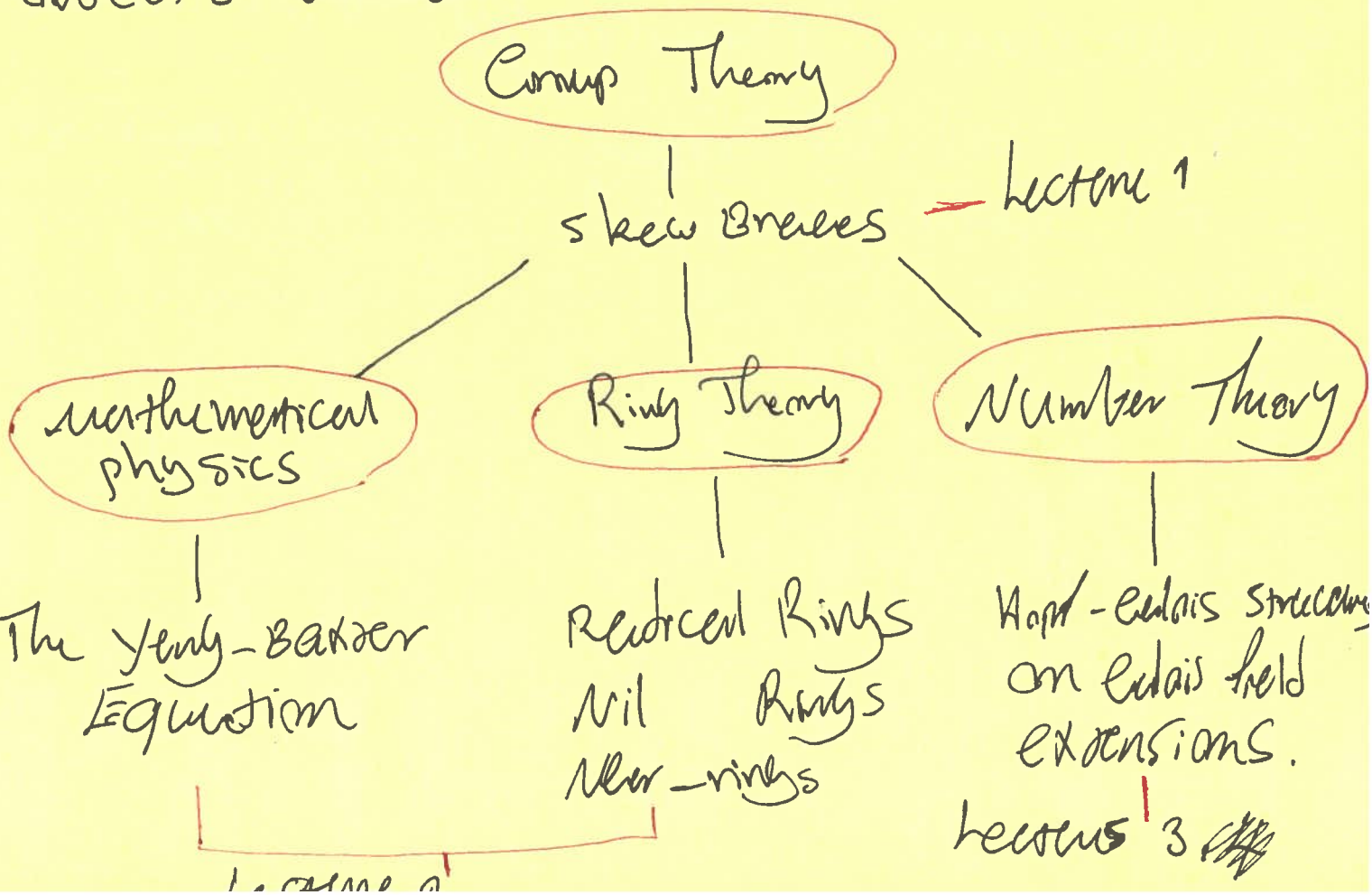
Skew Brieces, The Yang-Baxter Equation, Rings, and Hopf-Galois Structures.

The main aim of these lecture series is to give a good introduction to the theory of skew braces, their applications, and connections to other areas of mathematics in part I and in part II to talk about some specific results relating to the classification of skew braces.

Skew braces are sets which become groups under two different operations that satisfy certain compatibility condition. They are group theoretic objects connected to many other areas.



Hence study skew braces offer problems in group theory, mathematical physics, ring theory and number theory.

Historical braces were introduced by W. Rump in 2007 as a generalisation of radical rings ~~[illegible]~~, and ~~[illegible]~~ as a tool to study the Yang-Baxter equation. Later braces were generalised to skew braces and their connections to other areas of mathematics was discovered.

In this session I would like to give a solid group theoretic introduction to skew braces. In the subsequent lectures I will mention applications and connections of skew braces to other areas.

<u>Def 1.</u> A <u>(left) skew brace</u> is a set B together with two operations $\oplus$ and $\odot$ such that $(B,\oplus)$ and $(B,\odot)$ are groups (we do not assume $\oplus$ or $\odot$ are commutative) but the two operations are compatible by

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

we write $(B,\oplus,\odot)$ or just B.

We call $(B,\oplus)$ the additive group of the skew brace and $(B,\odot)$ the multiplicative group of B. We also denote by 0 the identity of $(B,\oplus)$ and 1 the identity of $(B,\odot)$. We call B a cla[illegible] brace if $(B,\oplus)$ is [illegible]

Skew Braces

So skew braces are algebraic objects with more structure than groups, but not rings, but this is where the name 'brace' came from. Let us investigate some properties of skew braces.

Lemma 1. Let $(B, \oplus, \cdot)$ be a skew brace. The following holds.

i) We have $0 = 1$.

ii) We have $\ominus(a \cdot b) = \ominus a \oplus (a \cdot (\ominus b)) \ominus a$.

Proof. i) $a \cdot 0 = a \cdot (a \oplus 0) = a \cdot a \ominus a \oplus (a \cdot 0)$

$\Rightarrow \quad 0 = \ominus a \oplus (a \cdot 0) \Rightarrow a = a \cdot 0 \Rightarrow 1 = 0.$

ii) $a = a \cdot 0 = a \cdot (b \ominus b) = (a \cdot b) \ominus a \oplus (a \cdot (\ominus b))$

$\Rightarrow -(a \cdot b) = \ominus a \ominus (a \cdot (\ominus b)) \ominus a$. $\square$

A map between two skew brace $\varphi : (B_1, \ominus_1, \cdot_1) \to (B_2, \ominus_2, \cdot_2)$ is a map of set which respects the addition and multiplication structures. We define

$$\ker \varphi = \{ a \in B_1 \mid \varphi(a) = 1 \}$$

$$\text{Im } \varphi = \{ \varphi(a) \mid a \in B_1 \}$$

A subbrace of a skew brace B is a subset $A \subset B$, such that $A \hookrightarrow B$ is a map of skew braces.

One can similarly define quantum skew braces.

Note we see that

$$\mathrm{Hom}_{Br}(B_1, B_2) \hookrightarrow \mathrm{Hom}^{\oplus}_{Gr}(B_1, B_2)$$
$$\mathrm{Hom}_{Br}(B_1, B_2) \hookrightarrow \mathrm{Hom}^{\Delta}_{Gr}(B_1, B_2)$$

Let us look at some examples of skew braces.

E.g. 1) Let $(B, \oplus)$ be any group. Define $a \odot b = e \oplus b$ for any $a, b \in B$. Then

$$a \odot (b \oplus c) = a \oplus b \ominus e \oplus c = a \oplus b \ominus a \ominus e \oplus c$$
$$= (a \ominus b) \ominus a \oplus a \odot c.$$

This is called the trivial skew brace structure on $(B, \oplus)$.

- One can also define on $(B, \oplus)$ $a \odot b = b \oplus a$. Then $(B, \oplus, \odot)$ is also a skew brace.

- Let $(B, \oplus) = (\mathbb{Z}/p^n\mathbb{Z}, +)$. Define for $r = 1, \dots, n$ $a \odot b = a + b + ab p^r$. Then

$$a \odot (b \oplus c) = a + b + c + a(b + c)p^r$$
$$= a + b - a + a + c + abp^r + acp^r$$
$$= (a \odot b) \ominus a \oplus (a \odot c).$$

Skew Braces

Let's look at more group-theoretic properties of skew braces. We shall recall some definitions first. For a group N we denote by $\mathrm{Aut}(N)$ the group of all automorphisms of N under composition. For an element $\eta \in N$ and $\alpha \in \mathrm{Aut}(N)$ we write

$$\eta^{\alpha} = \alpha(\eta).$$

The holomorph of N is defined as

$$\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) = \{\eta\alpha \mid \eta \in N, \alpha \in \mathrm{Aut}(N)\}$$

under the multiplication rule

$$(\eta\alpha)(\gamma\beta) = \eta\gamma^{\alpha}\alpha\beta.$$

The permutation group of N, $\mathrm{Perm}(N)$ is defined as the group of all bijections from N to itself.

Fact 1. We have $N \subset \mathrm{Perm}(N)$ as left translations and $\mathrm{Hol}(N) \subset \mathrm{Perm}(N)$ can be identified with the normaliser of N.

A subgroup $G \subset \mathrm{Perm}(N)$ is called regular if the map

$$G \times N \longrightarrow N \times N$$
$$(f, \eta) \longmapsto (f(\eta), \eta)$$

is a bijection.

The multiplicative group of
We shall shortly show that every skew brace
can be embedded canonically inside the holomorph
of its additive group.

Let $(B, \oplus, \cdot)$ be a skew brace. For any $a \in B$
define a map

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

Lemma 2. The following holds.

i) We have $\lambda_a \in Aut(B, \oplus)$ for all $a \in B$.

ii) The map $\lambda : (B, \cdot) \longrightarrow Aut(B, \oplus)$
$$a \longmapsto \lambda_a$$
is a group homomorphism.

Proof. i) Need to show λ_a is invertible, surjective, and
a group homomorphism for every $a \in B$. Let $a \in B$.
Suppose $\lambda_a(b) = 1$. Then

$$\ominus a \oplus (a \cdot b) = 1 = 0 \qquad \text{by Lemma 1. i)}$$
$$\Rightarrow a \cdot b = a \Rightarrow b = 1$$

Let $x \in B$. Then $\lambda_a(a^{-1} \cdot (a \oplus x))$

$$= \ominus a \oplus (a \cdot a^{-1} \cdot (a \oplus x)) = x.$$

Let $b, c \in B$. Then $\lambda_a(b \oplus c)$

$$= \ominus a \oplus (a \cdot (b \oplus c)) = \ominus a \oplus (a \cdot b) \oplus a \oplus (a \cdot c)$$
$$= \lambda_a(b) \oplus \lambda_a(c).$$

ii) Let $a, b \in B$. Then

$$\lambda_{a\odot b}(c) = \ominus(a\odot b)\oplus(a\odot b\odot c)$$

$$= \ominus a\oplus(a\odot(\ominus b)\ominus a\oplus(a\odot b\odot c) \quad \text{by Lemma 1. ii)}$$

$$= \ominus a\oplus(a\odot(\ominus b\oplus(b\odot c))) \quad \text{using (*)}$$

$$= \ominus a\oplus(a\odot\lambda_b(c)) = \lambda_a(\lambda_b(c)) = \lambda_a\lambda_b(c). \square$$

Note, $\operatorname{Ker}\lambda = \{a\in B \mid \lambda_a(b) = b \text{ for all } b\in B\}$

$= \{a\in B \mid a\odot b = a\oplus b \text{ for all } b\in B\}$

which is a subbrace of B with trivial skew brace structure.

Def 2 (Ideal, Socle, Annihilator). An ideal of a skew brace B is a subset $I\subset B$ which is a normal subgroup with respect to addition and multiplication and $\lambda_a(I)\subset I$ for $a\in B$.

The socle of B is defined as

$$\operatorname{Soc}(B) = \{a\in B \mid a\oplus b = a\odot b,\ b\oplus(b\odot a) = (b\odot a)\oplus b \text{ for all } b\in B\}$$

$$= \operatorname{Ker}\lambda \cap Z(B,\oplus)$$

is an ideal of B.

The annihilator of B is defined to be

$$\mathrm{Ann}(B) = \mathrm{Soc}(B) \cap Z(B,\odot)$$
$$= \ker\lambda \cap Z(B,\oplus) \cap Z(B,\odot).$$

is also an ideal of B.

Let us define for any $a \in B$ a map

$$m_a : B \longrightarrow B$$
$$b \longmapsto a \odot b.$$

Lemma 3. The following hold.

i) We have $m_a \in \mathrm{Aut}(B,\oplus)$ for all $a \in B$.

ii) The map $m : (B,\odot) \longrightarrow \mathrm{Aut}(B,\oplus)$

$$a \longmapsto m_a$$

is an injective group homomorphism whose image is a regular subgroup.

Proof. i) Note $m_a(b) = a \odot b = a \oplus \lambda_a(b)$. Now by Lemma 2, i) we have $\lambda_a \in \mathrm{Aut}(B,\oplus)$, so $m_a \in \mathrm{Aut}(B,\oplus)$.

ii) Suppose $m_a(b) = b$ for all $b \in B$. Then $a \odot 1 = 1 \Rightarrow a = 1$, so m is injective.

Now $m_{a\odot b}(c) = (a \odot b) \oplus \lambda_{a\odot b}(c)$

$= (a \oplus \lambda_a(b)) \oplus \lambda_a\lambda_b(c)$ by Lemma 2, ii)

$= (a\lambda_a)(b\lambda_b)(c)$ for all $c \in B \Rightarrow$

$m_{a\odot b} = m_a m_b$. Finally, note

Skew Braces

The the map $\mathrm{Im}\, m \times B \longrightarrow B \times B$
$(ma, b) \longmapsto (a \circ b, b)$
is a bijection. □

It turns out that every regular subgroup of $\mathrm{Hol}(B, +)$ gives a skew brace structure on $(B, +)$.

Proposition 1. There exists a bijective correspondence between isomorphism classes of skew braces with additive group isomorphic to $(B, +)$ and classes of regular subgroups of $\mathrm{Hol}(B, +)$ under conjugation by elements of $\mathrm{Aut}(B, +)$.

Proof. Lemma 3 shows that every skew brace $(B, +, \circ)$ has unique embedding

$$m : (B, \circ) \hookrightarrow \mathrm{Hol}(B, +)$$

Now suppose $f : (B, +, \circ_1) \longrightarrow (B, +, \circ_2)$ is an isomorphism of skew braces. Then we have $f \in \mathrm{Aut}(B, +)$. And if we define by $C_f : \mathrm{Hol}(B, +) \longrightarrow \mathrm{Hol}(B, +)$
$\eta \alpha \longmapsto \eta^f f \alpha f^{-1}$;
then we have a commutative diagram

$$\begin{array}{ccc} (B, \circ_1) & \xrightarrow{m_1} & \mathrm{Hol}(B, +) \\ \downarrow f & & \downarrow \\ (B, \circ_2) & \xrightarrow{m_2} & \mathrm{Hol}(B, +) \end{array}$$

showing that images of m_1 is conjugate to image of m_2.

Conversely, given a regular subgroup $G \subset \mathrm{Aut}(B, \oplus)$. The map $\psi : G \to B$ is a bijection, so we

$$\eta_a \longmapsto a$$

Can define the $\odot$ operation on $(B, \oplus)$ by

$$a \odot b = \psi(\psi^{-1}(a)\,\psi^{-1}(b)).$$

Now since $\psi^{-1}(a) = a\eta_a$ for all $a \in B$, we have

$$a \odot b = \psi(a\eta_a b \eta_b) = a\eta_a(b),$$

so $a \odot (b \oplus c) = a\eta_a(b \oplus c)$

$$= a\eta_a(b) \oplus a\eta_a(c) = (a \odot b) \oplus (a \odot c)$$

Furthermore $(B, \odot) \xrightarrow{m} \mathrm{Aut}(B, \oplus)$ has G as its image, and if $G_1 = f G_2 f^{-1}$ for some $f \in \mathrm{Aut}(B, \oplus)$, then

$$f(a \odot_1 b) = f\psi(\psi^{-1}(a)\psi^{-1}(b))$$
$$= f(a) f\eta_a(b)$$
$$= a \odot_2 b. \quad \square$$

Skew Braces

Corollary 1. (Automorphism groups of skew braces). Let $(B, \oplus, \odot)$ be a skew brace. Then there exists a natural identification

$$Aut_{Br}(B,\oplus,\odot) \cong \{\alpha \in Aut(B,\oplus) \mid \alpha(Im\, m)\alpha^{-1} \subseteq Im\, m\}$$

Proof. Follows from the observation that if $\alpha \in Aut_{Br}(B,\oplus,\odot)$, then we have

$$\begin{array}{ccc} (B,\odot) & \xrightarrow{m} & Hol(B,\oplus) \\ \downarrow \alpha & & \downarrow C_\alpha \\ (B,\odot) & \xrightarrow{m} & Hol(B,\oplus). \end{array} \quad \square$$

Notation 1. We shall call a skew brace $(B,\oplus,\odot)$ such that $(B,\oplus) \cong N$ and $(B,\odot) \cong G$ a G-skew brace of type N.

Remark 1. Proposition 1 implies that to find non-isomorphic G-skew braces of N type, it suffices to classify the set $\tilde{S}(G,N) = \{H \subseteq Hol(N) \mid H \text{ regular and } H \cong G\}$ and then extract a maximal subset whose elements are not conjugate by any element of $Aut(N)$.

Some open problems:

(Q1) Let $m \in \mathbb{N}$, the generalised quaternion group is $Q_{4m} = \langle a, b \mid a^m = b^2, a^{2m} = 1, b^{-1}ab = a^{-1} \rangle$ classify quaternion-braces.

(Q2) Let B be a finite skew brace with solvable additive group. Is the multiplicative group solvable

(Q3) Let B be a finite skew brace with nilpotent multiplicative group. Is the additive group solvable?

(Q4) Let B be a skew brace with multiplicative group isomorphic to $\mathbb{Z}$. Is the additive group of isomorphic to $\mathbb{Z}$.

Skew braces can also equivalent to bijective 1-cocycles, not skew cycle sets.
See 'on skew braces' for more information.

Skew Braces, The Yang-Baxter Equation, and Ring

In this section I would like to tell about the connection between skew braces to mathematical physics and ring theory. I will also show some of the current results and open problems.

Recall from before: A (left) skew brace $(B, \oplus, \odot)$ is a set such that $(B, \oplus)$ and $(B, \odot)$ are groups and

$$a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c).$$

Lemma 3 showed that the map

$$\begin{aligned} m : (B, \oplus) &\longrightarrow \mathrm{Aut}(B, \oplus) = \mathrm{Aut}(B, \oplus) \rtimes \mathrm{Aut}(B, \oplus) \\ a &\longmapsto (m_a : b \longmapsto a \odot b) \end{aligned}$$

is a regular embedding. $(m_a = \lambda_a \rho_a)$

Proposition 4 showed that

$$\left\{ \begin{array}{l} \text{isomorphism classes} \\ \text{of skew braces} \\ \text{of type } N \text{ i.e. } (B, \oplus) \cong N \end{array} \right\} \overset{\text{bij}}{\longleftrightarrow} \left\{ \begin{array}{l} \text{classes of regular} \\ \text{subgroups of } \mathrm{Hol}(N) \\ \text{under conjugation by } \mathrm{Aut}(N) \end{array} \right\}$$

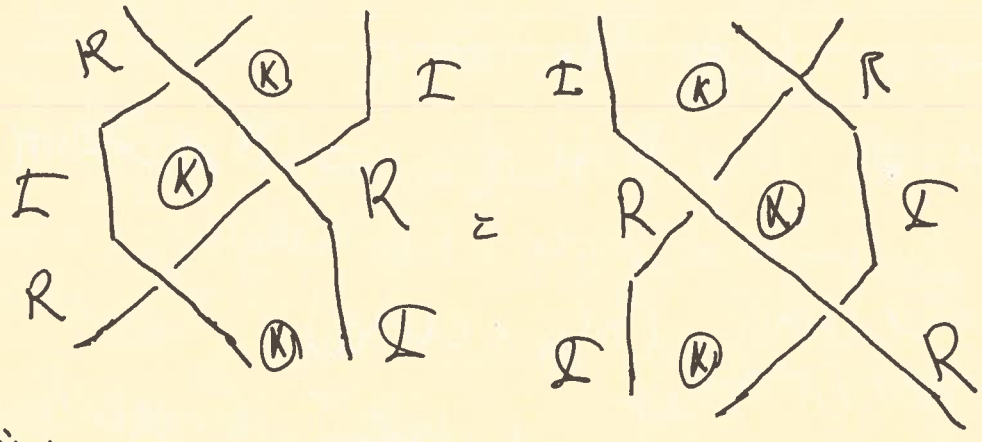
We will first look at how skew braces give solutions to the Yang-Baxter equation.

The Yang-Baxter equation 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 Yang-Baxter equation if

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

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

The above equation can be pictorially represented by



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

Def 3. A set-theoretic solution of the Yang-Baxter equation is a pair (X, r) where X is a set, and

non-empty

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

is a map such that r is a bijection and

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

The Yang-Baxter Equation and Rings

The solution is called non-degenerate if σ_x and τ_x are bijections for all $x \in X$. We shall only be concerned with non-degenerate solutions. A non-degenerate solution is called involutive if $r^2 = id$.

A map between two solutions (X, r) and (X', r') is a map of sets $\varphi : X \to X'$ which commutes with r and r', i.e., $r'(\varphi \times \varphi) = (\varphi \times \varphi) r$.

Example 2. Let X be a non-empty set. The map

$$r : X \times X \to X \times X$$
$$(x, y) \mapsto (y, x)$$

makes (X, r) a set-theoretic solution called the trivial solution.

$r(x,y) = (xyx^{-1}, x)$. For X a group.

More generally, let $f, g \in X \to X$ be maps. Then the map $r(x,y) = (f(y), g(x))$ makes (X, r) into a solution if and only if $fg = gf$. It is non-degenerate if f and g are bijections and involutive if $f = g^{-1}$.

Two such solutions are isomorphic if $f = hgh^{-1}$ for some bijection $h : X \to X$. These are called permutation solutions and are due to Lyubeshenko.

From now by a set-theoretic solution, we shall mean a non-degenerate set-theoretic solution and set

$$r : X \times X \to X \times X \quad \text{given by} \quad r(x,y) = (f_x(y), g_y(x)).$$

Lemma 4. For (K,r) a Leo-Hurewicz solution structure. Then

i) we have

$$f_{f_x(y)} f_{g_y(x)} = f_x f_y$$

$$g_{f_{g_y(x)}(z)} f_x = f_{g_{f_y(z)}(x)} g_z$$

$$g_z g_y = g_{g_z(y)} g_{f_y(z)}$$

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

i.e. $f_{f_x(y)} f_{g_y(x)} = f_x f_y$ and $g_x g_y = g_{g_x(y)} g_{f_y(x)}$

$$g_{f_{g_y(x)}(z)} f_x = f_{g_{f_y(z)}(x)} g_z$$

ii) If r is indecomposable, then

$$f_{f_x(y)} g_y(x) = x \quad \text{and} \quad g_{g_{y(x)}} f_x(y) = y$$

for all $x,y \in K$.

Let us now define some relevant objects of (K,r).

The Yang-Baxter Equation and Rings

Def 4. Let (X,r) be a non-degenerate solution. The structure group of (X,r) is defined by

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

We denote by $i_G : X \longrightarrow G(X,r)$ the natural map. The map i_G is not in general injective. (Exercise)

Example 3. If (X,r) is the trivial solution, then

$$G(X,r) = \mathbb{Z}^X.$$

Let us study the structure of $G(X,r)$ briefly. Let $\mathrm{Aut}(X)$ be the group of permutations of X, and $\mathbb{Z}^X$ as before the free abelian group spanned by X. Denote the generator of $\mathbb{Z}^X$ corresponding to x by t_x, so

$$\mathbb{Z}^X = \langle t_x \mid x \in X \text{ and } t_x t_y = t_y t_x \rangle.$$

Then $\mathrm{Aut}(X)$ acts on $\mathbb{Z}^X$ by $(\alpha, t_x) \longmapsto t_{\alpha(x)}$. Denote by $M_X = \mathbb{Z}^X \rtimes \mathrm{Aut}(X)$. Then we have the following.

Proposition 2. Assume (K,r) is involutive. Then the assignment

$G(K,r)$ is abelian by finite

$$\varphi_l : G(K,r) \longrightarrow M_K$$
$$n \longmapsto t_{f_n(n)} f_n = f_n t_n$$

is a well-defined injective group homomorphism.

Proof. Exercise (or see ETINGOF 1998).

"Set-theoretic solutions to the quantum Yang-Baxter Equation

Now let us finally see how skew braces give set-theoretic solutions to the Yang-Baxter equation.

Q1) when is $G(K,r)$ torsion free? (D. Bachiller 2016)

Theorem 1. Let $A=(B,\oplus,\odot)$ be a skew brace. Then the map

$$r_A : A \times A \longrightarrow A \times A$$
$$(a,b) \longmapsto (\ominus a \oplus (a \odot b) \,,\, (\ominus a \oplus (a \odot b)) \odot a \odot b)$$
$$(\lambda_a(b) \,,\, \lambda_a(b)^{-1} \odot a \odot b)$$

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

Proof. Check directly (or see Guarnieri 2016 "skew braces and the Yang-Baxter equation".

Also we have the following.

The Yang-Baxter Equation and Rings.

set-theoretic

Theorem 2. Let (X,r) be a non-degenerate solution of the Yang-Baxter equation. Then there exists a unique skew left structure over the group $G=G(X,r)$ such that

$$(\iota_G x \iota_G)\, r = r\,(\iota_G x \iota_G).$$

where $\iota_G : X \longrightarrow G(X,r)$ is the canonical map as before. Moreover, the pair $(G(X,r), \iota_G)$ has the property that if B is a skew brace and $f: X \to B$ is a map such that $(f \times f) r = r_B (f \times f)$, then there exists a unique morphism of skew braces $\phi : G \longrightarrow B$ such that $\phi \iota_G = f$, and $(\phi \times \phi) r_G = r_B (\phi \times \phi)$.

Proof: "On skew Braces" Rump

The skew brace $G(X,r)$ is defined as the structure skew brace of the solution (X,r).

Questions about the $\mathrm{Soc}(G(X,r))$.

Next Let us look at ring theoretic and other properties of skew braces. These were developed by A. Smoktunowicz and L. Rump

Ring theory. Skew braces generalise nilpotent rings.

Def 5. A radical ring is a ring $(R,+,\cdot)$ — not necessarily with 1 — which coincides with its own Jacobson radical ($J(R)=R$) or equivalently if under the Jacobson circle operation

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

becomes a group.

Def 6. A skew brace $(B,\oplus,\odot)$ is called two sided if

$$(a\oplus b)\odot c = (a\odot c)\ominus c\oplus(b\odot c).$$

Let $(R,+,\cdot)$ be a radical ring. Then

$$x\circ(y+z) = x+y+z+xy+xz$$
$$= x+y+xy-x+x+z+xz$$
$$= (x\circ y)-x+(x\circ z),$$

so $(R,+,\circ)$ is a brace (i.e. skew brace with abelian additive group). Furthermore,

$$(x+y)\circ z = x+y+z+xz+yz$$
$$= x+z+xz-z+y+z+yz$$
$$= (x\circ z)-z+(y\circ z),$$

so $(R,+,\circ)$ is two sided.

The Yang-Baxter equation and Rings

On the other hand let $(B, \oplus, \circ)$ be a two-side brace and define $a \otimes b = \ominus a \oplus (a \circ b) \ominus b$. Then $(B, \oplus, \otimes)$ becames a nedrced ring. Note,

$$a \otimes (b \oplus c) = \ominus a \oplus (a \circ (b \oplus c)) \ominus b \ominus c$$
$$= \ominus a \oplus a \circ b \ominus a \oplus a \circ c \ominus b \ominus c$$
$$= \ominus a \oplus a \circ b \ominus b \ominus a \oplus a \circ c \ominus c$$
$$= (a \otimes b) \oplus (a \otimes c)$$

Similarly since B is two-sided we get

$$(a \oplus b) \otimes c = a \otimes c \oplus b \otimes c.$$

Furthermore, we have

$$a \circ b = a \oplus b \oplus a \otimes b$$
$$= a \oplus b \ominus a \oplus (a \circ b) \ominus b = a \circ b,$$

So $(B, \oplus, \otimes)$ is a nedrced ring.

More generally, for an skew brace $(B, \oplus, \circ)$ define the operation $\otimes$ by

$$a \otimes b = \ominus a \oplus (a \circ b) \ominus b = \lambda_a(b) \ominus b.$$

Then currently some try to understand the purpose $(B, \oplus, \otimes)$ as an algebraic structure. The object $(B, \oplus, \otimes)$ is a ~~ring~~ when $(B, \oplus)$ is abelian and B is two-sided, but some of the ring theoretic methods can still be used to study $(B, \oplus, \otimes)$ in general case.

Recall an ideal $\Sigma \subset (B, \oplus, \odot)$ is a subset Σ which is a normal subgroup with respect to both $\oplus$ and $\odot$ and $\lambda_a(I) \subset I$. A skew brace B is said to be simple if its only ideals are 0 and B. Simple skew brace are graded very inversely.

operations on ideals. Let $(B, \oplus, \odot)$ be a skew brace we can define three operations on ideals of B. Let $I, J \subset B$ be ideals we can define

$I \cap J$ which is an ideal of B.

Define $I \oplus J$ the subgroup of $(B, \oplus)$ generated by all element $u \oplus v$ for $u \in I$ and $v \in J$.

Define $I \otimes J$ to be the subgroup of $(B, \oplus)$ generated by

$u \otimes v$ for $u \in I$ and $v \in J$.

The Yang–Baxter Equation and Rings

It can be shown that $I \circ J$ and $I \circledast J$ are ideals of B.

A skew brace is said to be prime if for all non-zero ideals I and J one has $I \circledast J \neq 0$.

Simple non-trivial skew braces are prime but converse does not hold.

Some problems:

(Q1) Are there simple two-sided skew braces of nilpotent type?

(Q2) Let B be a prime ~~brace~~ skew brace of nilpotent type. Is A simple?

(Q3) Are there prime two sided skew braces of nilpotent type?

→ Smoktunowicz and Vendramin.

Read 'em skew braces and their ideals for more.

Finally, skew braces are connected to Near-rings and nilpotent rings, we shall briefly talk about the connection to Near-rings.

Def 7. A near-ring is a set N with two operations $\oplus$ and $\cdot$, so that $(N,+)$ is a group, $(N,\cdot)$ is a semigroup and $x\cdot(y\oplus z) = x\cdot y \oplus x\cdot z$ for all $x,y,z \in N$. Assume that our near-rings contain a multiplicative identity denoted by 1.

Example 4. Let G be a group. Then $\mathrm{Map}(G,G)$ is a near-ring under pointwise multiplication and composition.

A subgroup M of $(N,\oplus)$ is said to be a constructive subgroup if $1+M$ is a subgroup of $N^\times$ of units of N.

Proposition 3. Let N be a near-ring and M a constructive subgroup. Then M is a skew brace under

$$m \oplus m' = m+m', \text{ and } m\odot m' = m + (1+m)\cdot m'.$$

Proof. 'On skew braces' page 14 □.

Skew braces and Hopf-Galois structures

Today I would like to talk about the first connection of skew braces to other areas. It turns out skew braces parametrise algebraic objects called Hopf-Galois structure which get used in certain areas of number theory.

Let us first recall. A skew brace is a set B together with two operations $\oplus$ and $\odot$ such that $(B,\oplus)$ and $(B,\odot)$ are groups and

$$a\odot(b\oplus c) = (a\odot b)\ominus a\oplus(a\odot c).$$

In lecture 1 we saw that there is a bijective correspondence

$$\left\{\begin{array}{l}\text{isom classes of skew}\\ \text{braces of type}\\ N\end{array}\right\} \overset{\text{bij}}{\longleftrightarrow} \left\{\begin{array}{l}\text{Class of regular}\\ \text{subgroups of } \mathrm{Hol}(N)\\ \text{under conjugation by } \mathrm{Aut}(N)\end{array}\right\}$$

In lecture 2 we saw that for a skew brace $(B,\oplus,\odot)$ the map

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

makes (B,r) into a set-theoretic solution of the Yang-Baxter equation and the connection of skew braces to radical rings. In this lecture we show that skew braces parametrise Hopf-Galois structures.

Hopf-Galois theory. Two aims in studying Hopf-Galois theory. Initially it was introduced to generalize the classical Galois theory. Later it was used to study properties of rings of integers of extensions of local or global fields.

Let's look at number theoretic considerations. Let us fix L/K to be a finite separable extension of fields (or we may assume L/K is Galois with Galois group G.

Assume L/K is an extension of number fields, or p-adic fields for a prime number p, with rings by $\mathcal{O}_L$ and $\mathcal{O}_K$.

The normal basis theorem tells us that L is a free $K[G]$-module of rank one.

Now $\mathcal{O}_L$ is also a module over $\mathcal{O}_K[G]$, so one can ask if $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$.

The answer to this question is no in general. In some cases $\mathcal{O}_K[G]$ is too small!

Hopf-Galois structures

To consider a bigger ring we can look at the associated order of $\mathcal{O}_L$ in $K[G]$ by

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

and now ask the question if $\mathcal{O}_L$ can be free over its associated order. Again the answer is no in general. Can we replace $K[G]$ with any other K-Hopf algebra? Yes. Byott in 1996 showed that for $|G|=n$, if $\gcd(n, \phi(n)) \neq 1$, there are other options for $K[G]$, these giving L/K a Hopf-Galois structure.

Hopf-Galois structures are analogous to $K[G]$: they are K-Hopf algebras acting on L with a certain property.

We shall proceed to define these in a general setting. Let us fix R to be a commutative ring with a unit. We first define what it means to have a Galois extension of R.

Def 8. Let S be a finite commutative R-algebra (i.e. finitely generated projective R-module). Suppose $G \subseteq \mathrm{Aut}_R(S)$ is a finite group of R-algebra automorphisms of S. Define the cross products

$$D(S,G) = \left\{ \sum_{\sigma \in G} s_\sigma \sigma \;\middle|\; s_\sigma \in S \right\}.$$

Then we say S is a Galois extension of R with Galois group G if the R-module map

$$j : D(S,G) \longrightarrow \mathrm{End}_R(S)$$
$$s_\sigma \sigma \longmapsto (t \longmapsto s_\sigma \sigma(t))$$

is a bijection.

Example 5. For L/K with $G = \mathrm{Gal}(L/K)$ the cross product $D(L,G)$ and $\mathrm{End}_K(L)$ have the same dim $[L:K]$, and since the elements of G are L-linearly independent, the map j is injective and hence bijective.

The classical Galois extensions are covered by Def 8.

Example 6. If L/K is an extension of number fields, then $\mathcal{O}_L/\mathcal{O}_K$ is Galois if and only if L/K is unramified

Hopf-Galois structures

Next we shall define what it means for S/R to be an H-Galois extension for a K-Hopf algebra H.

First we recall:

Def 9. An R-Hopf algebra is an R-module which is both an algebra and a coalgebra over R such that the comultiplication and counit maps

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

are homomorphisms of algebras; the multiplication and the unit maps

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

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

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

Let us define by $\tau : H \otimes H \longrightarrow H \otimes H$ the switch map $\tau(h_1 \otimes h_2) = h_2 \otimes h_1$. Then an R-Hopf algebra is called cocommutative if $\mu\tau = \mu$ and commutative if $\tau\Delta = \Delta$.

Example 7. The group algebra $R[G]$ with

$$\Delta(G) = G \otimes G, \quad \varepsilon(G) = 1, \quad \text{and} \quad \lambda(G) = G^{-1}$$

for $G \in G$, is an R-Hopf algebra, which is cocommutative.

Now we can define an H-Galois extension.

Def 10. Let H be a finite cocommutative R-Hopf algebra. A finite commutative R-algebra S is called an H-Galois extension of R, or H endows S/R with a Hopf-Galois structure if (or we say) S is a left H-module algebra such that the R-module homomorphism

$$j : S \otimes_R H \longrightarrow End_R(S)$$
$$s \otimes h \longmapsto (t \longmapsto sh(t))$$

is an isomorphism (of R-algebras for the smash product structure on $S \otimes_R H$).

Examples • For the Galois extension L/K, the Hopf algebra $K[G]$ together with its action on L is called the classical Hopf-Galois structure on L/K.

Remark 2. Algebro-geometric interpretation.

Suppose H gives a Hopf-Galois on S/R. Let $H^* = Hom_R(H, R)$, note H^* is commutative.

Let $X = Spec(R)$ and $Y = Spec(S)$. Then $Y \to X$ is a principal homogeneous space for the group scheme $G = Spec(H^*)$.

Hopf-Galois structures

Now suppose L/K is an extension of number fields, or p-adic fields, and H embeds L/K with a Hopf-Galois structure. We define the associated order of $\mathcal{O}_L$ in H by

$$\mathfrak{A}_H = \{\alpha \in H \mid \alpha(\mathcal{O}_L) \subseteq \mathcal{O}_L\}.$$

Then one can ask if $\mathcal{O}_L$ is free over $\mathfrak{A}_H$.

Question is how to find all Hopf-Galois structures on L/K.

Greither-Pareigis Theory. They reduced the problem of finding Hopf-Galois structures to a problem in number theory.

Theorem 3. Hopf-Galois structures on L/K correspond bijectively to regular subgroups of $\mathrm{Perm}(G)$ which are normalised by the image of G as left translations inside $\mathrm{Perm}(G)$.

Proof GP 1987.

In particular, they showed every H which endows L/K with a Hopf-Galois structure is of the form $(L[N])^G$ for some regular subgroup $N \subseteq \mathrm{Perm}(G)$. ($N$ is the type)

Problem. The group $Perm(G)$ can be too large. The solution to this problem is to work with the holomorph of groups rather than the permutation group.

Theorem 4. Let G and N be finite groups. Then there exists a bijection between the sets

$$\mathcal{N} = \{ \alpha : N \hookrightarrow Perm(G) \mid \alpha(N) \text{ is regular normalized by the left translations} \}$$

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

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

Proof. (Byott 1996)

This theorem helps in finding Hopf-Galois structures on L/K by finding regular subgroups of $Hol(N)$. In particular, if we let $e(G,N)$ denote the number of Hopf-Galois structure 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 $Hol(N)$ which are isomorphic to G.

Hopf-Galois structures

Recall from the first lecture every skew brace of type N can be embedded inside $\mathrm{Hol}(N)$. Now we can immediately see the connection between Hopf-Galois structures and skew braces. We shall make it more explicit. Let $(B,\oplus,\odot)$ be a skew brace. Let us define for any $a \in B$ a map

$$\lambda_a : B \longrightarrow B, \quad b \longmapsto a \ominus b.$$

Lemma 5. The map

$$\lambda : (B,\oplus) \longrightarrow \mathrm{Perm}(B,\odot); \ a \mapsto \lambda_a$$

is a regular embedding and $\mathrm{Im}\,\lambda$ is normalised by the left translations.

Proof. It is clear that λ is a regular embedding. Let $a,b,c \in B$. Then we have

$$b \odot (\lambda_a(b^{-1} \odot c)) = b \odot (a \oplus (b^{-1} \odot c))$$
$$= (b \odot a) \ominus b \oplus c = \lambda_{(b\odot a)\ominus b}(c),$$

So $b\,\lambda_a b^{-1} = \lambda_{(b\odot a)\ominus b}$ and $b\,\mathrm{Im}\,\lambda_a\, b^{-1} \subseteq \mathrm{Im}\,\lambda$.

Now this gives an action of $(B,\odot)$ on $(B,\oplus)$ by

$$a \cdot b = (a \odot b) \ominus a \text{ for } a \in (B,\odot) \text{ and } b \in (B,\oplus).$$
$$= a \oplus \lambda_a(b) \ominus a.$$

Proposition 4. There exists a bijective correspondence between isomorphism classes of skew braces with multiplicative group isomorphic to $(B,\cdot)$ and regular subgroups of $\mathrm{perm}(B,\cdot)$ which are normalised by $(B,\cdot)$ under conjugation by $\mathrm{Aut}(B,\cdot)$.

Proof. Similar to proposition 1 cut NZ 2018

Corollary 2. There exists a bijective correspondence between isomorphism classes of skew braces — skew braces and classes of Hopf-Galois structures on L/K under the equivalence relation $L[N_1]G \sim L[N_2]G$ if $N_2 = \alpha N_1 \alpha^{-1}$ for some $\alpha \in \mathrm{Aut}(G)$, where $N_1, N_2 \subset \mathrm{perm}(G)$ are normalised by the left translations

Proof. NZ 2018

Corollary 3. For $(B,\oplus,\circ)$ a skew brace we have

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

Proof. NZ 2018.

Let $S(G,N) = \{N \subseteq \mathrm{perm}(G) \mid N \text{ is regular and normalised by the left translations}\}$

Denote by B_G^N the isomorphism classes of G-skew brace of type N, and. Firstly, note that $\mathrm{Aut}(G)$ acts on $S(G,N)$, via its action on $\mathrm{perm}(G)$ by conjugation by elements of $\mathrm{Aut}(G)$, and a set of orbit representatives $\{N_1, \ldots, N_s\}$, give a

Hopf-cebris structures

list of non-isomorphic skew braces. By Theorem 3 we have $e(G,N) = |S(G,N)|$, and so we have

$$e(G,N) \leq \sum_{i=1}^{s} |orb(N_i)|$$

$$= \sum_{i=1}^{s} \frac{|Aut(G)|}{|stab(N_i)|} = \sum_{B_G^N} \frac{|Aut(G)|}{|Aut_{Br}(B_G^N)|}.$$

This gives the number of Hopf-cebris structures as parametrised by skew braces.

(1) check on the arithmetic invariants of the Hopf-cebris structures corresponding to a skew brace $(B, \oplus, \circ)$?