Skew braces and solutions to the Yang–Baxter equation

Ilaria Colazzo

Contents

The notes correspond to the series of lectures on *Skew braces and solutions to the Yang–Baxter equation* taught as part of the conference Introduction to Modern Advances in Algebra.

This version was compiled on Sunday 3$^{\text{rd}}$ March, 2024 at 12:24.

Ilaria Colazzo
Exeter (UK)

University of Exeter – Exeter (UK)
E-mail address: ilariacolazzo@gmail.com.

Lecture 1. 22/02/2024

§ 1.1. Exercises and Problems.

Exercise 1.1. Let (X,r) be a set-theoretic solution to the Yang–Baxter equation. Define for all $x,y\in X$

$$\bar{r}(x,y)=\tau r\tau(x,y)=(\rho_x(y),\lambda_y(x)).$$

Then $(X,\bar{r})$ is a set-theoretic solution to the Yang–Baxter equation.

§ 1.2. Shelfs and racks.

Exercise 1.2. Let X be a non-empty set. Let $\triangleleft : X\times X\to X$ be a binary operation and define $r: X\times X\to X\times X$ such that $r(x,y)=(y,x\triangleleft y)$. Then r satisfies equation **??** if and only if $(x\triangleleft y)\triangleleft z=(x\triangleleft z)\triangleleft(y\triangleleft z)$ holds for all $x,y,z\in X$. Moreover, r is bijective if and only if the maps $\rho_y : X\to X, x\mapsto x\triangleleft y$ are bijective.

Definition 1.3. A *(right) shelf* is a pair $(X,\triangleleft)$ where X is a non-empty set and $\triangleleft$ is a binary operation such that

$$(x\triangleleft y)\triangleleft z=(x\triangleleft z)\triangleleft(y\triangleleft z).$$

If, in addition, the maps $\rho_y : X\to X, x\mapsto x\triangleleft y$ are bijective for all $y\in X$, then $(X,\triangleleft)$ is called a *(right) rack*.

Proposition 1.4. *Let X be a non-empty set with a binary operation $\triangleleft : X\times X\to X$. Then $r(x,y)=(y,x\triangleleft y)$ is a set-theoretic solution to the Yang–Baxter equation if and only if $(X,\triangleleft)$ is a rack.*

Proof. Follows from exercise 1.2. □

Exercise 1.5. Let G be a group. Then (G,r) where $r(x,y)=(y,y^{-1}xy)$ is a non-degenerate set-theoretic solution to the Yang–Baxter equation.

Exercise 1.6. Let (X,r) be a solution. Define

$$x\triangleleft y=\lambda_y\rho_{\lambda_x^{-1}(xy}(x).$$

Prove that $(X,\triangleleft)$ is a shelf.

§ 1.3. An intriguing connection between group actions and solutions. The following theorem is the core result of the paper [**2**] by Lu, Yan Zhu.

Theorem 1.7. *Let G be a group, let $\lambda : G\times G\to G, (x,y)\mapsto\lambda_x(y)$ a left group action of G on itself as a set and $\rho : G\times G\to G, (x,y)\mapsto\rho_y(x)$ a right group action of G on itself as a set. If the "compatibility" condition*

$$uv=\lambda_u(v)\rho_v(u) \tag{1.1}$$

holds, then (G,r), where

$$r: G\times G\to G\times G,\qquad (x,y)\mapsto(\lambda_x(y),\rho_y(x))$$

is a solution.

Exercise 1.8. Prove Theorem 1.7

Exercise 1.9. Let p be a prime number and let $A=\mathbb{Z}/(p^2)$ the ring of integers modulo p^2. Prove that A with respect to the usual sum and the operation given by $x\circ y = x+y+pxy$ is a skew brace.

Exercise 1.10. Let A be a skew brace. Prove that

$$\rho_b(a)=\lambda^{-1}_{\lambda_a(b)}(-(a\circ b)+a+a\circ b)$$

Exercise 1.11. Let $(A,+)$ be a (not necessarily abelian) group.

1) Prove that a structure of skew brace over A is equivalent to an operation $A\times A\to A$ $(a,b)\mapsto a*b$, such that

$$a*(b+c)=a*b+b+a*c-b$$

holds for all $a,b,c\in A$ and the operation $a\circ b = a+a*b+b$ turns A into a group.

2) Deduce that radical rings are examples of skew braces.

Exercise 1.12. Let A be a skew brace and $a*b=\lambda_a(b)-b=-a+a\circ b-b$. Prove the following identities:

1) $a*(b+c)=a*b+b+a*c-b$.

2) $(a\circ b)*c=(a*(b*c))+b*c+a*c$.

Exercise 1.13. Let $(A,+,\circ)$ be a triple, where $(A,+)$ and $(A,\circ)$ are groups, and $\lambda : A\to \mathrm{Sym}(A)$, $a\mapsto \lambda_a$ with $\lambda_a(b)=-a+a\circ b$. Prove that the following statements are equivalent:

1) $(A,+,\circ)$ is a skew brace.

2) $\lambda_a\lambda_b(c)=\lambda_{a\circ b}(c)$, for all $a,b,c\in A$.

3) $\lambda_a(b+c)=\lambda_a(b)+\lambda_a(c)$, for all $a,b,c\in A$.

Exercise 1.14 (The semidirect product). Let A,B be skew braces. Let $\alpha : (B,\circ)\to \mathrm{Aut}(A,+,\circ)$ be a homomorphism of groups. Define two operations on $A\times B$ by

$$(a,x)+(b,y)=(a+b,x+y)$$
$$(a,x)\circ(b,y)=(a\circ\alpha_x(b),x\circ y),$$

for all $a,b\in A$ and $x,y\in B$. Prove that $(A\times B,+,\circ)$ is a skew brace.
This skew brace is the *semidirect product* of the skew brace A by B via α, and it is denoted by $A\rtimes_\alpha B$.

Exercise 1.15. Consider the semidirect product $A=\mathbb{Z}/(3)\rtimes\mathbb{Z}/(2)$ of the trivial skew braces $\mathbb{Z}/(3)$ and $\mathbb{Z}/(2)$ via the non-trivial action of $\mathbb{Z}/(2)$ over $\mathbb{Z}/(3)$. Prove that $\mathrm{Fix}(B)$ is not an ideal of A.

EXERCISE 1.16. A map $f : A \to B$ between two skew braces A and B is a *homomorphism* of skew braces if $f(a+b) = f(a) + f(b)$ and $f(a \circ b) = f(a) \circ f(b)$, for all $a, b \in A$.The *kernel* of f is

$$\ker f = \{a \in A \colon f(a) = 0\}.$$

Let $f : A \to B$ be a homomorphism of two skew braces A and B. Prove that $\ker f$ is an ideal of A.

EXERCISE 1.17. Let $f : A \to B$ be a homomorphism of skew braces. Prove that $A/\ker f \cong f(A)$.

EXERCISE 1.18. Let A be a skew brace and let B be a subbrace of A. Prove that if I is an ideal of A, then $B \circ I$ is a subbrace of A, $B \cap I$ is an ideal of B and $(B \circ I)/I \cong B/(B \cap I)$.

EXERCISE 1.19. Let A be a skew brace and I and J be ideals of A. Prove that if $I \subseteq J$, then $A/J \cong (A/I)/(J/I)$.

EXERCISE 1.20. Let A be a skew brace and let I be an ideal of A. Prove that there is a bijective correspondence between (left) ideals of A containing I and (left) ideals of A/I.

EXERCISE 1.21. Let A be a skew brace and I be a characteristic subgroup of the additive. Prove that I is a left ideal of A.

EXERCISE 1.22. Let A and B be skew braces. Prove that $f : A \to B$ is a homomorphism of skew braces if and only if $f(a+b) = f(a) + f(b)$ and $f(\lambda_a(b)) = \lambda_{f(a)}(f(b))$, for all $a, b \in B$.

Lecture 2. 23/02/2024

§ 2.1. From solutions to skew braces.

Definition 2.1. Let (X,r) be a solution. The *structure group* of (X,r) is the group

$$G(X,r) = \langle X : xy = \lambda_x(y)\rho_y(x) \text{ for all } x,y \in X\rangle.$$

The *derived structure group* of (X,r) is the group

$$A(X,r) = \langle X : x\lambda_x(y) = \lambda_x(y)\lambda_{\lambda_x(y)}\rho_y(x) \text{ for all } x,y \in X\rangle.$$

Theorem 2.2 ([**1**] or [**2**]). *Let (X,r) be a solution. Then, there exists a unique structure of skew brace with multiplicative group the structure group isomorphic to $G(X,r)$, additive strucutre isomorphic to $A(X,r)$ and such that $\lambda_{i(x)}(i(y)) = i(\lambda_x(y))$ for all $x,y \in X$, where $\iota : X \to G(X,r), x \mapsto x$ is the canoical map.*

Proof. Omitted. □

Note that the map i in the previous theorem is not necessarily injective.

Example 2.3. Let $X = \{1,2,3,4\}$, $\lambda = (1\ 2)$ and $\rho = (3\ 4)$. Since $\lambda\rho = \rho\lambda$, we have that $r : X \times X \to X \times X$ defined by $r(x,y) = (\lambda(y), \rho(x))$ gives a solution. In $G(X,r)$ the elements 1 and 2 are identified and also 3 and 4. Indded in $G(X,r)$ we have

$$1 \circ 1 = \lambda(1) \circ \rho(1) = 2 \circ 1 \implies 1 = 2,$$
$$3 \circ 3 = \lambda(3) \circ \rho(3) = 3 \circ 4 \implies 3 = 4.$$

Therefore, i is not injective.

The structure skew brace defined in the previous theorem satisfies the following universal property.

Proposition 2.4. *Let $(B,+,\circ)$ be a skew brace, $j \colon X \to B$ be a map such that $\lambda_{j(x)}(j(y)) = j(\lambda_x(y))$ and $j(x) \circ j(y) = j(\lambda_x(y)) \circ j(\rho_y(x))$, for all $x,y \in X$. Then there exists a unique homomorphism of skew braces $f \colon G(X,r) \to B$ such that $fi = j$, i.e.*

$$\begin{tikzcd} X \arrow[r, "j"] \arrow[d, "i"'] & B \arrow[dl, dashed, "f"'] \\ G(X,r) & \end{tikzcd}$$

Proof. Omitted. □

§ 2.2. The permutation group of a solution.

If (X,r) is a finite solution we can consider a finite quotient (as skew brace) of the strucure group that governs important property of such solution.

Let (X,r) be a solution. Consider the structure group $G(X,r)$ of the solution (X,r). Let $i \colon X \to G(X,r)$ be the natural map.

The *permutation group* of (X,r) is the subgroup

$$\mathscr{G}(X,r) = \langle (\lambda_x, \rho_x^{-1}) : x \in X\rangle \subseteq \operatorname{Sym}_X \times \operatorname{Sym}_X.$$

Since

$$\lambda_x\lambda_y = \lambda_{\lambda_x(y)}\lambda_{\rho_y(x)} \quad \text{and} \quad \rho_x^{-1}\rho_y^{-1} = \rho^{-1}_{\lambda_x(y)}\rho^{-1}_{\rho_y(x)}$$

for all $x,y \in X$, there exists a unique group homomorphism $h\colon G(X,r) \to \mathscr{G}(x,r)$ such that $hi(x) = (\lambda_x, \rho_x^{-1})$ for all $x \in X$. We write $h(a) = (\lambda_a, \rho_a^{-1})$, for all $a \in G(X,r)$. By Theorem 2.2, $G(X,r)$ has a unique structure of skew brace with multiplicative group the structure group $G(X,r)$ and $\lambda_{i(x)}(i(y)) = i(\lambda_x(y))$ for all $x,y \in X$. One can prove that $\ker h$ is an ideal of the skew brace $G(X,r)$. Hence, $\mathscr{G}(X,r)$ inherits a skew brace structure form $G(X,r)$.

Given a skew brace $(A,+,\circ)$ with $(A,+)$ abelian, Bachiller, Cedó and Jespers in [] provided a method to recostruct all (involutive) solutions such that $\mathscr{G}(X,r)$ is isomorphic as skew brace to A. In [], Bchiller generalised this construction dropping the assumption $(A,+)$ abelian.

§ 2.3. Simple solutions. Describing simple solution is a very hard and challenging task. A strategy to tackle such problem is to focus on “building blocks”, such us indecomposable solutions and simple solutions.

Definition 2.5. A solution (X,r) is said to be *decomposable* if there exist $\emptyset \neq Y,Z \subseteq X$ such that $Y \cup Z = X$, $Y \cap Z = \emptyset$ and $r(Y \times Y) \subseteq Y \times Y$, $r(Z \times Z) \subseteq Z \times Z$. Otherwise, (X,r) is said *indecomposable*.

It is not difficult to prove that a solution (X,r) is indecomposable if the group $\langle \lambda_x, \rho_y \colon x,y \in \rangle$ acts transitivelly on X.

Definition 2.6. A solution (X,r) is said to be *simple* if for any epimorphism of solutions $\varphi : (X,r) \to (Y,t)$, we have either φ an isomorphis or Y as singleton.

One can prove that a simple solution is in particular indecomposable.

Cedó and Okniński in [] proved that ome simple skew brace with additive structure abelian provide examples of (involutive) simple solutions.

Joyce in 1982 studied simple racks and provided an algebraic characterisation of such racks. By Proposition 1.4, a rack provide a solution and it is not difficult to see that simple racks are in particular examples of simple solutions.

In join work with Jespers, Kubat and Van Antwerpen [], we obtain a brace theoretic classification of simple solutions.

Theorem 2.7. *A simple solution (X,r) is one of the following type:*

1) *(X,r) is a simple permutation solution,*
2) *(X,r) is a simple square-free*[1] *derived solution (i.e. it is a simple quandle*[2]*),*
3) *(X,r) is a simple solution embedded in a solution associated to a finite skew brace.*

2.3.1. *Simple permutation solution.* Recall that a (X,r) is a permutation solution if there exist λ, ρ commuting permutations such that $r(x,y) = (\lambda(y), \rho(x))$.

We can give a combinatorial characterisation of simple permutation solutions.

Proposition 2.8. *A permutation solution (X,r) is simple if and only if the caridnality of X is a prime number p, the group $H = \langle \lambda, \rho \rangle$ is cyclic of order p.*

In particular, (X,r) solution is isomorphic to $(\mathbb{Z}_p, t)$ such that $t(x,y) = (y+a, x+b)$ with $,a,b \in \mathbb{Z}$ and$(a,b) \neq (0,0)$.

[1] A solution (X,r) is square-free if $r(x,x) = (x,x)$ for every $x \in X$.

[2] A rack $(X,\triangleleft)$ is a quandle if $x \triangleleft x = x$, for every $x \in X$.

2.3.2. *Simple quandle.* The description of simple square-free derived solutions coiced with the description obtained by Joyce of simple quandles.

Proposition 2.9. *A square-free derived solution (X,r) is simple if and only if (X,r) embedd in a solution (A,r) where A is a finite group and $r(y,y^{-1}xy)$ such that*

- *X is a conjucacy class genereting A,*
- *the derived subgroup $[A,A]$ is the smallest non-zero normal subgroup of A,*
- *the quotient group $A/[A,A]$ is a cyclic group,*
- *the center $Z(A)$ is trivial.*

2.3.3. *Simple solutions embedded in solutions associated to finite skew braces.* Let $(A,+,\circ)$ be a skew brace. In analogy with radical rings, we can associate to A another binary operation $*: A\times A\to A$ such that $a*b=-a+a\circ b+b$, for every $a,b\in A$.

Exercise 2.10. Let $(A,+,\circ)$ be a skew brace. Define A^2 the additive subgroup generated by $\{a*b=-a+a\circ b-b\colon\ a,b\in A\}$. Prove that A^2 is an ideal of A.

The ideal A^2 plays for skew braces a simplar role that the derived subgroup plays for groups. With this observation in mind, it might be not surpising the following proposition.

Proposition 2.11. *A square-free solution (X,r) which is not a derived solution nor a permutation solution is simple if and only if (X,r) embedd in a solution asoociated to a non-trivial skew brace (A,r_A) such that*

- *X generates additively A,*
- *the ideal A^2 is the smallest non-zero ideal of A,*
- *the quotient skew brace A/A^2 is trivial skew brace with additive (and multiplicative) group cyclic,*
- *the action of A^2 on X is transitive.*

Let us explain what the last item means. Let A be a skew brace, $X\subset A$ and I an ideal of A. We say that I *acts* on X if X is invariant uder the action of the group $(I,+)\rtimes(I,\circ)$ (where the semidirect product is given by the λ-map).

Appendix

§ 2.4. Radical rings.

Definition 2.12. A non-empty set R with two binary operations the addition $+$ (addition) and the multiplication $\cdot$ is a *ring* if

- $(R,+)$ is an abelian group,
- $(R,\cdot)$ is a semigroup (i.e. $\cdot$ is associative),
- The multiplication is distributive with respect to the addition, i.e.

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c) \qquad \text{(left distributivity)}$$
$$(b+c)\cdot a=(b\cdot a)+(c\cdot a) \qquad \text{(right distributivity)}$$

for all $a,b,c\in R$.

A ring $(R,+,\cdot)$ is *unitary* if there is an element 1 in R such that $a\cdot 1=1\cdot a=a$ for all $a\in R$ (i.e., 1 is the *multiplicative identity*).

Let R be a non-unitary ring. Consider $R_1=\mathbb{Z}\times R$ with the addition defined component-wise and multiplication

$$(k,a)(l,b)=(kl,kb+la+ab)$$

for all $k,l\in\mathbb{Z}$ and $a,b\in R$.

Then R_1 is a ring and $(1,0)$ is its multiplicative identity.

Note that $\{0\}\times R$ is isomorphic to R as non-unitary rings.

Exercise 2.13. Let R be a non-unitary ring. Consider $R_1=\mathbb{Z}\times R$ as before. If $(k,x)\in R_1$ is invertible, then $k\in\{1,-1\}$.

Definition 2.14. Let R be a unitary ring. The *(Jacobson) radical* $J(R)$ of R is defined as the intersection of all maximal left ideals[3] of R.

Exercise 2.15. Let R be a unitary ring.

1) Prove that $J(R)$ in an ideal of R.
2) Prove that $x\in J(R)$ if and only if $1+rx$ is invertible for all $r\in R$.

Definition 2.16. A non-unitary ring R is a *(Jacobson) radical ring* if it is isomorphic to the Jacobson radical of a unitary ring.

Proposition 2.17. *Let R be a non-unitary ring. The following statements are equivalent.*

1) *R is a radical ring.*
2) *For all $a\in R$ there exists a unique $b\in R$ such that $a+b+ab=a+b+ba=0$.*
3) *R is isomorphic to $J(R_1)$.*

Proof. Let us first prove that 1) implies 2). Let M be a unitary ring such that R is isomorphic to its Jacobson radical $J(M)$ and let $\psi: R\to M$ be a homomorphism such that $\psi(R)$ is isomorphic

[3] A *left ideal* of R is an additive subgroup I of R such that $ax\in I$ for all $a\in R$ and $x\in I$.

to $J(M)$. Now, if $a \in R$, then $\psi(a) \in J(M)$. By Exercise 2.15, $1+\psi(a)$ is invertible, i.e. there exists $c \in M$ such that

$$(1+\psi(a))(1+c) = 1 = (1+c)(1+\psi(a)).$$

It follows that $c \in J(M)$, i.e. $c = \psi(b)$ for some $b \in R$. Moreover, since ψ is a homomorphism

$$\begin{aligned} 1 &= (1+\psi(a))(1+c) = (1+\psi(a))(1+\psi(b)) \\ &= 1+\psi(a)+\psi(b)+\psi(a)\psi(b) = 1+\psi(a+b+ab) \end{aligned}$$

and

$$\begin{aligned} 1 &= (1+c)(1+\psi(a)) = (1+\psi(b))(1+\psi(a)) \\ &= 1+\psi(b)+\psi(a)+\psi(b)\psi(a) = 1+\psi(a+b+ba). \end{aligned}$$

Hence, 2) holds.

Now let us prove 2) implies 3). Let $a \in R$, we aim to prove that $(1,a) \in R_1$ is invertible. By 2) there exists $b \in R$ such that

$$\begin{aligned} (1,a)(1,b) &= (1,a+b+ab) = (1,0) \\ (1,b)(1,a) &= (1,b+a+ba) = (1,0). \end{aligned}$$

Now, consider $(k,a) \in J(R_1)$. We want to prove that $k = 0$, i.e. $J(R_1) \subseteq \{0\} \times R$. Since $(k,a) \in J(R_1)$ follows that $(1,0)+(3,0)(k,a) =)(1+3k,3a)$ is invertible by Exercise 2.15, and so $k = 0$. Therefore $J(R_1) \subseteq \{0\} \times R$. Moreover, let $(0,R) \in \{0\} \times R$. then

$$(1,0)+(k,a)(0,x) = (1,0)+(0,kx+ka) = (1,kx+ka)$$

which is invertible. So $(0,x) \in J(R_1)$. Finally the implication 3) implies 1) is trivially true. □

Definition 2.18. Let R be any ring. Define on R the binary operation $\circ$ called the *adjoint multiplication* of R

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

for all $a,b \in R$.

Lemma 2.19. *Then* $(R,\circ)$ *is a monoid with neutral element* 0.

Exercise 2.20. Prove Lemma 2.19.

Convention 1. If $a \in R$ is invertible in the monoid $(R,\circ)$, we will denote by a' its inverse.

Examples 2.21.

1) Let p be a prime and let $A = \mathbb{Z}/(p^2) = \mathbb{Z}/p^2\mathbb{Z}$ be the ring of integers modulo p^2. Then $(A,+)$ with a new multiplication $*$ defined by $a * b = pab$ is a radical ring. In this case, $a \circ b = a+b+pab$, and $a' = -a+pa^2$.

2) Let n be an integer such that $n > 1$. Let

$$A = \left\{ \frac{nx}{ny+1} : x,y \in \mathbb{Z} \right\} \subseteq \mathbb{Q}.$$

A is a (non-unitary) subring of $\mathbb{Q}$. In fact, A is a radical ring. A straightforward computation shows

$$\left(\frac{nx}{ny+1}\right)' = \frac{-nx}{n(x+y)+1}.$$

Some solutions

1.1. It is enough to apply Proposition **??**.

??. First, let us prove note that $s(x,y)=(y,\sigma_y(x))$ satisfies the Yang–Baxter equation if and only if

$$\sigma_z\sigma_y=\sigma_{\sigma_z(y)}\sigma_z.$$

Note that 2) in Proposition **??**, implies that

$$\lambda_x\sigma_y=\sigma_{\lambda_x(y)}\lambda_x. \tag{2.1}$$

Indeed, for any $x,y,z\in X$ it holds

$$\lambda_{\rho_{\lambda_y(z)}(x)}\rho_z(y)=\lambda_{\rho_{\lambda_y(z)}(x)}\lambda^{-1}_{\lambda_y(z)}\sigma_{\lambda_y(z)}(y)\overset{1)}{=}\lambda^{-1}_{\lambda_x\lambda_y(z)}\lambda_x\sigma_{\lambda_y(z)}(y)$$

and

$$\rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y)=\lambda^{-1}_{\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)}\sigma_{\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)}\lambda_x(y)\overset{1)}{=}\lambda^{-1}_{\lambda_x\lambda_y(z)}\sigma_{\lambda_x\lambda_y(z)}\lambda_x(y)$$

Moreover, 3) in Proposition **??**, implies that

$$\sigma_z\sigma_y=\sigma_{\sigma_z(y)}\sigma_z.$$

Indeed

$$\begin{aligned}\rho_z\rho_y(x)&=\lambda^{-1}_{\lambda_{\rho_y(x)}(z)}\sigma_{\lambda_{\rho_y(x)}(z)}\lambda^{-1}_{\lambda_x(y)}\sigma_{\lambda_x(y)}(x)\overset{(2.1)}{=}\lambda^{-1}_{\lambda_{\rho_y(x)}(z)}\lambda^{-1}_{\lambda_x(y)}\sigma_{\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)}\sigma_{\lambda_x(y)}(x)\\&\overset{1)}{=}\lambda^{-1}_{\lambda_{\rho_y(x)}(z)}\lambda^{-1}_{\lambda_x(y)}\sigma_{\lambda_x\lambda_y(z)}\sigma_{\lambda_x(y)}(x).\end{aligned}$$

and

$$\begin{aligned}\rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x)&=\lambda^{-1}_{\lambda_{\rho_{\lambda_y(z)}(x)\rho_z(y)}}\lambda^{-1}_{\lambda_x\lambda_y(z)}\sigma_{\lambda_x\lambda_{\lambda_y(z)}\rho_z(y)}\sigma_{\lambda_x\lambda_y(z)}(x)\\&\overset{1)\&2)}{=}\lambda^{-1}_{\rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y)}\lambda^{-1}_{\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)}\sigma_{\lambda_x\sigma_{\lambda_y(z)}(y)}\sigma_{\lambda_x\lambda_y(z)}(x)\\&\overset{1)}{=}\lambda^{-1}_{\lambda_{\rho_y(x)}(z)}\lambda^{-1}_{\lambda_x(y)}\sigma_{\sigma_{\lambda_x\lambda_y(z)}\lambda_x(y)}\sigma_{\lambda_x\lambda_y(z)}(x).\end{aligned}$$

Hence, for all $x,y,z\in X$

$$\sigma_{\lambda_x\lambda_y(z)}\sigma_{\lambda_x(y)}(x)=\sigma_{\sigma_{\lambda_x\lambda_y(y)}\lambda_x(z)}\sigma_{\lambda_x\lambda_y(z)}(x)$$

and the wanted equality follows.

This prove that s satisfies the Yang–Baxter equation.

Now to prove that r is bijective if and only if s is non-degenerate (i.e. all σ_y bijective). Let us first notice that $\varphi r\varphi^{-1}=s$ where $\varphi(x,y)=(x,\lambda_x(y))$. Indeed

$$\varphi r\varphi^{-1}(x,y)=\varphi r(x,\lambda^{-1}x(y))=\varphi(\lambda_x\lambda^{-1}x(y),\rho_{\lambda^{-1}x(y)}(x))=(y,\lambda_y\rho_{\lambda^{-1}x(y)}(x))=(y,\sigma_y(x)).$$

It follows that r is bijective if and only if s is bijective. Finally clearly s is bijective if and only if σ_y is bijective for every $y\in X$.

1.2. For every $x,y\in X$ let us write $\lambda_x=\mathrm{id}_X$ and $\rho_y(x)=x\triangleleft y$. We want to apply Proposition **??**. First note that clearly $\lambda_x\lambda_y=\mathrm{id}_X=\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}$, i.e. 1) is satisfied. Moreover,$\lambda_{\rho_{\lambda_y(z)}(x)}\rho_z(y)=\rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y)$ reduce to the trivial identity $\rho_z(y)=\rho_z(y)$. Finally, $\rho_z\rho_y(x)=\rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x)$ is equivalent to $(x\triangleleft y)\triangleleft z=(x\triangleleft z)\triangleleft(y\triangleleft z)$.

Now assume that r is bijective. If $x_1,x_2\in X$ such that $\rho_y x_1=\rho_y(x_2)$, then $r(x_1,y)=r(x_2,y)$ and so $x_1=x_2$, i.e. ρ_y is injective. Now, let $z\in X$ and let $x\in X$ such that $r(x,y)=(y,z)$. It follows that $\rho_y(x)=z$ and ρ_y is bijective. Similarly one obtains the converse.

1.8. Let us write $r_1=r\times\mathrm{id}$ and $r_2=\mathrm{id}\times r$,

$$\begin{aligned} r_1r_2r_1(x,y,z)&=(\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z),\rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y),\rho_z\rho_y(x))\\ &=(u_1,v_1,w_1),\end{aligned}$$

and

$$\begin{aligned} r_2r_1r_2(x,y,z)&=(\lambda_x\lambda_y(z),\lambda_{\rho_{\lambda_y(z)}(x)}\rho_z(y),\rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x))\\ &=(u_2,v_2,w_2).\end{aligned}$$

Then we obtain

$$\begin{aligned} u_1v_1w_1&=\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)\rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y)\rho_z\rho_y(x)\\ &\overset{(1.1)}{=}\lambda_x(y)\lambda_{\rho_y(x)}(z)\rho_z\rho_y(x)\\ &\overset{(1.1)}{=}\lambda_x(y)\rho_y(x)z\\ &\overset{(1.1)}{=}xyz\end{aligned}$$

and, similarly

$$\begin{aligned} u_2v_2w_2&=\lambda_x\lambda_y(z)\lambda_{\rho_{\lambda_y(z)}(x)}\rho_z(y)\rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x)\\ &\overset{(1.1)}{=}\lambda_x\lambda_y(z)\rho_{\lambda_y(z)}(x)\rho_z(y)\\ &\overset{(1.1)}{=}x\lambda_y(z)\rho_z(y)\\ &\overset{(1.1)}{=}xyz.\end{aligned}$$

Hence

$$u_1v_1w_1=xyz=u_2v_2w_2. \tag{2.2}$$

Moreover, since λ is a left action of G on itself, we get

$$u_1=\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)=\lambda_{\lambda_x(y)\rho_y(x)}(z)\overset{(1.1)}{=}\lambda_{xy}(z)=\lambda_x\lambda_y(z)=u_2.$$

Similarly, since ρ is a right action

$$w_2=\rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x)=\rho_{\lambda_y(z)\rho_z(y)}(x)\overset{(1.1)}{=}\rho_{yz}(x)=\rho_z\rho_y(x)=w_1.$$

From (2.2) and G being a group it follows that also $v_1=v_2$. Moreover, λ_x and ρ_x are bijective maps by assumption. It is left to prove that r is bijective. First let us write $r(u,v)=(x,y)$, hence $\lambda_u(v)=x$, $\rho_v(u)=y$, and $uv=xy$. Now, since λ is an action and in particular $\lambda_v^{-1}=\lambda_{v^{-1}}$, we get

$$\lambda_y(v^{-1})u=\lambda_y(v^{-1})\rho_v^{-1}(y)=\lambda_y(v^{-1})\rho_{v^{-1}}(y)\overset{(1.1)}{=}yv^{-1}=x^{-1}u=(\lambda_u(v))^{-1}u,$$

and so

$$(\lambda_u(v))^{-1} = \lambda_{\rho_v(u)}(v^{-1}). \tag{2.3}$$

Similarly, expanding $v\rho_x(u^{-1})$ one proves

$$(\rho_v(u))^{-1} = \rho_{\lambda_u(v)}(u^{-1}). \tag{2.4}$$

Define

$$r'(x,y) = ((\rho_{x^{-1}}(y^{-1}))^{-1}, (\lambda_{y^{-1}}(x^{-1}))^{-1}).$$

Then

$$\begin{aligned} rr'(x,y) &= (\lambda_{(\rho_{x^{-1}}(y^{-1}))^{-1}}((\lambda_{y^{-1}}(x^{-1}))^{-1}), \rho_{(\lambda_{y^{-1}}(x^{-1}))^{-1}}((\rho_{x^{-1}}(y^{-1}))^{-1})) \\ &\overset{(2.3)\&(2.4)}{=} (\lambda^{-1}_{\rho_{x^{-1}}(y^{-1})}\lambda_{\rho_{x^{-1}}(y^{-1})}(x), \rho^{-1}_{\lambda_{y^{-1}}(x^{-1})}\rho_{\lambda_{y^{-1}}(x^{-1})}(y)) \\ &= (x,y). \end{aligned}$$

And

$$\begin{aligned} r'r(x,y) &= ((\rho_{(\lambda_x(y))^{-1}}((\rho_y(x))^{-1}))^{-1}, (\lambda_{(\rho_y(x))^{-1}}((\lambda_x(y))^{-1}))^{-1}) \\ &\overset{(2.3)\&(2.4)}{=} ((\rho^{-1}_{\lambda_x(y)}\rho_{\lambda_x(y)}(x^{-1}))^{-1}, (\lambda^{-1}_{\rho_y(x)}\lambda_{\rho_y(x)}(y^{-1}))^{-1}) \\ &= ((x^{-1})^{-1}, (y^{-1})^{-1}) = (x,y). \end{aligned}$$

??. Consider the map $\varphi : A \to B \times C, (x) \mapsto (x_B, -x_C)$. Clearly, φ is bijective. Moreover, for $x, y \in A$ we have

$$\varphi(x \circ y) = \varphi(x_B + y + x_C) = \varphi(x_B + y_B + y_C + x_C) = (x_B + y_B, -(y_C + x_C)) = (x_B + y_B, -x_C - y_C),$$

and

$$\varphi(x) + \varphi(y) = (x_B, -x_C) + (y_B, -y_C) = (x_B + y_B, -x_C - y_C).$$

Hence φ is an isomorphism from $(A, \circ$ to the direct product $B \times C$.

Now, let $x, y, z \in A$. Then

$$\begin{aligned} x \circ y - x + x \circ z &= x_B + y + x_C - (x_B + x_C) + x_B + z + x_C \\ &= x_B + y + z + x_C = x \circ (y + z). \end{aligned}$$

Hence $(A, +, \circ)$ is a skew brace.

??. Let $a, b, c \in A$. We have that

$$a \circ (a' + b) \overset{(??)}{=} a \circ a' - a + a \circ b \overset{0=1}{=} 0 - a + a \circ b = \lambda_a(b).$$

Hence, $\lambda_a(b) = a \circ (a' + b)$. Moreover,

$$\rho_b(a) = (\lambda_a(b))' \circ a \circ b = (a \circ (a' + b))' \circ a \circ b = (a' + b)' \circ b.$$

1.15. Note that

$$\begin{aligned}\lambda_{(a,x)}(b,y) &= -(a,x)+(a,x)\circ(b,y)\\ &= -(a,x)+(a+(-1)^x b, x+y)\\ &= ((-1)^x b, y).\end{aligned}$$

and hence $\mathrm{Fix}(A)=\{(0,0),(0,1)\}$ is not a normal subgroup of $(A,\circ)$. In particular, $\mathrm{Fix}(A)$ is not an ideal of A.

??. Let us compute

$$(x,y)=r^{-1}r(x,y)=(\hat{\lambda}_{\lambda_x(y)}\rho_y(x),\hat{\rho}_{\rho_y(x)}\lambda_x(y)).$$

It follows that

$$(x,\lambda_x^{-1}y)=(\hat{\lambda}_y\rho_{\lambda_x^{-1}(y)}(x),\hat{\rho}_{\rho_{\lambda_x^{-1}(y)(x)}}(y)),$$

hence $\hat{\lambda}_y^{-1}(x)=\rho_{\lambda_x^{-1}(y)}(x)$ and $\lambda_x^{-1}(y)=\hat{\rho}_{\hat{\lambda}_y^{-1}(x)}(y)$. Similarly

$$(\rho_y^{-1}(x),y)=(\hat{\lambda}_{\lambda_{\rho_y^{-1}(x)}(y)}(x),\hat{\rho}_x\lambda_{\rho_y^{-1}(x)}(y)),$$

hence $\hat{\rho}_x^{-1}(y)=\lambda_{\rho_y^{-1}(y)}(y)$ and $\rho_y^{-1}(x)=\hat{\lambda}_{\hat{\rho}_x^{-1}(y)}(x)$.

References

[1] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.

[2] J.-H. Lu, M. Yan, and Y.-C. Zhu. On the set-theoretical Yang-Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000.

Index