Construction of groups associated to Lie- and to Leibniz-algebras

Manon Didry

Institut Elie Cartan - U.M.R. 7502
Université Henri Poincaré (Nancy I)
B.P.239
54506 Vandœuvre-lès-Nancy Cedex
France
e-mail: didrym@iecn.u-nancy.fr

Abstract

We describe a method for associating to a Lie algebra $\mathfrak{g}$ over a ring $\mathbb{K}$ a sequence of groups $(G_n(\mathfrak{g}))_{n\in\mathbb{N}}$, which are *polynomial groups* in the sense of [1]. Using a description of these groups by generators and relations, we prove the existence of an action of the symmetric group Σ_n by automorphisms. The subgroup of fixed points under this action, denoted by $J_n(\mathfrak{g})$, is still a polynomial group and we can form the projective limit $J_\infty(\mathfrak{g})$ of the sequence $(J_n(\mathfrak{g}))_{n\in\mathbb{N}}$. The formal group $J_\infty(\mathfrak{g})$ associated in this way to the Lie algebra $\mathfrak{g}$ may be seen as a generalisation of the formal group associated to a Lie algebra over a field of characteristic zero by the Campbell-Haussdorf formula.

AMS subject classification : 17B65, 14L05.

Keywords : Lie algebra, Leibniz algebra, polynomial group, formal group, exponential map, Campbell-Haussdorf formula, dual numbers.

1 Introduction and presentation of results

In this work, we provide a method to associate to each Lie algebra $\mathfrak{g}$ (over a field or a ring $\mathbb{K}$) a family of groups $(G_n(\mathfrak{g}))_{n\in\mathbb{N}}$. If $\mathbb{K}$ is a field of characteristic zero, then $G_n(\mathfrak{g})$ is essentially isomorphic to the polynomial group obtained by truncating the Campbell-Haussdorf formula in degree n. However, our approach is much simpler from a combinatorial point of view and, in addition, it has the advantage of being valid in arbitrary characteristic.

Let us introduce some notations and definitions in order to state the results.

The letter $\mathbb{K}$ denotes a commutative ring with unit, and the quotient ring $\mathbb{K}[x]/(x^2)$ is denoted by $T\mathbb{K}$. This ring is also called the ring of dual numbers over $\mathbb{K}$, which is the algebraic model of the "tangent bundle of $\mathbb{K}$", given by $\mathbb{K}[\varepsilon] = \mathbb{K} \oplus \varepsilon\mathbb{K}$ with $\varepsilon^2 = 0$: the product is described by

$$(x + \varepsilon x')(y + \varepsilon y') = xy + \varepsilon(xy' + x'y).$$

Define by induction on n the ring $T^n\mathbb{K} := T(T^{n-1}\mathbb{K})$. This ring may be described by n generators $\varepsilon_1, \ldots, \varepsilon_n$ satisfying the relations $\varepsilon_i\varepsilon_j = \varepsilon_j\varepsilon_i$ and $\varepsilon_i^2 = 0$ for all i, j. These elements are called *infinitesimal units.*

It is then obvious that

$$T^n\mathbb{K} = \mathbb{K} \oplus \bigoplus_{\alpha\in I_n} \varepsilon^\alpha\mathbb{K},$$

where we use the following multi-index notation: the symbol I_n denotes the set of non-zero multi-indices of order n, taking values in $\{0, 1\}$:

$$I_n = \{0, 1\}^n \setminus \{(0, \ldots, 0)\}.$$

For each $\alpha \in I_n$, the symbol ε^α denotes the infinitesimal number $\prod_{i=1}^n \varepsilon_i^{\alpha_i}$.

Similarly, if $\mathfrak{g}$ is a $\mathbb{K}$-module, the extension of $\mathfrak{g}$ by the ring $T^n\mathbb{K}$ is given by

$$\mathfrak{g} \otimes_{\mathbb{K}} T^n\mathbb{K} = \mathfrak{g} \oplus G_n(\mathfrak{g}),$$

where

$$G_n(\mathfrak{g}) := \bigoplus_{\alpha\in I_n} \varepsilon^\alpha\mathfrak{g}$$

is the kernel of the projection of $\mathfrak{g} \otimes_{\mathbb{K}} T^n\mathbb{K}$ onto $\mathfrak{g}$.

If $\mathfrak{g}$ is endowed with a structure of an algebra over $\mathbb{K}$, the module $\mathfrak{g}\otimes_{\mathbb{K}} T^n\mathbb{K}$ inherits an algebra structure over $T^n\mathbb{K}$. The set $G_n(\mathfrak{g})$ is then an ideal, called the augmentation ideal of this extension. In particular, $G_n(\mathfrak{g})$ is endowed with a structure of nilpotent algebra.

We consider on the set I_n the lexicographic ordering: explicitly, $(\alpha_i) < (\beta_i)$ if and only if there exists $j \in \{1, \ldots, n\}$ such that $\alpha_i = \beta_i$ for all $i < j$ and $\alpha_j < \beta_j$. For instance, in the set I_3,

$$(001) < (010) < (011) < (100) < (101) < (110) < (111).$$

Let α be in I_n. The length $\sum_{i=1}^n \alpha_i$ of the multi-index α is denoted by $|\alpha|$. For an integer $m \in \{2, \ldots, |\alpha|\}$, $P^m(\alpha)$ stands for the set of increasing partitions (for the lexicographic ordering) in m subsets of the multi-index α :

$$P^m(\alpha) = \{(\lambda^1, \ldots, \lambda^m) \in I_n^m | \alpha = \sum_{i=1}^{m} \lambda^i, \lambda^1 < \ldots < \lambda^m\}.$$

For instance,

$$P^2(111) = \{(001, 110), (010, 101), (011, 100)\}.$$

At this point, we can state the following theorem.

Theorem A (The group structure). *Assume that $\mathfrak{g}$ is endowed with a structure of Lie algebra over $\mathbb{K}$, with bracket denoted by $[.,.]$. Then the set $G_n(\mathfrak{g})$ carries a group structure whose product is given by the formula*

$$\sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha \cdot \sum_{\alpha \in I_n} \varepsilon^\alpha y_\alpha = \sum_{\alpha \in I_n} \varepsilon^\alpha (x \cdot y)_\alpha$$

with

$$(x \cdot y)_\alpha = x_\alpha + y_\alpha + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} [\ldots[[x_{\lambda^m}, y_{\lambda^1}], y_{\lambda^2}], \ldots y_{\lambda^{m-1}}]. \tag{1}$$

The unit element of this group is 0 *and the inverse of an element* $x = \sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha$ *is* $x^{-1} = \sum_{\alpha \in I_n} \varepsilon^\alpha (x^{-1})_\alpha$*, where*

$$(x^{-1})_\alpha = -x_\alpha + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \ldots x_{\lambda^1}]. \tag{2}$$

Finally, the map associating the group $(G_n(\mathfrak{g}), \cdot)$ to the Lie algebra $(\mathfrak{g}, [.,.])$ is functorial.

One of the properties satisfied by this product is that each element of $G_n(\mathfrak{g})$ can be uniquely written as a strictly increasing product of pure elements (a pure element is of type $\varepsilon^\alpha x$, with $x \neq 0$). This point is crucial in the proof of the associativity, and the existence of an inverse follows immediately.

Theorem A can be seen as an "integration theorem", comparable to the theorem which associates to every Lie algebra over a field of characteristic zero a formal group (see [4], [10]). Conversely, a result of "differentiation" has been proved in [1], where the formulae (1) and (2) have been introduced in order to describe the structure of the iterated tangent group $T^n G = T(T^{n-1}G)$ of a Lie group G, respectively the structure of its n-jet $J^n G$ (see below, Theorem C).

Next, we prove that the relations

$$\varepsilon^\alpha x \cdot \varepsilon^\alpha y = \varepsilon^\alpha (x + y)$$

(i.e., the "axis" $\varepsilon^\alpha \mathfrak{g}$ is an abelian subgroup) and

$$\varepsilon^\alpha x \cdot \varepsilon^\beta y = \varepsilon^\beta y \cdot \varepsilon^\alpha x \cdot \varepsilon^\alpha \varepsilon^\beta [x, y] \tag{3}$$

(commutation relation), satisfied for all pairs (x, y) of elements of $G_n(\mathfrak{g})$ and for all multi-indices $\alpha, \beta \in I_n$, characterize the group structure of $G_n(\mathfrak{g})$. Note that the commutation relation can be written, using the commutator of two elements of the group, in the following way :

$$[\varepsilon^\alpha x, \varepsilon^\beta y] = \begin{cases} \varepsilon^{\alpha+\beta}[x, y] \text{ if } \alpha + \beta \in I_n \\ 0 \text{ otherwise.} \end{cases}$$

We thus obtain a description of the group $G_n(\mathfrak{g})$ by generators and relations.

Theorem B (Generators and relations). *Under the assumptions of Theorem A, the group $G_n(\mathfrak{g})$ is defined by the family of generators $I = I_n \times \mathfrak{g}$ and the following relations, with $\alpha, \beta \in I_n$, $x, y \in \mathfrak{g}$:*

- $(\alpha, 0)$,
- $(\alpha, x + y)(\alpha, x)^{-1}(\alpha, y)^{-1}$,
- $(\alpha, x)(\beta, y)(\alpha, x)^{-1}(\beta, y)^{-1}$ *if* $\alpha + \beta \notin I_n$,
- $(\alpha, x)(\beta, y)(\alpha + \beta, [x, y])^{-1}(\alpha, x)^{-1}(\beta, y)^{-1}$ *if* $\alpha + \beta \in I_n$.

This description gives rise to a natural action of the n-th order symmetric group on $G_n(\mathfrak{g})$.

Theorem C (Action of the permutation group). *Under the assumptions of Theorem A, the symmetric group Σ_n acts by automorphisms on the group $G_n(\mathfrak{g})$.*

1. *If $x = \prod_{i=1}^k \varepsilon^{\alpha_i} x_i$ is an element of $G_n(\mathfrak{g})$, written as a strictly increasing product of pure elements, the action of the symmetric group is given by the formula*
$$\sigma.x = \prod_{i=1}^k \varepsilon^{\sigma.\alpha_i} x_i.$$

2. *The subgroup of fixed points under this action is*
$$J_n(\mathfrak{g}) = \bigoplus_{i=1}^n \delta^{(i)} \mathfrak{g},$$
where $\delta^{(i)} = \sum_{\alpha, |\alpha| = i} \varepsilon^\alpha$.

However, the group structure of $J_n(\mathfrak{g})$ is complicated, and we content ourselves with the calculation of first terms.

The nature of the action of Σ_n is more subtle than one might think at a first glance: of course, there is an action of Σ_n on the ring $T^n(\mathbb{K})$ by automorphisms, and hence a canonical $\mathbb{K}$-linear action on $G_n(\mathfrak{g})$, but this is not the action we consider here (except for the case when $\mathfrak{g}$ is abelian). For instance, if $k=2$, the action of the transposition $(1,2)$ is given by the "flip automorphism":

$$(1,2)(\varepsilon^{01}x_{01}+\varepsilon^{10}x_{10}+\varepsilon^{11}x_{11}) = \varepsilon^{01}x_{10}+\varepsilon^{10}x_{01}+\varepsilon^{11}(x_{11}+[x_{01},x_{10}]).$$

Note that this action is not $\mathbb{K}$-linear since it contains a "bilinear term". Nevertheless, by Dot 2 of Theorem C, the action we consider has the same fixed point set as the "canonical" action.

Lastly, we exploit the fact that the group structure obtained on $G_n(\mathfrak{g})$ is a polynomial group structure. The Lie algebra associated to this polynomial group is the natural algebra structure induced by the Lie algebra $\mathfrak{g}$ we started with.

Then we establish that we can form the projective limit $G_\infty(\mathfrak{g})$ of the polynomial group sequence $(G_n(\mathfrak{g}))$. The projective system that we consider is compatible with the action of the symmetric group. Consequently, taking the projective limit of the subgroups $J_n(\mathfrak{g})$, we obtain a subgroup of $G_\infty(\mathfrak{g})$, denoted by $J_\infty(\mathfrak{g})$. The structure of this group is simpler than the one of $G_\infty(\mathfrak{g})$: this group is identified with a formal series module. Hence it may be seen as a formal group associated to the Lie algebra $\mathfrak{g}$. The map sending the Lie algebra $\mathfrak{g}$ to this formal group is functorial. We then study the connection between this functor and the one which associates the formal group given by the Campbell-Haussdorf formula to a Lie algebra over a field of characteristic zero (section 5.3).

To this end, we use general results on polynomial groups described in [1]. Assuming $\mathbb{K}$ to be a field, we obtain a polynomial and canonical exponential map

$$\exp_n : G_n(\mathfrak{g}) \longrightarrow G_n(\mathfrak{g})$$

and an inverse map $\log_n$. We then establish that the product

$$x \star y = \log_n(\exp_n(x)\cdot\exp_n(y))$$

is given by the Campbell-Haussdorf formula for the Lie bracket described above.

Some of these results are still true in a more general framework. Let us recall that a *Leibniz algebra* ([7]) is a $\mathbb{K}$-module $\mathfrak{g}$ endowed with a bilinear map $[.,.] : \mathfrak{g}\times\mathfrak{g} \longrightarrow \mathfrak{g}$ such that the Leibniz identity

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

is satisfied for all triples (x,y,z) in $\mathfrak{g}$. This condition is equivalent to the fact that the maps $ad(z) : x \longmapsto [x,z]$ are derivations of the bracket, for all $z\in\mathfrak{g}$.

Note that if the bracket is antisymmetric, the Leibniz identity is equivalent to the Jacobi identity, which proves that every Lie algebra is a Leibniz algebra.

Now assume that $\mathfrak{g}$ is a Leibniz algebra. We show that the set $G_n(\mathfrak{g})$ is still endowed with a group structure (see Theorem 1 below). Nevertheless, the commutation relation (3) does no longer hold in this group. Consequently, the group can not be presented by the same generators and relations. In this case, it seems to be more difficult to identify an action of the symmetric group.

However, the group $G_n(\mathfrak{g})$, as a polynomial one, gives rise to a Lie algebra described by

$$[\sum_{\alpha\in I_n} \varepsilon^\alpha x_\alpha, \sum_{\alpha\in I_n} \varepsilon^\alpha y_\alpha] = \sum_{\alpha>\beta} \varepsilon^\alpha \varepsilon^\beta ([x_\alpha, y_\beta] - [y_\alpha, x_\beta]).$$

This provides a functor from the category of Leibniz algebras to the category of Lie algebras.

We mention some further topics and problems related to this work.

First, a natural question is to study the case of *Lie triple systems*, as a generalisation of the preceding case. Indeed, every Lie algebra can be seen as a Lie triple system, as every Lie group can be seen as a symmetric space. Thus we can ask if such a construction can be done starting from a Lie triple system, namely can we associate to every Lie triple system a “polynomial symmetric space” ?

Using the standard embedding of Lie triple systems, we will show in [5] that if $\mathfrak{q}$ denotes a Lie triple system over the ring $\mathbb{K}$, the augmentation ideal $G_n(\mathfrak{q})$ of $\mathfrak{q}$ by the ring $T^n\mathbb{K}$ can be endowed with a reflection space structure ([8]), i.e. with a product μ satisfying the following relations:

- $\mu(x, x) = x$,
- $\mu(x, \mu(x, y)) = y$
- $\mu(x, \mu(y, z)) = \mu(\mu(x, y), \mu(x, z))$.

Furthermore, we check that

$$\mu(0, x) = -x$$

and thus, $G_n(\mathfrak{q})$ is endowed with a “symmetric space” structure, which is polynomial, in a natural way (Theorem 3).

Lastly, it remains to point out the functoriality of this construction.

The results presented in this paper are part of the author’s PHD thesis [5], supervised by Pr. Wolfgang Bertram.

Notation: Throughout the text, $\mathbb{K}$ denotes a commutative ring with unit and $\mathfrak{g}$ denotes a module over $\mathbb{K}$. We keep definitions and notations introduced above.

2 Proof of Theorem A

As mentioned above, Theorem A is still valid in a more general framework. Thus we will prove the following theorem.

Theorem 1. *Let $\mathfrak{g}$ be a Leibniz algebra over $\mathbb{K}$, with bracket denoted by $[.,.]$. Then the formula (1) defines a group structure on the set $G_n(\mathfrak{g})$.*

Let us write out these group structures in the cases $n = 1, 2, 3$. The group structure of $G_1(\mathfrak{g}) = \mathfrak{g}$ is the vector group structure: for $x, y \in \mathfrak{g}$,

$$x \cdot y = x + y.$$

For all pairs (x, y) of elements of $G_2(\mathfrak{g})$, if $x = \varepsilon^{01}x_{01} + \varepsilon^{10}x_{10} + \varepsilon^{11}x_{11}$ and $y = \varepsilon^{01}y_{01} + \varepsilon^{10}y_{10} + \varepsilon^{11}y_{11}$, we have

$$x \cdot y = \varepsilon^{01}(x_{01} + y_{01}) + \varepsilon^{10}(x_{10} + y_{10}) + \varepsilon^{11}(x_{11} + y_{11} + [x_{10}, y_{01}]).$$

If $n = 3$, for elements $x = \sum_{\alpha\in I_3} \varepsilon^\alpha x_\alpha$ and $y = \sum_{\alpha\in I_3} \varepsilon^\alpha y_\alpha$ of $G_3(\mathfrak{g})$, we get

$$x \cdot y = \sum_{\alpha\in I_3} \varepsilon^\alpha (x \cdot y)_\alpha$$

with, for instance,

$$(x\cdot y)_{111} = x_{111}+y_{111}+[x_{110}, y_{001}]+[x_{101}, y_{010}]+[x_{100}, y_{011}]+[[x_{100}, y_{001}], y_{010}].$$

In order to prove Theorem 1, we assume that the module $\mathfrak{g}$ is a Leibniz algebra over $\mathbb{K}$.

First, let us give the following definition and state some remarks.

Definition 1. *A pure element of $G_n(\mathfrak{g})$ is an element of type $\varepsilon^\alpha x$, with $x \neq 0$. The set of pure elements of $G_n(\mathfrak{g})$ is denoted by $\mathcal{P}_n(\mathfrak{g})$.*

Remark 1. *For all $z \in G_n(\mathfrak{g})$, the map $x \longmapsto x \cdot z - z$ is linear over $\mathbb{K}$.*

Remark 2. *Let $\varepsilon^\alpha x, \varepsilon^\beta y$ be two pure elements of $G_n(\mathfrak{g})$. If $\alpha \le \beta$, then*

$$\varepsilon^\alpha x \cdot \varepsilon^\beta y = \varepsilon^\alpha x + \varepsilon^\beta y.$$

Using these remarks, we obtain the following lemma.

Lemma 1. *For all $x \in G_n(\mathfrak{g})$, there exists a unique sequence of pure elements $(\varepsilon^{\alpha_i} x_i)_{i\in\{1,\dots,k\}}$, with $(\alpha_i)_{i\in\{1,\dots,k\}}$ strictly increasing, such that*

$$x = ((\dots(\varepsilon^{\alpha_1}x_1 \cdot \varepsilon^{\alpha_2}x_2) \cdot \dots) \cdot \varepsilon^{\alpha_k}x_k).$$

More precisely, if $(\theta_i)_{i\in\{1,\dots,2^n-1\}}$ denotes the strictly increasing sequence of elements of I_n,

$$\Sigma_{i=1}^{2^n-1}\varepsilon^{\theta_i}x_i = \prod_{i, x_i\neq 0} \varepsilon^{\theta_i}x_i,$$

where we use the notation $\prod_{i=1}^k \varepsilon^{\alpha_i}y_i = ((\dots(\varepsilon^{\alpha_1}y_1 \cdot \varepsilon^{\alpha_2}y_2) \cdot \dots) \cdot \varepsilon^{\alpha_k}y_k)$.

Proof. The proof is by induction on the number l of indices i for which $x_i \neq 0$. The case $l = 1$ is obvious. The following calculation provides the heredity property : if $(\alpha_i)_{i\in\{1,\ldots,k\}} \in (I_n)^k$ and $\beta > \alpha_i$ for all $i \in \{1,\ldots,k\}$, we obtain, using Remarks 1 et 2,

$$\begin{aligned}(\sum_{i=1}^{k} \varepsilon^{\alpha_i} x_i) \cdot \varepsilon^{\beta} x &= \sum_{i=1}^{n} \varepsilon^{\alpha_i} x_i \cdot \varepsilon^{\beta} x - (k-1)\varepsilon^{\beta} x \\ &= \sum_{i=1}^{n} (\varepsilon^{\alpha_i} x_i + \varepsilon^{\beta} x) - (k-1)\varepsilon^{\beta} x \\ &= \sum_{i=1}^{n} \varepsilon^{\alpha_i} x_i + \varepsilon^{\beta} x.\end{aligned}$$

□

Definition 2. *The length of an element x of $G_n(\mathfrak{g})$ is the number of pure elements involved in the decomposition of x as a strictly increasing product of pure elements.*

Let us check the associativity of the product. The aim is to establish the equality

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

for all triples (x, y, z) of elements of $G_n(\mathfrak{g})$. The proof is by induction on the length of the element z.

If the result is true for elements z of length k and for pure elements x and y, then the following calculation, where z is of length k and z' is pure, proves that the result is true for elements of length $k + 1$:

$$\begin{aligned}(x \cdot y) \cdot (z \cdot z') &= ((x \cdot y) \cdot z) \cdot z' \\ &= (x \cdot (y \cdot z)) \cdot z' \\ &= x \cdot ((y \cdot z) \cdot z') \\ &= x \cdot (y \cdot (z \cdot z')).\end{aligned}$$

Thus, in order to prove associativity, it remains to prove :

Lemma 2. *Let x, y, z be three elements in $G_n(\mathfrak{g})$. If z is pure, then*

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

Proof. Let $x = \sum_{\alpha\in I_n} \varepsilon^{\alpha} x_{\alpha}$, $y = \sum_{\alpha\in I_n} \varepsilon^{\alpha} y_{\alpha}$ and $z = \sum_{\alpha\in I_n} \varepsilon^{\alpha} z_{\alpha}$ be three elements in $G_n(\mathfrak{g})$. Assume z is pure: there exists $\theta \in I_n$ such that $z_{\alpha} = 0$ for all multi-indices α different from θ, $z_{\theta} \neq 0$.

We denote by A_{α} the expression $(x \cdot (y \cdot z))_{\alpha} - ((x \cdot y) \cdot z)_{\alpha}$. The lemma will be proved if we check that this expression is zero for all multi-indices α.

Let $\alpha \in I_n$. Then

$$\begin{aligned} A_\alpha &= \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} ([[y_{\lambda^m}, z_{\lambda^1}], \dots z_{\lambda^{m-1}}] + [[x_{\lambda^m}, yz_{\lambda^1}] \dots yz_{\lambda^{m-1}}] \\ & -[[xy_{\lambda^m}, z_{\lambda^1}], \dots z_{\lambda^{m-1}}] - [[x_{\lambda^m}, y_{\lambda^1}], \dots, y_{\lambda^{m-1}}]), \end{aligned}$$

and this expression can be further expanded into a sum of iterated brackets in elements of type $x_{\lambda_i}, y_{\lambda_i}, z_{\lambda_i}$, with $i \in \{1, \dots, m\}$, $m \in \{1, \dots, |\alpha|\}$, and $\lambda \in P^m(\alpha)$.

More precisely, after having carried out this development (and noticed that the bracket $[[y_{\lambda^m}, z_{\lambda^1}], \dots z_{\lambda^{m-1}}]$ reduces with the development of the bracket $[[xy_{\lambda^m}, z_{\lambda^1}], \dots z_{\lambda^{m-1}}]$), we obtain

$$A_\alpha = \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} C^\alpha(m, \lambda),$$

where $C^\alpha(m, \lambda)$ denotes the sum of iterated brackets in m arguments in A_α, involving m elements of the set

$$\{x_{\lambda^m}, y_{\lambda^1}, \dots, y_{\lambda^{m-1}}, z_\theta\}.$$

At this point, we show by induction on $|\alpha|$ that $C^\alpha(m, \lambda) = 0$ for all $m \in \{2, \dots, |\alpha|\}$, $\lambda \in P^m(\alpha)$.

If $|\alpha| = 2$, then $m = 2$.We thus get for $\lambda \in P^2(\alpha)$

$$\begin{aligned} C^\alpha(m, \lambda) &= [x_{\lambda^2}, y_{\lambda^1}] + [x_{\lambda^2}, z_{\lambda^1}] - [x_{\lambda^2}, z_{\lambda^1}] - [x_{\lambda^2}, y_{\lambda^1}] \\ &= 0. \end{aligned}$$

Assume now that the property is true for all multi-indices of length lower than or equal to r. Let α be a multi-index of length $r + 1$, $m \in \{2, \dots, r + 1\}$, $\lambda \in P^m(\alpha)$.

Suppose first that for all $i \in \{1, \dots, m - 1\}$, λ^i is distinct from θ. Then

$$\begin{aligned} C^\alpha(m, \lambda) &= [[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-1}}] - [[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-1}}] \\ &= 0. \end{aligned}$$

Conversely, assume there exists $i \in \{1, \dots, m - 1\}$ such that $\lambda^i = \theta$. We distinguish two cases.

If $i = m - 1$,

$$\begin{aligned} C^\alpha(m, \lambda) &= [[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-1}}] + [[[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-2}}], z_\theta] \\ & -[[[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-2}}], z_\theta] - [[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-1}}] \\ &= 0. \end{aligned}$$

Assume now $i \neq m-1$. We introduce the following notation: for fixed i_0, i_1, and for $X \in \mathfrak{g}$, let

$$[X, y_{\lambda^{i_0<k<i_1}}] = [[[X, y_{\lambda^{i_0+1}}], y_{\lambda^{i_0+2}}]], \dots y_{\lambda^{i_1-1}}].$$

Then

$$\begin{aligned}
C^\alpha(m,\lambda) &= [[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-1}}] + [[x_{\lambda^m}, y_{\lambda^{k<i}}], z_\theta], y_{\lambda^{i<k}}] \\
&\quad -[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k}}], z_\theta] - [[x_{\lambda^m}, y_{\lambda^1}], \dots y_{\lambda^{m-1}}] \\
&\quad + \sum_{j=i+1}^{m-1} [[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<j}}], [y_{\lambda^j}, z_\theta]], y_{\lambda^{j<k}}] \\
&= [[[x_{\lambda^m}, y_{\lambda^{k<i}}], z_\theta], y_{\lambda^{i<k}}] - [[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k}}], z_\theta] \\
&\quad + \sum_{j=i+1}^{m-1} [[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<j}}], [y_{\lambda^j}, z_\theta]], y_{\lambda^{j<k}}].
\end{aligned}$$

We consider the multi-index $\alpha' = \alpha - \lambda^{m-1}$ and we denote by λ' the partition $(\lambda^1, \dots, \lambda^{m-2}, \lambda^m)$ of α'.

We thus get, similarly to the former computation,

$$\begin{aligned}
C^{\alpha'}(m-1,\lambda') &= [[x_{\lambda^m}, y_{\lambda^{k<i}}], z_\theta], y_{\lambda^{i<k<m-1}}] - [[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<m-1}}], z_\theta] \\
&\quad + \sum_{j=i+1}^{m-2} [[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<j}}], [y_{\lambda^j}, z_\theta]], y_{\lambda^{j<k}}].
\end{aligned}$$

Let us introduce the expression

$$\begin{aligned}
B &= [[[x_{\lambda^m}, y_{\lambda^{k<i}}], z_\theta] y_{\lambda^{i<k<m}}] \\
&\quad + \sum_{j=i+1}^{m-2} [[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<j}}], [y_{\lambda^j}, z_\theta]], y_{\lambda^{j<k<m-1}}].
\end{aligned}$$

Then

$$\begin{aligned}
B &= C^{\alpha'}(m-1,\lambda') + [[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<m-1}}], z_\theta] \\
&= [[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<m-1}}], z_\theta],
\end{aligned}$$

where we used the induction hypothesis, $C^{\alpha'}(m-1,\lambda') = 0$.

Moreover

$$\begin{aligned}
C^\alpha(m,\lambda) &= [B, y_{\lambda^{m-1}}] - [[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k}}], z_\theta] \\
&\quad +[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<m-1}}], [y_{\lambda^{m-1}}, z_\theta]],
\end{aligned}$$

hence, using that $[., z_\theta]$ is a bracket derivation,

$$\begin{aligned}
C^\alpha(m,\lambda) &= [[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<m-1}}], z_\theta]], y_{\lambda^{m-1}}] \\
&\quad -[[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<m-1}}], y_{\lambda^{m-1}}], z_\theta] \\
&\quad +[[[x_{\lambda^m}, y_{\lambda^{k<i}}], y_{\lambda^{i<k<m-1}}], [y_{\lambda^{m-1}}, z_\theta]] \\
&= 0.
\end{aligned}$$

This calculation achieves induction and establishes associativity. ☐

The proof of the existence of an inverse is based on the following remark.

Remark 3. *For all pure elements $x = \varepsilon^{\alpha} x_{\alpha}$, we have*

$$\varepsilon^{\alpha} x_{\alpha} \cdot \varepsilon^{\alpha}(-x_{\alpha}) = \varepsilon^{\alpha}(-x_{\alpha}) \cdot \varepsilon^{\alpha} x_{\alpha} = 0.$$

Consequently, every pure element is invertible and the inverse of $x = \varepsilon^{\alpha} x_{\alpha}$ is given by $x^{-1} = \varepsilon^{\alpha}(-x_{\alpha})$.

It follows immediately that the inverse of any element $x = x_1 \cdot x_2 \cdot \ldots \cdot x_n$ of $G_n(\mathfrak{g})$, written as a strictly increasing product of pure elements $(x_1, \ldots, x_n)$, is given by

$$x^{-1} = x_n^{-1} \cdot \ldots \cdot x_1^{-1}.$$

Finally, we have shown that the product defined by (1) endows the set $G_n(\mathfrak{g})$ with a group structure.

Let us prove the explicit formula for the inverse of an element.

Proposition 1. *The inverse of an element $x = \sum_{\alpha \in I_n} \varepsilon^{\alpha} x_{\alpha}$ of $G_n(\mathfrak{g})$ is given by $x^{-1} = \sum_{\alpha \in I_n} \varepsilon^{\alpha} (x^{-1})_{\alpha}$ where*

$$(x^{-1})_{\alpha} = -x_{\alpha} + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \ldots x_{\lambda^1}].$$

Proof. The result is true for x of length 1. Assume the result is true for all x of length k. Let x be of length $k+1$. There exist a strictly increasing sequence $(\alpha_1, \ldots, \alpha_{k+1})$ of multi-indices and some non-zero elements $x_{\alpha_1}, \ldots, x_{\alpha_{k+1}}$ of the Leibniz algebra $\mathfrak{g}$ such that

$$x = \varepsilon^{\alpha_1} x_{\alpha_1} \cdot \ldots \cdot \varepsilon^{\alpha_{k+1}} x_{\alpha_{k+1}}.$$

We denote by y the element $\varepsilon^{\alpha_1} x_{\alpha_1}$ and by z the element $\varepsilon^{\alpha_2} x_{\alpha_2} \cdot \ldots \cdot \varepsilon^{\alpha_{k+1}} x_{\alpha_{k+1}}$. We thus obtain $x = y \cdot z$ where $y = \sum_{\alpha \in I_n} \varepsilon^{\alpha} y_{\alpha}$ is a pure element ($y_{\alpha} = x_{\alpha}$ if $\alpha = \alpha_1$, $y_{\alpha} = 0$ otherwise) and $z = \sum_{\alpha \in I_n} \varepsilon^{\alpha} z_{\alpha}$ is of length k ($z_{\alpha} = x_{\alpha}$ if $\alpha = \alpha_k$ with $k > 1$, $z_{\alpha} = 0$ otherwise).

Using the induction hypothesis, we get $z^{-1} = \sum_{\alpha \in I_n} \varepsilon^{\alpha} (z^{-1})_{\alpha}$ with

$$(z^{-1})_{\alpha} = -z_{\alpha} + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} (-1)^m [[z_{\lambda^m}, z_{\lambda^{m-1}}], \ldots z_{\lambda^1}].$$

Remark that if $\alpha - \alpha_1 \notin \{0,1\}^n$, then

$$(z^{-1})_{\alpha} = -x_{\alpha} + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \ldots x_{\lambda^1}],$$

and if $\alpha - \alpha_1 \in I_n$, then

$$(z^{-1})_\alpha = -x_\alpha + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha), \lambda^i \neq \alpha_1} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \dots x_{\lambda^1}].$$

Let $\alpha \in I_n$. We obtain

$$\begin{aligned}
(x^{-1})_\alpha &= (z^{-1} \cdot y^{-1})_\alpha \\
&= (z^{-1})_\alpha + (y^{-1})_\alpha \\
&\quad + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} (-1)^m [[(z^{-1})_{\lambda^m}, (y^{-1})_{\lambda^1}], \dots (y^{-1})_{\lambda^{m-1}}]
\end{aligned}$$

Moreover, we know that y^{-1} is the pure element $-\varepsilon^{\alpha_1} x_1$. We distinguish three cases.

If $\alpha = \alpha_1$, then

$$\begin{aligned}
(x^{-1})_\alpha &= (y^{-1})_{\alpha_1} \\
&= -x_{\alpha_1}.
\end{aligned}$$

If $\alpha - \alpha_1 \notin I_n$ and $\alpha \neq \alpha_1$, then

$$\begin{aligned}
(x^{-1})_\alpha &= (z^{-1})_\alpha \\
&= -x_\alpha + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \dots x_{\lambda^1}].
\end{aligned}$$

Assume now $\alpha - \alpha_1 \in I_n$. We denote by β the multi-index such that $(\alpha_1, \beta) \in P^2(\alpha)$. We notice that $|\alpha| = |\beta| + |\alpha_1|$.

Therefore

$$\begin{array}{rcl}
(x^{-1})_\alpha & = & (z^{-1})_\alpha + [(z^{-1})_\beta, (y^{-1})_{\alpha_1}] \\
& = & (z^{-1})_\alpha - [(z^{-1})_\beta, x_{\alpha_1}] \\
& = & -x_\alpha + \displaystyle\sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha), \lambda^i \neq \alpha_1} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \dots x_{\lambda^1}] \\
& & +[x_\beta, x_{\alpha_1}] - \displaystyle\sum_{m=2}^{|\beta|} \sum_{\lambda \in P^m(\beta)} (-1)^m [[[x_{\lambda^m}, x_{\lambda^{m-1}}], \dots, x_{\lambda^1}], x_{\alpha_1}] \\
& = & -x_\alpha + \displaystyle\sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha), \lambda^1 \neq \alpha_1} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \dots x_{\lambda^1}] \\
& & + \displaystyle\sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha), \lambda^1 = \alpha_1} (-1)^m [[[x_{\lambda^m}, x_{\lambda^{m-1}}], \dots x_{\lambda^1}] \\
& = & -x_\alpha + \displaystyle\sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} (-1)^m [[x_{\lambda^m}, x_{\lambda^{m-1}}], \dots x_{\lambda^1}].
\end{array}$$

At last, we have shown that the inverse formula holds for all elements of length $k+1$, which achieves the induction.

□

Now, we investigate the functoriality of the construction.

Let $f : \mathfrak{g} \longrightarrow \mathfrak{h}$ be a Leibniz algebra morphism. We claim that the map

$$\begin{array}{rccc}
\widetilde{f}: & G_n(\mathfrak{g}) & \longrightarrow & G_n(\mathfrak{h}) \\
& \sum \varepsilon^\alpha x_\alpha & \longmapsto & \sum \varepsilon^\alpha f(x_\alpha),
\end{array}$$

(i.e., the restriction of the map $f \otimes_{\mathbb{K}} \mathbb{K}[\varepsilon_1, \dots, \varepsilon_n]$ to the augmentation ideal $G_n(\mathfrak{g})$), is a group morphism.

Indeed, let us consider two elements of $G_n(\mathfrak{g})$, denoted by $x = \sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha$ and $y = \sum_{\alpha \in I_n} \varepsilon^\alpha y_\alpha$. Then $x \cdot y = \sum_{\alpha \in I_n} \varepsilon^\alpha (x \cdot y)_\alpha$, with

$$(x \cdot y)_\alpha = x_\alpha + y_\alpha + \sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} [\dots [[x_{\lambda^m}, y_{\lambda^1}], y_{\lambda^2}], \dots, y_{\lambda^{m-1}}].$$

Moreover, $\widetilde{f}(x) = \sum_{\alpha \in I_n} \varepsilon^\alpha f(x_\alpha)$ and $\widetilde{f}(y) = \sum_{\alpha \in I_n} \varepsilon^\alpha f(y_\alpha)$. Therefore, we obtain $\widetilde{f}(x) \cdot \widetilde{f}(y) = \sum_{\alpha \in I_n} (\widetilde{f}(x) \cdot \widetilde{f}(y))_\alpha$, with

$$\begin{array}{rcl}
(\widetilde{f}(x) \cdot \widetilde{f}(y))_\alpha & = & f(x_\alpha) + f(y_\alpha) \\
& & + \displaystyle\sum_{m=2}^{|\alpha|} \sum_{\lambda \in P^m(\alpha)} [\dots [[f(x_{\lambda^m}), f(y_{\lambda^1})], f(y_{\lambda^2})], \dots, f(y_{\lambda^{m-1}})].
\end{array}$$

Since f is a Leibniz algebra morphism, it is plain that

$$\widetilde{f}(x) \cdot \widetilde{f}(y) = \widetilde{f}(x \cdot y),$$

which proves that $\widetilde{f}$ is a group morphism.

3 Proof of Theorem B

From now on, the module $\mathfrak{g}$ is required to be endowed with a Lie algebra structure. By the preceding section, the set $G_n(\mathfrak{g})$ is endowed with a group structure. The aim of this section is to establish the description of this group structure by generators and relations, ([3]), given in Theorem B.

Let us recall that every element of $G_n(\mathfrak{g})$ can be uniquely written as a strictly increasing product of pure elements.

Moreover, for all pairs (x, y) of elements of $\mathfrak{g}$ and all multi-indices $\alpha \in I_n$,

$$\varepsilon^\alpha x \cdot \varepsilon^\alpha y = \varepsilon^\alpha (x + y).$$

Then, we show that for all pairs $(\varepsilon^\alpha x, \varepsilon^\alpha y)$ of pure elements of $G_n(\mathfrak{g})$, we have the following commutation relation

$$\varepsilon^\alpha x \cdot \varepsilon^\beta y = \varepsilon^\beta y \cdot \varepsilon^\alpha x \cdot \varepsilon^\alpha \varepsilon^\beta [x, y].$$

Indeed, the product formula (1) provides the identity in the case $\alpha \geq \beta$. Right-multiplying the two sides of the equality by

$$(\varepsilon^\alpha \varepsilon^\beta [x, y])^{-1} = \varepsilon^\alpha \varepsilon^\beta (-[x, y]) = \varepsilon^\alpha \varepsilon^\beta [y, x],$$

we obtain the identity in the remaining case. We remark that the bracket antisymmetry is a crucial point in the proof of this commutation relation. There does not exist such a relation if $\mathfrak{g}$ is only assumed to be a Leibniz algebra.

We are going to prove that these identities characterize the group structure of $G_n(\mathfrak{g})$.

We denote by $F(I)$ the free group on the set I and by N the smallest normal subgroup of $F(I)$ containing the relations given in Theorem B. We have to prove that the group $G_n(\mathfrak{g})$ is isomorphic to the quotient group $F(I)/N$.

Let us recall that every element x of the free group over I can be written in a unique way as (see [6])

$$x = \prod_{i=1}^{m} (\alpha_i, x_i)^{\xi_i},$$

where $m \in \mathbb{N}$, $((\alpha_i, x_i)) \in I^m$, $(\xi_i) \in \{+1, -1\}^m$, and with the condition

$$(\alpha_i, x_i) = (\alpha_{i+1}, x_{i+1}) \Rightarrow \xi_i \xi_{i+1} = 1.$$

We denote by $\sim$ the equivalence relation defined on $F(I)$ by the normal subgroup N : explicitly, we have $X \sim Y$ if and only if $XY^{-1} \in N$.

We introduce the following set :

$$F(I)^+ = \{\prod_{i=1}^{m}(\alpha_i, x_i) | m \in \mathbb{N}, ((\alpha_i, x_i)) \in I^m, x_i \neq 0\}.$$

Note that this set is a submonoid of $F(I)$.

Definition 3. *A permutation map is a map of type $T^{(r,r+1)}$, with*

$$T^{(r,r+1)} : F(I)^+ \longrightarrow F(I)^+$$

defined for a positive integer r in the following way.
Let $X = \prod_{i=1}^{k}(\alpha_i, x_i)$ be an element of $F(I)^+$.
If $k \leq r$, let

$$T^{(r,r+1)}(X) = X.$$

If $k > r$ and if $\alpha_r + \alpha_{r+1} \notin I_n$ or $[x_r, x_{r+1}] = 0$ holds, let

$$\begin{aligned} T^{(r,r+1)}(X) &= (\alpha_1, x_1) \dots (\alpha_{r-1}, x_{r-1})(\alpha_{r+1}, x_{r+1}) \\ &\quad (\alpha_r, x_r)(\alpha_{r+2}, x_{r+2}) \dots (\alpha_k, x_k). \end{aligned}$$

At last, if $k > r$ and if $\alpha_r + \alpha_{r+1} \in I_n$ and $[x_r, x_{r+1}] \neq 0$ hold, let

$$\begin{aligned} T^{(r,r+1)}(X) &= (\alpha_1, x_1) \dots (\alpha_{r-1}, x_{r-1})(\alpha_{r+1}, x_{r+1})(\alpha_r, x_r) \\ &\quad (\alpha_r + \alpha_{r+1}, [x_r, x_{r+1}])(\alpha_{r+2}, x_{r+2}) \dots (\alpha_k, x_k). \end{aligned}$$

Definition 4. *Let X, Y be two elements of $F(I)^+$. Then X is said to be in relation with Y (then we write $X\mathcal{R}Y$) if and only if there exists a finite sequence of permutation maps $(T_1, \dots, T_p)$ such that $T_1 \circ \dots \circ T_p(X) = Y$.*

Remark 4. *This relation is reflexive and transitive, but is not symmetric.*

It follows easily that if $X\mathcal{R}Y$, then $X \sim Y$.

Lemma 3. *This relation is compatible with the left product on $F(I)^+$: namely if $X\mathcal{R}Y$, then $(A \cdot X)\mathcal{R}(A \cdot Y)$ for all $A \in F(I)^+$.*

Proof. The compatibility with the left product is easily seen: we define, for all natural integer k, a map denoted by L_k associating the permutation map $T^{(l+r,l+r+1)}$ to a permutation map $T^{(r,r+1)}$. We then notice that if X, Y are two elements of $F(I)^+$ such that $T(X) = Y$ for a permutation map T, then for all element A in $F(I)^+$, $L_k(T)(A \cdot X) = A \cdot Y$.
Therefore, $X\mathcal{R}Y$ implies $(A \cdot X)\mathcal{R}(A \cdot Y)$ for all $A \in F(I)^+$. □

For a multi-index α in I_n, we define the following map Π_α:

$$\begin{array}{cccc} \Pi_\alpha : & F(I)^+ & \longrightarrow & F(I)^+ \\ & \prod_{i=1}^{k}(\alpha_i, x_i) & \longmapsto & \prod_{i,\alpha_i=\alpha}(\alpha_i, x_i). \end{array}$$

Lemma 4. *Let X be an element of $F(I)^+$, and α be a multi-index. There exist two elements in $F(I)^+$, denoted by X_α and X^α, such that :*

- $X\mathcal{R}(X_\alpha \cdot X^\alpha)$
- $\Pi_\alpha(X_\alpha) = X_\alpha$,
- $\Pi_\alpha(X^\alpha) = \emptyset$,
- *for all* $\beta < \alpha$, $\Pi_\beta(X^\alpha) = \Pi_\beta(X)$.

Proof. The proof is by induction. We introduce the following induction hypothesis. (H_l): for every element X in $F(I)^+$ containing l pure elements lying on the axis $\{\alpha\} \times \mathfrak{g}$, there exist some elements in $F(I)^+$, denoted by X_l and X^l, such that

- $X\mathcal{R}(X_l \cdot X^l)$
- $\Pi_\alpha(X_l) = X_l$,
- $\Pi_\alpha(X^l) = \emptyset$,
- for all $\beta < \alpha$, $\Pi_\beta(X^l) = \Pi_\beta(X)$.

The hypothesis (H_0) is obviously verified. Let l be such that the hypothesis (H_l) is true as well.

We consider an element $X = \prod_{i=1}^k (\alpha_i, x_i)$ of $F(I)^+$ such that $l+1$ of the α_i are equal to α. Let i be such that $\alpha_i = \alpha$. Plainly,

$$T^{(1,2)} \circ \ldots \circ T^{(i-1,i)}(X)$$

is of type

$$(\alpha_i, x_i) \cdot X'$$

where X' is an element of $F(I)^+$ having l pure elements lying on the axis $\{\alpha\} \times \mathfrak{g}$ and verifying, for all $\beta < \alpha$, $\Pi_\beta(X') = \Pi_\beta(X)$.

By induction hypothesis, there exist two elements X_l, X^l in $F(I)^+$ such that

- $X'\mathcal{R}(X_l \cdot X^l)$
- $\Pi_\alpha(X_l) = X_l$,
- $\Pi_\alpha(X^l) = \emptyset$,
- for all $\beta < \alpha$, $\Pi_\beta(X^l) = \Pi_\beta(X')$.

Then

$$((\alpha_i, x_i) \cdot X')\mathcal{R}((\alpha_i, x_i) \cdot X_l \cdot X^l)$$

and by transitivity,

$$X\mathcal{R}((\alpha_i, x_i) \cdot X_l \cdot X^l).$$

Let $X_{l+1} = \alpha_i, x_i.X_l$ and $X^{l+1} = X^l$. We thus obtain

- $X\mathcal{R}(X_{l+1} \cdot X^{l+1})$
- $\Pi_\alpha(X_{l+1}) = \varepsilon^{\alpha_i} x_i.\Pi_\alpha(X_l) = \varepsilon^{\alpha_i} x_i.X_l = X_{l+1}$,
- $\Pi_\alpha(X^{l+1}) = \Pi_\alpha(X^l) = \emptyset$,
- for all $\beta < \alpha$, $\Pi_\beta(X^{l+1}) = \Pi_\beta(X^l) = \Pi_\beta(X') = \Pi_\beta(X)$.

which proves (H_{l+1}).

□

Let us introduce the set $F(I)^{\nearrow}$ (resp. the set $F(I)^{\uparrow}$) of elements $\prod_{i=1}^{k}(\alpha_i, x_i)$ in $F(I)^+$ for whose $(\alpha_i)_{i\in\{1,\ldots,k\}}$ is an increasing sequence (resp. a strictly increasing sequence). The lemma leads to the following proposition.

Proposition 2. *For every element X in $F(I)^+$, there exists an element Y in $F(I)^{\nearrow}$ such that $X\mathcal{R}Y$.*

Proof. We denote by (θ_i) the increasing sequence of elements of I_n.

Let us define by induction a sequence $(X_k, X^k)_{k\in\{1,\ldots,2^n-1\}}$ of pairs of elements of $F(I)^+$.

Using the lemma, we know existence of elements X_1, X^1 in $F(I)^+$ such that

- $X\mathcal{R}(X_1 \cdot X^1)$
- $\Pi_{\theta_1}(X_1) = X_1$,
- $\Pi_{\theta_1}(X^1) = \emptyset$.

Assume X_k, X^k are defined. Using the lemma once more, there exist elements X_{k+1}, X^{k+1} in $F(I)^+$ such that

- $X^k\mathcal{R}(X_{k+1} \cdot X^{k+1})$
- $\Pi_{\theta_{k+1}}(X_{k+1}) = X_{k+1}$,
- $\Pi_{\theta_{k+1}}(X^{k+1}) = \emptyset$.
- for all $l < k+1$, $\Pi_{\theta_l}(X^{k+1}) = \Pi_{\theta_l}(X^k)$.

By induction, we check that for all $k \in \{1, \ldots, 2^n - 1\}$, the element X^k satisfies to $\Pi_{\theta_l}(X^k) = \emptyset$ for all $l \leq k$. In particular, $X^{2^n-1} = \emptyset$.

Furthermore, notice that $Y = X_1 \cdot X_2 \cdot \ldots \cdot X_{2^n-1}$ belongs to $F(I)^{\nearrow}$. Since the relation is transitive and left-product stable, we finally obtain

$$X\mathcal{R}Y,$$

which completes the proof.

□

Proposition 3. *The quotient set $F(I)/N$ is in bijection with the set $F(I)^{\uparrow}$.*

Proof. Since the elements $(\alpha, 0)$ and $(\alpha, x+y)(\alpha, x)^{-1}(\alpha, y)^{-1}$ belong to N, the element

$$(\alpha, -x)(\alpha, x) = ((\alpha, 0)^{-1}(\alpha, x + (-x))(\alpha, x)^{-1}(\alpha, -x)^{-1})^{-1}$$

is still in N.

Let X be an element of the free group $F(I)$. Using relations of type $(\alpha, 0)$ and $(\alpha, x)(\alpha, -x)$, we obtain the existence of $Y \in F(I)^+$ such that $X \sim Y$. From above, there is $Y' \in F(I)^{\nearrow}$ such that $Y\mathcal{R}Y'$. Then $Y \sim Y'$.

From relations of the type

$$(\alpha, x + y)(\alpha, -x)(\alpha, -y),$$

it is plain that there exists $Y'' \in F(I)^{\uparrow}$ such that $Y' \sim Y$. Thus $X \sim Y''$.

Assume that there exists $Z \in F(I)^{\uparrow}$ such that $X \sim Z$. We can deduce $Y'' \sim Z$ and therefore $Y''Z^{-1} \in N$. Furthermore, we know that elements of N can be written as $r = \prod_{i=1}^{k} g_i r_i g_i^{-1}$, where r_i stand for relations, and g_i are elements of $F(I)$. Such an element is of type $\prod_{i-1}^{r}(\alpha_i, x_i)\prod_{i=1}^{x}(\beta_i, y_i)^{-1}$, with (α_i) a strictly increasing sequence and (β_i) a strictly decreasing sequence, if and only if $r = \emptyset$. Hence $Y''Z^{-1} \in N$ implies $Y''Z^{-1} = \emptyset$ and $Y'' = Z$.

Finally, the set $F(I)/N$ is in bijection with $F(I)^{\uparrow}$. $\square$

The map

$$\begin{array}{ccc} I & \longrightarrow & G_n(\mathfrak{g}) \\ (\alpha, x) & \longmapsto & \varepsilon^{\alpha} x \end{array}$$

can uniquely be extended to a group morphism $\varphi : F(I) \longmapsto G_n(\mathfrak{g})$.This morphism is surjective since if $x = \sum_{i=1}^{2^n-1} \varepsilon^{\theta_i} x_i$ belongs to $G_n(\mathfrak{g})$ (where (θ_i) denotes the increasing sequence of elements of I_n), then

$$\varphi(\prod_{i=1}^{2^n-1}(\theta_i, x_i)) = x.$$

Furthermore, if r is a relation, then it is obvious that $\varphi(r) = 0$. As a consequence, the map φ gives rise to an onto morphism $\psi : F(I)/N \longrightarrow G_n(\mathfrak{g})$.

Thus, the proof of Theorem B will be complete with the following proposition.

Proposition 4. *The map ψ is a group isomorphism of $F(I)/N$ onto $G_n(\mathfrak{g})$.*

Proof. It remains to prove the injectivity of the map.

Let $X = \prod_{i=1}^{k}(\alpha_i, x_i)$, $Y = \prod_{i=1}^{l}(\beta_i, y_i)$ be two elements of $F(I)^{\uparrow}$ such that $\varphi(X) = \varphi(Y)$. Then $\prod_{i=1}^{k} \varepsilon^{\alpha_i} x_i = \prod_{i=1}^{l} \varepsilon^{\beta_i} y_i$. Since the sequences (α_i) and (β_i) are strictly increasing, we obtain

$$\sum_{i=1}^{k} \varepsilon^{\alpha_i} x_i = \sum_{i=1}^{l} \varepsilon^{\beta_i} y_i,$$

and therefore $k = l$, $\alpha_i = \beta_i$ and $x_i = y_i$. It proves that $X = Y$ and that the map ψ is injective.

$\square$

4 Proof of Theorem C

We keep the framework of the preceding section: namely, the module $\mathfrak{g}$ is endowed with a Lie algebra structure. We are going to show that the n-th order symmetric group Σ_n acts in a natural way by morphisms on the group $G_n(\mathfrak{g})$.

The n-th order symmetric group acts on the set I by $\sigma.(\alpha, x) = (\sigma.\alpha, x)$. Consequently, it acts by morphisms on the free group $F(I)$. Since $\sigma.r \in N$ for every relation r, it gives rise to an action by automorphisms on

$$G_n(\mathfrak{g}) \simeq F(I)/N.$$

Explicitly, the isomorphism ψ provides the following formula: for $\sigma \in \Sigma_n$ and $x = \prod_{i=1}^n \varepsilon^{\alpha_i} x_i \in G_n(\mathfrak{g})$ written as a strictly increasing product of pure elements, we get

$$\sigma(x) = \prod_{i=1}^n \varepsilon^{\sigma.\alpha_i} x_i.$$

Thus, Part 1 of Theorem C is proved.

The set $J_n(\mathfrak{g})$ of elements of $G_n(\mathfrak{g})$ fixed under the action of the symmetric group is a subgroup of $G_n(\mathfrak{g})$.

In order to prove Part 2, we remark that the n-th order symmetric group acts in a natural way on the ring $T^n\mathbb{K}$ too: if $x + \sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha$ is an element of $T^n\mathbb{K}$, and if σ is a permutation of $\{1, \ldots, n\}$, the action is given by

$$\sigma(x + \sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha) = x + \sum_{\alpha \in I_n} \varepsilon^{\sigma.\alpha} x_\alpha.$$

We denote by $J^n\mathbb{K}$ the subring of $T^n\mathbb{K}$ of fixed points under the action of Σ_n. For $i \in \{1, \ldots, n\}$, let $\delta^{(i)}$ denote the element

$$\sum_{\alpha \in I_n, |\alpha| = i} \varepsilon^\alpha.$$

It is then easy to check that

$$J^n\mathbb{K} = \{x + \sum_{i=1}^n \delta^{(i)} x_i | x, x_i \in \mathbb{K}\}.$$

We are going to show that the subgroup $J_n(\mathfrak{g})$ is the augmentation ideal of the extension of the algebra $\mathfrak{g}$ by the ring $J^n\mathbb{K}$:

Proposition 5. *The set* $\bigoplus_{i=1}^{n} \delta^{(i)}\mathfrak{g}$ *is a subgroup of* $G_n(\mathfrak{g})$. *More precisely,*

$$\bigoplus_{i=1}^{n} \delta^{(i)}\mathfrak{g} = J_n(\mathfrak{g}).$$

Proof. It suffices to show that $J_n(\mathfrak{g}) = \bigoplus_{i=1}^{n} \delta^{(i)}\mathfrak{g}$.

First, we prove by induction on n that $\bigoplus_{i=1}^{n} \delta^{(i)}\mathfrak{g} \subset J_n(\mathfrak{g})$. The case $n = 1$ is obvious. We denote by (k_n) the sequence whose general term is $2^n - 1$ and by $(\theta_i^n)_{1\leq i\leq k_n}$ the increasing sequence of elements of I_n. Moreover, let $\theta_0^n = (0, \ldots, 0)$. Thus

$$(\theta_i^{n+1})_{1\leq i\leq k_{n+1}} = ((0, \theta_1^n), \ldots, (0, \theta_{k_n}^n), (1, \theta_0^n), \ldots, (1, \theta_{k_n}^n)).$$

Assume the result is true at rank n: for all $x = \sum_{i=1}^{k_n} \varepsilon^{\theta_i^n} x_{|\theta_i^n|}$ element of $\bigoplus_{i=1}^{n} \delta^{(i)}\mathfrak{g}$, for all permutation $\sigma \in \Sigma_n$,

$$\sigma(x) = x.$$

Let $x = \sum_{i=1}^{k_{n+1}} \varepsilon^{\theta_i^{n+1}} x_{|\theta_i^{n+1}|}$ be an element of $\bigoplus_{i=1}^{n+1} \delta^{(i)}\mathfrak{g}$. Since (θ_i^{n+1}) is a strictly increasing sequence,

$$\begin{aligned} x &= \prod_{i=1}^{k_{n+1}} \varepsilon^{\theta_i^{n+1}} x_{|\theta_i^{n+1}|} \\ &= \prod_{i=1}^{k_n} \varepsilon^{(0,\theta_i^n)} x_{|\theta_i^n|} \cdot \prod_{i=0}^{k_n} \varepsilon^{(1,\theta_i^n)} x_{|\theta_i^n|+1}. \end{aligned}$$

Let $\sigma \in \Sigma_{n+1}$. Since Σ_{n+1} is generated by transpositions of type $(i, i+1)$, assume that σ is such a transposition.

We distinguish two cases. If $\sigma = (i, i+1)$ with i distinct from 1, then, with the notation $\sigma' = (i-1, i)$, we obtain

$$\begin{aligned} \sigma(x) &= \prod_{i=1}^{k_{n+1}} \varepsilon^{\sigma.\theta_i^{n+1}} x_{|\theta_i^{n+1}|} \\ &= \prod_{i=1}^{k_n} \varepsilon^{(0,\sigma'.\theta_i^n)} x_{|\theta_i^n|} \cdot \varepsilon^{(1,0,\ldots,0)} x_1 \cdot \prod_{i=1}^{k_n} \varepsilon^{(1,\sigma'.\theta_i^n)} x_{|\theta_i^n|+1}. \end{aligned}$$

Furthermore, by induction hypothesis,

$$\prod_{i}^{k_n} \varepsilon^{\sigma'.\theta_i^n} x_{|\theta_i^n|} = \prod_{i}^{k_n} \varepsilon^{\theta_i^n} x_{|\theta_i^n|}$$

and

$$\prod_{i}^{k_n} \varepsilon^{\sigma'.\theta_i^n} x_{|\theta_i^n|+1} = \prod_{i}^{k_n} \varepsilon^{\theta_i^n} x_{|\theta_i^n|+1}.$$

Hence
$$\prod_i^{k_n} \varepsilon^{(0,\sigma'.\theta_i^n)} x_{|\theta_i^n|} = \prod_i^{k_n} \varepsilon^{(0,\theta_i^n)} x_{|\theta_i^n|}$$
and
$$\prod_i^{k_n} \varepsilon^{(1,\sigma'.\theta_i^n)} x_{|\theta_i^n|+1} = \prod_i^{k_n} \varepsilon^{(1,\theta_i^n)} x_{|\theta_i^n|+1}.$$

As a result,
$$\begin{aligned} \sigma(x) &= \prod_{i=1}^{k_n} \varepsilon^{(0,\theta_i^n)} x_{|\theta_i^n|} \cdot \varepsilon^{(1,0,\ldots,0)} x_1 \cdot \prod_{i=1}^{k_n} \varepsilon^{(1,\theta_i^n)} x_{|\theta_i^n|+1} \\ &= x. \end{aligned}$$

Assume now that $\sigma = (1,2)$.

We get
$$\begin{aligned} (\theta_i^{n+1}) &= ((0,0,\theta_1^{n-1}), \ldots, (0,0,\theta_{k_{n-1}}^{n-1}), (0,1,\theta_0^{n-1}), \ldots, (0,1,\theta_{k_{n-1}}^{n-1}), \\ & \quad (1,0,\theta_0^{n-1}), \ldots, (1,0,\theta_{k_{n-1}}^{n-1}), (1,1,\theta_0^{n-1}), \ldots, (1,1,\theta_{k_{n-1}}^{n-1})). \end{aligned}$$

Then
$$x = x_{(0,0)} \cdot x_{(0,1)} \cdot x_{(1,0)} \cdot x_{(1,1)}$$
with
$$x_{(0,0)} = \prod_{i=1}^{k_{n-1}} \varepsilon^{(0,0,\theta_i^{n-1})} x_{|\theta_i^{n-1}|},$$
$$x_{(0,1)} = \prod_{i=0}^{k_{n-1}} \varepsilon^{(0,1,\theta_i^{n-1})} x_{|\theta_i^{n-1}|+1},$$
$$x_{(1,0)} = \prod_{i=0}^{k_{n-1}} \varepsilon^{(1,0,\theta_i^{n-1})} x_{|\theta_i^{n-1}|+1},$$
and
$$x_{(1,1)} = \prod_{i=0}^{k_{n-1}} \varepsilon^{(1,1,\theta_i^{n-1})} x_{|\theta_i^{n-1}|+2}.$$

Moreover,
$$\sigma(x) = x_{(0,0)} \cdot x_{(1,0)} \cdot x_{(0,1)} \cdot x_{(1,1)}.$$

Furthermore, using the relation $\varepsilon^\alpha y \cdot \varepsilon^\beta z = \varepsilon^\beta z \cdot \varepsilon^\alpha y \cdot \varepsilon^{\alpha+\beta}[y,z]$, we obtain
$$\begin{aligned} x_{(1,0)} \cdot x_{(0,1)} &= x_{(0,1)} \cdot x_{(1,0)} \cdot \prod_{i,j=0}^{k_{n-1}} \varepsilon^{(1,1,\theta_i^{n-1}+\theta_j^{n-1})} [x_{|\alpha_i^{n-1}|+1}, x_{|\alpha_j^{n-1}|+1}] \\ &= x_{(0,1)} \cdot x_{(1,0)} \cdot \prod_{0 \le i < j \le k_{n-1}} \varepsilon^{(1,1,\theta_i^{n-1}+\theta_j^{n-1})} \\ & \quad ([x_{|\alpha_i^{n-1}|+1}, x_{|\alpha_j^{n-1}|+1}] + [x_{|\alpha_j^{n-1}|+1}, x_{|\alpha_i^{n-1}|+1}]) \\ &= x_{(0,1)} \cdot x_{(1,0)}, \end{aligned}$$

since
$$[x_{|\alpha_i^{n-1}|+1}, x_{|\alpha_j^{n-1}|+1}] = -[x_{|\alpha_j^{n-1}|+1}, x_{|\alpha_i^{n-1}|+1}].$$

Consequently,
$$\sigma(x) = x,$$
which achieves the induction.

It remains to prove that $J_n(\mathfrak{g}) \subset \bigoplus_{i=1}^n \delta^{(i)}\mathfrak{g}$.

Let $x = \sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha \in J_n(\mathfrak{g})$. Ad absurdum, assume that $x \notin \bigoplus_{i=1}^n \delta^{(i)}\mathfrak{g}$. This means that the set
$$\{\alpha \in I_n | \exists \beta \in I_n, |\alpha| = |\beta|, x_\alpha \neq x_\beta\}$$
is not empty. We denote by θ the smallest of its elements (considering the lexicographic ordering). By definition, there exists β with $|\beta| = |\theta|$ and $x_\theta \neq x_\beta$.

Let σ be a permutation satisfying to $\sigma.\theta = \beta$ (such a permutation exists, since the lengths of θ and α are equal). We denote by $(\alpha_1, \ldots, \alpha_p)$ the strictly increasing sequence of multi-indices such that
$$X = ((\alpha_1, x_{\alpha_1}), \ldots, (\alpha_p, x_{\alpha_p})) \in F(I)^\uparrow$$
and
$$\varphi(X) = x.$$
Assume that $\theta = \alpha_k$ and $\beta = \alpha_l$. Then $\sigma.\alpha_k = \alpha_l$. By assumption, we have $k < l$. Moreover, we check that for all $i < k$, $|\alpha_i| < |\alpha_k|$ and $\varepsilon^{\alpha_i}\varepsilon^{\alpha_k} = 0$.

We have
$$\sigma.X = ((\sigma.\alpha_1, x_{\alpha_1}), \ldots, (\sigma.\alpha_p, x_{\alpha_p}))$$
and using the relations above, we show that
$$\sigma.X\mathcal{R}((\alpha_1, x_{\sigma.\alpha_1}), \ldots, (\alpha_k, x_{\alpha_l})) \cdot X'$$
where X' does not have any pure element lying on the axis of type $\{\alpha\} \times \mathfrak{g}$, with $\alpha < \alpha_k$.

We obtain then
$$\begin{aligned} \sigma(x) &= \varphi(\sigma.X) \\ &= \varphi(((\alpha_1, x_{\sigma.\alpha_1}), \ldots, (\alpha_k, x_{\alpha_l})) \cdot X'). \end{aligned}$$
Moreover, x is a fixed point under the action of Σ_n. Thus $\sigma.x = x$ and
$$\varphi(((\alpha_1, x_{\sigma.\alpha_1}), \ldots, (\alpha_k, x_{\alpha_l})) \cdot X') = \varphi(((\alpha_1, x_{\alpha_1}), \ldots, (\alpha_p, x_{\alpha_p}))),$$
which implies $x_{\sigma.\alpha_i} = x_{\alpha_i}$ for all $i \leq k$. In particular, $x_\theta = x_\beta$, a contradiction.

Finally, $J_n(\mathfrak{g}) \subset \bigoplus_{i=1}^n \delta^{(i)}\mathfrak{g}$ and we get therefore the equality of sets.

□

The set $J_n(\mathfrak{g}) = \bigoplus_{i=1}^n \delta^{(i)}\mathfrak{g}$ is a subgroup of $G_n(\mathfrak{g})$. This means that for all n-uplets $(x_i), (y_i) \in \mathfrak{g}^n$, there exists $(z_i) \in \mathfrak{g}^n$ such that

$$\sum_{i=1}^n \delta^{(i)} x_i \cdot \sum_{i=1}^n \delta^{(i)} y_i = \sum_{i=1}^n \delta^{(i)} z_i,$$

where (z_i) only depends on (x_i) and (y_i).

Let us write out the first terms :

$$\begin{array}{rcl}
z_1 & = & x_1 + y_1 \\
z_2 & = & x_2 + y_2 + [x_1, y_1] \\
z_3 & = & x_3 + y_3 + 2[x_2, y_1] + [[x_1, y_1], y_1] + [x_1, y_2] \\
z_4 & = & x_4 + y_4 + 3[x_3, y_1] + 3[x_2, y_2] + 3[[x_2, y_1], y_1] + [x_1, y_3] \\
& & +2[[x_1, y_2], y_1] + [[x_1, y_1], y_2] + [[[x_1, y_1], y_1], y_1] \\
z_5 & = & x_5 + y_5 + 4[x_4, y_1] + 6[x_3, y_2] + 6[[x_3, y_1], y_1] \\
& & +4[x_2, y_3] + 8[[x_2, y_2], y_1] + 4[[x_2, y_1], y_2] + 4[[[x_2, y_1], y_1], y_1] \\
& & +[x_1, y_4] + 3[[x_1, y_3], y_1] + 3[[x_1, y_2], y_2] + 3[[[x_1, y_2], y_1], y_1] \\
& & +2[[[x_1, y_1], y_2], y_1] + [[[x_1, y_1], y_1], y_2] + [[[[x_1, y_1], y_1], y_1], y_1], y_1].
\end{array}$$

Let us further give the explicit formula in the particular case where only one of the elements of each n-uplet (x_i) and (y_i) is non zero :

$$\delta^{(i)} x \cdot \delta^{(j)} y = \delta^{(i)} x + \delta^{(j)} y + \sum_{k \geq 1} C_{i,j,k} \delta^{(i+kj)} [\ldots [[x, y], y], \ldots], y]_k, \qquad (4)$$

where $\delta^{(r)} = 0$ if $r > n$, $[\ldots [[x, y], y] \ldots], y]_k$ denotes the iterated bracket of $[x, y]$ with y involving k times the element y, and

$$C_{i,j,k} = \binom{i + kj - 1}{i - 1} \binom{kj - 1}{j - 1} \binom{(k-1)j - 1}{j - 1} \cdots \binom{2j - 1}{j - 1} \binom{j - 1}{j - 1}.$$

Similarly, products of binomial coefficients are involved in the coefficients of the general formula for z_i, which will not be written here.

5 Complements

In this section, we assume that the module $\mathfrak{g}$ is endowed with a Lie algebra structure over the ring $\mathbb{K}$.

5.1 The polynomial group $G_n(\mathfrak{g})$

We use in this paragraph the notion of polynomial group developed in [1], which relies on the notion of polynomial maps on a ring (see [2], chapter IV). Let us first recall this definition.

Definition 5. *A $\mathbb{K}$-module G endowed with a structure of group (G, m) is called a polynomial group of order less than k if and only if the product m, the inversion i and the iterated products*

$$\begin{array}{rccc} m^{(j)}: & G^j & \longrightarrow & G \\ & (x_i) & \longmapsto & \prod_{i=1}^{j} x_i, \end{array}$$

for all $j \in \mathbb{N}$, are polynomial maps of degree less than k.

A module G endowed with a group structure (G, m) is said to be a polynomial group if and only if there exists $k \in \mathbb{N}$ such that (G, m) is a polynomial group of order less than k.

It follows from Theorem A that the group $(G_n(\mathfrak{g}), .)$ is polynomial (of order less than or equal to n). Consequently, the subgroup $(J_n(\mathfrak{g}), .)$ is polynomial, too.

To each polynomial group is associated a Lie algebra (restricting the Lie functor from formal group category to the Lie algebra one, [10] or [4]). If $\mathfrak{g}$ is a Lie algebra, the Lie algebra associated to the polynomial group $(G_n(\mathfrak{g}), .)$ is the natural structure of nilpotent algebra on $G_n(\mathfrak{g})$ given by:

$$[\sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha, \sum_{\alpha \in I_n} \varepsilon^\alpha y_\alpha] = \sum_{\alpha, \beta \in I_n} \varepsilon^\alpha \varepsilon^\beta [x_\alpha, y_\beta].$$

Using the formula (4), we show further that the Lie algebra associated to the polynomial group $J_n(\mathfrak{g})$ is given by the bilinear bracket on $J_n(\mathfrak{g})$ satisfying to:

$$[\delta^{(i)} x, \delta^{(j)} y] = \binom{i+j}{i} \delta^{(i+j)} [x, y].$$

Remark 5. *If $\mathfrak{g}$ is a Leibniz algebra, the Lie algebra associated to the polynomial group $G_n(\mathfrak{g})$ is the module $G_n(\mathfrak{g})$ endowed with the Lie bracket*

$$[\sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha, \sum_{\alpha \in I_n} \varepsilon^\alpha y_\alpha] = \sum_{\alpha > \beta} \varepsilon^\alpha \varepsilon^\beta ([x_\alpha, y_\beta] - [y_\alpha, x_\beta]).$$

This bracket is obviously antisymmetric and we know by construction that it satisfies to the Jacobi identity. Nevertheless, it is quite easy to prove directly this last point.

5.2 Projective limits

The map

$$\begin{array}{ccc} \mathbb{K}[x]/(x^2) & \longrightarrow & \mathbb{K} \\ [p] & \longmapsto & p(0) \end{array}$$

is a natural projection of the tangent ring $T\mathbb{K}$ onto the basis $\mathbb{K}$.

Using dual number presentation, we check that this projection associate the element x of $\mathbb{K}$ to the element $x + \varepsilon y$ of $T\mathbb{K}$. Similarly, there exist natural projections, denoted by $\pi_{n,k}$, from the ring $T^n(\mathbb{K})$ onto the ring $T^k(\mathbb{K})$, for $n \geq k$.

We denote by $p_{n,k}$ the projection of I_n onto $I_k \cup \{0\}$ defined by

$$p_{n,k}((\alpha_1, \dots, \alpha_n)) = \begin{cases} (\alpha_1, \dots, \alpha_k) \text{ if for all } i > k,\ \alpha_i = 0, \\ 0 \text{ otherwise.} \end{cases}$$

We define then

$$\pi_{n,k}\left(x + \sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha\right) = x + \sum_{\alpha \in I_n, p_{n,k}(\alpha) \neq 0} \varepsilon^{p_{n,k}(\alpha)} x_\alpha.$$

These projections obviously form a projective system of rings and the projective limit of the sequence $(T^n\mathbb{K})$, denoted by $T^\infty\mathbb{K}$, is therefore endowed with a ring structure.

We notice that the k-th order symmetric group Σ_k, naturally seen as a subgroup of Σ_n, acts both on $T^k\mathbb{K}$ and $T^n\mathbb{K}$. The projection $\pi_{n,k}$ is equivariant under this action. Consequently, we get a ring morphism of $T^n\mathbb{K}^{\Sigma_k}$ on $T^k\mathbb{K}^{\Sigma_k}$, considering the restriction of $\pi_{n,k}$ to the fixed point subrings. If $x + \sum_{i=1}^n \delta^{(i)} x_i$ belongs to $J^n\mathbb{K}$ (set included in $T^n\mathbb{K}^{\Sigma_k}$), its image under the projection $\pi_{n,k}$ must belong to $J^k\mathbb{K} = T^k\mathbb{K}^{\Sigma_k}$. We have thus shown that

$$\pi_{n,k}(x + \sum_{i=1}^n \delta^{(i)} x_i) = x + \sum_{i=1}^k \delta^{(i)} x_i.$$

Taking projective limit of the subrings $J^n\mathbb{K}$, we therefore obtain a subring of $T^\infty\mathbb{K}$, denoted by $J^\infty\mathbb{K}$.

If $\mathbb{K}$ is of characteristic zero, the ring $J^\infty\mathbb{K}$ may be seen as a ring of formal power series: indeed, if δ denotes the element $\delta^{(1)} = \sum_{i=1}^n \varepsilon_i$, we notice that

$$i!\delta^{(i)} = \delta^i,$$

and we get there, assuming that integers are invertible in $\mathbb{K}$,

$$\begin{aligned} J^\infty\mathbb{K} &= \{x + \sum_{i=1}^\infty \delta^{(i)} x_i | x, x_i \in \mathbb{K}\} \\ &= \{x + \sum_{i=1}^\infty \delta^i x_i | x, x_i \in \mathbb{K}\}, \end{aligned}$$

with $\delta^i \cdot \delta^j = \delta^{i+j}$.

Proposition 6. *The ring morphisms $\pi_{n,k} : T^n\mathbb{K} \longrightarrow T^k\mathbb{K}$ (resp. $\pi_{n,k} : J^n\mathbb{K} \longrightarrow J^k\mathbb{K}$), defined for all $n \geq k$, give rise to group morphisms $\Pi_{n,k} : G^n(\mathfrak{g}) \longrightarrow G^k(\mathfrak{g})$ (resp. $\Pi_{n,k} : J^n(\mathfrak{g}) \longrightarrow J^k(\mathfrak{g})$), which thus form a projective system of groups.*

Proof. We want to show that the projection $\Pi_{n,k} : G^n(\mathfrak{g}) \longrightarrow G^k(\mathfrak{g})$, defined for all $n \geq k$ by

$$\Pi_{n,k}\left(\sum_{\alpha\in I_n} \varepsilon^\alpha x_\alpha\right) = \sum_{\alpha\in I_n, p_{n,k}(\alpha)\neq 0} \varepsilon^{p_{n,k}(\alpha)} x_\alpha,$$

is a group morphism. But the map $\Pi_{n,k} : J_n(\mathfrak{g}) \longrightarrow J_k(\mathfrak{g})$, associating the element $\sum_{i=1}^k \delta^{(i)} x_i$ to an element $\sum_{i=1}^n \delta^{(i)} x_i$ of $J_n(\mathfrak{g})$, is the restriction of the preceding map to the subgroup $J_n(\mathfrak{g})$. Hence, it will be proved at the same time that this map is a group morphism.

Let us introduce the map

$$\begin{array}{cccc} i: & I_k & \longrightarrow & I_n \\ & (\alpha_1,\ldots,\alpha_k) & \longmapsto & (\alpha_1,\ldots,\alpha_k,0,\ldots,0). \end{array}$$

Let $x = \sum_{\alpha\in I_n} \varepsilon^\alpha x_\alpha, y = \sum_{\alpha\in I_n} \varepsilon^\alpha y_\alpha$ be two elements of $G_n(\mathfrak{g})$. We wish to show that $\Pi_{n,k}(x\cdot y) = \Pi_{n,k}(x)\cdot \Pi_{n,k}(y)$. We have

$$\begin{aligned} \Pi_{n,k}(x\cdot y) &= \sum_{\alpha\in I_n} \varepsilon^{p_{n,k}(\alpha)}(x\cdot y)_\alpha \\ &= \sum_{\theta\in I_k} \varepsilon^\theta (x\cdot y)_{i(\theta)}, \end{aligned}$$

with

$$(x\cdot y)_{i(\theta)} = x_{i(\theta)} + y_{i(\theta)} + \sum_{m=2}^{|i(\theta)|} \sum_{\lambda\in P^m(i(\theta))} [[[x_{\lambda^m}, y_{\lambda^1}], y_{\lambda^2}],\ldots, y_{\lambda^{m-1}}].$$

We denote by $\widetilde{x} = \sum_{\theta\in I_k} \varepsilon^\theta \widetilde{x}_\theta$ and $\widetilde{y} = \sum_{\theta\in I_k} \varepsilon^\theta \widetilde{y}_\theta$ the elements $\Pi_{n,k}(x)$ and $\Pi_{n,k}(y)$ of $G_k(\mathfrak{g})$. Hence, for all $\theta \in I_k$, $\widetilde{x}_\theta = x_{i(\theta)}$ and $\widetilde{y}_\theta = y_{i(\theta)}$. Therefore

$$\begin{aligned} \Pi_{n,k}(x)\cdot \Pi_{n,k}(y) &= \widetilde{x}\cdot\widetilde{y} \\ &= \sum_{\theta\in I_k} \varepsilon^\theta (\widetilde{x}\cdot\widetilde{y})_\theta, \end{aligned}$$

with

$$\begin{aligned} (\widetilde{x}\cdot\widetilde{y})_\theta &= \widetilde{x}_\theta + \widetilde{y}_\theta + \sum_{m=2}^{|\theta|} \sum_{\lambda\in P^m(\theta)} [[[\widetilde{x}_{\lambda^m}, \widetilde{y}_{\lambda^1}], \widetilde{y}_{\lambda^2}],\ldots, \widetilde{y}_{\lambda^{m-1}}] \\ &= x_{i(\theta)} + y_{i(\theta)} + \sum_{m=2}^{|\theta|} \sum_{\lambda\in P^m(\theta)} [[[x_{i(\lambda^m)}, y_{i(\lambda^1)}], y_{i(\lambda^2)}],\ldots, y_{i(\lambda^{m-1})}] \end{aligned}$$

It is then enough to notice that $|i(\theta)| = |\theta|$ and that

$$P^m(i(\theta)) = \{i(\lambda) | \lambda \in P^m(\theta)\}$$

in order to establish the required equality $(\widetilde{x} \cdot \widetilde{y})_\theta = (x \cdot y)_{i(\theta)}$. Finally, the map $\Pi_{n,k}$ is a group morphism.

$\square$

Remark 6. *We endow the module $\varepsilon_{n+1}(\mathfrak{g} \oplus G_n(\mathfrak{g}))$ with its natural vector structure of polynomial group. Then the map $\Pi_{n+1,n}$ provides the following exact sequence of polynomial groups:*

$$\{0\} \longrightarrow \varepsilon_{n+1}(\mathfrak{g} \oplus G_n(\mathfrak{g})) \longrightarrow G_{n+1}(\mathfrak{g}) \longrightarrow G_n(\mathfrak{g}) \longrightarrow \{0\},$$

which splits via

$$\begin{array}{ccc} G_n(\mathfrak{g}) & \longrightarrow & G_{n+1}(\mathfrak{g}) \\ \sum_{\alpha \in I_n} \varepsilon^\alpha x_\alpha & \longmapsto & \sum_{\alpha \in I_n} \varepsilon^{(\alpha,0)} x_\alpha. \end{array}$$

Hence $G_{n+1}(\mathfrak{g})$ is a semi-direct product of $G_n(\mathfrak{g})$ by the abelian group $\varepsilon_{n+1}(\mathfrak{g} \oplus G_n(\mathfrak{g}))$.

Corollary 1. *The group sequence $(G_n(\mathfrak{g}))$ (resp. $(J_n(\mathfrak{g}))$ admits a projective limit, denoted by $G_\infty(\mathfrak{g})$ (resp. $J_\infty(\mathfrak{g})$), and provided by the projective system $(\Pi_{n,k})$.*

We notice that the group $J_\infty(\mathfrak{g})$ is a subgroup of $G_\infty(\mathfrak{g})$. However, it seems difficult to identify directly an action of a symmetric group on $G_\infty(\mathfrak{g})$ and to deduce there a direct construction of $J_\infty(\mathfrak{g})$ from $G_\infty(\mathfrak{g})$.

In characteristic zero, we know that the ring $J^\infty\mathbb{K}$ may be seen as a ring of formal power series. Similarly, under the same assumptions, the group $J_\infty(\mathfrak{g})$ may be seen as a formal group associated to the Lie algebra $\mathfrak{g}$. The structure of $G_\infty(\mathfrak{g})$ is yet more difficult to understand.

Lastly, we point out that the map sending the Lie algebra $\mathfrak{g}$ to the group $G_\infty(\mathfrak{g})$ (respectively $J_\infty(\mathfrak{g})$) is functorial.

It remains to study the connection between the groups $J_\infty(\mathfrak{g}), G_\infty(\mathfrak{g})$ and the formal group $CH(\mathfrak{g})$ given by the Campbell-Haussdorf formula, in the case $\mathbb{K}$ is a field of characteristic zero.

5.3 Exponential map and Campbell-Haussdorf formula

From now on, we assume that $\mathbb{K}$ is a field of characteristic zero. Then there exists a polynomial analogue to the theorem on the existence of the exponential serie for formal groups (see [1]):

Theorem 2. *Let G be a polynomial group on the field of characteristic zero $\mathbb{K}$. There exists a unique polynomial map $\exp : G \longrightarrow G$ such that*

- *for all $x \in G$ and for all $n \in \mathbb{N}$, $\exp(nx) = (\exp x)^n$,*
- *the linear part of the map $\exp$ is the identity map.*

The polynomial map exp *is bijective and its inverse map, denoted by* log*, is still polynomial.*

The theorem provides in addition the explicit formulae of these two polynomial maps.

Denote by $\exp_n$, $\log_n$ the polynomial maps provided by the preceding theorem for the polynomial group $G_n(\mathfrak{g})$.

More explicitly, we obtain for an element $x = \sum_\alpha \varepsilon^\alpha x_\alpha$ of $G_n(\mathfrak{g})$,

$$\exp_n x = \sum_\alpha \varepsilon^\alpha (\exp_n x)_\alpha$$

where, ([1])

$$(\exp_n x)_\alpha = x_\alpha + \sum_{m=2}^{n} \frac{1}{m!} \sum_{\lambda \in \mathcal{P}_m(\alpha)} [[[x_{\lambda^m}, x_{\lambda^{m-1}}], \ldots, x_{\lambda^2}], x_{\lambda^1}].$$

We denote by $(G_n(\mathfrak{g}), \star)$ the formal group structure on the Lie algebra $G_n(\mathfrak{g})$ given by the Campbell-Haussdorf formula : for all pairs (x, y) of elements in $G_n(\mathfrak{g})$,

$$x \star y = x + y + \frac{1}{2}[x, y] + \frac{1}{12}([x, [x, y]] + [y, [y, x]]) + \ldots,$$

where $[.,.]$ denotes the natural Lie algebra structure of $G_n(\mathfrak{g})$. Since the Lie algebra $G_n(\mathfrak{g})$ is nilpotent, $(G_n(\mathfrak{g}), \star)$ is a polynomial group.

The relation between the two polynomial group structures defined on $G_n(\mathfrak{g})$ is made precise by the following proposition.

Proposition 7. *The map* $\exp_n : (G_n(\mathfrak{g}), \star) \longrightarrow (G_n(\mathfrak{g}), .)$ *is a polynomial group isomorphism.*

Proof. Since $\exp_n(mx) = \exp_n(x)^m$ for all element x in $G_n(\mathfrak{g})$ and all $m \in \mathbb{Z}$, then $\exp_n((\lambda+\lambda')x) = \exp_n(\lambda x) \cdot \exp_n(\lambda' x)$ for all scalars λ, λ'. Using Theorem 4, Ch. III, Par. 4 in [4], we get that the map $\exp_n$ is a formal group isomorphism. But this map is polynomial. Hence, it is a polynomial group isomorphism. $\square$

Corollary 2. *For all pairs* (x, y) *of elements of* $G_n(\mathfrak{g})$*,*

$$x \star y = \log_n(\exp_n(x) \cdot \exp_n(y)).$$

We point out that the exponential map of the polynomial group $J_n(\mathfrak{g})$ is provided by restricting the map $\exp_n$ to $J_n(\mathfrak{g})$. This can directly be deduced from the equality $\exp_n(\sigma.x) = \sigma.\exp_n(x)$, where σ is a permutation and x belongs to $G_n(\mathfrak{g})$. More generally, the exponential map commutes with each polynomial group automorphism (it comes from uniqueness of the exponential map). This implies the following corollary.

Corollary 3. *For all pairs* (x, y) *of elements in* $J_n(\mathfrak{g})$*,*

$$x \star y = \log_n(\exp_n(x) \cdot \exp_n(y)).$$

Lastly, we can check that the map sequence $(\exp_n)$ is compatible which the projective system $(\Pi_{n,k})$: for all $n \leq k$ and for all $x \in G_n(\mathfrak{g})$,

$$\exp_k(\Pi_{n,k}(x)) = \Pi_{n,k}(\exp_n(x)).$$

Hence, the projective limit of the sequence $(\exp_n)$ can be formed and we obtain an exponential map $\exp_\infty$ defined on $G_\infty(\mathfrak{g})$ (respectively on $J_\infty(\mathfrak{g})$). Similarly, the sequence $(\log_n)$ provides an inverse map $\log_\infty$ and then, for x, y elements of $G_\infty(\mathfrak{g})$ (respectively elements of $J_\infty(\mathfrak{g})$), we obtain

$$x \star y = \log_\infty(\exp_\infty(x) \cdot \exp_\infty(y)),$$

where $\star$ denotes the product given by the Campbell-Haussdorf formula for the natural Lie algebra structure of $G_\infty(\mathfrak{g})$ (respectively of $J_\infty(\mathfrak{g})$).

6 The case of Lie triple systems

In this part, we state some results obtained by pushing further the preceding construction. Proofs can be found in [5].

Let $\mathfrak{q}$ be a Lie triple system over the ring $\mathbb{K}$, namely $\mathfrak{q}$ is a $\mathbb{K}$-module, endowed with a trilinear bracket $[.,.,.]$ such that, for all $x, y, z, u, v \in \mathfrak{q}$, :

$$\begin{array}{ll} \text{(STL1)} & [x,y,z] = -[y,x,z] \\ \text{(STL2)} & [x,y,z] + [y,z,x] + [z,x,y] = 0 \\ \text{(STL3)} & [u,v,[x,y,z]] = [[u,v,x],y,z] + [x,[u,v,y],z] + [x,y,[u,v,z]]. \end{array}$$

We use the preceding construction (polynomial groups associated to a Lie algebra) in order to define a sequence of "polynomial symmetric spaces" associated to the Lie triple system $\mathfrak{q}$. Indeed, every Lie triple system can be embedded in a Lie algebra with involution, called its standard embedding. Roughly, this Lie algebra is given by

$$\mathfrak{g} = \mathfrak{q} \oplus [\mathfrak{q}, \mathfrak{q}],$$

and the Lie algebra involution σ is such that $\mathfrak{q}$ is its -1 eigenspace.

We denote by $\pi_{\mathfrak{q}}$, resp. $\pi_{[\mathfrak{q},\mathfrak{q}]}$ the projections from $\mathfrak{g}$ onto $\mathfrak{q}$, resp. $[\mathfrak{q}, \mathfrak{q}]$. The module $G_n(\mathfrak{g})$ is then the direct sum of the two sub-modules $G_n(\mathfrak{q})$ and $G_n([\mathfrak{q}, \mathfrak{q}])$. Furthermore, the projections $\pi_{\mathfrak{q}}$ and $\pi_{[\mathfrak{q},\mathfrak{q}]}$ give rise to projections from $G_n(\mathfrak{g})$ onto the two sub-modules $G_n(\mathfrak{q})$ and $G_n([\mathfrak{q}, \mathfrak{q}])$, which are still denoted by $\pi_{\mathfrak{q}}$ and $\pi_{[\mathfrak{q},\mathfrak{q}]}$. Similarly, the involution σ gives rise to an involution σ of the group $G_n(\mathfrak{g})$. Let us introduce the set

$$M_n(\mathfrak{q}) = \{X \in G_n(\mathfrak{g}) | \sigma(X) = X^{-1}\}$$

Theorem 3. *The map*

$$\begin{array}{cccc} \varphi : & M_n(\mathfrak{q}) & \longrightarrow & G_n(\mathfrak{q}) \\ & X & \longmapsto & \pi_{\mathfrak{q}}(X). \end{array}$$

is one-to-one, and the $\mathbb{K}$-module $G_n(\mathfrak{q})$, endowed with the product μ defined by

$$\mu(x,y) = \varphi(\varphi^{-1}(x) \cdot \sigma(\varphi^{-1}(y)) \cdot \varphi^{-1}(x)),$$

is a polynomial symmetric space.

The notion of polynomial symmetric space involved in this theorem is the natural one (where we refer to the notion of symmetric space given in [9]):

Definition 6. *Let V be a module over the ring $\mathbb{K}$, endowed with a product $\mu : V \times V \longrightarrow V$. The module V is said to be a polynomial symmetric space over $\mathbb{K}$ of degree at most k if and only if, for all $x, y, z \in V$,*

$$\begin{array}{ll} \textit{(SP1)} & \mu(x,x) = x, \\ \textit{(SP2)} & \mu(x,\mu(x,y)) = y, \\ \textit{(SP3)} & \mu(x,\mu(y,z)) = \mu(\mu(x,y),\mu(x,z)), \\ \textit{(SP4)} & \mu(0,x) = -x + deg(2), \end{array}$$

and for all integers $n > 1$, the map

$$\mu_n : (x_1, \ldots, x_n) \longrightarrow \mu(x_1, \mu(x_2, \ldots \mu(x_{n-1}, x_n)))$$

is polynomial of degree at most k.

The module V is said to be a polynomial symmetric space over $\mathbb{K}$ if and only if there exists $k \in \mathbb{N}$ such that V is a polynomial symmetric space over $\mathbb{K}$ of degree at most k.

Thus, we have associated to the Lie triple system $\mathfrak{q}$ a structure of polynomial symmetric space on the augmentation ideal $G_n(\mathfrak{q})$. However, except for small n, it seems to be difficult to get an explicit formula for the product μ.

In particular, the proof of the functoriality of this construction is rather involved (see [5]).

References

[1] W. Bertram. *Differential geometry, Lie groups and symmetric spaces over general base fields and rings.* Memoirs of the AMS, to appear. arXiv:math.DG/0502168, 2005.

[2] N. Bourbaki. *Éléments de mathématique. XI. Première partie: Les structures fondamentales de l'analyse. Livre II: Algèbre. Chapitre IV: Polynomes et fractions rationnelles. Chapitre V: Corps commutatifs.* Actualités Sci. Ind., no. 1102. Hermann et Cie., Paris, 1950.

[3] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris, 1970.

[4] N. Bourbaki. *Éléments de mathématique. Fasc. XXXVII. Groupes et algèbres de Lie. Chapitre II: Algèbres de Lie libres. Chapitre III: Groupes de Lie.* Hermann, Paris, 1972. Actualités Scientifiques et Industrielles, No. 1349.

[5] Manon Didry. *Sructures algébriques sur les espaces symétriques.* Thèse de doctorat, Nancy, 2006.

[6] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[7] J-L. Loday. Une version non commutative des algèbres de Lie: les algèbres de Leibniz. *Enseign. Math. (2)*, 39(3-4):269–293, 1993.

[8] O. Loos. Reflexion spaces and homogeneous symmetric spaces. *Bull. Amer. Math. Soc.*, 73:250–253, 1967.

[9] O. Loos. *Symmetric spaces. I: General theory.* W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[10] J-P. Serre. *Lie algebras and Lie groups*, volume 1964 of *Lectures given at Harvard University.* W. A. Benjamin, Inc., New York-Amsterdam, 1965.