Snapshots of modern mathematics
from Oberwolfach

№ 5/2021

Braid groups, the Yang–Baxter equation, and subfactors

Gandalf Lechner

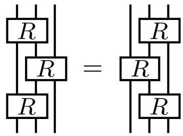
The Yang–Baxter equation is a fascinating equation that appears in many areas of physics and mathematics and is best represented diagramatically. This snapshot connects the mathematics of braiding hair to the Yang–Baxter equation and relates it to current research about systems of infinite dimensional algebras called "subfactors".

1 Introduction

What do ice crystals, braids, and quantum computers have in common with von Neumann algebras? The answer to this lies in a mathematical concept connected to all these topics, the so-called *Yang–Baxter equation*. This equation is named after Chen Ning Yang and Rodney Baxter, who discovered it independently in their research in quantum mechanics (scattering of particles) and statistical physics (crystals).

It seems surprising that two so different topics should lead to one and the same mathematical equation. But the Yang–Baxter equation and its variants play a prominent role not only in these, but also in many other fields. A few more examples are knot theory, particular models of quantum field theory, configurations of resistors in electrical circuits, and subfactors (certain pairs of infinite dimensional algebras in which the law of commutativity $xy = yx$ is maximally violated). The Yang–Baxter equation has even contributed significantly to the emergence of a whole new branch of mathematics (quantum groups) and is studied nowadays from various different points of view.

At this point it would seem appropriate to write down this Yang–Baxter equation. Here it is:



For the time being, this picture does not say much – it only indicates that the Yang–Baxter equation is an equation for an object "R" written in a little box, and that R appears three times on each side of the equation. How this diagram encodes a precise mathematical equation, and why the diagrammatical representation is much better than a formula, will be explained in this snapshot.

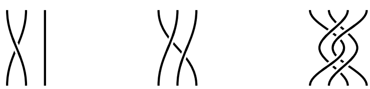
The plan for doing so is the following: At first (Section 2) we will talk about braids and meet an interesting mathematical structure, the so-called braid group. In Section 3 we then translate the abstract braid group into concrete objects, namely (multi-dimensional) tables of numbers. At this stage the Yang–Baxter equation appears as a crucial condition needed in order to ensure the consistency of the translation from braids to tables.

The solutions of this equation are only partially understood. The last part (Section 4) will draw the connection to the Oberwolfach workshop "Subfactors and Applications" on which this snapshot is based, and explain how higher mathematics can be used to study the solutions of the Yang–Baxter equation.

2 Braid groups

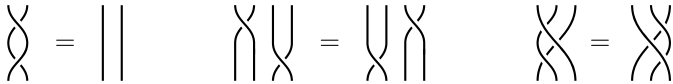
A good preparation for understanding the Yang–Baxter equation is combing your hair. When combing hair, one is usually interested in completely disentangling all strands, that is to arrange them in such a way that they are hanging down side by side without any crossings. Given a sufficiently fine comb and sufficient patience, this is in principle always possible.

From a mathematical point of view, combing hair is therefore not very interesting. It gets more exciting when we consider n strands that are fixed at their top ends (that is, at the head) but also at their bottom ends, and travel from top to bottom without looping back. In such a braid, the strands can be entangled in an arbitrary fashion, as shown in Figure (A1) in some simple examples with $n = 3$ and $n = 4$ strands instead of the usual $n \approx 100000$ strands of hair on a human head.



(A1)

In these diagrams, the little gaps at the crossings of two strands indicate which strand lies on top and which at the bottom. In slight idealization we think of the strands as arbitrarily elastic and untearable. We consider two braids to be identical when one of them can be transformed into the other by using fingers and comb, that is by stretching, twiddling, embroiling (but no cutting or tearing!) – in this case, we also say that the braids are related by a *continuous deformation*. In this sense, for example the following three equations hold:



(A2)

Since the strands are fixed at the top and bottom of their diagram, there exist infinitely many different braids that can not be transformed into each other. As soon as sufficiently many strands or crossings are involved, it is no longer easy to see whether a braid can be completely disentangled like in the first equation in (A2) or if that is impossible. Finding an algorithm that decides this question is a first mathematical problem with braid.[1]

For this and other questions it is important to learn more about the properties of the set of all braids with n strands, usually denoted B_n. The rich mathematical structure of B_n derives from the fact that any two braids a, b, represented by two arbitrary diagrams with n strands each, can be combined to a new braid, called ab. The rule defining this product is to join a and b by gluing the bottom end of a to the top end of b and then compressing the resulting diagram to the height of a and b:

(A3)

The colors and dashed lines used here are for illustration purposes only and will be omitted in the following. In general, the order in which two braids are glued together plays an important role. For example, in (A3) one has $ab \neq ba$. Do you see why?[2]

Apart from this violation of the law of commutativity there are however several analogies to multiplication of numbers: Analogous to the number 1 there exists a special braid e in B_n that satisfies $be = eb = b$ for all $b \in B_n$: The braid e consists of n parallel strands without any crossings (as on the right hand side of the first equation in (A2) or the third equation in (A4)). The product of

[1] This problem is known as the "word problem". The reason for using the term "word problem" is explained after Figure (A5). For a solution see for example [4].

[2] Hint: In this case it is sufficient to consider the end points of the strands.

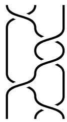
braids is associative, that is $(ab)c = a(bc)$ for all braids a, b, c. Furthermore, for each braid b there exists a corresponding inverse braid, denoted b^{-1}, that has the property that it "disentangles" b by multiplication. In a formula, this is expressed as $bb^{-1} = e = b^{-1}b$. For example:

$b =$  $b^{-1} =$  $bb^{-1} =$  $=$  $= e$ (A4)

Since such a structure is called a *group* in mathematics, one speaks of the *braid group* B_n on n strands.

Braids with a diagram having only a single crossing are called *elementary*, these are the braids that cross two neighboring strands once. In B_n there exist $2(n-1)$ elementary braids, called $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ and $\sigma_1^{-1}, \sigma_2^{-1}, \ldots, \sigma_{n-1}^{-1}$. Numbering the strands $1, 2, \ldots, n$ from the left to the right, σ_k moves strand k *over* strand $k+1$, and σ_k^{-1} moves strand k *under* strand $k+1$. For example, Fig. (A3) shows $a = \sigma_1$.

Using continuous deformations of strands, one realises that every braid in B_n can be written as a product of elementary braids. For example:

 $=$  $= \sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2.$ (A5)

Braids can be thought of as arbitrary "words" with the elementary braids σ_k and σ_k^{-1} playing the role of the "letters", for instance $\sigma_1\sigma_{10}\sigma_8^{-1}\sigma_8^{-1}\sigma_4$. Whether such a "word" can be simplified to the trivial braid e is the question posed in the "word problem" in footnote 1.

The elementary braids σ_k are well suited for an algebraic approach to the braid group. To calculate with them one only has to take into account that they satisfy the following equations:

$$\sigma_k\sigma_k^{-1} = e = \sigma_k^{-1}\sigma_k, \tag{B1}$$

$$\sigma_k\sigma_l = \sigma_l\sigma_k \quad \text{if} \;\; l \neq k \pm 1, \tag{B2}$$

$$\sigma_k\sigma_{k+1}\sigma_k = \sigma_{k+1}\sigma_k\sigma_{k+1}\,. \tag{B3}$$

These relations are easy to verify with diagrams. Fig. (A2) shows the three equations $\sigma_1\sigma_1^{-1} = e$ (left), $\sigma_1\sigma_3 = \sigma_3\sigma_1$ (middle) and $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ (right).

The equations (B1–B3) summarise the complete mathematical structure of B_n: Already in 1925, Emil Artin has shown that there are no further independent relations in the braid group [1]. That means that all equations that hold in B_n can be traced back to the fundamental equations (B1–B3). For example, the equation $\sigma_1^{-1}\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2^{-1}$ holds in B_n, but this is no really new relation but rather a consequence of (B3) (exercise). Instead of using diagrams one can work just as well with the equations (B1–B3); depending on the question the graphical or algebraic point of view is more efficient.

The algebraic view on the braid group plays a central role in several applications. Taking advantage of the fact that the equations (B1–B3) can be implemented well on a computer, there exist cryptography protocols based on the braid group [6]. Secure cryptography applications are designed in such a way that for decoding a message without the key one has to solve a computationally very demanding problem. Instead of the widely used protocol based on the difficulty of the factorization problem (find the factorization of a large integer into prime factors), the so-called conjugation problem was suggested in the context of braid groups. (Given $a, b \in B_n$, decide whether there exists $x \in B_n$ such that $a = xbx^{-1}$.)

Another application comes from physics, where braid groups appear in the description of elementary particles moving in a two-dimensional plane. A description of a set of elementary particles $t_1, \ldots, t_n$ must take into account that elementary particles of the same kind (e.g. electrons) are indistinguishable, and hence a permutation of the particles can have no observable effect. While this is formulated in terms of the symmetric group for particles moving in three dimensions, one has to use the braid group for lower dimensional systems.

Also on a purely mathematical level, the braid group still poses many challenging questions, for example in the context of knot theory or so-called representations of braids by more concrete mathematical objects as we will discuss them in the next section.

Quiz 1:

- Find the inverses of the braids shown in Fig. (A1) and (A2).
- Find a braid z in B_3 that is different from the trivial braid e and still has the property $zx = xz$ for all braids x in B_3. (Hint: First find a braid δ satisfying $\delta\sigma_1 = \sigma_2\delta$ and $\delta\sigma_2 = \sigma_1\delta$. Then consider $z = \delta\delta$.)

3 Tensor diagrams and the Yang–Baxter equation

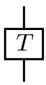
We now turn to the question of representing braids by more concrete mathematical objects. That is, we are searching for objects satisfying equations analogous to (B1–B3). “Representing” is strictly defined mathematical terminology that we will discuss in an example in the following. Studying such representations is by no means restricted to the braid group: When a mathematician encounters a group, she is often interested not only in the group as such, but also in realizing the relations in the group with concrete objects. This is a concept of fundamental importance in pure mathematics as well as its applications.

Looking at the braid grou B_n we can motivate the study of representations in different ways: One the one hand, braids only have *ambiguous* realizations as braid diagrams; each braid corresponds to infinitely many different diagrams (see (A2) for examples). In contrast, in a representation we will associated a *unique* object to each braid b. These objects will be so-called *tensors* which we may think of as multi-dimensional tables.

On the other hand, the specific representations that we will discuss in the following have several applications, in particular in quantum physics. In that field, observable quantities of a physical system (like energy, momentum, spin, ...) are in the simplest case realized by matrices which can be composed to tensors. The representations described below also appear in certain models of topological quantum computers.

So much for openers. Multi-dimensional tables? What is that supposed to mean?

To get started, let us consider a usual two-dimensional quadratic table T with d rows and d columns (also called $d \times d$ matrix):



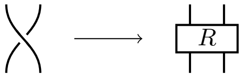
$$= T = \begin{pmatrix} T^1_1 & T^1_2 & \dots & T^1_d \\ T^2_1 & T^2_2 & \dots & T^2_d \\ \vdots & & \ddots & \vdots \\ T^d_1 & T^d_2 & \dots & T^d_d \end{pmatrix}$$

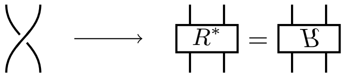
To read off an entry from such a table, one has to know the row and column number of the entry: The entry T^i_j is the number in row i and column j. Since there are d rows and columns, where $d = 1, 2, \dots$ is a parameter chosen by us, both i and j can take the values $1, 2, \dots, d$ independently of each other. The figure on the left hand side is a tensor diagram in which the upper line of T represents the upper index (row index) and the lower line represents the lower index (column index) – such diagrams will soon turn out to be very useful.

Let us now imagine a multi-dimensional table T storing numbers (entries) that depend not only on two parameters i and j, but rather on $2n$ parameters $i_1, \dots, i_n$, $j_1, \dots, j_n$, where each of these parameters can take the values $1, 2, \dots, d$. Then T has d^{2n} entries in total, and we denote these entries as $T^{i_1 \dots i_n}_{j_1 \dots j_n}$. Such a $2n$-dimensional table is difficult to write down on paper, but fits very well with tensor diagrams

with n upper and n lower lines. Here the upper lines correspond to the upper indices $i_1, \dots, i_n$ and the lower lines correspond to the lower indices $j_1, \dots, j_n$ of T (sorted from left to right). We call such a table a *tensor of size* n.

In the following we aim for a translation scheme that translates arbitrary braids b on n strands into tensors $T(b)$ of size n.[3] To find such a scheme, we will in particular need two special tensors R and R^* of size 2 to represent over- and under crossings in braid diagrams:

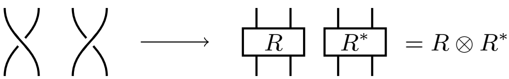




As an under crossing is the mirror image of an over crossing at a horizontal line, the same should be true for R and R^*. To achieve that, we define R^* by exchanging the upper with the lower indices of R, namely[4] $(R^*)^{i_1 i_2}_{j_1 j_2} = R^{j_1 j_2}_{i_1 i_2}$. Note that with this definition, R^* is now uniquely fixed by R.

A braid diagram can be built from its crossings by connecting the strands horizontally and vertically. Analogously, we now need rules to built a tensor diagram from R and R^* by horizontal and vertical composition. This is done by the following graphical calculus which also appears in knot theory [5].

Diagrammatically, the **horizontal composition** simply consists of writing two tensor diagrams side by side. When we write a tensor diagram T with n upper/lower lines (that is, of size n) to the left of a tensor diagram S of size m, we get a tensor diagram with $n+m$ upper and lower lines. The corresponding tensor is denoted $T \otimes S$, and its entries are defined by $(T \otimes S)^{i_1 \dots i_n a_1 \dots a_m}_{j_1 \dots j_n b_1 \dots b_m} = T^{i_1 \dots i_n}_{j_1 \dots j_n} \cdot S^{a_1 \dots a_m}_{b_1 \dots b_m}$. This horizontal composition enables us to translate a braid diagram consisting of non-overlapping crossings into a corresponding tensor. For example, the following simple braid in B_4 gets translated into a tensor of size 4 like this:



In order to also be able to translate braid diagrams such as  into tensors, we also need a tensor of size 1 for a vertical line without crossings. That is the "unit matrix" I,

---

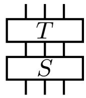
[3] We will soon see that the definition of the tensor $T(b)$ requires the specification of a special tensor R of size two. We will therefore write $T_R(b)$ instead of $T(b)$ to indicate the dependence on R.

[4] In general, the entries of R can be *complex* numbers. In that case the definition of R^* has to be supplemented by a complex conjugation of all its entries.

$$\longrightarrow \qquad I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

which as a table has 1's on the diagonal and 0's everywhere else. That is, $I^i_j = 1$ for $i = j$ and $I^i_j = 0$ for $i \neq j$.

For the **vertical composition** we consider two tensors T and S of size n and define a product TS that again is a tensor of size n. We do this in analogy to the product of braids by gluing the bottom end of the diagram of T to the top end of the diagram of S. For example, if T and S have size 3, we get

$TS =$ 

In this diagram the lower lines of T coincide with the upper lines of S. We therefore define TS as the tensor whose entries $(TS)^{i_1 \dots i_n}_{j_1 \dots j_n}$ are built from the products $T^{i_1 \dots i_n}_{k_1 \dots k_n} S^{k_1 \dots k_n}_{j_1 \dots j_n}$ (lower indices of T equal to upper indices of S), namely by summation over all d^n possibilities $k_1, \dots, k_n \in \{1, \dots, d\}$. Written as a formula, we define the tensor TS of size n as

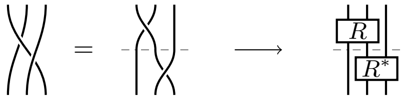
$$(TS)^{i_1 \dots i_n}_{j_1 \dots j_n} = \sum_{k_1, \dots, k_n = 1}^{d} T^{i_1 \dots i_n}_{k_1 \dots k_n} S^{k_1 \dots k_n}_{j_1 \dots j_n}.$$

To give an example, let us take $n = 1$ (just a single upper/lower index) and $d = 2$, so that T and S are (2×2)-matrices. Then our product is

$$\begin{pmatrix} T^1_1 & T^1_2 \\ T^2_1 & T^2_2 \end{pmatrix} \begin{pmatrix} S^1_1 & S^1_2 \\ S^2_1 & S^2_2 \end{pmatrix} = \begin{pmatrix} T^1_1 S^1_1 + T^1_2 S^2_1 & T^1_1 S^1_2 + T^1_2 S^2_2 \\ T^2_1 S^1_1 + T^2_2 S^2_1 & T^2_1 S^1_2 + T^2_2 S^2_2 \end{pmatrix},$$

which you might know as the *matrix product* from elsewhere. This again is a product for which the law of commutativity does *not* hold, that is in general $TS \neq ST$. One easily checks that $AI = A = IA$ holds for all matrices A, justifying our graphical notation for I (empty line without a box).

This completes our definition of the translation map $b \mapsto T_R(b)$ from braids in B_n to tensors $T_R(b)$ of size n. As mentioned before, the lower index R on T_R indicates that the mapping $b \mapsto T_R(b)$ depends crucially on the choice of R. As soon as R is fixed, we can view any braid in B_n (with an arbitrary number n of strands) as a tensor of size n. As an example, we consider the braid b from Fig. (A4):

$b =$  $= (R \otimes I)(I \otimes R^*) = T_R(b)$

All d^6 entries of $T_R(b)$ can be calculated on the basis of the composition rules described above and expressed in terms of the entries of R. To check that you have memorised these rules, you can verify that in this example (for $d = 3$)

$$T_R(b)^{123}_{211} = R^{12}_{21}R^{11}_{13} + R^{12}_{22}R^{11}_{23} + R^{12}_{23}R^{11}_{33}.$$

As a crucial point of our construction, we however still have to check that the translation from braids into tensors is consistent and does not run into contradictions. This is not evident because a diagram of a given braid can be twisted and bent into a different diagram which still represents the same braid and hence ought to be translated into the same tensor. Each such deformation can be expressed in terms of the three cases depicted in Fig. (A2) graphically and in (B1–B3) in formulae. We therefore have to make sure that in each of these three cases, the left and right hand sides of the equation correspond to the same tensor under our translation map.

It turns out that the second equation (middle of Fig. (A2) and formula (B2)) is automatically satisfied according to our rules of horizontal and vertical composition, i.e. it does not pose any conditions on R. Do you see why?[5] The first and third equation (left and right in Fig. (A2)) take the following form for tensor diagrams:

(X)

The two diagrammatic equations (X) correspond to two concrete conditions on R. The first equation poses a condition called *unitarity* which is satisfied by many tensors. The second equation is however a much more involved condition on R – this is the *Yang–Baxter equation* mentioned at the beginning, which we can now understand precisely as an equation for tensors of size 2. The tensors R solving both equations (X) simultaneously are called unitary "R-matrices".

Given any unitary R-matrix R, the map T_R is well-defined and – as mentioned before – is called *representation* by mathematicians. That means that it carries

[5] One can check that

$$(R \otimes I \otimes I)(I \otimes I \otimes R) = R \otimes R = (I \otimes I \otimes R)(R \otimes I \otimes I)$$

holds for all tensors R of size two.

products of braids into (vertical) products of tensors, i.e. satisfies $T_R(bb') = T_R(b)T_R(b')$ for all braids $b, b' \in B_n$. The tensors $T_R(\sigma_k)$ satisfy equations analogous to (B1–B3), for example $T_R(\sigma_3)T_R(\sigma_1) = T_R(\sigma_1)T_R(\sigma_3)$. In all known cases the $T_R(b)$ satisfy also additional relations that depend on R (one is in the situation of a so-called non-faithful representation) that we will however not discuss here.

To appreciate the complexity of the Yang–Baxter equation one should realise that this really is a system of d^6 coupled cubic equations (the left and right hand sides of the equation are tensors of size 3) for d^4 unknowns (the entries of the tensor R of size 2). In the simplest case $d = 2$ this amounts to 64 equations for 16 unknowns. It is not very illuminating to write down these equations explicitly, the diagrammatical form is much clearer.

An example of a solution with $d = 2$ is

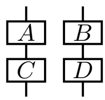
$$R = \frac{1}{\sqrt{2}}(I \otimes I + A \otimes B), \qquad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Here $\otimes$ denotes the horizontal composition defined above, and I is the (2×2) unit matrix. The sum of tensors is defined entry by entry, and the prefactor $\frac{1}{\sqrt{2}}$ multiplies all entries of the tensor.

For $d = 2$, all solutions of (X) are known. But already for $d = 3$, let alone for general d, this is no longer the case.

Quiz 2:

- Given four arbitrary tensors A, B, C, D of size 1 (that is, $(d \times d)$ matrices), consider the quadratic diagram

  Show that it does not matter whether one first horizontally composes the matrices A, B and C, D standing side by side, and then composes the resulting tensors vertically, or if one first vertically composes the matrices A, C and B, D standing on top of each other, and then composes the resulting tensors horizontally.
- Define a tensor R of size 2 as follows: $R^{i_1 i_2}_{j_1 j_2} = 1$ if $i_1 = j_2$ and $i_2 = j_1$, and $R^{i_1 i_2}_{j_1 j_2} = 0$ in all other cases. Check that R is a unitary R-matrix, solving both equations in (X).

4 From R-Matrices to subfactors and back again

The Yang–Baxter equation keeps inspiring mathematicians to come up with new ideas to learn something about its solutions. On the one hand, there is fairly concrete motivation like possible applications of R-matrices to the modelling of logical gates in a quantum computer. On the other hand, there is fundamental mathematical interest in the structure of the set of its solutions. A fascinating aspect of this equation is that it not only plays a role in so many different areas, but also that it allows for completely different approaches. For example, there exist methods based on the idea of quantisation (the transition from a system of classical mechanics to a system in quantum mechanics), or abstract algebraic methods. In this last section I want to indicate how one can approach solutions of the Yang–Baxter equation by a detour through infinite-dimensional analysis.

Let us summarise where we are after Sections 2 and 3: There exist certain tensors of size 2 that are called unitary R-matrices. The condition defining them is complicated and involves the Yang–Baxter equation. We know some examples, but we have no good overview over the set of all R-matrices. However, we do know that each R-matrix R defines a representation of braids b on n strands by tensors $T_R(b)$ of size n. These tensors can be multiplied (vertically) with each other, but they can also be added and multiplied with numbers. Hence it makes sense to talk about polynomials in the tensors $T_R(b)$. These form the algebra

$$\mathcal{N}_{R,n} = \{\text{All polynomials in } T_R(b) \text{ for arbitrary braids } b \text{ on } n \text{ strands}\}.$$

This is a finite-dimensional algebra in which the law of commutativity does not hold, as already remarked in the context of the vertical product. But the second exercise in Quiz 1 also shows that $\mathcal{N}_{R,n}$ still contains many elements Z that satisfy $ZT = TZ$ for all $T \in \mathcal{N}_{R,n}$. In this sense, $\mathcal{N}_{R,n}$ is not completely non-commutative.

This changes when one takes the limit $n \to \infty$; at the same time taking this limit also exhibits the characteristic analytic aspects of subfactors. The limit is taken in two steps: In the first step, one considers the algebra $\mathcal{N}_{R,\infty}$ defined as the union of the $\mathcal{N}_{R,n}$ over all natural numbers n. Thus $\mathcal{N}_{R,\infty}$ contains representations of braids with any arbitrary (but finite) number of strands.

While $\mathcal{N}_{R,\infty}$ is still a purely algebraic object, the second step leads to braids with infinitely many strands and relies on concepts from analysis in a crucial manner. This will be described only briefly here: One considers the so-called *trace* τ, that is the map from $\mathcal{N}_{R,\infty}$ to (complex) numbers that maps a tensor $T \in \mathcal{N}_{R,\infty}$ of size n to the number $\tau(T) = d^{-n} \sum_{i_1,\ldots,i_n=1}^{d} T_{i_1\ldots i_n}^{i_1\ldots i_n}$.[6] With the help of τ one can define the *norm* $\|T\| := \sqrt{\tau(T^*T)} \geq 0$ on $\mathcal{N}_{R,\infty}$. The norm has many similarities to the absolute value function $x \mapsto |x|$ on the rational numbers $x \in \mathbb{Q}$. Recall that the absolute value defines in particular the distance $|x - y|$ between two rational numbers x, y, and limits of sequences

[6] Diagrammatically the trace looks like this (in an example of a tensor T of size 2):

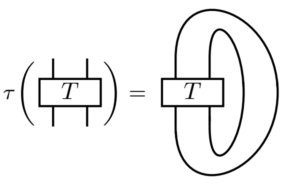
of rational numbers. When one adds all possible limits to the set of rational numbers one obtains the real numbers $\mathbb{R}$ that contain also irrational numbers like $\sqrt{2}$ and π and form the basis of analysis.

In analogy to the "completion" of $\mathbb{Q}$ to $\mathbb{R}$, also our algebra $\mathcal{N}_{R,\infty}$ can be completed with the help of the trace τ and the norm $\|\cdot\|$ to a larger algebra $\mathcal{N}_R$ (we do not give details here). In contrast to $\mathcal{N}_{R,\infty}$, the enlarged algebra $\mathcal{N}_R$ contains also representations of braids with infinitely many strands. Furthermore, this algebra contains an identity $\mathbf{I}$ corresponding to the braid with infinitely many strands and no crossings, and is "extremely non-commutative" in the sense that only multiples of $Z = \mathbf{I}$ satisfy $ZT = TZ$ for all $T \in \mathcal{N}_R$. Since $\mathcal{N}_R$ also has the right analytic properties (suitably defined limits of sequences in $\mathcal{N}_R$ also lie in $\mathcal{N}_R$), one speaks of a *factor* – a specific sort of algebra defined by John von Neumann in his research on the mathematical foundations of quantum mechanics.

Together with Francis Murray, von Neumann has organised factors in three broad types, called type I, II, and III. This classification was later refined by Alain Connes. On the basis of these results one can show that the factor $\mathcal{N}_R$ does not contain any interesting information about R; independently of R one essentially always gets the same algebra $\mathcal{N}_R$, with the official (but slightly clumsy) name "hyperfinite factor of type II_1". This sobering news seems to call into question the approach based on the algebras $\mathcal{N}_R$. However, it can be fixed: If one considers not only the factor $\mathcal{N}_R$ on its own, but also a smaller factor $\mathcal{N}_R^<$ contained in it[7], one obtains a so-called subfactor $\mathcal{N}_R^< \subset \mathcal{N}_R$, that is an inclusion of two factors. This far more complex structure contains relevant information on R and provides mathematical tools to extract this information.

Since Vaughan Jones' (1952–2020) discovery [2] of a numerical invariant measuring the relative size of the smaller factor in the bigger factor, subfactors are an intense field of study.[8] Also the workshop on which this snapshot is

---



$$= \frac{1}{d^2} \sum_{i_1,i_2=1}^{d} T^{i_1 i_2}_{i_1 i_2}.$$

[7] The smaller factor is defined by the same idea that underlies Hilbert's paradox of the Grand Hotel [8]: In the braid group with infinitely many strands one can shift all crossings to the right by one strand. The resulting braids do not entangle the first strand and lead to the smaller factor $\mathcal{N}_R^<$.

[8] Interestingly, there is also a connection in the other direction, starting from subfactors and leading to braid groups: Jones' works on subfactors led to surprising insights on representations of the braid group, and the famous Jones polynomial from knot theory [3].

based was dedicated to this topic.

With this and other methods one can study the set of all unitary R-matrices and, despite the astonishing detour from a finite tensor R over an inclusion of two infinite-dimensional algebras, obtain concrete information on the solutions of the Yang–Baxter equation. In a special case, this has already led to a complete classification [7], but in general a lot remains to be done!

A better understanding of this classification problem could have applications in quantum physics: It would clarify the status of unitary R-matricds as logical gates in a (so far hypothetical) topological quantum computer, and contribute to the understanding of quantum field theoretic models.

Image credits

All figures were produced by the author with the help of the TikZ library *knots* for this Snapshot.

References

[1] E. Artin, *Theorie der Zöpfe*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **4** (1925), 47–72.

[2] V. F. R. Jones, *Index for subfactors*, Inventiones Mathematicae **72** (1983), no. 1, 1–25.

[3] V. F. R. Jones, *Hecke algebra representations of braid groups and link polynomials*, Annals of Mathematics **126** (1987), 335–388.

[4] C. Kassel and V. Turaev, *Braid Groups*, Springer, 2008.

[5] L. Kauffman, *Knots and Physics*, World Scientific, 1993.

[6] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, *New Public-Key Cryptosystem using Braid Groups*, Advances in Cryptology – CRYPTO 2000 (Mihir Bellare, ed.), Lecture Notes in Computer Science, vol. 1880, Springer, 2000, p. 166–183.

[7] G. Lechner, U. Pennig, and S. Wood, *Yang-Baxter representations of the infinite symmetric group*, Advances in Mathematics **355** (2019), 106769.

[8] Wikipedia, *Hilbert's paradox of the grand hotel*, 2014, https://en.wikipedia.org/wiki/Hilbert%27s_paradox_of_the_Grand_Hotel, visited on September 22, 2020.

Gandalf Lechner *is Reader at Cardiff University.*

Mathematical subjects
Algebra and Number Theory, Analysis, Geometry and Topology

Connections to other fields
Physics

DOI
10.14760/SNAP-2021-005-EN

Snapshots of modern mathematics from Oberwolfach provide exciting insights into current mathematical research. They are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the interested public worldwide. All snapshots are published in cooperation with the IMAGINARY platform and can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

ISSN 2626-1995

Mathematisches
Forschungsinstitut
Oberwolfach

Member of
Leibniz
Association

IMAGINARY
open mathematics