude that either $Q = 1$ or $N_{\mathcal{B}} = 1$ for some maximal subgroup M of G. Assume the later.

Now, $F \cap M \leq (F \cap M)\mathrm{Stab}(x)$, and $F \cap M$ is normal in G. Then $F \cap M \leq \mathrm{Core}((F \cap M)\mathrm{Stab}(x)) = N_{\mathcal{B}} = 1$. So $F \cap M = 1$, and it follows that F is a minimal normal subgroup of

G. Therefore, the cardinality of F is a power of a prime p. Moreover p has to divide $|X|$, but $|F|$ is not necessarily a divisor of $|X|$. We will find a non-trivial subgroup V of F, which is Q-invariant, $C_V(Q) = 1$, and such that its cardinality is a divisor of $|X|$. Consider an F-orbit C containing an element $x \in X$ which is not stabilized by Q. Since q does not divide $|C|$, we may find an element $a \in C$, such that $Q \leq \mathrm{Stab}_G(a)$. We know that $\mathrm{Core}_G(\mathrm{Stab}_G(a)) = 1$, hence $F\mathrm{Stab}_G(a)$ is the stabilizer of some block C_a in a non trivial block system $\mathcal{C}$ of X. Again, the blocks in $\mathcal{C}$ are exactly the F-orbits in X. And $C = C_a$. Moreover, $Q \leq \mathrm{Stab}_G(a)$, so Q stabilizes C_a. In addition, F is an abelian group of order coprime with q, whence $F = C_F(Q) \times [F, Q]$. Since G solvable, $C_G(F) \leq F$, and it follows that $[F, Q] \neq 1$. Now, $\mathrm{Stab}_{[F,Q]}(a)$ is Q-invariant, and, by Maschke's Theorem, there is a Q-invariant complement of $\mathrm{Stab}_{[F,Q]}(a)$ in $[F, Q]$. Call it V. Consequently $V \cap \mathrm{Stab}_{[F,Q]}(a) = 1$, so V acts faithfully on C_a, and $|V|$ must be a divisor of $|X|$. We will prove that $[F, Q]$ cannot stabilize a.

Since Q does not stabilizes every element in C_a, we have that there is some $w_z \in Q$, and $y \in C_a$ with $w_z(y) \neq y$. F is transitive on C_a, so there is some $k \in F$, such that $f_k(a) = y$. Then

$$[f_k, w_z](a) = f_k^{-1} w_z^{-1} f_k w_z(a) = f_k^{-1} w_z^{-1}(y),$$

which is different to a. Therefore, $[F, Q]$ cannot stabilize a, and $V \neq 1$.

So far, we have that V is Q-invariant and $C_V(Q) = 1$, so that VQ is not abelian. Therefore, some non trivial epimorphic image of Q is isomorphic to a subgroup of $GL(t, p)$, where $|V| = p^t$. Then q divides some $p^n - 1$, with $n \leq t$. Finally, by the hypothesis, $Q = 1$, finishing the first part of the statement.

For the last part, if Q is non trivial and q does not divide any $p^l - 1$, with $l \leq m - 1$, then a minimal Q-invariant subgroup W of V has to have cardinality p^m. Then, W is transitive on X and Q is a maximal subgroup of WQ. Therefore, $Q = \mathrm{Stab}_{WQ}(a)$ and we deduce that the action of WQ on X is primitive. Therefore, the whole action f is primitive on X. □

THEOREM 205. *Let G be an IYB-group with indecomposable solution (X, S). If G has an element of prime order q, then either:*

- *q divides $|X|$, or*
- *q divides some $p^n - 1$, with p prime and p^n dividing $|X|$.*

In particular, if $|X| = p^m$ and $p \neq q$, q has to divide $p^r - 1$, for some $r \leq m - 1$.

PROOF. For the first part, if $Q \in \mathrm{Syl}_p(G)$, then $G \in \mathcal{S}(Q)$, and the result follows from the lemma. In the case $|X| = p^m$, we may use the lemma too, but we need the additional hypothesis f not primitive. If f is primitive, we deduce $m = 1$ from main result in [14], and G has to be cyclic of order p from [38, Theorem 2.2]. □

The aforementioned theorem extends certain cohetanian findings from [16] and [55]. In the following we turn this theorem into a decomposability criterion.

COROLLARY 206. *Let G an IYB-group with solution (X, S). Assume $|X| = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, with p_i primes. If G has an element of prime order q, such that q does not divide $|X|$, nor any $p_i^n - 1$ with $n \leq n_i$, for $i = 1, \ldots, k$, then (X, S) is decomposable.*

As the following example shows, we cannot restrict the primes dividing the cardinality of an indecomposable IYB-group to the primes dividing the cardinality of X.

EXAMPLE 207. Consider the Yang-Baxter solution for $X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$ given by $S(x_i, x_j) = (g_{x_i}(x_j), f_{x_j}(x_i))$ where:

$$g_{x_1} = (1,6)(2,5)(3,8)(4,7), \quad g_{x_2} = (1,2,3,8)(4,7,6,5), \quad g_{x_3} = (1,8,5,4)(2,3,6,7),$$
$$g_{x_4} = (1,6)(2,7)(3,4)(5,8), \quad g_{x_5} = (1,4,5,8)(2,7,6,3), \quad g_{x_6} = (1,8,3,2)(4,5,6,7),$$
$$g_{x_7} = (1,2)(3,4)(5,6)(7,8), \quad g_{x_8} = (1,4)(2,5)(3,6)(7,8).$$

The diagonal map T corresponds with the permutation $(1,2,3,4,5,6)(7,8)$ of order 6. However the cardinality of the set $|X|$ equals 8, and the IYB-group has a permutation of order 3, $g_{x_1} * g_{x_2} = (1,5,3)(2,4,6)$. As claimed in Theorem A, $q = 3$ is a prime not dividing $|X| = 2^3$ but dividing $2^2 - 1$.

REMARK 208. From all known examples, that is, for all indecomposable solutions (X, S) of the YBE with $|X| \leq 10$, the above example is, up to isomorphism, the only known case where a prime q dividing the cardinality of the IYB-group, is not dividing $|X|$ (see [1] for the computation of such solutions, or download the GAP package enumeration from Leandro Vendramin's GitHub).

Index

Nomenclature

$\bowtie$	Zappa-Szép product
Δ	Garside element
δ	Minimal Garside element
Δ_a	Generator of the quasi-center
Γ	$\{(u,1) \mid u \in \mathrm{FA}_n\}$
(X,S)	Set-theoretic solution of the YBE
$\mathcal{G}_{(X,S)}$	Permutation group, IYB group
$\parallel x \parallel$	Norm of an element
ϕ	Map associated with an IYB group
$\mathrm{Div}\,(\Delta)$	Set of divisors of Δ
FA_n	Free-abelian group of rank n
Fa_n	Free-abelian monoid of rank n
$\mathrm{Ret}\,(X,S)$	Retracted solution of (X,S)
$\mathrm{Ret}^k\,(X,S)$	k-th retracted solution of (X,S)
$\mathrm{Supp}_{G^+}\,(\delta)$	Set of atoms of G^+ dividing δ
$N_1, N_2, ..., N_i$	Quasi-central decomposition of G
$\vee_L, \vee_R$	Least common multiple on the left and on the right
$\wedge_L, \wedge_R$	Greatest common divisor on the left and on the right
A	Maximal normal abelian subgroup
d	Dehornoy class of a solution
f_x	Second compoenent of the map S
$G(X,S)$	Structure group of a solution
G^+	Underlying Garside monoid
g_x	First compoenent of the map S
G_δ	Subgroup generated by $\mathrm{Supp}_{G^+}(\delta)$
G_Y^+	Submonoid generated by Y
N_i	Quasi-central factor of G
$QZ\,(G)$	Quasi-centralizer of X in the Garside group G
$QZ\,(M)$	Quasi-center of the Garside monoid M
T	Diagonal map of a solution
u_i	Element of Fa_n
W	Coxeter-like quotient of G
$x_i^{[k]}$	Frozen element of length k associated with x_i

Bibliography

[1] Ö. Akgün, M. Mereb, and Leandro Vendramin. Enumeration of set-theoretic solutions to the Yang-Baxter equation. *Mathematics of Computation*, 91(335):1469–1481, 2022. 3.4, 208

[2] Bernhard Amberg, Silvana Franciosi, and Francesco de Giovanni. *Products of Groups*. Oxford Mathematical Monographs. Oxford University Press, 1993. 114

[3] David Bachiller Pérez. Study of the algebraic structure of left braces and the Yang-Baxter equation. (document), 3.2

[4] A. Ballester-Bolinches. Finite groups versus finite left braces. *talk in MiniWorkshop: Algebraic Tools for Solving the Yang-Baxter Equation, Oberwolfach,*, November 2019. 3.4

[5] Rodney Baxter. Eight-vertex model in lattice statistics and one-dimensional anisotropic heisenberg chain. i. some fundamental eigenvectors. *Annals of Physics*, 76(1):1–24, 1973. (document), 3.1

[6] Joan S Birman, Volker Gebhardt, and Juan González-Meneses. Conjugacy in garside groups i: cyclings, powers and rigidity. *Groups, Geometry, and Dynamics*, 1(3):221–279, 2007. 1.8

[7] Sergio Camp-Mora and Raúl Sastriques. A Criterion for Decomposabilty in QYBE. *International Mathematics Research Notices*, 12 2021. rnab357. (document), 7, 17, 195

[8] M. Castelli, G. Pinto, and W. Rump. On the indecomposable involutive set-theoretic solutions of the Yang-Baxter equation of prime-power size. *Arxiv*, 2019. 3.4

[9] Francesco Catino, Ilaria Colazzo, and Paola Stefanelli. On regular subgroups of the affine group. *Bulletin Of The Australian Mathematical Society*, 91(1):76–85, 2015. (document)

[10] Ferran Cedó. Left braces: solutions of the Yang-Baxter equation. *Adv. Group Theory Appl.*, 5:33–90, 2018. 3.3

[11] Ferran Cedó, Eric Jespers, and Ángel del Río. Involutive Yang-Baxter groups. *Trans. Amer. Math. Soc.*, 362(5):2541–2558, 2010. 3.2, 130, 131, 132, 133, 3.2

[12] Ferran Cedó, Eric Jespers, and Jan Okniński. Retractability of set theoretic solutions of the Yang-Baxter equation. *Advances in Mathematics*, 224(6):2472–2484, 2010. 3.2, 3.4, 158, 159

[13] Ferran Cedó, Eric Jespers, and Jan Okniński. Braces and the Yang-Baxter equation. *Communications in Mathematical Physics*, 327(1):101–116, 2014. 134, 136, 3.4, 151, 3.4, 152, 3.4, 3.4

[14] Ferran Cedó, Eric Jespers, and Jan Okniński. Primitive set-theoretic solutions of the Yang-Baxter equation. *Communications in Contemporary Mathematics*, page 2150105, 2022. 3.4, 160, 5

[15] Ferran Cedó and Jan Okniński. Constructing finite simple solutions of the Yang-Baxter equation. *Advances in Mathematics*, 391:107968, 2021. 3.4, 3.4

[16] Ferran Cedó and Jan Okniński. Indecomposable solutions of the Yang-Baxter equation of square-free cardinality. *Arxiv*, 2022. (document), 3.4, 153, 154, 3.4, 161, 162, 163, 164, 5

[17] Ferran Cedó and Jan Okniński. New simple solutions of the Yang-Baxter equation and solutions associated to simple left braces. *Journal of Algebra*, 600:125–151, 2022. 3.4

[18] R. Charney, J. Meier, and K. Whittlesey. Bestvina's normal form complex and the homology of garside groups. *Geometriae Dedicata*, 105(1):171–188, Apr 2004. 37

[19] Fabienne Chouraqui. Garside groups and Yang-Baxter equation. *Comm. Algebra*, 38(12):4441–4460, 2010. (document), 1.2, 117, 3.5, 165, 166, 167, 169, 3.5

[20] Fabienne Chouraqui. Construction of a group of automorphisms for an infinite family of garside groups. *Arxiv*, 2014. 3.5, 3.6, 3.6

[21] Fabienne Chouraqui and Eddy Godelle. Finite quotients of groups of i-type. 258:46 – 68. 168, 3.6

[22] Fabienne Chouraqui and Eddy Godelle. Folding of set-theoretical solutions of the Yang-Baxter equation. 15(6):1277–1290. (document), 169, 170, 173, 174, 175, 176

[23] Alfred H Clifford and Gordon B Preston. The algebraic theory of semigroups, vol. 1. *Amer. Math. Soc. Surveys*, 7(1961):1967, 1961. 1.2

[24] Harold SM Coxeter. The complete enumeration of finite groups of the form r i 2=(r i r j) kij= 1. *Journal of the London Mathematical Society*, 1(1):21–25, 1935. 1.1

[25] María Cumplido, Volker Gebhardt, Juan González-Meneses, and Bert Wiest. On parabolic subgroups of artin–tits groups of spherical type. *Advances in Mathematics*, 352:572–610, 2019. 1.4

[26] Nir Ben David. *On groups of central type and involutive Yang-Baxter groups: a cohomological approach*. Technion-Israel Institute of Technology, Faculty of Mathematics, 2012. (document)

[27] Patrick Dehornoy. Groupes de garside. In *Annales scientifiques de l'Ecole normale supérieure*, volume 35, pages 267–306. No longer published by Elsevier. 1.2, 1.8

[28] Patrick Dehornoy. Gaussian groups are torsion free. *Journal of Algebra*, 210(1):291 – 297, 1998. 85

[29] Patrick Dehornoy. Coxeter-like groups for set-theoretic solutions of the Yang-Baxter equation. *C. R. Math. Acad. Sci. Paris*, 351(11-12):419–424, 2013. (document), 3.6, 3.6, 180

[30] Patrick Dehornoy. Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs. *Adv. Math.*, 282:93–127, 2015. (document), 3.6, 3.6, 3.6, 3.6, 3.6, 184, 185, 187, 3.6

[31] Patrick Dehornoy, François Digne, and Jean Michel. Garside families and garside germs. *Journal of Algebra*, 380:109 – 145, 2013. (document)

[32] Patrick Dehornoy, Francois Digne, Eddy Godelle, Daan Krammer, and Jean Michel. Foundations of garside theory. (document)

[33] Patrick Dehornoy and Luis Paris. Gaussian groups and garside groups, two generalisations of artin groups. 79(3):569–604. (document), 1.1, 1.2, 1.2, 1.2, 40, 1.8

[34] V. G. Drinfel'd. On some unsolved problems in quantum group theory. In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992. 3.1, 157

[35] Michael Eisermann. Yang-Baxter deformations of quandles and racks. *Algebraic & Geometric Topology*, 5(2):537–562, 2005. (document)

[36] Pavel Etingof. Geometric crystals and set-theoretical solutions to the quantum Yang-Baxter equation. *Communications in Algebra*, 31(4):1961–1973, 2003. (document)

[37] Pavel Etingof and Shlomo Gelaki. A method of construction of finite-dimensional triangular semisimple hopf algebras. *arXiv preprint math/9806072*, 1998. (document)

[38] Pavel Etingof, Travis Schedler, and Alexandre Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999. (document), 1.2, 3.1, 120, 124, 125, 127, 3.1, 3.2, 145, 147, 156, 157, 3.4, 5, 5

[39] S. Featherstonhaugh, Andrea Caranti, and L. Childs. Abelian hopf galois structures on prime-power galois field extensions. *Transactions of the American Mathematical Society*, 364(7):3675–3684, 2012. (document)

[40] Edouard Feingesicht. Dehornoy's class and sylows for set-theoretical solutions of the Yang-Baxter equation, 2023. 186

[41] Nuno Franco and Juan González-Meneses. Conjugacy problem for braid groups and garside groups. *Journal of Algebra*, 266(1):112–132, 2003. (document)

[42] Neus Fuster i Corral. Left braces and the Yang-Baxter equation. (document)

[43] Tatiana Gateva-Ivanova. Noetherian properties of skew polynomial rings with binomial relations. *Transactions of the American Mathematical Society*, 343(1):203–219, 1994. (document)

[44] Tatiana Gateva-Ivanova. Skew polynomial rings with binomial relations. *Journal of Algebra*, 185(3):710–753, 1996. (document)

[45] Tatiana Gateva-Ivanova. A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation. *Journal of mathematical physics*, 45(10):3828–3858, 2004. 151

[46] Tatiana Gateva-Ivanova. Garside structures on monoids with quadratic square-free relations. *Algebras and representation theory*, 14(4):779–802, 2011. 3.5, 3.5, 3.5

[47] Tatiana Gateva-Ivanova and Michel Van den Bergh. Semigroups ofi-type. *Journal of Algebra*, 206(1):97–112, 1998. (document), 1.2, 3.5, 3.6

[48] Volker Gebhardt and Stephen Tawn. Zappa-Szép products of garside monoids. *Mathematische Zeitschrift*, 282(1):341–369, Feb 2016. (document), 1.6, 64, 65, 69, 1.6, 70, 71, 73, 74, 89

[49] Eddy Godelle. Parabolic subgroups of garside groups. 317(1):1 – 16. (document), 32, 1.2, 1.4, 45, 47, 48, 49, 50, 52, 1.4, 53, 54, 55

[50] Eddy Godelle and Luis Paris. Pregarside monoids and groups, parabolicity, amalgamation, and fc property. *International Journal of Algebra and Computation*, 23(06):1431–1467, 2013. (document)

[51] Meng Hangyang, Adolfo Ballester-Bolinches, Ramon Esteban-Romero, and N. Fuster-Corral. On finite involutive Yang-Baxter groups. *Proceedings of the American Mathematical Society*, 149:1, 12 2020. 3.2

[52] Přemysl Jedlička, Agata Pilitowska, and Anna Zamojska-Dzienio. The construction of multipermutation solutions of the Yang-Baxter equation of level 2. *Journal of Combinatorial Theory, Series A*, 176:105295, 2020. 3.4

[53] Přemysl Jedlička, Agata Pilitowska, and Anna Zamojska-Dzienio. Indecomposable involutive solutions of the Yang-Baxter equation of multipermutational level 2 with abelian permutation group. *Forum Mathematicum*, 33(5):1083–1096, 2021. 3.4

[54] Eric Jespers and Jan Okniński. Monoids and groups of I-type. *Algebr. Represent. Theory*, 8(5):709–729, 2005. (document), 3.1, 144, 3.5, 5

[55] Victoria Lebed, Santiago Ramírez, and Leandro Vendramin. Involutive Yang-Baxter: cabling, decomposability, dehornoy class, 2022. (document), 178, 179, 4, 198, 5

[56] Eon-Kyung Lee and Sang-Jin Lee. Abelian subgroups of garside groups. *Communications in Algebra*, 36, 10 2006. (document), 36, 84

[57] Eon-Kyung Lee and Sang Jin Lee. Translation numbers in a garside group are rational with uniformly bounded denominators. *Journal of Pure and Applied Algebra*, 211(3):732 – 743, 2007. (document), 68, 86, 87, 1.8, 88

[58] Eon-Kyung Lee and Sang-Jin Lee. Periodic elements in garside groups. *Journal of Pure and Applied Algebra*, 215(10):2295 – 2314, 2011. (document), 35, 39

[59] Sang Jin Lee. Garside groups are strongly translation discrete. *Journal of Algebra*, 309(2):594–609, 2007. 1.8

[60] N.P. Mukherjee and Prabir Bhattacharya. On the intersection of a class of maximal subgroups of a finite group. *Canadian Journal of Mathematics*, 39(3):603–611, 1987. 203

[61] Matthieu Picantin. *Petits Groupes Gaussiens*. PhD thesis, 2000. 42

[62] Matthieu Picantin. The center of thin gaussian groups. *Journal of Algebra*, 245(1):92 – 122, 2001. (document), 1.2, 1.5, 56, 57, 1.5, 59, 61, 75

[63] Matthieu Picantin. The conjugacy problem in small gaussian groups. *Communications in Algebra*, 29(3):1021–1039, 2001. (document), 33, 82

[64] Matthieu Picantin. Garside monoids vs divisibility monoids. *Mathematical Structures in Computer Science*, 15(2):231–242, 2005. 34

[65] Matthieu Picantin. Tree products of cyclic groups and hnn extensions. *arXiv preprint arXiv:1306.5724*, 2013. (document), 1.7, 77, 78, 80, 81

[66] David E. Radford. *Hopf algebras*, volume 49. World Scientific, 2011. (document)

[67] Santiago Ramírez and Leandro Vendramin. Decomposition theorems for involutive solutions to the Yang-Baxter equation. *International Mathematics Research Notices*, 2021. (document), 148, 149, 188, 189

[68] Wolfgang Rump. Braces, radical rings, and the quantum Yang-Baxter equation. 307(1):153 – 170. (document), 150

[69] Wolfgang Rump. A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation. *Adv. Math.*, 193(1):40–55, 2005. (document), 126, 149, 194, 5

[70] Wolfgang Rump. Right l-groups, geometric garside groups, and solutions of the quantum Yang-Baxter equation. *Journal of Algebra*, 439:470–510, 2015. (document)

[71] Wolfgang Rump. Classification of non-degenerate involutive set-theoretic solutions to the Yang-Baxter equation with multipermutation level two. *Algebras and Representation Theory*, 25(5):1293–1307, 2022. (document), 137, 141

[72] Joan S. Birman, Volker Gebhardt, and Juan Gonzalez-Meneses. Conjugacy in garside groups i: Cyclings, powers, and rigidity. *Groups, Geometry, and Dynamics*, 1, 06 2006. 42

[73] Hervé Sibert. Tame garside monoids. *Journal of Algebra*, 281(2):487–501, 2004. (document), 83, 1.8
[74] Agata Smoktunowicz. On engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation. *Transactions of the American Mathematical Society*, 370(9):6535–6564, 2018. 137, 138, 139
[75] Agata Smoktunowicz and Alicja Smoktunowicz. Set-theoretic solutions of the Yang-Baxter equation and new classes of r-matrices. *Linear Algebra and its Applications*, 546:86–114, 2018. 142, 143, 146, 155
[76] Alexandre Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. 3.4
[77] Yaroslav P. Sysak. Products of groups and local nearrings. *Note di Matematica*, 28(suppl. 2):177–211, 2010. (document)
[78] John Tate and Michel Van den Bergh. Homological properties of sklyanin algebras. *Inventiones mathematicae*, 124(1):619–648, 1996. (document)
[79] Leandro Vendramin. Extensions of set-theoretic solutions of the Yang-Baxter equation and a conjecture of gateva-ivanova. *Journal of Pure and Applied Algebra*, 220(5):2064–2076, 2016. 3.4, 3.4
[80] AP Veselov. Yang-Baxter maps and integrable dynamics. *Physics Letters A*, 314(3):214–221, 2003. (document)
[81] Chen-Ning Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Physical Review Letters*, 19(23):1312, 1967. (document), 3.1