Skew braces and solutions to the Yang–Baxter equation

Ilaria Colazzo

Contents

Lecture 1. 21/02/2024 3
§ 1.1. The Yang–Baxter equation 3
§ 1.2. The set-theoretic version 3
§ 1.3. A characterisation 3
§ 1.4. First examples 4
§ 1.5. Set-theoretic solutions to the Yang–Baxter equation and III Reidemeister move 4
§ 1.6. The derived solution 5
§ 1.7. Involutive solutions 5
§ 1.8. Skew braces 6
§ 1.9. First examples 7
§ 1.10. Basic properties of skew braces 7
§ 1.11. Skew braces and solutions 9
§ 1.12. Subbraces and ideals. 10
§ 1.13. The isomorphism theorems 11
Lecture 2. 22/02/2024 12
§ 2.1. Exercises and Problems 12
§ 2.2. Shelfs and racks 12
§ 2.3. An intriguing connection between group actions and solutions 12
Lecture 3. 23/02/2024 15
§ 3.1. From solutions to skew braces 15
§ 3.2. The permutation group of a solution 15
§ 3.3. The retraction of a solution. 16
Appendix 18
§ 3.4. Radical rings 18
Some solutions 20
References 24
Index 25
Index 25

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 Tuesday 20th February, 2024 at 16:25.

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

Ilaria Colazzo
Exeter (UK)

Lecture 1. 21/02/2024

§ 1.1. The Yang–Baxter equation. The Yang-Baxter equation (YBE) is one important equation in mathematical physics. It first appeared in two independent papers of Yang [**7**] and Baxter [**1**].

Definition 1.1. A solution of the *Yang–Baxter eqution* is a linear map $R : V \otimes V \to V \otimes V$, where V is a vector space such that

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

where R_{ij} denotes the map $V \otimes V \otimes V \to V \otimes V \otimes V$ acting as R on the (i, j) factor and as the identity on the remaining factor.

Let $\tau : V \otimes V \to V \otimes V$ be the map $\tau(u \otimes v) = v \otimes u$ for $u, v \in V$. It's easy to check (try!) that $R : V \otimes V \to V \otimes V$ is a solution of the Yang–Baxter equation if and only if $\bar{R} := \tau R$ satisfies

$$\bar{R}_{12}\bar{R}_{23}\bar{R}_{12} = \bar{R}_{23}\bar{R}_{12}\bar{R}_{23}.$$

An interesting class of solutions of the Yang–Baxter equation arises when V has a R-invariant basis X. In such a case the solution is said to be set-theoretic.

§ 1.2. The set-theoretic version. Drinfeld in [**2**] observed it makes sense to consider the Yang–Baxter equation in the category of sets and stated that

it would be interesting to study set-theoretic solutions.

These lectures will focus on set-theoretic solutions to the Yang-Baxter equation and their connection with known and "new" algebraic structures.

Definition 1.2. A *set-theoretic solution to the Yang–Baxter equation* is a pair (X, r) where X is a non-empty set and $r : X \times X \to X \times X$ is a map such that

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r) \tag{1.1}$$

Convention 1. If (X, r) is a set-theoretic solution to the Yang–Baxter equation, we write

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

where $\lambda_x, \rho_x : X \to X$.

Definition 1.3. Let (X, r) be a set-theoretic solution to the Yang–Baxter equation. We say that

- (X, r) is *bijective* if r is bijective.
- (X, r) is *finite* if X is finite.
- (X, r) is *non-degenerate* if λ_x, ρ_x are bijective for all $x \in X$.

§ 1.3. A characterisation.

Proposition 1.4. *Let X be a non-empty set and $r : X \times X \to X \times X$ be a map, written ase $r(x, y) = (\lambda_x(y), \rho_y(x))$. Then r satisfies equation 1.1 if and only if*

1) $\lambda_x\lambda_y = \lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}$
2) $\lambda_{\rho_{\lambda_y(z)}(x)}\rho_z(y) = \rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y)$
3) $\rho_z\rho_y = \rho_{\rho_z(y)}\rho_{\lambda_y(z)}$

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

In particular, (X, r) is a solution to the Yang–Baxter equation when r is bijective.

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

$$\begin{aligned} r_1r_2r_1(x,y,z) &= r_1r_2(\lambda_x(y), \rho_y(x), z) \\ &= r_1(\lambda_x(y), \lambda_{\rho_y(x)}(z), \rho_z\rho_y(x)) \\ &= (\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z), \rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y), \rho_z\rho_y(x)), \end{aligned}$$

and

$$\begin{aligned} r_2r_1r_2(x,y,z) &= r_2r_1(x, \lambda_y(z), \rho_z(y)) \\ &= r_2(\lambda_x\lambda_y(z), \rho_{\lambda_y(z)}(x), \rho_z(y)) \\ &= (\lambda_x\lambda_y(z), \lambda_{\rho_{\lambda_y(z)}(x)}\rho_z(y), \rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x)). \end{aligned}$$

Therefore $r_1r_2r_1 = r_2r_1r_2$ if and only if $1), 2)$ and $3)$ hold. □

§ 1.4. First examples.

EXAMPLES 1.5. Let X be a non-empty set.

1) The pair $(X, \mathrm{id}_{X\times X})$ is a set-theoretic solution to the Yang–Baxter equation. Note that $(X, \mathrm{id}_{X\times X})$ is not non-degenerate, since $\lambda_x(y) = x$ and $\rho_y(x) = y$, for all $x, y \in X$.

2) Let $\tau : X \times X \to X \times X$ be the flip map, i.e. $\tau(x,y) = (y,x)$ for all $x, y \in X$. Then, the pair (X, τ) is a set-theoretic solution to the Yang–Baxter equation. Moreover, it is non-degenerate since $\lambda_x = \rho_x = \mathrm{id}_X$ for all $x \in X$.

3) Let λ, ρ be permutations of X. Then $r(x,y) = (\lambda(y), \rho(x))$ is a non-degenerate set-theoretic solution to the Yang–Baxter equation if and only if $\lambda\rho = \rho\lambda$. Moreover, (X, r) is involutive if and only if $\rho = \lambda^{-1}$. The solution (X, r) is called a *permutational solution* or a *Lyubashenko's solution*.

If, on the set X, we have a bit more structure, we can define some more sophisticated solutions.

EXAMPLE 1.6. Let G be a group and, let

$$\begin{aligned} r_1(x,y) &= (y, y^{-1}xy) \\ r_2(x,y) &= (x^2y, y^{-1}x^{-1}y). \end{aligned}$$

Then (X, r_1) and (X, r_2) are bijective non-degenerate set-theoretic solutions to the Yang–Baxter equation.

§ 1.5. Set-theoretic solutions to the Yang–Baxter equation and III Reidemeister move. Let us represent the map $r : X \times X \to X \times X$ as a crossing and the identity on X as a straight line; see Figure 1.

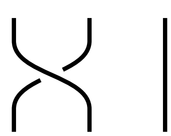

FIGURE 1. The map r represented by a crossing and the identity as a straight line.

Then the Yang–Baxter equation can be pictured as in Figure 2.

Moreover, we have the following lemma under the assumption of (X, r) being non-degenerate

LEMMA 1.7. *Let (X, r) be a solution to the Yang–Baxter equation.*

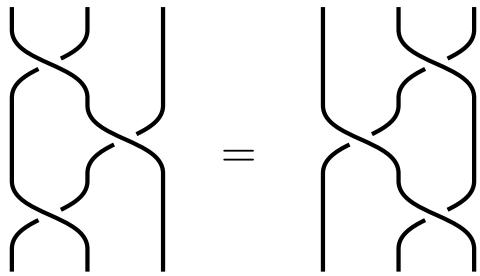

FIGURE 2. The Yang–Baxter equation.

1) *Given $x,u \in X$, there exist unique $y,v \in X$ such that $r(x,y) = (u,v)$.*
2) *Given $y,v \in X$, there exist unique $x,u \in X$ such that $r(x,y) = (u,v)$.*

PROOF. For the first claim take $y = \lambda_x^{-1}(u)$ and $v = \rho_y(x)$. For the second, $x = \rho_y^{-1}(v)$ and $u = \lambda_x(y)$. □

So, the bijectivity of r means that any row in Figure 3 determines the whole square. By Lemma 1.7 we have that non-degeneracy means that any column in Figure 3 also determines the entire square.

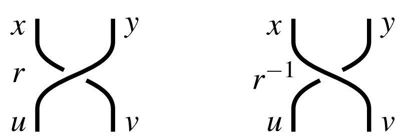

FIGURE 3. Any row or column determines the whole square.

§ 1.6. The derived solution.

PROPOSITION 1.8. *Let (X,r) be a non-degenerate set-theoretic solution to the Yang–Baxter equation. For any $x,y \in X$ consider*

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

Then $s : X \times X \to X \times X$ defined by $s(x,y) = (y, \sigma_y(x))$ is a solution to the Yang-Baxter equation. Moreover, r is bijective if and only if σ_y is bijective for every $y \in X$.

EXERCISE 1.9. Prove Proposition 1.8.

CONVENTION 2. From now on, a *solution* will always mean a non-degenerate bijective set-theoretic solution to the Yang–Baxter equation.

DEFINITION 1.10. Let (X,r) be a solution. The pair (X,s) is called the *derived solution* of the solution (X,r).

§ 1.7. Involutive solutions. In [**6**], Rump proved that radical rings provide examples of involutive solutions.

DEFINITION 1.11. A ring $(R,+,\cdot)$ is said to be *radical* if R with respect the binary operation $\circ$ defined by $x \circ y = x + y + xy$ is a group. We denote by x' the inverse of x with respect to $\circ$.

DEFINITION 1.12. A solution (X,r) is said to be *involutive* if $r^2 = \mathrm{id}_{X\times X}$.

PROPOSITION 1.13. *Let R be a radical ring. Then (R,r), where*

$$r(x,y) = (-x+x\circ y, (-x+x\circ y)'\circ x\circ y) \tag{1.2}$$

is an involutive solution to the YBE.

EXERCISE 1.14. Let X be a non-empty set and $\lambda_x : X \to X$ bijective maps. Define $r : X\times X \to X\times X$ by $r(x,y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x))$. Prove that (X,r) is an involutive map satisfying (1.1) if and only if

$$\lambda_x\lambda_{\lambda_x^{-1}(y)} = \lambda_y\lambda_{\lambda_y^{-1}(x)},$$

for all $x,y\in X$.

§ 1.8. Skew braces. Do we need radical rings to produce solutions of the form (1.2)?

DEFINITION 1.15. A *skew (left) brace* is a triple $(A,+,\circ)$, where $(A,+)$ and $(A,\circ)$ are (not necessarily abelian) groups and

$$a\circ(b+c) = (a\circ b) - a + (a\circ c) \tag{1.3}$$

holds for all $a,b,c\in A$.

The groups $(A,+)$ and $(A,\circ)$ are respectively the *additive* and *multiplicative* group of the skew brace A.

One says that a skew left brace A is of *abelian type* (it also is simply called a left brace) if $(A,+)$ is an abelian group. In general, the properties of the additive group determine the type of a skew brace[1].

REMARK 1.16. Even though we use the additive notation, the group $(A,+)$ is not necessarily abelian.

CONVENTION 3. The identity of $(A,+)$ will be denoted by 0 and the inverse of an element a will be denoted by $-a$.

As for radical rings, we write a' to denote the inverse of a with respect to the circle operation $\circ$.

Right left braces are defined similarly.

DEFINITION 1.17. A *skew right brace* is a triple $(A,+,\circ)$, where $(A,+)$ and $(A,\circ)$ are groups and

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

holds for all $a,b,c\in A$.

EXERCISE 1.18. Prove that there exists a bijective correspondence between skew left braces and skew right braces.

CONVENTION 4. From now on, with the term skew brace, we will always mean a skew left brace.

EXAMPLES 1.19. Let $(A,+)$ be a group.

[1]Such terminology is borrowed from Hopf-Galois extension where the additive group determines the type of the extension.

1) Then A is a skew brace with $a \circ b = a + b$ for all $a, b \in A$. Such a skew brace is called a *trival skew brace*.
2) Similarly, the operation $a \circ b = b + a$ turns A into a skew brace. Such a skew brace is called an *almost trivial skew brace*.

§ 1.9. First examples.

Example 1.20. Let $(A, +)$ be a group. Then A is a skew brace with $a \circ b = a + b$ for all $a, b \in A$. Such a skew brace is called a *trivial skew brace*.

Example 1.21. Let $(A, +)$ be a group. The operation $a \circ b = b + a$ turns A into a skew brace. Such a skew brace is called an *almost trivial skew brace*.

Definition 1.22. Let A and B be skew braces. Then $A \times B$ with

$$(a,b) + (a_1, b_1) = (a + a_1, b + b_1),$$
$$(a,b) \circ (a_1, b_1) = (a \circ a_1, b \circ b_1),$$

is a skew brace. This is the *direct product* of the skew braces A and B.

Exercise 1.23. Let $(A, +)$ and $(M, +)$ be groups and let $\alpha \colon A \to \mathrm{Aut}(M)$ be a group homomorphism. Prove that $M \times A$ with

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

is a skew brace. Similarly, prove that $M \times A$ with

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

is a skew brace.

Exercise 1.24. Let $(A, +)$ be a group with an *exact factorisation* through the subgroups B and C (i.e. B and C are subgroups of A such that $B \cap C = \{0\}$ and $A = B + C$). This means that each $x \in A$ can be written in a unique way as $x = x_B + x_C$, for some $x_B \in B$ and $x_C \in C$. Set

$$x \circ y = x_B + y + x_C.$$

Prove that

1) $(A, \circ)$ is a group isomorphic to $B \times C$, the direct product of B and C.
2) $(A, +, \circ)$ is a skew brace.

§ 1.10. Basic properties of skew braces.

Lemma 1.25. *Let A be a skew brace. The following statements hold.*

1) $1 = 0$*, where* 0 *denotes the identity of* $(A, +)$ *and by* 1 *the identity of* $(A, \circ)$.
2) $-(a \circ b) = -a + a \circ (-b) - a$*, for all* $a, b \in A$.

Proof. By (1.3) we have

$$0 = 1 \circ 0 = 1 \circ (0 + 0) = 1 \circ 0 - 1 + 1 \circ 0 = -1.$$

Hence $0 = 1$. Now, let $a, b \in B$. From what we just proved and by (1.3) we have

$$a = a \circ 0 = a \circ (b - b) = a \circ b - a + a \circ (-b).$$

and 2) follows. □

PROPOSITION 1.26. *Let A be a skew brace. For each $a \in A$, the map*

$$\lambda_a : A \to A, b \mapsto -a + a \circ b$$

is an automorphism of $(A, +)$.

Moreover, the map $\lambda : (A, \circ) \to \mathrm{Aut}(A, +), a \mapsto \lambda_a$, is a group homomorphism.

PROOF. First, let us prove that λ_a is an endomorphism of $(A, +)$, for all $a \in A$. We have that

$$\lambda_a(b + c) = -a + a \circ (b + c) \overset{(1.3)}{=} -a + a \circ b - a + a \circ c,$$

for all $b, c \in A$. Now, for any $b \in A$,

$$\lambda_0(b) = -0 + 0 \circ b \overset{1=0}{=} b,$$

hence $\lambda_0 = \mathrm{id}_A$. Moreover, for any $a, b, c \in A$,

$$\lambda_a\lambda_b(c) = -a + a \circ (-b + b \circ c) = -a + a \circ (-b) - a + a \circ b \circ c = -(a \circ b) + a \circ b \circ c = \lambda_{a \circ b}(c).$$

Hence, $\lambda_a\lambda_b = \lambda_{a \circ b}$, for all $a, b \in A$. It follows that for any $a \in A$, the map λ_a is bijective with inverse $\lambda_{a'}$. □

EXERCISE 1.27. Let A be a skew brace. Prove that

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

for all $a, b \in A$. As a consequence, we have that $\rho_b(a) = (a' + b)' \circ b$, for all $a, b \in A$.

PROPOSITION 1.28. *Let A be a brace. For each $a \in A$, the map*

$$\rho_b \colon A \to A, \quad \mapsto (\lambda_a(b))' \circ a \circ b,$$

is bijective. Moreover, the map $\rho \colon (A, \circ) \to \mathrm{Sym}(A)$, $b \mapsto \rho_b$, satisfies $\rho_c\rho_b = \rho_{b \circ c}$, for all $b, c \in A$.

PROOF. By Exercise 1.27, we get that $\rho_b(a) = (a' + b)' \circ b$, for all $a, b \in A$. Now, for all $a \in A$, we have that

$$\rho_0(a) = (a' + 0)' \circ 0 = a,$$

i.e., $\rho_0 = \mathrm{id}_A$. Moreover, for all $a, b, c \in A$, we have

$$\begin{aligned}\rho_c\rho_b(a) &= ((\rho_b(a))' + c)' \circ c = (((a' + b)' \circ b)' + c)' \circ c \\ &= ((b' \circ (a' + b) + c)' \circ c = (b' \circ a' - b + c)' \circ c \\ &= (b' \circ (a' + b \circ c))' \circ c = (a' + b \circ c)' \circ b \circ c \\ &= \rho_{b \circ c}(a),\end{aligned}$$

i.e., $\rho_{b \circ c} = \rho_c\rho_b$. It also follows that ρ_b is bijective with inverse $\rho_{b'}$ for every $b \in A$. □

§ 1.11. Skew braces and solutions. Now we can state the theorem that gives a first connection of skew braces with solutions. The following result has been proved by Guarnieri and Vendramin in [**4**] extending an analogous result proved by Rump in [**6**] for involutive solutions.

THEOREM 1.29. *Let A be a skew brace. Then (A,r_A), where*

$$r_A(x,y) = (-x+x\circ y, (-x+x\circ y)'\circ x\circ y)$$

is a bijective solution to the YBE. Moreover, (A,r_A) is involutive if and only if A is of abelian type.

PROOF. As before, let us set

$$\begin{aligned}\lambda_x(y) &= -x+x\circ y\\ \rho_y(x) &= (\lambda_x(y))'\circ x\circ y.\end{aligned}$$

By Proposition 1.26 and Proposition 1.28, we have that $\lambda: A\to \operatorname{Aut}(A,+)$ is a left action of A on itself and $\rho: A\to \operatorname{Sym}(A)$ is a right action of A on itself. Moreover, by definition

$$\lambda_x(y)\circ\rho_y(x) = x\circ y,$$

i.e. condition (2.1) in Theorem 2.7 is satisfied. Hence, by Theorem 2.7, (A,r_A) is a solution.

Now let us compute r_A^2,

$$r_A^2(x,y) = (-\lambda_x(y)+\lambda_x(y)\circ\rho_y(x), (-\lambda_x(y)+\lambda_x(y)\circ\rho_y(x))'\circ\lambda_x(y)\circ\rho_y(x)).$$

First if we assume $(A,+)$ abelian, we have

$$\begin{aligned}-\lambda_x(y)+\lambda_x(y)\circ\rho_y(x) &= -(-x+x\circ y)+x\circ y = -(x\circ y)+x+x\circ y\\ &\overset{\text{Lemma 1.25}}{=} -x+x\circ(-y)+x\circ y = x\circ(-y)-x+x\circ y\\ &\overset{(1.3)}{=} x\circ(-y+y) = x\end{aligned}$$

and

$$(-\lambda_x(y)+\lambda_x(y)\circ\rho_y(x))'\circ\lambda_x(y)\circ\rho_y(x) = x'\circ x\circ y = y.$$

Hence, (A,r_A) is involutive.

Now let us assume (A,r_A) involutive. In particular, for all $x,y\in A$

$$x = -\lambda_x(y)+\lambda_x(y)\circ\rho_y(x) = -(x\circ y)+x+x\circ y.$$

For the arbitrary of y and since $(A,\circ)$ is a group, it follows $x=-y+x+y$, for all $x,y\in A$, i.e. $(A,+)$ is abelian. □

EXERCISE 1.30. Let A be a skew brace. Prove that

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

and

$$a\circ b = a+\lambda_a(b)$$

§ 1.12. Subbraces and ideals.

DEFINITION 1.31. Let A be a skew brace.

A *subbrace* f A is a subset B of A such that $(B,+)$ is a subgroup of $(A,+)$ and $(B,\circ)$ is a subgroup of $(A,\circ)$.

A *left ideal* of A is a subgroup $(I,+)$ of $(A,+)$ such that $\lambda_b(I) \subseteq I$ for all $b \in B$, i.e. $\lambda_b(x) \in I$ for all $b \in A$ and $x \in I$.

A *strong left ideal* of A is a left ideal I of A such that $(I,+)$ is a normal subgroup of $(A,+)$.

LEMMA 1.32. *A left ideal I of a skew brace A is a subbrace of B.*

PROOF. We need to prove that $(I,\circ)$ is a subgroup of $(A,\circ)$. Clearly I is non-empty, as it is an additive subgroup of A. If $x,y \in I$, then

$$x \circ y = x - x + x \circ y = x + \lambda_x(y) \in I + I = I$$

and

$$x' = -\lambda_{x'}(x) \in I.$$

□

EXERCISE 1.33. Let A be a skew brace. Then

$$\mathrm{Fix}(A) = \{b \in B \colon \lambda_x(b) = b,\ \forall b \in A\}$$

is a left ideal of A.

DEFINITION 1.34. An *ideal* of a skew brace A is a strong left ideal I of A such that $(I,\circ)$ is a normal subgroup of $(A,\circ)$.

In general, left ideals, strong left ideals and ideals are different notions.

DEFINITION 1.35. Let A be a skew brace. The subset $\mathrm{Soc}(A) = \ker\lambda \cap Z(A,+)$ is the *socle* of A.

PROOF. First, $\mathrm{Soc}(A) \neq$, since $0 \in \mathrm{Soc}(A)$. Moreover, if $x \in \mathrm{Soc}(A)$, then $x' = \lambda_x(x') = -x$. It follows that if $x,y \in \mathrm{Soc}(A)$ then

$$\lambda_{x-y} = \lambda_{x\circ y'} = \lambda_x\lambda_{y'} = \lambda_x\lambda_y^{-1} = \mathrm{id}_A,$$

and, clearly $x - y \in Z(A,+)$. Hence, $\mathrm{Soc}(A)$ is an additive subgroup of A and since $\mathrm{Soc}(A)$ is a subgroup of $Z(A,+)$ it is also a normal additive subgroup of A. Moreover, for all $x \in \mathrm{Soc}(A)$ and $a \in A$:

$$\lambda_a(x) = a \circ x - a \tag{1.4}$$

$$\lambda_a(x) = a \circ x \circ a'. \tag{1.5}$$

For the first equality we have that applying Exercise 1.30

$$\lambda_a(x) = a \circ (a' + x) = a \circ (x + a') \overset{(1.3)}{=} a \circ x - a,$$

for the second equality

$$\lambda_a(x) = a \circ (a' + x) = a \circ (x \circ \lambda_x(a')) = a \circ x \circ a'.$$

It follows that, for all $x \in \operatorname{Soc}(A)$ and $a, b \in A$, we have

$$\lambda_{\lambda_a(x)} \overset{(1.4)}{=} \lambda_{a \circ x \circ a'} = \lambda_a \lambda_x \lambda_a^{-1} = \lambda_a \lambda_a^{-1} = \mathrm{id}_A$$

and, by Exercise 1.30,

$$\begin{aligned} b + \lambda_a(x) = b \circ \lambda_b^{-1} \lambda_a(x) = b \circ \lambda_{b' \circ a}(x) &\overset{(1.5)}{=} a \circ x \circ a \circ b \\ &\overset{(1.5)}{=} \lambda_a(x) \circ b = \lambda_a(x) + \lambda_{\lambda_a(x)}(b) = \lambda_a(x) + b, \end{aligned}$$

i.e., $\lambda_a(x) \in Z(A,+)$. Finally, it also follows that for any $a \in A$ and $x \in \operatorname{Soc}(A)$, $a \circ x \circ a' \in \operatorname{Soc}(A)$. Therefore, $\operatorname{Soc}(A)$ is an ideal of A. $\square$

Exercise 1.36. Let A be a skew brace. Prove that $\operatorname{Soc}(A) = \ker \lambda \cap \ker \rho$.

Definition 1.37. Let A be a skew brace. The subset $\operatorname{Ann}(A) = \operatorname{Soc}(A) \cap Z(B, \circ)$ is the *annihilator* of B.

Proposition 1.38. *The annihilator of a skew brace A is an ideal of A.*

Proof. First, if $x, y \in \operatorname{Ann}(A)$, then $x - y \in \operatorname{Soc}(A)$ and for any $a \in A$

$$(x-y) \circ a = x \circ y' \circ a = x \circ a \circ y' a \circ x \circ y' = a \circ (x-y),$$

i.e. $x - y \in \operatorname{Ann}(A)$. Now, since $\operatorname{Ann}(A) \subseteq Z(A,+) \cap Z(A,\circ)$, we only need to prove $\lambda_a(x) \in \operatorname{Ann}(A)$, for all $x \in \operatorname{Ann}(A)$ and $a \in A$. By (1.4) we have that $\lambda_a(x) = a \circ x \circ a' = x \circ a \circ a' = x \in \operatorname{Ann}(A)$. $\square$

§ 1.13. The isomorphism theorems. If A is a skew brace and I is an ideal of A, then $a + I = a \circ I$ for all $a \in A$.

This allows us to prove that there exists a unique skew brace structure over A/I such that the map

$$A \mapsto A/I, \quad a \mapsto a + I = a \circ I,$$

is a homomorphism of skew braces.

Definition 1.39. The skew brace A/I is the *quotient skew brace* of A modulo I.

It is possible to prove the isomorphism theorems for skew braces. (See Exercises 2.17–2.20).

Lecture 2. 22/02/2024

§ 2.1. Exercises and Problems.

EXERCISE 2.1. 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.

§ 2.2. Shelfs and racks.

EXERCISE 2.2. 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 1.1 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 2.3. 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 2.4. *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 2.2. □

EXERCISE 2.5. 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 2.6. 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.

§ 2.3. An intriguing connection between group actions and solutions.

The following theorem is the core result of the paper [**5**] by Lu, Yan Zhu.

THEOREM 2.7. *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*

$$uv = \lambda_u(v)\rho_v(u) \tag{2.1}$$

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 2.8. Prove Theorem 2.7

EXERCISE 2.9. 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 2.10. Let A be a skew brace. Prove that

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

EXERCISE 2.11. 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 $a \circ b = a + a * b + c$ turns A into a group.

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

EXERCISE 2.12. 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 2.13. 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 2.14 (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 2.15. 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 2.16. 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 2.17. Let $f : A \to B$ be a homomorphism of skew braces. Prove that $A/\ker f \cong f(A)$.

EXERCISE 2.18. 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 2.19. 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 2.20. 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 2.21. 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 2.22. 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 3. 23/02/2024

§ 3.1. From solutions to skew braces.

Definition 3.1. Let (X,r) be a solution. The *structure group* of (X,r) is the group

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

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

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

Theorem 3.2 ([**3**] or [**5**]). *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. □

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

Proposition 3.3. *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. □

§ 3.2. The permutation group of a 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

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

Since

$$\sigma_x\sigma_y = \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)} \quad \text{and} \quad \tau_x^{-1}\tau_y^{-1} = \tau^{-1}_{\sigma_x(y)}\tau^{-1}_{\tau_y(x)}$$

for all $x,y \in X$, there exists a unique group homomorphism $h\colon G(X,r) \to \mathscr{G}(x,r)$ such that $hi(x) = (\sigma_x, \tau_x^{-1})$ for all $x \in X$. We write

$$h(a) = (\sigma_a, \tau_a^{-1})$$

for all $a \in G(X,r)$. By Theorem **??**, $G(X,r)$ has a unique structure of skew brace with multiplicative group the structure group $G(X,r)$ and $\lambda_{i(x)}(i(y)) = i(\sigma_x(y))$ for all $x,y \in X$. We shall see that $\ker h$ is an ideal of the skew brace $G(X,r)$. Note that

$$\mu_{i(y)}(i(x)) = \lambda_{i(x)}(i(y))^{-1} i(x)i(y) = i(\sigma_x(y))^{-1} i(x)i(y) = i(\tau_y(x))$$

for all $x,y \in X$, by the defining relations of $G(X,r)$.

§ 3.3. The retraction of a solution. Let (X,r) be a solution and define on X the following relation

$$x \sim y \iff \lambda_x = \lambda_y \text{ and } \rho_x = \rho_y.$$

Let $\bar{X} = X/\sim$ denote the set of equivalence classes and let $[x]$ denote the class of x.

LEMMA 3.4. *Let (X,r) be a solution and write $r^{-1}(x,y) = (\hat{\lambda}_x(y), \hat{\rho}_y(x))$. Then*

$$\hat{\lambda}_y^{-1}(x) = \rho_{\lambda_x^{-1}(y)}(x), \tag{3.1}$$

$$\lambda_x^{-1}(y) = \hat{\rho}_{\hat{\lambda}_y^{-1}(x)}(y), \tag{3.2}$$

$$\hat{\rho}_x^{-1}(y) = \lambda_{\rho_y^{-1}(y)}(y), \tag{3.3}$$

$$\rho_y^{-1}(x) = \hat{\lambda}_{\hat{\rho}_x^{-1}(y)}(x). \tag{3.4}$$

EXERCISE 3.5. Prove Lemma 3.4.

THEOREM 3.6. *Let (X,r) be a solution. Then r induce a solution $\bar{r}$ on $\bar{X}$ by*

$$\bar{r}([x],[y]) = ([\lambda_x(y)], [\rho_y(x)]),$$

for all $x,y \in X$.

PROOF. First of all, let us prove that $\bar{r}$ is well-defined. Let $x,x',y,y' \in X$ such that $x \sim x'$ and $y \sim y'$, i.e. $\lambda_x = \lambda_{x'}$, $\rho_x = \rho_{x'}$, and $\lambda_y = \lambda_{y'}$, $\rho_y = \rho_{y'}$. From Proposition 1.4 we have

$$\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)} = \lambda_x\lambda_y = \lambda_x\lambda_{y'} = \lambda_{\lambda_x(y')}\lambda_{\rho_{y'}(x)} = \lambda_{\lambda_x(y')}\lambda_{\rho_y(x)}$$

and since (X,r) is non-degenerate we get $\lambda_{\lambda_x(y)} = \lambda_{\lambda_x(y')} = \lambda_{\lambda_{x'}(y')}$. Similarly,

$$\rho_{\rho_y(x)}\rho_{\lambda_x(y)} = \rho_x\rho_y = \rho_x\rho_{y'} = \rho_{\rho_{y'}(x)}\rho_{\lambda_x(y')} = \rho_{\rho_y(x)}\rho_{\lambda_x(y')}$$

and so $\rho_{\lambda_x(y)} = \rho_{\lambda_x(y')} = \rho_{\lambda_{x'}(y')}$. Hence

$$\lambda_x(y) \sim \lambda_{x'}(y').$$

Following the same procedure we get

$$\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)} = \lambda_x\lambda_y = \lambda_{x'}\lambda_y = \lambda_{\lambda_{x'}(y)}\lambda_{\rho_y(x')} = \lambda_{\lambda_x(y)}\lambda_{\rho_{y'}(x')},$$

i.e., $\lambda_{\rho_y(x)} = \lambda_{\rho_{y'}(x')}$. And

$$\rho_{\rho_y(x)}\rho_{\lambda_x(y)} = \rho_x\rho_y = \rho_{x'}\rho_y = \rho_{\rho_y(x')}\rho_{\lambda_x(y)} = \rho_{\rho_{y'}(x')}\rho_{\lambda_x(y)},$$

i.e., $\rho_{\rho_y(x)} = \rho_{\rho_{y'}(x')}$. Hence,

$$\rho_y(x) \sim \rho_{y'}(x').$$

Therefore, r is well-defined.

Now let us prove that $\bar{r}$ is bijective. Since (X,r) is a solution in particular r is bijective. Let us write

$$r^{-1}(x,y) = (\hat{\lambda}_x(y), \hat{\rho}_y(x)).$$

Since (X, r^{-1}) is a solution with the same arguments as before we have that $\overline{r^{-1}}$ is well-defined. Moreover, if $z \in X$, then

$$\hat{\lambda}_x^{-1}(z) \overset{(3.1)}{=} \rho_{\lambda_x^{-1}(z)}(x) \sim \rho_{\lambda_{x'}^{-1}(z)}(x) \sim \rho_{\lambda_{x'}^{-1}(z)}(x') \sim \hat{\lambda}_{x'}^{-1}(z)$$

$$\overline{r^{-1}}\,\overline{r}(x,y) = \overline{r^{-1}}([\lambda_x(y)]$$

□

Theorem 3.7. *Let (X, r) be a finite multipermutation solution to the YBE. If $|X| > 1$, then r has even order.*

Proof. Since $(X, r) \to \mathrm{Ret}(X, r)$, $x \mapsto [x]$ is a homomorphism of solutions, it follows that the order of the solution $\overline{r}$ divides the order of r. Assume that (X, r) has multipermutation level n. There exists a homomorphism of solutions $(X, r) \to \mathrm{Ret}^{n-1}(X, r)$, thus it is enough to prove the theorem when $r(x,y) = (\lambda(y), \rho(x))$ for commuting permutations λ and ρ, i.e. multipermutation solutions of level 1. If r has order $2k+1$, then

$$(x,y) = r^{2k+1}(x,y) = (\lambda^{k+1}\rho^k(y), \lambda^k\rho^{k+1}(x)).$$

This implies that $\lambda^{k+1}\rho^k(y) = x$ for all $x, y \in X$. This equality in particular implies that $x = y$ because $\lambda^{k+1}\rho^k$ is a permutation, a contradiction. □

Appendix

§ 3.4. Radical rings.

Definition 3.8. 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 3.9. 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 3.10. Let R be a unitary ring. The *(Jacobson) radical* $J(R)$ of R is defined as the intersection of all maximal left ideals[2] of R.

Exercise 3.11. 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 3.12. A non-unitary ring R is a *(Jacobson) radical ring* if it is isomorphic to the Jacobson radical of a unitary ring.

Proposition 3.13. *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 $\psi\colon R\to M$ be a homomorphism such that $\psi(R)$ is isomorphic to $J(M)$. Now, if $a\in R$, then $\psi(a)\in J(M)$. By Exercise 3.11, $1+\psi(a)$ is invertible, i.e. there exists $c\in M$ such that

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

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

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 3.11, 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 3.14. 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 3.15. *Then* $(R,\circ)$ *is a monoid with neutral element* 0.

Exercise 3.16. Prove Lemma 3.15.

Convention 5. If $a \in R$ is invertible in the monoid $(R,\circ)$, we will denote by a' its inverse.

Examples 3.17.

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

2.1. It is enough to apply Proposition 1.4.

1.9. 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 1.4, implies that

$$\lambda_x \sigma_y = \sigma_{\lambda_x(y)} \lambda_x. \tag{3.5}$$

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 1.4, implies that

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

Indeed

$$\begin{aligned}
\rho_z \rho_y(x) &= \lambda^{-1}_{\lambda_{\rho_y(x)}(z)} \sigma_{\lambda_{\rho_y(x)}(z)} \lambda^{-1}_{\lambda_x(y)} \sigma_{\lambda_x(y)}(x) \overset{(3.5)}{=} \lambda^{-1}_{\lambda_{\rho_y(x)}(z)} \lambda^{-1}_{\lambda_x(y)} \sigma_{\lambda_{\lambda_x(y)} \lambda_{\rho_y(x)}(z)} \sigma_{\lambda_x(y)}(x) \\
&\overset{1)}{=} \lambda^{-1}_{\lambda_{\rho_y(x)}(z)} \lambda^{-1}_{\lambda_x(y)} \sigma_{\lambda_x \lambda_y(z)} \sigma_{\lambda_x(y)}(x).
\end{aligned}$$

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 $y \in X$.

2.2. 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 1.4. 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.

2.8. 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

$$\begin{aligned} u_1v_1w_1&=\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)\rho_{\lambda_{\rho_y(x)}(z)}\lambda_x(y)\rho_z\rho_y(x)\\ &\overset{(2.1)}{=}\lambda_x(y)\lambda_{\rho_y(x)}(z)\rho_z\rho_y(x)\\ &\overset{(2.1)}{=}\lambda_x(y)\rho_y(x)z\\ &\overset{(2.1)}{=}xyz\end{aligned}$$

and, similarly

$$\begin{aligned} u_2v_2w_2&=\lambda_x\lambda_y(z)\lambda_{\rho_{\lambda_y(z)}(x)}\rho_z(y)\rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x)\\ &\overset{(2.1)}{=}\lambda_x\lambda_y(z)\rho_{\lambda_y(z)}(x)\rho_z(y)\\ &\overset{(2.1)}{=}x\lambda_y(z)\rho_z(y)\\ &\overset{(2.1)}{=}xyz.\end{aligned}$$

Hence

$$u_1v_1w_1=xyz=u_2v_2w_2. \tag{3.6}$$

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

$$u_1=\lambda_{\lambda_x(y)}\lambda_{\rho_y(x)}(z)=\lambda_{\lambda_x(y)\rho_y(x)}(z)\overset{(2.1)}{=}\lambda_{xy}(z)=\lambda_x\lambda_y(z)=u_2.$$

Similarly, since ρ is a right action

$$w_2=\rho_{\rho_z(y)}\rho_{\lambda_y(z)}(x)=\rho_{\lambda_y(z)\rho_z(y)}(x)\overset{(2.1)}{=}\rho_{yz}(x)=\rho_z\rho_y(x)=w_1.$$

From (3.6) 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

$$\lambda_y(v^{-1})u=\lambda_y(v^{-1})\rho_v^{-1}(y)=\lambda_y(v^{-1})\rho_{v^{-1}}(y)\overset{(2.1)}{=}yv^{-1}=x^{-1}u=(\lambda_u(v))^{-1}u,$$

and so

$$(\lambda_u(v))^{-1} = \lambda_{\rho_v(u)}(v^{-1}). \tag{3.7}$$

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

$$(\rho_v(u))^{-1} = \rho_{\lambda_u(v)}(u^{-1}). \tag{3.8}$$

Define

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

Then

$$\begin{aligned} rr'(x,y) &= (\lambda_{(\rho_{x^{-1}}(y^{-1}))^{-1}}((\lambda_{y^{-1}}(x^{-1}))^{-1}), \rho_{(\lambda_{y^{-1}}(x^{-1}))^{-1}}((\rho_{x^{-1}}(y^{-1}))^{-1})) \\ &\overset{(3.7)\&(3.8)}{=} (\lambda^{-1}_{\rho_{x^{-1}}(y^{-1})}\lambda_{\rho_{x^{-1}}(y^{-1})}(x), \rho^{-1}_{\lambda_{y^{-1}}(x^{-1})}\rho_{\lambda_{y^{-1}}(x^{-1})}(y)) \\ &= (x,y). \end{aligned}$$

And

$$\begin{aligned} r'r(x,y) &= ((\rho_{(\lambda_x(y))^{-1}}((\rho_y(x))^{-1}))^{-1}, (\lambda_{(\rho_y(x))^{-1}}((\lambda_x(y))^{-1}))^{-1}) \\ &\overset{(3.7)\&(3.8)}{=} ((\rho^{-1}_{\lambda_x(y)}\rho_{\lambda_x(y)}(x^{-1}))^{-1}, (\lambda^{-1}_{\rho_y(x)}\lambda_{\rho_y(x)}(y^{-1}))^{-1}) \\ &= ((x^{-1})^{-1}, (y^{-1})^{-1}) = (x,y). \end{aligned}$$

1.24. 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.

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

$$a \circ (a' + b) \overset{(1.3)}{=} a \circ a' - a + a \circ b \overset{0=1}{=} 0 - a + a \circ b = \lambda_a(b).$$

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

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

2.15. 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.

3.5. 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] R. J. Baxter. Eight-vertex model in lattice statistics. *Phys. Rev. Lett.*, 26:832–833, 1971.

[2] V. G. Drinfeld. On some unsolved problems in quantum group theory. In *Quantum Groups (Leningrad 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992.

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

[4] L. Guarnieri and L. Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

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

[6] W. Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.

[7] C. N. Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Phys. Rev. Lett.*, 19:1312–1315, 1967.

Index

I

III Reidemeister move 4

R

Rack 12
Ring 18

S

Set-theoretic solution 3
  Finite 3
  Non-degenerate 3
Shelf 12
Solution
  permutation group 15

Y

Yang–Baxter equation 3