Radical Rings, Quantum Groups, and "Theory of the Unknot"

Wolfgang Rump

In this talk, I will throw a bridge from radical rings to a variety of quantum-like mathematical structures related to Sklyanin algebras, virtual knot theory, and quantum groups.

1. What is a radical ring?

For any associative ring R, the *circle operation*

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

makes R into a semigroup with unity 0. Jacobson has shown that R is a *radical ring* (i. e. $\operatorname{Rad} R = R$) if and only if $(R, \circ)$ is a group. With respect to this *adjoint* group R°, a radical ring can be regarded as a right module, with right operation

$$x^a := xa + x, \quad x \in R, \ a \in R^\circ.$$

The identical map $\pi \colon R^\circ \to R$ then satisfies the 1-cocycle condition

$$\pi(a \circ b) = \pi(a)^b + \pi(b).$$

Thus every radical ring gives rise to a bijective 1-cocycle.

2. Braces

Definition 1. Define a *brace* to be an abelian group A with a multiplication (juxtaposition) so that

(I) $(a+b)c = ac + bc$

(II) $(A, \circ)$ is a group w.r.t. $a \circ b := ab + a + b$.

Condition (II) can be replaced by

(II_1) $a(bc + b + c) = (ab)c + ab + ac$

(II_2) The map $x \mapsto x^a := xa + x$ is bijective.

If A is left distributive, (II_1) turns into associativity. Braces are just equivalent to bijective 1-cocycles.

3. How do braces arise?

The following structure led to solutions of the quantum Yang-Baxter equation (QYBE).

Definition 2. We define a *cycle set* to be a set X with a bijective left multiplication $y \mapsto x \cdot y$, so that

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

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

By linear extension, the left multiplication defines a map

$$X \times \mathbb{N}^{(X)} \overset{\cdot}{\longrightarrow} \mathbb{N}^{(X)}.$$

What is less obvious, a unique extension to the first variable is also possible if we impose the condition

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

So we get a commutative diagram

$$\begin{tikzcd}
X \times \mathbb{N}^{(X)} \arrow[r] \arrow[d, hook] & \mathbb{N}^{(X)} \\
\mathbb{N}^{(X)} \times \mathbb{N}^{(X)} \arrow[ur, "\exists!"'] &
\end{tikzcd}$$

Proposition 1. *Let X be a cycle set. The above extension makes $\mathbb{N}^{(X)}$ into a cycle set.*

Definition 3. A cycle set A with an abelian group structure is *linear* if

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

(b) $(a+b) \cdot c = (a \cdot b) \cdot (a \cdot c)$ holds for $a, b, c \in A$.

- $\mathbb{N}^{(X)}$ is not linear since it is not a group.
- Every linear cycle set A is *non-degenerate*, i. e. the map $x \mapsto x \cdot x$ is bijective.

For example, the equation

$$a = ((-a) \cdot a) \cdot ((-a) \cdot a)$$

holds for a linear cycle set.

Proposition 2. *For a cycle set X, an extension*

$$\begin{tikzcd} X \times \mathbb{Z}^{(X)} \arrow[r] \arrow[d, hook] & \mathbb{Z}^{(X)} \\ \mathbb{Z}^{(X)} \times \mathbb{Z}^{(X)} \arrow[ur, "\exists!"'] & \end{tikzcd}$$

to a linear cycle set $\mathbb{Z}^{(X)}$ exists if and only if X is non-degenerate.

Which cycle sets are non-degenerate?

Proposition 3. *Every finite cycle set is non-degenerate.*

Thus finite cycle sets extend to linear ones. If A is linear, let $b \mapsto b^a$ denote the inverse of the left multiplication $b \mapsto a \cdot b$, and define

$$a \circ b := a^b + b.$$

Then the defining equations of A turn into

$$(a+b)^c = a^c + b^c \tag{1}$$

$$(a^b)^c = a^{b \circ c}. \tag{2}$$

Proposition 4. *Eq.* (2) *is equivalent to*

$$(a \circ b) \circ c = a \circ (b \circ c). \tag{2'}$$

Proof. $(a \circ b) \circ c = (a^b + b)^c + c = a^{b \circ c} + b^c + c = a^{b \circ c} + (b \circ c) = a \circ (b \circ c)$. $\square$

Furthermore, $(A, \circ)$ is a group with neutral element 0 and inverse $a' = -(a \cdot a)$.

In fact, $a' \circ a = (a \cdot (-a))^a + a = -a + a = 0$.

Corollary. $\boxed{\textit{Linear cycle sets=Braces}}$

In particular, every brace, hence every radical ring, gives rise to a solution of the QYBE.

4. Non-commutative group deformation

Definition 4. Let X be a finite set. A group structure $(\mathbb{Z}^{(X)}, \circ)$ with neutral element 0 is said to be of *I-type* (Tate, Van den Bergh 1996) if

$$\{x \circ a \mid x \in X\} = \{x + a \mid x \in X\}$$

holds for all $a \in \mathbb{Z}^{(X)}$.

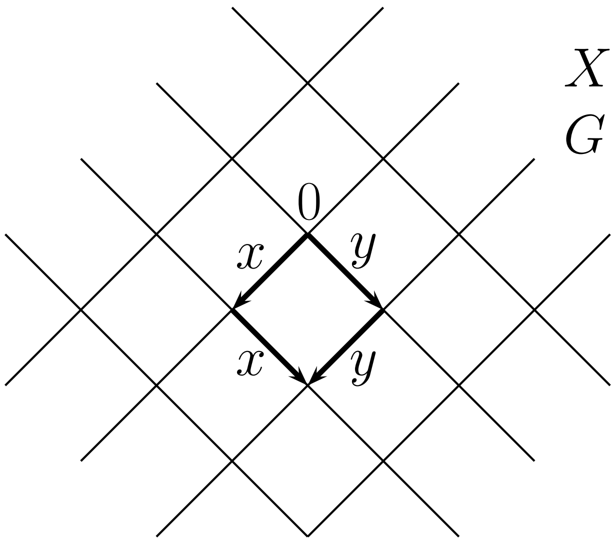
Proposition 5. *Every group* $(\mathbb{Z}^{(X)}, \circ)$ *of I-type defines a finite cycle set, and vice versa.*

Proof. Every $a \in \mathbb{Z}^{(X)}$ gives rise to a permutation $\sigma(a) \in \mathrm{S}(X)$ with $x + a = \sigma(a)(x) \circ a$. Define $x \cdot y := \sigma(x)(y)$ for $x, y \in X$. Then X becomes a cycle set.

Conversely, a finite cycle set X extends to a linear cycle set $\mathbb{Z}^{(X)}$. So $(\mathbb{Z}^{(X)}, \circ)$ is a group with $x + a = (a \cdot x)^a + a = (a \cdot x) \circ a$, for all $a \in \mathbb{Z}^{(X)}$, and $x \in X$. $\square$

Thus $G = (\mathbb{Z}^{(X)}, \circ)$ operates from the right on $\mathbb{Z}^{(X)}$. If we extend this operation to $\mathbb{R}^{(X)}$, we get a Bieberbach group G with fundamental domain $[0,1]^X$ (unit cube).

Example.



$$X = \{x, y\}$$
$$G = \langle X\,;\; x \circ x = y \circ y \rangle$$

$$(nx+my)\cdot x = \begin{cases} x & \text{for } n+m \text{ even;} \\ y & \text{for } n+m \text{ odd.} \end{cases}$$

The Quotient $\mathbb{R}^2/G$ is a Klein bottle.

5. Quandles (Joyce, Matveev 1982)

Up to weak equivalence, knots and links can be described by a set X with one binary operation.

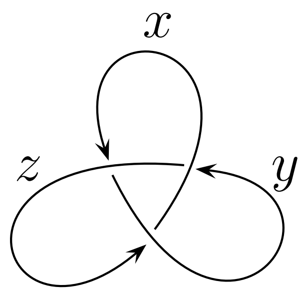
Definition 5. $(X, *)$ is said to be a *quandle* if the right multiplication $y \mapsto y * x$ is bijective, such that

$$x * x = x\,; \quad (x * y) * z = (x * z) * (y * z)$$

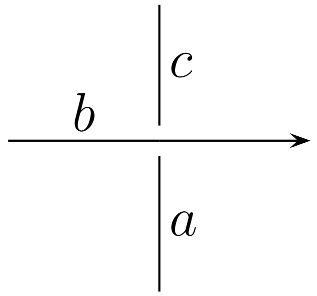
holds for all $x, y, z \in X$.

Every knot $\mathcal{K}$ defines a quandle $Q(\mathcal{K})$: Denote the arcs between successive undercrossings by variables.

Relations at each singularity:



$$x * z = y$$
$$z * y = x$$
$$y * x = z$$



$$a * b = c$$

Proposition 6 (Joyce, Matveev).

$$Q(\mathcal{K}) \cong Q(\mathcal{K}') \Longrightarrow (\mathbb{R}^3, \mathcal{K}) \cong (\mathbb{R}^3, \mathcal{K}').$$

(i. e. $\mathcal{K}, \mathcal{K}'$ are weakly equivalent)

Denote $-\mathcal{K} := \mathcal{K}$ with inverse orientation
$\mathcal{K}^* :=$ mirror image of $\mathcal{K}$.

Then

$$Q(\mathcal{K}) \cong Q(-\mathcal{K}^*).$$

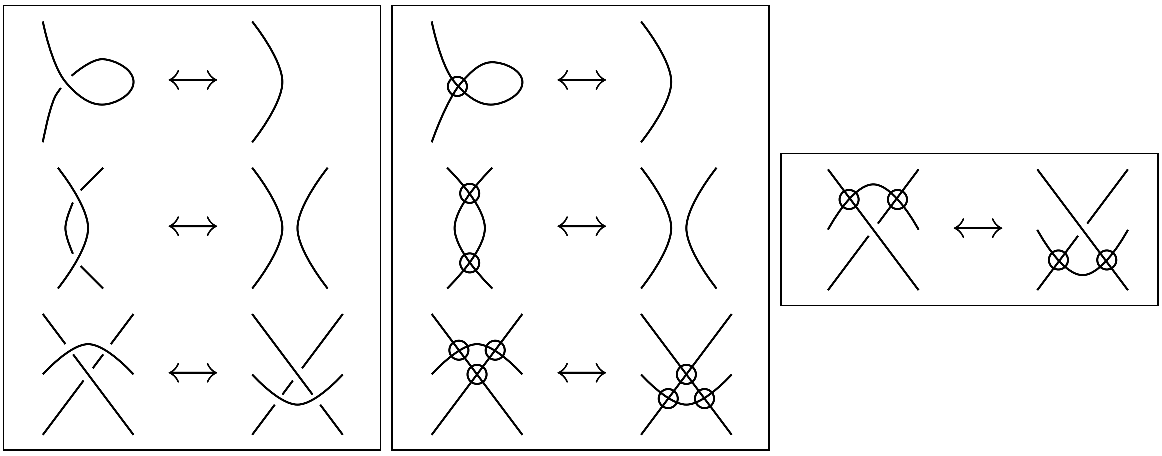
For example, the trefoil $\mathcal{K}$ satisfies $-\mathcal{K} \cong \mathcal{K}$. Hence

$$Q(\mathcal{K}^*) \cong Q(\mathcal{K}).$$

6. Virtual knots (Kauffman 1996)

Usual knots are represented by their projection into a thickened sphere, so that the crossings are maintained. If the genus of the sphere is increased, the diagram represents a *virtual knot*. Algebraically:

Definition 6 (Kauffman 1996). A *virtual* knot is given by a knot diagram with additional *virtual crossings* (at infinitesimal handles attached to the sphere), modulo generalized Reidemeister moves:



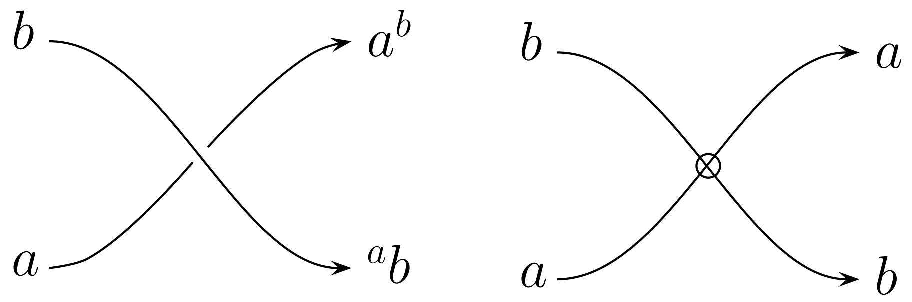
As virtual crossings merely arise from a global invariant of the ambient surface, but do not represent a singularity, they can be thrown over virtual and real crossings. Locally, virtual crossings can be treated as if they were not there!

Definition 7 (Kauffman 2004). A set X with two operations ${}^ab$ and a^b is called a *biquandle* if

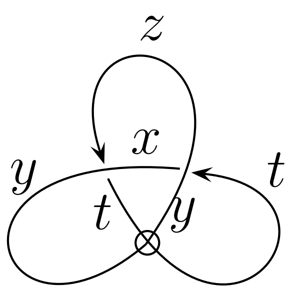
1. $a^{bc} = a^{({}^bc)(b^c)}$; ${}^{ab}c = {}^{({}^ab)(a^b)}c$; ${}^{(x^{({}^yz)})}(y^z) = ({}^xy)^{({}^{(x^y)}z)}$
2. $(a, b) \mapsto ({}^ab, a^b)$ is bijective.
3. $a \mapsto a^b$ and $a \mapsto {}^ba$ are bijective with inverse operations $a \mapsto b{\cdot}a$ and $a \mapsto b{\times}a$, respectively.
4. $(a \cdot a) \times (a \cdot a) = (a \times a) \cdot (a \times a) = a$.

(The simplified version of (4.) is due to Stanovský.)

Every virtual knot defines a biquandle: Denote the arcs between successive real crossings by variables, and consider the relations



For example,



$$x = t^y\,; \quad y = {}^z x$$
$$z = {}^t y\,; \quad t = z^x$$

Proposition 7. *A non-degenerate cycle set defines a biquandle via*

$${}^x y = x^y \cdot y.$$

Conversely, every biquandle with this property is a non-degenerate cycle set.

Now does this imply that finite cycle sets cover a part of virtual knot theory? To the contrary! Their intersection is just the unknot:

$$\{\text{finite cycle sets}\} \cap \{\text{virtual knots}\} = \{\bigcirc\}$$

Thus cycle sets are beyond virtual knot theory.

7. Minimal quantum groups

Now we return to braces, i. e. linear cycle sets. Recall that a *quantum group* is a quasi-triangular Hopf algebra.

Definition 8. A Hopf algebra H with an element $R \in (H \otimes H)^{\times}$ is said to be *quasi-triangular* if

$$\Delta^{\mathrm{op}}(a) = R\Delta(a)R^{-1}, \quad \forall\, a \in H$$
$$(\Delta \otimes 1)(R) = R^{13}R^{23}\,; \quad (1 \otimes \Delta)(R) = R^{13}R^{12}$$
$$(\varepsilon \otimes 1)(R) = (1 \otimes \varepsilon)(R) = 1.$$

The second line is a relation in $H^{\otimes 3}$ (braid relation). H is said to be *triangular* if, in addition, $R^{21}R = 1$.

Assume that H is quasi-triangular with

$$R = \sum_{i=1}^{n} a_i \otimes b_i,$$

such that n is minimal. Consider the subspaces $A := \langle a_1, \ldots, a_n \rangle$ and $B := \langle b_1, \ldots, b_n \rangle$. Then A and B are sub-Hopf algebras of H, and $B \cong A^{*\mathrm{cop}}$. Furthermore,

$$H_R := AB = BA$$

is a quasi-triangular sub-Hopf algebra. If $H = H_R$, the Hopf algebra H is called *minimal*. (This implies that H is finite dimensional!)

Proposition 8 (Radford 1993). *Let H be any finite dimensional Hopf algebra.*

(a) *The Drinfeld double $D(H)$ is minimal.*

(b) *Every minimal quasi-triangular Hopf algebra H is a quotient of a Drinfeld double.*

(c) *In (b), H is a Drinfeld double* $\Leftrightarrow \dim H = n^2$.

The first example of a minimal triangular semisimple Hopf algebra was found by Etingof and Gelaki in 1998. To give a description in terms of braces, we first observe:

Proposition 9. *Let A be any brace. As in Proposition 7, we set*

$$ {}^{a}b := a^{b} \cdot b. $$

Then the following equations hold in A:

$$ {}^{a\circ b}c = {}^{a}({}^{b}c) \qquad a^{b\circ c} = (a^{b})^{c} $$

$$ {}^{a}(b \circ c) = {}^{a}b \circ {}^{(a^{b})}c \qquad (a \circ b)^{c} = a^{({}^{b}c)} \circ b^{c}. $$

Let A be a finite brace. Proposition 9 states that the adjoint group A° operates on itself from the left and right, so that we have a matched product $G = A^{\circ} \bowtie A^{\circ}$ in the sense of Takeuchi. Write the elements of G as pairs (a, b). We define a triangular Hopf algebra $H(A)$ with basis G as follows.

The Hopf algebra $H(A)$ of a brace A:

Multiplication: $$(a,b)(c,d) = \begin{cases} (a, b\circ d) & \text{for } a^b = c \\ 0 & \text{otherwise.} \end{cases}$$

Comultiplication: $$\Delta(a,b) = \sum_{a=c\circ d} (c, {}^d b) \otimes (d,b)$$

Unit element: $$1 = \sum_{a\in A} (a,0)$$

Augmentation: $$\varepsilon(a,b) = \delta_{a,0}$$

Antipode: $$S(a,b) = \big((a\cdot b')\cdot a', a\cdot b'\big)$$

R-matrix: $$R = \sum_{a,b\in A} (a,b')\otimes(a\cdot b, a).$$

Proposition 10. *$H(A)$ is a minimal triangular semisimple Hopf algebra.*

The multiplication map

$$G := A^\circ \bowtie A^\circ \xrightarrow{m} A^\circ$$

has an abelian kernel

$$\operatorname{Ker} m = \{(a', a) \mid a\in A\}$$

isomorphic to the additive group of A. Therefore, G is a semidirect product

$$G = A^\circ \ltimes A$$

with abelian kernel.

8. Classification of cyclic braces

Of course, a classification of general braces is not feasible. There is a module theory over braces, and every brace is a (right) module over itself. (There are no left modules!) Every brace A admits a *radical series*

$$A \supset A^2 \supset A^3 \supset \cdots$$

where $A^{i+1} := A(A^i)$ is an *ideal* (defined as in ring theory), while the product of two ideals need not be an ideal. Even a finite brace need not be nilpotent!

Similarly, there is a socle series of ideals, where the *socle* of A is

$$\mathrm{Soc}(A) := \{x \in A \mid ax = 0,\ \forall\, a \in A\}.$$

Definition 9. We call a brace A *cyclic* if $(A, +)$ is cyclic.

Cyclic braces A are equivalent to *T-structures* on $\mathbb{Z}/n\mathbb{Z} = \mathrm{End}(A, +)$ in the sense of Etingof, Schedler, and Soloviev (Duke Math. J. 1999), i. e. permutations $T \in \mathrm{S}(\mathbb{Z}/n\mathbb{Z})$ which satisfy

$$T(ma) = mT^m(a),\ \forall\, a \in \mathbb{Z}/n\mathbb{Z},\ m \in \mathbb{Z}.$$

The T-structure of a cyclic brace A is given by

$$T(a) := a \cdot a.$$

Problem. At the end of their paper (1999), Etingof, Schedler, and Soloviev ask for a classification of T-structures on primary cyclic groups.

In other words: *classify primary cyclic braces!*

To solve this problem, we note first that for any cyclic brace $A = \mathbb{Z}/n\mathbb{Z}$, the operation $a \mapsto a^b$ can be written in the form

$$a^b = a\mu(b), \quad \text{(multiplication in the ring } \mathbb{Z}/n\mathbb{Z})$$

where $\mu\colon A \to A^\times$ is a *1-cycle*:

$$\mu(a)\mu(b) = \mu(a\mu(b) + b).$$

The kernel $\operatorname{Ker}\mu := \{a \in A \mid \mu(a) = 0\}$ coincides with the socle of A:

$$\operatorname{Ker}\mu = \operatorname{Soc}(A).$$

This leads to a commutative diagram

$$\begin{tikzcd}
A \arrow[r, "\mu"] \arrow[d, two heads, "q"] & A^\times \arrow[d, two heads, "q^\times"] \\
A/\operatorname{Soc}(A) \arrow[r, "\overline{\mu}"] \arrow[ur, hook, "\nu"] & (A/\operatorname{Soc}(A))^\times.
\end{tikzcd}$$

The *retraction* $B := A/\operatorname{Soc}(A)$ of A is *abelian*, i. e. its adjoint group B° is commutative.

Now we come back to radical rings.

Proposition 11. *Every abelian brace is a radical ring.*

Abelian cyclic braces admit an explicit description.

Theorem 1. *Let $n, d \in \mathbb{N}$ with $d|n$ be intergers with the same prime divisors. The 1-cycle*

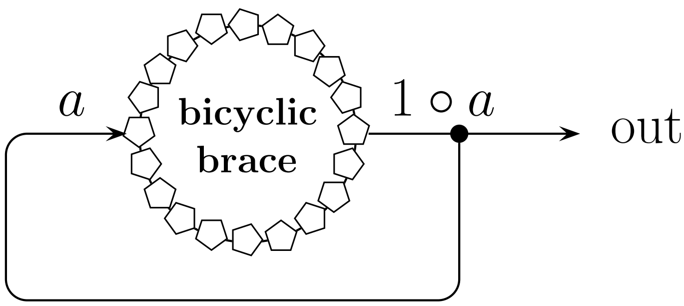
$$\mu(a) := 1 + ad$$

defines an abelian cyclic brace A with $|A| = n$ and $|\mathrm{Soc}(A)| = d$ (or $n = d = 0$ if A is infinite). Every abelian cyclic brace is of this form.

Let us now focus our attention to the primary case.

Proposition 12. *Let A be a cyclic brace with $|A| = p^m$ for an odd prime p. Then A is* bicyclic, *i. e. A° is cyclic.*

Bicyclic braces A produce random numbers: They are equivalent to *linear congruential generators* with full period $|A|$.



The sequence $(1^{\circ k})$ runs through all elements of A.

For example, if $n = 16$, and $|\mathrm{Soc}(A)| = 4$, this sequence looks as follows:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$1^{\circ k}$	0	1	6	15	12	13	2	11	8	9	14	7	4	5	10	3

It remains to consider the exceptional case: $p = 2$. Here the adjoint group A° has a cyclic subgroup of index 2. Such groups are well-known:

Proposition 13 (Hall, Zassenhaus). *Let G be a group of order 2^m with a cyclic subgroup of index 2. Then G belongs to exactly one of the following types.*

(1a) *G is cyclic.*

(1b) $G \cong C_2 \times C_{2^{m-1}}$ *with* $m \geqslant 2$ *(abelian, non-cyclic)*

(2a) $G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$ *with* $m \geqslant 3$ *(dihedral)*

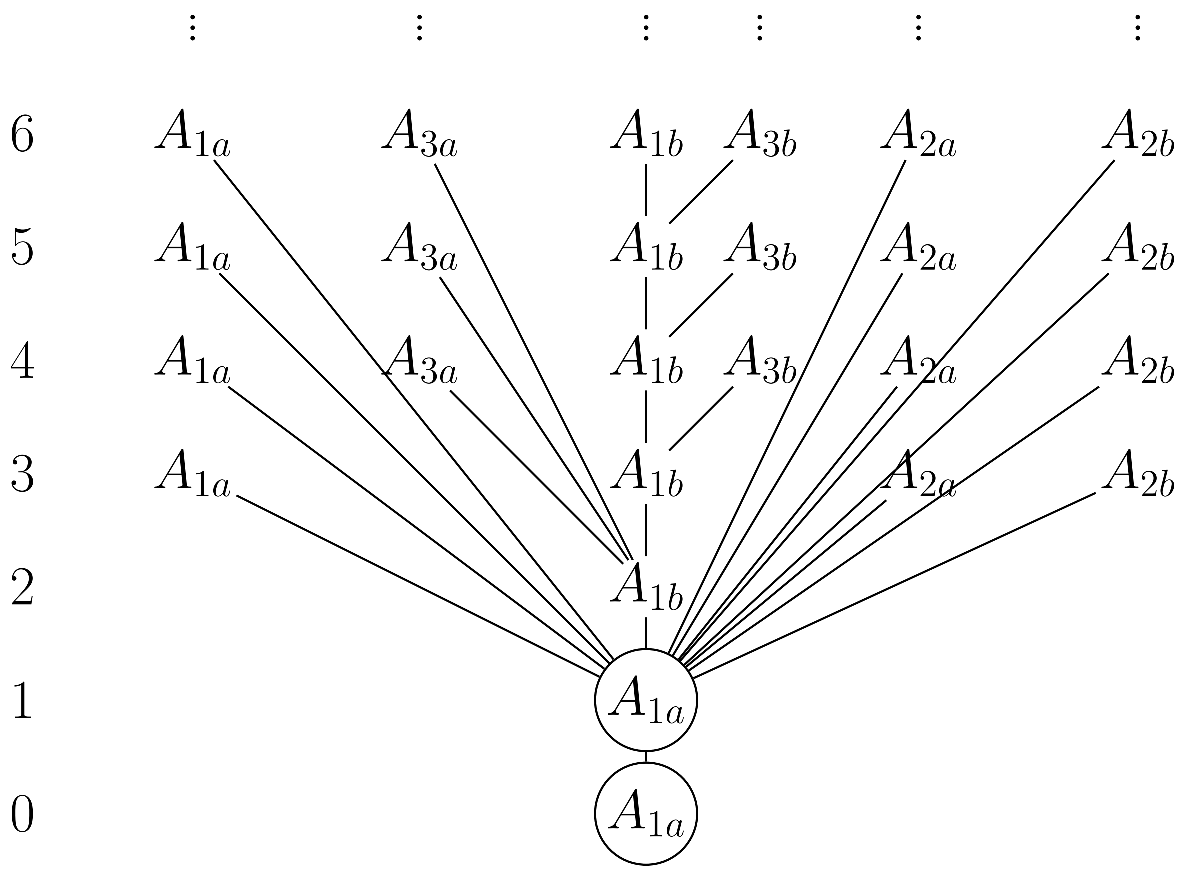
(2b) $G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = a^{2^{m-2}}, bab^{-1} = a^{-1} \rangle$ *with* $m \geqslant 3$ *(generalized quaternion)*

(3a) $G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, bab^{-1} = a^{-1+2^{m-2}} \rangle$ *with* $m \geqslant 4$

(3b) $G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, bab^{-1} = a^{1+2^{m-2}} \rangle$ *with* $m \geqslant 4$.

Using this classification, we obtain

Theorem 2. *Let A be a primary cyclic brace. If A is not bicyclic, then $|A| = 2^m$ with $m \geqslant 2$, and A° has a cyclic subgroup of index 2. Up to isomorphism, A is uniquely determined by A°. The isomorphism types of A form an infinite tree:*



The numbers m (left-hand side) refer to the size of each brace A, i. e. $|A| = 2^m$, while the subscript of A indicates the type of A°. The vertical axis consists of the abelian, non-bicyclic braces. In downward direction, each brace is connected to its retraction. Therefore, the whole tree is rooted in the zero brace.