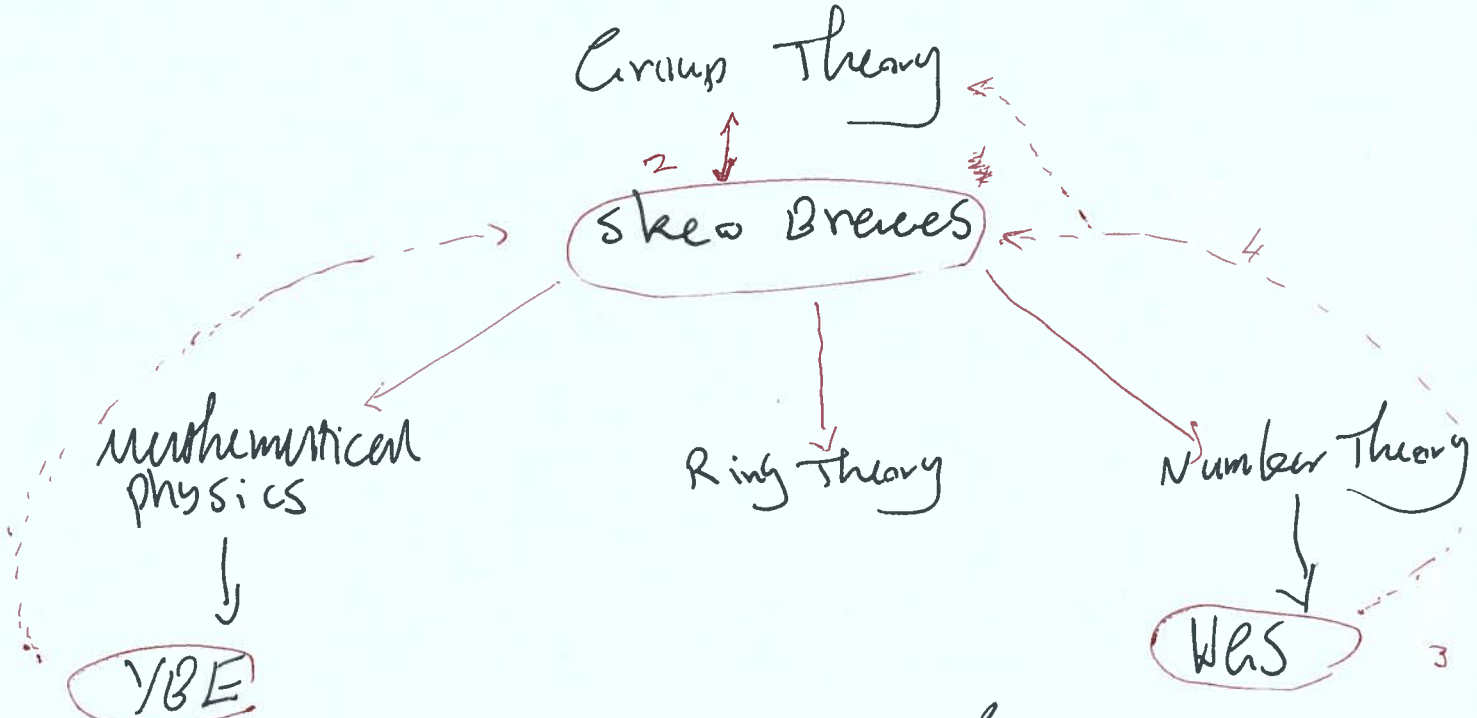
Hopf-Galois Theory and the Yang-Baxter Equation

1. Introduction.

In this ten hours seminar series I plan to give a short introduction to the Yang-Baxter equation (YBE) and Hopf-Galois structures (HGS) and how they came to be related via algebraic objects called skew braces. After this I will talk about some results relating to the classification of HGS and skew braces and the significance of these findings.

Skew braces are group theoretic objects. They can be with ten different and compatible group operations. It turns out that these objects are related to many other areas. In particular, they have connections to the following areas.



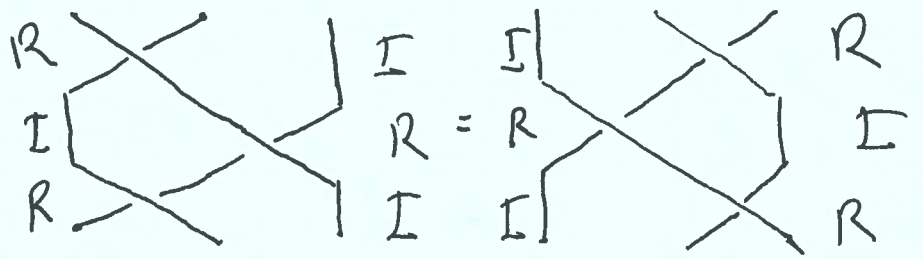
I start with YBE and show how skew braces can help solving the YBE. Then I will talk about HGS and show how they are related to skew braces

Finally I show some results relating to the classification of knots and skew braces.

1. <u>The Yang-Baxter Equation</u>. The YBE is a matrix equation for an element of $GL(V \otimes V)$, where V is a vector space. More precisely an element $R \in GL(V \otimes V)$ is said to satisfy the YBE if

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

This equation can be represented pictorially by



This equation was first introduced in mathematical physics and statistical mechanics by Yang and Baxter. It has since become one of the fundamental equations in quantum group theory, which has application in integrable systems, knot theory, and tensor categories.

Finding solutions of the YBE can be difficult, so in 1992 Drinfeld suggested studying the set-theoretic version of this equation.

Def 1. A set-theoretic solution of the Yang-Baxter equation is a pair (X,r) where X is a nonempty set and

$$r: X\times X \longrightarrow X\times X,$$
$$(x,y) \longmapsto (f_x(y), g_y(x))$$

is a bijective map such that

$$(r\times id)(id\times r)(r\times id) = (id\times r)(r\times id)(id\times r).$$

(X,r) is called non-degenerate if f_x and g_x are bijections and involutive if $r^2 = id$.

Example 1. Let X be a nonempty set.

- The map $r(x,y) = (y,x)$ makes (X,r) into a non-degenerate involutive solution
- Let $f,g: X\longrightarrow X$ be bijections with $fg=gf$. Then $r(x,y) = (f(y), g(x))$ is a non-degenerate solution which is involutive iff $f = g^{-1}$.
- If X is a group, then $r(x,y) = (y, y^{-1}xy)$ is a non-degenerate solution.

For a non-degenerate set-theoretic solution (X,r) one can define a group called the structure group of (X,r) by

$$G(X,r) = \langle X \mid xy = f_x(y)\, g_y(x) \text{ for all } x,y\in X\rangle.$$

which is one of the most important things studying (X,r). It is known that $G(X,r)$ is abelian-by-finite and the map $G(X,r)\longrightarrow \mathbb{Z}^X \rtimes \mathrm{Aut}(X)$ and the natural map $\iota: X\longrightarrow G(X,r)$ is not in general injective.

Question 1. How can we find more solutions of the Set-theoretic YBE? Skew braces provide non-degenerate set-theoretic solutions.

2. Skew Braces.

Def 2. A (left) skew brace is a set B together with two operations $\oplus$ and $\odot$ such that $(B,\oplus)$ and $(B,\odot)$ are groups, and the two operations are related by

$$a\odot(b\oplus c) = (a\odot b)\ominus a\oplus(a\odot c) \quad (*)$$

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

The group $(B,\oplus)$ is known as the additive, or type, of the skew brace $(B,\oplus,\odot)$ and $(B,\odot)$ as the multiplicative Group. If $(B,\oplus)$ is an abelian group we call $(B,\oplus,\odot)$ a brace.

Note, the compatibility condition $(*)$ looks like the distributivity condition for ring, but

$$a\odot 0 = a\odot(a\oplus 0) = (a\odot a)\ominus a\oplus(a\odot 0) \Rightarrow$$

$$a = a\odot a \Rightarrow 1 = 0.$$

Example 2. Let $(B,\oplus)$ be any group. Define

$a\odot b = a\oplus b$ then $(B,\oplus,\odot)$ is a skew brace.

Alternatively define $a\odot b = b\oplus a$. Again $(B,\oplus,\odot)$ is a skew brace.

For $n\geq 1$, let $(B,\oplus) = (\mathbb{Z}/p^n\mathbb{Z},+)$ and define

$$a\odot b = a+b+ab\,p^r \text{ for } r = 1,\dots,n.$$

Heit and YBE $(B, \oplus, \circ) \to a \circledast b = a \circ a \oplus a \circ b \oplus b$ paper 3
$(B, +, \cdot) \to a \circ b = a - ab - b$

History of skew braces. In 2007 Rump introduced braces as a generalisation of radical ring, and he obtained a correspondence between braces and non-degenerate involutive set-theoretic solutions of the YBE. Later the classification of these solutions was reduced to that of braces by Bachiller, Cedo, Jespers, and Okniński. Recently in article of Bachiller, Ced, Rump, and Vendramin introduced skew braces as a generalisation of braces. The connection of skew braces to ring theory and Hopf-Galois theory was studied by Bachiller, Byott, Smoktunowicz, and Vendramin (Konovalov). In particular, the classification of skew braces of a given order remains widly open and is an active area of research for example

-) 2007 Rump classified cyclic braces
-) 2015 Bachiller classified braces of order p^3
-) 2017 Acri and Bonatto computer assisted results and further generations
-) 2017-2018 NZ classified skew braces of order p^3
-) 2018 Dietzel studied braces of order p^2q.

Question: what is the correspondence between skew braces and the YBE?

Theorem 1 (Guarnieri-Vendramin 2017). Let $(B, \oplus, \circ)$ be a skew brace. Then the map

$$r_B : B \times B \longrightarrow B \times B$$
$$(a,b) \longmapsto (\ominus a \oplus (a \circ b), (\ominus a \oplus a \circ b)^{-1} \circ a \circ b)$$

is a non-degenerate set-theoretic solution of the YBE, which is involutive if and only if $(B, \oplus)$ is abelian.

Conversely, for every non-degenerate set-theoretic solution of YBE (X, r) the structure group $G = G(X,r)$ can be given a unique skew brace structure such that

$$\begin{array}{ccc} X \times X & \xrightarrow{r} & X \times X \\ \downarrow \lambda_G \times \lambda_G & & \downarrow \lambda_G \times \lambda_G \\ G \times G & \xrightarrow{r_G} & G \times G \end{array}$$

in a universal way i.e. if B is a skew brace and $f : X \longrightarrow B$ is a map with

$$\begin{array}{ccc} X \times X & \xrightarrow{r} & X \times X \\ \downarrow f \times f & & \downarrow f \times f \\ B \times B & \xrightarrow{r_B} & B \times B \end{array}$$

then there exists a unique map $\phi : G \longrightarrow B$ with

$$\begin{array}{ccc} X & \xrightarrow{\lambda_G} & G \\ & \searrow^{f} & \downarrow \phi \\ & & B \end{array} \quad \text{and} \quad \begin{array}{ccc} G \times G & \xrightarrow{r_G} & G \times G \\ \downarrow \phi \times \phi & & \downarrow \phi \times \phi \\ B \times B & \xrightarrow{r_B} & B \times B \end{array}.$$

3. Hopf-Galois theory. There are two main aims in Hopf-Galois theory. Initially it was developed to introduced Galois theory for inseperable extensions of fields. Later it was adapted to study rings of integers of extensions of local or global fields. I will mainly be concerned with the latter usage. Let's look at a motivating question. Suppose L/k is a Galois extension of number fields, or p-adic fields for a prime p, with Galois group G, and denote by $\mathcal{O}_L$ and $\mathcal{O}_k$ the rings of integers of $\mathcal{O}_L$ and $\mathcal{O}_k$, respectively. The normal basis theorem tells us that L is a free $k[G]$-module of rank 1.

Now, $\mathcal{O}_k[G]$ acts on $\mathcal{O}_L$, so we can ask if $\mathcal{O}_L$ is a free module over $\mathcal{O}_k[G]$.

This is not in general true, sometimes $\mathcal{O}_k[G]$ is too small. We can define the associated order of $\mathcal{O}_L$ in $k[G]$ by

$$A_{k[G]} = \{\alpha \in k[G] \mid \alpha(\mathcal{O}_L) \subseteq \mathcal{O}_L\}.$$

Is $\mathcal{O}_L$ free over $A_{k[G]}$? Can we replace $k[G]$ with any other k-algebra?

Byott 1996 If $|G| = n$, then there are other options for $k[G]$ if and only if $\gcd(n, \varphi(n)) \neq 1$: in this case there can more than one 'Hopf-Galois structure on L/k'.

Hopf-Galois structures. Let L/k be a Galois extension with Galois group G. Hopf-Galois structures on L/k are analogous to $K[G]$: They are K-Hopf algebras which act on L satisfying a certain property.

We can define these in a general setting. Let K be a commutative ring with a unit.

Recall an K-Hopf algebra H is an K-module which is both an algebra and a coalgebra over K such that the comultiplication and the counit maps

$$\Delta : H \longrightarrow H \otimes H \quad \text{and} \quad \varepsilon : H \longrightarrow K$$

are homomorphisms of algebras; the multiplication and the unit maps

$$\mu : H \otimes H \longrightarrow H \quad \text{and} \quad \iota : K \longrightarrow H$$

are homomorphisms of coalgebras, and there exists an antipode map $\lambda : H \longrightarrow H$ with

$$\mu(id \otimes \lambda)\Delta = \mu(\lambda \otimes id)\Delta = \iota\varepsilon.$$

H is called commutative if $\mu\tau = \mu$ and cocommutative if $\tau\Delta = \Delta$ where $\tau(x \otimes y) = y \otimes x$.

Example: The group algebra $K[G]$ for any group G with

$$\Delta(g) = g \otimes g$$
$$\varepsilon(g) = 1$$
$$\lambda(g) = g^{-1} \quad \text{for } g \in G$$

is an K-Hopf algebra, which is cocommutative.

Hes and YBE

S/R is eclois for $G \subseteq \mathrm{Aut}_R(S)$ if $O(S,G) \to \mathrm{End}_R(S)$

Def 3. Let H be a finite (finitely generated and projective as a module) cocommutative Hopf algebra. A finite commutative R-algebra S is an H-eclois extension of R, or H endows S/R with a Hopf-eclois structure if S is a left H-module algebra, and the R-module homomorphism

$$j : S \otimes_R H \longrightarrow \mathrm{End}_R(S)$$
$$s \otimes h \longmapsto (t \longmapsto sh(t))$$

is an isomorphism. ($\Rightarrow$ S is a locally free rank one H-module.)

Example 4. For the eclois extension L/K, the K-Hopf algebra $K[G]$ with its natural action on L endows L/K with the classical Hopf-eclois structure.

Now suppose L/K is an extension of number fields or p-adic fields, and H endows L/K with a Hopf-eclois structure. Define the associated order of O_L in H by

$$A_H = \{ \alpha \in H \mid \alpha(O_L) \subseteq O_L \}$$

are an investigate the freeness of O_L as a module over A_H.

Question 3. How can we find all Hes on L/K?

Through the works of Greither and Pareigis 1987 and Byott 1996 the classification of Hes was reduced

to the classification of regular subgroups of holomorphs

Theorem 2 (Greither–Pareigis 1987). Hopf–Galois structures on L/k correspond bijectively to the regular subgroups of $\mathrm{Perm}(G)$ which are normalised by the image of G, as left translations, inside $\mathrm{Perm}(G)$.

They showed that every k-Hopf algebra which endows L/k with a Hopf–Galois structure is of the form $L[N]^G$ for some regular subgroup $N \subset \mathrm{Perm}(G)$ normalised by G.

The isomorphism type of N is known as the type of the Hopf–Galois structure.

Problem 1. The group $\mathrm{Perm}(G)$ can be large.

Instead of working with $\mathrm{Perm}(G)$ we can work with

$$\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N).$$

Theorem 3 (Byott 1996). Let G and N be groups.

There exists a bijection between the sets

$$\mathcal{N} = \{\alpha : N \hookrightarrow \mathrm{Perm}(G) \mid \alpha(N) \text{ is regular normalised by } G\}$$

$$\mathcal{G} = \{\beta : G \hookrightarrow \mathrm{Hol}(N) \mid \beta(G) \text{ is regular}\}.$$

In particular if $\alpha, \alpha' \in \mathcal{N}$ correspond to $\beta, \beta' \in \mathcal{G}$, then $\alpha(N) = \alpha'(N)$ if and only if $\beta(G)$ and $\beta'(G)$ are conjugate by an element of $\mathrm{Aut}(N)$.

It follows that if $e(G,N)$ denotes the number of HES on L/K of type N, then we have

$$e(G,N) = \frac{|Aut(G)|}{|Aut(N)|} e'(G,N),$$

where $e'(G,N)$ is the number of regular subgroups of $Hol(N)$ isomorphic to G.

Remark 1. Byott in 1999 found cases where $\mathcal{O}_L$ can be free over $\mathcal{A}_N$ for a non-classical Hopf-Galois structure on L/K but not free over $\mathcal{A}_{K[G]}$.

Question 4. How are HES are related to skew braces? It turns out skew braces preserve HES; in particular we have

$$\left\{\begin{array}{l}\text{isomorphism classes of}\\ \text{skew braces}\\ \text{with } (B,\circ)\cong G\end{array}\right\} \overset{\text{bij}}{\longleftrightarrow} \left\{\begin{array}{l}\text{classes of regular subgroups}\\ \text{of } Perm(G), \text{ which are}\\ \text{normalised by } G, \text{ under}\\ \text{conjugation by } Aut(G)\end{array}\right\}$$

I will explain this in the next hour.

HGS and YBE

In this second hour I would like to talk about how skew braces are related to Hopf-Galois structures. I will then talk about one of the ways for classifying them. Finally, I will results relating to the classification of skew braces and HGS of order p^3 for a prime p, and talk about the significance of these findings.

0. Recap. Recall a skew brace is a triple $(B, \oplus, \odot)$ such that $(B, \oplus)$ and $(B, \odot)$ are groups and for all $a, b, c \in B$ we have $a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c)$. These provide solutions of the Yang-Baxter equation.

. For a field extension L/K with Galois group G a Hopf Galois structure on L/K is a K-Hopf algebra which acts in a certain manner on L.

. Greither and Pareigis $\xrightarrow{\text{HGS}}$ all are of the form $L[N]^G$ for $N \subset \mathrm{Perm}(G)$ a regular subgroup normalised by $\lambda(G)$.

. Byott $\longrightarrow$ $\#(\text{HGS on } L/K \text{ of type } N) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} \#(\text{regular subgroups of } \mathrm{Hol}(N))$,

Notation: For a skew brace $(B, \oplus, \odot)$ if $(B, \odot) \cong G$ and $(B, \oplus) = N$, we call $(B, \oplus, \odot)$ a G-skew brace of type N.

1. Skew braces and HGS. Let $(B, \oplus, \odot)$ be a skew brace we can produce a HGS on a field extension L/K with Galois group $(B, \odot)$ as follows. The group $(B, \oplus)$ acts on $(B, \odot)$ by $(a, b) \longmapsto a \oplus b$. This gives a homomorphism

$$\delta : (B, \oplus) \longrightarrow \mathrm{Perm}(B, \odot)$$
$$a \longmapsto (\delta_a : b \longmapsto a \oplus b).$$

$\mathrm{Im}\, \delta$ is a regular subgroup. Now for any $a, b, c \in G$ we have $b \delta_a b^{-1}(c) = b \ominus (a \oplus (b^{-1} \ominus c)) = (b \odot a) \ominus b \odot c$ so $b \delta_a b^{-1} = \delta_{(b \odot a) \ominus b}$ which implies that $\mathrm{Im}\, \delta$ is normalised by the left translations and gives an action of $(B, \odot)$ on $(B, \oplus)$ by $a \cdot b = (a \odot b) \ominus a$.

Fix L/K with Galois group $(B, \odot)$. Using Greither and Pareigis' theorem we obtain that $L[\mathrm{Im}\, \delta]^{(B, \odot)}$ endows L/K with a Hopf-Galois structure of type $(B, \oplus)$.

Conversely, suppose $H = L[N]^{(B, \odot)}$ endows L/K with a Hopf-Galois structure, then $N \subseteq \mathrm{Perm}\,(B, \odot)$ is a regular subgroup normalised by the left translations. In this case we have a bijection

$$\phi : N \longrightarrow (B, \odot)$$
$$n \longmapsto n.1,$$

so define $\oplus$ on B by

$$a \oplus b = \phi(\phi^{-1}(a)\, \phi^{-1}(b)),$$

this gives a group $(B, \oplus) \cong N$, and since N is normalised by the left translations, we find that $(B, \oplus, \odot)$ is a $(B, \odot)$-skew brace of type N.

Moreover, if $f : (B, \oplus_1, \odot) \longrightarrow (B, \oplus_2, \odot)$ is an isomorphism of skew braces, then we have the following commutative diagram.

$$\begin{array}{ccc} (B,\oplus_1) & \xrightarrow{\lambda_1} & \mathrm{Perm}(B,\circ) \\ f \downarrow & \square & \downarrow Cf \\ (B,\oplus_2) & \xrightarrow{\lambda_2} & \mathrm{Perm}(B,\circ) \end{array} \qquad \text{i.e., } f\lambda_1 f^{-1} = \lambda_2 f.$$

Similarly, if $N_1, N_2 \subset \mathrm{Perm}(B)$ are regular subgroups normalized by $\lambda_B(B,\circ)$ and $N_1 = fN_2f^{-1}$ for some $f \in \mathrm{Aut}(B,\circ)$ then $(B,\circ)$-skew braces corresponding N_1 and N_2 are isomorphic. This gives a bijective correspondence

$$\left\{\begin{array}{l}\text{isomorphism classes}\\ \text{of skew braces with}\\ \text{multiplicative group } G\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{classes of HLS on } L[N]\\ \text{under } L[N_1]^G \sim L[N_2]^G\\ \text{if } N_1 = fNf^{-1} \text{ for some}\\ f \in \mathrm{Aut}(G)\end{array}\right\}$$

i.e. given a G-skew brace of type N then we get the following HLS $\underset{(B,\oplus,\circ)}{}$

$$\left\{ L[\alpha \,\mathrm{Im}\,\lambda\, \alpha^{-1}]^{(B,\circ)} \;\middle|\; \alpha \in \mathrm{Aut}(B,\circ) \right\}$$

$$= \left\{ L[\alpha N \alpha^{-1}]^G \;\middle|\; \alpha \in \mathrm{Aut}(G) \right\}.$$

Automorphism group of skew braces. If $f:(B,\oplus,\circ) \to (B,\oplus,\circ)$ is an automorphism, i.e. $f \in \mathrm{Aut}(B,\oplus)$ and $f \in \mathrm{Aut}(B,\circ)$, then we have $f\,\mathrm{Im}\,\lambda f^{-1} = \mathrm{Im}\,\lambda$, so f normalizes $\mathrm{Im}\,\lambda$. (Conversely if an automorphism of $(B,\circ)$ normalizes $\mathrm{Im}\,\lambda$, it gives an automorphism of $(B,\oplus,\circ)$.

In particular, we find

$$Aut_{Br}(B,\oplus,\circ) \cong \{f \in Aut(B,\circ) \mid f \circ Im\, d \circ f^{-1} = Im\, d\}$$

2. Classification of skew braces and YBEs. Let G and N be finite groups.

Theoretical: Let

$$\mathcal{S}(G,N) = \{N \leq perm(G) \mid N \text{ is regular and normalised by left translations}\}$$

Denote by B_G^N the isomorphism class of a G-skew brace $(B,\oplus,\circ)$ of type N. The group $Aut(G)$ acts on $\mathcal{S}(G,N)$ via conjugation inside $perm(G)$ and a set of orbit representatives, say $\{N_1, \dots, N_s\}$, gives a list of non-isomorphic G-skew braces.

For YBEs we [illegible] have $e(G,N)$ as $|\mathcal{S}(G,N)|$, so we have

$$e(G,N) = \sum_{i=1}^{s} |Orb(N_i)| = \sum_{i=1}^{s} \frac{|Aut(G)|}{|Stab(N_i)|} = \sum_{B_G^N} \frac{|Aut(G)|}{|Aut_{Br}(B_G^N)|}$$

This gives the number of YBEs as parametrised by skew braces.

Again in practice we should like to work with holomorphs rather than the permutation groups. This is easily done by working with the action of $(B,\circ)$ on $(B,\oplus)$ by $(a,b) \mapsto a \circ b$, instead of the action of $(B,\oplus)$ on $(B,\oplus)$.

Recall YBE

For a skew brace $(B, \oplus, \cdot)$ we have an action of $(B, \cdot)$ on $(B, \oplus)$ by $(a, b) \mapsto a \cdot b$.

This gives a map

$$m : (B, \cdot) \longrightarrow \mathrm{Hol}(B, \oplus) = (B, \oplus) \rtimes \mathrm{Aut}(B, \oplus)$$
$$a \longmapsto (m_a : b \mapsto a \cdot b)$$

To see this it suffices to check that the map

$$\lambda_a : (B, \oplus) \longrightarrow (B, \oplus)$$
$$b \longmapsto \ominus a \oplus (a \cdot b)$$

is an automorphism for each $a \in B$, and that the map

$$\lambda : (B, \cdot) \longrightarrow \mathrm{Aut}(B, \oplus)$$
$$a \longmapsto \lambda_a : b \mapsto \ominus a \oplus (a \cdot b)$$

is a group homomorphism. Then $m = \lambda \cdot$ Furthermore, $\mathrm{Im}\, m$ is a regular subgroup. Conversely, if $G \subset \mathrm{Hol}(B, \oplus)$ is a regular subgroup. Then define $\cdot$ operation on $(B, \oplus)$ to be the push forward of the operation of G. Also isomorphic braces with additive group $(B, \oplus)$ give rise to conjugate subgroups of $\mathrm{Hol}(B, \oplus)$ by elements of $\mathrm{Aut}(B, \oplus)$. This gives us a bijective correspondence

$$\left\{\begin{array}{l}\text{isomorphism classes}\\ \text{of skew braces with}\\ \text{additive group } N\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{classes of regular}\\ \text{subgroups of } \mathrm{Hol}(N)\\ \text{under conjugation by}\\ \text{elements of } \mathrm{Aut}(N)\end{array}\right\}$$

In particular, we find another identification

$$\mathrm{Aut}_{Br}(B,\oplus,\odot) \cong \{\alpha \in \mathrm{Aut}(B,\oplus) \mid \alpha \circ m \circ \alpha^{-1} = m\}$$

Therefore, to find the skew braces of type N, it suffices to classify

$$S(G,N) = \{G \subseteq \mathrm{Hol}(N) \mid G \text{ is regular}\}$$

and moreover a maximal subset $\tilde{S}(G,N)$ whose elements are not conjugate by any element of $\mathrm{Aut}(N)$.

To find the G_i's find for each $G_i \in \tilde{S}(G,N) = \{G_1, \dots, G_s\}$

$$\mathrm{Stab}(G_i) = \{\alpha \in \mathrm{Aut}(N) \mid \alpha G_i \alpha^{-1} = G_i\}$$

Then as before we have

$$e(G,N) = \sum_{G_i} \frac{|\mathrm{Aut}(G_i)|}{|\mathrm{Stab}(G_i)|}.$$

The classification of skew braces and RCS is an active area of research

Hess and YBE

For skew braces as in mentioned

Rump $\xrightarrow{2007}$ cyclic braces

Bachiller $\xrightarrow{2015}$ braces of order p^3

Cedo-Jespers-Okninski $\xrightarrow{2017}$ computer assisted results

NZ $\xrightarrow{2018}$ skew braces of order p^3

Cedo et al. $\xrightarrow{2018}$ skew braces with non-trivial annihilator

Dietzel $\xrightarrow{2018}$ braces of order p^2q.

For Hopf-Galois structures

Byott $\xrightarrow{1996}$ if $|G|=n$, then there exists a unique Hopf-Galois structure if and only if $\gcd(n, \phi(n)) = 1$

Kohl $\xrightarrow{1998}$ Hess for $G = G_{pn}$ for $n > 2$.

Byott $\xrightarrow{96,04}$ $|G| = p^2$, pq and when G is a [redacted] nonabelian simple group.

Carnahan and childs $\xrightarrow{99,05}$ $G = G_p^n$ and S_n

Byott $\xrightarrow{2007}$ $G = G_{2^n}$

Alabadi and Byott $\xrightarrow{2017}$ $|G|$ is squarefree

NZ $\xrightarrow{2018}$ $|G| = p^3$ for a prime p

Nigel's new student Lenge working on G = cyclic.

3. Main results. A summary of main results on classification of Hess and skew braces of order p^3 for a prime $p > 3$. Let G and N be groups of order p^3.

Theorem 4. The number of G-skew braces of type N is given by the table below

$\tilde{e}(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	$C_p^2 \rtimes C_p$	$C_{p^2} \rtimes C_p$
C_{p^3}	3	—	—	—	—
$C_{p^2} \times C_p$	—	5	—	—	$4p+1$
C_p^3	—	—	9	$2p+1$	—
$C_p^2 \rtimes C_p$	—	—	$2p+1$	$2p^2-p-3$	—
$C_{p^2} \rtimes C_p$	—	$4p+1$	—	—	$4p^2-3p-1$

Let L/K be a Galois extension with Galois group G.

Theorem 5. The number of braces on L/K of type N is given by the table below.

$e'(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	$C_p^2 \rtimes C_p$	$C_{p^2} \rtimes C_p$
C_{p^3}	p^2	—	—	—	—
$C_{p^2} \times C_p$	—	$(2p-1)p^2$	—	—	$(2p-1)(p-1)p^2$
C_p^3	—	—	$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	—
$C_p^2 \rtimes C_p$	—	—	$(p^3+p-1)p^2$	$(2p^3-3p^2+1)p^2$	—
$C_{p^2} \rtimes C_p$	—	$(2p-1)p^2$	—	—	$(2p-1)(p-1)p^2$

4. Strategy for the proof.

There are five groups of order p^3.

1. Study $\mathrm{Aut}(N)$ for each N.

$$\mathrm{Aut}(C_{p^3}) \cong C_{p^2} \times C_{p-1}$$

$$1 \to C_p^2 \to \mathrm{Aut}(C_{p^2} \times C_p) \to L(\mathbb{F}_p) \to 1$$

$$\mathrm{Aut}(C_p^3) \cong GL_3(\mathbb{F}_p)$$

$$1 \to C_p^2 \to \mathrm{Aut}(C_p^2 \times C_p) \to GL_2(\mathbb{F}_p) \to 1$$

$$1 \to C_p^2 \to \mathrm{Aut}(C_{p^2} \times C_p) \to L_1(\mathbb{F}_p) \to 1$$

where $L(\mathbb{F}_p) = \left\{ A \in GL_2(\mathbb{F}_p) \mid A = \begin{pmatrix} a_1 & 0 \\ a_2 & a_4 \end{pmatrix} \right\}$

$$L_1(\mathbb{F}_p) = \left\{ A \in GL_2(\mathbb{F}_p) \mid A = \begin{pmatrix} a_1 & 0 \\ a_3 & 1 \end{pmatrix} \right\}$$

2. Classify regular subgroups of $\mathrm{Hol}(N)$ for each N.

Organise the regular subgroups according to the size of their image under

$$\theta : \mathrm{Hol}(N) \to \mathrm{Aut}(N)$$
$$\eta(\lambda) \mapsto \lambda .$$

For each prime m with $m \mid |N|$ find all regular subgroups with $|\theta(H)| = m$.

To do this take subgroups of order m of $Aut(N)$ say

$$H_2 = \langle \alpha_1, \dots \alpha_s \rangle \subseteq Aut(N),$$

take subgroups of order $|N|/m$ of N, say

$$H_1 = \langle \eta_1, \dots \eta_r \rangle \subseteq N,$$

take general elements $\nu_1, \dots \nu_s \in N$. Then consider a subgroup $U = \langle \eta_1, \dots \eta_r \nu_1 \alpha_1, \dots \nu_s \alpha_s \rangle$. Search for ν_i so that H is regular, i.e. it has the same size as N and acts freely on N.

For H to have the same size as N we need that for every relation $R(\alpha_1, \dots \alpha_s) = 1$ in H_2 to have

$$R(u_1(\nu_1\alpha_1)w_1, \dots, u_s(\nu_s\alpha_s)w_s) \in H_1$$

for all $u_i, w_i \in H_1$. For H to act freely on N we need for every word $w(\alpha_1, \dots \alpha_s)$ in H_2 to have

$$w(u_1(\nu_1\alpha_1)w_1, \dots u_s(\nu_s\alpha_s)w_s)\, w(\alpha_1, \dots \alpha_s)^{-1} \notin H_1$$

Finally also need to check if some elements of H generate a group of order $|N|$.

3. If $H = \langle \eta_1, \dots, \eta_r, \nu_1\alpha_1, \dots, \nu_s\alpha_s \rangle \subset \mathrm{Hol}(N)$ is a regular subgroup, study its orbit and stabiliser under conjugation by elements of $\mathrm{Aut}(N)$.

Examples. Let $p > 2$, $n > 1$, and $C_{p^n} = \langle 6 \mid 6^{p^n} = 1 \rangle$. Then we know $\mathrm{Hol}(C_{p^n}) = \langle 6 \rangle \rtimes \langle \beta, \gamma \rangle$, with $\beta(6) = 6^{p+1}$. Skew braces are given by

$$\langle 6 \rangle, \langle 6\beta \rangle, \dots, \langle 6\beta^{p^{n-2}} \rangle$$

and $\mathrm{Aut}_{Br}(\langle 6\beta^{p^m} \rangle) = \langle \beta^{p^{n-m-2}} \rangle$ for $m = 0, \dots, n-2$.

$e(e, N) =$ ~~$p^n \cdot \frac{1}{p^n}$~~

$$p^{n-1}(p-1)\left(\frac{1}{p^{n-1}(p-1)} + \frac{1}{p^{n-1}} + \frac{1}{p^{n-2}} + \dots + \frac{1}{p} \right)$$

$$= 1 + (p-1) + \dots + p^{n-2}(p-1) = 1 + (p-1)\left(\frac{1-p^{n-1}}{1-p} \right)$$

$$= p^{n-1}.$$

5. Scopes for the results.

1. Recall for a skew brace $(B, \oplus, \odot)$ the map

$$r_B : B \times B \longrightarrow B \times B$$
$$(a, b) \longmapsto (\lambda_a(b), \lambda_a(b)^{-1} \odot a \odot b)$$

is a non-degenerate set-theoretic solution of the YBE.

Study the structure of

$$e(B,r) = \langle B \mid ab = \lambda_a(b)\, \lambda^a(b) \odot a \odot b \rangle$$

for these skew braces.

2. To what extend the pattern

$$e(a,N) = e(N,a) \text{ hold?}$$

Does it hold when N [illegible] for N [illegible] is an extension of two groups?

3. Study the invariants of Hopf-cubic structures corresponding to a skew brace.

4. What can be said about group of the form

$$(C_{pe} \times C_f) \rtimes C_{pg}\,?$$