TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 362, Number 5, May 2010, Pages 2541–2558
S 0002-9947(09)04927-7
Article electronically published on December 3, 2009

INVOLUTIVE YANG-BAXTER GROUPS

FERRAN CEDÓ, ERIC JESPERS, AND ÁNGEL DEL RÍO

Abstract. In 1992 Drinfeld posed the question of finding the set-theoretic solutions of the Yang-Baxter equation. Recently, Gateva-Ivanova and Van den Bergh and Etingof, Schedler and Soloviev have shown a group-theoretical interpretation of involutive non-degenerate solutions. Namely, there is a one-to-one correspondence between involutive non-degenerate solutions on finite sets and groups of I-type. A group $\mathcal{G}$ of I-type is a group isomorphic to a subgroup of $\mathrm{Fa}_n \rtimes \mathrm{Sym}_n$ so that the projection onto the first component is a bijective map, where Fa_n is the free abelian group of rank n and Sym_n is the symmetric group of degree n. The projection of $\mathcal{G}$ onto the second component Sym_n we call an involutive Yang-Baxter group (IYB group). This suggests the following strategy to attack Drinfeld's problem for involutive non-degenerate set-theoretic solutions. First classify the IYB groups and second, for a given IYB group G, classify the groups of I-type with G as associated IYB group. It is known that every IYB group is solvable. In this paper some results supporting the converse of this property are obtained. More precisely, we show that some classes of groups are IYB groups. We also give a non-obvious method to construct infinitely many groups of I-type (and hence infinitely many involutive non-degenerate set-theoretic solutions of the Yang-Baxter equation) with a prescribed associated IYB group.

1. Introduction

In a paper on statistical mechanics by Yang [18], the quantum Yang-Baxter equation appeared. It turned out to be one of the basic equations in mathematical physics and it lies at the foundation of the theory of quantum groups. One of the important unsolved problems is to discover all the solutions R of the quantum Yang-Baxter equation

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}$$

(here $R : V \otimes V \to V \otimes V$, with V a vector space, R a linear map and R_{ij} denotes the map $V \otimes V \otimes V \to V \otimes V \otimes V$ acting as R on the (i, j) tensor factor (in this order) and as the identity on the remaining factor). In recent years, many

Received by the editors March 26, 2008.

2010 *Mathematics Subject Classification.* Primary 81R50, 20F29, 20B35, 20F16.

Key words and phrases. Yang-Baxter equation, involutive non-degenerate solutions, group of I-type, finite solvable group.

The first author was partially supported by grants of DGI MEC-FEDER (Spain) MTM2005-00934 and Generalitat de Catalunya 2005SGR00206.

The second author was partially supported by grants of Onderzoeksraad of Vrije Universiteit Brussel, Fonds voor Wetenschappelijk Onderzoek (Belgium) and Flemish-Polish bilateral agreement BIL2005/VUB/06.

The third author was partially supported by grants of DGI MEC-FEDER (Spain) MTM2006-06865 and Fundación Séneca of Murcia 04555/GERM/06.

solutions have been found and the related algebraic structures have been intensively studied (see for example [12]). Drinfeld, in [3], posed the question of finding the simplest solutions, that is, the solutions R that are induced by a linear extension of a mapping $\mathcal{R} : X \times X \to X \times X$, where X is a basis for V. In this case, one says that $\mathcal{R}$ is a set-theoretic solution of the quantum Yang-Baxter equation.

Let $\tau : X^2 \to X^2$ be the map defined by $\tau(x, y) = (y, x)$. Observe that $\mathcal{R}$ is a set-theoretic solution of the quantum Yang-Baxter equation if and only if the mapping $r = \tau \circ \mathcal{R}$ is a solution of the braided equation (or a solution of the Yang-Baxter equation, in the terminology used for example in [6, 7])

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}.$$

Set-theoretic solutions $\mathcal{R} : X^2 \to X^2$ of the quantum Yang-Baxter equation (with X a finite set) that are (left) non-degenerate and such that $r = \tau \circ \mathcal{R}$ is involutive (i.e., r^2 is the identity map on X^2) have recently received a lot of attention by Etingof, Schedler and Soloviev [5], Gateva-Ivanova and Van den Bergh [6, 8], Lu, Yan and Zhu [13], Rump [16, 17], Jespers and Okniński [10, 11] and others.[1] Recall that a bijective map

$$\begin{array}{cccc} r\colon & X \times X & \longrightarrow & X \times X \\ & (x, y) & \mapsto & (f_x(y), g_y(x)) \end{array}$$

is said to be left (respectively, right) non-degenerate if each map f_x (respectively, g_x) is bijective. Note that, since X is finite, one can show that an involutive solution of the braided equation is right non-degenerate if and only if it is left non-degenerate (see [10, Corollary 2.3] and [11, Corollary 8.2.4]).

Gateva-Ivanova and Van den Bergh in [8], and Etingof, Schedler and Soloviev in [5], gave a beautiful group-theoretical interpretation of involutive non-degenerate solutions of the braided equation. In order to state this, we need to introduce some notation. Let FaM_n be the free abelian monoid of rank n with basis $u_1, \dots, u_n$. A monoid S generated by a set $X = \{x_1, \dots, x_n\}$ is said to be of left I-type if there exists a bijection (called a left I-structure) $v\colon \mathrm{FaM}_n \longrightarrow S$ such that $v(1) = 1$ and $\{v(u_1 a), \dots, v(u_n a)\} = \{x_1 v(a), \dots, x_n v(a)\}$, for all $a \in \mathrm{FaM}_n$. In [8] it is shown that these monoids S have a presentation

$$S = \langle x_1, \dots, x_n \mid x_i x_j = x_k x_l \rangle,$$

with $\binom{n}{2}$ defining relations so that every word $x_i x_j$ with $1 \leq i, j \leq n$ appears at most once in one of the relations. Such a presentation induces a bijective map $r\colon X \times X \longrightarrow X \times X$ defined by

$$r(x_i, x_j) = \begin{cases} (x_k, x_l), & \text{if } x_i x_j = x_k x_l \text{ is a defining relation for } S; \\ (x_i, x_j), & \text{otherwise.} \end{cases}$$

Furthermore, r is an involutive right non-degenerate solution of the braided equation. Conversely, for every involutive right non-degenerate solution of the braided equation $r\colon X \times X \longrightarrow X \times X$ and every bijection $v : \{u_1, \dots, u_n\} \to X$ there is a unique left I-structure $v : \mathrm{FaM}_n \to S$ extending v, where S is the semigroup given by the following presentation: $S = \langle X \mid ab = cd, \text{ if } r(a, b) = (c, d)\rangle$ ([11, Theorem 8.1.4.]). Furthermore, it is proved in [8] that a monoid of left I-type has a group of fractions, which is called a group of left I-type.

[1] The set-theoretic solutions $\mathcal{R}$ such that r is involutive are called unitary in [16], and in [5] one then says that (X, r) is a symmetric set.

In [10], Jespers and Okniński proved that a monoid S is of left I-type if and only if it is of right I-type and obtained an alternative description of monoids and groups of I-type. Namely, it is shown that a monoid is of I-type if and only if it is isomorphic to a submonoid S of the semidirect product $\mathrm{FaM}_n \rtimes \mathrm{Sym}_n$, with the natural action of Sym_n on FaM_n (that is, $\sigma(u_i) = u_{\sigma(i)}$ for $\sigma \in \mathrm{Sym}_n$), so that the projection onto the first component is a bijective map, that is,

$$S = \{(a, \phi(a)) \mid a \in \mathrm{FaM}_n\},$$

for some map $\phi\colon \mathrm{FaM}_n \to \mathrm{Sym}_n$. In that case the map ϕ extends uniquely to a map $\phi\colon \mathrm{Fa}_n \to \mathrm{Sym}_n$, where Fa_n is the free abelian group of rank n, and the corresponding group of I-type SS^{-1} is isomorphic to a subgroup $\mathcal{G}$ of the semidirect product $\mathrm{Fa}_n \rtimes \mathrm{Sym}_n$ so that the projection onto the first component is a bijective map, that is,

$$\mathcal{G} = \{(a, \phi(a)) \mid a \in \mathrm{Fa}_n\}. \tag{1}$$

Note that if we put $f_{u_i} = \phi(u_i)$, then $S = \langle (u_i, f_{u_i}) \mid 1 \leq i \leq n\rangle$ and one can easily obtain the associated involutive non-degenerate solution $r : X^2 \to X^2$ defining the monoid of I-type. Indeed, if we set $X = \{u_1, \dots, u_n\}$, then $r(u_i, u_j) = (f_{u_i}(u_j), f^{-1}_{f_{u_i}(u_j)}(u_i))$. Obviously, $\phi(\mathrm{Fa}_n) = \langle \phi(a) \mid a \in \mathrm{FaM}_n\rangle = \langle f_{u_i} \mid 1 \leq i \leq n\rangle$. Note that, because of Proposition 2.2 in [5], if $(x, g) \mapsto (f_x(y), g_y(x))$ is an involutive non-degenerate solution of the braided equation, then $T^{-1}g_x^{-1}T = f_x$, where $T : X \to X$ is the bijective map defined by $T(y) = g_y^{-1}(y)$. Hence $\langle f_x : x \in X\rangle$ is isomorphic with $\langle g_x : x \in X\rangle$.

So, in order to describe all involutive non-degenerate solutions of the braided equation (equivalently the non-degenerate unitary set-theoretic solutions of the quantum Yang-Baxter equation) one needs to characterize the groups of I-type. An important first step in this direction is to classify the finite groups that are of the type $\phi(\mathrm{Fa}_n)$ for some group of I-type $\mathcal{G}$, as in (1) (equivalently the groups of the form $\langle f_x : x \in X\rangle$, for $(x, y) \in X^2 \mapsto (f_x(y), g_y(x))$ a non-degenerate involutive solution of the braided equation). A finite group with this property we will call an *involutive Yang-Baxter* (IYB, for short) group. A second step is to describe all groups of I-type that have a fixed associated IYB group G.

In [5, Theorem 2.15], Etingof, Schedler and Soloviev proved that any group of I-type is solvable. As a consequence, every IYB group is solvable. In [5, Theorem 2.9] it is also proved that a group $\mathcal{G}$ is of I-type if and only if there is a bijective 1-cocycle $\mathcal{G} \to \mathrm{Fa}_n$ with respect to some action of $\mathcal{G}$ on Fa_n which factors through the natural action of Sym_n on $\{u_1, \dots, u_n\}$.

Now, if $\mathcal{G} = \{(a, \phi(a)) \mid a \in \mathrm{Fa}_n\}$ is a group of I-type, then the IYB group $G = \phi(\mathrm{Fa}_n)$ naturally acts on the quotient group $A = \mathrm{Fa}_n/K$, where $K = \{a \in \mathrm{Fa}_n \mid \phi(a) = 1\}$ and we obtain a bijective associated 1-cocycle $G \to A$ with respect to this action. By a result of Etingof and Gelaki [4], this bijective 1-cocycle yields a non-degenerate 2-cocycle on the semidirect product $H = A \rtimes G$. This has been generalized by Ben David and Ginosar [1] to more general extensions H of A by G with a bijective 1-cocycle from G to A. This construction of Etingof and Gelaki and of Ben David and Ginosar gives rise to a group of central type in the sense of [1], i.e. a finite group H with a 2-cocycle $c \in Z^2(H, \mathbb{C}^*)$ such that the twisted group algebra $\mathbb{C}^c H$ is isomorphic to a full matrix algebra over the complex numbers, or equivalently $H = K/Z(K)$ for a finite group K with an irreducible character of degree $\sqrt{[K : Z(K)]}$. This provides a nice connection between IYB groups and groups of central type that should be investigated. The authors thank Eli Aljadeff for pointing out this connection.

It is worth mentioning that the semigroup algebra FS of a monoid of I-type S over an arbitrary field F shares many properties with the polynomial algebra in finitely many commuting variables. For example, in [8], it is shown that FS is a domain that satisfies a polynomial identity and that it is a maximal order in its classical ring of quotients. In particular, the group of I-type SS^{-1} is finitely generated abelian-by-finite and torsion free, i.e., it is a Bieberbach group ([8, Theorem 1.7]; see also [10, Corollary 8.27]). The homological properties for FS were the main reasons for studying monoids of I-type in [8], and it was inspired by earlier work of Tate and Van den Bergh on Sklyanin algebras.

In this paper we investigate group-theoretical properties of IYB groups. The content of the paper is as follows. In Section 2 we collect several characterizations of IYB groups that can be found in the literature [5, 16, 17]. These allow us in Section 3 to prove that the class of IYB groups includes the following: finite abelian-by-cyclic groups, finite nilpotent groups of class 2, direct products and wreath products of IYB groups, semidirect products $A \rtimes H$ with A a finite abelian group and H an IYB group, Hall subgroups of IYB groups, Sylow subgroups of symmetric groups Sym_n. These results imply that any finite solvable group is isomorphic to a subgroup of an IYB group, and any finite nilpotent group is a subgroup of an IYB nilpotent group. It is unclear whether the class of IYB groups is closed for taking subgroups. As a consequence, we do not even know whether the class of IYB groups contains all finite nilpotent groups. At this point it nevertheless is tempting to conjecture that the class of IYB groups coincides with that of all solvable finite groups. To prove this, one would like to be able to lift the IYB structure from subgroups H or quotient groups $\overline{G}$ of a given group G to G. In Section 4, we give some examples of IYB groups of minimal order that are not covered by the general results of Section 3. The last example, a 3-group of class 3, shows that not every IYB homomorphism (see Section 2 for the definition) of a quotient of G can be lifted to an IYB homomorphism of G. This indicates that there is no obvious inductive process to prove that nilpotent finite groups are IYB. In Section 5 we consider the connection between set-theoretic solutions of the quantum Yang-Baxter equation and IYB groups from a different perspective. If $r(x_1, x_2) = (f_{x_1}(x_2), g_{x_2}(x_1))$ is an involutive non-degenerate solution on a finite set X of the braided equation, then it is easy to produce, in an obvious manner, infinitely many solutions with the same associated IYB group, namely for every set Y let $r_Y : (X \cup Y)^2 \to (X \cup Y)^2$ be given by $r_Y((x_1, y_1), (x_2, y_2)) = ((f_{x_1}(x_2), y_1), (g_{x_2}(x_1), y_2))$. We show an alternative way of obtaining another involutive non-degenerate solution on $X \times X$ of the braided equation with the same associated IYB group, hence providing, in a non-obvious fashion, infinitely many set-theoretic solutions of the Yang-Baxter equation for the same IYB group.

2. A characterization of IYB groups

In this section we collect several characterizations of IYB groups that can be found in the literature [5, 16, 17].

In [16], Rump introduces cycle sets. A cycle set is a set X with a binary operation $X^2 \to X$, denoted by $(x, y) \mapsto x \cdot y$, such that the left multiplication $y \mapsto x \cdot y$ is bijective for all $x \in X$, and the equation

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z)$$

holds for all $x, y, z \in X$. By [16, Proposition 1 and Theorem 2], there is a bijective correspondence between finite cycle sets and non-degenerate unitary set-theoretic solutions of the quantum Yang-Baxter equation. Indeed, for a finite cycle set X the corresponding involutive non-degenerate solution of the braided equation is $r\colon X^2 \to X^2$ defined by

$$r(x, y) = (f_x(y), g_y(x)),$$

where $g_x^{-1}(y) = x \cdot y$ and $f_y(x) = g_x(y) \cdot x$ for all $x, y \in X$.

A cycle set A with an abelian group structure is called linear [16, 17] if $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c)$ for every $a, b, c \in A$.

In [17], Rump introduced a new entity, called a brace. Recall that this is an abelian (additive) group A with a multiplication $A \times A \to A$ such that for all $a, b, c \in A$,

(1) $(a + b)c = ac + bc$,
(2) $a(bc + b + c) = (ab)c + ab + ac$,
(3) the map $x \mapsto xa + x$ is bijective.

Let A be a brace. The circle operation on A is defined by

$$a \circ b = ab + a + b.$$

By [17, Proposition 4], A is a group with respect to the circle operation, denoted by A°, and it is called the adjoint group of the brace A. The neutral element of the adjoint group A° is 0, the same as the neutral element of the abelian group A. The inverse of $a \in A^\circ$ is denoted by a'.

Theorem 2.1. *The following conditions are equivalent for a finite group G.*

(i) *$G \cong \langle f_x : x \in X\rangle$ (equivalently $G \cong \langle g_x : x \in X\rangle$), for $(x, y) \in X^2 \mapsto (f_x(y), g_y(x))$ a non-degenerate involutive solution of the braided equation.*
(ii) *$G \cong \phi(\mathrm{Fa}_n)$ for a subgroup $\{(a, \phi(a)) : a \in \mathrm{Fa}_n\}$ of $\mathrm{Fa}_n \rtimes \mathrm{Sym}_n$.*
(iii) *There is an abelian group A, an action of G on A and a bijective 1-cocycle $G \to A$.*
(iv) *There is a finite cycle set X such that $G \cong \langle \sigma(X)\rangle$, where $\sigma\colon X \to \mathrm{Sym}_X$ is the map defined by $\sigma(x)(y) = x \cdot y$.*
(v) *There is a finite linear cycle set A such that $G \cong (A, \circ)$, where $\circ$ is the operation defined by $a \circ b = \sigma(b)^{-1}(a) + b$ and $\sigma\colon A \to \mathrm{Sym}_A$ is the map defined by $\sigma(x)(y) = x \cdot y$.*
(vi) *There is a brace A such that $G \cong A^\circ$.*
(vii) *There exists a group homomorphism $\eta : G \to \mathrm{Sym}_G$ satisfying*

$$\eta(x)(y)x = \eta(y)(x)y, \tag{2}$$

for all $x, y \in G$.

(viii) *There exist a generating subset Z of G and a group homomorphism $\eta : G \to \mathrm{Sym}_Z$ satisfying (2) for all $x, y \in Z$.*

Proof. The equivalence of (i)-(iii) is proved in [5] (see Proposition 2.2, Theorems 2.9 and 2.10 and Proposition 2.11 of [5], noting that for every bijective cocycle datum (G, A, ρ, π), there exists a faithful generating set structure (X, ρ', ϕ)). The equivalence of (i) and (iv) follows from Proposition 1 in [16]. More precisely, if $(x, y) \mapsto (f_x(y), g_y(x))$ is an involutive solution of the braided equation, then $x \cdot y =$

$g_x^{-1}(y)$ makes X into a cycle set. Conversely, if $x \cdot y = \sigma(x)(y)$ endows X with a cycle set structure, then $(x, y) \mapsto (f_x(y), g_y(x))$ is an involutive solution of the braided equation, where $g_x(y) = \sigma(x)^{-1}(y)$, and $f_x(y) = g_y(x) \cdot y$ for every $x, y \in X$. The equivalence of (iii), (v) and (vi) follows from Propositions 2, 3 and 5 and Remark 2 of [17].

(vi) *implies* (vii). Let A be a brace and assume that $G = A^\circ$. Then $\eta(a)(b) = ba' + b$ defines a group homomorphism $\eta : G \to \mathrm{Sym}_G$ and we have $\eta(a)(b) \circ a = (ba'+b)a+ba'+b+a = (ba')a+ba+ba'+b+a = b(a'a+a+a')+b+a = b0+b+a = b+a$. Hence $\eta(a)(b) \circ a = \eta(b)(a) \circ b$.

(vii) *implies* (viii) is obvious.

(viii) *implies* (iv). Let $\eta : G = \langle Z \rangle \to \mathrm{Sym}_Z$ be a map satisfying condition (2). Let $\alpha : G \to \mathrm{Sym}_Y$ be a group monomorphism, for some finite set Y such that $Y \cap Z = \emptyset$. Let $X = Y \cup Z$. We define

$$y \cdot x = x, \quad z \cdot y = \alpha(z)(y) \quad \text{and} \quad z \cdot z' = \eta(z)(z'),$$

for all $x \in X$, $y \in Y$ and $z, z' \in Z$. Let $\sigma \colon X \to \mathrm{Sym}_X$ be the map defined by $\sigma(x)(t) = x \cdot t$. Since α and η are group homomorphisms, the restriction of σ to Z, $\sigma|_Z \colon Z \to \mathrm{Sym}_X$, extends to a group homomorphism $f : G \to \mathrm{Sym}_X$ which is injective, because so is α. Thus $G \cong f(G) = \langle \sigma(X) \rangle$. Furthermore, if $x \in Y$ and $t, w \in X$, we have

$$(x \cdot t) \cdot (x \cdot w) = t \cdot w = (t \cdot x) \cdot (t \cdot w),$$

since $t \cdot x \in Y$. If $x, t \in Z$ and $w \in X$, then

$$\begin{aligned} (x \cdot t) \cdot (x \cdot w) &= \eta(x)(t) \cdot \sigma(x)(w) = \sigma(\eta(x)(t))(\sigma(x)(w)) \\ &= f(\eta(x)(t)x)(w) = f(\eta(t)(x)t)(w) \qquad \text{by (2)} \\ &= \sigma(\eta(t)(x))(\sigma(t)(w)) = \eta(t)(x) \cdot \sigma(t)(w) \\ &= (t \cdot x) \cdot (t \cdot w). \end{aligned}$$

It follows that $(X, \cdot)$ is a cycle set. □

Let G be a finite group. Suppose that there exist a generating subset Z of G and a group homomorphism $\eta \colon G \to \mathrm{Sym}_Z$ such that $\eta(x)(y)x = \eta(y)(x)y$ for all $x, y \in Z$. Note that if G^{op} denotes the opposite group of G, then the map $\mu \colon G^{op} \to \mathrm{Sym}_Z$ defined by $\mu(x) = \eta(x)^{-1}$ is a group homomorphism and in G^{op} we have

$$x\mu(x)^{-1}(y) = y\mu(y)^{-1}(x) \tag{3}$$

for all $x, y \in Z$. Since $G \cong G^{op}$, it follows from Theorem 2.1 that a finite group G is IYB if and only if there exist a generating subset Z of G and a group homomorphism $\mu \colon G \to \mathrm{Sym}_Z$ satisfying (3) for all $x, y \in Z$. In that case, there exists a group homomorphism $\mu : G \to \mathrm{Sym}_G$ satisfying condition (3). Such a group homomorphism we call an *IYB morphism* of G.

3. The class of IYB groups

In this section we prove that some classes of groups consist of IYB groups and that the class of IYB groups is closed under some constructions. We start with some easy consequences of the characterization of IYB groups in terms of 1-cocycles.

Recall from the introduction that every group of I-type is solvable, and henceforth so is every IYB group. For the sake of completeness, we include a proof, which is essentially the proof of [5, Theorem 2.15]. Indeed, if $\pi : G \to A$ is a bijective

1-cocycle, then the 1-cocycle condition implies that if B is a characteristic subgroup of A, then $\pi^{-1}(B)$ is a subgroup of G. In particular, if p is a prime and P is the Hall p'-subgroup of A, then $\pi^{-1}(P)$ is a Hall p'-subgroup of G. By a theorem of P. Hall [15, 9.1.8], G is solvable.

Corollary 3.1. *If G is an IYB group, then its Hall subgroups are also IYB.*

Proof. Assume that G is an IYB group. By Theorem 2.1 there is a bijective 1-cocycle $\pi : G \to A$, for some abelian group A. If B is a Hall subgroup of A, then B is invariant under the action of G and hence $H = \pi^{-1}(B)$ is a subgroup of G of the same order as B. Then the restriction of π to H, $\pi|_H : H \to B$, is a bijective 1-cocycle, with respect to the action of H restricted to B. □

Corollary 3.2. *The class of IYB groups is closed under direct products.*

Proof. Let G_1 and G_2 be IYB groups. By Theorem 2.1 there are bijective 1-cocycles $\pi_i : G_i \to A_i$ with respect to some action of G_i on an abelian group A_i $(i = 1, 2)$. Then $\pi_1 \times \pi_2 : G_1 \times G_2 \to A_1 \times A_2$ is a bijective 1-cocycle with respect to the obvious action of $G_1 \times G_2$ on $A_1 \times A_2$, namely $(g_1, g_2)(a_1, a_2) = (g_1(a_1), g_2(a_2))$. □

The next two results provide more closure properties of the class of IYB groups.

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. Suppose that there is a bijective 1-cocycle $\pi : H \to B$, with respect to an action of H on the abelian group B 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 IYB.

Proof. Let $N = \{(h^{-1}, \pi(h)) \in H \times B \mid h \in H \cap A\}$. Since $H \cap A$ acts trivially on B, $\pi(ah) = \pi(a)\pi(h)$ for every $a \in A \cap H$ and $h \in H$. It follows that N is a subgroup of $A \times B$.

Let $C = (A \times B)/N$ and let $\overline{(a, b)}$ denote the class of $(a, b) \in A \times B$ modulo N. Note that $|G| = |C|$. Define the following action of G on C:

$$g\overline{(a, b)} = \overline{(gag^{-1}, h(b))},$$

for all $a \in A$, $b \in B$ and $g = a'h \in G$, with $a' \in A$ and $h \in H$. We shall see that this is well defined and it indeed is an action. Let $a, a' \in A$ and $b, b' \in B$ such that $\overline{(a, b)} = \overline{(a', b')}$. We have $h^{-1} = a^{-1}a' \in H \cap A$ and $\pi(h) = b^{-1}b'$. Let $g = a_1h_1 = a_2h_2 \in G$, with $a_1, a_2 \in A$ and $h_1, h_2 \in H$. Since A is an abelian normal subgroup of G, we have

$$(gag^{-1})^{-1}ga'g^{-1} = h_1a^{-1}a'h_1^{-1} = h_1h^{-1}h_1^{-1} \in H \cap A$$

and

$$h_2^{-1}h_1 = h_2^{-1}(h_1h_2^{-1})h_2 = h_2^{-1}(a_1^{-1}a_2)h_2 \in H \cap A.$$

Since $h, h_2^{-1}h_1 \in H \cap A$ and $H \cap A$ acts trivially on B, we have

$$\begin{aligned}
\pi(((gag^{-1})^{-1}ga'g^{-1})^{-1}) &= \pi(h_1hh_1^{-1}) = \pi(h_1)h_1(\pi(hh_1^{-1})) \\
&= \pi(h_1)h_1(\pi(h)\pi(h_1^{-1})) = \pi(h_1)h_1(\pi(h))h_1(\pi(h_1^{-1})) \\
&= \pi(h_1)h_1(\pi(h_1^{-1}))h_1(\pi(h)) = \pi(h_1h_1^{-1})h_1(\pi(h)) \\
&= h_1(\pi(h)) = h_1(b^{-1}b') \\
&= h_1(b)^{-1}h_1(b') = h_2(b)^{-1}h_1(b').
\end{aligned}$$

Hence $\overline{(gag^{-1}, h_2(b))} = \overline{(ga'g^{-1}, h_1(b'))}$. Furthermore, if $g, g' \in G$, $g = bh$ and $g' = b'h'$, with $b, b' \in A$ and $h, h' \in H$, then we have $gg' = (bhb'h^{-1})hh'$ and

$$(gg')\overline{(a,b)} = \overline{((gg')a(gg')^{-1}, (hh')(b))} = \overline{(g(g'ag'^{-1})g^{-1}, h(h'(b)))} = g(g'\overline{(a,b)}).$$

Therefore we have a well-defined action of G on C.

We define $\bar{\pi} \colon G \to C$ by

$$\bar{\pi}(g) = \overline{(a, \pi(h))}$$

for all $g \in G$ with $g = ah$, where $a \in A$ and $h \in H$. Note that if $g = ah = a'h'$ with $a, a' \in A$ and $h, h' \in H$, then $a^{-1}a' = hh'^{-1} \in H \cap A$, $h^{-1}h' = h'^{-1}(hh'^{-1})^{-1}h' \in H \cap A$ and hence

$$\begin{aligned} \pi((a^{-1}a')^{-1}) &= \pi(h'h^{-1}) = \pi(h')h'(\pi(h^{-1})) \\ &= \pi(h')hh^{-1}h'(\pi(h^{-1})) = \pi(h')h(\pi(h^{-1})) \\ &= \pi(h')\pi(h)^{-1}, \end{aligned}$$

because $H \cap A$ acts trivially on B. Hence $\bar{\pi}$ is well defined. Let $g_1 = a_1h_1$ and $g_2 = a_2h_2$, with $a_1, a_2 \in A$ and $h_1, h_2 \in H$. We have

$$\begin{aligned} \bar{\pi}(g_1g_2) &= \bar{\pi}((a_1h_1a_2h_1^{-1})h_1h_2) = \overline{(a_1h_1a_2h_1^{-1}, \pi(h_1h_2))} \\ &= \overline{(a_1h_1a_2h_1^{-1}, \pi(h_1)h_1(\pi(h_2)))} = \overline{(a_1, \pi(h_1))}\ \overline{(h_1a_2h_1^{-1}, h_1(\pi(h_2)))} \\ &= \overline{(a_1, \pi(h_1))}g_1\overline{(a_2, \pi(h_2))} = \bar{\pi}(g_1)g_1(\bar{\pi}(g_2)). \end{aligned}$$

Hence $\bar{\pi}$ is a bijective 1-cocycle and we conclude that G is an IYB group, by Theorem 2.1. □

Note that in the framework of braces, Theorem 3.3 can be rephrased as follows. Let G be a finite group so that $G = AH$ with A an abelian normal subgroup and assume that the subgroup H is the adjoint group of a brace B such that $H \cap A$ acts trivially on B (i.e., $bh + b = b$ for every $b \in B$ and $h \in H \cap A$). Then G is IYB. The proof in this context however is not shorter.

Theorem 3.4. *Let N and H be IYB groups and let $\pi_N : N \to A$ be a bijective 1-cocycle with respect to an action of N on an abelian group A. If $\gamma : H \to \operatorname{Aut}(N)$ and $\delta : H \to \operatorname{Aut}(A)$ are actions of H on N and A respectively such that $\delta(h)\pi_N = \pi_N\gamma(h)$ for every $h \in H$, then the semidirect product $N \rtimes H$, with respect to the action γ, is an IYB group.*

Proof. Let $\alpha : N \to \operatorname{Aut}(A)$ be an action of N on the abelian group A such that $\pi_N : N \to A$ is a bijective 1-cocycle. Let $\pi_H : H \to B$ be a bijective 1-cocycle with respect to the action $\beta : H \to \operatorname{Aut}(B)$. We are going to denote by α_n, β_h, γ_h and δ_h the images of $n \in N$ or $h \in H$ under the respective maps α, β, γ and δ.

If $h \in H$ and $n_1, n_2 \in N$, then

$$\begin{aligned} \delta_h\pi_N(n_1)\ \delta_h\alpha_{n_1}(\pi_N(n_2)) &= \delta_h(\pi_N(n_1)\ \alpha_{n_1}(\pi_N(n_2))) = \delta_h\pi_N(n_1n_2) \\ &= \pi_N\gamma_h(n_1n_2) = \pi_N(\gamma_h(n_1)\gamma_h(n_2)) \\ &= \pi_N\gamma_h(n_1)\alpha_{\gamma_h(n_1)}(\pi_N\gamma_h(n_2)) \\ &= \delta_h\pi_N(n_1)\alpha_{\gamma_h(n_1)}\delta_h(\pi_N(n_2)). \end{aligned}$$

This shows that

$$\delta_h\alpha_n = \alpha_{\gamma_h(n)}\delta_h \qquad (4)$$

for every $h \in H$ and $n \in N$.

Now we define the following map $\sigma : G = N \rtimes H \to \operatorname{Aut}(A \times B)$:

$$\sigma_{nh}(a,b) = (\alpha_n\delta_h(a), \beta_h(b)),$$

for all $n \in N$ and $h \in H$. Since both α_n and δ_h are automorphisms of A and β_h is an automorphism of B, σ_{nh} is an automorphism of $A \times B$. Now we check that σ is a group homomorphism. Let $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Then

$$\begin{aligned}
\sigma_{n_1h_1n_2h_2}(a,b) &= \sigma_{n_1\gamma_{h_1}(n_2)h_1h_2}(a,b) = (\alpha_{n_1\gamma_{h_1}(n_2)}\delta_{h_1h_2}(a), \beta_{h_1h_2}(b)) \\
&= (\alpha_{n_1}\alpha_{\gamma_{h_1}(n_2)}\delta_{h_1}\delta_{h_2}(a), \beta_{h_1}\beta_{h_2}(b)) \\
&= (\alpha_{n_1}\delta_{h_1}\alpha_{n_2}\delta_{h_2}(a), \beta_{h_1}\beta_{h_2}(b)) \quad \text{(by (4))} \\
&= \sigma_{n_1h_1}\sigma_{n_2h_2}(a,b).
\end{aligned}$$

Thus σ is an action of G on $A \times B$.

Let $\pi : G \to A \times B$ be given by $\pi(nh) = (\pi_N(n), \pi_H(h))$. Since both $\pi_N : N \to A$ and $\pi_H : H \to B$ are bijective, so is π. Moreover

$$\begin{aligned}
\pi(n_1h_1n_2h_2) &= \pi(n_1\gamma_{h_1}(n_2)h_1h_2) = (\pi_N(n_1\gamma_{h_1}(n_2)), \pi_H(h_1h_2)) \\
&= (\pi_N(n_1)\alpha_{n_1}\pi_N\gamma_{h_1}(n_2), \pi_H(h_1)\beta_{h_1}(\pi_H(h_2))) \\
&= (\pi_N(n_1)\alpha_{n_1}\delta_{h_1}\pi_N(n_2), \pi_H(h_1)\beta_{h_1}(\pi_H(h_2))) \\
&= (\pi_N(n_1), \pi_H(h_1))(\alpha_{n_1}\delta_{h_1}\pi_N(n_2), \beta_{h_1}(\pi_H(h_2))) \\
&= \pi(n_1h_1)\sigma_{n_1h_1}(\pi(n_2h_2)),
\end{aligned}$$

for all $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Thus π is a bijective 1-cocycle and we conclude that G is an IYB group. □

Corollary 3.5. *Let G be an IYB group and H an IYB subgroup of* Sym_n. *Then the wreath product $G \wr H$ of G and H is an IYB group.*

Proof. Recall that $W = G \wr H$ is the semidirect product $G^n \rtimes H$, where the action of H on G^n is given by $\gamma_h(g_1, \dots, g_n) = (g_{h(1)}, \dots, g_{h(n)})$. Since G is an IYB group, there is an action on an abelian group A which admits a bijective 1-cocycle $\pi : G \to A$. This action, applied componentwise, induces an action α of G^n on A^n and the map $\bar{\pi} : G^n \to A^n$, which acts as π componentwise, is a bijective 1-cocycle (see the proof of Corollary 3.2). Furthermore the map $\delta : H \to \operatorname{Aut}(A^n)$, given by $\delta_h(a_1, \dots, a_n) = (a_{h(1)}, \dots, a_{h(n)})$, for all $h \in H$ and $(a_1, \dots, a_n) \in A^n$, is an action of H on A^n such that $\delta_h\bar{\pi} = \bar{\pi}\gamma_h$ for every $h \in H$. Thus W is an IYB group, by Theorem 3.4. □

Corollary 3.6. *Any finite solvable group is isomorphic to a subgroup of an IYB group.*

Proof. Let G be a finite solvable group. By [9, Satz I.15.9], it is easy to see that G is isomorphic to a subgroup of $(\dots((A_1 \wr A_2) \wr A_3)\dots) \wr A_n$, where

$$\langle 1 \rangle = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

is a subnormal series for G with abelian quotients $A_i = G_i/G_{i-1}$, for $i = 1, \dots, n$. Since finite abelian groups are IYB groups, the result follows by Corollary 3.5. □

Corollary 3.7. *Let n be a positive integer. Then the Sylow subgroups of* Sym_n *are IYB groups.*

Proof. It is known that the Sylow p-subgroups of Sym_n are isomorphic to a group of the form $G_1 \times G_2$ or $G_3 \wr C_p$, where G_1, G_2, G_3 are Sylow p-subgroup of Sym_{m_1}, Sym_{m_2}, Sym_{m_3}, respectively, for some $m_1, m_2, m_3 < n$, [14, pages 10,11]. Since C_p is an IYB group, the result follows from Corollaries 3.2 and 3.5 by induction on n. □

As a consequence of this result and Corollary 3.2, we have the following result.

Corollary 3.8. *Any finite nilpotent group is isomorphic to a subgroup of an IYB nilpotent group.*

The next result yields many examples of IYB groups.

Theorem 3.9. *Let G be a finite group having a normal sequence*

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

satisfying the following conditions:

(i) *For every $1 \le i \le n$, $G_i = G_{i-1}A_i$ for some abelian subgroup A_i.*
(ii) $(G_{i-1} \cap (A_i \cdots A_n), G_{i-1}) = 1$.
(iii) *A_i is normalized by A_j for every $i \le j$.*

Then G is an IYB group.

Proof. Assumption (iii) implies that for every $1 \le i, j \le n$, either A_i normalizes A_j or A_j normalizes A_i. Thus A_iA_j is a subgroup of G and $A_iA_j = A_jA_i$. Furthermore $G_i = A_1 \dots A_i$ and, in particular, $Z = A_1 \cup \cdots \cup A_n$ is a generating subset of G. We set $H_i = A_{i+1} \dots A_n$ for every $1 \le i \le n$. Then A_i normalizes G_j and H_i normalizes A_j for every $j \le i$. In particular, $G_i \trianglelefteq G$ for every i. Every $g \in G$ can be written, in a non-necessarily unique way, as $g = g_{i1}g_{i2}$ with $g_{i1} \in G_i$ and $g_{i2} \in H_i$.

Define $\mu \colon G \to \mathrm{Sym}_Z$ by

$$\mu(g)(a) = g_{(i-1)2}ag_{(i-1)2}^{-1},$$

for every $g \in G$ and $a \in A_i$, with $i \ge 1$. We need to show that the map μ is well defined. So let $g = a_1 \dots a_n = b_1 \dots b_n$, with $a_j, b_j \in A_j$, for every $j = 1, \dots, n$ and let $a \in A_i$. We can take $g_{i1} = a_1 \dots a_i \in G_i$ and $g_{i2} = a_{i+1} \dots a_n \in H_i$, or we can take $\bar{g}_{i1} = b_1 \dots b_i \in G_i$ and $\bar{g}_{i2} = b_{i+1} \dots b_n \in H_i$. Since $G_i \trianglelefteq G$ and $g_{i1}g_{i2} = \bar{g}_{i1}\bar{g}_{i2}$,

$$\bar{g}_{i2}^{-1}g_{i2} = \bar{g}_{i2}^{-1}g_{i1}^{-1}\bar{g}_{i1}\bar{g}_{i2} \in G_i \cap H_i.$$

Hence, by condition (ii), $\bar{g}_{i2}^{-1}g_{i2}ag_{i2}^{-1}\bar{g}_{i2} = a$. Thus

$$g_{i2}ag_{i2}^{-1} = \bar{g}_{i2}a\bar{g}_{i2}^{-1} \in A_i.$$

Since A_i is abelian, conjugating by a_i on the left side of the previous equality and by b_i on the right side we have

$$g_{(i-1)2}ag_{(i-1)2}^{-1} = \bar{g}_{(i-1)2}a\bar{g}_{(i-1)2}^{-1}.$$

Suppose that $a \in A_i \cap A_{i'}$ with $i' < i$. Since H_i normalizes both A_i and $A_{i'}$ and A_i is abelian we have

$$g_{(i-1)2}ag_{(i-1)2}{}^{-1} = a_ig_{i2}ag_{i2}^{-1}a_i^{-1} \in A_{i'} \cap A_i \subseteq G_{i-1} \cap A_i.$$

Since $g_{(i'-1)2}g^{-1}_{(i-1)2} = a_{i'}a_{i'+1}\cdots a_{i-1} \in G_{i-1}$, by (ii),

$$g_{(i-1)2}ag^{-1}_{(i-1)2} = g_{(i'-1)2}ag^{-1}_{(i'-1)2}.$$

Therefore μ is well defined.

Let $g, h \in G$ and $a \in A_i$. Then, with the above notation,

$$\begin{aligned} \mu(gh)(a) &= \mu(g_{i1}g_{i2}h_{i1}h_{i2})(a) = \mu((g_{i1}g_{i2}h_{i1}g_{i2}^{-1})(g_{i2}h_{i2}))(a) \\ &= \mu(g_{i2}h_{i2})(a) = g_{i2}h_{i2}ah_{i2}^{-1}g_{i2}^{-1} = \mu(g)\mu(h)(a). \end{aligned}$$

Hence μ is a group homomorphism.

Let $a \in A_i$ and $b \in A_j$ with $i \leq j$. Then

$$a\mu(a)^{-1}(b) = ab = bb^{-1}ab = b\mu(b)^{-1}(a).$$

By Theorem 2.1, G is an IYB group. □

Corollary 3.10. *Let G be a finite group. If $G = NA$, where N and A are two abelian subgroups of G and N is normal in G, then G is an IYB group.*

In particular, every abelian-by-cyclic finite group is IYB.

Corollary 3.11. *Every finite nilpotent group of class 2 is IYB.*

Proof. Let G be a finite nilpotent group of class 2. Then there exist $x_1, \dots, x_n \in G$ such that $G/Z(G)$ is the inner direct product of $\langle \bar{x}_1 \rangle, \dots, \langle \bar{x}_n \rangle$, where $\bar{x}$ denotes the class of $x \in G$ modulo its center $Z(G)$. Let $A_i = \langle \{x_i\} \cup Z(G) \rangle$, for all $i = 1, \dots, n$. Let $G_i = A_1 \cdots A_i$, for all $i = 1, \dots, n$. It is easy to check that the group G and the subgroups A_i and G_i satisfy the hypotheses of Theorem 3.9. Hence G is an IYB group. □

4. Examples

In Section 3 we have given some sufficient conditions for a finite group to be IYB. In this section we present some examples of IYB that are not covered by these results.

Example 4.1. A group of smallest order not satisfying the conditions of Theorem 3.9 is

$$G = Q_8 \rtimes C_3 = \langle x, y, a \mid x^4 = x^2y^2 = a^3 = 1, x^y = x^{-1}, axa^{-1} = y, aya^{-1} = xy \rangle.$$

One may try to show that G is IYB by using Theorem 3.3 and Corollary 3.10. However, the straightforward approach does not work. Nevertheless, we can still show that G is IYB as follows.

Let $Z = \{x, x^{-1}, y, y^{-1}, xy, yx, a\}$ and define $\mu\colon Z \to \mathrm{Sym}_Z$ by

$$\begin{aligned} \mu(x) = \mu(x^{-1}) = (x, x^{-1})(y, y^{-1}), &\quad \mu(y) = \mu(y^{-1}) = (y, y^{-1})(xy, yx), \\ \mu(xy) = \mu(yx) = (x, x^{-1})(xy, yx), &\quad \mu(a) = (x, y, xy)(x^{-1}, y^{-1}, yx). \end{aligned}$$

Note that $\mu(x)\mu(y) = \mu(xy)$, $\mu(x)^4 = \mu(x)^2\mu(y)^2 = \mu(a)^3 = \mathrm{id}$, $\mu(x)^{\mu(y)} = \mu(x^{-1}), \mu(a)\mu(x)\mu(a)^{-1} = \mu(y), \mu(a)\mu(y)\mu(a)^{-1} = \mu(x)\mu(y)$. Hence μ extends to a homomorphism $\mu\colon Q_8 \rtimes C_3 \to \mathrm{Sym}_Z$. It is easy to check that

$$u\mu(u^{-1})(v) = v\mu(v)^{-1}(u)$$

for all $u, v \in Z$. Therefore, $Q_8 \rtimes C_3$ is an IYB group, by Theorem 2.1. □

Example 4.2. By Corollary 3.10, every abelian-by-cyclic group is IYB. However it is not clear whether every cyclic-by-abelian group is IYB. In this example we show that some class of cyclic-by-abelian groups consists of IYB groups. It includes all cyclic-by-two generated abelian p-groups.

Consider the following cyclic-by-abelian group of order nq_1q_2:

$$G = \langle a, b, c \mid a^n = 1, bab^{-1} = a^{r_1}, cac^{-1} = a^{r_2}, b^{q_1} = a^{s_1}, c^{q_2} = a^{s_2}, cbc^{-1} = a^t b\rangle.$$

Then the following conditions hold, where $o_n(r)$ denotes the multiplicative order of r modulo n (for $(r,n)=1$):

$$\begin{array}{ll} o_n(r_i)|q_i & \text{(because } (a, b_i^{q_i}) = 1\text{)},\\ s_i(r_i - 1) \equiv 0 \mod n & \text{(because } (a^{s_1}, b) = 1 = (a^{s_2}, c)\text{)},\\ t\sum_{j=0}^{q_1-1} r_1^j \equiv s_1(r_2 - 1) \mod n & \text{(because } (a^t b)^{q_1} = ca^{s_1}c^{-1}\text{)},\\ -t\sum_{j=0}^{q_2-1} r_2^j \equiv s_2(r_1 - 1) \mod n & \text{(because } (a^{-t}c)^{q_2} = ba^{s_2}b^{-1}\text{)}. \end{array}$$

We also assume that there is an integer u such that

$$r_1 - 1 \equiv u(r_2 - 1) \mod n. \tag{5}$$

Let $A = \langle a\rangle$. Set $Z = \{a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b, c\}$, a generating subset of G, and let $f, g \in \mathrm{Sym}_Z$ be given by

$$f : \begin{cases} a^i \mapsto a^{ir_1} & (1 \le i < n),\\ a^j b \mapsto a^{tu + r_1 j} b & (0 \le j < n),\\ c \mapsto c, \end{cases}$$

$$g(x) = cxc^{-1}, \text{ for each } x \in Z.$$

We claim that

$$f^{q_1} = g^{q_2} = (f, g) = 1. \tag{6}$$

Since $c^{q_2} = a^{s_2}$ and $s_2(r_2 - 1) \equiv 0 \mod n$ and $s_2(r_1 - 1) \equiv us_2(r_2 - 1) \equiv 0 \mod n$, one has that $c^{q_2} \in Z(G)$ and so $g^{q_2} = 1$. Notice that $f(a^i) = ba^ib^{-1}$ for each i. Since $b^{q_1} \in \langle a\rangle$, one has $f^{q_1}(a^i) = a^i$. On the other hand,

$$tu(1 + r_1 + r_1^2 + \dots + r_1^{q_1-1}) \equiv us_1(r_2 - 1) \equiv s_1(r_1 - 1) \equiv 0 \mod n.$$

Using this and that $o_n(r_1)|q_1$, one has

$$f^{q_1}(a^j b) = a^{tu(1 + r_1 + r_1^2 + \dots + r_1^{q_1-1}) + r_1^{q_1} j} b = a^j b.$$

This shows that $f^{q_1} = 1$. Now we check that $gf = fg$. Since the actions of f and g on the powers of a are by conjugation by b and c, respectively, the action of (f, g) on these powers is by conjugation by $(b, c) = a^t$ and so $(f, g)(a^i) = a^i$. Finally

$$\begin{aligned} gf(a^j b) &= g(a^{tu + r_1 j} b) = a^{(tu + r_1 j)r_2 + t} b = a^{tu(r_2 - 1) + tu + r_1 r_2 j + t} b\\ &= a^{t(r_1 - 1) + tu + r_1 r_2 j + t} b = a^{tu + r_1(r_2 j + t)} b = f(a^{r_2 j + t} b) = fg(a^j b). \end{aligned}$$

This proves the claim.

Since $G/A \cong C_{q_1} \times C_{q_2}$, there is a group homomorphism $\mu : G \to \mathrm{Sym}_Z$ such that $\mu(a) = \mathrm{id}$, $\mu(b) = f$ and $\mu(c) = g$. Now we check (3) for all $x, y \in Z$. If $x \in \langle a\rangle$, then $\mu(x) = \mathrm{id}$ and $\mu(y)(x) = yxy^{-1}$. Thus $x\mu(x)^{-1}(y) = xy = y(y^{-1}xy) = y\mu(y)^{-1}(x)$ as wanted. If $x = c$, then $\mu(y)(x) = x$ and $\mu(x)(y) = xyx^{-1}$. Again $x\mu(x)^{-1}(y) = xx^{-1}yx = yx = y\mu(y)^{-1}(x)$. By symmetry, (3) also holds if $y \in \langle a\rangle \cup \{c\}$. If v is an inverse of r_1 modulo n, then $f^{-1}(a^jb) = a^{v(j-tu)}b$. Thus, for $x = a^ib, y = a^jb$, one has

$$\begin{aligned} x\mu(x)^{-1}(y) = xf^{-1}(y) = a^iba^{v(j-tu)}b = a^{i+r_1v(j-tu)}b^2 = a^{i+j-tu}b^2 \\ = a^{j+r_1v(i-tu)}b^2 = a^jba^{v(i-tu)}b = yf^{-1}(x) = y\mu(y)^{-1}(x). \end{aligned}$$

We conclude that if condition (5) holds, then, by Theorem 2.1, G is an IYB group. Notice that if n is a prime power, then, by interchanging the roles of b and c if needed, one may assume that condition (5) holds because the lattice of additive subgroups of $\mathbb{Z}_n$ is linearly ordered. So if G has a normal cyclic p-subgroup A such that G/A is 2-generated and abelian, then G is IYB. □

Example 4.3. By Corollaries 3.10 and 3.11 every nilpotent group of class at most 2 is IYB and every group which is a product of two abelian subgroups, one of them normal, is IYB. In this example we consider a 3-group of minimal order not satisfying any of these properties. Namely let G be the group given by the following presentation:

$$\begin{aligned} G \quad = \quad & \langle a, b, c, d, e \mid a, b \in Z(G), dc = acd, ec = bce, \\ & \qquad ed = cde, a^3 = b^3 = c^3 = d^3 = e^3 = 1\rangle. \end{aligned}$$

If $i_1, i_2 \in \{0, 1, 2\}, j_1, j_2 \in \{0, 1\}$, then

$$d^{i_1}e^{j_1}d^{i_2}e^{j_2} = a^{2i_2(i_2-1)j_1+i_1i_2j_1}c^{i_2j_1}d^{i_1+i_2}e^{j_1+j_2}. \tag{7}$$

Let $H = \langle G', d\rangle$ and $Z = H \cup He$. Let $D, E \in \mathrm{Sym}_Z$ be given by

$$D(nd^ie^j) = dnd^{-1}a^{i+2ij}b^{2i}c^{2j}d^ie^j \quad \text{and} \quad E(nd^ie^j) = ene^{-1}d^{i+j}e^j$$

($n \in G', i = 0, 1, 2; j = 0, 1$).

If $n \in G'$, $i = 0, 1, 2$ and $j = 0, 1$, then

$$D^k(nd^ie^j) = D^k(n)D^k(d^i)D^k(e^j) = d^knd^{-k}a^{k(i+2ij)+k(k-1)j}b^{2ik}c^{2kj}d^ie^j \tag{8}$$

and

$$E^k(nd^ie^j) = E^k(n)E^k(d^i)E^k(e^j) = e^kne^{-k}d^{i+kj}e^j, \tag{9}$$

for all positive integer k. Moreover,

$$\begin{aligned} ED(nd^ie^j) \quad &= \quad E(dnd^{-1}a^{i+2ij}b^{2i}c^{2j}d^ie^j) = ednd^{-1}e^{-1}a^{i+2ij}b^{2(i+j)}c^{2j}d^{i+j}e^j \\ &= \quad c(dene^{-1}d^{-1})c^{-1}a^{i+2ij}b^{2(i+j)}c^{2j}d^{i+j}e^j \\ &= \quad dene^{-1}d^{-1}a^{i+2ij}b^{2(i+j)}c^{2j}d^{i+j}e^j \\ &= \quad D(ene^{-1}d^{i+j}e^j) = DE(nd^ie^j). \end{aligned}$$

Thus $ED = DE$ and $D^3 = E^3 = 1$ and therefore there is a unique group homomorphism $\mu : G \to \mathrm{Sym}_Z$ such that $\mu(G') = 1$, $\mu(d) = D$ and $\mu(e) = E$. We will check (3) for all $x, y \in Z$. Let $x = m_1d^{i_1}e^{j_1}$ and $y = m_2d^{i_2}e^{j_2}$, with $m_1, m_2 \in G'$,

$i_1, i_2 \in \{0,1,2\}$ and $j_1, j_2 \in \{0,1\}$. We have

$$\begin{aligned}
x\mu(x)^{-1}(y) &= m_1 d^{i_1} e^{j_1} \mu(m_1 d^{i_1} e^{j_1})^{-1}(m_2 d^{i_2} e^{j_2}) \\
&= m_1 m_2 d^{i_1} e^{j_1} E^{2j_1} D^{2i_1}(d^{i_2} e^{j_2}) && \text{(by (8) and (9))} \\
&= m_1 m_2 d^{i_1} e^{j_1} \\
&\quad \cdot E^{2j_1}(a^{2i_1(i_2+2i_2j_2)+2i_1(2i_1-1)j_2} b^{i_1i_2} c^{i_1j_2} d^{i_2} e^{j_2}) && \text{(by (8))} \\
&= m_1 m_2 d^{i_1} e^{j_1} a^{2i_1(i_2+2i_2j_2)+2i_1(2i_1-1)j_2} b^{i_1i_2+2i_1j_1j_2} \\
&\quad \cdot c^{i_1j_2} d^{i_2+2j_1j_2} e^{j_2} && \text{(by (9))} \\
&= m_1 m_2 a^{2i_1(i_2+2i_2j_2)+2i_1(2i_1-1)j_2+i_1^2j_2} b^{i_1i_2} c^{i_1j_2} d^{i_1} e^{j_1} d^{i_2+2j_1j_2} e^{j_2}
\end{aligned}$$

$$\begin{aligned}
&= m_1 m_2 a^{2i_1(i_2+2i_2j_2)+2i_1(2i_1-1)j_2+i_1^2j_2+2(i_2+2j_1j_2)(i_2+2j_1j_2-1)j_1+i_1(i_2+2j_1j_2)j_1} \\
&\quad \cdot b^{i_1i_2} c^{i_1j_2+(i_2+2j_1j_2)j_1} d^{i_1+i_2+2j_1j_2} e^{j_1+j_2} && \text{(by (7))} \\
&= m_1 m_2 a^{2i_1i_2+i_1i_2j_2+2i_1^2j_2+i_1j_2+2i_2^2j_1+2i_2j_1^2j_2+2j_1^3j_2^2-2i_2j_1-j_1^2j_2+i_1i_2j_1+2i_1j_1^2j_2} \\
&\quad \cdot b^{i_1i_2} c^{i_1j_2+i_2j_1+2j_1^2j_2} d^{i_1+i_2+2j_1j_2} e^{j_1+j_2} \\
&= m_1 m_2 a^{2i_1i_2+i_1i_2j_2+2i_1^2j_2+i_1j_2+2i_2^2j_1+2i_2j_1j_2+2j_1j_2-2i_2j_1-j_1j_2+i_1i_2j_1+2i_1j_1j_2} \\
&\quad \cdot b^{i_1i_2} c^{i_1j_2+i_2j_1+2j_1j_2} d^{i_1+i_2+2j_1j_2} e^{j_1+j_2} \quad \text{(since } j_1^2 = j_1 \text{ and } j_2^2 = j_2\text{)} \\
&= m_1 m_2 a^{2i_1i_2+i_1i_2(j_1+j_2)+2(i_1^2j_2+i_2^2j_1)+i_1j_2+i_2j_1+2(i_1+i_2)j_1j_2+j_1j_2} \\
&\quad \cdot b^{i_1i_2} c^{i_1j_2+i_2j_1+2j_1j_2} d^{i_1+i_2+2j_1j_2} e^{j_1+j_2}.
\end{aligned}$$

This expression is invariant by interchanging m_1 and m_2, i_1 and i_2, and j_1 and j_2. Hence it follows that $x\mu(x)^{-1}(y) = y\mu(y)^{-1}(x)$. By Theorem 2.1, G is IYB. □

Let μ be an IYB morphism of G. We prove the following equality:

$$\mu(x)(yz) = \mu(x)(y) \cdot \mu(\mu(y)^{-1}(x^{-1}))^{-1}(z) \qquad (x,y,z \in G). \tag{10}$$

Indeed

$$\begin{aligned}
\mu(x)(yz) &= xx^{-1}\mu(x^{-1})^{-1}(yz) = xyz\mu(yz)^{-1}(x^{-1}) \\
&= xyz\mu(z)^{-1}(\mu(y)^{-1}(x^{-1})) \\
&= xy\mu(y)^{-1}(x^{-1})\mu(\mu(y)^{-1}(x^{-1}))^{-1}(z) \\
&= xx^{-1}\mu(x^{-1})^{-1}(y)\mu(\mu(y)^{-1}(x^{-1}))^{-1}(z) \\
&= \mu(x)(y)\mu(\mu(y)^{-1}(x^{-1}))^{-1}(z).
\end{aligned}$$

Note that $\ker(\mu)$ is abelian. If $x \in G$ and $k \in \ker(\mu)$, then

$$\mu(x)(k) = xx^{-1}\mu(x^{-1})^{-1}(k) = xk\mu(k)(x^{-1}) = xkx^{-1}. \tag{11}$$

This implies, by (10), that if N is a normal subgroup of G contained in $\ker(\mu)$, then $\mu(x)(Ny) = N\mu(x)(y)$ and therefore (with the usual bar notation) the map $\overline{\mu} : \overline{G} = G/N \to S_{\overline{G}}$ given by

$$\overline{\mu}(\overline{x})(\overline{y}) = \overline{\mu(x)(y)}$$

is well defined and it is easy to show that $\overline{\mu}$ is an IYB morphism of $\overline{G}$. We say that μ is a lifting of $\overline{\mu}$.

It is somehow natural to try to prove that every solvable group is IYB with the following induction strategy: Let G be a non-trivial solvable group. Take a non-trivial abelian normal subgroup N of G. Assume, by induction, that $\overline{G} = G/N$

has an IYB morphism λ and prove that λ admits a lifting to G, i.e. $\lambda = \overline{\mu}$ for some IYB morphism μ of G. Notice that if this strategy works, then every non-trivial solvable group should have a non-injective IYB morphism. This is the case for all the examples of IYB groups G that we have computed. This leads us to the following natural question: Does every IYB group admit a non-injective IYB morphism? Equivalently, in the framework of braces [17]: if A is a finite brace, does there then exist a brace B with non-zero socle so that the adjoint groups of A and B are isomorphic? Note that in [17] an example is given of a finite brace with zero socle. In fact, all the IYB morphisms which appear implicitly in the results of Section 3 or in the above examples are non-injective and therefore they are liftings of IYB morphisms of proper quotients. These examples may lead to the impression that every IYB morphism of G/N, for an abelian normal subgroup N of G, can be lifted to an IYB morphism of G. However this is false as the following example shows.

Example 4.4. Let G be the group of Example 4.3. We claim that the trivial IYB morphism of G/G' does not lift to an IYB morphism of G. Indeed, assume that μ is an IYB morphism of G which lifts the trivial IYB morphism of G/G'. Then, clearly, $\mu(d)$ and $\mu(e)$ commute. Furthermore, by (11), $\mu(g)(n) = gng^{-1}$ for every $g \in G$ and $n \in G'$ and there are $x_j \in G'$ $(j = 1, 2, 3)$, with

$$\mu(d)(d) = x_1 d, \quad \mu(e)(d) = x_2 d, \quad \mu(e)(e) = x_3 e. \tag{12}$$

Then, by (10),

$$dx_2d^{-1}x_1d = \mu(d)(x_2d) = \mu(d)\mu(e)(d) = \mu(e)\mu(d)(d) = \mu(e)(x_1d) = ex_1e^{-1}x_2d.$$

Therefore $(e, x_1) = (d, x_2) \in \langle a\rangle \cap \langle b\rangle = \{1\}$ and hence $x_1, x_2 \in Z(G)$. This implies, by (10) and (11), that $\mu(d^j)(d^k) = x_1^{jk}d^k$ and $\mu(e^j)(d^k) = x_2^{jk}d^k$, for every j, k. Then $\mu(d)(e) = dd^{-1}\mu(d^{-1})^{-1}(e) = de\mu(e)^{-1}(d^{-1}) = dex_2d^2 = x_2c^2e$. Thus

$$\mu(e)\mu(d)(e) = \mu(e)(x_2c^2e) = x_2b^2c^2x_3e$$

and

$$\mu(d)\mu(e)(e) = \mu(d)(x_3e) = dx_3d^{-1}x_2c^2e.$$

Therefore $b^2x_3 = dx_3d^{-1}$ and so $b^2 = (d, x_3) \in \langle a\rangle$, a contradiction. □

5. Solutions to the Yang-Baxter equation associated to one IYB group

Let X be a finite set. We have seen in Section 2 that if X is a cycle set, then the map

$$r\colon X \times X \longrightarrow X \times X$$

defined by $r(x, y) = (f_x(y), g_y(x))$, where $g_x^{-1}(y) = x \cdot y$ and $f_y(x) = g_x(y) \cdot x$ for all $x, y \in X$, is an involutive non-degenerate solution of the braided equation. We also know, by Theorem 2.1, that $\langle f_x : x \in X\rangle$ is an IYB group. One can ask how many involutive non-degenerate solutions of the braided equation are associated to the same IYB group. Note that for any finite set X, the cycle set structure given by $x \cdot y = y$, for all $x, y \in X$, is associated to the trivial group. Note also that if X_i is a finite cycle set associated to the IYB group G_i, for $i = 1, \dots, n$, then it is easy to see that if $X = \bigcup_{i=1}^n X_i$ is a disjoint union, then X is a cycle set with the binary operation defined by

$$x * y = \begin{cases} x \cdot y & \text{if there exists } i \text{ such that } x, y \in X_i, \\ y & \text{otherwise} \end{cases}$$

associated to the direct product $\prod_{i=1}^n G_i$. Notice that this also gives another proof for Corollary 3.2. Hence, since $\langle 1 \rangle \times G \cong G$, one can associate with each IYB group, in an obvious way, infinitely many involutive non-degenerate solutions of the braided equation. Now we give a non-obvious construction of an infinite family of involutive non-degenerate solutions of the braided equation associated to a fixed IYB group.

Lemma 5.1. *Let X be a set and let $\sigma \colon X \to \mathrm{Sym}_X$ be a map. Let $\psi \colon \mathrm{Sym}_X \to \mathrm{Sym}_{X^2}$ be the map defined by $\psi(\tau)(x, y) = (\tau(x), \sigma(\tau(x))\tau\sigma(x)^{-1}(y))$ for all $\tau \in \mathrm{Sym}_X$ and $x, y \in X$. Then ψ is a monomorphism.*

Proof. Let $\tau_1, \tau_2 \in \mathrm{Sym}_X$ and $x, y \in X$. We have:

$$\begin{aligned} \psi(\tau_1\tau_2)(x, y) &= (\tau_1\tau_2(x), \sigma(\tau_1\tau_2(x))\tau_1\tau_2\sigma(x)^{-1}(y)) \\ &= (\tau_1(\tau_2(x)), \sigma(\tau_1(\tau_2(x)))\tau_1\sigma(\tau_2(x))^{-1}(\sigma(\tau_2(x))\tau_2\sigma(x)^{-1}(y))) \\ &= \psi(\tau_1)(\tau_2(x), \sigma(\tau_2(x))\tau_2\sigma(x)^{-1}(y)) \\ &= \psi(\tau_1)\psi(\tau_2)(x, y). \end{aligned}$$

Hence ψ is a homomorphism. It is easy to see that it is injective. □

Lemma 5.2. *Let X be a cycle set. Let $\sigma \colon X \to \mathrm{Sym}_X$ be the map defined by $\sigma(x)(y) = x \cdot y$. Let $\mu \colon X^2 \to \mathrm{Sym}_X$ be the map defined by $\mu(x, y) = \sigma(y)\sigma(x)$ for all $x, y \in X$. Let $\sigma_2 \colon X^2 \to \mathrm{Sym}_{X^2}$ be the map defined by $\sigma_2 = \psi\mu$, where ψ is as in Lemma* 5.1*. Then X^2 with the binary operation defined by $(x, y) \cdot (z, t) = \sigma_2(x, y)(z, t)$ is cycle set.*

Proof. We denote $\sigma(x)^{-1}(y) = y^x$. Note that

$$\begin{aligned} (x, y) \cdot (z, t) &= \psi(\sigma(y)\sigma(x))(z, t) \\ &= (\sigma(y)\sigma(x)(z), \sigma(\sigma(y)\sigma(x)(z))\sigma(y)\sigma(x)\sigma(z)^{-1}(t)) \\ &= (y \cdot (x \cdot z), (y \cdot (x \cdot z)) \cdot (y \cdot (x \cdot (t^z)))), \end{aligned}$$

for all $x, y, z, t \in X$.

We have

$$\begin{aligned} &((x, y) \cdot (z, t)) \cdot ((x, y) \cdot (u, v)) \\ &\qquad = (y \cdot (x \cdot z), (y \cdot (x \cdot z)) \cdot (y \cdot (x \cdot (t^z)))) \\ &\qquad\quad \cdot (y \cdot (x \cdot u), (y \cdot (x \cdot u)) \cdot (y \cdot (x \cdot (v^u)))) \\ &\qquad = (((y \cdot (x \cdot z)) \cdot (y \cdot (x \cdot (t^z)))) \cdot ((y \cdot (x \cdot z)) \cdot (y \cdot (x \cdot u))), \\ &\qquad\quad (((y \cdot (x \cdot z)) \cdot (y \cdot (x \cdot (t^z)))) \cdot ((y \cdot (x \cdot z)) \cdot (y \cdot (x \cdot u)))) \\ &\qquad\quad \cdot (((y \cdot (x \cdot z)) \cdot (y \cdot (x \cdot (t^z)))) \cdot ((y \cdot (x \cdot z)) \cdot ((y \cdot (x \cdot (v^u))))))). \end{aligned}$$

So, in order to prove the lemma, we need to show that

$$\begin{aligned}&((y\cdot(x\cdot z))\cdot(y\cdot(x\cdot(t^z))))\cdot((y\cdot(x\cdot z))\cdot(y\cdot(x\cdot u)))\\ &\quad=((t\cdot(z\cdot x))\cdot(t\cdot(z\cdot(y^x))))\cdot((t\cdot(z\cdot x))\cdot(t\cdot(z\cdot u))).\end{aligned}\tag{13}$$

Now we have

$$\begin{aligned}(y\cdot(x\cdot z))\cdot(y\cdot(x\cdot(t^z))) &= ((x\cdot z)\cdot y)\cdot((x\cdot z)\cdot(x\cdot(t^z)))\\ &= ((x\cdot z)\cdot y)\cdot((z\cdot x)\cdot(z\cdot(t^z)))\\ &= ((x\cdot z)\cdot y)\cdot((z\cdot x)\cdot t).\end{aligned}$$

Hence (13) is equivalent to

$$\begin{aligned}&(((x\cdot z)\cdot y)\cdot((z\cdot x)\cdot t))\cdot((y\cdot(x\cdot z))\cdot(y\cdot(x\cdot u)))\\ &\quad=(((z\cdot x)\cdot t)\cdot((x\cdot z)\cdot y))\cdot((t\cdot(z\cdot x))\cdot(t\cdot(z\cdot u))).\end{aligned}\tag{14}$$

Since $(y\cdot(x\cdot z))\cdot(y\cdot(x\cdot u))=((x\cdot z)\cdot y)\cdot((x\cdot z)\cdot(x\cdot u))=((x\cdot z)\cdot y)\cdot((z\cdot x)\cdot(z\cdot u))$ and $(t\cdot(z\cdot x))\cdot(t\cdot(z\cdot u))=((z\cdot x)\cdot t)\cdot((z\cdot x)\cdot(z\cdot u))$, we get that (14) is true and therefore the lemma is proved. □

Note that, with the notation of Lemma 5.2, if $1\in\sigma(X)$, then $\langle\sigma(X)\rangle\cong\langle\sigma_2(X^2)\rangle$. Thus, in this way, we can construct infinitely many involutive non-degenerate solutions of the braided equation associated to the IYB group $\langle\sigma(X)\rangle$.

It seems a difficult problem to describe all the involutive non-degenerate solutions of the braided equation associated to a given IYB group.

References

1. N. Ben David and Y. Ginosar, On groups of central type, non-degenerate and bijective cohomology classes, Israel J. Math. to appear, ArXiv: 0704.2516v1 [math.GR].
2. F. Cedó, E. Jespers and J. Okniński, The Gelfand-Kirillov dimension of quadratic algebras satisfying the cyclic condition, Proc. AMS 134 (2005), 653-663. MR2180881 (2006g:16051)
3. V. G. Drinfeld, On unsolved problems in quantum group theory. Quantum Groups, Lecture Notes in Math. 1510, Springer-Verlag, Berlin, 1992, 1–8. MR1183474 (94a:17006)
4. P. Etingof and S. Gelaki, A method of construction of finite-dimensional triangular semisimple Hopf algebras, Mathematical Research Letters 5 (1998), 551–561. MR1653340 (99i:16069)
5. P. Etingof, T. Schedler and A. Soloviev, Set-theoretical solutions to the quantum Yang-Baxter equation, Duke Math. J. 100 (1999), 169-209. MR1722951 (2001c:16076)
6. T. Gateva-Ivanova, A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation, J. Math. Phys. 45 (2004), 3828–3858. MR2095675 (2005h:16077)
7. T. Gateva-Ivanova and S. Majid, Matched pairs approach to set theoretic solutions of the Yang-Baxter equation, J. Algebra 319 (2008), no. 4, 1462–1529. MR2383056
8. T. Gateva-Ivanova and M. Van den Bergh, Semigroups of *I*-type, J. Algebra 206 (1998), 97-112. MR1637256 (99h:20090)
9. B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967. MR0224703 (37:302)
10. E. Jespers and J. Okniński, Monoids and Groups of *I*-Type, Algebr. Represent. Theory 8 (2005), 709-729. MR2189580 (2007b:20071)
11. E. Jespers and J. Okniński, *Noetherian Semigroup Algebras*, Springer, Dordrecht, 2007. MR2301033 (2007k:16001)
12. C. Kassel, *Quantum Groups*, Graduate Text in Mathematics 155, Springer-Verlag, New York, 1995. MR1321145 (96e:17041)
13. Jiang-Hua Lu, Min Yan and Yong-Chang Zhu, On the set-theoretical Yang-Baxter equation, Duke Math. J. 104 (2000),153-170. MR1769723 (2001f:16076)
14. D. S. Passman, *Permutation Groups*, Benjamin, New York, 1968. MR0237627 (38:5908)
15. D. K. Robinson, *A course in the theory of groups*, second edition, Springer-Verlag, New York, 1996. MR1357169 (96f:20001)
16. W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation, Adv. Math. 193 (2005), 40–55. MR2132760 (2005k:81132)

17. W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (2007), 153–170. MR2278047 (2007m:16065)
18. C.N. Yang, Some exact results for the many-body problem in one dimension with repulsive delta-function interaction, Phys. Rev. Lett. 19 (1967), 1312–1315. MR0261870 (41:6480)

Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain
E-mail address: cedo@mat.uab.cat

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium
E-mail address: efjesper@vub.ac.be

Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain
E-mail address: adelrio@um.es