A Lazard correspondence between post-Lie rings and skew braces

Senne Trappeniers

March 26, 2025

VRIJE UNIVERSITEIT BRUSSEL

Overview

1. The Lazard correspondence between Lie rings and groups.
2. Skew braces and post-Lie rings are the same structures, just living in different worlds.
3. When can we effectively use the Lazard correspondence to travel between these worlds?

Lie rings

Definition

A Lie ring is a triple $(\mathfrak{g}, +, [-,-])$ (henceforth simply denoted by $\mathfrak{g}$) such that $(\mathfrak{g}, +)$ is an abelian group and

$$\mathfrak{g}^2 \to \mathfrak{g} : (x, y) \mapsto [x, y],$$

is a biadditive skew symmetric operation on $\mathfrak{g}$ satisfying the Jacobi identity, i.e. for all $x, y, z \in \mathfrak{g}$:

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

Some Lie theory

Let G be a Lie group and $\mathfrak{g}$ its associated Lie algebra, then the exponential map

$$\exp : \mathfrak{g} \to G$$

restricts to a diffeomorphism of a neighbourhood of $0 \in U \subseteq \mathfrak{g}$ and $1 \in V \subseteq G$. The Baker-Campbell-Hausdorff formula is the formula that locally expresses the group structure of G in terms of $\mathfrak{g}$, i.e. for $x, y \in U$,

$$\exp(x)\exp(y) = \exp(\mathrm{BCH}(x, y)).$$

The BCH formula

The first few terms of the Baker–Campbell–Hausdorff formula are given by

$$\mathrm{BCH}(x, y) = x + y + \frac{1}{2}[x, y] + \frac{1}{12}([x, [x, y]] + [y, [y, x]]) + \dots$$

and ignoring the precise terms appearing we find the following coefficients for the first few degrees:

degree	1	2	3	4	5	6
denominator coefficient	1	2	12	24	720	1440

Lemma

The prime factors appearing in the denominator of the coefficients of degree n *in the BCH formula never exceed* n.

Lazard correspondence

Definition

A filtration on a Lie ring $\mathfrak{g}$ is a descending chain of ideals

$$\mathfrak{g} = \mathfrak{g}_1 \supseteq \mathfrak{g}_2 \supseteq \dots$$

such that $[\mathfrak{g}_i, \mathfrak{g}_j] \subseteq \mathfrak{g}_{i+j}$ for all $i, j \geq 1$.

Definition

A filtered Lie ring $\mathfrak{g}$ is Lazard if

- $\mathfrak{g}_d = 0$ for some $d \geq 1$,
- for all $i, n \geq 1$ such that the prime factors of n are at most i and for all $a \in \mathfrak{g}_i$, there exists a unique $b \in \mathfrak{g}_i$ such that $nb = a$. We write $b = \frac{1}{n}a$.

Lazard correspondence

Theorem (Lazard, 1954)

Let $\mathfrak{g}$ be a Lazard Lie ring and $x, y \in \mathfrak{g}$, then $\mathrm{BCH}(x, y)$ is a well defined element in $\mathfrak{g}$ and moreover $\mathfrak{g}$ is a group for the operation BCH. We denote the resulting group $\mathbf{Laz}(\mathfrak{g})$.

Some observations:

- The neutral element of $\mathbf{Laz}(\mathfrak{g})$ is 0.
- If $x, y \in \mathfrak{g}$ commute, then $\mathrm{BCH}(x, y) = x + y$.
- As a special case of the above, $\mathrm{BCH}(x, x) = 2x$ for all $x \in \mathfrak{g}$ and more generally powers in $\mathbf{Laz}(\mathfrak{g})$ correspond to multiples in $\mathfrak{g}$.

Lazard correspondence

Definition

A filtration on a group G is a descending chain of normal subgroups

$$G = G_1 \supseteq G_2 \supseteq \ldots$$

such that $[G_i, G_j] \subseteq G_{i+j}$ for all $i, j \geq 1$.

Definition

A filtered group G is Lazard if

- $G_d = 1$ for some $d \geq 1$,
- for all $i, n \geq 1$ such that the prime factors of n are at most i and for all $g \in G_i$, there exists a unique $h \in G_i$ such that $h^n = g$.

Lazard correspondence

Theorem (Lazard, 1954)

For every Lazard group G there exists a unique Lazard Lie ring $\mathfrak{g}$ such that $\mathbf{Laz}(\mathfrak{g}) = G$ and such that $\mathfrak{g}_i = G_i$ for all i. In particular, we obtain a correspondence between Lazard Lie rings and Lazard groups.

Some examples of Lazard Lie rings and groups

- A nilpotent Lie algebra $\mathfrak{g}$ over a field of characteristic 0 is Lazard for the filtration coming from its lower central series, i.e.
$$\mathfrak{g}_1 = \mathfrak{g}, \mathfrak{g}_2 = [\mathfrak{g}, \mathfrak{g}], \mathfrak{g}_3 = [\mathfrak{g}, \mathfrak{g}_2], \ldots$$
- A nilpotent (real or complex) Lie group G is Lazard for the filtration coming from its lower central series, i.e.
$$G_1 = G, G_2 = [G, G], G_3 = [G, [G, G]], \ldots$$
- A Lie ring of order p^n for some prime p is Lazard if it is nilpotent of class $< p$, with the filtration coming from its lower central series.
- A group of order p^n for some prime p is Lazard if it is nilpotent of class $< p$, with the filtration coming from its lower central series.

Lazard correspondence for Lie groups

As a special case we obtain:

$$\left\{ \begin{array}{c} \text{finite dimensional} \\ \text{nilpotent real Lie} \\ \text{algebras} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{nilpotent simply} \\ \text{connected real Lie} \\ \text{groups} \end{array} \right\}$$
$$\mathfrak{g} \mapsto \mathbf{Laz}(\mathfrak{g})$$

Moreover, the Lie algebra associated to $\mathbf{Laz}(\mathfrak{g})$ is isomorphic to $\mathfrak{g}$.

Lazard correspondence for finite groups

Let p be a prime and $k < p$. Within the context of finite group theory, the Lazard correspondence is usually meant to refer to the following special case:

$$\left\{ \begin{array}{c} \text{Lie rings of order } p^n \\ \text{and nilpotency class } k \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{groups of order } p^n \text{ and} \\ \text{nilpotency class } k \end{array} \right\}$$
$$\mathfrak{g} \mapsto \mathbf{Laz}(\mathfrak{g})$$

Newman, O'Brien, Vaughan-Lee (2004): classification of groups of order p^6 for $p \geq 5$ through Lie rings.

Skew braces

Definition

A skew (left) brace is a triple $(A, \cdot, \circ)$ with A a set, $(A, \cdot)$ and $(A, \circ)$ group structures, and for all $a, b, c \in A$,

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

with a^{-1} the inverse in $(A, \cdot)$. If $(A, \cdot)$ is abelian, then A is a brace

The holomorph of a group

Let $(A, \cdot)$ be a group. We define the holomorph of $(A, \cdot)$ as the semi-direct product

$$\mathrm{Hol}(A, \cdot) := (A, \cdot) \rtimes \mathrm{Aut}(A, \cdot).$$

So explicitly,

$$(a, \lambda)(b, \rho) = (a \cdot \lambda(b), \lambda\rho).$$

There is a natural action $\star$ of $\mathrm{Hol}(A, \cdot)$ on A, the affine action, given by

$$(a, \lambda) \star b = a \cdot \lambda(b).$$

Skew braces and regular subgroups of the holomorph

Proposition (Bachiller, 2016; Guarnieri, Vendramin, 2017)

Let $(A, \cdot)$ be a group. There exists a bijective correspondence between operations $\circ$ making $(A, \cdot, \circ)$ into a skew brace and regular (=simply transitive) subgroups of $\operatorname{Hol}(A, \cdot)$.

A subgroup G of $\operatorname{Hol}(A, \cdot)$ is regular if and only if every element of A appears precisely once as the first component of an element in G.

Idea of the correspondence

From (B) we obtain a somewhat more symmetric condition by multiplying by a^{-1} on the left

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

If we define $\lambda_a(b) := a^{-1} \cdot (a \circ b)$ then this can be compactly written as

$$\lambda_a(b \cdot c) = \lambda_a(b) \cdot \lambda_a(c).$$

So λ_a is an automorphism of $(A, \cdot)$, for any $a \in A$. The regular subgroup of $\mathrm{Hol}(A, \cdot)$ associated to this skew brace is then

$$G = \{(a, \lambda_a) \mid a \in A\}.$$

Post-Lie rings

Definition

A post-Lie ring is a pair $(\mathfrak{a}, \triangleright)$ with $\mathfrak{a}$ a Lie ring and $\triangleright$ a bilinear operation on $\mathfrak{a}$ satisfying for all $x, y, z \in \mathfrak{a}$:

$$x \triangleright [y, z] = [x \triangleright y, z] + [y, x \triangleright z],$$
$$[x, y] \triangleright z = x \triangleright (y \triangleright z) - (x \triangleright y) \triangleright z - y \triangleright (x \triangleright z) + (y \triangleright x) \triangleright z.$$

Definition

A post-Lie ring $(\mathfrak{a}, \triangleright)$ such that $\mathfrak{a}$ is abelian is a pre-Lie ring. Then the first equation is trivially satisfied and the second simplifies to:

$$x \triangleright (y \triangleright z) - (x \triangleright y) \triangleright z = y \triangleright (x \triangleright z) - (y \triangleright x) \triangleright z.$$

The affine Lie ring

Let $\mathfrak{a}$ be a Lie ring. Recall that an additive map $\delta : \mathfrak{a} \to \mathfrak{a}$ is a *derivation* if for all $a, b \in \mathfrak{a}$:

$$\delta([a,b]) = [\delta(a), b] + [a, \delta(b)].$$

The derivations of $\mathfrak{a}$, denoted $\mathfrak{der}(\mathfrak{a})$, form a Lie ring for the commutator bracket

$$[\delta, \rho] = \delta\rho - \rho\delta.$$

The semi-direct sum $\mathfrak{aff}(\mathfrak{a}) = \mathfrak{a} \oplus \mathfrak{der}(\mathfrak{a})$ is the Lie ring with abelian group $\mathfrak{a} \oplus \mathfrak{der}(\mathfrak{a})$ and bracket

$$[(x,\delta),(y,\rho)] = ([x,y] + \delta(y) - \rho(x), [\delta,\rho]),$$

for $x, y \in \mathfrak{a}$, $\delta, \rho \in \mathfrak{der}(\mathfrak{a})$.

A characterization of post-Lie rings

Proposition (Burde, Dekimpe, Vercammen, 2012)

Let $\mathfrak{a}$ be a Lie ring. There is a bijective correspondence between operations $\triangleright$ such that $(\mathfrak{a}, \triangleright)$ is a post-Lie ring and sub Lie rings $\mathfrak{g}$ of $\mathfrak{aff}(\mathfrak{a}) = \mathfrak{a} \rtimes \mathfrak{Der}(\mathfrak{a})$ such that the projection map

$$\mathfrak{g} \to \mathfrak{a} : (x, \delta) \to x,$$

is a bijection.

Sub Lie rings of $\mathfrak{aff}(\mathfrak{a})$ that satisfy the above condition are called *t*-bijective.

Idea of correspondence

Let $(\mathfrak{a}, \triangleright)$ be a post-Lie ring and let $\mathcal{L}_a$ denote the left multiplications $b \mapsto a \triangleright b$. Then

$$\mathfrak{g} := \{(a, \mathcal{L}_a) \mid a \in \mathfrak{a}\},$$

is its associated t-bijective sub-Lie ring of $\mathfrak{aff}(\mathfrak{a})$.

Something to remember

Skew braces and post-Lie rings are the same structures, just living in different worlds.

Left and strong nilpotency

Definition

A post-Lie ring $(\mathfrak{a}, \triangleright)$ is

- left nilpotent if there exists some n such that $a_1 \triangleright (a_2 \triangleright (\cdots \triangleright (a_{n-1} \triangleright a_n))) = 0$ for all $a_1, \ldots, a_n \in \mathfrak{a}$.
- strongly nilpotent if there exists some n such that every $\triangleright$-product of length n is 0.

Left and strong nilpotency

In a skew brace $(A, \cdot, \circ)$ we define an additional (non-associative) operation

$$a * b := a^{-1} \cdot (a \circ b) \cdot b^{-1} = \lambda_a(b) \cdot b^{-1}.$$

Definition (Incorrect but captures the essence)

A skew brace $(A, \cdot, \circ)$ is

- left nilpotent if there exists some n such that $a_1 * (a_2 * (\cdots * (a_{n-1} * a_n))) = 1$ for all $a_1, \dots, a_n \in A$.
- strongly nilpotent if there exists some n such that every $*$-product of length n is 1.

From skew braces to post-Lie rings

- Auslander (1977): Construction of a pre-Lie algebra starting from a regular affine action of a Lie group on $\mathbb{R}^n$.
- Iyudu (2020): Construction of associated graded pre-Lie ring of strongly nilpotent brace.
- Smoktunowicz (2022): Construction of pre-Lie ring starting from strongly nilpotent brace of order p^n with $n < p - 1$.
- Burde, Dekimpe, Deschamps (2009); Bai, Guo, Sheng, Tang (2023): differentiation of post-Lie group (=skew brace on Lie groups) to obtain post-Lie algebra.

And back

- Agrachev, Gamkrelidze (1981): Construction of group of flows of a complete (≈strongly nilpotent) pre-Lie algebra, which yields a brace structure.
- Smoktunowicz (2022): Construction of a brace starting from a left nilpotent pre-Lie ring of order p^n with $n < p - 1$.
- Bai, Guo, Sheng, Tang (2023): formal integration of complete (≈strongly nilpotent + nilpotent underlying Lie algebra) post-Lie algebras to obtain a skew brace.

The finite case

Theorem (Smoktunowicz, 2022)

Let p be a prime and $k, n < p-1$. There is an (explicit) bijective correspondence

$$\left\{ \begin{array}{c} \text{strongly nilpotent pre-Lie} \\ \text{rings of class at most } k \\ \text{and cardinality } p^n \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{strongly nilpotent braces} \\ \text{of class at most } k \text{ and} \\ \text{cardinality } p^n \end{array} \right\}$$

- How necessary is strong nilpotency?
- To mimic the geometric approach, we ideally would like to relate $\mathfrak{der}(\mathfrak{a})$ and $\mathrm{Aut}(\mathfrak{a}) = \mathrm{Aut}(\mathbf{Laz}(\mathfrak{a}))$, but in general neither are nilpotent, so definitely not Lazard.

A nice Lie ring of derivations

Proposition

Let $\mathfrak{a}$ be a filtered Lie ring, then

$$\mathfrak{der}_f(\mathfrak{a}) := \{\delta \in \mathfrak{der}(\mathfrak{a}) \mid \delta(\mathfrak{a}_i) \subseteq \mathfrak{a}_{i+1} \text{ for all } i \geq 1\},$$

is a filtered Lie ring for the filtration

$$\mathfrak{der}_f(\mathfrak{a})_j := \{\delta \in \mathfrak{der}(\mathfrak{a}) \mid \delta(\mathfrak{a}_i) \subseteq \mathfrak{a}_{i+j} \text{ for all } i \geq 1\}.$$

Moreover, if $\mathfrak{a}$ is Lazard, then so is $\mathfrak{der}_f(\mathfrak{a})$.

A nice group of automorphisms

Proposition

Let A be a filtered group, then

$$\mathrm{Aut}_f(A) = \{\phi \in \mathrm{Aut}(A) \mid \phi(a)a^{-1} \in A_{i+1} \text{ for all } a \in A_i \text{ and } i \geq 1\},$$

is a filtered group for the filtration

$$\mathrm{Aut}_f(A)_j = \{\phi \in \mathrm{Aut}(A) \mid \phi(a)a^{-1} \in A_{i+j} \text{ for all } a \in A_i \text{ and } i \geq 1\}.$$

Moreover, if A is Lazard, then so is $\mathrm{Aut}_f(A)$.

Behaviour under Lazard correspondence

Theorem (T., 2024)

Let $\mathfrak{a}$ be a filtered Lie ring which is Lazard, then

$$\exp : \mathfrak{Der}_f(\mathfrak{a}) \to \mathrm{Aut}_f(\mathbf{Laz}(\mathfrak{a})) : \delta \mapsto \exp(\delta),$$

is a bijection which yields an isomorphism of filtered groups

$$\mathbf{Laz}(\mathfrak{Der}_f(\mathfrak{a})) \cong \mathrm{Aut}_f(\mathbf{Laz}(\mathfrak{a})).$$

Filtered affine Lie ring

Lemma

Let $\mathfrak{a}$ be a filtered Lie ring. The semidirect sum

$$\mathfrak{aff}_f(\mathfrak{a}) := \mathfrak{a} \oplus \mathfrak{der}_f(\mathfrak{a}),$$

is filtered with respect to the filtration

$$\mathfrak{aff}_f(\mathfrak{a})_i = \mathfrak{a}_i \oplus \mathfrak{der}_f(\mathfrak{a})_i.$$

Moreover, if $\mathfrak{a}$ is Lazard, then so is $\mathfrak{aff}_f(\mathfrak{a})$.

Filtered holomorph

Lemma

Let A be a filtered group. The semidirect product

$$\mathrm{Hol}_f(A) := A \rtimes \mathrm{Aut}_f(A),$$

is filtered with respect to the filtration

$$\mathrm{Hol}_f(A)_i := A_i \rtimes \mathrm{Aut}_f(A)_i$$

Moreover, if A is Lazard, then so is $\mathrm{Hol}_f(A)$.

Behaviour under Lazard correspondence

Theorem (T, 2024)

Let $\mathfrak{a}$ be a filtered Lie ring which is Lazard, then the exists an isomorphism of filtered groups

$$\gamma : \mathbf{Laz}(\mathfrak{aff}_f(\mathfrak{a})) \cong \mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a})),$$

The map γ yields a bijective correspondence between $\boldsymbol{t}$-bijective Lazard sub-Lie rings of $\mathfrak{aff}_f(\mathfrak{a})$ and regular Lazard subgroups of $\mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a}))$.

Lazard post-Lie rings and skew braces

Definition

A post-Lie ring $(\mathfrak{a}, \triangleright)$ on a Lazard Lie ring $\mathfrak{a}$ is Lazard if its t-bijective sub Lie ring of $\mathfrak{aff}(\mathfrak{a})$ is a Lazard sub Lie ring of $\mathfrak{aff}_f(\mathfrak{a})$. We define Lazard skew braces in a similar way.

Theorem (T., 2024)

There exists a bijective correspondence between Lazard post-Lie rings and Lazard skew braces.

L-nilpotency

Let $(A, \cdot, \circ)$ be a skew brace and define $L^1(A) = A$ and

$$L^{n+1}(A) = \langle a * b, [a, b] \mid a \in A, b \in L^n(A) \rangle.$$

Proposition

A skew brace $(A, \cdot, \circ)$ with $|A| = p^n$ is Lazard with respect to some filtration on $\mathfrak{a}$ if and only if $L^p(A) = 1$.

Definition

If there exists some k such that $L^{k+1}(A) = \{1\}$, then A is L-nilpotent. If k is minimal, then A is L-nilpotent of class k.

A Lazard correspondence for post-Lie rings and skew braces

Theorem (T., 2024)

Let p be a prime, $n \geq 1$ and $1 \leq k < p$, then there exists a correspondence

$$\left\{ \begin{array}{c} \text{post-Lie rings of order } p^n \\ \text{and } L\text{-nilpotency class} \\ < p \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{skew braces of order } p^n \\ \text{and } L\text{-nilpotency class} \\ < p \end{array} \right\}.$$

which restricts to

$$\left\{ \begin{array}{c} L\text{-nilpotent post-Lie rings} \\ \text{of order } p^k \end{array} \right\} \leftrightarrow \left\{ \text{ skew braces of order } p^k \right\}.$$

Thank you!