Regular subgroups, skew braces, gamma functions and Rota–Baxter operators

Andrea Caranti

Yaroslavl, 30 March 2022 — 17:00 MSK / 16:00 CEST

Introduction

In the past few years there has been considerable interest in skew braces, a novel algebraic structure.

Skew braces have many applications, such as

- finding solutions of the Quantum Yang–Baxter equation;
- classifying Hopf-Galois structures.

Skew braces are in one-to-one correspondence with the regular subgroups of the (permutational) holomorph of a group.

Skew braces can be dealt with via certain functions, called lambda in the literature on skew braces, and which I call gamma for legacy reasons.

These functions are characterised by a certain functional equation, and are related to Rota–Baxter operators.

Regular subgroups and group operations

A converse to Cayley's Theorem

Let $(G, 1)$ be a pointed set. A subgroup N of $\mathrm{Sym}(G)$ is regular if the map

$$N \to G, \qquad n \mapsto 1^n$$

is a bijection. In other words N is transitive on G, and all stabilisers are trivial. Every element of N can be written uniquely as $\nu(g)$, where $\nu : G \to N$ is the inverse of the above map, that is, $\nu(g)$ is the unique solution to

$$1^{\nu(g)} = g.$$

You can use transport of structure via these two maps to define a group structure $(G, \circ, 1)$ on G, such that $\nu : (G, \circ) \to N$ is an isomorphism, that is, $\nu(g \circ h) = \nu(g)\nu(h)$. Note that

$$g^{\nu(h)} = 1^{\nu(g)\nu(h)} = 1^{\nu(g \circ h)} = g \circ h,$$

which is a converse of Cayley's Theorem.

Two group operations

If in addition $(G, \cdot, 1)$ is a group, we have two (thus far unrelated) group operations "$\cdot$" and "$\circ$" on the set G.

Let $\rho : (G, \cdot) \to \mathrm{Sym}(G)$ be the right regular representation, $x^{\rho(g)} = x \cdot g$. So we have two (thus far unrelated) regular subgroups $\rho(G), N \leq \mathrm{Sym}(G)$.

Suppose

$$N \leq N_{\mathrm{Sym}(G)}(\rho(G)) = \mathrm{Aut}(G)\rho(G) = \mathrm{Hol}(G). \tag{1}$$

Here $\mathrm{Hol}(G)$ is the *permutational* holomorph of G. (The abstract holomorph is the semidirect product $\mathrm{Aut}(G)G$.)

Why this condition (1)?

Normalising: the holomorph

Normalising makes sense

The condition $N \leq N_{\mathrm{Sym}(G)}(\rho(G)) = \mathrm{Aut}(G)\rho(G) = \mathrm{Hol}(G)$ naturally occurs in **cryptographic applications:**

A.C., F. Dalla Volta and M. Sala,
Abelian regular subgroups of the affine group and radical rings.
Publ. Math. Debrecen **69** (2006), no. 3, 297–308.

(this is where gamma functions were first introduced), and **applications to Hopf-Galois structures:**

S.C. Featherstonhaugh, A.C. and L.N. Childs
Abelian Hopf Galois structures on prime-power Galois field extensions
Trans. Amer. Math. Soc., **364** (2012), no. 7, 3675–3684

Both situations are actually best dealt with via radical rings.

⏩ Skip radical rings

An aside: Radical Rings

A (commutative) ring $(A, +, \star)$ is said to be radical if it coincides with its Jacobson radical.

In other words, A is a group both with respect to addition and with respect to the Jacobson/Kuroš circle operation

$$a \circ b = a - a \star b + b.$$

Radical rings are the blueprint for (skew) braces, and a posteriori a particular case of (skew) braces.

When $(G, +)$ is abelian, and N is a regular, abelian subgroup of $\mathrm{Hol}(G)$, there is an operation $\star$ on G such that $(G, +, \star)$ is a commutative, radical ring, and

$$a^{\nu(b)} = a \circ b = a - a \star b + b.$$

(Recall: $N = \{\, \nu(b) : b \in G \,\}$ and $\nu(a \circ b) = \nu(a)\nu(b)$.)

Enter gamma

Let $N = \{\nu(g) : g \in G\} \leq \mathrm{Aut}(G)\rho(G)$ be a regular subgroup of $\mathrm{Sym}(G)$. Then

$$\nu(g) = \gamma(g)\rho(g),$$

for some function $\gamma : G \to \mathrm{Aut}(G)$. We have

$$\begin{aligned}\nu(g \circ h) &= \nu(g)\nu(h) = \gamma(g)\rho(g)\gamma(h)\rho(h) \\ &= \gamma(g)\gamma(h)\rho(g)^{\gamma(h)}\rho(h) = \gamma(g)\gamma(h)\rho(g^{\gamma(h)}h) \\ &= \nu(g^{\gamma(h)}h) = \gamma(g^{\gamma(h)}h)\rho(g^{\gamma(h)}h).\end{aligned}$$

In other words, we have

$$g \circ h = g^{\gamma(h)}h,$$

and it turns out that these gamma functions are *characterised* by the functional equation

$$\gamma(g^{\gamma(h)}h) = \gamma(g)\gamma(h).$$

Skew braces

γ is a function $G \to \mathrm{Aut}(G, \cdot)$. Thus for $a, b, c \in G$ we have

$$(a \cdot b)^{\gamma(c)} = a^{\gamma(c)} \cdot b^{\gamma(c)}.$$

Rephrasing in terms of

$$x \circ c = x^{\gamma(c)} c, \quad \text{that is,} \quad x^{\gamma(c)} = (x \circ c) \cdot c^{-1}$$

we get

$$((a \cdot b) \circ c) \cdot c^{-1} = (a \circ c) \cdot c^{-1} \cdot (b \circ c) \cdot c^{-1},$$

which is the axiom for a (right) skew brace $(G, \cdot, \circ)$.

Groups having the same holomorph

Groups having the same holomorph

There is a sizeable literature, particularly by Russian authors, on groups having the same holomorph. This thread has been revived in recent years by Timothy Kohl.

G and the regular subgroup $N \leq \mathrm{Sym}(G)$ are said to have the same holomorph if $G \cong N$, and

$$\mathrm{Hol}(G) = N_{\mathrm{Sym}(G)}(\rho(G)) = N_{\mathrm{Sym}(G)}(N) \cong \mathrm{Hol}(N).$$

A result of Miller states the the multiple holomorph of G

$$N_{\mathrm{Sym}(G)}(N_{\mathrm{Sym}(G)}(\rho(G))) = N_{\mathrm{Sym}(G)}(\mathrm{Hol}(G))$$

acts transitively by conjugation on the set of these N, so the quotient group

$$T(G) = N_{\mathrm{Sym}(G)}(\mathrm{Hol}(G))/\mathrm{Hol}(G)$$

acts regularly on the set of regular subgroup N such that $G \cong N$ and $\mathrm{Hol}(G) = N_{\mathrm{Sym}(G)}(N)$.

Same holomorph via gamma functions

In terms of γ's, it is natural to consider first the weaker condition

$$N \trianglelefteq \mathrm{Hol}(G) = \mathrm{Aut}(G)\rho(G),$$

which translates to

$$\gamma(g^\beta) = \gamma(g)^\beta, \qquad \text{for } g \in G, \text{ and } \beta \in \mathrm{Aut}(G), \tag{2}$$

and then sift through these γ (and their associated regular subgroups N) to find those that satisfy the additional conditions.

(2) states that $\mathrm{Aut}(G,\cdot) \leq \mathrm{Aut}(G,\circ)$ in the skew brace $(G,\cdot,\circ)$.

In the abelian case, one has the commutative rings in which the automorphisms of the additive group are also ring automorphisms.

A.C. and F. Dalla Volta

The multiple holomorph of a f.g. abelian group

J. Algebra **481** (2017), 327–347

Perfect groups, and gamma functions taking values in the inner automorphism group

Some identities

One can rephrase the functional equation

$$\gamma(g^{\gamma(h)}h) = \gamma(g)\gamma(h)$$

as

$$\gamma(gh) = \gamma(g^{\gamma(h)^{-1}})\gamma(h).$$

If $\gamma(g^\beta) = \gamma(g)^\beta$ for all $g \in G$ and $\beta \in \mathrm{Aut}(G)$, then in particular

$$\begin{aligned}\gamma(gh) &= \gamma(g^{\gamma(h)^{-1}})\gamma(h)\\ &= \gamma(g)^{\gamma(h)^{-1}}\gamma(h)\\ &= \gamma(h)\gamma(g)\gamma(h)^{-1}\gamma(h)\\ &= \gamma(h)\gamma(g),\end{aligned}$$

that is, γ is an anti-homomorphism. In particular

$$1 = \gamma(gg^{-1}) = \gamma(g^{-1})\gamma(g), \quad \text{so that} \quad \gamma(g^{-1}) = \gamma(g)^{-1}.$$

Perfect Groups

Write

$$\iota : G \to \mathrm{Aut}(G), \qquad g \mapsto (x \mapsto x^g = g^{-1}xg).$$

We have

$$\begin{aligned}\gamma([g,h]) &= \gamma(g^{-1}g^{\iota(h)}) = \gamma(g^{\iota(h)})\gamma(g)^{-1} \\ &= \gamma(g)^{\iota(h)}\gamma(g)^{-1} = [\iota(h), \gamma(g)^{-1}] \\ &= \iota([h, \gamma(g)^{-1}]) \in \mathrm{Inn}(G).\end{aligned}$$

Thus, in a perfect group $G = \langle\, [g,h] : g, h \in G \,\rangle$, the gamma functions of regular subgroups having the same holomorph as G take values in the inner automorphism group $\mathrm{Inn}(G)$.

A.C. and F. Dalla Volta

Groups that have the same holomorph as a finite perfect group

J. Algebra **507** (2018), 81–102

Bi-skew braces, brace blocks and the normalising graph

Bi-skew braces

A skew brace $(G, \cdot, \circ)$ is said to be a bi-skew brace if $(G, \circ, \cdot)$ is also a skew brace.

L. N. Childs

Bi-skew braces and Hopf Galois structures

New York Journal of Mathematics **25** (2019), 574–588

A.C.

Bi-skew braces and regular subgroups of the holomorph.

J. Algebra **562** (2020), 647–665

Bi-skew braces are characterised in terms of gamma functions by any two out of the three identities

$$\gamma(a^{\gamma(b)}b) = \gamma(a)\gamma(b), \quad \gamma(ab) = \gamma(b)\gamma(a), \quad \gamma(a^{\gamma(b)}) = \gamma(a)^{\gamma(b)},$$

so all $N \trianglelefteq \mathrm{Hol}(G)$ yield examples.

Mutual normalisation

Let $(G, 1)$ be a pointed set. Let N, M be two regular subgroups of $\mathrm{Sym}(G)$, affording the operations "$\cdot$" and "$\circ$" on the set G.

Then the following are equivalent

- $(G, \cdot, \circ)$ is a bi-skew brace.
- N, M normalise each other, i.e. $[N, M] \leq N \cap M$.

The normalising graph appear to be an interesting object of study:

- the vertices are the regular subgroups of $\mathrm{Sym}(G)$
- two vertices are joined by an undirected edge if they normalise each other.

This graph has been first studied from the equivalent point of view of brace blocks.

Brace blocks

Alan Koch

Abelian maps, brace blocks, and solutions to the Yang-Baxter equation

arXiv:2102.06104, 2021, *JPAA*, 2022

Let $(G, 1)$ be a pointed set. A family $\mathfrak{B}$ of group operations on $(G, 1)$ is said to be a brace block if for all $\circ_1, \circ_2 \in \mathfrak{B}$ we have that $(G, \circ_1, \circ_2)$ is a (bi-)skew brace.

A brace block corresponds to a clique (complete subgraph) in the normalising graph.

A.C., L. Stefanello

Brace blocks from bilinear maps and liftings of endomorphisms

arXiv:2110.11028, 2022

Gamma functions with values in the inner automorphism group, and Rota–Baxter operators

Koch's construction

Koch studied the gamma functions that take values in the inner automorphism group. Koch's gamma functions are of the form

$$\gamma(g) = \iota((g^{-1})^{\psi}),$$

for some endomorphism $\psi \in \mathrm{End}(G)$ with an abelian image.

(Recall $\iota : G \to \mathrm{Aut}(G), g \mapsto (x \mapsto x^g = g^{-1}xg)$.)

Koch showed that for any such γ, and $g \circ h = g^{\gamma(h)}h$, we have that $(G, \cdot, \circ)$ is a bi-skew brace. Moreover, Koch showed that

1. $\psi \in \mathrm{End}(G, \circ)$
2. ψ has an abelian image also in $(G, \circ)$,

so that you can iterate the construction, and get a sequence of group operations. Koch showed that all these operations yield a brace block.

Bilinear maps, and liftings

With Lorenzo Stefanello we generalised this situation, by allowing central bilinear maps, and liftings of endomorphisms:

- Take $K \leq A \leq G$, with $K \leq Z(G)$, and A/K abelian.
- Let $\mathcal{A} = \left\{ \psi \in \mathrm{End}(G/K) : (G/K)^{\psi} \leq A/K \right\}$; it is a ring under pointwise operations.
- Let $\mathcal{B}$ be the set of bilinear maps $G \times G \to K$ having K in both kernels.
- Then $\gamma(g) = \iota(g^{\psi})$, for $\psi \in \mathcal{A}$, is a well defined gamma function, even when ψ does not lift to an endomorphism of G.
- Any two operations of the form

$$g \circ h = g^{\gamma(h)} \cdot h \cdot \beta(g, h),$$

  for γ, β as above, yield a bi-skew brace.
- So all these operations yield a brace block.

Rota–Baxter operators: a short bibliography

Glen Baxter

An analytic problem whose solution follows from a simple algebraic identity

Pacific J. Math. **10** (1960), 731–742

Li Guo, Honglei Lang, and Yunhe Sheng

Integration and geometrization of R-B Lie algebras

Adv. Math. **387** (2021), Paper No. 107834, 34pp

Valeriy G. Bardakov and Vsevolod Gubarev

R–B groups, skew left braces, and the Y–B equation

J. Algebra **596** (2022), 328–351

`https://arxiv.org/abs/2105.00428`

A.C., L. Stefanello

Skew braces from R–B operators *etc*

arXiv:2201.03936, 2022

Rota–Baxter operators and gamma functions

A Rota–Baxter operator on the group G is a map $B : G \to G$ such that

$$B(g^{B(h)}h) = B(B(h)^{-1}gB(h)h) = B(g)B(h).$$

Since gamma functions $\gamma : G \to \mathrm{Aut}(G)$ are characterised by the equation

$$\gamma(g^{\gamma(h)}h) = \gamma(g)\gamma(h),$$

it is clear that a Rota–Baxter operator B yields a gamma function

$$\gamma(g) = \iota(B(g)) \in \mathrm{Inn}(G), \tag{3}$$

via

$$G \xrightarrow{B} G \xrightarrow{\iota} \mathrm{Inn}(G).$$
$$\gamma$$

(Recall $\iota : G \to \mathrm{Inn}(G)$, $\iota : g \mapsto (x \mapsto g^{-1}xg)$.)

Conversely, if $\gamma : G \to \mathrm{Inn}(G)$ is a gamma function, does it come from a Rota–Baxter operator via (3)?

Lifting Morphisms

Let U, V be groups, and A be an abelian, normal subgroup of V. Let $\varphi : U \to V/A$ be a morphism.

What is the condition for φ to lift to a morphism $U \to V$?

A is a V-module under conjugation, and thus a V/A-module, as it is abelian. A is then a U-module via φ.

Lift φ to a map $C : U \to V$, that is

$$\varphi(u) = C(u)A \quad \text{for } u \in U.$$

Since φ is a morphism, we will have

$$C(xy) = C(x)C(y)\kappa(x, y),$$

for some function $\kappa : U \times U \to A$.

Lifting Morphisms

$C : U \to V$ is a lift of the morphism $\varphi : U \to V/A$.

$$C(xy) = C(x)C(y)\kappa(x, y).$$

Enforcing associativity on U, that is, computing in two ways

$$C((xy)z) = C(x(yz)),$$

we obtain that κ is a 2-cocycle. κ depends on the choice of C, but its cohomology class in $\mathrm{H}^2(U, A)$ is independent of C. We have

Proposition

The following are equivalent.

- $\varphi : U \to V/A$ *lifts to a morphism* $U \to V$.
- *The class of* κ *in* $\mathrm{H}^2(U, A)$ *is trivial.*

A cohomological setting for Rota–Baxter operators

Let $\gamma : G \to \mathrm{Inn}(G)$ be a gamma function, $g \circ h = g^{\gamma(h)} h$. We have

$$(G, \circ) \xrightarrow{\gamma} \mathrm{Inn}(G) \xrightarrow{\sim} G/Z(G), \qquad \varphi$$

Lift the morphism φ to a map $C : G \to G$ s.t. $\gamma(g) = \iota(C(g))$. Then

$$\begin{aligned} C(g^{C(h)} h) &= C(g^{\iota(C(h))} h) = C(g^{\gamma(h)} h) \\ &= C(g \circ h) = C(g) C(h) \kappa(g, h), \end{aligned}$$

where $\kappa : (G, \circ) \times (G, \circ) \to Z(G)$ is a 2-cocycle, which depends on the choice of C, but whose class in $\mathrm{H}^2((G, \circ), Z(G))$ does not.

Proposition

The following are equivalent.

- *γ comes from a Rota–Baxter operator B, i.e. $\gamma(g) = \iota(B(g))$.*
- *κ is trivial in $\mathrm{H}^2((G, \circ), Z(G))$.*

An example

Let

$$(G, \cdot) = \langle\, u, v, k : u^p, v^p, k^p, [u, v] = k, [u, k], [v, k] \,\rangle.$$

be the Heisenberg group of order p^3, for a prime $p > 2$.

Let $A = G$, and $K = Z(G) = \langle\, k \,\rangle$. Take $\psi \in \mathrm{End}(G/K)$ given by $(gK)^\psi = (gK)^\alpha$, for $\alpha \in \mathbf{Z}/p\mathbf{Z}$. Define $\gamma(g) = \iota(g^\psi)$.

- When $\alpha \neq -1/2$, the gamma function γ comes from the Rota–Baxter operator

$$B(u^i \cdot v^j \cdot k^r) = u^{i\alpha} \cdot v^{j\alpha} \cdot k^{\alpha^2(r-ij\alpha)(1+2\alpha)^{-1}},$$

  for $0 \leq i, j, r < p$.
- When $\alpha = -1/2$, the gamma function $\gamma(g) = \iota(g^\alpha)$ does *not* come from a Rota–Baxter operator. (Here $(G, \circ)$ is abelian: Baer, Lazard, Baker–Campbell–Hausdorff.)

⏩ Skip Baer

Baer

Reinhold Baer

Groups with abelian central quotient group

Trans. Amer. Math. Soc. **44** (1938), no. 3, 357–386

Let G be a group of nilpotence class two admitting unique square roots. Define

$$g \circ h = g \cdot h \cdot [g,h]^{-1/2}.$$

Then $(G, \circ)$ is an abelian group.

⏩ Skip calculation

$$\begin{aligned} h \circ g &= h \cdot g \cdot [h,g]^{-1/2} \\ &= g \cdot h \cdot [h,g] \cdot [h,g]^{-1/2} \\ &= g \cdot h \cdot [h,g]^{1/2} \\ &= g \circ h. \end{aligned}$$

Rota–Baxter operators via Extensions

Consider the standard sequence

$$1 \to Z(G) \to \underbrace{Z(G) \times (G, \circ)}_{\text{set-theoretic product}} \to (G, \circ) \to 1$$

associated to the cocycle κ in $\mathrm{H}^2((G, \circ), Z(G))$. The operation is given by

$$(z_1, g_1)(z_2, g_2) = (z_1 z_2 \kappa(g_1, g_2), g_1 \circ g_2).$$

If the extension does not split, i.e. κ is non-trivial in $\mathrm{H}^2((G, \circ), Z(G))$, we know that γ does not come from a Rota–Baxter operator.

If the extension does split, a complement to $Z(G)$ naturally determines a coboundary $\sigma : G \to Z(G)$, which is the correction to be made to C to obtain a Rota–Baxter operator; recall

$$C(g^{C(h)} h) = C(g) C(h) \kappa(g, h).$$

How do we know if it splits or not?

In the case of the sequence

$$1 \to Z(G) \to \underbrace{Z(G) \times (G, \circ)}_{\text{set-theoretic product}} \to (G, \circ) \to 1,$$

where

$$(G, \cdot) = \langle\, u, v, k : u^p, v^p, k^p, [u, v] = k, [u, k], [v, k] \,\rangle.$$

is the Heisenberg group, one computes

$$[(1, u), (1, v)] = (k^{-\alpha(\alpha+1)}, k^{1+2\alpha}).$$

- If $\alpha = -1/2$ (so that $(G, \circ)$ is abelian) the sequence cannot split, otherwise the extension $Z(G) \times (G, \circ)$ would be abelian;
- if $\alpha \neq -1/2$, the subgroup $\langle\, (1, u), (1, v) \,\rangle$ intersects $Z(G) \times 1$ trivially, and thus it is a complement. The sequence splits (explicitly).

That's All, Thanks!