VNIVERSITAT DE VALÈNCIA

Programa de Doctorat en Matemàtiques

Left Braces and the Yang-Baxter Equation

Tesi doctoral presentada per
Neus Fuster i Corral

Dirigida per
Adolfo Ballester Bolinches
Ramon Esteban Romero

Febrer de 2021

Agraïments

Aquesta tesi és el resultat del treball realitzat aquests últims anys i només ha estat possible gràcies a moltes persones que m'heu fet costat i ajudat al llarg d'aquest viatge.

En primer lloc, vull agrair a el suport i l'acompanyament que he rebut en tot moment dels meus directors, Adolfo Ballester Bolinches i Ramon Esteban Romero, dels quals he après tantes coses al llarg d'aquests anys. Moltíssimes gràcies per la vostra dedicació i entrega i, sobretot, per la infinita paciència.

Gràcies a les persones de l'àrea d'àlgebra del Departament de Matemàtiques de la Universitat de València que, d'una manera o altra, us heu creuat al meu camí com a investigadora i m'heu fet créixer al vostre costat. I m'agradaria fer una menció especial a les companyes de la secretaria del departament que m'han ajudat cada vegada que tenia un problema administratiu, que no han sigut poques. També vull donar les gràcies a Raúl Sastriques i Hangyang Meng per totes les experiències i els moments de distensió que hem viscut com a companys de doctorat. D'altra banda, estic molt agraïda a la Universitat de València per concedir-me un contracte predoctoral dins del programa *Atracció de Talent* durant aquests anys, que a més de l'ajuda econòmica, m'ha permés aprendre i gaudir de la vessant docent.

També al meu pare, Robert Fuster, i a la meua mare, Cristina Corral, els quals m'han donat l'oportunitat de conéixer i estimar des de ben menuda aquest món exacte i màgic de les matemàtiques. I a la meua germana Laia, que suporta estoicament les nostres converses matemàtiques.

També vull donar les gràcies als meus companys de grau i bons amics Carolina Liern, Núria Molner i Àlex Fonollosa, que sempre m'han fet costat i m'han escoltat i comprés en els moments més difícils. I, per suposat, a Caridad Aguilar, Elena Gómez, Inés Gómez i Andrea Mascarell, amigues incondicionals des de menudes i que em recolzen, animen i aconsellen en tot moment. Finalment, no puc deixar d'agrair a Clara Martínez i Júlia Navarro, les meues companyes en el món coral i part fonamental de la meua família escollida, que han estat amb mi cada dia, m'han ajudat a seguir endavant i m'han donat la força per acabar aquest procés i aquesta investigació.

Resum

L'any 1967, en l'article [34] de Yang, va aparéixer l'equació quàntica de Yang-Baxter (o YBE, per les seues inicials en anglès) per primera vegada. Aquesta és una equació important en la física matemàtica que, a més, estableix la base d'algunes teories matemàtiques interessants, com ara, la teoria dels grups quàntics. Un dels problemes oberts fonamentals és trobar-ne totes les solucions.

En 1992, Drinfeld va plantejar en [17] la qüestió de trobar-ne totes les solucions conjuntistes: una solució conjuntista és un parell (X, r) on X és un conjunt no buit i $r\colon X \times X \to X \times X$ és una aplicació que satisfà que

$$r_{12} \circ r_{23} \circ r_{12} = r_{23} \circ r_{12} \circ r_{23},$$

on $r_{ij}\colon X \times X \times X \to X \times X \times X$ actua com r en les components (i, j) i com la identitat en l'altra component.

Una subclasse d'aquestes solucions, la de les solucions involutives i no degenerades, ha sigut molt estudiada en els últims anys, ja que aquest tipus de solucions no només és interessant per les aplicacions que té la YBE a la física, sinó també per la seua connexió amb altres teories matemàtiques, com per exemple els anells radicals (veieu [27]), els grups trifactoritzats (veieu [31]) o les àlgebres de Hopf (veieu [25]). D'ara endavant, ens referirem a les solucions conjuntistes, involutives i no degenerades de la YBE simplement com *solucions*, ja que aquestes seran les que estudiarem al llarg de la memòria.

En aquest context, Etingof, Schedler i Soloviev van introduir l'any 1999 en [19] dos grups fonamentals associats a una solució (X, r) donada: el grup d'estructura i el grup de permutacions, que van denotar per $G(X, r)$ i $\mathcal{G}(X, r)$, respectivament. Aquests dos grups resulten molt interessants perquè ens permeten estudiar les solucions utilitzant els mètodes de la teoria de grups.

D'altra banda, en 2007 Rump va introduir en [27] una nova estructura algebraica que serveix per a estudiar les solucions de la YBE: les brides (o braces) a esquerra, que consisteixen en una terna $(B, +, \cdot)$ on $(B, +)$ és un grup abelià, $(B, \cdot)$ és un grup i ambdues operacions estan relacionades

mitjançant l'equació

$$a \cdot (b + c) = a \cdot b - a + a \cdot c, \quad \text{per a qualssevol } a, b, c \in B.$$

En [14], Cedó, Jespers i Okniński van provar explícitament que cada brida a esquerra té associada una solució de l'equació de Yang-Baxter ([14, Lema 2]) i també que, donada una solució de la YBE, tant el seu grup d'estructura com el de permutacions tenen estructura de brides a esquerra. A més a més, cada solució finita (X, s) és isomorfa a una altra solució que està inclosa en la solució associada a la brida a esquerra que forma el seu grup d'estructura, $G(X, s)$ ([14, Teorema 1]). En conseqüència, podem concloure que el problema de construir totes les solucions finites de la YBE és equivalent a descriure totes les brides a esquerra finites, per la qual cosa, és clar que les brides a esquerra són una bona eina per a estudiar les solucions de l'equació de Yang-Baxter.

També cal destacar el concepte de grup involutiu de Yang-Baxter, més conegut com IYB-grup, definit en 2010 per Cedó, Jespers i del Río en [13]. Es diu que un grup G és un IYB-grup si és isomorf al grup multiplicatiu $(B, \cdot)$ d'una brida a esquerra $(B, +, \cdot)$.

Amb tot això, el nostre treball ha anat en tres direccions, que mostrarem en cadascun dels tres capítols que conté aquesta memòria, i que són, respectivament, l'estudi de les propietats de les brides a esquerra com a estructures algebraiques, la recerca dels grups que poden ser IYB-grups, i una nova interpretació dels grups de permutació i d'estructura mitjançant el graf de Cayley.

Després de llegir els articles [12] de Cedó, Gateva-Ivanova i Smoktunowicz i [6] de Bachiller, Cedó, Jespers i Okniński, vam decidir estudiar les brides a esquerra com a estructures independents (és a dir, sense relacionar-les amb les solucions de l'equació de Yang-Baxter, simplement treballant-hi des del punt de vista algebraic) perquè vam pensar que seria una bona forma de comprendre-les millor i, a llarg termini, poder classificar-les. Així, en el primer capítol hem recollit els resultats que hem obtingut en aquesta direcció, provant de buscar conceptes anàlegs als de la teoria de grups. En primer lloc, hem definit sèries principals i de composició per a brides a esquerra i hem provat un anàleg al teorema de Jordan-Hölder.

Definició 1.2.4. Donada una brida a esquerra B, una sèrie

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$$

on B_i és un ideal de B i B_{i+1}/B_i és un ideal minimal de B/B_i per a tot $i \in \{0, \ldots, n-1\}$ l'anomenem una *sèrie principal* i els factors B_{i+1}/B_i els anomenem *factors principals*.

Definició 1.2.6. Donada una brida a esquerra B, una sèrie

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$$

on B_i és un ideal de B_{i+1} i B_{i+1}/B_i és simple per a tot $i \in \{0, \ldots, n-1\}$ l'anomenem una *sèrie de composició* i els factors B_{i+1}/B_i els anomenem *factors de composició.*

Teorema 1.2.13.(Jordan-Hölder per a brides). *Dues sèries principals (o de composició) d'una brida a esquerra B són equivalents.*

D'altra banda, basant-nos en la definició de brides a esquerra resolubles presentada en [6], hem definit el concepte de brida a esquerra superresoluble.

Definició 1.2.14.([6, Definició 2.2]) Una brida a esquerra B és *resoluble* si té una sèrie

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

amb B_i ideal de B_{i+1} per a tot $i \in \{0, \ldots, m-1\}$ i tal que tots els seus factors són brides trivials.

Definició 1.2.18. Diem que una brida a esquerra $(B, +, \cdot)$ és *superresoluble* si té una sèrie d'ideals

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

tal que B_i és un ideal de B i $|B_{i+1}/B_i|$ és un nombre primer per a cada $i \in \{0, 1, \ldots, m-1\}$.

En [12], Cedó, Gateva-Ivanova i Smoktunowicz defineixen les brides a esquerra nilpotents per la dreta i nilpotents per l'esquerra. Nosaltres hem trobat una caracterització de les primeres i un resultat que les relaciona amb les brides superresolubles.

Definició 1.2.20.([12]) Direm que una brida a esquerra B és *nilpotent per l'esquerra* si existeix un enter positiu n tal que $B^n = 0$. Una brida a esquerra B és *nilpotent per la dreta* si existeix un enter positiu tal que $B^{(n)} = 0$.[1]

[1] B^n i $B^{(n)}$ fan referència a les cadenes que presenta Rump en [27].

Proposició 1.2.21. *Una brida a esquerra B és nilpotent per la dreta si, i només si, té una sèrie $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$ tal que B_i és un ideal de B i $B_i/B_{i-1} \subseteq \mathrm{Soc}(B/B_{i-1})$ per a cada $i \in \{1, \ldots, n\}$.*

Proposició 1.2.23. *Si $(B, +, \cdot)$ és una brida a esquerra que és nilpotent per l'esquerra i per la dreta, llavors B és superresoluble.*

També hem vist que l'ideal derivat d'una brida a esquerra superresoluble no és necessàriament nilpotent per l'esquerra i proposem la qüestió següent:

Qüestió 1.2.26. Si B és una brida a esquerra superresoluble, el seu ideal derivat B^2 és nilpotent per la dreta?

Finalment, a la darrera secció d'aquest capítol hem recordat resultats de [19], [30] i [23] que tracten sobre algunes propietats de les brides a esquerra que es poden deduir a partir de propietats del seu grup multiplicatiu subjacent (o al contrari) i, en aquest sentit, hem obtingut el resultat següent:

Proposició 1.3.10. *Si $(B, +, \cdot)$ és una brida a esquerra finita i el seu grup multiplicatiu $(B, \cdot)$ té una torre de Sylow, llavors B és una brida a esquerra resoluble.*

En el capítol 2, ens hem fixat en els IYB-grups. Recordem que un grup G és un IYB-grup si és isomorf al grup multiplicatiu d'una brida a esquerra (veieu [13]). Dels resultats de Etingof, Schedler i Soloviev en [19], sabem que tots els IYB-grups són grups resolubles. Per la seua banda, Cedó, Jespers i del Río es preguntaren en [13] si l'afirmació contrària també era certa, és a dir, si tot grup resoluble podia ser un IYB-grup. Arran d'això, van aparéixer nous resultat provant que determinades subclasses de grups resolubles, com ara els grups abelians, els nilpotents de classe dos, o de classe tres i ordre senar, o els grups A-resolubles, són IYB-grups (veieu [13], [15] i [18]). Però, finalment, Bachiller va mostrar un contraexemple en [2].

Malgrat tot, per [13, Corol·lari 3.1], se sap que tot IYB-grup és un producte de dos IYB-grups, fet que inspira una altra qüestió interessant: *sota quines condicions podem assegurar que un grup G és un IYB-grup, si $G = NH$ es pot factoritzar com a producte de dos IYB-grups N i H, amb N normal en G?* En aquesta tesi, mostrem un nou teorema en aquesta direcció que millora els resultats que Cedó, Jespers i del Río ([13, Teorema 3.3]) i Eisele ([18, Proposició 2.2]) havien trobat en aquest sentit.

Teorema 2.2.20. *Suposem que el grup A actua sobre el grup $G = NH$, on N i H són subgrups A-invariants de G i $N \trianglelefteq G$. Suposem que N i H són IYB-grups amb IYB-estructures A-equivariants (U, π_N) i (V, π_H), respectivament, que satisfan les condicions següents:*

(C1) $N \cap H \subseteq \mathrm{Ker}(\mathrm{Z}(N) \operatorname{on} U) \cap \mathrm{Ker}(H \operatorname{on} V)$.

(C2) (U, π_N) *també és IYB-estructura H-equivariant sobre N respecte a l'acció per conjugació de H sobre N: ${}^h n = hnh^{-1}$ per a $n \in N$, $h \in H$.*

Llavors G té una IYB-estructura A-equivariant (W, π) tal que

$$\mathrm{Ker}(N \operatorname{on} U)\, \mathrm{C}_{\mathrm{Ker}(H \operatorname{on} V)}(N) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

A més, hem obtingut noves famílies de IYB-grups gràcies a alguns corol·laris d'aquest teorema i hem donat un exemple d'una família concreta d'IYB-grups que verifica les hipòtesis del nostre teorema però que no pot aparéixer com a conseqüència dels resultats de [13] o [18]. Els resultats originals del capítol 2 han estat publicats a [24].

Corol·lari 2.2.21. *Siga un grup A que actua sobre un grup $G = N \times H$ que és el producte directe de dos subgrups A-invariants N i H. Suposem que N i H són IYB-grups amb IYB-estructures A-equivariants (U, π_N) i (V, π_H), respectivament. Llavors G té una IYB-estructura A-equivariant (W, π_G) tal que*

$$\mathrm{Ker}(N \operatorname{on} U)\, \mathrm{Ker}(H \operatorname{on} V) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

Corol·lari 2.2.22. *Siga G un grup nilpotent de classe dos amb un 2-subgrup de Sylow abelià. Aleshores G té una IYB-estructura totalment equivariant (W, π_G) tal que $\mathrm{Z}(G) \subseteq \mathrm{Ker}(G \operatorname{on} W)$.*

Corol·lari 2.2.23. *Siga $G = NH$ un grup tal que N és un subgrup normal nilpotent de classe dos i H és un IYB-grup amb IYB-estructura (V, π). Suposem que se satisfan les condicions següents:*

1. *$N \cap H \subseteq \mathrm{Z}(N)$;*
2. *$[H, \mathrm{O}_2(N)] \subseteq \mathrm{Z}(N)$;*
3. *$H \cap N$ actua trivialment sobre V.*

Aleshores G és un IYB-grup.

Corol·lari 2.2.24. *Siga $G = NH$ un grup tal que N i H són dos subgrups nilpotents de classe dos i N és normal en G. Si $N \cap H \subseteq \mathrm{Z}(G)$ i $[H, \mathrm{O}_2(N)] \subseteq \mathrm{Z}(N)$, llavors G és un IYB-grup.*

Corol·lari 2.2.25. *Siga un grup $G = N_1 N_2 \cdots N_s$, producte de s subgrups $N_1, \ldots, N_s$ que satisfan*

1. *N_i és un grup nilpotent de classe dos amb un 2-subgrup de Sylow abelià, per a tot $i = 1, \ldots, s$;*
2. *N_i és normalitzat per N_j, per a tot $1 \leq i < j \leq s$;*
3. *$N_1 \cdots N_i \cap N_{i+1} = \mathrm{Z}(G)$, per a tot $i = 1, \ldots, s-1$.*

Llavors G és un IYB-grup.

Exemple 2.2.26. *Siga $p \geq 3$ un nombre primer, siga $m \geq 2$ un nombre natural i siga G el grup amb la presentació següent*

$$G = \langle a, b, c \mid a^{p^m} = b^{p^m} = 1,\ c^{p^m} = a^{p^{m-1}},\ a^b = a^{1+p^{m-1}},\\ a^c = aa^{-p}b^{-p},\ b^c = ba \rangle.$$

Aleshores, es pot emprar el corol·lari 2.2.24 per provar que G és un IYB-grup. Ara bé, el fet que G és un IYB-grup no es pot obtenir a partir dels resultats de [18] ni de [15].

Per últim, com hem comentat a l'inici, en [14], els autors van provar que donada una solució (X, r) de la YBE, tant el grup d'estructura, $G(X, r)$, com el de permutacions, $\mathcal{G}(X, r)$, tenen una estructura natural de brida a esquerra. Sabent açò, en el capítol 3 hem fet una descripció d'aquesta estructura des d'una perspectiva nova: utilitzant el graf de Cayley. Els resultats d'aquest capítol es poden trobar a [8].

El primer pas ha sigut definir una suma sobre el grup de permutacions $\mathcal{G}(X, r)$. Concretament, hem fet el següent: donats $\alpha \in \mathcal{G}(X, r)$ i un generador f_x, escrivim

$$\alpha + f_x = \alpha f_{\alpha^{-1}(x)},$$
$$\alpha + (-f_x) = \alpha f^{-1}_{g^{-1}_{\alpha^{-1}(x)}(\alpha^{-1}(x))}.$$

Tot seguit, amb l'ajuda d'una sèrie de lemes tècnics, hem pogut estendre aquesta suma a tots els elements de $\mathcal{G}(X, r)$ i demostrar que el grup de permutacions $\mathcal{G}(X, r)$ amb aquesta addició i la composició habitual d'aplicacions té estructura de brida a esquerra.

Teorema 3.1.4. *Considerem dos elements $\alpha, \beta \in \mathcal{G}(X,r)$, que es poden veure com*

$$\alpha = (\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m} \in \mathcal{G}(X,r),$$
$$\beta = (\cdots(\eta_1 f_{y_1} + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s} \in \mathcal{G}(X,r),$$

amb $\varepsilon_i \in \{-1,1\}$, $x_i \in X$, $1 \leq i \leq m$; $\eta_j \in \{-1,1\}$, $y_j \in X$, $1 \leq j \leq s$. L'assignació

$$\alpha + \beta = (\cdots((((\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m}) + \eta_1 f_{y_1}) + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s},$$

$\alpha + 1 = 1 + \alpha = \alpha$, $1 + 1 = 1$, defineix una operació binària interna sobre $\mathcal{G}(X,r)$ de manera que $(\mathcal{G}(X,r), +, \circ)$ és una brida a esquerra.

També hem vist que podem obtindre el graf de Cayley de $(\mathcal{G}(X,r),+)$ a partir del graf de Cayley de $(\mathcal{G}(X,r),\circ)$, i també al contrari, simplement canviant-ne les etiquetes dels arcs.

Teorema 3.1.5. *Considereu el graf de Cayley de $(\mathcal{G}(X,r),\circ)$ i recordeu que els seus arcs són de la forma $\alpha \xrightarrow{x} \alpha f_x$, $x \in X$, $\alpha \in \mathcal{G}(X,r)$. Si canviem les etiquetes de cadascuna d'aquests arcs per $\alpha(x)$, obtenint arcs de la forma $\alpha \xrightarrow{\alpha(x)} \alpha f_x$, aleshores el graf etiquetat obtingut d'aquesta manera és el graf de Cayley del grup abelià $(\mathcal{G}(X,r),+)$, on $+$ denota l'operació definida prèviament.*

El següent pas ha estat obtindre una descripció del grup d'estructura $G(X,r)$ utilitzant el graf de Cayley del grup additiu del grup de permutacions, $(\mathcal{G}(X,r),+)$. Ho hem aconseguit amb una construcció anàloga a la presentada en [7] per Ballester Bolinches, Cosme Llópez i Esteban Romero.

Hem considerat el graf de Cayley de $(\mathcal{G}(X,r),+)$ i hem denotat per E el conjunt dels seus arcs. El grup multiplicatiu del grup de permutacions, $(\mathcal{G}(X,r),\circ)$, actua per l'esquerra sobre E de la següent forma: si $\gamma \in \mathcal{G}(X,r)$ i $(\alpha \xrightarrow{\alpha(x)} \alpha f_x) \in E$, llavors

$$\gamma * \left(\alpha \xrightarrow{\alpha(x)} \alpha f_x\right) = \left(\gamma\alpha \xrightarrow{\gamma\alpha(x)} \gamma\alpha f_x\right) \in E.$$

Seguidament hem estés aquesta acció a W, el $\mathbb{Z}$-mòdul abelià amb base E, i hem construït el producte semidirecte $[W]\mathcal{G}(X,r)$.

A continuació hem identificat tots els arcs de $(\mathcal{G}(X,r),+)$ que tingueren la mateixa etiqueta prenent quocients mòdul

$$K = \langle e_{\alpha,y} - e_{\beta,y} \mid y \in X,\ \alpha,\beta \in \mathcal{G}(X,r)\rangle\,,$$

on $e_{\alpha,y}$ denota l'arc que comença en α i té etiqueta y, això és, $\alpha \xrightarrow{y} \alpha f_{\alpha^{-1}(y)}$.

Després d'això, hem considerat el grup quocient

$$[W]\mathcal{G}(X,r)/K \cong [W/K]\mathcal{G}(X,r)$$

i hem pres el subgrup

$$H = \langle (e_{1,x} + K, f_x) \mid x \in X \rangle \leq [W/K]\mathcal{G}(X,r).$$

Finalment, hem simplificat la notació del grup H i hem provat que aquest és isomorf al grup d'estructura $G(X,r)$.

Teorema 3.2.3. *Siga $H = \langle (\bar{x}, f_x) \mid x \in X \rangle \leq \left[\mathbb{Z}^X\right] \mathcal{G}(X,r)$ el subgrup que acabem de construir. Aleshores H és isomorf al grup d'estructura $G(X,r)$.*

També hem estudiat l'aspecte dels elements de H i hem definit una suma sobre H per provar que $(H,+,\cdot)$ és una brida a esquerra.

Teorema 3.2.4. *Siga H com en el Teorema 3.2.3, llavors:*

1. $H = \left\{ \left(\sum_{x\in X} a_x \bar{x}, \sum_{x\in X} a_x f_x \right) \,\middle|\, a_x \in \mathbb{Z}, x \in X \right\}$.
2. *El producte de H té la forma*

$$\left(\sum_{x\in X} a_x \bar{x}, \alpha \right) \cdot \left(\sum_{x\in X} b_x \bar{x}, \beta \right) = \left(\sum_{x\in X} \left(a_x + b_{\alpha^{-1}(x)} \right) \bar{x}, \alpha\beta \right),$$

on $\alpha = \sum_{x\in X} a_x f_x$, $\beta = \sum_{x\in X} b_x f_x$.

Teorema 3.2.5. *Siga (X,r) una solució de la YBE i siga H com en el Teorema 3.2.3. Si definim en H una operació $+$ com*

$$\left(\sum_{x\in X} a_x \bar{x}, \alpha \right) + \left(\sum_{x\in X} b_x \bar{x}, \beta \right) = \left(\sum_{x\in X} (a_x + b_x) \bar{x}, \alpha + \beta \right),$$

on $\alpha = \sum_{x\in X} a_x f_x$, $\beta = \sum_{x\in X} b_x f_x$, aleshores $(H,+,\cdot)$ és una brida a esquerra i l'aplicació $\pi \colon H \longrightarrow \mathcal{G}(X,r)$ donada per $\pi\left(\sum_{x\in X} a_x \bar{x}, \alpha \right) = \alpha$ és un homomorfisme de brides a esquerra.

Les següents dues seccions les hem dedicades, respectivament, a donar una interpretació geomètrica d'aquesta visió amb grafs i a comparar les addicions que hem emprat amb altres ja existents. Finalment, a l'última secció hem presentat alguns resultats que es dedueixen fàcilment com aplicacions de la

perspectiva que empra el graf de Cayley. Hem començat amb una forma de trobar els parells congelats, un concepte introduït per Chouraqui i Godelle en [16].

Definició 3.5.1. Siga (X, r) una solució de la YBE. Si considerem l'acció natural de r sobre $X \times X$, els punts fixos d'aquesta acció s'anomenen *parells congelats*.

Proposició 3.5.2. *Siga $x \in X$. Considerem en el graf de Cayley del grup additiu de $\mathcal{G}(X, r)$ el camí de longitud dos que comença en 1 amb els dos arcs etiquetats com x i considerem els arcs corresponents en el graf de Cayley del grup multiplicatiu de $\mathcal{G}(X, r)$, amb etiquetes x, y, respectivament. Llavors $r(x, y) = (x, y)$. A més a més, (x, y) és l'únic parell de la forma (x, z) amb $z \in X$ tal que $r(x, z) = (x, z)$.*

A continuació hem mostrat que les relacions explícitament mencionades en la definició del grup d'estructura i les trivials de la forma $xy = xy$, són les úniques relacions formades per igualtats de productes de dos generadors que es poden trobar en aquest grup.

Teorema 3.5.4. *Siguen $x, y, z, t \in X$ vistos com elements del grup d'estructura $G(X, r)$. Aleshores $xy = zt$ si, i només si, $x = z$ i $y = t$ o $r(x, y) = (z, t)$.*

També hem trobat una forma més senzilla de provar que la retracció d'una solució de la YBE és de nou una solució, resultat que ja apareixia en els articles [19] i [14], però era difícil de comprovar, i hem descrit una manera d'obtenir el graf de Cayley del grup de permutacions associat a la retracció d'una solució de la YBE.

La nostra darrera aplicació és una caracterització de quan un grup de permutacions d'una solució de la YBE és una brida trivial.

Proposició 3.5.11. *Les afirmacions següents a prop d'una solució de la YBE són equivalents.*

1. *El grup de permutacions $\mathcal{G}(X, r)$ és una brida trivial.*
2. *Per a cada x, $y \in X$, si existeix $\alpha \in \mathcal{G}(X, r)$ tal que $\alpha(x) = y$, llavors $f_x = f_y$ (és a dir, x i y estan relacionats per la relació de retracció).*

Resumen

El año 1967, en el artículo [34] de Yang, apareció la ecuación cuántica de Yang-Baxter (o YBE, por sus iniciales en inglés) por primera vez. Esta es una ecuación importante en la física matemática que, además, establece la base de algunas teorías matemáticas interesantes, como por ejemplo, la teoría de los grupos cuánticos. Uno de los problemas abiertos fundamentales es encontrar todas las soluciones.

En 1992, Drinfeld planteó en [17] la cuestión de encontrar todas las soluciones conjuntistas: una solución conjuntista es un par (X, r) donde X es un conjunto no vacío y $r\colon X \times X \to X \times X$ es una aplicación que satisface que

$$r_{12} \circ r_{23} \circ r_{12} = r_{23} \circ r_{12} \circ r_{23},$$

donde $r_{ij}\colon X \times X \times X \to X \times X \times X$ actúa como r en las componentes (i, j) y como la identidad en la otra componente.

Una subclase de estas soluciones, la de las soluciones involutivas y no degeneradas, ha sido muy estudiada en los últimos años, puesto que este tipo de soluciones no solo es interesante por las aplicaciones que tiene la YBE a la física, sino también por su conexión con otras teorías matemáticas, como por ejemplo los anillos radicales (véase [27]), los grupos trifactorizados (véase [31]) o las álgebras de Hopf (véase [25]). De ahora en adelante, nos referiremos a las soluciones conjuntistas, involutivas y no degeneradas de la YBE simplemente como *soluciones*, puesto que estas serán las que estudiaremos a lo largo de la memoria.

En este contexto, Etingof, Schedler y Soloviev introdujeron en 1999 en [19] dos grupos fundamentales asociados a una solución (X, r) dada: el grupo de estructura y el grupo de permutaciones, que denotaron por $G(X, r)$ y $\mathcal{G}(X, r)$, respectivamente. Estos dos grupos resultan muy interesantes porque nos permiten estudiar las soluciones utilizando los métodos de la teoría de grupos.

Por otro lado, en 2007 Rump introdujo en [27] una nueva estructura algebraica que sirve para estudiar las soluciones de la YBE: las brazas a izquierda, que consisten en una terna $(B, +, \cdot)$ donde $(B, +)$ es un grupo

abeliano, $(B, \cdot)$ es un grupo y ambas operaciones están relacionadas mediante la ecuación

$$a \cdot (b + c) = a \cdot b - a + a \cdot c, \quad \text{para cualesquiera } a, b, c \in B.$$

En [14], Cedó, Jespers y Okniński probaron explícitamente que cada braza a izquierda tiene asociada una solución de la ecuación de Yang-Baxter ([14, Lema 2]) y también que, dada una solución de la YBE, tanto su grupo de estructura como el de permutaciones tienen estructura de brazas a izquierda. Además, cada solución finita (X, s) es isomorfa a otra solución que está incluida en la solución asociada a la braza a izquierda que forma su grupo de estructura, $G(X, s)$ ([14, Teorema 1]). En consecuencia, podemos concluir que el problema de construir todas las soluciones finitas de la YBE es equivalente a describir todas las brazas a izquierda finitas, por lo cual, está claro que las brazas a izquierda son una buena herramienta para estudiar las soluciones de la ecuación de Yang-Baxter.

También hay que destacar el concepto de grupo involutivo de Yang-Baxter, más conocido como IYB-grupo, definido en 2010 por Cedó, Jespers y del Río en [13]. Se dice que un grupo G es uno IYB-grupo si es isomorfo al grupo multiplicativo $(B, \cdot)$ de una braza a izquierda $(B, +, \cdot)$.

Con todo esto, nuestro trabajo ha ido en tres direcciones, que mostraremos en cada uno de los tres capítulos que contiene esta memoria, y que son, respectivamente, el estudio de las propiedades de las brazas a izquierda como estructuras algebraicas, la investigación de los grupos que pueden ser IYB-grupos, y una nueva interpretación de los grupos de permutación y de estructura mediante el grafo de Cayley.

Después de leer los artículos [12] de Cedó, Gateva-Ivanova y Smoktunowicz y de Bachiller, [6] Cedó, Jespers y Okniński, decidimos estudiar las brazas a izquierda como estructuras independientes (es decir, sin relacionarlas con las soluciones de la ecuación de Yang-Baxter, simplemente trabajando desde el punto de vista algebraico) porque pensamos que sería una buena forma de comprenderlas mejor y, a largo plazo, poder clasificarlas. Así, en el primer capítulo hemos recogido los resultados que hemos obtenido en esta dirección, tratando de buscar conceptos análogos a los de la teoría de grupos. En primer lugar, hemos definido series principales y de composición para brazas a izquierda y hemos probado un análogo al teorema de Jordan-Hölder.

Definición 1.2.4. Dada una braza a izquierda B, una serie

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$$

donde B_i es un ideal de B y B_{i+1}/B_i es un ideal minimal de B/B_i, para todo $i \in \{0, \ldots, n-1\}$ se denomina una *serie principal* y los factores B_{i+1}/B_i se denominan *factores principales*.

Definición 1.2.6. Dada una braza a izquierda B, una serie

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$$

donde B_i es un ideal de B_{i+1} y B_{i+1}/B_i es simple para todo $i \in \{0, \ldots, n-1\}$ se denomina una *serie de composición* y los factores B_{i+1}/B_i se denominan *factores de composición*.

Teorema 1.2.13.(Jordan-Hölder para brazas). *Dos series principales (o de composición) de una braza a izquierda B son equivalentes.*

Por otro lado, basándonos en la definición de brazas a izquierda resolubles presentada en [6], hemos definido el concepto de braza a izquierda superresoluble.

Definición 1.2.14.([6, Definición 2.2]) Una braza a izquierda B es *resoluble* si tiene una serie

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

con B_i ideal de B_{i+1} para todo $i \in \{0, \ldots, m-1\}$ y tal que todos sus factores son brazas triviales.

Definición 1.2.18. Decimos que una braza a izquierda $(B, +, \cdot)$ es *superresoluble* si tiene una serie de ideales

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

tal que B_i es un ideal de B y $|B_{i+1}/B_i|$ es un número primo para cada $i \in \{0, 1, \ldots, m-1\}$.

En [12], Cedó, Gateva-Ivanova y Smoktunowicz definen las brazas a izquierda nilpotentes por la derecha y nilpotentes por la izquierda. Nosotros hemos encontrado una caracterización de las primeras y un resultado que las relaciona con las brazas superresolubles.

Definición 1.2.20.([12]) Diremos que una braza a izquierda B es *nilpotente por la izquierda* si existe un entero positivo n tal que $B^n = 0$. Una braza a izquierda B es *nilpotente por la derecha* si existe un entero positivo tal que $B^{(n)} = 0$.[2]

[2] B^n y $B^{(n)}$ hacen referencia a las cadenas que presenta Rump en [27].

Proposición 1.2.21. *Una braza a izquierda B es nilpotente por la derecha si, y solo si, tiene una serie $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$ tal que B_i es un ideal de B y $B_i/B_{i-1} \subseteq \mathrm{Soc}(B/B_{i-1})$ para cada $i \in \{1, \ldots, n\}$.*

Proposición 1.2.23. *Si $(B, +, \cdot)$ es una braza a izquierda que es nilpotente por la izquierda y por la derecha, entonces B es superresoluble.*

También hemos visto que el ideal derivado de una braza a izquierda superresoluble no es necesariamente nilpotente por la izquierda y proponemos la cuestión siguiente:

Cuestión 1.2.26. Si B es una braza a izquierda superresoluble, ¿su ideal derivado B^2 es nilpotente por la derecha?

Finalmente, en la última sección de este capítulo hemos recordado resultados de [19], [30] y [23] que tratan sobre algunas propiedades de las brazas a izquierda que se pueden deducir a partir de propiedades de su grupo multiplicativo subyacente (o al contrario) y, en este sentido, hemos obtenido el resultado siguiente:

Proposición 1.3.10. *Si $(B, +, \cdot)$ es una braza a izquierda finita y su grupo multiplicativo $(B, \cdot)$ tiene una torre de Sylow, entonces B es una braza a izquierda resoluble.*

En el capítulo 2, nos hemos fijado en los IYB-grupos. Recordamos que un grupo G es uno IYB-grupo si es isomorfo al grupo multiplicativo de una braza a izquierda (véase [13]). De los resultados de Etingof, Schedler y Soloviev en [19], sabemos que todos los IYB-grupos son grupos resolubles. Por su parte, Cedó, Jespers y del Río se preguntaron en [13] si la afirmación contraria también era cierta, es decir, si todo grupo resoluble podía ser un IYB-grupo. A raíz de esto, aparecieron nuevos resultado probando que determinadas subclases de grupos resolubles, como por ejemplo los grupos abelianos, los nilpotentes de clase dos, o de clase tres y orden impar, o los grupos A-resolubles, son IYB-grupos (véase [13], [15] y [18]). Pero, finalmente, Bachiller mostró un contraejemplo en [2].

A pesar de todo, por [13, Corolario 3.1], se sabe que todo IYB-grupo es un producto de dos IYB-grupos, hecho que inspira otra cuestión interesante: *¿bajo qué condiciones podemos asegurar que un grupo G es un IYB-grupo, si $G = NH$ se puede factoritzar como producto de dos IYB-grupos N y H, con N normal en G?* En esta tesis, mostramos un nuevo teorema en esta dirección

que mejora los resultados que Cedó, Jespers y del Río ([13, Teorema 3.3]) y Eisele ([18, Proposición 2.2]) habían encontrado en este sentido.

Teorema 2.2.20. *Supongamos que el grupo A actúa sobre el grupo $G = NH$, donde N y H son subgrupos A-invariantes de G y $N \trianglelefteq G$. Supongamos que N y H son IYB-grupos con IYB-estructuras A-equivariantes (U, π_N) y (V, π_H), respectivamente, que satisfacen las condiciones siguientes:*

(C1) $N \cap H \subseteq \mathrm{Ker}(\mathrm{Z}(N) \operatorname{on} U) \cap \mathrm{Ker}(H \operatorname{on} V)$.

(C2) *(U, π_N) también es IYB-estructura H-equivariante sobre N respecto a la acción por conjugación de H sobre N: ${}^h n = hnh^{-1}$ para $n \in N$, $h \in H$.*

Entonces G tiene una IYB-estructura A-equivariante (W, π) tal que

$$\mathrm{Ker}(N \operatorname{on} U)\, \mathrm{C}_{\mathrm{Ker}(H \operatorname{on} V)}(N) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

Además, hemos obtenido nuevas familias de IYB-grupos gracias a algunos corolarios de este teorema y hemos dado un ejemplo de una familia concreta de IYB-grupos que verifica las hipótesis de nuestro teorema pero que no puede aparecer como consecuencia de los resultados de [13] o [18]. Los resultados originales del capítulo 2 han sido publicados en [24].

Corolario 2.2.21. *Sea A un grupo que actúa sobre un grupo $G = N \times H$ que es el producto directo de dos subgrupos A-invariantes N y H. Supongamos que N y H son IYB-grupos con IYB-estructuras A-equivariantes (U, π_N) y (V, π_H), respectivamente. En ese caso, G tiene una IYB-estructura A-equivariante (W, π_G) tal que*

$$\mathrm{Ker}(N \operatorname{on} U)\, \mathrm{Ker}(H \operatorname{on} V) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

Corolario 2.2.22. *Sea G un grupo nilpotente de clase dos con un 2-subgrupo de Sylow abeliano. Entonces G tiene una IYB-estructura totalmente equivariante (W, π_G) tal que $\mathrm{Z}(G) \subseteq \mathrm{Ker}(G \operatorname{on} W)$.*

Corolario 2.2.23. *Sea $G = NH$ un grupo tal que N es un subgrupo normal nilpotente de clase dos y H es un IYB-grupo con IYB-estructura (V, π). Supongamos que se satisfacen las condiciones siguientes:*

1. *$N \cap H \subseteq \mathrm{Z}(N)$;*
2. *$[H, \mathrm{O}_2(N)] \subseteq \mathrm{Z}(N)$;*

3. $H \cap N$ *actúa trivialmente sobre* V.

Entonces G *es un IYB-grupo.*

Corolario 2.2.24. *Sea* $G = NH$ *un grupo tal que* N *y* H *son dos subgrupos nilpotentes de clase dos y* N *es normal en* G. *Si* $N \cap H \subseteq \mathrm{Z}(G)$ *y* $[H, \mathrm{O}_2(N)] \subseteq \mathrm{Z}(N)$, *entonces* G *es un IYB-grupo.*

Corolario 2.2.25. *Sea un grupo* $G = N_1 N_2 \cdots N_s$, *producto de* s *subgrupos* $N_1, \ldots, N_s$ *que satisfacen*

1. N_i *es un grupo nilpotente de clase dos con un* 2*-subgrupo de Sylow abeliano, para todo* $i = 1, \ldots, s$;
2. N_i *es normalizado por* N_j, *para todo* $1 \leq i < j \leq s$;
3. $N_1 \cdots N_i \cap N_{i+1} = \mathrm{Z}(G)$, *para todo* $i = 1, \ldots, s-1$.

Entonces G *es un IYB-grupo.*

Ejemplo 2.2.26. *Sea* $p \geq 3$ *un número primo, sea* $m \geq 2$ *un número natural y sea* G *el grupo con la presentación siguiente*

$$G = \langle a, b, c \mid a^{p^m} = b^{p^m} = 1,\ c^{p^m} = a^{p^{m-1}},\ a^b = a^{1+p^{m-1}}, \tag{1}$$

$$a^c = aa^{-p}b^{-p},\ b^c = ba \rangle. \tag{2}$$

Entonces, se puede emplear el corolario 2.2.24 para probar que G *es un IYB-grupo. Ahora bien, el hecho de que* G *es un IYB-grupo no se puede obtener a partir de los resultados de [18] ni de [15].*

Por último, como hemos comentado al inicio, en [14], los autores probaron que dada una solución (X, r) de la YBE, tanto el grupo de estructura, $G(X, r)$, como el de permutaciones, $\mathcal{G}(X, r)$, tienen una estructura natural de braza a izquierda. Sabiendo esto, en el capítulo 3 hemos hecho una descripción de esta estructura desde una perspectiva nueva: utilizando el grafo de Cayley. Los resultados de este capítulo se pueden encontrar en [8].

El primer paso ha sido definir una suma sobre el grupo de permutaciones $\mathcal{G}(X, r)$. Concretamente, hemos hecho lo siguiente: dados $\alpha \in \mathcal{G}(X, r)$ y un generador f_x, escribimos

$$\alpha + f_x = \alpha f_{\alpha^{-1}(x)}, \tag{3}$$

$$\alpha + (-f_x) = \alpha f^{-1}_{g^{-1}_{\alpha^{-1}(x)}(\alpha^{-1}(x))}. \tag{4}$$

A continuación, con la ayuda de una serie de lemas técnicos, hemos podido extender esta suma a todos los elementos de $\mathcal{G}(X,r)$ y demostrar que el grupo de permutaciones $\mathcal{G}(X,r)$ con esta adición y la composición habitual de aplicaciones tiene estructura de braza a izquierda.

Teorema 3.1.4. *Consideremos dos elementos $\alpha, \beta \in \mathcal{G}(X,r)$, que se pueden ver como*

$$\alpha = (\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m} \in \mathcal{G}(X,r), \tag{5}$$
$$\beta = (\cdots(\eta_1 f_{y_1} + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s} \in \mathcal{G}(X,r), \tag{6}$$

con $\varepsilon_i \in \{-1,1\}$, $x_i \in X$, $1 \leq i \leq m$; $\eta_j \in \{-1,1\}$, $y_j \in X$, $1 \leq j \leq s$. La asignación

$$\alpha + \beta = (\cdots((((\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m}) \tag{7}$$
$$+ \eta_1 f_{y_1}) + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s}, \tag{8}$$

$\alpha + 1 = 1 + \alpha = \alpha$, $1 + 1 = 1$, define una operación binaria interna sobre $\mathcal{G}(X,r)$ de forma que $(\mathcal{G}(X,r), +, \circ)$ es una braza a izquierda.

También hemos visto cómo obtener el grafo de Cayley de $(\mathcal{G}(X,r), +)$ a partir del grafo de Cayley de $(\mathcal{G}(X,r), \circ)$, y también al contrario, simplemente cambiando las etiquetas de los arcos.

Teorema 3.1.5. *Consideremos el grafo de Cayley de $(\mathcal{G}(X,r), \circ)$ y recordemos que sus arcos son de la forma $\alpha \xrightarrow{x} \alpha f_x$, $x \in X$, $\alpha \in \mathcal{G}(X,r)$. Si cambiamos las etiquetas de cada uno de estos arcos por $\alpha(x)$, obteniendo arcos de la forma $\alpha \xrightarrow{\alpha(x)} \alpha f_x$, entonces el grafo etiquetado obtenido de este modo es el grafo de Cayley del grupo abeliano $(\mathcal{G}(X,r), +)$, donde $+$ denota la operación definida previamente.*

El siguiente paso ha sido obtener una descripción del grupo de estructura $G(X,r)$ utilizando el grafo de Cayley del grupo aditivo del grupo de permutaciones, $(\mathcal{G}(X,r), +)$. Lo hemos conseguido con una construcción análoga a la presentada en [7] por Ballester Bolinches, Cosme Llópez y Esteban Romero.

Hemos considerado el grafo de Cayley de $(\mathcal{G}(X,r), +)$ y hemos denotado por E el conjunto de sus arcos. El grupo multiplicativo del grupo de permutaciones, $(\mathcal{G}(X,r), \circ)$, actúa por la izquierda sobre E de la siguiente forma: si $\gamma \in \mathcal{G}(X,r)$ y $(\alpha \xrightarrow{\alpha(x)} \alpha f_x) \in E$, entonces

$$\gamma * \left(\alpha \xrightarrow{\alpha(x)} \alpha f_x\right) = \left(\gamma\alpha \xrightarrow{\gamma\alpha(x)} \gamma\alpha f_x\right) \in E.$$

Seguidamente hemos extendido esta acción a W, el $\mathbb{Z}$-módulo abeliano con base E, y hemos construido el producto semidirecto $[W]\mathcal{G}(X,r)$.

A continuación hemos identificado todos los arcos de $(\mathcal{G}(X,r),+)$ que tuvieran la misma etiqueta tomando cocientes módulo

$$K = \langle e_{\alpha,y} - e_{\beta,y} \mid y \in X,\ \alpha,\beta \in \mathcal{G}(X,r)\rangle\,,$$

donde $e_{\alpha,y}$ denota el arco que empieza en α y tiene etiqueta y, esto es, $\alpha \xrightarrow{y} \alpha f_{\alpha^{-1}(y)}$.

Después de esto, hemos considerado el grupo cociente

$$[W]\mathcal{G}(X,r)/K \cong [W/K]\mathcal{G}(X,r)$$

y hemos tomado el subgrupo

$$H = \langle (e_{1,x} + K, f_x) \mid x \in X\rangle \leq [W/K]\mathcal{G}(X,r).$$

Finalmente, hemos simplificado la notación del grupo H y hemos probado que este es isomorfo al grupo de estructura $G(X,r)$.

Teorema 3.2.3. *Sea $H = \langle (\bar{x}, f_x) \mid x \in X\rangle \leq \left[\mathbb{Z}^X\right]\mathcal{G}(X,r)$ el subgrupo que acabamos de construir. Entonces H es isomorfo al grupo de estructura $G(X,r)$.*

También hemos estudiado el aspecto de los elementos de H y hemos definido una suma sobre H para probar que $(H,+,\cdot)$ es una braza a izquierda.

Teorema 3.2.4. *Sea H cómo en el Teorema 3.2.3, entonces:*

1. $H = \left\{ \left(\sum_{x\in X} a_x\bar{x}, \sum_{x\in X} a_x f_x\right) \,\middle|\, a_x \in \mathbb{Z}, x \in X \right\}$.
2. *El producto de H tiene la forma*

$$\left(\sum_{x\in X} a_x\bar{x}, \alpha\right)\cdot\left(\sum_{x\in X} b_x\bar{x}, \beta\right) = \left(\sum_{x\in X}\left(a_x + b_{\alpha^{-1}(x)}\right)\bar{x}, \alpha\beta\right),$$

donde $\alpha = \sum_{x\in X} a_x f_x$, $\beta = \sum_{x\in X} b_x f_x$.

Teorema 3.2.5. *Sea (X,r) una solución de la YBE y sea H cómo en el Teorema 3.2.3. Si definimos en H una operación $+$ como*

$$\left(\sum_{x\in X} a_x\bar{x}, \alpha\right) + \left(\sum_{x\in X} b_x\bar{x}, \beta\right) = \left(\sum_{x\in X}(a_x + b_x)\bar{x}, \alpha + \beta\right),$$

donde $\alpha = \sum_{x\in X} a_x f_x$, $\beta = \sum_{x\in X} b_x f_x$, *entonces* $(H, +, \cdot)$ *es una braza a izquierda y la aplicación* $\pi\colon H \longrightarrow \mathcal{G}(X, r)$ *dada por* $\pi\left(\sum_{x\in X} a_x \bar{x}, \alpha\right) = \alpha$ *es un homomorfismo de brazas a izquierda.*

Hemos dedicado las siguientes dos secciones, respectivamente, a dar una interpretación geométrica de esta visión con grafos y a comparar las adiciones que hemos empleado con otras ya existentes. Finalmente, en la última sección hemos presentado algunos resultados que se deducen fácilmente como aplicaciones de la perspectiva que emplea el grafo de Cayley. Hemos empezado con una forma de encontrar los pares congelados, un concepto introducido por Chouraqui y Godelle en [16].

Definición 3.5.1. Sea (X, r) una solución de la YBE. Si consideramos la acción natural de r sobre $X \times X$, los puntos fijos de esta acción se denominan *pares congelados.*

Proposición 3.5.2. *Sea* $x \in X$. *Consideremos en el grafo de Cayley del grupo aditivo de* $\mathcal{G}(X, r)$ *el camino de longitud dos que empieza en* 1 *con los dos arcos etiquetados cómo* x *y consideremos los arcos correspondientes en el grafo de Cayley del grupo multiplicativo de* $\mathcal{G}(X, r)$, *con etiquetas* x, y, *respectivamente. Entonces* $r(x, y) = (x, y)$. *Además,* (x, y) *es el único par de la forma* (x, z) *con* $z \in X$ *tal que* $r(x, z) = (x, z)$.

A continuación hemos mostrado que las relaciones explícitamente mencionadas en la definición del grupo de estructura y las triviales de la forma $xy = xy$, son las únicas relaciones formadas por igualdades de productos de dos generadores que se pueden encontrar en este grupo.

Teorema 3.5.4. *Sean* x, y, z, $t \in X$ *vistos como elementos del grupo de estructura* $G(X, r)$. *Entonces* $xy = zt$ *si, y solo si,* $x = z$ *y* $y = t$ *o* $r(x, y) = (z, t)$.

También hemos encontrado una forma más sencilla de probar que la retracción de una solución de la YBE es de nuevo una solución, resultado que ya aparecía en los artículos [19] y [14], pero era difícil de comprobar, y hemos descrito una manera de obtener el grafo de Cayley del grupo de permutaciones asociado a la retracción de una solución de la YBE.

Nuestra última aplicación es una caracterización de cuándo un grupo de permutaciones de una solución de la YBE es una braza trivial.

Proposición 3.5.11. *Las afirmaciones siguientes acerca de una solución de la YBE son equivalentes.*

1. *El grupo de permutaciones $\mathcal{G}(X, r)$ es una braza trivial.*

2. *Para cada x, $y \in X$, si existe $\alpha \in \mathcal{G}(X, r)$ tal que $\alpha(x) = y$, entonces $f_x = f_y$ (es decir, x e y están relacionados por la relación de retracción).*

Contents

Agraïments **iii**

Resum **v**

Resumen **xv**

Introduction **1**

1 The left brace structure **5**
1.1 Definition and first properties 5
1.2 Study of the structure 12
1.3 Relation with the multiplicative group 20

2 IYB-groups **27**
2.1 Solutions of the Yang-Baxter Equation 27
2.2 Involutive Yang-Baxter groups 33
2.2.1 Some examples and preliminary results 37
2.2.2 New results on IYB-groups 40
2.2.3 A concrete example 46

3 A new approach using graphs **49**
3.1 The permutation group as a left brace 49
3.2 The structure group as a left brace 57
3.3 A geometrical interpretation 64
3.4 A comparison with other definitions 67
3.5 Some applications 69

Bibliography **76**

Introduction

The quantum Yang-Baxter equation is an important equation in mathematical physics that appeared for the first time in 1967 in the paper [34] of Yang and later in 1973 in the paper [10] of Baxter. This equation is not only interesting from its applications to physics, but also because it establishes the bases of the theory of quantum groups. One of the fundamental open problems about the Yang-Baxter equation is to find all its solutions: a solution of the quantum Yang-Baxter equation is a pair $(V, \mathcal{R})$ where V is a vector space and $\mathcal{R}\colon V \otimes V \to V \otimes V$ is a linear map that satisfies

$$\mathcal{R}_{12} \circ \mathcal{R}_{23} \circ \mathcal{R}_{12} = \mathcal{R}_{23} \circ \mathcal{R}_{12} \circ \mathcal{R}_{23},$$

where $\mathcal{R}_{ij}\colon V \otimes V \otimes V \to V \otimes V \otimes V$ acts as $\mathcal{R}$ on the tensor factor (i, j) and as the identity on the other factor.

In 1992, Drinfeld defined in [17] a specific subtype of solutions, the set-theoretic ones, and proposed the question of finding all of them. A set-theoretic solution is a pair (X, r) where X is a non-empty set and $r\colon X \times X \to X \times X$ is a map satisfying

$$r_{12} \circ r_{23} \circ r_{12} = r_{23} \circ r_{12} \circ r_{23},$$

where r_{ij} acts as r on components (i, j) and as the identity on the other one. Note that if X is a basis of the vector space V, the set-theoretic solution (X, r) induces a solution on V.

In addition, in the recent years, a subclass of these set-theoretic solutions has been largely studied, namely, the non-degenerate and involutive ones, which are also quite interesting because of their connections with other mathematical theories such as radical rings (see [27]), trifactorized groups (see [31]), and Hopf algebras (see [25]), for instance. Since these are the solutions we are going to consider throughout the memoir, from now on, the involutive, non-degenerate, set-theoretic solutions of the Yang-Baxter equation will be called just as *solutions* for short.

In order to study these solutions, in 2007 Rump ([27]) introduced the concept of left braces, a new algebraic structure consisting of a non-empty

set B with two binary operations $+$ and $\cdot$ such that $(B,+)$ is an abelian group, $(B,\cdot)$ is a group and both operations are related by the following distributivity-like equation

$$a\cdot(b+c)=a\cdot b-a+a\cdot c,\quad \text{for all } a,b,c\in B.$$

In fact, the definition we just stated is not the original one from Rump; it is the equivalent definition presented by Cedó, Jespers, and Okniński in [14]. We will work with this version. Implicitly in Rump's article [27] and explicitly in [14], the authors proved that every left brace B has a solution of the Yang-Baxter equation associated to it, and also, every solution is isomorphic to a solution included in the associated solution of a particular left brace. Hence, it is clear that left braces are an appropriate tool to study the solutions of the Yang-Baxter equation.

Consequently, in our first chapter we will deal with left braces as independent structures (in other words, without relating them to the solutions, just working with them from the algebraic structure view) in order to enlarge our knowledge about them and understand them better. This idea crossed our minds after reading the definitions of left and right nilpotency of a left brace given by Cedó, Gateva-Ivanova, and Smoktunowicz (see [12]) and the definition of solvable left brace introduced by Bachiller, Cedó, Jespers, and Okniński (see [6]). We will as well reserve a section of Chapter 1 to study some properties of a left brace $(B,+,\cdot)$ which can be deduced from properties of the underlying multiplicative group $(B,\cdot)$ and vice versa, following the idea of papers like [30], [12] or [23].

On the other hand, in 2010 Cedó, Jespers and del Río defined in [13] the concept of involutive Yang-Baxter group, or just IYB-group. A group G is said to be an IYB-group if it is isomorphic to the multiplicative group of a left brace. Again, the original definition is not written in this form but in an equivalent one which the authors themselves proposed in their work along with some other equivalences (see [13, Theorem 2.1]). However, we will use this form because our main objective from the beginning are left braces. Since from the results of Etingof, Schedler, and Soloviev ([19]) it was known that any IYB-group is a solvable group, Cedó, Jespers, and del Río also asked in [13] if the converse was true, that is, if every solvable group could be an IYB-group. After that, there were new results proving that some subclasses of solvable groups such as abelian groups, nilpotent groups of class two or of class three and odd order, abelian-by-cyclic groups or solvable A-groups, for example, are indeed IYB-groups (see [13], [15], and [18]). Even though all those results seemed to lead to a positive answer to the question, Bachiller showed a counterexample in [2]. Nonetheless, from [13, Corollary 3.1], it can

be deduced that every IYB-group is a product of two IYB-groups, and that fact motivates another interesting question: *under which conditions can be ensured that a group G is an IYB-group, if $G = NH$ can be factorized as a product of two IYB-groups N and H, being N normal in G?*

In Chapter 2, after the first section which will verse about solutions of the Yang-Baxter equation, we will study IYB-groups and we will show a new theorem in the direction of last question that improves the results that Cedó, Jespers, and del Río ([13, Theorem 3.3]) and Eisele ([18, Proposition 2.2]) proposed in this same direction. We will also obtain new families of IYB-groups using some consequences of that theorem and we will construct a concrete family of IYB-groups that fit with the hypothesis of our theorem but cannot appear as a consequence of the results of [13] or [18]. The original results of this chapter have been published in [24].

Returning to the solutions of the Yang-Baxter equation, Etingof, Schedler, and Soloviev introduced in [19] two fundamental groups associated to a given solution (X, r): the structure group, denoted by $G(X, r)$, and the permutation group, $\mathcal{G}(X, r)$. They are very interesting because they allow the study of the solutions using methods from group theory. In particular, it is possible to deduce properties of a solution from the characteristics of its structure or permutation group (see [12], [29] or [5], for instance). Furthermore, in [14], the authors showed that both groups $G(X, r)$ and $\mathcal{G}(X, r)$ have a natural structure of left brace.

Our goal in Chapter 3 will be to describe this structure with a new approach, concretely, using Cayley graphs. We believe that this is a useful approach to obtain new results and clarify some known properties. First, we will define an addition $+$ over the permutation group $(\mathcal{G}(X, r), \circ)$ in such a way that $(\mathcal{G}(X, r), +, \circ)$ will become a left brace. Also, that addition will allow us to obtain the Cayley graph of $(\mathcal{G}(X, r), +)$ from the one of $(\mathcal{G}(X, r), \circ)$ just by changing the labels of its edges. Secondly, we will use the Cayley graph of $(\mathcal{G}(X, r), +)$ to construct a left brace $(H, +, \cdot)$ whose multiplicative group $(H, \cdot)$ will be isomorphic to the structure group $G(X, r)$. This construction is motivated by the one presented by Ballester-Bolinches, Cosme-Llópez, and Esteban-Romero in [7]. Finally, we will expose a geometrical interpretation and some applications which can be easily proved with this vision and were difficult to prove or understand otherwise. The original results showed in Chapter 3 are collected in [8].

Chapter 1

The left brace structure

The concept of *brace* was first introduced in 2007 by Rump in [27] as a new tool to study the non-degenerate, involutive, set-theoretic solutions of the quantum Yang-Baxter equation, which we will cover in Chapter 2. Later, in 2014, Cedó, Jespers, and Okniński proposed in their paper [14] an equivalent definition of this algebraic structure which will be the one we will use in this memoir.

In this first chapter, we recall the definition of left brace and we study its intrinsic properties without even relating them with the solutions of the Yang-Baxter equation, just considering it as an independent algebraic structure.

1.1 Definition and first properties

We begin with a section recalling the definition and some elementary properties of left braces. Most of these results are well-known and can be find in [14], [23] or [11]. However, we include here the proofs in order to make our exposition self-contained.

Definition 1.1.1. A triple $(B, +, \cdot)$ with B a set and $+$ and $\cdot$ two binary operations is called a *left brace* if it verifies that $(B, +)$ is an abelian group, $(B, \cdot)$ is a group and

$$a \cdot (b + c) = a \cdot b - a + a \cdot c, \tag{1.1}$$

for all $a, b, c \in B$. We call $(B, +)$ and $(B, \cdot)$ the additive and the multiplicative groups of the left brace, respectively.

A *right brace* is defined analogously, replacing condition (1.1) by

$$(a + b) \cdot c = a \cdot c - c + b \cdot c.$$

A left brace $(B, +, \cdot)$ that is also a right brace is called a *two-sided brace*.

We will refer to a left brace $(B, +, \cdot)$ simply as B if the operations are clear from the context. Also, we will usually write ab instead of $a \cdot b$.

Definition 1.1.2. A left brace B will be called *trivial* if it satisfies that $a \cdot b = a + b$ for all $a, b \in B$.

Note that every trivial left brace is in fact a two-sided brace.

Examples 1.1.3. Once recalled the definition, let us see some examples.

(1) Any abelian group can be seen as a trivial two-sided brace.

(2) Given the ring $(\mathbb{Z}_n, +, \cdot)$ with $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where each p_i is a prime number, if we take a natural number m such that $p_1 \cdots p_s | m$ and consider the operation $\bar{x} \circ \bar{y} = \bar{x} + \bar{y} + m\bar{x} \cdot \bar{y}$, for $\bar{x}, \bar{y} \in \mathbb{Z}_n$, then $(\mathbb{Z}_n, +, \circ)$ is a two-sided brace.

(3) If $(2, n) = 1$, then $(\mathbb{Z}_{2n}, +, \circ)$ where $+$ is the usual sum and $\bar{x} \circ \bar{y} = \bar{x} + (-1)^x \bar{y}$, for $\bar{x}, \bar{y} \in \mathbb{Z}_{2n}$, is a left brace but it is not two-sided.

Next lemma shows some elementary properties which will be useful for calculations.

Lemma 1.1.4. *Let $(B, +, \cdot)$ be a left brace. Then for any $a, b, c \in B$, we have:*

(1) the neutral elements of $(B, +)$ and $(B, \cdot)$ coincide;

(2) $a \cdot (-b) = a - a \cdot b + a$;

(3) $a \cdot (b - c) = a \cdot b - a \cdot c + a$.

Proof. (1) Let us denote by 0 and 1 the neutral elements of $(B, +)$ and $(B, \cdot)$, respectively. Now it is enough to apply condition (1.1) of the definition of left brace to any $a \in B$ and $b = c = 0$:

$$a \cdot (0 + 0) = a \cdot 0 - a + a \cdot 0 \iff a \cdot 0 = a \cdot 0 - a + a \cdot 0 \iff a = a \cdot 0.$$

As this hold for any $a \in B$, $0 = 1$.

(2) Again applying (1.1), we obtain

$$\begin{aligned} a \cdot (b - b) = a \cdot b - a + a \cdot (-b) &\iff a \cdot 0 = a \cdot b - a + a \cdot (-b) \\ &\iff a \cdot (-b) = a - a \cdot b + a. \end{aligned}$$

(3) Using (1.1) and the previous property, we can easily compute

$$\begin{aligned} a \cdot (b - c) &= a \cdot b - a + a \cdot (-c) = a \cdot b - a + a - a \cdot c + a \\ &= a \cdot b - a \cdot c + a. \end{aligned}$$

□

Next, we define the lambda homomorphism, which will be very useful in the study of the left brace structure. For instance, we will use it to define important substructures: the ideals and the left ideals.

Proposition 1.1.5. *Given a left brace B, the map $\lambda\colon (B, \cdot) \to \mathrm{Aut}(B, +)$ defined by $\lambda(a) = \lambda_a$ where $\lambda_a(b) = -a + ab$ for all $b \in B$ is a homomorphism of groups.*

Proof. First of all, for all $a \in B$, as

$$\lambda_a(b + c) = -a + a(b + c) = -a + ab - a + ac = \lambda_a(b) + \lambda_a(c)$$

holds for every $b, c \in B$, λ_a is a homomorphism of $(B, +)$. Also,

$$\begin{aligned} \lambda_a(\lambda_b(c)) &= -a + a(-b + bc) = -a + a(-b) - a + a(bc) \\ &= -a + a - ab + a - a + a(bc) = -ab + (ab)c = \lambda_{ab}(c), \end{aligned}$$

and in particular, $\lambda_a \circ \lambda_{a^{-1}} = \lambda_{a^{-1}} \circ \lambda_a = \lambda_0$ and $\lambda_0(c) = -0 + 0c = c$, for all $c \in B$, which implies that λ_a is bijective for all $a \in B$. Since $\lambda_{ab} = \lambda_a \circ \lambda_b$ for all a, $b \in B$, λ is a group homomorphism. □

Definition 1.1.6. Given a left brace B, the maps $\lambda_a \in \mathrm{Aut}(B, +)$ for $a \in B$ of Proposition 1.1.5 will be called the *lambda maps* of B.

Note that the commutativity of the law + is not required in the proofs of Lemma 1.1.4 and Proposition 1.1.5. Hence these results are also valid for skew left braces, a generalization of left braces introduced by Guarnieri and Vendramin in [21] in which the commutativity of the additive group is removed. However, the commutativity of + will be an essential part of the proofs of the following results.

Lemma 1.1.7. *Let B be a left brace. The following properties hold:*

(i) $a\lambda_a^{-1}(b) = b\lambda_b^{-1}(a)$.

(ii) $\lambda_a \lambda_{\lambda_a^{-1}(b)} = \lambda_b \lambda_{\lambda_b^{-1}(a)}$.

Proof. Provided that $\lambda\colon (B,\cdot) \to \mathrm{Aut}(B,+)$ is a group homomorphism and $\lambda_a^{-1} = \lambda_{a^{-1}}$ for all $a \in B$, we find that

$$\begin{aligned} a\lambda_a^{-1}(b) &= a\lambda_{a^{-1}}(b) = a(-a^{-1} + a^{-1}b) = a(-a^{-1}) - a + aa^{-1}b \\ &= a - aa^{-1} + a - a + b = a + b = b + a \\ &= b - bb^{-1} + b - b + a = b(-b^{-1}) - b + bb^{-1}a \\ &= b(-b^{-1} + b^{-1}a) = b\lambda_{b^{-1}}(a) = b\lambda_b^{-1}(a), \end{aligned}$$

and hence (i) holds. We can prove (ii) easily from (i):

$$\lambda_a\lambda_{\lambda_a^{-1}(b)} = \lambda_{a\lambda_a^{-1}(b)} = \lambda_{b\lambda_b^{-1}(a)} = \lambda_b\lambda_{\lambda_b^{-1}(a)}. \qquad \square$$

Now we are ready for our next step: defining some substructures.

Definition 1.1.8. A subset of a left brace B which is both a subgroup of $(B,+)$ and a subgroup of $(B,\cdot)$ will be called a *subbrace* of B.

A subgroup L of the additive group of a left brace B is called a *left ideal* of B if it is closed for the lambda maps, in other words, if $\lambda_a(b) \in L$ whenever $b \in L$ and $a \in B$. Note that if L is a left ideal of B, then it is also a subbrace of B because $ab^{-1} = -\lambda_{ab^{-1}}(b) + a \in L$ for all $a, b \in L$.

Finally, a subset I of a left brace B is an *ideal* of B if it is a normal subgroup of the multiplicative group $(B,\cdot)$ and $\lambda_a(b) \in I$ whenever $b \in I$ and $a \in B$. Note that if I is an ideal of B, then $(I,+)$ is also a subgroup of $(B,+)$ because $a - b = \lambda_b(b^{-1}a) \in I$ for all $a, b \in I$ and hence it is a left ideal too.

Example 1.1.9. Let B be a finite left brace. Then, for any positive integer n, the additive subgroup $nB = \{na \mid a \in B\}$ is closed by the lambda maps, because $\lambda_b(na) = n\lambda_b(a)$. Hence, nB is a left ideal. In particular, every Hall subgroup of $(B,+)$ is a left ideal of B.

Proposition 1.1.10. *Let B be a left brace and let $I \subseteq B$ be an ideal. Then, we can define a structure of left brace over the quotient B/I.*

Proof. As $(I,\cdot)$ is a normal subgroup of $(B,\cdot)$, the group $(B/I,\cdot)$ is well-defined. In a similar way, we can define the abelian group $(B/I,+)$. It is also true that for any $b \in B$, $bI = b+I$ because for any $a \in I$, $b\cdot a = b+\lambda_b(a) \in b+I$ and $b + a = b \cdot \lambda_{b^{-1}}(a) \in bI$, and hence the quotient inherits the brace property. $\square$

Definition 1.1.11. We define the *socle* of a left brace B, and denote it by $\mathrm{Soc}(B)$, as the kernel of the lambda map, that is,

$$\mathrm{Soc}(B) = \{a \in B \mid \lambda_a = \mathrm{id}_B\} = \{a \in B \mid a \cdot b = a + b, \forall b \in B\}.$$

Proposition 1.1.12. *The socle of a left brace B is an ideal of the left brace.*

Proof. Clearly, $(\mathrm{Soc}(B), \cdot)$ is a subgroup of $(B, \cdot)$ because if $a, b \in \mathrm{Soc}(B)$, then $\lambda_{ab^{-1}} = \lambda_a \circ \lambda_{b^{-1}} = \mathrm{id} \circ \lambda_b^{-1} = \mathrm{id}^{-1} = \mathrm{id}$, so $ab^{-1} \in \mathrm{Soc}(B)$. Let us see it is normal: let $a \in B$ and $b \in \mathrm{Soc}(B)$, then $\lambda_{a^{-1}ba} = \lambda_{a^{-1}}\lambda_b\lambda_a = \lambda_a^{-1}\,\mathrm{id}\,\lambda_a = \mathrm{id}$, and thus $a^{-1}ba \in \mathrm{Soc}(B)$.

Finally, we should see that it is closed under the λ maps. If $a \in B$ and $b \in \mathrm{Soc}(B)$, using Lemma 1.1.7, we have that

$$\lambda_{a^{-1}}\lambda_{\lambda_a(b)} = \lambda_b\lambda_{\lambda_{b^{-1}}(a^{-1})} = \mathrm{id} \circ \lambda_{\mathrm{id}(a^{-1})} = \lambda_{a^{-1}} \Longrightarrow \lambda_{\lambda_a(b)} = \mathrm{id}$$

and hence, $\lambda_a(b) \in \mathrm{Soc}(B)$. □

Definition 1.1.13. A left brace B will be called *simple* if 0 and B are its only ideals.

Example 1.1.14. For any prime number p, the trivial left brace $\mathbb{Z}_p$ is simple. In fact, those are the unique left braces which can be trivial and simple at the same time.

Definition 1.1.15. We define the star operation $*$ on a left brace B as

$$a * b := -a + a \cdot b - b = (\lambda_a - \mathrm{id})(b), \quad \text{for all } a, b \in B.$$

There is an equivalent definition for left ideal and for ideal of a brace which uses the star operation defined by Rump in [27] and which also allows us to define a *right ideal*. It is as follows:

Let $(B, +, \cdot)$ be a left brace. A non-empty subset I of B is said to be a left (right) ideal of B if $(I, +) \leq (B, +)$ and $b * a \in I$ ($a * b \in I$) for every $a \in I$ and $b \in B$. I is called an ideal of B if it is both a left and a right ideal of B.

Rump also noted in [27] that two-sided braces are equivalent to radical rings because given a radical ring $(R, +, \cdot)$, we can define a two-sided brace $(R, +, \circ)$ with product $r \circ r' := r \cdot r' + r + r'$, for any $r, r' \in R$. In this case, the star operation of the brace coincides with the product of the ring. Conversely, given any two-sided brace $(B, +, \circ)$, we can define a radical ring $(B, +, \cdot)$ using the star product of the brace as product of the ring: $b \cdot b' := b \circ b' - b - b'$. Thus, in this sense, left braces are a generalization of radical rings.

The following lemma shows some properties of the star operation and in the next one, we will use the new definition of ideal to prove that the product of two ideals is again an ideal.

Lemma 1.1.16. *Let $(B, +, \cdot)$ be a left brace. Then, for any $a, b, c \in B$, we have:*

1. $a * (b + c) = a * b + a * c$;
2. $a * 0 = 0 * a = 0$;
3. $a * (-b) = -(a * b)$;
4. $(a \cdot b) * c = a * (b * c) + b * c + a * c$.

Proof. The first three properties follow easily by simple calculation and using Lemma 1.1.4. Let us see the last one:

$$\begin{aligned}(a \cdot b) * c &= -a \cdot b + (a \cdot b) \cdot c - c = -a \cdot b + a \cdot (b \cdot c) - c \\ &= -a \cdot b + a \cdot (b + b * c + c) - c \\ &= -a \cdot b + a \cdot b - a + a \cdot (b * c) - a + a \cdot c - c \\ &= -a + a \cdot (b * c) + a * c \\ &= -a + a \cdot (b * c) - b * c + b * c + a * c \\ &= a * (b * c) + b * c + a * c.\end{aligned}$$

□

Lemma 1.1.17. *If I and J are ideals of B, then IJ is also an ideal of B.*

Proof. On the one hand, as $IJ = I + J$, it is clear that $(IJ, +) \leq (B, +)$. On the other hand, as I and J are ideals of B, if $ij \in IJ$ and $b \in B$, then by Lemma 1.1.16,

$$\begin{aligned}(ij) * b &= i * (j * b) + i * b + j * b \in IJ; \\ b * (ij) &= b * (i * j + i + j) = b * (i * j) + b * i + b * j \in IJ.\end{aligned}$$

Hence, IJ is an ideal of B. □

Another important contribution of Rump in [27] is the introduction of two series of subbraces of B which will be used to define left and right nilpotency of a left brace. They start with $B = B^1 = B^{(1)}$ and then B^n and $B^{(n)}$ are defined inductively as

$$B^{n+1} = B * B^n = \left\{ \sum_{i=1}^{m} a_i * b_i \,|\, a_i \in B, b_i \in B^n, \text{for every } i \right\},$$
$$B^{(n+1)} = B^{(n)} * B = \left\{ \sum_{i=1}^{m} a_i * b_i \,|\, a_i \in B^{(n)}, b_i \in B, \text{for every } i \right\},$$

for all positive integers n. Note that $B^{(2)} = B^2$, but $B^{(3)}$ and B^3 are different because $*$ is not associative in general. Also, as a consequence of the following lemma, we can see that the subbraces B^i of the first series are left ideals of B and the ones of the second one, $B^{(i)}$, are ideals for any i.

Lemma 1.1.18. *Let B be a left brace, L a left ideal of B and I an ideal of B. Then $I * L$ is a left ideal of B. Moreover, $I * B$ is an ideal of B.*

Proof. If $x \in I * L$, then there exist some elements $a_i \in I, b_i \in L$ such that $x = \sum_{i=1}^{n} a_i * b_i$. Given $y \in B$, $\lambda_y(x) = \lambda_y(\sum_{i=1}^{n} a_i * b_i) = \sum_{i=1}^{n} \lambda_y(a_i * b_i)$. Therefore, it is enough to prove that $\lambda_y(a * b) \in I * L$ for each $a \in I, b \in L$.

$$\begin{aligned}\lambda_y(a * b) &= \lambda_y(\lambda_a(b) - b) = (\lambda_y \circ \lambda_a)(b) - \lambda_y(b)\\ &= \lambda_{ya}(b) - \lambda_y(b) = \lambda_{(yay^{-1})y}(b) - \lambda_y(b)\\ &= \lambda_{yay^{-1}}(\lambda_y(b)) - \lambda_y(b)\\ &= (yay^{-1}) * \lambda_y(b).\end{aligned}$$

Since I is an ideal of B, $(I, \cdot) \trianglelefteq (B, \cdot)$ and hence $yay^{-1} \in I$. Also, as L is a left ideal of B, we have that $\lambda_y(b) \in L$. Thus $\lambda_y(a * b) \in I * L$, as desired.

We prove now that $I * B$ is an ideal of B. It is enough to show that $(I * B, \cdot) \trianglelefteq (B, \cdot)$. If $x \in I * B$ and $y \in B$, then

$$\begin{aligned}y^{-1}xy &= y^{-1}(xy) - y^{-1} + y^{-1} = \lambda_{y^{-1}}(xy) + y^{-1}\\ &= \lambda_{y^{-1}}(x * y + x + y) + y^{-1}\\ &= \lambda_{y^{-1}}(x * y) + \lambda_{y^{-1}}(x) + \lambda_{y^{-1}}(y) + y^{-1}\\ &= \lambda_{y^{-1}}(x * y) + \lambda_{y^{-1}}(x).\end{aligned}$$

Note that, since I is an ideal of B, x also belongs to I, and then $x * y \in I * B$. Now, since $I * B$ is a left ideal of B, we have that both $\lambda_{y^{-1}}(x * y)$ and $\lambda_{y^{-1}}(x)$ belong to $I * B$. Thus $y^{-1}xy \in I * B$. □

Remark 1.1.19. It is easy to see that if I is an ideal of B, then the quotient brace B/I is a trivial brace if, and only if, $B^2 \subseteq I$.

To end this section, we define the concept of homomorphism of left braces and show some properties related with it. The typical isomorphism theorems also hold for left braces.

Definition 1.1.20. Let B_1 and B_2 be two left braces. A map $f : B_1 \to B_2$ is a *homomorphism of left braces* if $f(a+b) = f(a)+f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$, for all $a, b \in B_1$. The *kernel* of f is defined as $\mathrm{Ker}(f) = \{a \in B_1 \mid f(a) = 1_{B_2}\}$, as usual. Also, the set of automorphisms of the left brace B_1 forms a group with the composition and is denoted by $\mathrm{Aut}(B_1)$.

Proposition 1.1.21. *Given a homomorphism of left braces $f : B_1 \to B_2$, its kernel is an ideal of B_1.*

Proof. Let us denote by I the kernel of f. Then both $(I,+) \trianglelefteq (B,+)$ and $(I,\cdot) \trianglelefteq (B,\cdot)$ because they are the kernels of a group homomorphism from $(B_1,+)$ to $(B_2,+)$ and from $(B_1,\cdot)$ to $(B_2,\cdot)$, respectively. Finally, if $a \in B_1$ and $b \in \operatorname{Ker}(f)$, then $\lambda_a(b) \in \operatorname{Ker}(f)$:

$$f(\lambda_a(b)) = f(-a+ab) = -f(a) + f(a)\cdot f(b) = -f(a) + f(a) = 0. \qquad \square$$

Example 1.1.22. Let B_1 and B_2 be two left braces. If there exists a homomorphism of groups $\eta\colon (B_2,\cdot) \to \operatorname{Aut}(B_1)$, we can take the semidirect product of the multiplicative groups of B_1 and B_2 via η, $[B_1]B_2$, and consider an addition over it defined componentwise. In that case, the semidirect product has structure of left brace. As a particular case, the direct product of two left braces is also a left brace.

Theorem 1.1.23 (First isomorphism theorem)**.** *Let $f : B_1 \to B_2$ be a homomorphism of left braces. Then $B_1/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.*

Theorem 1.1.24 (Second isomorphism theorem)**.** *Let B be a left brace, H a subbrace of B and N an ideal of B. Then $H \cap N$ is an ideal of H, HN is a subbrace of B, and $HN/N \cong H/(H \cap N)$.*

Theorem 1.1.25 (Third isomorphism theorem)**.** *Let B be a left brace and let N and H be two ideals of B with $N \subseteq H \subseteq B$. Then, $(B/N)/(H/N) \cong B/H$.*

1.2 Study of the structure

Once covered the first definitions and properties of a left brace, we are going to study this algebraic structure by defining analogous concepts to the ones used in group theory. We will start with chief and composition series and follow with solvability, supersolvability, and nilpotency. We decided to follow this line of research after reading [6] and [12], in which Bachiller, Cedó, Jespers, and Okniński defined when a left brace is solvable, and Cedó, Gateva-Ivanova, and Smoktunowicz introduced left and right nilpotent left braces, respectively.

Definition 1.2.1. An ideal I of a left brace B will be called *minimal* if there is no other ideal J of B with $0 \neq J \subseteq I$.

Remark 1.2.2. Given an ideal I of B and a subbrace J of B, we have that J/I is an ideal of B/I if, and only if, J is an ideal of B with $I \subseteq J$.

Proof. Assume that I and J are ideals of B with $I \subseteq J$. Then, clearly $(J/I, +) \leq (B/I, +)$. Also, given $aI \in J/I$ and $bI \in B/I$, we have that

$$aI * bI = aI \cdot bI - aI - bI = (ab - a - b)I = (a * b)I$$

belongs to J/I because $a * b \in J$. Analogously, $bI * aI \in J/I$, proving that J/I is an ideal of B/I.

Conversely, let us suppose now that J/I is an ideal of B/I. Clearly, $(J, +) \leq (B, +)$ and $I \subseteq J$. In addition, if $a \in J$ and $b \in B$, as $aI * bI = (a * b)I \in J/I$, we have $a * b \in J$. And analogously, $b * a \in J$, and thus J is an ideal of B. □

Definition 1.2.3. Given a left brace B, a series $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$ such that each B_i is an ideal of B will be called an *ideal series*. If instead of that condition, each B_i is an ideal of B_{i+1}, it will be called a *subideal series*. A *refinement* of an ideal (or subideal) series is any ideal (subideal) series containing the original one.

Definition 1.2.4. Given a left brace B, an ideal series

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$$

with B_{i+1}/B_i minimal ideal of B/B_i for all $i \in \{0, \ldots, n-1\}$ is called a *chief series* and the factors B_{i+1}/B_i are called *chief factors*.

Proposition 1.2.5. *An ideal series which can not be refined is a chief series.*

Proof. Suppose $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$ is an ideal series that does not admit any non trivial refinement. Then, for all i, B_{i+1}/B_i is a minimal ideal of B/B_i, because in other case, we would find an ideal I of B with $B_i \subsetneq I \subsetneq B_{i+1}$ and the series $0 = B_0 \subseteq \cdots \subseteq B_i \subset I \subset B_{i+1} \subseteq \cdots \subseteq B_n = B$ would be a refinement of the original one. □

Definition 1.2.6. Given a left brace B, a subideal series

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$$

with B_{i+1}/B_i simple for all $i \in \{0, \ldots, n-1\}$ is called a *composition series* and the factors B_{i+1}/B_i are called *composition factors*.

Proposition 1.2.7. *A subideal series which cannot be refined is a composition series.*

Proof. Suppose $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$ is a subideal series that does not admit any non trivial refinement. Suppose B_{i+1}/B_i is not simple for some i. Then, there exists a non trivial ideal I/B_i of B_{i+1}/B_i, which means that I is an ideal of B_{i+1} with $B_i \subsetneq I \subsetneq B_{i+1}$ and then the series $0 = B_0 \subseteq \cdots \subseteq B_i \subset I \subset B_{i+1} \subseteq \cdots \subseteq B_n = B$ is a refinement of the original one, which is a contradiction. □

Remark 1.2.8. In a finite left brace B, there always exist a chief series and a composition series: we just start with the trivial series $0 = B_0 \subseteq B_1 = B$ and refine it until we obtain the desired series.

Our next goal is to prove an equivalent of the Jordan-Hölder Theorem for both chief and composition series of a left brace. To achieve it, we will adapt to the new structure (in Proposition 1.2.11) the proof of that theorem presented in [9] by Baumslag.

Lemma 1.2.9. *Asumme L, N and T are ideals of a left brace B with $T \subseteq L$. Then*

$$\frac{LN}{TN} = \frac{LTN}{TN} \cong \frac{L}{TN \cap L} = \frac{L}{T(N \cap L)}.$$

Definition 1.2.10. Two series of a left brace B are called *equivalent* if there exists a bijection between their factors such that corresponding factors are isomorphic.

Proposition 1.2.11. *Two ideal series of a left brace B,*

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B,$$
$$0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_m = B,$$

can be refined to two equivalent ideal series.

Proof. For each i, let us consider

$$B_i = (B_{i+1} \cap A_0)B_i \subseteq (B_{i+1} \cap A_1)B_i \subseteq \cdots \subseteq (B_{i+1} \cap A_m)B_i = B_{i+1}.$$

Note that each step is an ideal of B: as each B_i and A_j are ideals of B, $(B_{i+1} \cap A_j)$ is an ideal of B and by Lemma 1.1.17, $(B_{i+1} \cap A_j)B_i$ is also an ideal of B.

Thus, we have obtained a new ideal series which is a refinement of the first one and have nm terms. Analogously, we can obtain a refinement of the second series of mn terms by adding the terms

$$A_j = (A_{j+1} \cap B_0)A_j \subseteq (A_{j+1} \cap B_1)A_j \subseteq \cdots \subseteq (A_{j+1} \cap B_n)A_j = A_{j+1}.$$

Finally, using twice Lemma 1.2.9, we have that

$$\begin{aligned}\frac{(B_{i+1}\cap A_{j+1})B_i}{(B_{i+1}\cap A_j)B_i} &\cong \frac{B_{i+1}\cap A_{j+1}}{(B_{i+1}\cap A_j)(B_i\cap B_{i+1}\cap A_{j+1})}\\ &= \frac{B_{i+1}\cap A_{j+1}}{(B_{i+1}\cap A_j)(B_i\cap A_{j+1})}\\ &= \frac{A_{j+1}\cap B_{i+1}}{(A_{j+1}\cap B_i)(A_j\cap B_{i+1})}\\ &= \frac{A_{j+1}\cap B_{i+1}}{(A_{j+1}\cap B_i)(A_j\cap A_{j+1}\cap B_{i+1})}\\ &\cong \frac{(A_{j+1}\cap B_{i+1})A_j}{(A_{j+1}\cap B_i)A_j},\end{aligned}$$

and so the factors in the new series can be paired so that corresponding factors are isomorphic. □

Remark 1.2.12. With a little patience and some calculations, one can prove that if the series of the former proposition,

$$\begin{aligned}0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B,\\ 0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_m = B,\end{aligned}$$

are subideal series instead of ideal ones, then the series used in the proof,

$$\begin{aligned}B_i = (B_{i+1}\cap A_0)B_i \subseteq (B_{i+1}\cap A_1)B_i \subseteq \cdots \subseteq (B_{i+1}\cap A_m)B_i = B_{i+1},\\ A_j = (A_{j+1}\cap B_0)A_j \subseteq (A_{j+1}\cap B_1)A_j \subseteq \cdots \subseteq (A_{j+1}\cap B_n)A_j = A_{j+1},\end{aligned}$$

are also subideal series, and hence we can adapt last proposition and obtain that, in that case, we can refine the original series to two equivalent subideal series.

Theorem 1.2.13 (Jordan-Hölder)**.** *Any two chief (or composition) series of a left brace B are equivalent.*

Note that with the latter proposition and remark, the Jordan-Hölder-like theorem is clear. Now we continue with solvability.

Definition 1.2.14. A left brace B will be called *solvable* if it has a subideal series with all its factors of prime order.

As mentioned above, the concept of solvable left braces was introduced in [6] by Bachiller, Cedó, Jespers, and Okniński, but their definition was slightly diferent, it reads:

Definition 1.2.15. A left brace B is a *solvable* brace if it has a subideal series

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

such that all its factors are trivial braces.

However, this two definitions are equivalent: assume $(B, +, \cdot)$ is solvable in the sense of [6]. Then, there exists a series

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

such that B_i is an ideal of B_{i+1}, and B_{i+1}/B_i is a trivial brace for every $i \in \{0, 1, \ldots, m-1\}$.

Suppose that there exists $j \in \{0, 1, \ldots, m-1\}$ such that $|B_{j+1}/B_j|$ is not a prime number. As B_{j+1}/B_j is trivial, all subgroups $(A/B_j, +)$ of $(B_{j+1}/B_j, +)$ are ideals of the left brace because $aB_j * bB_j = B_j = bB_j * aB_j$ whenever $aB_j \in A/B_j$ and $bB_j \in B_{j+1}/B_j$.

Therefore, we can find

$$B_j/B_j = A_0/B_j \subseteq A_1/B_j \subseteq \cdots \subseteq A_n/B_j = B_{j+1}/B_j$$

with A_i/B_j ideal of B_{j+1}/B_j (and of A_{i+1}/B_j) and $|(A_{i+1}/B_j)/(A_i/B_j)| = |A_{i+1}/A_i|$ a prime number for all $i \in \{0, \ldots, n-1\}$.

In particular, B_j is an ideal of A_1 and $|A_1/B_j|$ is prime. Thus, we can complete the initial series to obtain a new one with all its factors of prime order:

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_j \subseteq A_1 \subseteq \cdots \subseteq A_n = B_{j+1} \subseteq \cdots \subseteq B_m = B.$$

Conversely, as for any prime p the unique left brace of order p is the trivial one, every subideal series with all its factors of prime order has all its factors trivial.

In [6] the authors also note the following properties.

Proposition 1.2.16. *Let B be a left brace. Then*

(a) If we define $d_1(B) = B^2$ and $d_{i+1}(B) = d_i(B)^2$ for every positive integer i, then B is a solvable left brace if and only if $d_k(B) = 0$ for some k.

(b) Let I be an ideal of B. If I and B/I are solvable left braces, then B is also solvable.

(c) If B is solvable, then any subbrace and any quotient of B is solvable.

Definition 1.2.17. Let B be a solvable left brace. Then the series

$$0 = d_k(B) \subseteq d_{k-1}(B) \subseteq \cdots \subseteq d_1(B) \subseteq B$$

will be called the *derived series* or *solvable series* of B, and $d_1(B) = B^2$ will be the *derived ideal* of B.

Following the idea of solvable left braces, we can define the concept of supersolvable left braces.

Definition 1.2.18. We say that a left brace $(B, +, \cdot)$ is *supersolvable* if it has an ideal series

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

such that $|B_{i+1}/B_i|$ is a prime number for any $i \in \{0, 1, \ldots, m-1\}$.

Clearly, a supersolvable left brace is always solvable. Also, if the left brace is supersolvable, in particular, its multiplicative group is supersolvable. Next we will see some straightforward properties and then we will deal with nilpotency.

Proposition 1.2.19. *The following properties hold:*

(a) Any subbrace and any quotient of a supersolvable left brace are supersolvable.

(b) The direct product of a finite number of supersolvable left braces is a supersolvable left brace.

Definition 1.2.20. We say that a left brace B is *left nilpotent* if there exists a positive integer n such that $B^n = 0$. A left brace B is *right nilpotent* if there exists a positive integer n such that $B^{(n)} = 0$.

The following characterization of right nilpotent left braces shows that this concept is similar to the one of nilpotent group, where the role of the center of a group is played by the socle of a left brace.

Proposition 1.2.21. *A left brace B is right nilpotent if, and only if, it has an ideal series $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$ with $B_i/B_{i-1} \subseteq \mathrm{Soc}(B/B_{i-1})$ for every $i \in \{1, \ldots, n\}$.*

Proof. Assume that B is right nilpotent. Then, there exists a natural number m such that $B^{(m)} = 0$ and also $0 = B^{(m)} \subseteq B^{(m-1)} \subseteq \ldots B^{(2)} \subseteq B$ is an ideal series for B. Let us see that $B^{(i)}/B^{(i+1)} \subseteq \mathrm{Soc}(B/B^{(i+1)})$ for all

$i \in \{0, \dots, m-1\}$. If $aB^{(i+1)} \in B^{(i)}/B^{(i+1)}$, we should see that $\lambda_{aB^{(i+1)}} = \mathrm{id}_{B/B_{(i+1)}}$. Let $bB^{(i+1)}$ be any element in $B/B^{(i+1)}$, then

$$\begin{aligned}\lambda_{aB^{(i+1)}}(bB^{(i+1)}) = bB^{(i+1)} &\iff (aB^{(i+1)})(bB^{(i+1)}) - aB^{(i+1)} = bB^{(i+1)} \\ &\iff (ab - a - b)B^{(i+1)} = B^{(i+1)} \\ &\iff a * b \in B^{(i+1)},\end{aligned}$$

and the last equivalence is true by definition of $B^{(i+1)}$.

Assume now that B has an ideal series $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = B$ with $B_i/B_{i-1} \subseteq \mathrm{Soc}(B/B_{i-1})$. In particular, $\mathrm{Soc}(B/B_{n-1}) = B/B_{n-1}$. Therefore, for all $a, b \in B$, $\lambda_{aB_{n-1}}(bB_{n-1}) = bB_{n-1}$, or equivalently, $a * b \in B_{n-1}$. Thus, $B^{(2)} \subseteq B_{n-1}$. Note that $B_i/B_{i-1} \subseteq \mathrm{Soc}(B/B_{i-1})$ implies $b*a \in B_{i-1}$ whenever $b \in B_i$ and $a \in B$. Hence, if $b \in B^{(2)} \subseteq B_{n-1}$ and $a \in B$, then $b * a \in B_{n-2}$ and so $B^{(3)} \subseteq B_{n-2}$. Following like this, we have that $B^{(n+1)} \subseteq B_0 = 0$ and B is right nilpotent. □

Remark 1.2.22. For every left brace B, $d_n(B) \subseteq B^{n+1} \cap B^{(n+1)}$. Hence every left nilpotent left brace is solvable, and every right nilpotent left brace is solvable. However, there exist solvable left braces which are neither left nilpotent nor right nilpotent: it is enough to take B_1 a right nilpotent left brace which is not left nilpotent and B_2 a left nilpotent left brace which is not right nilpotent, and consider their direct product. Easily, $B_1 \times B_2$ is a solvable left brace but is not left nilpotent nor right nilpotent. For a concrete example, take B_1 and B_2 as Example 1.2.24 and Example 1.2.25 later in this section, respectively.

In [30], Smoktunowicz proposed another series of ideals $B^{[n]}$ in the following way:

$$B^{[1]} = B \text{ and } B^{[n+1]} = \sum_{i=1}^{n} B^{[i]} * B^{[n+1-i]}, \quad \text{for all positive integers } n.$$

She also proved that, if m and n are natural numbers with $A^n = A^{(m)} = 0$, then $A^{[s]} = 0$ for some number s (see [30, Theorem 3.1]). We can use this property to prove the next result.

Proposition 1.2.23. *If $(B, +, \cdot)$ is a finite left brace that is both left and right nilpotent, then B is supersolvable.*

Proof. By Smoktunowicz's results, if the left brace B is both left and right nilpotent, there exists a natural number s such that $B^{[s]} = 0$. Let us consider the series

$$0 = B^{[s]} \subseteq B^{[s-1]} \subseteq \cdots \subseteq B^{[1]} = B.$$

We know that $B^{[i]}$ is an ideal of B for every $i \in \{1, \dots, s\}$. Suppose that there exists a natural $j \in \{1, \dots, s-1\}$ such that $|B^{[j]}/B^{[j+1]}|$ is not a prime number.

Let $(I, +)$ be a subgroup of $(B^{[j]}, +)$ containing $B^{[j+1]}$. If $i \in I$ and $b \in B$, then

$$i * b \in I * B \subseteq B^{[j]} * B \subseteq \sum_{k=1}^{j} B^{[k]} * B^{[j+1-k]} = B^{[j+1]} \subseteq I;$$

$$b * i \in B * I \subseteq B * B^{[j]} \subseteq \sum_{k=1}^{j} B^{[k]} * B^{[j+1-k]} = B^{[j+1]} \subseteq I.$$

Consequently, any subgroup of $(B^{[j]}, +)$ containing $B^{[j+1]}$ is an ideal of the whole brace B. Thus, we can refine the series:

$$0 = B^{[s]} \subseteq \cdots \subseteq B^{[j+1]} = I_0 \subseteq I_1 \subseteq \cdots \subseteq I_m = B^{[j]} \subseteq \cdots \subseteq B^{[1]} = B$$

with I_{k+1}/I_k of prime order, for all $k \in \{0, \dots, m-1\}$. Then, B is a supersolvable left brace. □

The following examples show that last result is not necessarily true if the brace satisfies just one of the conditions about nilpotency but not the other one. They can be found in [6] and [3], respectively.

Example 1.2.24. Consider the trivial left braces $K = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_3$ and let $\alpha : \mathbb{Z}_3 \longrightarrow \mathrm{Aut}(K, +)$ be the action defined by $\alpha(x) = \alpha_x$ with

$$\alpha_x(y, z) = (y, z) \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^x$$

for all $x \in \mathbb{Z}_3$ and $y, z \in \mathbb{Z}_2$. Then, the semidirect product $B = [K]\mathbb{Z}_3$ is a left brace which is right nilpotent (and then, solvable) but not left nilpotent. Also, the multiplicative group of the left brace B is isomorphic to the alternating group of degree 4, which is not supersolvable, implying that the left brace is not supersolvable either.

Example 1.2.25. Consider the left brace $(B, +, \cdot)$ having as additive group $(B, +) = (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$ and product defined by

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + z_1y_2 + x_1z_2 + y_1z_2 + x_1z_1z_2 \\ y_1 + y_2 + z_1z_2 + x_1z_2 + y_1z_1z_2 \\ z_1 + z_2 \end{pmatrix}.$$

This left brace is left nilpotent but is not right nilpotent. Also, it has no ideals of order 2, so it is not supersolvable.

On the other hand, both B^2 and B/B^2 are supersolvable, so this example shows us that a left brace B having an ideal I such that both I and B/I are supersolvable is not necessarily supersolvable.

To end this section, as in group theory the derived subgroup of a supersolvable group is always nilpotent, we would like to know if there is a parallel result for left braces. With the help of GAP [20], and in particular using the package [33] about combinatorial solutions for the Yang-Baxter equation by Vendramin and Konovalov, we found a supersolvable left brace of order 12 whose derived ideal is not left nilpotent:

```
gap> B:=SmallBrace(12,5);
<brace of size 12>
gap> s:=SolvableSeries(B);
[ <brace of size 12>, <brace of size 6>, <brace of size 3>,
  <brace of size 1> ]
gap> List(s, x->IsIdeal(B,x));
[ true, true, true, true ]
gap> # As every subbrace in the solvable series of B is an
     ideal and the factors have prime order, B is also a
     supersolvable left brace.
gap> # Let us see that the derived ideal is not left nilpotent:
gap> B2:=s[2];
<brace of size 6>
gap> IsLeftNilpotent(B2);
false
```

Thus, it is not true that the derived ideal of a supersolvable left brace is left nilpotent. However, every supersolvable left brace of the library of small braces contained in the package [33] satisfies that its derived ideal is right nilpotent. Hence, we propose the following question:

Question 1.2.26. If B is a supersolvable left brace, is its derived ideal B^2 right nilpotent?

1.3 Relation with the multiplicative group

The last section of this chapter will be about some properties of the left brace which can be deduced from properties of its underlying multiplicative group and vice versa. All the left braces considered in this section will be finite.

The first result in this direction was proved by Etingof, Schedler, and Soloviev in [19] and shows that the multiplicative group of a left brace is always a solvable group.

Proposition 1.3.1. *Let B be a finite left brace. Then its multiplicative group, $(B, \cdot)$, is solvable.*

Proof. Let p be any prime number dividing the order of B and let $(H, +)$ be the Hall p'-subgroup of $(B, +)$. We claim that $(H, \cdot)$ is also a subgroup of $(B, \cdot)$: for any $x, y \in H$,

$$xy^{-1} = xy^{-1} - x + x = \lambda_x(y^{-1}) + x \in H$$

because H is a left ideal (recall Example 1.1.9). Therefore, $(H, \cdot)$ is a Hall p'-subgroup of $(B, \cdot)$. Hence, $(B, \cdot)$ is solvable by P. Hall's Theorem (see [26, 9.1.8]). □

A very important result in this direction is due to Smoktunowicz and can be found in [30]. It says that a finite left brace is left nilpotent if and only if its multiplicative group is nilpotent. However, this result is quite difficult to prove directly, but we can see it in an easier way as a consequence of the following results by Ballester-Bolinches, Esteban-Romero, and Meng (see [23]).

First, we need a few definitions: let X, Y be subsets of the left brace B and define

$$X * Y = \langle x * y \mid x \in X, y \in Y \rangle_+,$$

where $\langle S \rangle_+$ denotes the subgroup generated by the set $S \subseteq B$ in $(B, +)$. Note that if $(Y, +)$ is a subgroup of $(B, +)$, it follows from Lemma 1.1.16 (3) that

$$X * Y = \left\{ \sum_{i=1}^{m} x_i * y_i \mid x_i \in X, y_i \in Y \right\}.$$

Also, note that if Y and Z are subgroups of $(B, +)$, we have that $X*(Y+Z) = (X * Y) + (X * Z)$ by Lemma 1.1.16 (1).

Definition 1.3.2. Given two subsets X, Y of a left brace B, we define inductively $\mathrm{L}_{m+1}(X, Y) = X * \mathrm{L}_m(X, Y)$ for every $m \in \mathbb{N}$, where $\mathrm{L}_1(X, Y) = X * Y$. Note that in particular $L_n(B, B) = B^{n+1}$.

Lemma 1.3.3. *Let $(B, +, \cdot)$ be a brace. Assume that Y and Z are subgroups of $(B, +)$. Then*

$$\mathrm{L}_n(X, Y + Z) = \mathrm{L}_n(X, Y) + \mathrm{L}_n(X, Z), \quad \textit{for all } n \in \mathbb{N}.$$

Proof. We argue by induction on n. If $n = 0$, then the result is clear. We may assume that $n \geq 1$ and $\mathrm{L}_{n-1}(X, Y + Z) = \mathrm{L}_{n-1}(X, Y) + \mathrm{L}_{n-1}(X, Z)$ holds.

Then

$$\begin{aligned} \mathrm{L}_n(X, Y+Z) &= X * \mathrm{L}_{n-1}(X, Y+Z) \\ &= X * (\mathrm{L}_{n-1}(X, Y) + \mathrm{L}_{n-1}(X, Z)) \\ &= X * \mathrm{L}_{n-1}(X, Y) + X * \mathrm{L}_{n-1}(X, Z) \\ &= \mathrm{L}_n(X, Y) + \mathrm{L}_n(X, Z). \end{aligned}$$ □

Definition 1.3.4. Let B be a left brace and let p be a prime. We say that B is *left p-nilpotent* if $\mathrm{L}_n(B, B_p) = 0$ for some $n \in \mathbb{N}$, where B_p is the Sylow p-subgroup of the additive group $(B, +)$.

Lemma 1.3.5. *Let B be a finite brace. Then B is left nilpotent if and only if B is left p-nilpotent for all primes p dividing its order.*

Proof. Denote by $\pi(B)$ the set of all the primes dividing the order of B. It is clear that the lemma holds when $B = \{0\}$. Thus we may assume that $B \neq \{0\}$.

Assume that B is left nilpotent. Then $\mathrm{L}_n(B, B) = 0$ for some integer $n \geq 1$. Now, for every prime p dividing the order of B, we have that $\mathrm{L}_n(B, B_p) \subseteq \mathrm{L}_n(B, B) = 0$, where B_p is the Sylow p-subgroup of $(B, +)$. Hence B is left p-nilpotent.

Conversely, assume that B is left p-nilpotent for every prime $p \in \pi(B)$. Then, there exist some positive integers $n(p)$ (depending on p) such that $\mathrm{L}_{n(p)}(B, B_p) = 0$, where each B_p is the Sylow p-subgroup of $(B, +)$. Let $m = \max\{n(p) \mid p \in \pi(B)\}$. Then

$$\mathrm{L}_m(B, B_p) = 0, \text{for all } p \in \pi(B).$$

Observe that $B = \sum_{p \in \pi(B)} B_p$. It follows from Lemma 1.3.3 that

$$\mathrm{L}_m(B, B) = \mathrm{L}_m\left(B, \sum_{p \in \pi(B)} B_p\right) = \sum_{p \in \pi(B)} \mathrm{L}_m(B, B_p) = 0.$$

Hence B is left nilpotent. □

To continue with this approach, we will need to describe the sets $\mathrm{L}_n(X, Y)$ in terms of commutators of the semidirect product $G = [(B, +)](B, \cdot)$ via the action λ (recall Proposition 1.1.5).

Let $a \in (B, +)$ and $b \in (B, \cdot)$. Then, viewed in G, $a = (a, 1)$ and $b = (0, b)$, and we have

$$\begin{aligned} [a, b^{-1}] &= [(a, 1), (0, b)^{-1}] = (-a, 1)(0, b)(a, 1)(0, b^{-1}) \\ &= (-a, b)(a, b^{-1}) = (-a + \lambda_b(a), bb^{-1}) \\ &= (-a + b \cdot a - b, 1) = (b * a, 1) \in (B, +) \subseteq G. \end{aligned}$$

More generally, if Y is a subgroup of $(B,+)$ and X is a subgroup of $(B,\cdot)$, then

$$[Y,X]=\langle [y,x^{-1}] \mid x\in X, y\in Y\rangle_+ = \langle x*y \mid x\in X, y\in Y\rangle_+ = X*Y,$$

and hence,

$$\mathrm{L}_n(X,Y)=[\cdots[Y,X],X],\ldots,X]=[Y,X,\ldots,X],$$

where X appears n times.

Lemma 1.3.6 ([27, Corollary of Proposition 8])**.** *Let B be a finite brace such that $|B|=p^n$ for some prime p and $n\geq 0$. Then $\mathrm{L}_n(B,B)=0$.*

Proof. As B has order p^n for some prime p, $n\geq 1$, we have that the direct product $G=[(B,+)](B,\cdot)$ is a p-group and so it is nilpotent. Also, we can see that $\mathrm{L}_n(B,B)=B^{n+1}$ is a normal subgroup of G contained in $(B,+)$ for all n: let $(a_1,a_2)\in G$ and $(b,1)\in B^{n+1}$, then

$$\begin{aligned}(a_1,a_2)^{-1}(b,1)(a_1,a_2) &= (-\lambda_{a_2}^{-1}(a_1),a_2^{-1})(b+a_1,a_2)\\ &= (-\lambda_{a_2}^{-1}(a_1)+\lambda_{a_2}(b+a_1),1)\\ &= (\lambda_{a_2}(-a_1+b+a_1),1)\\ &= (\lambda_{a_2}(b),1)\in B^{n+1}\end{aligned}$$

because $b\in B^{n+1}$, which is a left ideal of B. Now, if $\mathrm{L}_i(B,B)\neq 0$, then we have that

$$L_{i+1}(B,B)=[\mathrm{L}_i(B,B),B]=[B^{i+1},B]\leq [B^{i+1},G]\lneq B^{i+1}=\mathrm{L}_i(B,B)$$

applying [22, 5.1.6 (iii)]. Thus, as B is finite, there exists a positive integer n such that $\mathrm{L}_n(B,B)=0$. □

Theorem 1.3.7. *Let $(B,+,\cdot)$ be a finite left brace and let p be a prime. Assume that $B_{p'}$ and B_p are the Hall p'-subgroup and Sylow p-subgroup of the group $(B,+)$, respectively. Then the following statements are equivalent:*

1. *B is a left p-nilpotent left brace.*
2. *$B_{p'}*B_p=0$.*
3. *$B_{p'}*\Omega((B_p,+))=0$, where $\Omega((B_p,+))$ is the group generated by all elements of order p in $(B_p,+)$.*
4. *The multiplicative group $(B,\cdot)$ is p-nilpotent.*

Proof. Let us start with 1 implies 2. If B is p-nilpotent, there exists a positive integer n with $\mathrm{L}_n(B, B_p) = 0$ and in particular, $\mathrm{L}_n(B_{p'}, B_p) = 0$. Considering the action of $(B_{p'}, \cdot)$ on $(B_p, +)$, we have that $\mathrm{L}_n(B_{p'}, B_p) = [B_p, B_{p'}, \ldots, B_{p'}] = 0$ and then we can apply [22, 8.2.7 (b)] to obtain that $B_{p'} * B_p = [B_p, B_{p'}] = 0$.

It is clear that 2 implies 3.

Let us continue with 3 implies 4. Considering again the action of $(B_{p'}, \cdot)$ on $(B_p, +)$, we have that

$$[\Omega((B_p, +)), B_{p'}] = B_{p'} * \Omega((B_p, +)) = 0.$$

It implies that $B_{p'}$ acts trivially on $\Omega((B_p, +))$. Then it follows from [22, 8.4.3] that $B_{p'}$ acts trivially on $(B_p, +)$, so that $B_{p'} * B_p = 0$. Hence we have $B_{p'} * B = B_{p'} * (B_p + B_{p'}) = B_{p'} * B_{p'} \subseteq B_{p'}$ and thus $B_{p'}$ is a right ideal of B. As by Example 1.1.9 we know that $B_{p'}$ is also a left ideal of B, we conclude that $B_{p'}$ is an ideal of B and so $(B_{p'}, \cdot)$ is a normal subgroup of $(B, \cdot)$. Hence $(B, \cdot)$ is p-nilpotent.

We finish with 4 implies 1. Since $(B, \cdot)$ is p-nilpotent, we have $(B_{p'}, \cdot)$ is a normal subgroup of $(B, \cdot)$ and by Example 1.1.9, $B_{p'}$ is a left ideal of B, which implies $B_{p'}$ is an ideal of B. Consequently, as B_p is a left ideal of B again by Example 1.1.9, we know that $B_{p'} * B_p \subseteq B_{p'} \cap B_p = 0$. Now we claim that

$$\mathrm{L}_n(B, B_p) = \mathrm{L}_n(B_p, B_p) \quad \text{for all } n \geq 1.$$

It suffices to prove that $\mathrm{L}_n(B, B_p) \subseteq \mathrm{L}_n(B_p, B_p)$ for all $n \geq 1$. We argue by induction on n. Assume that $n = 1$, let $x = ab \in B$, where $a \in B_p$ and $b \in B_{p'}$, and let $y \in B_p$. Then, by Lemma 1.1.16,

$$x * y = (ab) * y = a * (b * y) + a * y + b * y = a * y \in B_p * B_p$$

since $b * y = 0$. Thus we have $\mathrm{L}_1(B, B_p) = B * B_p \subseteq B_p * B_p = \mathrm{L}_1(B_p, B_p)$. Now we may assume that the result holds for $n - 1$. Arguing as above, we obtain that $B * \mathrm{L}_{n-1}(B_p, B_p) \subseteq B_p * \mathrm{L}_{n-1}(B_p, B_p)$. Therefore

$$\begin{aligned} \mathrm{L}_n(B, B_p) &= B * \mathrm{L}_{n-1}(B, B_p) \subseteq B * \mathrm{L}_{n-1}(B_p, B_p) \\ &\subseteq B_p * \mathrm{L}_{n-1}(B_p, B_p) = \mathrm{L}_n(B_p, B_p). \end{aligned}$$

Finally, since by Lemma 1.3.6 there exists an m such that $\mathrm{L}_m(B_p, B_p) = 0$, we have that $\mathrm{L}_m(B, B_p) = \mathrm{L}_m(B_p, B_p) = 0$. Consequently, B is a left p-nilpotent left brace and the circle of implications is complete. □

Now Smoktunowicz's result follows by Theorem 1.3.7 and Lemma 1.3.5.

Corollary 1.3.8 ([30, Theorem 1.1])**.** *A finite left brace B is left nilpotent if and only if its multiplicative group is nilpotent.*

Our next goal is to show that if the multiplicative group of a left brace has a Sylow tower, then this brace is solvable, but to achieve it, we will need the next result, that can be found as Proposition 4.2.1 in Bachiller's PhD Thesis [3].

Proposition 1.3.9. *Let B be a finite left brace. Assume that one of the Hall subgroups H of $(B,\cdot)$ is normal. Then, H is an ideal of B.*

Proof. As H is a Hall subgroup, we can assume that $|H| = n$ and $|B : H| = m$ with $(m, n) = 1$. In addition, we know that mB is a left ideal of B (see Example 1.1.9) of order n. Now, as H is a normal subgroup in $(B,\cdot)$, which is solvable, we have that H is the unique Hall subgroup of $(B,\cdot)$ of order n, and thus $H = (mB,\cdot)$. Then the result is clear because a left ideal with normal multiplicative group is an ideal. □

Proposition 1.3.10. *If $(B,+,\cdot)$ is a finite left brace and its multiplicative group $(B,\cdot)$ has a Sylow tower, then B is a solvable left brace.*

Proof. Provided that $(B,\cdot)$ has a Sylow tower, we can find a series

$$0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$$

with $B_i \trianglelefteq B$ for every $i \in \{0,\dots,m\}$ such that for every prime number p dividing the order of B, there exists a unique $k \in \{1,\dots,m\}$ such that B_k/B_{k-1} is isomorphic to a Sylow p-subgroup of B.

In particular, $B_1 = B_1/B_0$ is a normal Sylow p-subgroup of B for some p, and then by Proposition 1.3.9, B_1 is also an ideal of B, and then, an ideal of B_2.

Assume now that B_{k-1} is an ideal of B_k. As $B_{k-1} \trianglelefteq B$, we can consider the series

$$B_{k-1}/B_{k-1} \subseteq B_k/B_{k-1} \subseteq \cdots \subseteq B/B_{k-1},$$

and then B_k/B_{k-1} is a normal Sylow q-subgroup of B/B_{k-1} for some prime q, and again by Proposition 1.3.9, B_k/B_{k-1} is an ideal of B/B_{k-1} and of B_{k+1}/B_{k-1}. This means that, for all $a_k \in B_k$ and all $a_{k+1} \in B_{k+1}$, we have that

$$(a_kB_{k-1}) * (a_{k+1}B_{k-1}) = (a_k * a_{k+1})B_{k-1} \in B_k/B_{k-1} \Longrightarrow (a_k * a_{k+1}) \in B_k,$$
$$(a_{k+1}B_{k-1}) * (a_kB_{k-1}) = (a_{k+1} * a_k)B_{k-1} \in B_k/B_{k-1} \Longrightarrow (a_{k+1} * a_k) \in B_k,$$

which imply that B_k is an ideal of B_{k+1}.

In addition, as B_1 and B_2/B_1 have prime power order, they are left nilpotent left braces and then, they are solvable left braces. Now by Proposition 1.2.16, we know that B_2 is also a solvable left brace. Continuing in this way, we see that each B_i is solvable and, in particular, the original left brace $(B, +, \cdot)$ is solvable. □

Chapter 2

IYB-groups

In this chapter, we will recall the definitions and some properties of a certain subclass of the solutions of the Yang-Baxter equation, namely, the involutive, non-degenerate, set-theoretic ones, and we will see its connection with left braces. After that, we will study the notion of IYB-group and we will try to improve the knowledge about under which conditions a group factorized as a product of IYB-groups is again an IYB-group.

2.1 Solutions of the Yang-Baxter Equation

The quantum Yang-Baxter equation (YBE) is an important equation in mathematical physics that lays the foundations of some interesting mathematical theories, such as the theory of quantum groups. It appeared in the papers on statistical mechanics by C. N. Yang [34] and R. Baxter [10] and one of the fundamental open problems is to find all its solutions. However, following the idea of Drinfeld in [17], we will deal with the set-theoretic ones.

Definition 2.1.1. A *set-theoretic solution* of the Yang-Baxter equation is a pair (X, r), where X is a non-empty set and $r\colon X \times X \to X \times X$ is a map such that

$$r_{12} \circ r_{23} \circ r_{12} = r_{23} \circ r_{12} \circ r_{23}, \tag{2.1}$$

where $r_{12} = r \times \mathrm{id}$ and $r_{23} = \mathrm{id} \times r$. We will denote the components of the map r by $r(x, y) = (f_x(y), g_y(x))$, for any $x, y \in X$.

A subclass of this solutions, the involutive and non-degenerate ones, has received a lot of attention in last years because this type of solutions is of interest, not only for the applications of the YBE to physics, but also for its connections with some mathematical topics of recent interest such as radical

rings (we have already mentioned the paper by Rump, [27]), trifactorized groups ([31]), and Hopf algebras ([25]).

Definition 2.1.2. A solution (X, r) is *non-degenerate* if f_x, g_x are invertible for any $x \in X$ and we say that (X, r) is *involutive* if $r^2 = \mathrm{id}$.

From now on, we will always refer to involutive, non-degenerate set-theoretic solutions of the YBE, although we will call them just *solutions* for short.

Definition 2.1.3. Consider two solutions of the YBE (X, r) and (Y, s). A map $\varphi\colon X \to Y$ is called a *homomorphism of solutions* if $s(\varphi(x_1), \varphi(x_2)) = (\varphi \times \varphi)(r(x_1, x_2))$ for all $x_1, x_2 \in X$.

The following two results are well-known and follow directly from the definitions. We include them here because we will need them in Chapter 3.

Lemma 2.1.4. *Given a solution (X, r), if x, $y \in X$, then $f_x f_y = f_{f_x(y)} f_{g_y(x)}$ and $g_x g_y = g_{g_x(y)} g_{f_y(x)}$.*

Proof. Since r is a solution of the Yang-Baxter equation, by (2.1) we have that

$$\begin{aligned} r_{12}r_{23}r_{12}(x, y, z) &= r_{12}r_{23}(f_x(y), g_y(x), z) \\ &= f_{12}(f_x(y), f_{g_y(x)}(z), g_z(g_y(x))) \\ &= (f_{f_x(y)}(f_{g_y(x)}(z)), g_{f_{g_y(x)}(z)}(f_x(y)), g_z(g_y(x))) \end{aligned}$$

and

$$\begin{aligned} r_{23}r_{12}r_{23}(x, y, z) &= r_{23}r_{12}(x, f_y(z), g_z(y)) \\ &= r_{23}(f_x(f_y(z)), g_{f_y(z)}(x), g_z(y)) \\ &= (f_x(f_y(z)), f_{g_{f_y(z)}(x)}(g_z(y)), g_{g_z(y)}(g_{f_y(z)}(x))) \end{aligned}$$

coincide. We obtain the result by comparing the first and the third components of both triples. □

Lemma 2.1.5. *Given a solution (X, r), if x, $y \in X$, then $f_{f_x(y)}(g_y(x)) = x$ and $g_{g_y(x)}(f_x(y)) = y$. In particular, for every x, $y \in X$, $g_y(x) = f^{-1}_{f_x(y)}(x)$, $f_x(y) = g^{-1}_{g_y(x)}(y)$.*

Proof. Since (X, r) is involutive, $r^2(x, y) = (f_{f_x(y)}(g_y(x)), g_{g_y(x)}(f_x(y))) = (x, y)$. The second part is true because it is also non-degenerate. □

Etingof, Schedler, and Soloviev introduced in [19] two groups associated to a solution of the YBE. They are defined as follows: if (X, r) is a solution of the YBE, then its *structure group* $G(X, r)$ is the one defined by the presentation

$$G(X, r) = \langle X \mid xy = f_x(y)g_y(x), \text{ for } x, y \in X \rangle,$$

and its *permutation group* is

$$\mathcal{G}(X, r) = \langle f_x \mid x \in X \rangle,$$

which is a subgroup of the symmetric group Sym_X on X. These two groups are really important because they allow us to study the solutions of the Yang-Baxter equation from the group theory perspective. In addition, Cedó, Jespers, and Okniński proved in [14] that for every solution (X, r) of the YBE, both groups $G(X, r)$ and $\mathcal{G}(X, r)$ have a natural structure of left brace. In Chapter 3, we will describe this structure using a new approach.

On the other hand, in [14], the authors also proved that given a left brace, we can always construct a solutions of the YBE with the next result. Hence, left braces are a suitable structure to study these solutions.

Proposition 2.1.6. *Let B be a left brace and consider the map $r : B \times B \to B \times B$ defined by $r(x, y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x))$. Then (B, r) is a non-degenerate involutive set-theoretic solution of the Yang-Baxter equation.*

Proof. Let us denote $f_x(y) = \lambda_x(y)$ and $g_y(x) = \lambda^{-1}_{\lambda_x(y)}(x)$, as usual. Note that the following equation holds for any $x, y \in B$ because of the properties of left braces:

$$xy = \lambda_x(y) + x = \lambda_x(y)\lambda^{-1}_{\lambda_x(y)}(x) = f_x(y)g_y(x). \tag{2.2}$$

First of all, we shall see that both f_x and g_y are bijective for any $x, y \in X$. For f_x, the result is clear because $\lambda_x \in \mathrm{Aut}(B, +)$. The case of g_x is not immediate: we will find an equivalent expression for $g_x(y)$ and will give its inverse.

$$\begin{aligned} g_y(x) &= \lambda^{-1}_{\lambda_x(y)}(x) = \lambda^{-1}_{\lambda_x(y)}(\lambda_x(y) + x - \lambda_x(y)) \\ &= \lambda^{-1}_{\lambda_x(y)}(xy - \lambda_x(y)) = (\lambda_x(y))^{-1}(xy - \lambda_x(y)) - (\lambda_x(y))^{-1} \\ &= (\lambda_x(y))^{-1}xy = ((xy)^{-1}\lambda_x(y))^{-1} \\ &= ((xy)^{-1}(xy - x))^{-1} = (-y^{-1} + (xy)^{-1})^{-1} \\ &= (-y^{-1} + y^{-1}x^{-1})^{-1} = (y^{-1}(x^{-1} + y))^{-1}. \end{aligned} \tag{2.3}$$

With this, it is easy to check that $g_y^{-1}(x) = (yx^{-1} - y)^{-1}$ is the inverse of $g_y(x)$ and hence g_y is bijective.

Next, let us see that r satisfies Equation (2.1), or equivalently, that the next three equations hold (see the proof of Lemma 2.1.4) for any $x, y, z \in X$:

$$\begin{aligned} f_x \circ f_y &= f_{f_x(y)} \circ f_{g_y(x)}; \\ g_{f_{g_y(x)}(z)}(f_x(y)) &= f_{g_{f_y(z)}(x)}(g_z(y)); \\ g_z \circ g_y &= g_{g_z(y)} \circ g_{f_y(z)}. \end{aligned}$$

The first one follows using Equation (2.2) and from the fact that λ is a homomorphism of groups (see Proposition 1.1.5):

$$f_x \circ f_y = \lambda_x \circ \lambda_y = \lambda_{xy} = \lambda_{f_x(y)g_y(x)} = \lambda_{f_x(y)} \circ \lambda_{g_y(x)} = f_{f_x(y)} \circ f_{g_y(x)}.$$

Let us see the second one. On the one hand,

$$\begin{aligned} g_{f_{g_y(x)}(z)}(f_x(y)) &= \lambda^{-1}_{\lambda_{f_x(y)}(f_{g_y(x)}(z))}(f_x(y)) \\ &= \lambda^{-1}_{f_{f_x(y)}(f_{g_y(x)}(z))}(f_x(y)) \\ &= \lambda^{-1}_{f_x(f_y(z))}(f_x(y)). \end{aligned}$$

On the other hand,

$$\begin{aligned} f_{g_{f_y(z)}(x)}(g_z(y)) &= f_{g_{f_y(z)}(x)}(\lambda^{-1}_{\lambda_y(z)}(y)) \\ &= \lambda_{g_{f_y(z)}(x)}(\lambda_{(\lambda_y(z))^{-1}}(y)) \\ &= \lambda_{g_{f_y(z)}(x)(\lambda_y(z))^{-1}}(y) \\ &= \lambda_{((f_y(z))^{-1}(x^{-1}+f_y(z)))^{-1}(\lambda_y(z))^{-1}}(y) \quad \text{(by Equation (2.3))} \\ &= \lambda_{(x^{-1}+f_y(z))^{-1}f_y(z)(f_y(z))^{-1}}(y) \\ &= \lambda_{(x^{-1}+f_y(z))^{-1}}(y) \\ &= \lambda_{(x^{-1}\lambda_x(f_y(z)))^{-1}}(y) \\ &= \lambda_{(f_x(f_y(z)))^{-1}x}(y) \\ &= \lambda^{-1}_{f_x(f_y(z))}(\lambda_x(y)) \\ &= \lambda^{-1}_{f_x(f_y(z))}(f_x(y)). \end{aligned}$$

To obtain the third one, we will use Equation (2.3) repeatedly to prove that $g_{yz} = g_z \circ g_y$:

$$\begin{aligned} g_z(g_y(x)) &= g_z((y^{-1}(x^{-1}+y))^{-1}) = (z^{-1}(y^{-1}(x^{-1}+y)+z))^{-1} \\ &= (z^{-1}y^{-1}(x^{-1}+y)-z^{-1})^{-1} = ((yz)^{-1}x^{-1}-(yz)^{-1})^{-1} \\ &= ((yz)^{-1}(x^{-1}+yz))^{-1} = g_{yz}(x). \end{aligned}$$

Hence,

$$g_z \circ g_y = g_{yz} = g_{f_y(z)g_z(y)} = g_{g_z(y)} \circ g_{f_y(z)},$$

as desired.

Finally, by direct computation, $r^2 = \mathrm{id}$. Thus, (B, r) is a non-degenerate involutive set-theoretic solution of the YBE. □

Definition 2.1.7. Let B be a left brace. The set-theoretic solution of the Yang-Baxter equation (B, r) defined in the former proposition is called the solution of the Yang-Baxter equation associated to the left brace B.

We finish this section by recalling the definitions of retract relation, retraction of a solution and multipermutation solution. We will also recall some results which will help us relate multipermutation solutions with right nilpotent left braces.

Definition 2.1.8. Let (X, r) be a solution of the YBE. The equivalence relation on X given by $x \sim y$ if and only if $f_x = f_y$, is called the *retract relation*. The solution induced by this equivalence relation is the *retraction* of (X, r) and is denoted by $\mathrm{Ret}(X, r)$. In Section 3.5 we will prove that $\mathrm{Ret}(X, r)$ is indeed a well-defined solution.

In addition, one defines recursively $\mathrm{Ret}^{m+1}(X, r) = \mathrm{Ret}(\mathrm{Ret}^m(X, r))$ for all m. A solution (X, r) of the YBE is said to be a *multipermutation* solution of level m if m is the minimal positive integer such that $\mathrm{Ret}^m(X, r)$ has only one element. In this case, the *multipermutation level* is denoted by $\mathrm{mpl}(X, r) = m$. A solution (X, r) of the YBE is said to be *irretractable* if $\mathrm{Ret}(X, r) = (X, r)$.

Proposition 2.1.9 ([14, Lemma 3[1]])**.** *Let B be a left brace and let (B, r) be the solution of the YBE associated to B. If $(B/\operatorname{Soc}(B), r')$ is the solution of the YBE associated to the left brace $B/\operatorname{Soc}(B)$ then $(B/\operatorname{Soc}(B), r') = \mathrm{Ret}(B, r)$.*

Proof. First, let us see that $B/\!\sim$ and $B/\operatorname{Soc}(B)$ coincide as sets. If $a \in B$, its equivalence class is

$$\begin{aligned}[a] &= \{b \in B \mid \lambda_b = \lambda_a\} = \{b \in B \mid \lambda_{a^{-1}b} = \mathrm{id}\} \\ &= \{b \in B \mid a^{-1}b \in \operatorname{Soc}(B)\} = a \operatorname{Soc}(B),\end{aligned}$$

and thus $B/\!\sim = \{[a] \mid a \in B\} = \{a \operatorname{Soc}(B) \mid a \in B\} = B/\operatorname{Soc}(B)$.

[1] In fact, the original result is from Rump (see Proposition 7 in [27]), but we follow the notation of [14].

Now, if we call $\operatorname{Ret}(B,r) = (B/\!\sim, \tilde{r})$, it remains to prove that $\tilde{r}$ coincides with the solution associated to the left brace $B/\operatorname{Soc}(B)$, r'. Let $a, b \in B$, and let us call $\operatorname{Soc}(B) = S$ to simplify the notation. Then

$$\begin{aligned}
\tilde{r}([a],[b]) &= \Big([\lambda_a(b)], [\lambda^{-1}_{\lambda_a(b)}(a)]\Big) = \big([ab-a], [\lambda^{-1}_{ab-a}(a)]\big) \\
&= \big([ab-a], [(ab-a)^{-1}a - (ab-a)^{-1}]\big) \\
&= \big((ab-a)S, ((ab-a)^{-1}a - (ab-a)^{-1})S\big) \\
&= \big(aSbS - aS, (ab-a)^{-1}SaS - (ab-a)^{-1}S\big) \\
&= \Big(\lambda_{aS}(bS), \lambda^{-1}_{(ab-a)S}(aS)\Big) = \Big(\lambda_{aS}(bS), \lambda^{-1}_{\lambda_{aS}(bS)}(aS)\Big) \\
&= r'(aS, bS) = r'(a\operatorname{Soc}(B), b\operatorname{Soc}(B)),
\end{aligned}$$

as desired. □

Proposition 2.1.10 ([12, Proposition 6])**.** *Let B be a nonzero left brace and let (B,r) be its associated solution of the YBE. Then the multipermutation level of (B,r) is $m < \infty$ if and only if $B^{(m+1)} = 0$ and $B^{(m)} \neq 0$.*

Proof. We begin proving the direct implication by induction. If $\operatorname{mpl}(B,r) = 1$, then for all $a, b \in B$, $a \sim b$, that is, $\lambda_a = \lambda_b$. In particular, $\lambda_a = \lambda_1 = \mathrm{id}_B$ for all $a \in B$. With that, for any $a, b \in B$, $\lambda_a(b) = a * b + b = b$ and thus $a * b = 0$. Hence $B^{(2)} = 0$ and $B^{(1)} = B \neq 0$.

Assume that $\operatorname{mpl}(B,r) = m$. Then, by the definition of the retraction, $\operatorname{mpl}(\operatorname{Ret}(B,r)) = m - 1$. Recall that $\operatorname{Ret}(B,r) = (B/\operatorname{Soc}(B), r')$ by Proposition 2.1.9, where $(B/\operatorname{Soc}(B), r')$ is the solution of the YBE associated to the left brace $B/\operatorname{Soc}(B)$. We obtain by induction that $(B/\operatorname{Soc}(B))^{(m)} = 0$ and $(B/\operatorname{Soc}(B))^{(m-1)} \neq 0$. It can be proved easily that $(B/\operatorname{Soc}(B))^{(m)} = B^{(m)}/\operatorname{Soc}(B)$, hence we have that $B^{(m)} \subseteq \operatorname{Soc}(B)$ but $B^{(m-1)} \nsubseteq \operatorname{Soc}(B)$. Therefore, $B^{(m+1)} = B^{(m)} * B \subseteq \operatorname{Soc}(B) * B = 0$ and $B^{(m)} \neq 0$ because

$$\operatorname{Soc}(B) = \{a \in B \mid \lambda_a = \mathrm{id}_B\} = \{a \in B \mid a * b = 0, \forall b \in B\}.$$

Now, let us prove the inverse implication by induction too. If $B^{(2)} = 0$, $a * b = 0$ for all $a, b \in B$, so $\operatorname{Soc}(B) = B$ and thus $\operatorname{Ret}(B,r) = (B/\operatorname{Soc}(B), r')$ has just one element, that is, $\operatorname{mpl}(B,r) = 1$.

Assume $B^{(m+1)} = 0$ but $B^{(m)} \neq 0$. Provided that $B^{(m+1)} = B^{(m)} * B = 0$, we have that $B^{(m)} \subseteq \operatorname{Soc}(B)$ and then $(B/\operatorname{Soc}(B))^{(m)} = B^{(m)}/\operatorname{Soc}(B) = 0$. In a similar way, $B^{(m)} \neq 0$ implies $(B/\operatorname{Soc}(B))^{(m-1)} = B^{(m-1)}/\operatorname{Soc}(B) \neq 0$. Hence, by induction and Proposition 2.1.9 again, $\operatorname{mpl}(\operatorname{Ret}(B,r)) = m - 1$ and therefore $\operatorname{mpl}(B,r) = m$. □

Remark 2.1.11. It is obvious from last proposition that the solution associated to a left brace B is a multipermutation solution if, and only if, B is a right nilpotent left brace.

2.2 Involutive Yang-Baxter groups

Once recalled the definitions and some properties of the solutions of the Yang-Baxter equation, we come back to our main topic: left braces. Concretely, we will try to improve our knowledge about which groups can become IYB-groups.

Definition 2.2.1. A finite group G is called an *involutive Yang-Baxter group*, or simply an *IYB-group*, if G is isomorphic to the multiplicative group of a left brace.

The original definition of IYB-groups presented by Cedó, Jespers, and del Río in [13] is not exactly this one, but an equivalent one. Originally, a group G is an IYB-group if there exists an involutive non-degenerate solution of the Yang-Baxter equation (X, r) with $G \cong \mathcal{G}(X, r)$. In fact, the authors show in [13, Theorem 2.1] that both definitions are equivalent, and that IYB-groups are also related to other interesting concepts such as cycle sets, linear cycle sets or 1-cocycles. Another interesting and useful equivalence is the one proposed by Syzak in [32] considering trifactorized groups. However, the best one for our purposes is the approach using 1-cocycles, hence next we recall their definition and some elementary properties.

Recall that given a group G, a left G-module is a pair (V, ρ) where V is an abelian group and ρ is a left action of G on V which is compatible with the abelian structure of V, this is, $\rho\colon G \longrightarrow \mathrm{Sym}(V)$ is a group homomorphism such that $\rho_g(a+b) = \rho_g(a)+\rho_g(b)$ for all $g \in G$ and $a, b \in V$, where $\rho_g = \rho(g)$. We will usually denote $\rho_g(a)$ as ga. When there is no possible confusion, we omit the action an call the G-module just as V. We will also denote the kernel of the action as $\mathrm{Ker}(G \operatorname{on} V) = \mathrm{Ker}(\rho) = \{g \in G \mid \rho_g = \mathrm{id}_V\}$.

Definition 2.2.2. Let G be a group and let V be a G-module. A map $\pi\colon G \longrightarrow V$ such that $\pi(gh) = \pi(g) + g\pi(h)$ for every g, $h \in G$ is called a 1-*cocycle* or *derivation*.

Lemma 2.2.3. *Let G be a group, V be a G-module and $\pi\colon G \longrightarrow V$ a bijective* 1-cocycle. *Then, the following properties hold:*

1. $\pi(1_G) = 0_V$.
2. $g\pi(g^{-1}) = -\pi(g)$, *for all* $g \in G$.
3. *If* $x \in \mathrm{Ker}(G \operatorname{on} V)$ *and* $g \in G$, *then* $\pi(xg) = \pi(x) + \pi(g)$.
4. *If* $x \in \mathrm{Ker}(G \operatorname{on} V)$ *and* $g \in G$, *then* $\pi(gxg^{-1}) = g\pi(x)$.

Proof. Let v be an arbitrarily chosen element of V. Since π is bijective, there exists a unique $g \in G$ such that $v = \pi(g)$. Then,

$$\pi(1_G) + v = \pi(1_G) + 1_G\pi(g) = \pi(g) = v \Rightarrow \pi(1_G) = 0_V,$$

and the first statement holds. For the second one, if $g \in G$, we have:

$$0_V = \pi(1_G) = \pi(gg^{-1}) = \pi(g) + g\pi(g^{-1}) \Rightarrow g\pi(g^{-1}) = -\pi(g).$$

Now, if $x \in \mathrm{Ker}(G \operatorname{on} V)$, it is, x acts trivially on V, it is clear that

$$\pi(xg) = \pi(x) + x\pi(g) = \pi(x) + \pi(g),$$

and Statement 3 follows. Finally, we prove Statement 4:

$$\begin{aligned}\pi(gxg^{-1}) &= \pi(g) + g\pi(xg^{-1}) \\ &= \pi(g) + g(\pi(x) + \pi(g^{-1})) \\ &= \pi(g) + g\pi(g^{-1}) + g\pi(x) \\ &= \pi(gg^{-1}) + g\pi(x) = g\pi(x),\end{aligned}$$

as desired. □

Now we are ready to prove that IYB-groups are equivalent to bijective 1-cocycles.

Theorem 2.2.4. *A finite group G is an IYB-group if, and only if, there exist a left G-module V and a bijective 1-cocycle $\pi\colon G \longrightarrow V$.*

Proof. Assume that V is a left G-module and $\pi\colon G \longrightarrow V$ is a bijective 1-cocycle. Let us consider the following operation on G:

$$g_1 + g_2 = \pi^{-1}(\pi(g_1) + \pi(g_2)), \quad \text{for all } g_1, g_2 \in G.$$

We just need to prove that $(G, +, \cdot)$ is a left brace. Let $g_1, g_2, g_3 \in G$, then

$$\begin{aligned}g_1 + (g_2 + g_3) &= g_1 + \pi^{-1}(\pi(g_2) + \pi(g_3)) \\ &= \pi^{-1}(\pi(g_1) + \pi(\pi^{-1}(\pi(g_2) + \pi(g_3)))) \\ &= \pi^{-1}(\pi(g_1) + \pi(g_2) + \pi(g_3)) \\ &= \pi^{-1}(\pi(\pi^{-1}(\pi(g_1) + \pi(g_2))) + \pi(g_3)) \\ &= \pi^{-1}(\pi(g_1) + \pi(g_2)) + g_3 \\ &= (g_1 + g_2) + g_3,\end{aligned}$$

and hence the associativity holds. As $\pi(1_G) = 0_V$, it is easy to see that 1_G is the neutral element for this new operation. Also, if $g \in G$, $h = \pi^{-1}(-\pi(g))$ is

its symmetric element. Thus, $(G,+)$ is a group and it is abelian because V is. Finally, as $\pi(g_1 \cdot g_2) = \pi(g_1) + g_1\pi(g_2)$ implies $g_1 \cdot g_2 = \pi^{-1}(\pi(g_1) + g_1\pi(g_2))$, we have that

$$\begin{aligned} g_1 \cdot (g_2 + g_3) + g_1 &= \pi^{-1}(\pi(g_1) + g_1(\pi(g_2 + g_3))) + g_1 \\ &= \pi^{-1}(\pi(g_1) + g_1(\pi(\pi^{-1}(\pi(g_2) + \pi(g_3))))) + g_1 \\ &= \pi^{-1}(\pi(g_1) + g_1(\pi(g_2) + \pi(g_3))) + g_1 \\ &= \pi^{-1}(\pi(\pi^{-1}(\pi(g_1) + g_1(\pi(g_2) + \pi(g_3)))) + \pi(g_1)) \\ &= \pi^{-1}(\pi(g_1) + g_1(\pi(g_2)) + g_1(\pi(g_3)) + \pi(g_1)) \\ &= \pi^{-1}(\pi(g_1 \cdot g_2) + \pi(g_1 \cdot g_3)) \\ &= g_1 \cdot g_2 + g_1 \cdot g_3, \end{aligned}$$

and G is an IYB-group.

Conversely, if G is an IYB-group, there exists an addition on G such that $(G,+,\cdot)$ is a left brace, and then we can consider trivially $(G,+)$ as a G-module with respect to the left action λ. The map $\pi = \mathrm{id}\colon G \longrightarrow G$ is a bijective 1-cocycle:

$$\pi(gh) = gh = g + gh - g = g + \lambda_g(h) = \pi(g) + \lambda_g(\pi(h)) = \pi(g) + g\pi(h),$$

for all $g, h \in G$. □

Definition 2.2.5. The pair (V,π) of Theorem 2.2.4 will be called an *IYB-structure* on the group G.

The notion of IYB-structure was introduced by Eisele in [18] along with another quite useful notion to study IYB-groups: equivariant IYB-structures. Next, we define them, but we need to establish some notation before.

Notation 2.2.6. Suppose that a group A acts on the left on an IYB-group G with an IYB-structure (V,π). If $a \in A$ and $g \in G$, we denote with ${}^a g \in G$ the result of the action of $a \in A$ on $g \in G$.

Definition 2.2.7. Let A be a group acting on an IYB-group G with an IYB-structure (V,π). The IYB-structure (V,π) will be called *A-equivariant* if there exists a group action of A on V such that

$$\pi({}^a g) = a\pi(g)$$

for all $a \in A$, $g \in G$, where we denote with av the result of the action of $a \in A$ on $v \in V$. In fact, since π is bijective, such action of A on V is uniquely determined by the action of A on G by means of $av = \pi({}^a\pi^{-1}(v))$ for every $a \in A$, $v \in V$.

Definition 2.2.8. An IYB-structure (V, π) on a group G will be called *fully equivariant* if (V, π) is $\mathrm{Aut}(G)$-equivariant, under the natural action of $\mathrm{Aut}(G)$ on G. Note that in this case (V, π) will be A-equivariant for every group A acting on G.

In [19], Etingof, Schedler, and Soloviev showed that any IYB-group is a solvable group (recall Proposition 1.3.1) and implicitly asked whether the converse was also true, that is, whether every solvable group can be an IYB-group. Later, Cedó, Jespers, and del Río asked that same question explicitly in [13], and proved that abelian groups, nilpotent groups of class two, abelian-by-cyclic groups, and solvable A-groups[2] are IYB-groups. They also showed that every finite solvable group is isomorphic to a subgroup of an IYB-group. In addition, in [15] it is proved that all nilpotent groups of class three and odd order are IYB-groups, and in [18] Eisele proposed a way to show that all 2-groups of order up to and including 512 and all other p-groups of order strictly less than 1024 are IYB-groups using GAP.

All those results seemed to lead to a positive answer to the question. However, Bachiller found a counterexample in [2]: he showed that there exist a prime p and a p-group G of order p^{10} and nilpotency class 9 which is not an IYB-group. Thus, not every solvable group is an IYB-group. Nevertheless, another result from [13] motivated a new interesting question. The result says as follows.

Lemma 2.2.9 ([13, Corollary 3.1])**.** *If G is an IYB-group, then its Hall subgroups are also IYB-groups.*

Proof. By Theorem 2.2.4, as G is an IYB-group, we can find an IYB-structure (V, π). Then if W is a Hall subgroup of V, it is G-invariant and $H = \pi^{-1}(W)$ is a subgroup of G of the same order. With that, (W, π_H) is an IYB-structure on H, where π_H is the restriction of π to H, and thus H is an IYB-group. □

Therefore, as every IYB-group is solvable, applying Lemma 2.2.9, we know that every IYB-group is a product of two IYB-groups, and the following question arises.

Question 2.2.10. Let $G = NH$ be a finite group which is the product of the subgroups N and H. Assume that N and H are IYB-groups and N is normal in G. Under which conditions can we ensure that G is an IYB-group?

In this context, Cedó, Jespers, and del Río in [13] and Eisele in [18] proved the following results.

[2] A solvable A-group is a solvable group with all its Sylow subgroups abelian.

Theorem 2.2.11 ([13, Theorem 3.3]). *Let G be a finite group such that $G = AH$, where A is an abelian normal subgroup of G and H is an IYB-subgroup of G with associated IYB-structure (B, π) such that $H \cap A$ acts trivially on B. Then G is an IYB-group. In particular, every semidirect product $A \rtimes H$ of a finite abelian group A by an IYB-group H is an IYB-group.*

Theorem 2.2.12 ([18, Proposition 2.2]). *Let $G = [N]H$ be a finite group. If H is an IYB-group and N has an H-equivariant IYB-structure, then G is an IYB-group.*

Our goal from here to the end of this chapter will be proving a result in this same direction that significantly improves both Theorem 2.2.11 and Theorem 2.2.12 by removing the abelianity condition on N and the requirement for the group G to be a semidirect product. To achieve this aim, in the next subsection we will collect some examples and some preliminary results which we will need later. After that, in Subsection 2.2.2 we will prove our result and show some corollaries which help us obtain new families of IYB-groups. Finally, we construct in Subsection 2.2.3 a family of IYB-groups that appear as a consequence of our results, but cannot appear as a consequence of the results of [13] or [18].

In the sequel, all groups considered will be finite. The results from here to the end of the chapter have been published in [24].

2.2.1 Some examples and preliminary results

We begin with a lemma which makes it easier to see whether an IYB-structure on a group G is A-equivariant for a group A acting on G or not.

Lemma 2.2.13. *Let $(G, \cdot)$ be an IYB-group with IYB-structure (V, π) and let A be a group acting on G. Let us consider the left brace $(G, +, \cdot)$ with the addition in the proof of Theorem 2.2.4:*

$$g + h = \pi^{-1}(\pi(g) + \pi(h)) \quad \text{for all } g,\, h \in G.$$

Then (V, π) is A-equivariant if and only if A is a group of automorphisms of the left brace G.

Proof. Suppose that (V, π) is A-equivariant. Then there exists an action of A on V, whose result is denoted by av for $a \in A$, $v \in V$, such that

$$\pi({}^a g) = a\pi(g) \quad \text{for all } a \in A,\, g \in G.$$

Given g, $h \in G$ and $a \in A$,

$$\begin{aligned}\pi({}^a(g+h)) &= a\pi(g+h) = a(\pi(g)+\pi(h)) = a\pi(g)+a\pi(h)\\ &= \pi({}^ag)+\pi({}^ah) = \pi({}^ag+{}^ah).\end{aligned}$$

Since π is bijective, this implies that ${}^a(g+h) = {}^ag+{}^ah$. Hence the action of A on G preserves the addition, as desired.

Conversely, assume that A is a group of automorphisms of the left brace G. Let $a \in A$, $v \in V$. Since

$$\begin{aligned}\pi({}^a(\pi^{-1}(v)+\pi^{-1}(w))) &= \pi({}^a\pi^{-1}(v)+{}^a\pi^{-1}(w))\\ &= \pi({}^a\pi^{-1}(v))+\pi({}^a\pi^{-1}(w)),\end{aligned}$$

we have that the assignment $av = \pi({}^a\pi^{-1}(v))$, $a \in A$, $v \in V$, defines a group action of A on V. Moreover, given $a \in A$, $g \in G$, as $\pi(g) \in V$, we have that

$$a\pi(g) = \pi({}^a\pi^{-1}(\pi(g))) = \pi({}^ag),$$

which implies that (V,π) is A-equivariant. □

Now, we show some examples which will be useful to prove the corollaries of Theorem 2.2.20.

Example 2.2.14. Every abelian group G is an IYB-group. We can consider $V = G$ as a trivial G-module and take $\pi = \mathrm{id}_G$ as the bijective 1-cocycle. Thus, obviously, (V,π) is fully equivariant and $\mathrm{Ker}(G \operatorname{on} V) = G$.

Example 2.2.15 ([18, Remark 2.7])**.** Let $(G,\cdot)$ be an odd order nilpotent group of class two. Then for every element $g \in G$ there exists a unique element h such that $g = h^2$. We will denote it by $h = \sqrt{g}$. Let us define an addition $+$ on G by means of

$$g_1 + g_2 = g_1 g_2 \sqrt{[g_2, g_1]}.$$

It can be checked that $(G,+)$ is an abelian group. We give $V = (G,+)$ a structure of G-module by means of the law

$$\rho_g(v) = g \cdot v + g^{-1},$$

where $\rho_g = \rho(g)$ for $g \in G$ and $\rho\colon G \longrightarrow \mathrm{Sym}(V)$ is a group homomorphism. If we set $\pi = \mathrm{id}_G$, then (V,π) is a fully equivariant IYB-structure on G and $\mathrm{Ker}(G \operatorname{on} V) = \mathrm{Z}(G)$.

Note that the following example is a special case of [1].

Example 2.2.16. Suppose that $(G,\cdot)$ is a nilpotent group of class two. Set $Z = \mathrm{Z}(G)$ and write $G/Z = \langle a_1 Z\rangle \times \cdots \times \langle a_n Z\rangle$. Thus every element of G can be written in the form $a_1^{t_1}\cdots a_n^{t_n} z$, where $z \in Z$. We can define an addition on G by means of

$$a_1^{t_1}\cdots a_n^{t_n} z + a_1^{s_1}\cdots a_n^{s_n} z' = a_1^{t_1+s_1}\cdots a_n^{t_n+s_n} zz'.$$

It is not difficult to check that $(G,+,\cdot)$ is a two-side brace. We give $V = (G,+)$ a structure of G-module by means of the following law:

$$\rho_g(v) = g\cdot v - g = v \prod_{1\le j<i\le n} [a_i, a_j]^{t_i s_j},$$

where $\rho_g = \rho(g)$, $\rho\colon G \longrightarrow \mathrm{Sym}(V)$ is a homomorphism, $g = a_1^{t_1}\cdots a_n^{t_n} z \in G$ and $v = a_1^{s_1}\cdots a_n^{s_n} z' \in V$. If we set $\pi = \mathrm{id}_G$, we have that (V,π) is an IYB-structure on G.

Definition 2.2.17. An automorphism α of a group G is called *central* if $\alpha(g)g^{-1} \in \mathrm{Z}(G)$ for all $g \in G$. The set of all central automorphisms of G is denoted by $\mathrm{Aut}_c(G)$ and is a normal subgroup of $\mathrm{Aut}(G)$ (for example, see [28]).

Proposition 2.2.18. *Let $(G,\cdot)$ be a nilpotent group of class two. There exists an IYB-structure (V,π) on G such that (V,π) is $\mathrm{Aut}_c(G)$-equivariant and $\mathrm{Z}(G) \subseteq \mathrm{Ker}(G \operatorname{on} V)$.*

Proof. Write $A = \mathrm{Aut}_c(G)$ and choose the IYB-structure (V,π) on G as defined in Example 2.2.16. It is not difficult to see that $\mathrm{Z}(G) \subseteq \mathrm{Ker}(G \operatorname{on} V)$. We must only show that (V,π) is A-equivariant. By Lemma 2.2.13, it suffices to show that every central automorphism preserves the addition on G defined in Example 2.2.16. Let $g = a_1^{t_1}\cdots a_n^{t_n} z$, $h = a_1^{s_1}\cdots a_n^{s_n} z' \in G$, where $z, z' \in \mathrm{Z}(G)$ and $\alpha \in A$. As α is central, we may assume that $\alpha(a_i) = a_i z_i$, where $z_i \in \mathrm{Z}(G)$, $i = 1,\ldots,n$.

$$\begin{aligned}
\alpha(g+h) &= \alpha(a_1^{t_1+s_1}\cdots a_n^{t_n+s_n} zz')\\
&= \alpha(a_1)^{t_1+s_1}\cdots\alpha(a_n)^{t_n+s_n}\alpha(z)\alpha(z')\\
&= (a_1z_1)^{t_1+s_1}\cdots(a_nz_n)^{t_n+s_n}\alpha(z)\alpha(z')\\
&= a_1^{t_1+s_1}\cdots a_n^{t_n+s_n} z_1^{t_1}\cdots z_n^{t_n}\alpha(z) z_1^{s_1}\cdots z_n^{s_n}\alpha(z')\\
&= a_1^{t_1}\cdots a_n^{t_n} z_1^{t_1}\cdots z_n^{t_n}\alpha(z) + a_1^{s_1}\cdots a_n^{s_n} z_1^{s_1}\cdots z_n^{s_n}\alpha(z')\\
&= (a_1z_1)^{t_1}\cdots(a_nz_n)^{t_n}\alpha(z) + (a_1z_1)^{s_1}\cdots(a_nz_n)^{s_n}\alpha(z')\\
&= \alpha(a_1)^{t_1}\cdots\alpha(a_n)^{t_n}\alpha(z) + \alpha(a_1)^{s_1}\cdots\alpha(a_n)^{s_n}\alpha(z')\\
&= \alpha(g) + \alpha(h),
\end{aligned}$$

as desired. □

We end this subsection with a necessary lemma for the proof of our main theorem.

Lemma 2.2.19. *Let A be a group acting on a group G with A-equivariant IYB-structure (V, π), which determines the unique action of A on V. Then for every $a \in A$, $g \in G$ and $v \in V$,*

$$({}^a g)v = a(g(a^{-1}v)).$$

Proof. Since $a^{-1}v \in V$ and π is bijective, we may assume that $\pi(x) = a^{-1}v$ for some $x \in G$. Note that $g\pi(x) = \pi(gx) - \pi(g)$. Hence we have

$$\begin{aligned} a(g(\pi(x))) &= a\pi(gx) - a\pi(g) \\ &= \pi({}^a(gx)) - \pi({}^a g) \\ &= \pi(({}^a g)({}^a x)) - \pi({}^a g) \\ &= ({}^a g)\pi({}^a x) = ({}^a g)a\pi(x). \end{aligned}$$

Note that $a\pi(x) = v$, and thus $({}^a g)v = ({}^a g)a\pi(x) = a(g(\pi(x))) = a(g(a^{-1}v))$, as desired. □

2.2.2 New results on IYB-groups

We are now ready to state and prove our main theorem in the direction of solving Question 2.2.10.

Theorem 2.2.20. *Suppose that the group A acts on the group $G = NH$, where N and H are A-invariant subgroups of G and $N \trianglelefteq G$. Suppose that N and H are IYB-groups with A-equivariant IYB-structures (U, π_N) and (V, π_H), respectively, satisfying the following conditions:*

(C1) $N \cap H \subseteq \mathrm{Ker}(\mathrm{Z}(N) \operatorname{on} U) \cap \mathrm{Ker}(H \operatorname{on} V)$.

(C2) *(U, π_N) is also an H-equivariant IYB-structure on N with respect to the action by conjugation of H on N: ${}^h n = hnh^{-1}$ for $n \in N$, $h \in H$.*

Then G has an A-equivariant IYB-structure (W, π) such that

$$\mathrm{Ker}(N \operatorname{on} U)\, \mathrm{C}_{\mathrm{Ker}(H \operatorname{on} V)}(N) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

Proof. Note that, since (U, π_N) and (V, π_H) are A-equivariant, there exist actions of A on U and V such that $\pi_N({}^a n) = a\pi_N(n)$ and $\pi_H({}^a h) = a\pi_H(h)$ for all $a \in A, n \in N$ and $h \in H$. Thus we can view $U \oplus V$ as an A-module via the law:

$$a(u, v) = (au, av), a \in A, (u, v) \in U \oplus V.$$

Let us consider $X = \{(\pi_N(x^{-1}), \pi_H(x)) \in U \oplus V : x \in H \cap N\}$. By hypothesis (C1), $N \cap H$ acts trivially on U and V, and $N \cap H \subseteq \mathrm{Z}(N)$. Note that for every x, $y \in N \cap H$, it follows from Lemma 2.2.3 (3) that

$$\begin{aligned}(\pi_N(x^{-1}), \pi_H(x)) + (\pi_N(y^{-1}), \pi_H(y)) &= (\pi_N(x^{-1}y^{-1}), \pi_H(xy)) \\ &= (\pi_N((xy)^{-1}), \pi_H(xy)) \in X.\end{aligned}$$

Moreover, if $a \in A$ and $x \in N \cap H$,

$$a(\pi_N(x^{-1}), \pi_H(x)) = (a\pi_N(x^{-1}), a\pi_H(x)) = (\pi_N({}^a(x)^{-1}), \pi_H({}^a x)) \in X.$$

Hence, X is an A-submodule of $U \oplus V$.

Consider the quotient A-module $W = (U \oplus V)/X$. By hypothesis (C2), there exists a unique action of H on U such that $\pi_N({}^h n) = h\pi_N(n)$ for every $h \in H$, $n \in N$, where hu denotes the result of the action of $h \in H$ on $u \in U$. Now we consider the assignment $G \times W \longrightarrow W$ given by

$$(g, (u, v) + X) \mapsto g((u, v) + X) = (n(hu), hv) + X,$$

where $g = nh$, $n \in N$, $h \in H$ and $(u, v) \in U \oplus V$. We need to check that this assigment is an action of G on W. We first prove that it is a well-defined map: let $g = nh = n'h'$ and suppose that $(u, v) + X = (u', v') + X$, where $n' \in N$, $h' \in H$, $(u', v') \in U \oplus V$. It suffices to show that

$$(n(hu), hv) + X = (n'(h'u'), h'v') + X.$$

Write $t = n^{-1}n' = h(h')^{-1} \in N \cap H$ and so t acts trivially on U and V. Thus $h'u' = (t^{-1}h)u' = t^{-1}(hu') = hu'$ and $h'v' = t^{-1}(hv') = hv'$. Furthermore, $n'(h'u') = n(t(hu')) = n(hu')$. Hence it is enough to show that

$$(n(h(u - u')), h(v - v')) \in X.$$

Note that as $(u - u', v - v') \in X$, there exists some $x \in N \cap H$ such that $u - u' = \pi_N(x^{-1})$ and $v - v' = \pi_H(x)$. Also, by hypothesis (C2), $h\pi_N(x^{-1}) = \pi_N(hx^{-1}h^{-1})$. Now, as both $hx^{-1}h^{-1}$ and x act trivially on U and V, it follows from Lemma 2.2.3 (4) that $n\pi_N(hx^{-1}h^{-1}) = \pi_N(nhx^{-1}h^{-1}n^{-1})$ and $h\pi_H(x) = \pi_H(hxh^{-1})$. Since $hxh^{-1} \in \mathrm{Z}(N)$, we can conclude that

$$\begin{aligned}(n(h(u - u')), h(v - v')) &= (n(h\pi_N(x^{-1})), h\pi_H(x)) \\ &= (\pi_N((hxh^{-1})^{-1}), \pi_H(hxh^{-1})) \in X,\end{aligned}$$

so this assignment is a map from $G \times W$ to W.

Next, let us check that it is indeed an action. Let $g_1 = n_1h_1$ and $g_2 = n_2h_2$ with $n_i \in N$ and $h_i \in H$, and $(u, v) + X \in W$. It follows that

$$\begin{aligned}(g_1g_2)((u,v)+X) &= (n_1h_1n_2h_1^{-1}h_1h_2)((u,v)+X)\\ &= ((n_1h_1n_2h_1^{-1})((h_1h_2)u), (h_1h_2)v) + X\\ &= (n_1({}^{h_1}n_2((h_1h_2)u)), h_1(h_2v)) + X\\ &= (n_1(h_1(n_2(h_2u))), h_1(h_2v)) + X\\ &= g_1((n_2(h_2u), h_2v) + X)\\ &= g_1(g_2((u,v)+X)),\end{aligned}$$

where the fourth equality holds by Lemma 2.2.19. Hence this map is an action of G on W, as desired, and it is easy to see that $N \cap H \subseteq \mathrm{Ker}(G \operatorname{on} W)$.

Our next step is to define a bijective 1-cocycle from G to W. Consider the assignment $\pi\colon G \longrightarrow W$ given by

$$\pi(g) = (\pi_N(n), \pi_H(h)) + X,$$

where $g = nh$, $n \in N$, $h \in H$. The first thing to show is that π is a map. Note that if $g = nh = n'h'$ with $n, n' \in N$ and $h, h' \in H$, we have that $z = n^{-1}n' = h((h')^{-1}) \in N \cap H \subseteq \mathrm{Z}(N)$, and $z^{-1} = n'^{-1}n = n'(n')^{-1}n(n')^{-1} = n(n')^{-1}$. The fact that $H \cap N$ acts trivially on U and V implies that

$$\begin{aligned}\pi_N(z^{-1}) &= \pi_N(n(n')^{-1})\\ &= \pi_N(n) + n\pi_N((n')^{-1})\\ &= \pi_N(n) + n'(z^{-1}\pi_N((n')^{-1}))\\ &= \pi_N(n) + n'\pi_N((n')^{-1})\\ &= \pi_N(n) - \pi_N(n'),\end{aligned}$$

where the last equality follows by Lemma 2.2.3 (2), and by a similar calculation, we have that $\pi_H(z) = \pi_H(h) - \pi_H(h')$. As

$$\begin{aligned}\pi(nh) = \pi(n'h') &\iff (\pi_N(n), \pi_H(h)) + X = (\pi_N(n'), \pi_H(h')) + X\\ &\iff (\pi_N(n) - \pi_N(n'), \pi_H(h) - \pi_H(h')) \in X\\ &\iff (\pi_N(z^{-1}), \pi_H(z)) \in X,\end{aligned}$$

and the last line is true by definition of X, we have that the assignment π is a map between G and W.

Secondly, given $(u, v) + X \in W$, as π_N and π_H are bijective, we can take $g = \pi_N^{-1}(u)\pi_H^{-1}(v)$ and clearly $\pi(g) = (u, v) + X$, hence π is surjective. Furthermore, as

$$|G| = \frac{|N||H|}{|N \cap H|} = \frac{|U||V|}{|X|} = |W|,$$

we conclude that π is bijective.

Finally, we prove that π is a 1-cocycle of the G-module W. Let $g_1 = n_1h_1$ and $g_2 = n_2h_2$, with $n_i \in N$ and $h_i \in H$. Then

$$\begin{aligned}\pi(g_1g_2) &= \pi(n_1h_1n_2h_2) = \pi(n_1h_1n_2h_1^{-1}h_1h_2)\\ &= (\pi_N(n_1h_1n_2h_1^{-1}), \pi_H(h_1h_2)) + X\\ &= ((\pi_N(n_1), \pi_H(h_1)) + X) + ((n_1\pi_N(h_1n_2h_1^{-1}), h_1\pi_H(h_2)) + X)\\ &= \pi(g_1) + ((n_1(h_1\pi_N(n_2)), h_1\pi_H(h_2)) + X)\\ &= \pi(g_1) + g_1((\pi_N(n_2), \pi_H(h_2)) + X)\\ &= \pi(g_1) + g_1\pi(g_2).\end{aligned}$$

Hence (W, π) is an IYB-structure on G. Let us show that it is A-equivariant. Let $g = nh \in G$ with $n \in N, h \in H$ and $a \in A$. Recalling the action of A on W above, we easily conclude that

$$\begin{aligned}a\pi(g) &= a((\pi_N(n), \pi_H(h)) + X) = (a\pi_N(n), a\pi_H(h)) + X\\ &= (\pi_N({}^an), \pi_H({}^ah)) + X = \pi({}^an{}^ah) = \pi({}^ag),\end{aligned}$$

as desired.

The last part is to check that

$$\mathrm{Ker}(N \operatorname{on} U)\, \mathrm{C}_{\mathrm{Ker}(H \operatorname{on} V)}(N) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

Take $g = nh$ with $n \in \mathrm{Ker}(N \operatorname{on} U)$ and $h \in \mathrm{C}_{\mathrm{Ker}(H \operatorname{on} V)}(N)$, and let $(u, v)+X$ be any element of W. As π_N is bijective, there exists a unique $n' \in N$ such that $\pi_N(n') = u$. Thus, since n acts trivially on U and h acts trivially on V and centralizes N, we have that

$$\begin{aligned}g((u, v) + X) &= (n(hu), hv) + X = (hu, v) + X = (h\pi_N(n'), v) + X\\ &= (\pi_N({}^hn'), v) + X = (\pi_N(n'), v) + X = (u, v) + X\end{aligned}$$

and the theorem is proved. □

Next, we consider some interesting consequences. Our first corollary shows that the direct product case follows directly from Theorem 2.2.20.

Corollary 2.2.21. *Let a group A act on a group $G = N \times H$ which is the direct product of two A-invariant subgroups N and H. Suppose that N, and H are IYB-groups with A-equivariant IYB-structures (U, π_N) and (V, π_H), respectively. Then G has an A-equivariant IYB-structures (W, π_G) such that*

$$\mathrm{Ker}(N \operatorname{on} U)\, \mathrm{Ker}(H \operatorname{on} V) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

The next result appears as a consequence of Corollary 2.2.21.

Corollary 2.2.22. *Let G be a nilpotent group of class two with an abelian Sylow 2-subgroup. Then G has a fully equivariant IYB-structure (W, π_G) such that $\mathrm{Z}(G) \subseteq \mathrm{Ker}(G \operatorname{on} W)$.*

Proof. We call $N = \mathrm{O}_2(G)$ and $H = \mathrm{O}_{2'}(G)$. Then, $G = N \times H$, N is abelian and H is an odd order nilpotent group of class two. By Example 2.2.14, N has a fully equivariant IYB-structure (U, π_N) with $\mathrm{Ker}(N \operatorname{on} U) = N$. Also, by Example 2.2.15, H has a fully equivariant IYB-structure (V, π_H) with $\mathrm{Ker}(H \operatorname{on} V) = \mathrm{Z}(H)$. Taking $A = \mathrm{Aut}(G)$ and applying Corollary 2.2.21, we have that G has a fully equivariant IYB-structure (W, π_G) such that $\mathrm{Ker}(N \operatorname{on} U)\,\mathrm{Ker}(H \operatorname{on} V) \subseteq \mathrm{Ker}(G \operatorname{on} W)$. Finally, note that

$$\mathrm{Z}(G) = \mathrm{Z}(N)\,\mathrm{Z}(H) \subseteq N\,\mathrm{Z}(H) = \mathrm{Ker}(N \operatorname{on} U)\,\mathrm{Ker}(H \operatorname{on} V) \subseteq \mathrm{Ker}(G \operatorname{on} W).$$

□

The following corollary is an extension of Theorem 2.2.11.

Corollary 2.2.23. *Let $G = NH$ be a group such that N is a nilpotent normal subgroup of class two and H is an IYB-group with IYB-structure (V, π). Assume that the following conditions hold:*

1. *$N \cap H \subseteq \mathrm{Z}(N)$;*
2. *$[H, \mathrm{O}_2(N)] \subseteq \mathrm{Z}(N)$;*
3. *$H \cap N$ acts trivially on V.*

Then G is an IYB-group.

Proof. Name $N_1 = \mathrm{O}_2(N)$ and $N_2 = \mathrm{O}_{2'}(N)$ and note that $N = N_1 \times N_2$. Consider the action of H on N via conjugation: both N_1 and N_2 are H-invariant. As N_2 is nilpotent of class two with odd order, by Example 2.2.15, there exists a fully equivariant (and of course, H-equivariant) IYB-structure (U_2, π_{N_2}) on N_2 such that $\mathrm{Ker}(N_2 \operatorname{on} U_2) = \mathrm{Z}(N_2)$.

Note that $[H, N_1] \subseteq \mathrm{Z}(N) \cap N_1 = \mathrm{Z}(N_1)$, which means that every element of H acts on N_1 as a central automorphism. Then, by Example 2.2.16 and Proposition 2.2.18, there exists an $\mathrm{Aut}_c(N_1)$-equivariant (and hence also H-equivariant) IYB-structure (U_1, π_{N_1}) on N_1 with $\mathrm{Z}(N_1) \subseteq \mathrm{Ker}(N_1 \operatorname{on} U_1)$.

Applying Corollary 2.2.21, we obtain that N has an H-equivariant IYB-structure, (U, π_N) say, such that

$$\mathrm{Z}(N) = \mathrm{Z}(N_1)\,\mathrm{Z}(N_2) \subseteq \mathrm{Ker}(N_1 \operatorname{on} U_1)\,\mathrm{Ker}(N_2 \operatorname{on} U_2) \subseteq \mathrm{Ker}(N \operatorname{on} U).$$

Since $N \cap H$ is contained in $\mathrm{Z}(N)$ and acts trivially on V by conditions 1 and 3, we have that $N \cap H \subseteq \mathrm{Ker}(\mathrm{Z}(N) \operatorname{on} U) \cap \mathrm{Ker}(H \operatorname{on} V)$. Applying Theorem 2.2.20 for $A = 1$, we conclude that G is an IYB-group. □

Note that [13, Corollary 3.10] is a special case of the following result.

Corollary 2.2.24. *Let $G = NH$ be a group such that N and H are two nilpotent subgroups of class two and N is normal in G. If $N \cap H \subseteq \mathrm{Z}(G)$ and $[H, \mathrm{O}_2(N)] \subseteq \mathrm{Z}(N)$, then G is an IYB-group.*

Proof. As H is a nilpotent group of class two, it follows from Example 2.2.16 and Proposition 2.2.18 that there exists an IYB-structure (V, π_H) on H such that $\mathrm{Z}(H) \subseteq \mathrm{Ker}(H \operatorname{on} V)$. Since $N \cap H \subseteq \mathrm{Z}(G)$, we have that $N \cap H$ is contained in $\mathrm{Z}(N)$ and $\mathrm{Z}(H)$, which acts trivially on V. By Corollary 2.2.23, G is an IYB-group. □

Corollary 2.2.25. *Let a group $G = N_1 N_2 \cdots N_s$ be the product of s subgroups $N_1, \ldots, N_s$ satisfying*

1. *N_i is a nilpotent group of class two with an abelian Sylow 2-subgroup, for all $i = 1, \ldots, s$;*
2. *N_i is normalized by N_j, for all $1 \leq i < j \leq s$;*
3. *$N_1 \cdots N_i \cap N_{i+1} = \mathrm{Z}(G)$, for all $i = 1, \ldots, s-1$.*

Then G is an IYB-group.

Proof. Write $X_i = N_1 \cdots N_i$ and $H_i = N_{i+1} \cdots N_s$ for all $i = 1, \ldots, s$, where $H_s = N_{s+1} = 1$. We will use induction on i to prove the following result:

$$X_i \text{ has an } H_i\text{-equivariant IYB-structure } (U_i, \pi_i) \text{ such that } \mathrm{Z}(G) \subseteq \mathrm{Ker}(X_i \operatorname{on} U_i).$$

When $i = s$, we will have that G is an IYB-group.

For $i = 1$, X_1 has a fully-equivariant (then H_1-equivariant) IYB-structure (U_1, π_1) with $\mathrm{Z}(X_1) \subseteq \mathrm{Ker}(X_1 \operatorname{on} U_1)$ by Corollary 2.2.22. Also, by condition 3, $\mathrm{Z}(G) = X_1 \cap N_2$. Thus, $\mathrm{Z}(G) \subseteq \mathrm{Z}(X_1) \subseteq \mathrm{Ker}(X_1 \operatorname{on} U_1)$.

Assume it is true for the case $i-1$, this is, X_{i-1} has an H_{i-1}-equivariant IYB-structure (U_{i-1}, π_{i-1}) with $\mathrm{Z}(G) \subseteq \mathrm{Ker}(X_{i-1} \operatorname{on} U_{i-1})$. As $H_i \leq H_{i-1}$, we have that (U_{i-1}, π_{i-1}) is H_i-equivariant too. Note that H_i acts on the group $X_i = X_{i-1} N_i$, where $X_{i-1} \trianglelefteq X_i$, and X_{i-1} and N_i are H_i-invariant by condition 2. Applying again Corollary 2.2.22, N_i has a fully equivariant IYB-structure (V_i, ϕ_i) such that $\mathrm{Z}(N_i) \subseteq \mathrm{Ker}(N_i \operatorname{on} V_i)$. Since

$$X_{i-1} \cap N_i = \mathrm{Z}(G) \subseteq \mathrm{Ker}(\mathrm{Z}(X_{i-1}) \operatorname{on} U_{i-1}) \cap \mathrm{Ker}(N_i \operatorname{on} V_i),$$

it follows from Theorem 2.2.20 that X_i has an H_i-equivariant IYB-structure (U_i, π_i) such that $\mathrm{Ker}(X_{i-1} \operatorname{on} U_{i-1})\, \mathrm{C}_{\mathrm{Ker}(N_i \operatorname{on} V_i)}(X_{i-1}) \subseteq \mathrm{Ker}(X_i \operatorname{on} U_i)$. And finally, note that

$$\mathrm{Z}(G) \subseteq \mathrm{Ker}(\mathrm{Z}(X_{i-1}) \operatorname{on} U_{i-1}) \subseteq \mathrm{Ker}(X_{i-1} \operatorname{on} U_{i-1}) \subseteq \mathrm{Ker}(X_i \operatorname{on} U_i),$$

as desired. □

2.2.3 A concrete example

We close this chapter studying the following example, which shows that Theorem 2.2.20 actually improves Theorem 2.2.11 and Theorem 2.2.12.

Example 2.2.26. Let $p \geq 3$ be a prime, let $m \geq 2$ be a natural number and let G be the group with the following presentation

$$G = \langle a, b, c \mid a^{p^m} = b^{p^m} = 1,\, c^{p^m} = a^{p^{m-1}},\ a^b = a^{1+p^{m-1}},\\ a^c = aa^{-p}b^{-p},\ b^c = ba \rangle.$$

Then G is a group of order p^{3m} and nilpotency class $2m$ with derived subgroup $G' = \langle b^p, a \rangle$ and Frattini subgroup $\Phi(G) = \langle c^p, b^p, a \rangle$. Let $N = \langle a, b \rangle$ and let $H = \langle c \rangle$. Then $G = NH$, N is a normal subgroup of G, N is nilpotent of class two (in fact, a minimal non-abelian group) and $N \cap H = \langle c^{p^m} \rangle \subseteq \mathrm{Z}(G)$. By Corollary 2.2.24, G is an IYB-group.

Claim 1. The group G cannot be expressed as the product of an abelian normal subgroup of G and a proper supplement.

It will be enough to show that every abelian normal subgroup of G is contained in $\Phi(G)$. Let T be an abelian normal subgroup of G. Since T is abelian, for every $g \in G$ we have that the map $t \mapsto [t, g] = t^{-1}t^g$, $t \in T$, is an endomorphism of T. Note that $[a, b] = a^{p^{m-1}}$, $[a, c] = a^{-p}b^{-p}$, $[b, c] = a$, and that a^p, $b^p \in \mathrm{Z}(N)$. Every element of G has the form $c^k b^l a^r$ for suitable integers k, l, r. Suppose that $c^k b^l a^r \in T \setminus \Phi(G)$. Then $p \nmid k$ or $p \nmid l$.

Suppose first that $p \nmid k$. Then $[c^k b^l a^r, c] = [b, c]^l [a, c]^r = a^l (a^{-p}b^{-p})^r = a^{l-pr}b^{-pr} \in T$. Since $\gcd(l - pr, p^m) = 1$, there exist λ, $\mu \in \mathbb{Z}$ such that $\lambda(l - pr) + \mu p^m = 1$. Therefore $(a^{l-pr}b^{-pr})^\lambda = ab^{-\lambda pr} \in T$. Since T is abelian,

$$\begin{aligned} 1 &= [c^k b^l a^r, ab^{-\lambda pr}] = [c, ab^{-\lambda pr}]^k [b, ab^{-\lambda pr}]^r [a, ab^{-\lambda pr}]^r \\ &= ([a, b^{-\lambda pr}][a, c])^k [b, a]^r = a^{-pk} b^{-pk} a^{-rp^{m-1}} = a^{-pk - rp^{m-1}} b^{-pk}. \end{aligned}$$

It follows that $a^{-pk-rp^{m-1}} = b^{-pk} = 1$. Therefore $p^m \mid pk$, in particular, $p \mid k$, against our hypothesis on k.

Suppose now that $p \nmid l$. Then

$$[c^k, b^l, a^r, b] = [c,b]^k[b,b]^l[a,b]^r = a^{-k}a^{rp^{m-1}} = a^{-k+rp^{m-1}} \in T.$$

Since $\gcd(-k + rp^{m-1}, p^m) = 1$, we conclude that $a \in T$. Therefore

$$1 = [c^k b^l a^r, a] = [c,a]^k[b,a]^l[a,a]^r = a^{pk}b^{pk}a^{-lp^{m-1}} = a^{pk-lp^{m-1}}b^{pk}.$$

It follows that $a^{pk-lp^{m-1}} = b^{pk} = 1$. Consequently $p^m \mid pk$ and $p^m \mid pk - lp^{m-1}$, which implies that $p^m \mid lp^{m-1}$ and so $p \mid l$, against our hypothesis on l.

We conclude that all abelian normal subgroups of G are contained in $\Phi(G)$ and so the fact that G is an IYB-group cannot be obtained as a consequence of the results of [13].

Claim 2. The group G cannot be expressed as a non-trivial semidirect product of a normal subgroup and a complement.

Suppose that the result is false. Then there exists a normal subgroup N with a complement. In particular, N is not contained in $\Phi(G) = \langle c^p, b^p, a\rangle$.

Step 2.1. Let us prove that $\langle a, b^p\rangle \leq N$.

Suppose that $c^i b^j a^k \in N \setminus \Phi(G)$. Assume first that $p \nmid i$. By taking a suitable power, we can assume that $i = 1$. Therefore

$$\begin{aligned}[cb^j a^k, b] &= a^{-k}b^{-j}c^{-1}b^{-1}cb^j a^k b = a^{-k}b^{-j}a^{-1}b^{-1}b^j a^k b \\ &= a^{-k}a^{-1-jp^{m-1}}a^{k+kp^{m-1}} = a^{-1+(k-j)p^{m-1}} \in N.\end{aligned}$$

This element is a generator of $\langle a\rangle$, consequently $a \in N$. We conclude that $[a,c] = a^{-p}b^{-p} \in N$, and since $a \in N$, we obtain that $b^p \in N$. In particular, $\langle a, b^p\rangle \leq N$.

Suppose now that $p \nmid j$. Then

$$\begin{aligned}[c^i b^j a^k, c] &= [b^j a^k, c] = a^{-k}b^{-j}c^{-1}b^j a^k c = a^{-k}b^{-j}(ba)^j a^k a^{-pk}b^{-pk} \\ &= a^{-k}b^{-j}b^j a^{j+j(j-1)p^{m-1}/2}a^k a^{-pk}b^{-pk} = a^{j+j(j-1)p^{m-1}/2-pk}b^{-pk} \in N\end{aligned}$$

and p does not divide the exponent of a. Hence we can assume that N possesses an element of the form $c^i b^l$ with $p \nmid l$. Consequently $[c^i b^l, c] = a^{l+l(l-1)p^{m-1}/2} \in N$, and so $a \in N$. As above, since $[a,c] = a^{-p}b^{-p} \in N$ and $a \in N$, we have that $b^p \in N$ and again $\langle a, b^p\rangle \leq N$.

Step 2.2. Let us prove that N has no elements of the form $cb^j a^k$.

Since $G' = \langle a, b^p\rangle$ has order p^{2m-1} and $N \not\leq \Phi(G)$, we conclude that $|G/N| \leq p^m$. Suppose that $cb^j a^k \in N$, then $N\langle b\rangle = G$ and so N has a cyclic complement of order p. Suppose that $c^i b^l a^r$ is a generator of this complement. We can check by induction that, for $u \in \mathbb{N}$,

$$b^{c^u} = b^{\sum_{w=0}^{u-1}(-1)^w\binom{u+w-1}{2w}p^w}a^{\sum_{w=0}^{u-1}(-1)^w\binom{u+w}{2w+1}p^w}.$$

Now we have that

$$1 = (c^i b^l a^r)^p = c^{ip}(b^l a^r)^{c^{i(p-1)}} \cdots (b^l a^r)^{c^i}(b^l a^r). \tag{2.4}$$

We obtain that $c^{ip} \in \langle c \rangle \cap \langle a, b \rangle = \langle a^{p^{m-1}} \rangle$ and so $p^{m-1} \mid i$, that is, $i = tp^{m-1}$ for an integer t. Since $c^i b^l a^r$ cannot be in $\Phi(G) = \langle c^p, b^p, a \rangle$, we conclude that p does not divide l. The exponent s of b in the right hand side of Equation (2.4) satisfies that

$$\begin{aligned} s &\equiv l\left(p - \sum_{t=0}^{p-1} \binom{tp^{m-1}}{2} p\right) \pmod{p^2} \\ &\equiv l\left(p - \sum_{t=0}^{p-1} \frac{tp^m(tp^{m-1}-1)}{2}\right) \pmod{p^2} \\ &\equiv lp \pmod{p^2}, \end{aligned}$$

but $s \equiv 0 \pmod{p^2}$, and so $p \mid l$, against the previous remark. Hence no element of the form $cb^j a^k$ belongs to N.

Step 2.3. Final contradiction

Take $C = \langle c^r b^s a^t \rangle$ a complement to N in G. Since $c \in NC$, we have a power of $c^r b^s a^t$ in which the exponent of c is equal to 1. In other words, we can assume that $r = 1$ and $cb^s a^t \in C$. Note that $(cb^s a^t)^{p^k} \in \langle c^{p^k}, b^{p^k}, a^{p^k} \rangle$ for k natural, and so $(cb^s a^t)^{p^m} = c^{p^m} = a^{p^{m-1}} \in C \cap N$ with $c^{p^m} \neq 1$. This contradicts that C is a complement to N in G.

Therefore, the fact that G is an IYB-group cannot be obtained from the results of [18].

Since these groups have nilpotency class at least 4, they cannot be obtained as a consequence of the results of [15].

Chapter 3

A new approach using graphs

As mentioned in Chapter 2, it is known that given a non-degenerate involutive solution (X, r) of the YBE, both its structure group and its permutation group have a natural structure of left brace. In this chapter, we will describe these left brace structures of $\mathcal{G}(X, r)$ and $G(X, r)$ by means of the Cayley graph.

In the first section, we will define an addition over the permutation group such that $(\mathcal{G}(X, r), +, \circ)$ becomes a left brace and we will see how to obtain the Cayley graph of $(\mathcal{G}(X, r), +)$ from the one of $(\mathcal{G}(X, r), \circ)$ with respect to the natural generating set $\{f_x \mid x \in X\}$.

In section 3.2, we will obtain a description of $G(X, r)$ using the Cayley graph of $(\mathcal{G}(X, r), +)$ and we will use it to prove that it also has a left brace structure. Section 3.3 will verse about a geometrical interpretation and we will compare other definitions of the additions with our ones in section 3.4.

Finally, we will use the Cayley graph approach to give some interesting applications in section 3.5. The results of this chapter are collected in [8].

3.1 The permutation group as a left brace

In order to obtain a left brace structure over $\mathcal{G}(X, r)$, we need to define an addition. We start by defining the addition of elements of $\mathcal{G}(X, r)$ and its generators f_x, $x \in X$, or their opposites. Given $\alpha \in \mathcal{G}(X, r)$ and $x \in X$, we write

$$\begin{aligned} \alpha + f_x &= \alpha f_{\alpha^{-1}(x)}, \\ \alpha + (-f_x) &= \alpha f^{-1}_{g^{-1}_{\alpha^{-1}(x)}(\alpha^{-1}(x))}. \end{aligned}$$

We will use the abbreviation $\alpha - f_x$ to denote $\alpha + (-f_x)$. For $\alpha = 1_{\mathcal{G}(X,r)}$, we define $-f_x = 1 - f_x = f^{-1}_{g_x^{-1}(x)}$. The following technical lemmas gather the

information about this addition needed for our purposes.

Lemma 3.1.1. *Let $\alpha \in \mathcal{G}(X, r)$ and x, $y \in X$, then the following equalities hold:*

1. $(\alpha + f_x) - f_y = (\alpha - f_y) + f_x$.
2. $(\alpha + f_x) - f_x = (\alpha - f_x) + f_x = \alpha$.
3. $(\alpha + f_x) + f_y = (\alpha + f_y) + f_x$.
4. $(\alpha - f_x) - f_y = (\alpha - f_y) - f_x$.

Proof. We will begin with the first equation. Let us call $u = \alpha^{-1}(x)$ and $v = \alpha^{-1}(y)$. By definition, we have that

$$(\alpha + f_x) - f_y = \alpha f_u f^{-1}_{g^{-1}_{f_u^{-1}(v)}(f_u^{-1}(v))},$$
$$(\alpha - f_y) + f_x = \alpha f^{-1}_{g_v^{-1}(v)} f_{f_{g_v^{-1}(v)}(u)},$$

so it is enough to prove that

$$f_{g_v^{-1}(v)} f_u = f_{f_{g_v^{-1}(v)}(u)} f_{g^{-1}_{f_u^{-1}(v)}(f_u^{-1}(v))}.$$

Observe that by Lemma 2.1.4

$$f_{g_v^{-1}(v)} f_u = f_{f_{g_v^{-1}(v)}(u)} f_{g_u(g_v^{-1}(v))}.$$

Therefore it suffices to show that

$$g^{-1}_{f_u^{-1}(v)}(f_u^{-1}(v)) = g_u(g_v^{-1}(v)).$$

Note that $f_u^{-1}(v) = g_{f_v^{-1}(u)}(v)$ by Lemma 2.1.5. Hence have to show that

$$g^{-1}_{f_u^{-1}(v)}\left(g_{f_v^{-1}(u)}(v)\right) = g_u(g_v^{-1}(v)),$$

or, equivalently,

$$g_{f_v^{-1}(u)}(v) = g_{f_u^{-1}(v)}(g_u(g_v^{-1}(v))). \tag{3.1}$$

Let us call $z = g_v^{-1}(v)$, then $v = g_v(z)$. By Lemma 2.1.4,

$$g_{f_v^{-1}(u)} g_v = g_{g_{f_v^{-1}(u)}(v)} g_{f_v(f_v^{-1}(u))} = g_{f_u^{-1}(v)} g_u.$$

By applying this equality to z, we observe that Equation (3.1) holds and so $(\alpha + f_x) - f_y = (\alpha - f_y) + f_x$.

Now the rest of the statements follow easily. In order to prove the second equality, let us call $u = \alpha^{-1}(x)$. By the proof of the first one, we already have that $(\alpha + f_x) - f_x = (\alpha - f_x) + f_x$ and we only need to see they coincide with α. As

$$(\alpha + f_x) - f_x = \alpha f_u f^{-1}_{g^{-1}_{f_u^{-1}(u)}(f_u^{-1}(u))},$$

we only have to prove that $g^{-1}_{f_u^{-1}(u)}(f_u^{-1}(u)) = u$. This is a consequence of the fact that, by Lemma 2.1.5,

$$g_{f_u^{-1}(u)}(u) = f^{-1}_{f_u(f_u^{-1}(u))}(u) = f_u^{-1}(u).$$

Finally, to obtain equations 3 and 4, we apply 1 and 2.

$$\begin{aligned}(\alpha + f_x) + f_y &= (((\alpha + f_x) + f_y) + f_x) - f_x \\ &= (((\alpha + f_x) + f_y) - f_x) + f_x \\ &= (((\alpha + f_x) - f_x) + f_y) + f_x \\ &= (\alpha + f_y) + f_x.\end{aligned}$$

$$\begin{aligned}(\alpha - f_x) - f_y &= (((\alpha - f_x) - f_y) + f_x) - f_x \\ &= (((\alpha - f_x) + f_x) - f_y) - f_x \\ &= (\alpha - f_y) - f_x.\end{aligned}$$

□

From now on, we will write εf_x, for $\varepsilon \in \{-1, 1\}$ and $x \in X$, to denote f_x if $\varepsilon = 1$ and $-f_x$ if $\varepsilon = -1$.

Lemma 3.1.2. *The following properties hold:*

1. *Let σ be a permutation of $\{1, \dots, m\}$, $\varepsilon_j \in \{-1, 1\}$, $x_j \in X$, $1 \le j \le m$. Then*

$$\begin{aligned}&(\cdots((\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \varepsilon_3 f_{x_3}) + \cdots) + \varepsilon_m f_{x_m} \\ &\quad = \left(\cdots\left(\left(\varepsilon_{\sigma(1)} f_{x_{\sigma(1)}} + \varepsilon_{\sigma(2)} f_{x_{\sigma(2)}}\right) + \varepsilon_{\sigma(3)} f_{x_{\sigma(3)}}\right) + \cdots\right) + \varepsilon_{\sigma(m)} f_{x_{\sigma(m)}}.\end{aligned}$$

2. *If $(\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m} = (\cdots(\mu_1 f_{z_1} + \mu_2 f_{z_2}) + \cdots) + \mu_t f_{z_t}$ and $(\cdots(\eta_1 f_{y_1} + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s} = (\cdots(\nu_1 f_{w_1} + \nu_2 f_{w_2}) + \cdots) + \nu_u f_{w_u}$, with $\varepsilon_i \in \{-1, 1\}$, $x_i \in X$, $1 \le i \le m$; $\mu_j \in \{-1, 1\}$, $z_j \in X$, $1 \le j \le t$; $\eta_k \in \{-1, 1\}$, $y_k \in X$, $1 \le k \le s$; $\nu_h \in \{-1, 1\}$, $w_h \in X$, $1 \le h \le u$, then*

$$\begin{aligned}&(\cdots((((\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m}) \\ &\qquad + \eta_1 f_{y_1}) + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s} \\ &\quad = (\cdots((((\cdots(\mu_1 f_{z_1} + \mu_2 f_{z_2}) + \cdots) \\ &\qquad + \mu_t f_{z_t}) + \nu_1 f_{w_1}) + \nu_2 f_{w_2}) + \cdots) + \nu_u f_{w_u}.\end{aligned}$$

Proof. Statement 1 follows as a consequence of the equations of Lemma 3.1.1, the facts that $1 + \varepsilon_1 f_{x_1} = \varepsilon_1 f_{x_1}$ and $1 + \varepsilon_{\sigma(1)} f_{x_{\sigma(1)}} = \varepsilon_{\sigma(1)} f_{x_{\sigma(1)}}$ and the fact that the symmetric group of degree m is generated by the transpositions $(i, i+1)$, $1 \leq i \leq m-1$.

To prove Statement 2, we use Statement 1:

$$\begin{aligned}
&(\cdots((((\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m}) \\
&\qquad + \eta_1 f_{y_1}) + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s} \\
&= (\cdots((((\cdots(\mu_1 f_{z_1} + \mu_2 f_{z_2}) + \cdots) + \mu_t f_{z_t}) \\
&\qquad + \eta_1 f_{y_1}) + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s} \\
&= (\cdots((((\cdots(\eta_1 f_{y_1} + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s}) \\
&\qquad + \mu_1 f_{z_1}) + \mu_2 f_{z_2}) + \cdots) + \mu_t f_{z_t} \\
&= (\cdots((((\cdots(\nu_1 f_{w_1} + \nu_2 f_{w_2}) + \cdots) + \nu_u f_{w_u}) \\
&\qquad + \mu_1 f_{z_1}) + \mu_2 f_{z_2}) + \cdots) + \mu_t f_{z_t} \\
&= (\cdots((((\cdots(\mu_1 f_{z_1} + \mu_2 f_{z_2}) + \cdots) + \mu_t f_{z_t}) \\
&\qquad + \nu_1 f_{w_1}) + \nu_2 f_{w_2}) + \cdots) + \nu_u f_{w_u}.
\end{aligned}$$

□

Lemma 3.1.3. *The following properties hold:*

1. *If $x \in X$, then $f_x^{-1} = -f_{f_x^{-1}(x)}$.*
2. *If $\alpha \in \mathcal{G}(X, r)$ and $x \in X$, then we have $\alpha f_x^{-1} = \alpha - f_{\alpha(f_x^{-1}(x))}$ and $\alpha f_x = \alpha + f_{\alpha(x)}$.*
3. *If $\alpha \in \mathcal{G}(X, r)$, then $\alpha = 1_{\mathcal{G}(X,r)}$ or there exist $t \in \mathbb{N}$, $x_i \in X$ and $\varepsilon_i \in \{-1, 1\}$, $1 \leq i \leq t$, such that*

$$\alpha = \sum_{i=1}^{t} \varepsilon_i f_{x_i} = (\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_t f_{x_t}.$$

Proof. To prove the first statement, note that $-f_{f_x^{-1}(x)} = f^{-1}_{g^{-1}_{f_x^{-1}(x)}(f_x^{-1}(x))}$ and so it suffices to check that

$$g^{-1}_{f_x^{-1}(x)}(f_x^{-1}(x)) = x,$$

or equivalently, that $f_x\left(g_{f_x^{-1}(x)}(x)\right) = x$. But by Lemma 2.1.5,

$$f_x\left(g_{f_x^{-1}(x)}(x)\right) = f_x\left(f^{-1}_{f_x(f_x^{-1}(x))}(x)\right) = f_x(f_x^{-1}(x)) = x,$$

and so the equality holds.

Let us continue with the second statement:

$$\alpha - f_{\alpha(f_x^{-1}(x))} = \alpha f^{-1}_{g^{-1}_{\alpha^{-1}(\alpha(f_x^{-1}(x)))}(\alpha^{-1}(\alpha(f_x^{-1}(x))))} = \alpha f^{-1}_{g^{-1}_{f_x^{-1}(x)}(f_x^{-1}(x))} = \alpha f_x^{-1}$$

by the argument of Statement 1. Also, since $\alpha + f_{\alpha(x)} = \alpha f_{\alpha^{-1}(\alpha(x))} = \alpha f_x$, the second equality is clear.

Finally, the last statement is immediate by Statement 2 because every element of $\mathcal{G}(X,r)$ can be expressed as a finite product of elements of the form f_x or f_x^{-1}, with $x \in X$. □

Now we are ready to extend this addition to all elements of $\mathcal{G}(X,r)$ and show that the permutation group $\mathcal{G}(X,r)$ with this addition and the composition has in fact a structure of left brace.

Theorem 3.1.4. *Given two elements $\alpha, \beta \in \mathcal{G}(X,r)$, by Lemma 3.1.3 (3), they can be seen as*

$$\alpha = (\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m} \in \mathcal{G}(X,r),$$
$$\beta = (\cdots(\eta_1 f_{y_1} + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s} \in \mathcal{G}(X,r),$$

with $\varepsilon_i \in \{-1,1\}$, $x_i \in X$, $1 \le i \le m$; $\eta_j \in \{-1,1\}$, $y_j \in X$, $1 \le j \le s$. The assignment

$$\alpha + \beta = (\cdots((((\cdots(\varepsilon_1 f_{x_1} + \varepsilon_2 f_{x_2}) + \cdots) + \varepsilon_m f_{x_m}) + \eta_1 f_{y_1}) + \eta_2 f_{y_2}) + \cdots) + \eta_s f_{y_s},$$

$\alpha + 1 = 1 + \alpha = \alpha$, $1 + 1 = 1$, defines an internal binary operation in $\mathcal{G}(X,r)$ such that $(\mathcal{G}(X,r), +, \circ)$ is a left brace.

Proof. By Lemma 3.1.2 (2), we have that $+$ is an internal binary operation and an immediate consequence of Lemma 3.1.2 (1) is the commutativity of $+$. Also, 1 is the neutral element of $+$ by definition.

Next we prove that $+$ is associative. Note first that if $f = f_x$ or $f = -f_x$ for some $x \in X$, then $\alpha + (\beta + f) = (\alpha + \beta) + f$. We must prove that $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ when α, β, $\gamma \in \mathcal{G}(X,r)$. If $\gamma = 1$, the result is clear. If $\gamma \neq 1$, then there exist $t \in \mathbb{N}$, $x_i \in X$ and $\varepsilon_i \in \{-1,1\}$, $1 \le i \le t$, such that $\gamma = \sum_{i=1}^{t} \varepsilon_i f_{x_i}$. We argue by induction and assume that $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$ when δ can be expressed as a sum of $t-1$ terms $\varepsilon_i f_{x_i}$ (when $t = 1$, this sum is understood to be 1). We express $\gamma = \delta + \varepsilon_t f_{x_t}$,

where $\delta = \sum_{i=1}^{t-1} \varepsilon_i f_{x_i}$ is a sum of $t-1$ terms. By the induction hypothesis, $(\alpha+\beta)+\delta = \alpha+(\beta+\delta)$. Then

$$\begin{aligned}
(\alpha+\beta)+\gamma &= (\alpha+\beta)+(\delta+\varepsilon_t f_{x_t}) \\
&= ((\alpha+\beta)+\delta)+\varepsilon_t f_{x_t} && \text{(by the previous remark)} \\
&= (\alpha+(\beta+\delta))+\varepsilon_t f_{x_t} && \text{(by the inductive hypothesis)} \\
&= \alpha+((\beta+\delta)+\varepsilon_t f_{x_t}) && \text{(by the previous remark)} \\
&= \alpha+(\beta+(\delta+\varepsilon_t f_{x_t})) && \text{(by the previous remark)} \\
&= \alpha+(\beta+\gamma).
\end{aligned}$$

Hence the addition is associative.

By Lemma 3.1.1 (2), the commutativity, and the associativity, we have that if $\alpha = \sum_{i=1}^{t} \varepsilon_i f_{x_i}$, with $\varepsilon_i \in \{-1,1\}$ and $x_i \in X$, $1 \le i \le t$, and $\beta = \sum_{i=1}^{t} (-\varepsilon_i) f_{x_i}$, then $\alpha+\beta = \beta+\alpha = 1$ and β becomes the symmetric element of α. We conclude that $(\mathcal{G}(X,r),+)$ is an abelian group.

Finally, we must show that if α, β, $\gamma \in \mathcal{G}(X,r)$, then $\alpha(\beta+\gamma)+\alpha = \alpha\beta+\alpha\gamma$. The result is clear when $\gamma = 1$. We prove it now when $\gamma = f_x$, $x \in X$; recall the definition of the addition for the generators and Lemma 3.1.3 (2).

$$\begin{aligned}
\alpha(\beta+f_x)+\alpha &= \alpha\left(\beta f_{\beta^{-1}(x)}\right)+\alpha \\
&= (\alpha\beta) f_{\beta^{-1}(x)}+\alpha \\
&= \left(\alpha\beta+f_{\alpha(\beta(\beta^{-1}(x)))}\right)+\alpha \\
&= \alpha\beta+\left(f_{\alpha(\beta(\beta^{-1}(x)))}+\alpha\right) \\
&= \alpha\beta+\left(f_{\alpha(x)}+\alpha\right) \\
&= \alpha\beta+\left(\alpha+f_{\alpha(x)}\right) \\
&= \alpha\beta+\alpha f_{\alpha^{-1}(\alpha(x))} \\
&= \alpha\beta+\alpha f_x.
\end{aligned}$$

The result is also true for $\gamma = -f_x$, $x \in X$.

$$\begin{aligned}
\alpha(\beta-f_x)+\alpha &= \alpha\left(\beta f^{-1}_{g^{-1}_{\beta^{-1}(x)}(\beta^{-1}(x))}\right)+\alpha \\
&= (\alpha\beta) f^{-1}_{g^{-1}_{\beta^{-1}(x)}(\beta^{-1}(x))}+\alpha \\
&= \left(\alpha\beta-f_{\alpha(x)}\right)+\alpha \\
&= \alpha\beta+\left(\alpha-f_{\alpha(x)}\right) \\
&= \alpha\beta+\alpha f^{-1}_{g^{-1}_{\alpha^{-1}(\alpha(x))}(\alpha^{-1}(\alpha(x)))} \\
&= \alpha\beta+\alpha f^{-1}_{g_x^{-1}(x)} \\
&= \alpha\beta+\alpha(-f_x).
\end{aligned}$$

Now we suppose that $\gamma = \sum_{i=1}^{t} \varepsilon_i f_{x_i}$ with $t \in \mathbb{N}$, $\varepsilon_i \in \{-1, 1\}$, $x_i \in X$, $1 \leq i \leq t$. We argue by induction on t and we may suppose that $\alpha(\beta+\delta)+\alpha = \alpha\beta + \alpha\delta$ for $\delta = \sum_{i=1}^{t-1} \varepsilon_i f_{x_i}$ (when $t-1 = 0$, we agree that $\delta = 1$). Let $f = \varepsilon_t f_{x_t}$. Then

$$\begin{aligned}
\alpha(\beta+\gamma)+\alpha &= \alpha(\beta+(\delta+f))+\alpha \\
&= \alpha((\beta+\delta)+f)+\alpha \\
&= \alpha(\beta+\delta)+\alpha f \\
&= \alpha\beta+\alpha\delta-\alpha+\alpha f \\
&= \alpha\beta+(\alpha\delta+\alpha f)-\alpha \\
&= \alpha\beta+\alpha(\delta+f) \\
&= \alpha\beta+\alpha\gamma.
\end{aligned}$$

This shows that $(\mathcal{G}(X,r),+,\circ)$ is a left brace. □

To end with this section, we will show that be can obtain the Cayley graph of $(\mathcal{G}(X,r),+)$ just by relabelling the Cayley graph of $(\mathcal{G}(X,r),\circ)$ and we will present some examples. Recall that given a group G with generating set S, the *Cayley graph* $\Gamma(G,S)$ of G with respect to S has as vertices the elements of G and edges of the form $x \xrightarrow{s} xs$, labelled with s, for $x \in G$ and $s \in S$. For simplicity, in the Cayley graph of $\mathcal{G}(X,r)$ with respect to the natural generating set $\{f_x \mid x \in X\}$, the edge $\alpha \xrightarrow{f_x} \alpha f_x$ for $x \in X$ and $\alpha \in \mathcal{G}(X,r)$ will be represented as $\alpha \xrightarrow{x} \alpha f_x$, with label x instead of f_x.

Theorem 3.1.5. *Consider the Cayley graph of $(\mathcal{G}(X,r),\circ)$ and recall that its edges are of the form $\alpha \xrightarrow{x} \alpha f_x$, $x \in X$, $\alpha \in \mathcal{G}(X,r)$. If we replace the label of each such edge by $\alpha(x)$, obtaining edges of the form $\alpha \xrightarrow{\alpha(x)} \alpha f_x$, then the labelled graph obtained in this way is the Cayley graph of the abelian group $(\mathcal{G}(X,r),+)$, where $+$ denotes the operation studied during this whole section.*

Proof. First, notice that by Lemma 3.1.3 (3), the additive group $(\mathcal{G}(X,r),+)$ is generated by the same set as $(\mathcal{G}(X,r),\circ)$, that is, $\{f_x \mid x \in X\}$. Also, if $|X| = n$, the n edges with inicial vertex $\alpha \in \mathcal{G}(X,r)$ labelled by $\alpha(x)$ for each $x \in X$ cover the n different generators because the solution (X,r) is non-degenerate.

Now, the Cayley graph of $(\mathcal{G}(X,r),+)$ would be the one having the elements of $\mathcal{G}(X,r)$ as vertices and edges of the form $\alpha \xrightarrow{x} \alpha + f_x$, for any $\alpha \in \mathcal{G}(X,r)$ and $x \in X$. Thus, the edge starting in α and with label $\alpha(x)$ should end in the vertex $\alpha + f_{\alpha(x)}$ but $\alpha + f_{\alpha(x)} = \alpha f_x$ by Lemma 3.1.3 (2), and hence the graph obtained as stated in the theorem is the Cayley graph of $(\mathcal{G}(X,r),+)$. □

Remark 3.1.6. Note also that if we have the edge $\alpha \xrightarrow{x} \alpha + f_x$ in the Cayley graph of $(\mathcal{G}(X,r),+)$, as $\alpha + f_x = \alpha f_{\alpha^{-1}(x)}$, there is an edge in the Cayley graph of $(\mathcal{G}(X,r),\circ)$ joining α and $\alpha + f_x$ with label $\alpha^{-1}(x)$:

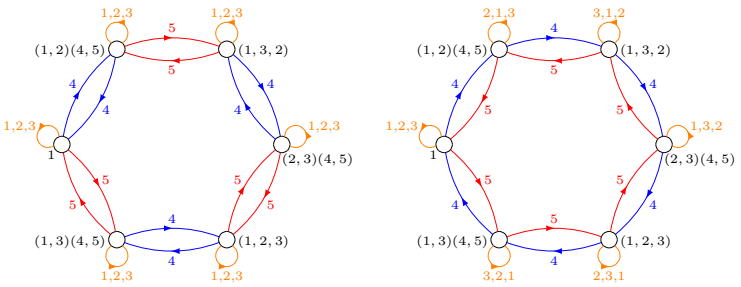
$$\alpha \xrightarrow{\alpha^{-1}(x)} \alpha + f_x.$$

Therefore, if we have the Cayley graph of the additive or the multiplicative group of $\mathcal{G}(X,r)$, we can obtain the other one just by relabelling the edges.

Example 3.1.7. Let (X,r) be the involutive non-degenerate solution of the Yang-Baxter equation such that $X = \{1,2,3,4,5\}$ and $f_1 = f_2 = f_3 = 1$, $f_4 = (1,2)(4,5)$, and $f_5 = (1,3)(4,5)$.

We can draw the Cayley graph of $(\mathcal{G}(X,r),\circ)$ (see Figure 3.1(a)) and use Theorem 3.1.5 to obtain the Cayley graph of $(\mathcal{G}(X,r),+)$ (see Figure 3.1(b)) just changing some labels. For example, the edge $(1,2)(4,5) \xrightarrow{5} (1,3,2)$ in the graph of $(\mathcal{G}(X,r),\circ)$ becomes $(1,2)(4,5) \xrightarrow{4} (1,3,2)$ in the graph of $(\mathcal{G}(X,r),+)$ because $(1,2)(4,5)(5) = 4$.

We have assigned different colors for the different labels $x \in X$ to visualize more easily the changes between the graphs. In addition, we have drawn the loops corresponding to the generators f_1, f_2, and f_3 as just one loop because they coincide and in this way we can simplify the picture, but there are actually three loops in each vertex.



(a) $(\mathcal{G}(X,r),\circ)$ (b) $(\mathcal{G}(X,r),+)$

Figure 3.1: Cayley graphs from Example 3.1.7.

Example 3.1.8. Let (X,r) be the involutive non-degenerate solution of the Yang-Baxter equation such that $X = \{1,2,3,4\}$ and $f_1 = f_3 = (1,2,3,4)$, $f_2 = f_4 = (1,4,3,2)$. In this case, we will simplify the graphs even more by using the assigned colors instead of the labels. The graphs corresponding to this example are shown in Figure 3.2.

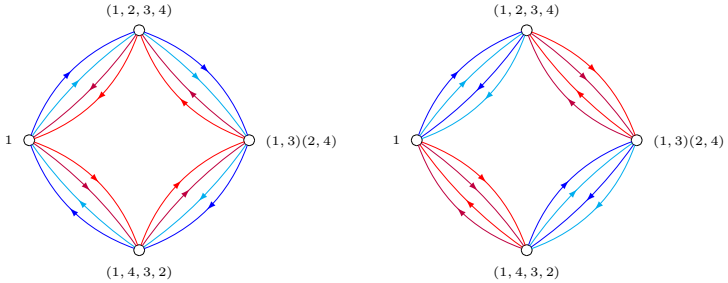


Figure 3.2: Cayley graphs of $(\mathcal{G}(X,r),\circ)$ and $(\mathcal{G}(X,r),+)$ for Example 3.1.8.

3.2 The structure group as a left brace

Our next goal will be obtaining a description of the structure group $G(X,r)$ by means of the Cayley graph of the additive group of the permutation group $(\mathcal{G}(X,r),+)$, with the addition introduced in the previous section. We will also note using this vision that $G(X,r)$ has structure of left brace too. To do so, we will use a construction that can be regarded as an analogue of the one described in [7] by Ballester-Bolinches, Cosme-Llópez, and Esteban-Romero.

Consider the Cayley graph of $(\mathcal{G}(X,r),+)$ and let us denote by E its set of edges. Let W be the free $\mathbb{Z}$-module with basis E. Then, the multiplicative group of the permutation group, $(\mathcal{G}(X,r),\circ)$, acts on the left on E as follows: if $\gamma \in \mathcal{G}(X,r)$ and $(\alpha \xrightarrow{\alpha(x)} \alpha f_x) \in E$, then

$$\gamma * \left(\alpha \xrightarrow{\alpha(x)} \alpha f_x\right) = \left(\gamma\alpha \xrightarrow{\gamma\alpha(x)} \gamma\alpha f_x\right) \in E.$$

Now we can extend the action to W: if $\sum_{e\in E} m_e e \in W$, with $m_e \in \mathbb{Z}$ for $e \in E$, then

$$\gamma * \left(\sum_{e\in E} m_e e\right) = \sum_{e\in E} m_e(\gamma * e) \in W \text{ for all } \gamma \in \mathcal{G}(X,r).$$

Therefore, we can construct the semidirect product $[W]\mathcal{G}(X,r)$.

The next step is identifying all edges in $(\mathcal{G}(X,r),+)$ with the same label, or equivalently, taking quotient modulo

$$K = \langle e_{\alpha,y} - e_{\beta,y} \mid y \in X,\ \alpha,\beta \in \mathcal{G}(X,r)\rangle\,,$$

where $e_{\alpha,y}$ denotes the edge starting in α and with label y, it is, $\alpha \xrightarrow{y} \alpha f_{\alpha^{-1}(y)}$. The following lemma shows that K is a normal subgroup of the semidirect product.

Lemma 3.2.1. *If K is as defined above, then $K \cong K \times 1 \trianglelefteq [W]\mathcal{G}(X,r)$.*

Proof. For each generator $e_{\alpha,y} - e_{\beta,y}$ of K and any $\gamma \in \mathcal{G}(X,r)$, we have that

$$\gamma * (e_{\alpha,y} - e_{\beta,y}) = \gamma * e_{\alpha,y} - \gamma * e_{\beta,y} = e_{\gamma\alpha,\gamma(y)} - e_{\gamma\beta,\gamma(y)},$$

which is also one of the generators of K. Thus, K is invariant for the action of $(\mathcal{G}(X,r), \circ)$.

Next, let us see that $K \trianglelefteq [W]\mathcal{G}(X,r)$. Let $e_{\alpha,y} - e_{\beta,y}$ be a generator of K and let $\left(\sum_{e\in E} m_e e, \gamma\right)$ be an element of $[W]\mathcal{G}(X,r)$. Then

$$\begin{aligned}
&\left(\sum_{e\in E} m_e e, \gamma\right)^{-1} (e_{\alpha,y} - e_{\beta,y}, 1) \left(\sum_{e\in E} m_e e, \gamma\right) \\
&= \left(\sum_{e\in E} (-m_e)(\gamma^{-1} * e), \gamma^{-1}\right) \left(e_{\alpha,y} - e_{\beta,y} + 1 * \left(\sum_{e\in E} m_e e\right), 1 \circ \gamma\right) \\
&= \left(\sum_{e\in E} (-m_e)(\gamma^{-1} * e) + \gamma^{-1} * \left(e_{\alpha,y} - e_{\beta,y} + \sum_{e\in E} m_e e\right), \gamma^{-1} \circ \gamma\right) \\
&= \left(\sum_{e\in E} (-m_e)(\gamma^{-1} * e) + \left(e_{\gamma^{-1}\alpha,\gamma^{-1}(y)} - e_{\gamma^{-1}\beta,\gamma^{-1}(y)}\right) + \sum_{e\in E} m_e(\gamma^{-1} * e), 1\right) \\
&= \left(e_{\gamma^{-1}\alpha,\gamma^{-1}(y)} - e_{\gamma^{-1}\beta,\gamma^{-1}(y)}, 1\right) \in K.
\end{aligned}$$

□

With this, we can construct the quotient group

$$[W]\mathcal{G}(X,r)/K \cong [W/K]\mathcal{G}(X,r)$$

and take the subgroup

$$H = \langle (e_{1,x} + K, f_x) \mid x \in X \rangle \leq [W/K]\mathcal{G}(X,r).$$

Finally, we shall prove that this group H we have just constructed using the Cayley graph of $(\mathcal{G}(X,r), +)$ is isomorphic to the structure group $G(X,r) = \langle X \mid xy = f_x(y)g_y(x),\ x, y \in X \rangle$.

To simplify the notation, as we have identified all the edges with the same label by taking quotients modulo K, we can regard the group H as

$$H = \langle (\bar{x}, f_x) \mid x \in X \rangle \leq \left[\mathbb{Z}^X\right] \mathcal{G}(X,r),$$

where $\bar{x} = e_{1,x} + K$ and $W/K \cong \mathbb{Z}^X$ is a free abelian group with basis X and the action of $\mathcal{G}(X,r)$ over W becomes the following action of $\mathcal{G}(X,r)$ over $\mathbb{Z}^X$:

$$\gamma * \left(\sum_{x\in X} a_x \bar{x}\right) = \sum_{x\in X} a_x \overline{\gamma(x)}, \quad \gamma \in \mathcal{G}(X,r).$$

Notation 3.2.2. In the proofs of the following three theorems, we will also omit the bars in the elements $\bar{x} = e_{1,x} + K$ of $W/K \cong \mathbb{Z}^X$ to work without worrying about them.

Theorem 3.2.3. *Let $H = \langle (\bar{x}, f_x) \mid x \in X \rangle \leq \left[\mathbb{Z}^X\right] \mathcal{G}(X, r)$ be the subgroup constructed above. Then H is isomorphic to the structure group $G(X, r)$.*

Proof. First of all, note that if (x, f_x) is a generator of H, $x \in X$, then $(x, f_x)^{-1} = (-f_x^{-1}(x), f_x^{-1})$, because, clearly,

$$(x, f_x)(-f_x^{-1}(x), f_x^{-1}) = (x - f_x(f_x^{-1}(x)), f_x f_x^{-1}) = (0, 1)$$

and

$$(-f_x^{-1}(x), f_x^{-1})(x, f_x) = (-f_x^{-1}(x) + f_x^{-1}(x), f_x^{-1} f_x) = (0, 1).$$

Let F be the free group on the set of generators X. Then there exists an epimorphism $\beta \colon F \longrightarrow G(X, r)$ sending each generator of F to the corresponding generator of $G(X, r)$. Note that the kernel of β is the normal closure of $\langle y^{-1}x^{-1}f_x(y)g_y(x) \mid x, y \in X \rangle$ in F. Moreover, as H is also an X-generated group, there exists an epimorphism $\gamma \colon F \longrightarrow H$ given by $\gamma(x) = (x, f_x)$.

Let us call $V = \operatorname{Ker} \gamma$ and $N = \operatorname{Ker} \beta$. We will prove now that $N \leq V$. It is enough to check that $y^{-1}x^{-1}f_x(y)g_y(x) \in V$ for $x, y \in X$.

$$\begin{aligned}
&\gamma(y^{-1}x^{-1}f_x(y)g_y(x)) \\
&\quad = (-f_y^{-1}(y), f_y^{-1})(-f_x^{-1}(x), f_x^{-1})(f_x(y), f_{f_x(y)})(g_y(x), f_{g_y(x)}) \\
&\quad = (-f_y^{-1}(y) - f_y^{-1}f_x^{-1}(x) + f_y^{-1}f_x^{-1}f_x(y) + f_y^{-1}f_x^{-1}f_{f_x(y)}(g_y(x)), \\
&\qquad\quad f_y^{-1}f_x^{-1}f_{f_x(y)}f_{g_y(x)}).
\end{aligned}$$

Recall that $f_x f_y = f_{f_x(y)} f_{g_y(x)}$ (Lemma 2.1.4) and then $f_y^{-1}f_x^{-1}f_{f_x(y)}f_{g_y(x)} = 1$. For the first component, it is clear that $-f_y^{-1}(y) + f_y^{-1}f_x^{-1}f_x(y) = 0$, and $f_{f_x(y)}(g_y(x)) = x$ (Lemma 2.1.5). Thus, we obtain that $y^{-1}x^{-1}f_x(y)g_y(x) \in V$. It follows that there exists an epimorphism $\eta \colon G(X, r) \longrightarrow H$ such that $\eta \circ \beta = \gamma$, that is, the following diagram is commutative.

$$\begin{array}{ccc}
F & \xrightarrow{\beta} & G(X, r) \\
& \searrow^{\gamma} & \downarrow{\scriptstyle \eta} \\
& & H
\end{array}$$

We will prove now that $N = V$. Let $w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in V$ with $x_i \in X$, $\varepsilon_i \in \{-1, 1\}$, $1 \leq i \leq n$. We prove by induction on n that $w \in N$. If $w = 1$,

that is, w has no letters, then it is clear that $w \in N$. Suppose that if a word with less than n letters or their inverses belongs to V, then it belongs to N.

Since the positive exponents contribute as positive coefficients in the free abelian group generated by X and the negative exponents contribute as negative coefficients, we have that the number of positive exponents coincides with the number of negative exponents and n is even, $n = 2m$, say. Since r is non-degenerate, given x, $z \in X$ there exists $y \in X$ such that $z = f_x(y)$ and so $y = f_x^{-1}(z)$. Therefore $n_{x,z} = (f_x^{-1}(z))^{-1}x^{-1}zg_{f_x^{-1}(z)}(x) \in N$. It follows that if

$$w = x_1^{\varepsilon_1} \cdots x_{i-1}^{\varepsilon_{i-1}} x^{-1} z x_{i+2}^{\varepsilon_{i+2}} \cdots x_r^{\varepsilon_r}$$

and

$$u = x_1^{\varepsilon_1} \cdots x_{i-1}^{\varepsilon_{i-1}} f_x^{-1}(z)(g_{f_x^{-1}(z)}(x))^{-1} x_{i+2}^{\varepsilon_{i+2}} \cdots x_r^{\varepsilon_r},$$

then $u^{-1}w = n_{x,z}^{\left(g_{f_x^{-1}(z)}(x)\right)^{-1} x_{i+2}^{\varepsilon_{i+2}} \cdots x_r^{\varepsilon_r}} \in N$, so $w \in N$ if, and only if, $u \in N$. Note also that $f_x^{-1}(z)$ and $g_{f_x^{-1}(z)}(x)$ are two elements of X. Therefore, in order to prove that all words in V which are products of $2m$ elements, m of them in X and m of them inverses of elements of X, belong to N, it is enough to do it for all words of the form $w_0 = x_1 \cdots x_m y_m^{-1} \cdots y_1^{-1} \in V$, with x_j, $y_j \in X$, $1 \leq j \leq m$.

Call $F_{i,t} = f_{x_i} \cdots f_{x_{t-1}}(x_t)$ for $1 \leq i < t$, with $F_{t,t} = x_t$, and $G_s = f_{x_1} \cdots f_{x_m} f_{y_m}^{-1} \cdots f_{y_s}^{-1}(y_s)$ for $1 \leq s \leq m$. Then

$$\begin{aligned}\gamma(w_0) &= (F_{1,1} + F_{1,2} + F_{1,3} + \cdots + F_{1,m} - G_m - G_{m-1} - \cdots - G_1, \\ &\qquad f_{x_1} \cdots f_{x_m} f_{y_m}^{-1} \cdots f_{y_1}^{-1}) \\ &= (0, 1).\end{aligned}$$

We conclude that $f_{x_1} \cdots f_{x_m} f_{y_m}^{-1} \cdots f_{y_1}^{-1} = 1$ and so $G_1 = y_1$. Since all $F_{1,j}$ for $1 \leq j \leq m$ and G_k for $1 \leq k \leq m$ are elements of X, there exists a t with $1 \leq t \leq m$ such that $y_1 = F_{1,t}$. Note that for $1 \leq k \leq t-1$, $n_k = F_{k,t} g_{F_{k+1,t}}(x_k) F_{k+1,t}^{-1} x_k^{-1} \in N$. Call

$$w_k = x_k^{-1} w_{k-1} n_k x_k$$

for $1 \leq k \leq t-1$. Then $w_k \in V$ for $1 \leq k \leq t-1$ and $w_k \in N$ if and only if $w_{k-1} \in N$. We check by induction on k that

$$w_k = x_{k+1} \cdots x_m y_m^{-1} \cdots y_2^{-1} g_{F_{2,t}}(x_1) \cdots g_{F_{k+1,t}}(x_k) F_{k+1,t}^{-1}$$

for $1 \leq k \leq t$. For $k = 1$, since $y_1 = F_{1,t}$, we have that

$$w_1 = x_1^{-1} w_0 (F_{1,t} g_{F_{2,t}}(x_1) F_{2,t}^{-1} x_1^{-1}) x_1 = x_2 \cdots x_m y_m^{-1} \cdots y_2^{-1} g_{F_{2,t}}(x_1) F_{2,t}^{-1}.$$

Suppose that $w_{k-1} = x_k \cdots x_m y_m^{-1} \cdots y_2^{-1} g_{F_{2,t}}(x_1) \cdots g_{F_{k,t}}(x_{k-1}) F_{k,t}^{-1}$. Then

$$\begin{aligned} w_k &= x_k^{-1} w_{k-1} (F_{k,t} g_{F_{k+1,t}}(x_k) F_{k+1,t}^{-1} x_k^{-1}) x_k \\ &= x_{k+1} \cdots x_m y_m^{-1} \cdots y_2^{-1} g_{F_{2,t}}(x_1) \cdots g_{F_{k+1,t}}(x_k) F_{k+1,t}^{-1}. \end{aligned}$$

We conclude that

$$w_{t-1} = x_t \cdots x_m y_m^{-1} \cdots y_2^{-1} g_{F_{2,t}(x_1)} \cdots g_{F_{t,t}}(x_{t-1}) F_{t,t}^{-1}.$$

Since $F_{t,t} = x_t$, we have that

$$x_t^{-1} w_{t-1} x_t = x_{t+1} \cdots x_m y_m^{-1} \cdots y_2^{-1} g_{F_{2,t}}(x_1) \cdots g_{F_{t,t}}(x_{t-1}),$$

so that $w_{t-1} \in V$ and $w_{t-1} \in N$ if and only if $x_t^{-1} w_{t-1} x_t \in N$. We conclude that $w_0 \in N$ if and only if $x_t^{-1} w_{t-1} x_t \in N$. But $x_t^{-1} w_{t-1} x_t$ can be expressed as a word with $2m-2$ elements of X or their inverses. By induction, $x_t^{-1} w_{t-1} x_t \in N$. We conclude that $V = N$.

Then we have proved that the homomorphism $\eta \colon G(X,r) \longrightarrow H$ is in fact an isomorphism. □

Theorem 3.2.4. *Let H be as in Theorem 3.2.3, then:*

1. $H = \left\{ \left(\sum_{x \in X} a_x \bar{x}, \sum_{x \in X} a_x f_x \right) \;\middle|\; a_x \in \mathbb{Z}, x \in X \right\}$.
2. *The product of H has the form*

$$\left(\sum_{x \in X} a_x \bar{x}, \alpha \right) \cdot \left(\sum_{x \in X} b_x \bar{x}, \beta \right) = \left(\sum_{x \in X} \left(a_x + b_{\alpha^{-1}(x)} \right) \bar{x}, \alpha\beta \right),$$

where $\alpha = \sum_{x \in X} a_x f_x$, $\beta = \sum_{x \in X} b_x f_x$.

Proof. In order to prove the first statement, note that, due to the associativity and the commutativity of the additions in $\mathcal{G}(X,r)$ and in $\mathbb{Z}^{(X)}$, it is enough to show that

$$H = \left\{ \left(\sum_{i=1}^{r} \varepsilon_i x_i, \sum_{i=1}^{r} \varepsilon_i f_{x_i} \right) \;\middle|\; r \in \mathbb{N} \cup \{0\}, \varepsilon_i \in \{-1, 1\}, x_i \in X, 1 \leq i \leq r \right\}, \quad (3.2)$$

where the element corresponding to $r = 0$ is the neutral element $(0,1)$. Let us call K the right hand side of Equation (3.2).

We prove first that $H \subseteq K$ by induction on the number of factors in $T \cup T^{-1}$ appearing in an element of H, where $T = \{(x, f_x) \mid x \in X\}$ is the natural generating set for H. Clearly, the generators (x, f_x) and their inverses $(x, f_x)^{-1} = (-f_x^{-1}(x), f_x^{-1}) = (-f_x^{-1}(x), -f_{f_x^{-1}(x)})$ belong to K for each $x \in X$. Suppose that $(w, \alpha) = \prod (x_i, f_{x_i})^{\varepsilon_i} \in K$. Then

$$(w, \alpha)(x, f_x) = (w + \alpha(x), \alpha f_x) = \left(w + \alpha(x), \alpha + f_{\alpha(x)}\right) \in K$$

and

$$\begin{aligned}(w, \alpha)(x, f_x)^{-1} &= (w, \alpha)\left(-f_x^{-1}(x), f_x^{-1}\right) = \left(w - \alpha f_x^{-1}(x), \alpha f_x^{-1}\right) \\ &= \left(w - \alpha f_x^{-1}(x), \alpha - f_{\alpha f_x^{-1}(x)}\right) \in K,\end{aligned}$$

where the last equalities hold by Lemma 3.1.3 (2). We conclude that $H \subseteq K$.

We prove now that $K \subseteq H$. We argue by induction on the number r of terms in $(v, \beta) = (\sum_{i=1}^{r} \varepsilon_i x_i, \sum_{i=1}^{r} \varepsilon_i f_{x_i}) \in K$. Let

$$(v_0, \beta_0) = \left(\sum_{i=1}^{r-1} \varepsilon_i x_i, \sum_{i=1}^{r-1} \varepsilon_i f_{x_i}\right) \in K.$$

By the inductive hypothesis, $(v_0, \beta_0) \in H$. Assume that $\varepsilon_r = 1$, then

$$\begin{aligned}(v, \beta) &= (v_0 + x_r, \beta_0 + f_{x_r}) = \left(v_0 + x_r, \beta_0 f_{\beta_0^{-1}(x_r)}\right) \\ &= (v_0, \beta_0)\left(\beta_0^{-1}(x_r), f_{\beta_0^{-1}(x_r)}\right) \in H.\end{aligned}$$

Assume now that $\varepsilon_r = -1$. Then

$$(v, \beta)\left(\beta^{-1}(x_r), f_{\beta^{-1}(x_r)}\right) = \left(v + x_r, \beta f_{\beta^{-1}(x_r)}\right) = (v + x_r, \beta + f_{x_r}) = (v_0, \beta_0),$$

which implies that $(v, \beta) = (v_0, \beta_0)\left(\beta^{-1}(x_r), f_{\beta^{-1}(x_r)}\right)^{-1} \in H$. This completes the proof of Statement 1.

Statement 2 follows from Statement 1 by applying the definition of the product in a semidirect product, that is, if $\left(\sum_{x \in X} a_x x, \alpha\right)$ and $\left(\sum_{x \in X} b_x x, \beta\right)$ are in H, with a_x, $b_x \in \mathbb{Z}$ for $x \in X$, then

$$\begin{aligned}\left(\sum_{x \in X} a_x x, \alpha\right) \cdot \left(\sum_{x \in X} b_x x, \beta\right) &= \left(\sum_{x \in X} a_x x + \sum_{x \in X} b_x \alpha(x), \alpha\beta\right) \\ &= \left(\sum_{x \in X} a_x x + \sum_{x \in X} b_{\alpha^{-1}(x)} x, \alpha\beta\right) \\ &= \left(\sum_{x \in X} \left(a_x + b_{\alpha^{-1}(x)}\right) x, \alpha\beta\right). \qquad \square\end{aligned}$$

Now that we have studied the aspect of the elements in H, in the following theorem we will define an addition over H such that $(H,+,\cdot)$ is a left brace. Therefore, we will have that given a finite involutive non-degenerate set-theoretic solution (X,r) of the YBE, we can construct its structure group $G(X,r)$ using the Cayley graph of the group $(\mathcal{G}(X,r),+)$ and prove that it has structure of left brace.

Theorem 3.2.5. *Let (X,r) be a solution of the YBE and let H be like in Theorem 3.2.3. If we define in H an operation $+$ by means of*

$$\left(\sum_{x\in X} a_x\bar{x},\alpha\right)+\left(\sum_{x\in X} b_x\bar{x},\beta\right)=\left(\sum_{x\in X}(a_x+b_x)\bar{x},\alpha+\beta\right),$$

where $\alpha=\sum_{x\in X} a_x f_x$, $\beta=\sum_{x\in X} b_x f_x$. Then $(H,+,\cdot)$ is a left brace and the map $\pi\colon H\longrightarrow \mathcal{G}(X,r)$ given by $\pi\left(\sum_{x\in X} a_x\bar{x},\alpha\right)=\alpha$ is a left brace homomorphism.

Proof. Since the additions in $\mathcal{G}(X,r)$ and $\mathbb{Z}^{(X)}$ make them abelian groups, only condition (1.1) of the definition of left brace is in doubt. Consider $\left(\sum_{x\in X} a_x x,\alpha\right)$, $\left(\sum_{x\in X} b_x x,\beta\right)$, $\left(\sum_{x\in X} c_x x,\gamma\right)\in H$. Then, bearing in mind that $(\mathcal{G}(X,r),+,\circ)$ is a left brace and Theorem 3.2.4 (2), we obtain:

$$\begin{aligned}
&\left(\sum_{x\in X} a_x x,\alpha\right)\left(\left(\sum_{x\in X} b_x x,\beta\right)+\left(\sum_{x\in X} c_x x,\gamma\right)\right)+\left(\sum_{x\in X} a_x x,\alpha\right)\\
&\quad=\left(\sum_{x\in X} a_x x,\alpha\right)\left(\sum_{x\in X}(b_x+c_x)x,\beta+\gamma\right)+\left(\sum_{x\in X} a_x x,\alpha\right)\\
&\quad=\left(\sum_{x\in X}\left(a_x+b_{\alpha^{-1}(x)}+c_{\alpha^{-1}(x)}\right)x,\alpha(\beta+\gamma)\right)+\left(\sum_{x\in X} a_x x,\alpha\right)\\
&\quad=\left(\sum_{x\in X}\left(a_x+b_{\alpha^{-1}(x)}+c_{\alpha^{-1}(x)}+a_x\right)x,\alpha(\beta+\gamma)+\alpha\right)\\
&\quad=\left(\sum_{x\in X}\left(a_x+b_{\alpha^{-1}(x)}+a_x+c_{\alpha^{-1}(x)}\right)x,\alpha\beta+\alpha\gamma\right)\\
&\quad=\left(\sum_{x\in X}\left(a_x+b_{\alpha^{-1}(x)}\right)x,\alpha\beta\right)+\left(\sum_{x\in X}\left(a_x+c_{\alpha^{-1}(x)}\right)x,\alpha\gamma\right)\\
&\quad=\left(\sum_{x\in X} a_x x,\alpha\right)\left(\sum_{x\in X} b_x x,\beta\right)+\left(\sum_{x\in X} a_x x,\alpha\right)\left(\sum_{x\in X} c_x x,\gamma\right).
\end{aligned}$$

It follows that $(H,+,\cdot)$ is a left brace. The fact that π is a left brace epimorphism is clear. □

3.3 A geometrical interpretation of the structure group in terms of the Cayley graph of the permutation group

In this section we present a geometrical interpretation of Theorem 3.2.3 in the line of [7]. Let G be a group with a generating set S and let F be the free group on S. There exists a unique epimorphism $\beta\colon F \longrightarrow G$ that sends the generators of F to the corresponding generators of G. If $w \in F$, then w is a word on $S \cup S^{-1}$, that is, $w = s_1^{\varepsilon_1} \dots s_r^{\varepsilon_r}$ with $r \geq 0$, $\varepsilon_i \in \{-1, 1\}$, $s_i \in S$, $1 \leq i \leq r$. If we have the Cayley graph of G with respect to S, we can consider a path of length r starting from 1 and following the edges labelled s_i, in the same sense if $\varepsilon_i = 1$ and in the opposite sense if $\varepsilon_i = -1$, for $1 \leq i \leq r$. The other end of this path is $\beta(w)$.

According to Theorem 3.1.5, if we draw the Cayley graph of the permutation group of $(\mathcal{G}(X,r), \circ)$ with respect to the natural generating set $S = \{f_x \mid x \in X\}$ and we replace in each edge of the form $\alpha \xrightarrow{x} \alpha f_x$, $x \in X$, $\alpha \in \mathcal{G}(X,r)$, the label x by $\alpha(x)$, then we obtain the Cayley graph of $(\mathcal{G}(X,r), +)$ with respect to the same generating set. We can use these Cayley graphs to obtain the images of elements of the free group on S in $(\mathcal{G}(X,r), \circ)$ and $(\mathcal{G}(X,r), +)$.

Example 3.3.1. Let (X,r) be the solution in Example 3.1.7, that was the one with $X = \{1,2,3,4,5\}$ and with $f_1 = f_2 = f_3 = 1$, $f_4 = (1,2)(4,5)$, and $f_5 = (1,3)(4,5)$. Recall that we can see the complete Cayley graphs of $(\mathcal{G}(X,r), \circ)$ and $(\mathcal{G}(X,r), +)$ in Figure 3.1. We show here a reduced version omitting the loops because we are not going to use them in these examples (see Figure 3.3).

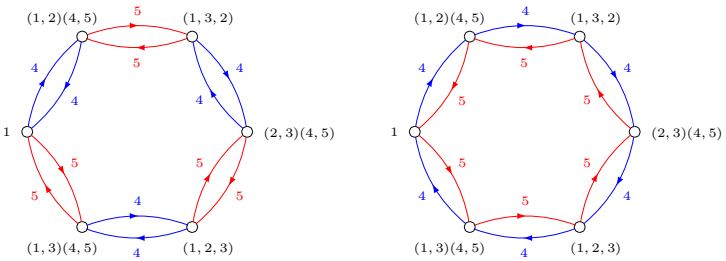


Figure 3.3: Cayley graphs of $(\mathcal{G}(X,r), \circ)$ and $(\mathcal{G}(X,r), +)$ (simplified).

Consider the free group F with basis X and the word $w = 445^{-1} \in F$. Its image in $(\mathcal{G}(X,r), +)$ will be $f_4 + f_4 - f_5$. This can be obtained by following

the path starting from 1 and with edges labelled 4, 4, and 5 (the last one reversed) in the Cayley graph of $(\mathcal{G}(X,r),+)$. The path is drawn in Figure 3.4 and we obtain that $f_4 + f_4 - f_5 = (2,3)(4,5)$.

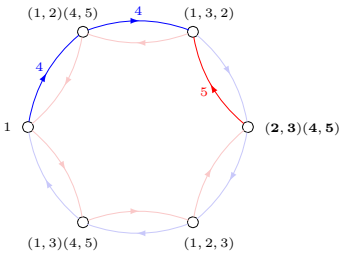


Figure 3.4: Path in the Cayley graph of $(\mathcal{G}(X,r),+)$

Now we compute the image of the same word $w = 445^{-1} \in F$ in the multiplicative group $(\mathcal{G}(X,r),\circ)$ by following the path starting from 1 and with edges labelled 4, 4, and 5 (this one reversed) in the Cayley graph of $(\mathcal{G}(X,r),\circ)$. The path is drawn in Figure 3.5. We see that $f_4 \circ f_4 \circ f_5^{-1} = (1,3)(4,5)$.

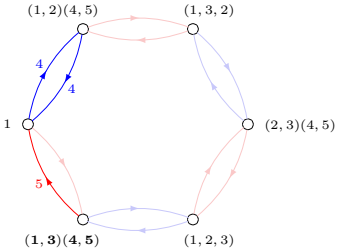


Figure 3.5: Path in the Cayley graphs of $(\mathcal{G}(X,r),\circ)$

Suppose now that we want to obtain an element of $(G(X,r),+)$. We can identify $G(X,r)$ with the subgroup H of Theorem 3.2.3 with generating set $T = \{(x, f_x) \mid x \in X\}$ identified in the obvious way with X. We can follow in the Cayley graph of $(\mathcal{G}(X,r),+)$ a path labelled with the terms as before. The last end of the path corresponds to the second component of the element in H. To obtain the first component, we can count in the same path how many edges labelled by each element $x \in X$ does the path traverse, taking into account that the edges traversed in the opposite direction of the edge would

count as negative. For each x, this number would be the coefficient $a_x \in \mathbb{Z}$ of the first component of the element in H, that will be $\sum_{x\in X} a_x \bar{x}$.

Finally, suppose that we want to obtain an element of $(G(X,r),\cdot)$, identified again with H with generating set T as in the previous paragraph. If we follow the path in the Cayley graph of $(\mathcal{G}(X,r),\circ)$ starting from 1 with edges labelled with the corresponding elements of X, the last end corresponds to the second component of the product. In order to find the first component of the product, we can follow the same path but in this occasion in the Cayley graph of $(\mathcal{G}(X,r),+)$, with the new assignments of labels, and again take into account the number of signed traversals of edges labelled with $x \in X$ to obtain the coefficients $b_x \in \mathbb{Z}$ of the first component $\sum_{x\in X} b_x \bar{x}$ of the product in H.

Example 3.3.2. Let us continue with Example 3.1.7, as before. The image in $(G(X,r),+)$ of the word $w = 445^{-1} \in F$ will have $f_4 + f_4 - f_5 = (2,3)(4,5)$ as second component. To obtain the first component, note that the path in Figure 3.4 contains two arcs labelled 4 and an arc labelled 5 traversed in the opposite direction. This means that w maps to $(\bar{4}, f_4) + (\bar{4}, f_4) - (\bar{5}, f_5) = (2\cdot\bar{4} + (-1)\cdot\bar{5}, (2,3)(4,5))$.

Now, the image in $(G(X,r),\cdot)$ of the word $w = 445^{-1} \in F$ will have $f_4 \circ f_4 \circ f_5^{-1} = (1,3)(4,5)$ as second component. To obtain the first component we have to consider the same path but in the Cayley graph of $(\mathcal{G}(X,r),+)$, with the labels changed according to Theorem 3.1.5. The new labels for these edges are now 4, 5, 4, respectively, the first two ones traversed in the direction of the edges and last one reversed. The path appears on the right hand side of Figure 3.6. The edges labelled 4 cancel because there is one traversed positively and another one traversed negatively, and there is an edge labelled 5 traversed positively. Consequently, the image of w in $(G(X,r),\cdot)$ is $(\bar{4}, f_4)\cdot(\bar{4}, f_4)\cdot(\bar{5}, f_5)^{-1} = (0\cdot\bar{4} + 1\cdot\bar{5}, (1,3)(4,5))$.

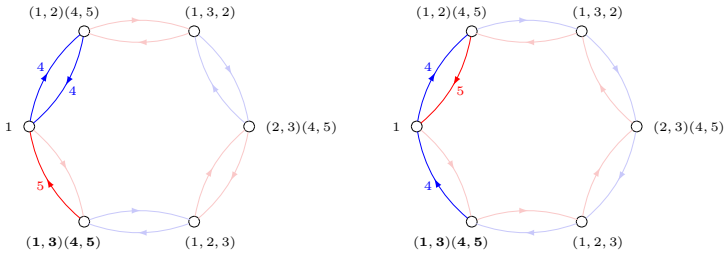


Figure 3.6: Same path in the Cayley graphs of $(\mathcal{G}(X,r),\circ)$ and $(\mathcal{G}(X,r),+)$

3.4 A comparison with other definitions of the addition

Bachiller, Cedó, and Jespers defined in [4] an addition in the structure group of a solution of the YBE which induces an addition in the permutation group such that both groups acquire brace structures. The aim of this section is to prove that both additions coincide, respectively, with our additions in the structure group and in the permutation group.

The definitions of the additions in [4] depend strongly on the isomorphism between the structure group and the subgroup of the semidirect product of the free abelian group $\mathbb{Z}^X$ with basis X and the symmetric group on X given by Etingof, Schedler, and Soloviev in [19]. For the reader's convenience, we summarize the arguments of [19] and we adapt their notation to the left actions we are considering here.

In [19], its authors prove that $G(X,r)$ is isomorphic to a subgroup of the semidirect product $M_X = [\mathbb{Z}^X]\mathrm{Sym}(X)$, where the action of $\mathrm{Sym}(X)$ on $\mathbb{Z}^X$ is the natural action of $\mathrm{Sym}(X)$ on X, extended by linearity to $\mathbb{Z}^X$. The product in M_X is defined as usual:

$$(a,\sigma)(b,\tau) = (a+\sigma(b),\sigma\tau), \quad \text{for all } a,\, b \in \mathbb{Z}^X,\, \sigma,\, \tau \in \mathrm{Sym}(X).$$

They define a group homomorphism $\psi\colon G(X,r) \longrightarrow M_X$ by means of $\psi(x) = (x, f_x) \in M_X$ for each $x \in X$ and write $\psi(h) = (\pi(h), \phi(h)) \in M_X$ for each $h \in G(X,r)$. If $h_1, h_2 \in G(X,r)$, then

$$\begin{aligned}(\pi(h_1h_2), \phi(h_1h_2)) &= \psi(h_1h_2) = \psi(h_1)\psi(h_2)\\ &= (\pi(h_1), \phi(h_1))(\pi(h_2), \phi(h_2))\\ &= (\pi(h_1) + \phi(h_1)(\pi(h_2)), \phi(h_1)\phi(h_2)).\end{aligned}$$

Therefore, the map $\phi\colon G(X,r) \longrightarrow \mathrm{Sym}(X)$ is a group homomorphism with image $\mathcal{G}(X,r)$ and $\phi(x) = f_x$ for $x \in X$, and the map $\pi\colon G(X,r) \longrightarrow \mathbb{Z}^X$ is a 1-cocycle with respect to the action of $G(X,r)$ on $\mathbb{Z}^X$ given by $h\sum_{x\in X} a_x x = \phi(h)\left(\sum_{x\in X} a_x x\right) = \sum_{x\in X} a_x \phi(h)(x)$, for $h \in G(X,r), a_x \in \mathbb{Z}$. Also, $\pi(x) = x$ for $x \in X$.

They prove that π is bijective by showing that it possesses an inverse $\rho\colon \mathbb{Z}^X \longrightarrow G(X,r)$. They call $\mathbb{Z}_k^X$ the set of elements of $\mathbb{Z}^X$ that can be expressed as a sum of at most k terms of the form x or $-x$ with $x \in X$. Thus, $\mathbb{Z}^X = \bigcup_{k\geq 1} \mathbb{Z}_k^X$ and they define the inverse ρ of π inductively. For elements of $\mathbb{Z}_1^X$, $\rho(0) = 1$, $\rho(x) = x$, and $\rho(-x) = (g_x^{-1}(x))^{-1}$ for $x \in X$. Now, if ρ has been already defined for elements of $\mathbb{Z}_{k-1}^X$ and $\eta \in \mathbb{Z}_k^X$, then $\eta = a + \xi$ for $a \in \mathbb{Z}_{k-1}^X$, $\xi \in \{x, -x\}$ for some $x \in X$. In this case, we consider

the right action of $G(X,r)$ on $\mathbb{Z}^X$ defined by $ah = \phi(h)^{-1}(a)$ for $a \in \mathbb{Z}^X$, $h \in G(X,r)$, and define $\rho(\eta) = \rho(a)\rho(\xi\rho(a))$. With this, it is easy to check that ρ is the inverse of π. Note that by definition of ρ in $\mathbb{Z}_1^X$,

$$\rho(x\rho(a)) = \rho(\phi(\rho(a))^{-1}(x)) = \phi(\rho(a))^{-1}(x); \tag{3.3}$$

$$\begin{aligned}\rho((-x)\rho(a)) &= \rho(\phi(\rho(a))^{-1}(-x)) = \rho(-\phi(\rho(a))^{-1}(x)) \\ &= (g_{\phi(\rho(a))^{-1}(x)}(\phi(\rho(a))^{-1}(x)))^{-1}.\end{aligned} \tag{3.4}$$

This construction is used by Bachiller, Cedó, and Jespers in [4] to define additions in $G(X,r)$ and $\mathcal{G}(X,r)$. The addition in $G(X,r)$ is defined by means of

$$h_1 + h_2 = \rho(\pi(h_1) + \pi(h_2)), \quad \text{for } h_1, h_2 \in G(X,r).$$

Given $h \in G(X,r)$ and $x \in X$, we obtain that

$$\begin{aligned}h + x &= \rho(\pi(h) + \pi(x)) = \rho(\pi(h) + x) = \rho(\pi(h))\rho(x\rho(\pi(h))) \\ &= h\rho(xh) = h\phi(h)^{-1}(x),\end{aligned}$$

where the last equality follows by (3.3), and so

$$\begin{aligned}\psi(h + x) &= (\pi(h\rho(xh)), \phi(h\phi(h)^{-1}(x))) \\ &= (\pi(h) + \phi(h)(\pi(\rho(xh))), \phi(h)\phi(\phi(h)^{-1}(x))) \\ &= \left(\pi(h) + x, \phi(h)f_{\phi(h)^{-1}(x)}\right).\end{aligned}$$

On the other hand,

$$\begin{aligned}h - x &= \rho(\pi(h) - \pi(x)) = \rho(\pi(h) - x) = \rho(\pi(h))\rho((-x)\rho(\pi(h))) \\ &= h\rho((-x)h) = h(g_{\phi(h)^{-1}(x)}(\phi(h)^{-1}(x)))^{-1},\end{aligned}$$

where the last equality follows by (3.4). Thus,

$$\begin{aligned}\psi(h - x) &= (\pi(h\rho((-x)h)), \phi(h(g_{\phi(h)^{-1}(x)}(\phi(h)^{-1}(x)))^{-1})) \\ &= \left(\pi(h) - x, \phi(h)f^{-1}_{g_{\phi(h)^{-1}(x)}(\phi(h)^{-1}(x))}\right).\end{aligned}$$

The addition in $\mathcal{G}(X,r)$, that coincides with the image of ϕ, is defined by $\phi(h_1) + \phi(h_2) = \phi(h_1 + h_2)$, where $h_1,\ h_2 \in G(X,r)$. Let $\alpha \in \mathcal{G}(X,r)$ and $x \in X$. Then $\alpha = \phi(h)$ for a certain $h \in G(X,r)$ and $f_x = \phi(x)$. Hence,

$$\alpha + f_x = \phi(h) + \phi(x) = \phi(h + x) = \phi(h)f_{\phi(h)^{-1}(x)} = \alpha f_{\alpha^{-1}(x)}$$

and

$$\begin{aligned}\alpha - f_x &= \phi(h) - \phi(x) = \phi(h - x) = \phi(h)f^{-1}_{g_{\phi(h)^{-1}(x)}(\phi(h)^{-1}(x))} \\ &= \alpha f^{-1}_{g_{\alpha^{-1}(x)}(\alpha^{-1}(x))}.\end{aligned}$$

We conclude that the additions obtained with the arguments of [19] and [4] coincide with our additions.

3.5 Some applications

We will close this chapter presenting some results that follow easily as applications of the Cayley graph approach. We will begin with a way of finding the frozen pairs, which were introduced by Chouraqui and Godelle in [16].

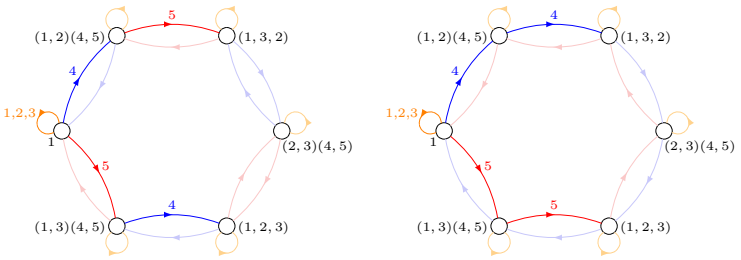
Definition 3.5.1. Let (X, r) be a solution of the YBE and consider the natural action of r on $X \times X$. The fixed points of this action are called *frozen pairs*.

Proposition 3.5.2. *Let $x \in X$. Consider in the Cayley graph of the additive group of $\mathcal{G}(X, r)$ the path of length two starting at 1 with both edges labelled with x and consider the corresponding edges on the Cayley graph of the multiplicative group of $\mathcal{G}(X, r)$, with labels x, y, respectively. Then $r(x, y) = (x, y)$. Moreover, (x, y) is the unique pair of the form (x, z) with $z \in X$ such that $r(x, z) = (x, z)$.*

Proof. We have that $f_x \circ f_y = f_x + f_{f_x(y)} = f_x + f_x$ and $x = f_x(y)$. Hence $y = f_x^{-1}(x)$. Now $r(x, y) = (f_x(y), f_{f_x(y)}^{-1}(x)) = (x, f_x^{-1}(x)) = (x, y)$.

Moreover, if $r(x, z) = (x, z)$, then $f_x(z) = x$ and so $z = f_x^{-1}(x) = y$, hence the unicity holds. □

Example 3.5.3. Consider again the solution (X, r) with $X = \{1, 2, 3, 4, 5\}$, $f_1 = f_2 = f_3 = 1$, $f_4 = (1, 2)(4, 5)$, and $f_5 = (1, 3)(4, 5)$. Figure 3.7 (b) shows the paths of length two starting at 1 and with the two edges labelled by the same x for each $x \in X$ in the Cayley graph of $(\mathcal{G}(X, r), +)$, and Figure 3.7 (a) show the corresponding paths in the Cayley graph of $(\mathcal{G}(X, r), \circ)$.



(a) $(\mathcal{G}(X, r), \circ)$ (b) $(\mathcal{G}(X, r), +)$

Figure 3.7: Paths to find the frozen pairs

Note that we have drawn just one loop to represent the edges labelled by 1, 2, and 3 to make the picture easier, but they are in fact three different

paths. Hence, applying Proposition 3.5.2, we find easily that the frozen pairs are $(1,1),(2,2),(3,3),(4,5)$, and $(5,4)$.

Next we will see that the relations explicitly mentioned in the definition of the structure group and the trivial ones of the form $xy = xy$ are the unique relations that can be found in this group involving equalities of products of two generators. The proof is already implicit in the proof of Theorem 3.2.3, but it becomes more evident from our description of the structure group.

Theorem 3.5.4. *Let x, y, z, $t \in X$ be regarded as elements of the structure group $G(X,r)$. Then $xy = zt$ if, and only if, $x = z$ and $y = t$ or $r(x,y) = (z,t)$.*

Proof. The element xy corresponds to a path of length 2 in the Cayley graph of $(\mathcal{G}(X,r),\circ)$ starting at 1 and with labels x and y, and the element zt corresponds to a path of length 2 in the Cayley graph of $(\mathcal{G}(X,r),\circ)$ starting at 1 and with labels z and t. They correspond to paths in the Cayley graph of the additive group of $\mathcal{G}(X,r)$ starting at 1 and with labels x, $f_x(y)$ for the first one, and z, $f_z(t)$ for the second one. Hence $\{x, f_x(y)\} = \{z, f_z(t)\}$. If $x = z$, then $f_x(y) = f_z(t) = f_x(t)$ and, since f_x is bijective, $y = t$ and we are in the first case. Now suppose that $x = f_z(t)$, $z = f_x(y)$. Then $r(x,y) = (f_x(y), f^{-1}_{f_x(y)}(x)) = (z, f_z^{-1}(x)) = (z,t)$ and we are in the second case. The converse is clear. □

Our next objective is to prove that the solution induced by the retract relation (recall Definition 2.1.8) is indeed a well-defined solution of the YBE, as mentioned in Chapter 2. To achieve this, we should recall the concepts of block and block system of an action: if G is a permutation group acting on a set Ω, a *block* of this action is a subset $B \subseteq \Omega$ such that for each $g \in G$, $gB = B$ or $gB \cap B = \emptyset$. Note that we are not requiring the action to be transitive. In addition, a *block system* is a partition of Ω formed by blocks.

Lemma 3.5.5. *Let (X,r) be a solution of the YBE. The equivalence classes for the retract relation $\sim$ on X are blocks for the natural action of $\mathcal{G}(X,r)$ on X.*

Proof. Suppose that $x \sim \bar{x}$, that is, $f_x = f_{\bar{x}}$. Then, given $\alpha \in \mathcal{G}(X,r)$, $\alpha f_x = \alpha f_{\bar{x}}$, that is, $\alpha + f_{\alpha(x)} = \alpha + f_{\alpha(\bar{x})}$, which implies that $f_{\alpha(x)} = f_{\alpha(\bar{x})}$. □

Remark 3.5.6. It is possible to prove Lemma 3.5.5 without using the description of the addition in $\mathcal{G}(X,r)$, but the proofs we know are not so immediate and intuitive. For completeness, we present one such proof.

Alternative proof of Lemma 3.5.5. Suppose that $x \sim \bar{x}$. It is enough to show that for each $t \in X$, $f_t^{-1}(x) \sim f_t^{-1}(\bar{x})$ and $f_t(x) \sim f_t(\bar{x})$.

For every $t \in X$, by Lemma 2.1.5 and Lemma 2.1.4 we have that

$$f_x f_{f_x^{-1}(t)} = f_{f_x(f_x^{-1}(t))} f_{g_{f_x^{-1}(t)}(x)} = f_t f_{f_t^{-1}(x)}$$

and so

$$f_{f_t^{-1}(x)} = f_t^{-1} f_x f_{f_x^{-1}(t)}.$$

Analogously,

$$f_{f_t^{-1}(\bar{x})} = f_t^{-1} f_{\bar{x}} f_{f_{\bar{x}}^{-1}(t)}.$$

Since $f_x = f_{\bar{x}}$, we conclude that $f_{f_t^{-1}(x)} = f_{f_t^{-1}(\bar{x})}$ and so $f_t^{-1}(x) \sim f_t^{-1}(\bar{x})$.

By Lemma 2.1.5 and Lemma 2.1.4, we have that

$$\begin{aligned} g_{f_x^{-1}(f_t^{-1}(t))}(g_x(t)) &= f^{-1}_{f_{g_x(t)}(f_x^{-1}(f_t^{-1}(t)))} \left(f^{-1}_{f_t(x)}(t)\right) \\ &= f^{-1}_{f_{g_x(t)}\left(f^{-1}_{g_x(t)}\left(f^{-1}_{f_t(x)}(t)\right)\right)} \left(f^{-1}_{f_t(x)}(t)\right) \\ &= f^{-1}_{f^{-1}_{f_t(x)}(t)} \left(f^{-1}_{f_t(x)}(t)\right) \\ &= f^{-1}_{g_x(t)} \left(f^{-1}_{f_t(x)}(t)\right) \\ &= f_x^{-1}(f_t^{-1}(t)). \end{aligned}$$

Therefore

$$g_x(t) = g^{-1}_{f_x^{-1}(f_t^{-1}(t))}(f_x^{-1}(f_t^{-1}(t))),$$

which implies, by Lemma 2.1.5, that

$$f_{f_t(x)} = f_t f_x f^{-1}_{g_x(t)} = f_t f_x f^{-1}_{g^{-1}_{f_x^{-1}(f_t^{-1}(t))}(f_x^{-1}(f_t^{-1}(t)))}.$$

Analogously,

$$f_{f_t(\bar{x})} = f_t f_{\bar{x}} f^{-1}_{g^{-1}_{f_{\bar{x}}^{-1}(f_t^{-1}(t))}(f_{\bar{x}}^{-1}(f_t^{-1}(t)))}.$$

Since $f_x = f_{\bar{x}}$, we have that $f_{f_t(x)} = f_{f_t(\bar{x})}$. Consequently $f_t(x) \sim f_t(\bar{x})$. □

We can use Lemma 3.5.5 to give an immediate justification for the construction of the solution associated to the retraction.

Proposition 3.5.7 (see [19] Section 3.2 and also [14])**.** *If (X, r) is a solution of the YBE, then the map $\tilde{r}\colon (X/\!\sim) \times (X/\!\sim)$ given by $\tilde{r}([x],[y]) = ([f_x(y)],[g_y(x)])$ is such that $(X/\!\sim, \tilde{r})$ is a solution of the YBE and the natural surjection $\varphi\colon X \longrightarrow X/\!\sim$ induces a homomorphism of solutions of the YBE.*

Proof. The only thing which is in doubt is that $\tilde{r}$ is a map, that is, if $x_1 \sim x_2$ and $y_1 \sim y_2$, then $f_{x_1}(y_1) \sim f_{x_2}(y_2)$ and $g_{y_1}(x_1) \sim g_{y_2}(x_2)$. Since $x_1 \sim x_2$, $f_{x_1} = f_{x_2}$. This together with Lemma 3.5.5 gives $f_{x_1}(y_1) = f_{x_2}(y_1) \sim f_{x_2}(y_2)$. Now $g_{y_1}(x_1) = f^{-1}_{f_{x_1}(y_1)}(x_1)$ and $g_{y_2}(x_2) = f^{-1}_{f_{x_2}(y_2)}(x_2)$ by Lemma 2.1.5. Since $f_{x_1}(y_1) \sim f_{x_2}(y_2)$, we have that $f_{f_{x_1}(y_1)} = f_{f_{x_2}(y_2)}$. Since $x_1 \sim x_2$, we have by Lemma 3.5.5 that $f^{-1}_{f_{x_1}(y_1)}(x_1) = f^{-1}_{f_{x_2}(y_2)}(x_1) \sim f^{-1}_{f_{x_2}(y_2)}(x_2)$. Hence $\tilde{r}$ is a map and φ induces a homomorphism of solutions of the YBE. □

Now we will deal with some results about the socle of the permutation group of a solution (X, r) of the Yang-Baxter equation and its relation with the permutation group of $\mathrm{Ret}(X, r)$. We will use them to obtain the multipermutation level of a multipermutation solution.

Lemma 3.5.8. *If (X, r) is a solution of the YBE, then*

$$\mathrm{Soc}(\mathcal{G}(X, r)) = \{\alpha \in \mathcal{G}(X, r) \mid \alpha \text{ induces the identity on } X/\!\sim\}.$$

Proof. Recall that the socle of a left brace $(B, +, \cdot)$ is

$$\mathrm{Soc}(B) = \{a \in B \mid \lambda_a = \mathrm{id}_B\} = \{a \in B \mid \text{ for all } b \in B, a + b = a \cdot b\}$$

(see Definition 1.1.11). Also, as $\lambda_a \in \mathrm{Aut}(B, +)$, in order to prove that $\lambda_a(b) = b$ for all $b \in B$, it is enough to check the condition for the elements of a generating set of $(B, +)$. If we assume that $B = \mathcal{G}(X, r)$, we obtain that

$$\mathrm{Soc}(\mathcal{G}(X, r)) = \{\alpha \in \mathcal{G}(X, r) \mid \text{for all } x \in X,\ \alpha + f_x = \alpha f_x\}.$$

Since $\alpha f_x = \alpha + f_{\alpha(x)}$ by Lemma 3.1.3 (2), we have that

$$\begin{aligned}\mathrm{Soc}(\mathcal{G}(X, r)) &= \{\alpha \in \mathcal{G}(X, r) \mid \text{for all } x \in X,\ \alpha + f_x = \alpha + f_{\alpha(x)}\} \\ &= \{\alpha \in \mathcal{G}(X, r) \mid \text{for all } x \in X,\ f_x = f_{\alpha(x)}\} \\ &= \{\alpha \in \mathcal{G}(X, r) \mid \text{for all } x \in X,\ x \sim \alpha(x)\},\end{aligned}$$

and the result follows. □

Proposition 3.5.9. *If (X, r) is a solution of the YBE and $(X/\!\sim, \tilde{r})$ is its retraction, then*

$$\mathcal{G}(X, r)/\mathrm{Soc}(\mathcal{G}(X, r)) \cong \mathcal{G}(X/\!\sim, \tilde{r}).$$

Proof. The permutation group $\mathcal{G}(X/\!\sim, \tilde{r})$ of the retraction $(X/\!\sim, \tilde{r})$ of (X, r) is

$$\mathcal{G}(X/\!\sim, \tilde{r}) = \langle \tilde{f}_{[x]} \mid x \in X \rangle,$$

where $\tilde{f}_{[x]}\colon X/\!\sim \longrightarrow X/\!\sim$ is given by $\tilde{f}_{[x]}([y]) = [f_x(y)]$. It is clear that all relations of $\mathcal{G}(X,r)$ are satisfied by $\mathcal{G}(X/\!\sim,\tilde{r})$, since if a product of elements of the form f_x or f_x^{-1} acts trivially on X, then it acts trivially on the blocks of $X/\!\sim$. By von Dyck's theorem, there exists a group epimorphism $\eta\colon \mathcal{G}(X,r) \longrightarrow \mathcal{G}(X/\!\sim,\tilde{r})$ such that $\eta(f_x) = \tilde{f}_{[x]}$. Then

$$\ker\eta = \{\alpha \in \mathcal{G}(X,r) \mid \alpha \text{ induces the identity on } X/\!\sim\} = \mathrm{Soc}(\mathcal{G}(X,r))$$

by Lemma 3.5.8 and therefore $\mathcal{G}(X,r)/\mathrm{Soc}(\mathcal{G}(X,r)) \cong \mathcal{G}(X/\!\sim,\tilde{r})$. □

We can use Proposition 3.5.9 to obtain the Cayley graph of the permutation group associated to the retraction of a solution of the YBE. We identify in X the elements related with respect to the retract relation. The arcs in the Cayley graph corresponding to the same retraction class will be identified and the vertices will be replaced by the permutation that this vertex induces on $X/\!\sim$. The elements of $\mathrm{Soc}(\mathcal{G}(X,r))$ will be mapped to $1_{X/\sim}$. We identify all vertices with the same labels, that will correspond to the same element of $\mathcal{G}(X,r)/\mathrm{Soc}(\mathcal{G}(X,r))$. This new graph will be the Cayley graph of $\mathcal{G}(X/\!\sim,\tilde{r}) \cong \mathcal{G}(X,r)/\mathrm{Soc}(\mathcal{G}(X,r))$.

Example 3.5.10. Let $X = \{1,2,3,4,5\}$ and let r be the solution of the YBE given by $f_1 = f_2 = f_3 = 1_X$, $f_4 = (1,2)(4,5)$, $f_5 = (1,3)(4,5)$. The Cayley graph of $(\mathcal{G}(X,r),\circ)$ is given in Figure 3.8, where each loop in the figure represents three loops with labels 1, 2, and 3, respectively.

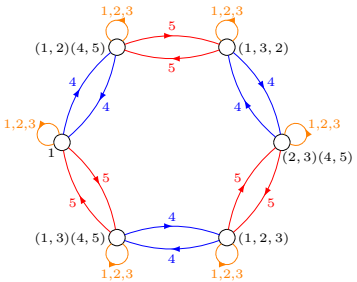


Figure 3.8: Cayley graph of the multiplicative group of $\mathcal{G}(X,r)$

The retraction classes are $\{1,2,3\}$, $\{4\}$, and $\{5\}$. We identify the arcs corresponding in each retraction class and we replace the vertices by the result of the action of $\mathcal{G}(X,r)$ on the blocks of $X/\!\sim$. The result is shown on Figure 3.9. We see that the vertices corresponding in Figure 3.8 to 1, $(1,3,2)$, and $(1,2,3)$ are replaced by 1 in Figure 3.9, because they are the elements of $\mathrm{Soc}(\mathcal{G}(X,r))$.

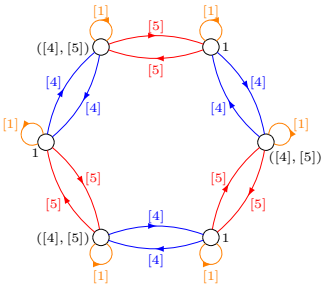


Figure 3.9: Identification in the Cayley graph of $\mathcal{G}(X, r)$ of the arcs in the same retraction class and substitution of the vertices by the result of the action on the blocks

Now the vertices with the same labels must be identified. This gives the graph with two vertices corresponding to $\mathcal{G}(X/\sim, \tilde{r}) = \{1, ([4], [5])\}$ that is drawn on Figure 3.10.

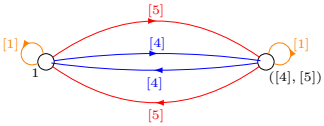


Figure 3.10: Identification of equal vertices in the retraction

We can also repeat the process to find that (X, r) is a multipermutation solution with multipermutation level 3. If we call $X_1 = X/\sim = \{[1] = \{1, 2, 3\}, [4] = \{4\}, [5] = \{5\}\}$, or $X_1 = \{1, 4, 5\}$ for shorter, and $r_1 = \tilde{r}$, its retraction is $X_2 = X_1/\sim = \{[1] = \{1\}, [4] = \{4, 5\}\}$ and Figure 3.11 shows the Cayley graph of $\mathcal{G}(X_2, r_2 = \tilde{r}_1)$.

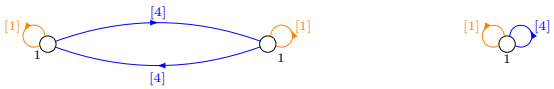


Figure 3.11: Cayley graph of $\mathcal{G}(X_1/\sim, \tilde{r}_1)$

Finally, the retraction of $X_2 = \{1, 4\}$ is $X_3 = \{[1] = \{1, 4\}\}$ which has only one element. Then, (X, r) has multipermutation level 3. The Cayley graph of $\mathcal{G}(X_3, r_3 = \tilde{r}_2)$ is drawn in Figure 3.12.

Figure 3.12: Cayley graph of $\mathcal{G}(X_2/\sim, \tilde{r}_2)$

Our last application is a characterization of when the permutation group of a solution of the YBE is a trivial brace. Since a left brace is trivial whenever it coincides with its socle, Lemma 3.5.8 can be used to obtain this last result.

Proposition 3.5.11. *The following statements are equivalent for a solution (X, r) of the YBE.*

1. *The permutation group $\mathcal{G}(X, r)$ is a trivial brace.*
2. *For every $x, y \in X$, if there exists $\alpha \in \mathcal{G}(X, r)$ such that $\alpha(x) = y$, then $f_x = f_y$ (in other words, x and y are related by the retract relation).*

Proof. The fact that the permutation brace becomes a trivial brace means that the Cayley graph of the composition and the addition of $\mathcal{G}(X, r)$ coincide. This is equivalent to state that for every $x \in X$ and for every $\alpha \in \mathcal{G}(X, r)$, $f_{\alpha(x)} = f_x$. The result holds immediately. □

Example 3.5.12. By the previous proposition, we know that the permutation group of the solution we have been working with (see Example 3.1.7) is not a trivial brace because $f_4 \neq f_5$ even though we can find $\alpha \in \mathcal{G}(X, r)$ with $\alpha(4) = 5$ (we can take f_4 as such α, for example).

Bibliography

[1] J. C. Ault and J. F. Watters. Circle groups of nilpotent rings. *Amer. Math. Monthly*, 80(1):48–52, 1973.

[2] D. Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016.

[3] D. Bachiller. *Study of the Algebraic Structure of Left Braces and the Yang-Baxter Equation*. PhD thesis, 2016.

[4] D. Bachiller, F. Cedó, and E. Jespers. Solutions of the Yang-Baxter equation associated with a left brace. *J. Algebra*, 463:80–102, 2016.

[5] D. Bachiller, F. Cedó, and L. Vendramin. A characterization of finite multipermutation solutions of the Yang-Baxter equation. *Publ. Mat.*, 62:641–649, 2018.

[6] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. Asymmetric product of left braces and simplicity; new solutions of the Yang-Baxter equation, 2017. arXiv:1705.08493.

[7] A. Ballester-Bolinches, E. Cosme-Llópez, and R. Esteban-Romero. Group extensions and graphs. *Expo. Math.*, 34(3):327–334, 2016.

[8] A. Ballester-Bolinches, R. Esteban-Romero, N. Fuster-Corral, and H. Meng. The structure group and the permutation group of a set-theoretic solution of the quantum Yang-Baxter equation. *Mediterr. J. Math.*, in press.

[9] B. Baumslag. A simple way of proving the Jordan-Hölder-Schreier theorem. *The American Mathematical Monthly*, 113(10):933–935, 2006.

[10] R. Baxter. Eight-vertex model in lattice statistics and one-dimensional anisotropic Heisenberg chain. I. Some fundamental eigenvectors. *Ann. Physics*, 76(1):1–24, 1973.

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

[12] F. Cedó, T. Gateva-Ivanova, and A. Smoktunowicz. On the Yang-Baxter equation and left nilpotent left braces. *J. Pure Appl. Algebra*, 221:751–756, 2017.

[13] F. Cedó, E. Jespers, and Á. del Río. Involutive Yang-Baxter groups. *Trans. Amer. Math. Soc.*, 362(5):2541–2558, 2010.

[14] F. Cedó, E. Jespers, and J. Okniński. Braces and the Yang-Baxter equation. *Commun. Math. Phys.*, 327:101–116, 2014.

[15] F. Cedó, E. Jespers, and J. Okniński. Nilpotent groups of class three and braces. *Publ. Mat.*, 60:55–79, 2016.

[16] F. Chouraqui and E. Godelle. Finite quotients of groups of I-type. *Adv. Math.*, 258:46–68, 2014.

[17] V. G. Drinfeld. On some unsolved problems in quantum group theory. In P. P. Kulish, editor, *Quantum groups. Proceedings of workshops held in the Euler International Mathematical Institute, Leningrad, fall 1990*, volume 1510 of *Lecture Notes in Mathematics*, pages 1–8. Springer-Verlag, Berlin, 1992.

[18] F. Eisele. On the IYB-property in some solvable groups. *Arch. Math. (Basel)*, 101(4):309–318, 2013.

[19] P. Etingof, T. Schedler, and A. Soloviev. Set theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100:169–209, 1999.

[20] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.0*, 2020. `http://www.gap-system.org`.

[21] L. Guarnieri and L. Vendramin. Skew-braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

[22] H. Kurzweil and B. Stellmacher. *The theory of finite groups. An introduction*. Universitext. Springer-Verlag, New York, 2004.

[23] H. Meng, A. Ballester-Bolinches, and R. Esteban-Romero. Left braces and the quantum Yang-Baxter equation. *Proc. Edinburgh Math. Soc.*, 62(2):595–608, 2019.

[24] H. Meng, A. Ballester-Bolinches, R. Esteban-Romero, and N. Fuster-Corral. On finite involutive Yang-Baxter groups. *Proc. Amer. Math. Soc.*, 149:793–804, 2021. Published electronically: December 17, 2020.

[25] D. E. Radford. *Hopf algebras*. World Scientific, 2012.

[26] D. J. S. Robinson. *A course in the theory of groups*. Springer-Verlag, New-York, second edition, 1996.

[27] W. Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307:153–170, 2007.

[28] P. R. Sanders. The central automorphisms of a finite group. *J. London Math. Soc.*, 1(1):225–228, 1969.

[29] A. Smoktunowicz. A note on set-theoretic solutions of the Yang-Baxter equation. *Journal of Algebra*, 500:3–18, 2018.

[30] A. Smoktunowicz. On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation. *Trans. Amer. Math. Soc.*, 370(9):6535–6564, 2018.

[31] Y. Sysak. Products of groups and local nearrings. *Note Mat.*, 28:181–216, 2008.

[32] Y. P. Sysak. Products of groups and quantum Yang-Baxter equation. Notes of a talk in *Advances in Group Theory and Applications*, Porto Cesareo, Lecce, Italy, 2011.

[33] L. Vendramin and A. Konovalov. *YangBaxter: Combinatorial Solutions for the Yang-Baxter equation*, November 2019. Version 0.9.0, `https://gap-packages.github.io/YangBaxter/`.

[34] C. N. Yang. Some exact results for many-body problem in one dimension with repulsive delta-function interaction. *Phys. Rev. Lett*, 19:1312–1315, 1967.