Publ. Math. Debrecen
61 / 1-2 (2002), 87–118

Tangential structure of formal Bruck loops

By GÁBOR P. NAGY (Szeged)

Abstract. In the theory of loops, the class of local analytic Bruck loop plays a substantial role, mainly because of its strong relation with symmetric spaces. Like for formal groups, one can derive the concept of formal loops from the classical theory of local analytic loops in a natural way. Also the process of localization of algebraic loops leads to formal loops. In this paper, we extend some results from the theory of local analytic Bruck loops and of formal groups to the category of formal Bruck loops.

1. Introduction

Natural generalizations of the concept of group are Moufang and Bol loops. An important subclass of the latter is the class of Bruck loops. Local Bruck loops are strongly related to local symmetric spaces (in the sense of Loos [Loo69]), since the local translations of local symmetric spaces define the set of (right) translations of a local Bruck loop and conversely (cf. [NS98], [NS02]).

The concept of formal loops (just like formal groups) is derived in a natural way from the classical theory of local analytic loops: instead of considering the absolutely convergent Taylor expansion of the loop multiplications, one can define formal "product" and "inverting rules" using formal power series over an arbitrary field ([Die57], [Die73], [Car62], [Sel67]).

In Section 2, we introduce the concept of formal Bruck loops and define their tangential structures as the vector space of certain derivations.

Mathematics Subject Classification: 14L05, 20N05, 16W60.
Key words and phrases: algebraic loop, Bruck loop, Bol loop, Lie triple system, formal groups, Cartier duality.

Supported by the "János Bolyai Fellowship" and the OTKA grants F030737, T029849.

We also explain the *process of localization*, creating a relationship between the category of algebraic loops and the category of formal loops.

In Section 3, we first consider the concept of *restricted Lie triple systems* and prove a result concerning their embeddability in restricted Lie algebras (Theorem 3.2). Using methods of the theory of local analytic Bruck loops we show that *the tangent space of a formal Bruck loop can be endowed with the structure of a (restricted) Lie triple system* (Theorem 3.6). In the last part of the section, we relate the infinitesimal Lie triple system of a formal Bruck loop with its *formal associator* (Proposition 3.8); also, this relation is motivated by methods of local analytic Bruck loops.

After these results, it is natural to ask to what extent one can invert the above functorial map from the category of formal Bruck loops to the category of (restricted) Lie triple systems. Knowing the analogous problem for formal (and algebraic) groups, one can expect a simple answer only for the characteristic 0. Indeed, the existence of a Campbell–Hausdorff series for local analytic Bruck loops with rational coefficients (cf. [Nag99]) solves this question immediately.

However, for characteristic $p > 0$, one needs much more elaborate tools in order to handle the subject. P. Cartier [Car62] proved a functorial equivalence between the category of formal groups *of height 0* and the category of restricted Lie algebras of characteristic $p > 0$. In Section 4, we generalize Cartier's construction and prove a *functorial equivalence* between the *category of formal Bruck loops of height 0* and the *category of restricted Lie triple systems* of characteristic 3 (Theorem 4.2).

The most commonly used notations of this paper are:

$L, \dots$	loops
$(x,y,z),\ \alpha(x,y,z)$	associator of loop elements
L'	associator subloop of L
K	algebraically closed field of definition
$\mathsf{K}[L]$	ring of regular functions on L
$\mathsf{K}[[T^1,\dots,T^n]]$	ring of formal power series in n indeterminates over K
$\mathsf{K}[[X^1,\dots,X^n,Y^1,\dots,Y^n]]$	ring of formal power series in $2n$ indeterminates over K

$\boldsymbol{T},\ \boldsymbol{X},\ \boldsymbol{Y}$	n-tuples $(T^1, \dots, T^n)$, $(X^1, \dots, X^n)$ and $(Y^1, \dots, Y^n)$
$\mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]])$	Lie algebra of derivations
$\mathrm{PDer}(\mathsf{K}[[\boldsymbol{T}]])$	space of point derivations
$\mathfrak{l}, \dots$	tangent algebras of the loops $L, \dots$
(x, y, z)	ternary operation in Lie triple systems

Definition. The set L endowed with the binary operation "$\cdot$" is a *loop* if there is a unit element $1 \in L$ such that for all $x \in L$ holds

$$x = 1 \cdot x = x \cdot 1 \tag{1}$$

and, furthermore, for any $a, b, c, d \in L$, the equations $x \cdot a = b$, $c \cdot y = d$ have unique solutions in x and y.

We denote the solutions by $x = b/a$ and $y = c\backslash d$. The property of unique solvability can be expressed equivalently by the identities

$$x \cdot (x\backslash y) = y, \quad (x/y) \cdot y = x, \quad x\backslash(x \cdot y) = y, \quad (x \cdot y)/y = x.$$

In order to define the class of *Bruck loops*, one needs the following identities:

$$x \cdot (y \cdot xz) = (x \cdot yx) \cdot z, \tag{3}$$

$$(xy)^{-1} = x^{-1}y^{-1}. \tag{4}$$

Identity (3) is called the *Bol identity*. It is known that (3) implies $1/x = x\backslash 1 = x^{-1}$ and the identity

$$x^{-1} \cdot xy = y \tag{5}$$

holds. This fact makes (4), the so called *automorphic inverse property*, meaningful.

The most common name of the class which satisfies (3) and (4) simultaneously is *Bruck loops* (cf. [NS02]). However, these loops are equivalently called *K-loops* as well; the equivalence of the different systems of axioms was shown explicitely in [KK95].

For Bruck loops, it is useful to require an extra property, namely that the map $x \mapsto x^2$ be a bijection of the underlying set L. Such loops are called *B-loops* by G. Glauberman [Gla64] and *2-divisible Bruck loops* by P. T. Nagy and K. Strambach [NS02]. However, as we will see, in the formal context this property is not relevant.

2. Algebraic and formal loops

The treatment of formal loops in this section will be the *naive* one (direct calculations with formal power series, terminology of Dieudonné), in Section 4, we will use a slightly more general definition.

2.1. Basic definitions

For this paper, X^i, Y^i, Z^i, T^i will denote indeterminates over the field K with $n \in \mathbb{N}$ and $i, j, k = 1, \dots, n$. We also put $\boldsymbol{X} = (X^1, \dots, X^n)$, $\boldsymbol{Y} = (Y^1, \dots, Y^n)$, $\boldsymbol{Z} = (Z^1, \dots, Z^n)$, $\boldsymbol{T} = (T^1, \dots, T^n)$. To avoid confusion, we use $\mathsf{K}[[\boldsymbol{T}]]$ for the ring of formal power series in n and $\mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ for the ring of formal power series in $2n$ variables. $\mathsf{K}[[\boldsymbol{T}]]$ is a local ring with unique maximal ideal $\mathcal{M}_{(\boldsymbol{T})}$ and complete with respect to the $\mathcal{M}_{(\boldsymbol{T})}$-adic topology.

The distinction between $\mathsf{K}[[\boldsymbol{T}]]$ and $\mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ is important, because for formal series the tensor product $\mathsf{K}[[\boldsymbol{T}]] \otimes \mathsf{K}[[\boldsymbol{T}]]$ is properly embedded in $\mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$. Moreover, the tensor product topology and the $\mathcal{M}_{(\boldsymbol{X}, \boldsymbol{Y})}$-adic topology are compatible and $\mathsf{K}[[\boldsymbol{T}]] \otimes \mathsf{K}[[\boldsymbol{T}]]$ can be canonically identified with a *dense subset* of $\mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$.

The definition of Bruck loops motivates the following

Definition. A *formal Bruck loop* is a system of n formal power series $\mu^i(\boldsymbol{X}, \boldsymbol{Y}) \in \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ in $2n$ variables and n power series $e^i(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ in n variables such that with the further notation $\boldsymbol{\mu} = (\mu^i)$, $\boldsymbol{e} = (e^i)$, the identities

$$\boldsymbol{X} = \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{0}) = \boldsymbol{\mu}(\boldsymbol{0}, \boldsymbol{X}) \tag{6}$$

$$\boldsymbol{\mu}(\boldsymbol{e}(\boldsymbol{X}), \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})) = \boldsymbol{Y} \tag{7}$$

$$\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Z}))) = \boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{X})), \boldsymbol{Z}) \tag{8}$$

$$\boldsymbol{e}(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})) = \boldsymbol{\mu}(\boldsymbol{e}(\boldsymbol{X}), \boldsymbol{e}(\boldsymbol{Y})) \tag{9}$$

hold.

Clearly, the identities (6)–(9) are formal analogues of the abstract loop identities (1), (5), (3) and (4), respectively.

The next lemma shows that the existence of formal inversion is not relevant for formal Bruck loops. Moreover, if $\mathrm{chr}(\mathsf{K}) \neq 2$, then the 2-divisibility is automatically given as well.

Lemma 2.1. *Let the system of formal series* $\mu^1(\boldsymbol{X},\boldsymbol{Y}),\dots,\mu^n(\boldsymbol{X},\boldsymbol{Y})\in \mathsf{K}[[\boldsymbol{X},\boldsymbol{Y}]]$ *over the field* K *satisfy the identity* (6).

a) *There exist formal power series* $e^1(\boldsymbol{T}),\dots,e^n(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ *satisfying* (7).

b) *If* $\mathrm{chr}(\mathsf{K}) \neq 2$, *then a system of power series* $\nu^1(\boldsymbol{T}),\dots,\nu^n(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ *exist with* $\boldsymbol{\mu}(\boldsymbol{\nu}(\boldsymbol{T}),\boldsymbol{\nu}(\boldsymbol{T})) = \boldsymbol{T}$ *and* $\boldsymbol{\nu}(\boldsymbol{\mu}(\boldsymbol{T},\boldsymbol{T})) = \boldsymbol{T}$.

Proof. From condition (6) follows that

$$\mu^i(\boldsymbol{X},\boldsymbol{Y}) = X^i + Y^i + \sum \text{terms of degree} \geq 1 \text{ w.r.t. } X^i \text{ and } Y^j.$$

We therefore deduce from the theorem of implicit functions for formal power series [Bou50, p. 64, Proposition 10 and p. 59, Proposition 4] that there exists n well defined formal series

$$e^i(\boldsymbol{T}) = -T^i + \sum \text{terms of degree} \geq 2 \text{ w.r.t. } T^i$$

such that (7) holds. For b), if $\mathrm{chr}(\mathsf{K}) \neq 2$, then the Jacobian of $\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{X})$ is not zero and a system of power series $\nu^1(\boldsymbol{T}),\dots,\nu^n(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ exists with $\boldsymbol{\mu}(\boldsymbol{\nu}(\boldsymbol{T}),\boldsymbol{\nu}(\boldsymbol{T})) = \boldsymbol{T}$ by the mentioned theorem of implicit functions. Furthermore, one has

$$\boldsymbol{\nu}(\boldsymbol{\mu}(\boldsymbol{\nu}(\boldsymbol{T}),\boldsymbol{\nu}(\boldsymbol{T}))) = \boldsymbol{\nu}(\boldsymbol{T}). \tag{10}$$

On the other hand, let $\mathfrak{M}$ be the unique maximal ideal of $\mathsf{K}[[\boldsymbol{T}]]$, generated by $\{T^1,\dots,T^n\}$. Calculation modulo $\mathfrak{M}^2$ shows that

$$\nu^i(T) = \frac{1}{2}T^i + \sum \text{terms of degree} \geq 2 \text{ w.r.t. } T^i,$$

thus $T^i \mapsto \nu^i(\boldsymbol{T})$ induces an automorphism of the ring $\mathsf{K}[[\boldsymbol{T}]]$. This means that (10) is equivalent with

$$\boldsymbol{\nu}(\boldsymbol{\mu}(\boldsymbol{T},\boldsymbol{T})) = \boldsymbol{T}$$

and the lemma is proved. □

It is well known that any automorphism U of the ring $\mathsf{K}[[\boldsymbol{T}]]$ is induced by some map $T^i \mapsto u^i(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ with non-singular "Jacobian" $\frac{\partial u^i}{\partial T^j}(\mathbf{0})$, and vice versa. By some abuse of language, we will simply call such maps *substitutions* or *changes of coordinates*.

The next lemma claims that with an appropriate change of coordinates, the inverting rule $\boldsymbol{e}$ of a formal loop can be brought to the simple form $-\boldsymbol{T}$.

Lemma 2.2. *Let a system of series $e^i(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ $(i = 1, \dots, n)$ be given such that*

$$e^i(\boldsymbol{e}(\boldsymbol{T})) = T^i \quad \text{and} \quad \frac{\partial e^i}{\partial T^j}(\mathbf{0}) = -\delta^i_j.$$

Then there exists a system of series $u^i(\boldsymbol{T}), v^i(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ such that

$$u^i(\boldsymbol{v}(\boldsymbol{T})) = T^i,\ v^i(\boldsymbol{u}(\boldsymbol{T})) = T^i, \quad \text{and} \quad u^i(\boldsymbol{e}(\boldsymbol{v}(\boldsymbol{T}))) = -T^i.$$

Proof. Let us define the series $u^i(\boldsymbol{T}) = e^i(\boldsymbol{T}) - T^i$. Obviously,

$$u^i(\boldsymbol{e}(\boldsymbol{Y})) = e^i(\boldsymbol{e}(\boldsymbol{Y})) - e^i(\boldsymbol{Y}) = Y^i - e^i(\boldsymbol{Y}) = -u^i(\boldsymbol{Y}). \tag{11}$$

However, we have $\frac{\partial u^i}{\partial T^j}(\mathbf{0}) = -2\delta^i_j$, hence, by the theorem of implicit functions, there exists a system of series $v^i(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ with

$$u^i(\boldsymbol{v}(\boldsymbol{T})) = T^i, \quad \text{and} \quad v^i(\boldsymbol{u}(\boldsymbol{T})) = T^i.$$

Substituting $\boldsymbol{Y} = \boldsymbol{v}(\boldsymbol{T})$ in (11), we get $u^i(\boldsymbol{e}(\boldsymbol{v}(\boldsymbol{T}))) = -T^i$. □

Now, for any algebra over K, we define *derivations* of $\mathsf{K}[[\boldsymbol{T}]]$ as K-linear maps $D : \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}[[\boldsymbol{T}]]$, satisfying the Leibniz rule

$$D(fg) = D(f)g + fD(g), \qquad (f, g \in \mathsf{K}[[\boldsymbol{T}]]).$$

A *point derivation* of $\mathsf{K}[[\boldsymbol{T}]]$ is a K-linear map $\delta : \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}$ with

$$\delta(fg) = \delta(f)g(\mathbf{0}) + f(\mathbf{0})\delta(g), \qquad (f, g \in \mathsf{K}[[\boldsymbol{T}]]).$$

Derivations and point derivations of $\mathsf{K}[[\boldsymbol{T}]]$ are uniquely determined by their effects on $T^1, \dots, T^n$ (cf. [Bou50, p. 61, Proposition 6]). Thus, they can be written in the form

$$a^i(\boldsymbol{T}) \frac{\partial}{\partial T^i}, \quad \text{and} \quad a^i \frac{\partial}{\partial T^i}\bigg|_{\boldsymbol{T}=\mathbf{0}},$$

with $a^i(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ and $a^i \in \mathsf{K}$, respectively.

Now, let a formal Bruck loop be given with formal product $(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$ and consider a point derivation $\alpha \in \mathsf{K}[[\boldsymbol{T}]]$. Then, the map $\alpha \otimes 1 : \mathsf{K}[[\boldsymbol{T}]] \otimes \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}[[\boldsymbol{T}]]$ has a unique continuous extension

$$\alpha \mathbin{\widehat{\otimes}} 1 : \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]] \to \mathsf{K}[[\boldsymbol{T}]].$$

On the other hand, the given formal loop induces a homomorphism $\Delta : \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ of commutative algebras by $T^i \mapsto \mu^i(\boldsymbol{X}, \boldsymbol{Y})$. Let us define the map

$$\widetilde{D}_\alpha = (\alpha \widehat{\otimes} 1) \circ \Delta : \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}[[\boldsymbol{T}]].$$

Lemma 2.3. *The map $\widetilde{D} : \alpha \mapsto \widetilde{D}_\alpha$ is a K-linear embedding*

$$\mathrm{PDer}(\mathsf{K}[[\boldsymbol{T}]]) \hookrightarrow \mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]]).$$

Moreover, for $\alpha = a^i \frac{\partial}{\partial T^i}\big|_{\boldsymbol{T}=\boldsymbol{0}}$ holds

$$\widetilde{D}_\alpha = a^i \frac{\partial \mu^j}{\partial X^i}(\boldsymbol{0}, \boldsymbol{T}) \frac{\partial}{\partial T^j}.$$

Remark. We call the derivations $\widetilde{D}_\alpha$ the *L-derivations* of the formal loop $(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$. The analogy with right invariant derivations of local Lie groups is obvious.

Proof. It suffices to calculate the formula for $\widetilde{D}_\alpha$. By definition, we have

$$\alpha \widehat{\otimes} 1 = a^i \left. \frac{\partial}{\partial X^i} \right|_{\boldsymbol{X}=\boldsymbol{0}, \boldsymbol{Y}=\boldsymbol{T}} \quad \text{and} \quad \Delta(f(\boldsymbol{T})) = f(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})).$$

Hence,

$$\begin{aligned} \widetilde{D}_\alpha(f(\boldsymbol{T})) &= \left(a^i \left. \frac{\partial}{\partial X^i} \right|_{\boldsymbol{X}=\boldsymbol{0}, \boldsymbol{Y}=\boldsymbol{T}} \right) (f(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}))) \\ &= a^i \frac{\partial \mu^j}{\partial X^i}(\boldsymbol{0}, \boldsymbol{T}) \frac{\partial f}{\partial T^j}(\boldsymbol{T}). \end{aligned}$$

□

2.2. Localization of algebraic loops

It is known that via the *localization process*, any algebraic group determines a formal group (see [Di57], [Sel67]). In this section, we explain this method for the class of algebraic Bruck loops and use it to describe abstractly the tangent algebra of an algebraic Bruck loop.

Let L be a Bruck loop which is an (affine) algebraic variety over the algebraically closed field K such that the $L \times L \to L$ maps $(x, y) \mapsto xy$, x/y, $x\backslash y$ are morphisms. For simplicity, we assume L to be connected of dimension n. Clearly, L is a smooth variety, that is, every point of L is simple.

We denote by $\mathfrak{o}_x(L)$ the ring of functions which are regular in x; we have $\mathsf{K}[L] = \bigcap_{x\in L} \mathfrak{o}_x(L)$ and $\mathsf{K}(L)$ is the fraction field of $\mathsf{K}[L]$. $\mathfrak{o}_x(L)$ is also called the *local ring of* L *at* x. For a simple point x of L, $\mathfrak{o}_x(L)$ is a regular local ring with maximal ideal $\mathfrak{M}_x$, we denote by $\mathfrak{O}_x(L)$ its completion with respect to the $\mathfrak{M}_x$-adic topology, and $\mathfrak{O}_x(L)$ can be identified with the ring of power series $\mathsf{K}[[\boldsymbol{T}]] = \mathsf{K}[[T^1,\dots,T^n]]$ in $n = \dim L$ indeterminates (see [Die57, no. 14]).

Let us now consider the $L\times L \to L$ morphism $\mu : (x,y) \to xy$. It maps the simple point (e,e) of $L\times L$ onto the simple point e of L, hence it defines a homomorphism μ^* of $\mathfrak{o}_e(L)$ into $\mathfrak{o}_{(e,e)}(L\times L) = \mathfrak{o}_e(L)\otimes\mathfrak{o}_e(L)$. By continuity, μ^* can be extended to a homomorphism

$$\Delta : \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}[[\boldsymbol{X},\boldsymbol{Y}]]$$

of the completions $\mathsf{K}[[\boldsymbol{T}]]$ and $\mathsf{K}[[\boldsymbol{X},\boldsymbol{Y}]]$ ($\boldsymbol{T} = (T^i),\ \boldsymbol{X} = (X^i),\ \boldsymbol{Y} = (Y^i)$). We call δ the *formal comultiplication* on $\mathsf{K}[[\boldsymbol{T}]]$. Now, for each $i = 1,\dots,n$, we define the power series $\mu^i(\boldsymbol{X},\boldsymbol{Y}) = \Delta(T^i)$.

We do the same for the inverting map $x \mapsto x^{-1}$ in order to define the power series $e^i(\boldsymbol{T})$. We write $\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}) = (\mu^i(\boldsymbol{X},\boldsymbol{Y}))$ and $\boldsymbol{e}(\boldsymbol{T}) = (e^i(\boldsymbol{T}))$. However, by Lemma 2.1, it suffices to consider the series $\mu^i(\boldsymbol{X},\boldsymbol{Y})$.

Lemma 2.4. *The formal power series* $\mu^i(\boldsymbol{X},\boldsymbol{Y})$ $(i = 1,\dots,n)$ *determine a formal Bruck loop in* n *variables.*

Proof. We start with showing the Bol identity. Let us consider the mappings

$$u_1 : (x_1,x_2,x_3,x_4) \mapsto x_1(x_2\cdot x_3x_4),$$
$$u_2 : (x_1,x_2,x_3,x_4) \mapsto (x_1\cdot x_2x_3)x_4,$$
$$v : (x_1,x_2,x_3) \mapsto (x_1,x_2,x_1,x_3).$$

We have

$$u_1^*(\boldsymbol{T}) = \boldsymbol{\mu}(\boldsymbol{X}_1,\boldsymbol{\mu}(\boldsymbol{X}_2,\boldsymbol{\mu}(\boldsymbol{X}_3,\boldsymbol{X}_4)));$$
$$u_2^*(\boldsymbol{T}) = \boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{X}_1,\boldsymbol{\mu}(\boldsymbol{X}_2,\boldsymbol{X}_3)),\boldsymbol{X}_4);$$
$$v^*(\boldsymbol{X}_1) = \boldsymbol{X}_1,\ v^*(\boldsymbol{X}_2) = \boldsymbol{X}_2,\ v^*(\boldsymbol{X}_3) = \boldsymbol{X}_1,\ v^*(\boldsymbol{X}_4) = \boldsymbol{X}_4,$$

where $\mathsf{K}[[\boldsymbol{T}]]$, $\mathsf{K}[[\boldsymbol{X}_1, \boldsymbol{X}_2, \boldsymbol{X}_3, \boldsymbol{X}_4]]$ and $\mathsf{K}[[\boldsymbol{X}_1, \boldsymbol{X}_2, \boldsymbol{X}_3]]$ are the completed local rings of L, L^4 and L^3 at e, (e, e, e, e) and (e, e, e), respectively. However, by the left Bol identity, we have $u_1 \circ v = u_2 \circ v$ and $v^* \circ u_1^* = v^* \circ u_2^*$, which implies the equality

$$\boldsymbol{\mu}(\boldsymbol{X}_1, \boldsymbol{\mu}(\boldsymbol{X}_2, \boldsymbol{\mu}(\boldsymbol{X}_1, \boldsymbol{X}_4))) = \boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{X}_1, \boldsymbol{\mu}(\boldsymbol{X}_2, \boldsymbol{X}_1)), \boldsymbol{X}_4)$$

of formal power series. This proves the Bol identity for $\boldsymbol{\mu}$, the other identities can be shown in a similar way. $\square$

A *point derivation* δ in $x \in L$ is a linear map $\mathfrak{o}_x(L) \to \mathsf{K}$ such that the Leibniz rule

$$\delta(fg) = \delta(f)g(x) + f(x)\delta(g)$$

holds for all $f, g \in \mathsf{K}[L]$. A *derivation* D on L is a linear map $\mathsf{K}(L) \to \mathsf{K}(L)$ such that

$$D(fg) = D(f)g + fD(g)$$

holds for all $f, g \in \mathsf{K}[L]$. Obviously, a (point) derivation is completely determined by its effect on $\mathsf{K}[L]$. More precisely, a linear map $\mathsf{K}[L] \to \mathsf{K}$ ($\mathsf{K}[L] \to \mathsf{K}[L]$) satisfying the Leibniz rule can be extended uniquely to a (point) derivation of $K(L)$.

It is well known that for a given point $x \in L$, the set of point derivations can be identified with the tangent space $T_x(L)$ of L in x (see [Hum75, p. 38]). Let us denote by $\mathfrak{l}$ the tangent space $T_e(L)$ at the unit element. One can associate any tangent vector $\alpha \in \mathfrak{l}$ to a derivation D_α in a well known way. For any $f \in \mathsf{K}[L]$, we define $D_\alpha(f)$ by

$$D_\alpha(f)(x) = \alpha(\tau_x f),$$

where the $\mathsf{K}(L) \to \mathsf{K}(L)$ mapping τ_x is defined by $(\tau_x f)(y) = f(yx)$. Indeed, one can use the calculations of [Hum75, p. 66 and 68] to show that $D : \alpha \mapsto D_\alpha$ is a linear embedding $\mathrm{PDer}(\mathsf{K}(L)) \hookrightarrow \mathrm{Der}(\mathsf{K}(L))$ and $D_\alpha = (\alpha \otimes 1) \circ \mu^*$ where μ^* is the loop comultiplication $\mathsf{K}[L] \to \mathsf{K}[L] \otimes \mathsf{K}[L]$.

As explained above, one can embed $\mathfrak{o}_e(L)$ in $\mathsf{K}[[\boldsymbol{T}]]$ ($\boldsymbol{T} = (T^1, \ldots, T^n)$) in a canonical way. Clearly, every (point) derivation of $\mathfrak{o}_e(L)$ can be extended to a (point) derivation of the ring of formal power series $\mathsf{K}[[\boldsymbol{T}]]$. This extension yields a natural homomorphism $\mathrm{Der}(\mathsf{K}[L]) \to \mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]])$ of Lie algebras.

In the next lemma, we use the terminology and notation of Lemma 2.3.

Lemma 2.5. *For the maps* $D : \alpha \mapsto D_\alpha$, $\widetilde{D} : \alpha \mapsto \widetilde{D}_\alpha$ *we have* $\widetilde{D}_\alpha \in \mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]])$ *and the diagram*

$$\begin{array}{ccc} T_eL & \xrightarrow{D} & \mathrm{Der}(\mathsf{K}[L]) \\ {\scriptstyle\text{natural}}\big\downarrow & & \big\downarrow{\scriptstyle\text{extensions}} \\ \mathrm{PDer}(\mathsf{K}[[\boldsymbol{T}]]) & \xrightarrow[\widetilde{D}]{} & \mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]]) \end{array}$$

commutes. The map $\mathrm{Der}(\mathsf{K}[L]) \to \mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]])$ *is an embedding of Lie algebras. Moreover, we have*

$$\widetilde{D}_\alpha = a^i \xi_i^j(\boldsymbol{T}) \frac{\partial}{\partial T^j}, \quad \text{with} \quad \alpha = a^i \frac{\partial}{\partial T^i}\bigg|_{\boldsymbol{T}=\boldsymbol{0}} \quad \text{and} \quad \xi_i^j(\boldsymbol{T}) = \frac{\partial \mu^j}{\partial X^i}(\boldsymbol{0}, \boldsymbol{T}).$$

Proof. The mappings of the diagram are well defined and the formula for $\widetilde{D}_\alpha$ holds by Lemma 2.3. Let α be a point derivation of $\mathsf{K}[L]$ with completion $\widetilde{\alpha} \in \mathrm{PDer}(\mathsf{K}[[\boldsymbol{T}]])$. The derivations $D_\alpha = (\alpha \otimes 1) \circ \mu^*$ and $\widetilde{D}_{\widetilde{\alpha}} = (\widetilde{\alpha} \mathbin{\widehat{\otimes}} 1) \circ \Delta$ are compatible since the formal comultiplication $\Delta : \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ is the completion of the comultiplication $\mu^* : \mathsf{K}[L] \to \mathsf{K}[L] \otimes \mathsf{K}[L]$ by definition. □

3. Tangential structures of formal Bruck loops

3.1. Restricted Lie triple systems

In this section, we define a restricted structure for Lie triple systems in the characteristic $p > 2$ setting, akin to the restricted structure for Lie algebras. These objects were also studied very recently and completely independently by T. L. Hodge [Hod00].

Definition. A finite dimensional vector space $\mathfrak{b}$ over a field K equipped with a trilinear operation $(.\,,.\,,.\,)$ is called a *Lie triple system* (abbrev. L.t.s.), if for all $x, y, z, u, v \in \mathfrak{b}$,

$$(x, x, y) = 0, \tag{12}$$

$$(x, y, z) + (y, z, x) + (z, x, y) = 0, \tag{13}$$

$$\begin{aligned}(u, v, (x, y, z)) = ((u, v, x), y, z) + (x, (u, v, y), z) \\ + (x, y, (u, v, z)).\end{aligned} \tag{14}$$

Given any Lie algebra $\mathfrak{g}$ and any L.t.s. $\mathfrak{b}$, we define the linear maps

$$\operatorname{ad} z : \begin{cases} \mathfrak{g} \to \mathfrak{g} \\ a \mapsto [a, x] \end{cases}, \quad \Delta_{x,y} : \begin{cases} \mathfrak{b} \to \mathfrak{b} \\ a \mapsto (a, x, y) \end{cases}, \quad D_{x,y} : \begin{cases} \mathfrak{b} \to \mathfrak{b} \\ a \mapsto (x, y, a) \end{cases}$$

and $\Delta_x = \Delta_{x,x}$ for $x, y \in \mathfrak{b}$ and $z \in \mathfrak{g}$.

Any Lie algebra $(\mathfrak{g}, [\,.\,,\,.\,])$ can be made into an L.t.s. with the operation $(x, y, z) = [[x, y], z]$. A theorem of N. Jacobson [Jac51] asserts that every L.t.s. $\mathfrak{b}$ is isomorphic to a subalgebra of a $(\mathfrak{g}, (\,.\,,\,.\,,\,.\,))$ with Lie algebra $\mathfrak{g}$. Moreover, if $\dim \mathfrak{b} = n < \infty$ then $\dim \mathfrak{g} \leq n + \binom{n}{2}$.

Given a set M, one may define a free Lie algebra $\mathfrak{L}(M)$ over the field K and $\mathfrak{L}(M) \subseteq \mathcal{F}(M)$, where $\mathcal{F}(M)$ is the free associative K-algebra on M (see [Bou89]).

By definition, the *free* L.t.s. $\mathfrak{B}(M)$ on M is a L.t.s. such that $M \subseteq \mathfrak{B}(M)$ and whenever $\mathfrak{N}$ is an L.t.s. over K and φ_0 a mapping of M into $\mathfrak{N}$, there is a unique L.t.s. homomorphism $\varphi : \mathfrak{B}(M) \to \mathfrak{N}$.

The free L.t.s. on M may be constructed by forming the free Lie algebra $\mathfrak{L}(M)$ on M, and taking the Lie triple subsystem $\mathfrak{B}$ of $(\mathfrak{L}(M), (\,.\,,\,.\,,\,.\,))$, generated by M.

If the ground field has characteristic p and if M consists of two elements x, y, then it is known that the element

$$\Lambda_p(x, y) = (x + y)^p - x^p - y^p$$

of $\mathcal{F}(M)$ is in fact in $\mathfrak{L}(M)$. Indeed, $\Lambda_p(x, y)$ is a homogenous $[\,.\,,\,.\,]$-polynomial of degree p, with integer coefficients. Therefore, if $p > 2$, $\Lambda_p(x, y)$ is a uniquely determined element of $\mathfrak{B}(M)$. Hence, it makes sense to define $\Lambda_p(u, v)$ whenever u and v are elements of an L.t.s. $\mathfrak{b}$ over K, as the image of $\Lambda_p(x, y)$ under the homomorphism of $\mathfrak{B}(M)$ into $\mathfrak{b}$ sending x into u, y into v (cf. [Sel67]).

We recall the definition of a restricted Lie algebra (Jacobson).

Definition. A *restricted Lie algebra* over a field K of prime characteristic p is a Lie algebra $\mathfrak{g}$ together with a mapping $z \mapsto z^{[p]}$ of $\mathfrak{b}$ into $\mathfrak{g}$ satisfying the identities:

$$[x, y^{[p]}] = [[x, \underbrace{y] \ldots, y}_{p}]; \tag{15}$$

$$(\alpha z)^{[p]} = \alpha^p z^{[p]}; \tag{16}$$

$$(y + z)^{[p]} = y^{[p]} + z^{[p]} + \Lambda_p(x, y); \tag{17}$$

This definition motivates the following

Definition. A *restricted Lie triple system* over a field K of prime characteristic p is an L.t.s. $\mathfrak{b}$ together with a mapping $z \mapsto z^{[p]}$ of $\mathfrak{b}$ into $\mathfrak{b}$ satisfying the identities:

$$(x, y^{[p]}, z) = (((x, \underbrace{y, y), \dots y, y), y}_{p}, z); \tag{18}$$

$$(\alpha z)^{[p]} = \alpha^p z^{[p]}; \tag{19}$$

$$(y+z)^{[p]} = y^{[p]} + z^{[p]} + \Lambda_p(x, y). \tag{20}$$

The identities (15) and (18) are equivalently expressed by $\mathrm{ad}(z^{[p]}) = (\mathrm{ad}\, z)^p$ and $D_{x,y^{[p]}} = D_{\Delta_y^{(p-1)/2}(x),y}$, respectively.

Lemma 3.1. *Let $\mathfrak{g}$ be a restricted Lie algebra over a field of characteristic $p > 2$. Let us suppose that the linear subspace $\mathfrak{b}$ of $\mathfrak{g}$ is closed under the operations $[[A, B], C]$ and $A \mapsto A^{[p]}$. Then, $\mathfrak{b}$ is a restricted Lie triple system with respect to these operations.*

Proof. Except for (18), all the defining properties of a L.t.s. can be checked easily. For (18), we have

$$\begin{aligned}(x, y^{[p]}, z) &= [[x, y^{[p]}], z] = [[[x, \underbrace{y], \dots y}_{p}], z] \\ &= (((x, \underbrace{y, y), \dots y, y), y}_{p}, z). \qquad \square\end{aligned}$$

Theorem 3.2. *Let $\mathfrak{b}$ be a restricted L.t.s. over a field of characteristic 3. Then $\mathfrak{b}$ can be embedded into a restricted Lie algebra $\mathfrak{g}$. Moreover, if $\dim \mathfrak{b} = n < \infty$, then $\dim \mathfrak{g} \le n + n^2$.*

Proof. Let us suppose that $\mathfrak{b}$ is an L.t.s. over a field K of characteristic $p = 3$. Derivations of Lie triple systems can be defined in the usual way. In order to modify Jacobson's embedding method, we need the concept of [3]-derivations. Let us put

$$\mathcal{D} = \{\delta \in \mathrm{Der}(\mathfrak{b}) \mid \delta(x^{[3]}) = (\delta(x), x, x) \quad \forall x \in \mathfrak{b}\}.$$

First we show that $\mathcal{D}$ is a restricted Lie algebra such that $D_{x,y} \in \mathcal{D}$. By (12), (13) and (18), one has $(x, y, z^{[p]}) = ((x, z, z), z, y) - ((y, z, z), z, x)$. Therefore, to show that $D_{x,y} \in \mathcal{D}$, we only have to prove the identity

$$((x, y, z), z, z) = ((x, z, z), z, y) - ((y, z, z), z, x). \tag{21}$$

We claim that (21) holds in the free L.t.s. $\mathfrak{B}$ on the set $M = \{x, y, z\}$. Indeed, $\mathfrak{B}$ is a subsystem of the free Lie algebra on M, which can be embedded in the free associative K-algebra $\mathcal{F}$. However, in $\mathcal{F}$ (21) becomes

$$[[x, y], z^3] = [[x, z^3], y] - [[y, z^3], x],$$

which follows from the Jacobi identity.

Let us now suppose $\delta, \epsilon \in \mathcal{D}$. We have

$$\begin{aligned}\delta^3(x^{[3]}) &= \delta(\delta(\delta(x), x, x)) = (\delta^3(x), x, x)\\ &\quad + 2(\delta^2(x), \delta(x), x) + (\delta^2, x, \delta(x)) + (\delta(x), x, \delta^2(x))\\ &= (\delta^3(x), x, x)\end{aligned}$$

and

$$\begin{aligned}[\delta, \epsilon](x^{[3]}) &= \delta(\epsilon(x), x, x) - \epsilon(\delta(x), x, x)\\ &= ([\delta, \epsilon](x), x, x) - 2(\delta(x), \epsilon(x), x)\\ &\quad + (\epsilon(x), x, \delta(x)) - (\delta(x), x, \epsilon(x))\\ &= ([\delta, \epsilon](x), x, x),\end{aligned}$$

whence $\delta^3, [\delta, \epsilon] \in \mathcal{D}$ and $\mathcal{D}$ is a restricted Lie subalgebra of $\mathrm{Der}(\mathfrak{b})$. Let us define the vector space $\mathfrak{g} = \mathfrak{b} \oplus \mathcal{D}$ with the operations

$$[x + \delta, y + \epsilon] = \delta(y) - \epsilon(x) + [\delta, \epsilon] + D_{x,y},$$

$$(y + \epsilon)^{[3]} = y^{[3]} + \epsilon^3 + \epsilon^2(y) - D_{\epsilon(y),y}.$$

(The [3]-map is motivated by $\Lambda_3(x, y) = (x, y, y) + (y, x, x)$.) Jacobson's proof shows that $(\mathfrak{g}, [.\,,.])$ is a Lie algebra and $\mathfrak{b} \to \mathfrak{g}$ is an embedding of an L.t.s.

Concerning the [3]-map, a straightforward calculation gives that both $[\delta, (y + \epsilon)^{[3]}]$ and $[[[\delta, y + \epsilon], y + \epsilon], y + \epsilon]$ are equal to

$$\delta(y^{[3]}) + \delta\epsilon^2(y) + [\delta, \epsilon^3] + D_{\delta\epsilon(y),y} + D_{\epsilon(y),\delta(y)}.$$

On the other hand, both $[x,(y+\epsilon)^{[3]}]$ and $[[[x,y+\epsilon],y+\epsilon],y+\epsilon]$ are equal to

$$-\epsilon^3(x)+(y,\epsilon(y),x)+D_{x,\epsilon^2(y)}+D_{x,y^{[3]}}.$$

This yields

$$[x+\delta,(y+\epsilon)^{[3]}]=[[[x+\delta,y+\epsilon],y+\epsilon],y+\epsilon],$$

which proves that $\mathfrak{g}$ is a restricted Lie algebra. Clearly, if $\dim\mathfrak{b}=n<\infty$, then $\dim\mathcal{D}\le\dim(\mathrm{Der}(\mathfrak{b}))\le n^2$. $\square$

Remark. In [Hod00], the result of the above theorem is obtained for general prime $p>2$ but under the assumption $\mathfrak{z}(\mathfrak{b})=\{z\in\mathfrak{b}\mid(z,x,y)=0\ \forall x,y\in\mathfrak{b}\}=\{0\}$.

3.2. Infinitesimal algebras of formal Bruck loops

In this section, we start using heavily the Bol property of our formal loops. The applied calculation methods rely on [Nôn61].

Let $\mu^i(\boldsymbol{X},\boldsymbol{Y})$, $e^i(\boldsymbol{T})$ define a formal Bruck loop, $i=1,\dots,n$, and let us introduce the power series $\varphi^i(\boldsymbol{X},\boldsymbol{Y})=\mu^i(\boldsymbol{X},\boldsymbol{\mu}(\boldsymbol{Y},\boldsymbol{X}))$.

Lemma 3.3. *Assume that K is a field of characteristic $\neq 2$. Then we have*

(i) $\dfrac{\partial\mu^i}{\partial X^j}(\boldsymbol{X},\boldsymbol{0})=\delta^i_j$, $\dfrac{\partial\mu^i}{\partial Y^j}(\boldsymbol{0},\boldsymbol{Y})=\delta^i_j$;

(ii) $\dfrac{\partial e^i}{\partial T^k}(\boldsymbol{0},\boldsymbol{0})=-\delta^i_k$;

(iii) $\dfrac{\partial\varphi^i}{\partial X^j}(\boldsymbol{0},\boldsymbol{0})=2\delta^i_j$, $\dfrac{\partial\varphi^i}{\partial Y^j}(\boldsymbol{0},\boldsymbol{Y})=\delta^i_j$.

(iv) *With the notations $\chi^i_k(\boldsymbol{T})=\dfrac{\partial\varphi^i}{\partial X^k}(\boldsymbol{0},\boldsymbol{T})$ and $\xi^i_k(\boldsymbol{T})=\dfrac{\partial\mu^i}{\partial X^k}(\boldsymbol{0},\boldsymbol{T})$, the matrices $(\chi^i_k(\boldsymbol{T}))_{i,k}$ and $(\xi^i_k(\boldsymbol{T}))_{i,k}$ are invertible over $\mathsf{K}[[\boldsymbol{T}]]$.*

Proof. Differentiating the identities

$$\mu^i(\boldsymbol{X},\boldsymbol{0})=X^i,\quad \mu^i(\boldsymbol{0},\boldsymbol{Y})=Y^i,\quad \varphi^i(\boldsymbol{0},\boldsymbol{Y})=Y^i,$$

we get (i) and the second equation of (iii). Differentiating the identity

$$\mu^i(\boldsymbol{e}(\boldsymbol{X}),\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}))=Y^i$$

by X^k, we have

$$\frac{\partial \mu^i}{\partial X^j}(\boldsymbol{e}(\boldsymbol{X}), \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}))\frac{\partial e^j}{\partial X^k}(\boldsymbol{X}) + \frac{\partial \mu^i}{\partial Y^j}(\boldsymbol{e}(\boldsymbol{X}), \mu(\boldsymbol{X}, \boldsymbol{Y}))\frac{\partial \mu^j}{\partial X^k}(\boldsymbol{X}, \boldsymbol{Y}) = 0.$$

Substituting $\boldsymbol{X} = \boldsymbol{Y} = \boldsymbol{0}$, we get

$$\frac{\partial \mu^i}{\partial X^j}(\boldsymbol{0}, \boldsymbol{0})\frac{\partial e^j}{\partial T^k}(\boldsymbol{0}) + \frac{\partial \mu^i}{\partial Y^j}(\boldsymbol{0}, \boldsymbol{0})\frac{\partial \mu^j}{\partial X^k}(\boldsymbol{0}, \boldsymbol{0}) = 0,$$

which implies (ii).

For the first equation of (iii), we differentiate both sides of $\varphi^i(\boldsymbol{X}, \boldsymbol{Y}) = \mu^i(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{X}))$ by X^j and put $\boldsymbol{Y} = \boldsymbol{0}$. Then we have

$$\frac{\partial \varphi^i}{\partial X^j}(\boldsymbol{X}, \boldsymbol{0}) = \frac{\partial \mu^i}{\partial X^j}(\boldsymbol{X}, \boldsymbol{X}) + \frac{\partial \mu^i}{\partial Y^j}(\boldsymbol{X}, \boldsymbol{X}), \tag{22}$$

which gives (iii) by (i).

Finally, by (i) and (iii), if $\mathrm{char}(\mathsf{K}) \neq 2$, then the power series $\det(\xi^i_k(\boldsymbol{T}))$, $\det(\chi^i_k(\boldsymbol{T}))$ are invertible elements of the ring $\mathsf{K}[[\boldsymbol{T}]]$, hence the matrices are invertible over $\mathsf{K}[[\boldsymbol{T}]]$. □

Lemma 3.4. *Let us consider the formal loop B over a field K with $\mathrm{char}(\mathsf{K}) \neq 2$. Let us assume that the formal product $(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$ of B satisfies the formal Bol identity* (8) *and define the elements*

$$\xi^i_j(\boldsymbol{Y}) = \frac{\partial \mu^i}{\partial X^j}(\boldsymbol{0}, \boldsymbol{Y}) \in \mathsf{K}[[\boldsymbol{Y}]] \quad \textit{and} \quad E_k = \xi^i_k(\boldsymbol{Y})\frac{\partial}{\partial Y^i} \in \mathrm{Der}(\mathsf{K}[[\boldsymbol{Y}]]).$$

Then the E_k's span the space $\mathcal{V}$ of L-derivations of B; the space $\mathcal{V}$ is closed under the operation $[[A, B], C]$.

Proof. We have to show the last statement only. The abstract Bol identity (3) is equivalent with the identity $t \cdot yx = (t \cdot xt) \cdot t^{-1}y$. Its formal version is

$$\mu^i(\boldsymbol{T}, \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})) = \mu^i(\boldsymbol{\varphi}(\boldsymbol{T}, \boldsymbol{X}), \boldsymbol{\mu}(\boldsymbol{e}(\boldsymbol{T}), \boldsymbol{Y})).$$

Differentiating by T^k and putting $\boldsymbol{T} = \boldsymbol{0}$ yields

$$\begin{aligned} \frac{\partial \mu^i}{\partial X^k}(\boldsymbol{0}, \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})) = {} & \frac{\partial \mu^i}{\partial X^j}(\boldsymbol{X}, \boldsymbol{Y})\frac{\partial \varphi^j}{\partial X^k}(\boldsymbol{0}, \boldsymbol{X}) \\ & - \frac{\partial \mu^i}{\partial Y^j}(\boldsymbol{X}, \boldsymbol{Y})\frac{\partial \mu^j}{\partial X^k}(\boldsymbol{0}, \boldsymbol{Y}). \end{aligned} \tag{23}$$

Let us define the $\mathsf{K}[[\boldsymbol{X},\boldsymbol{Y}]]$-derivations

$$A_k = \chi_k^i(\boldsymbol{X})\frac{\partial}{\partial X^i},$$

and put $F_k = A_k - E_k$. Then (23) can equivalently be written as

$$F_k(\mu^i(\boldsymbol{X},\boldsymbol{Y})) = \xi_k^i(\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y})). \tag{24}$$

Applying (24) several times, we get

$$\begin{aligned}
[[F_k,F_\ell],F_m](\mu^i) &= (F_kF_\ell F_m - F_\ell F_k F_m - F_m F_k F_\ell + F_m F_\ell F_k)(\mu^i)\\
&= F_kF_\ell(\xi_m^i(\boldsymbol{\mu})) - F_\ell F_k(\xi_m^i(\boldsymbol{\mu}))\\
&\quad - F_mF_k(\xi_\ell^i(\boldsymbol{\mu})) + F_mF_\ell(\xi_k^i(\boldsymbol{\mu}))\\
&= F_k\left(\frac{\partial \xi_m^i}{\partial Y^r}(\boldsymbol{\mu})\xi_\ell^r(\boldsymbol{\mu})\right) - F_\ell\left(\frac{\partial \xi_m^i}{\partial Y^r}(\boldsymbol{\mu})\xi_k^r(\boldsymbol{\mu})\right)\\
&\quad - F_m\left(\frac{\partial \xi_\ell^i}{\partial Y^r}(\boldsymbol{\mu})\xi_k^r(\boldsymbol{\mu})\right) + F_m\left(\frac{\partial \xi_k^i}{\partial Y^r}(\boldsymbol{\mu})\xi_\ell^r(\boldsymbol{\mu})\right)\\
&= U_{k\ell m}^i(\boldsymbol{\mu}),
\end{aligned}$$

where

$$\begin{aligned}
U_{k\ell m}^i(\boldsymbol{T}) = {}& \frac{\partial \xi_m^i}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi_\ell^r}{\partial Y^s}(\boldsymbol{T})\xi_k^s(\boldsymbol{T}) - \frac{\partial \xi_m^i}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi_k^r}{\partial Y^s}(\boldsymbol{T})\xi_\ell^s(\boldsymbol{T})\\
&- \frac{\partial \xi_\ell^i}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi_k^r}{\partial Y^s}(\boldsymbol{T})\xi_m^s(\boldsymbol{T}) + \frac{\partial \xi_k^i}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi_\ell^r}{\partial Y^s}(\boldsymbol{T})\xi_m^s(\boldsymbol{T})\\
&- \frac{\partial^2 \xi_\ell^i}{\partial Y^r \partial Y^s}(\boldsymbol{T})\xi_m^s(\boldsymbol{T})\xi_k^r(\boldsymbol{T}) + \frac{\partial^2 \xi_k^i}{\partial Y^r \partial Y^s}(\boldsymbol{T})\xi_m^s(\boldsymbol{T})\xi_\ell^r(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]].
\end{aligned}$$

On the other hand, straightforward calculation gives

$$[[E_k,E_\ell],E_m] = U_{k\ell m}^i(\boldsymbol{Y})\frac{\partial}{\partial Y^i}, \tag{25}$$

for the series $U_{k\ell m}^i(\boldsymbol{Y})$ with $k,\ell,m = 1,\dots,n$. Moreover, the invertibility of the matrices $(\chi_k^i(\boldsymbol{T}))_{i,k}$ and $(\xi_k^i(\boldsymbol{T}))_{i,k}$ implies the existence of elements

$w^i_{k\ell m}(\boldsymbol{T}), \bar{w}^i_{k\ell m}(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ such that

$$[[E_k, E_\ell], E_m] = w^i_{k\ell m}(\boldsymbol{Y})E_i, \qquad (26)$$
$$[[A_k, A_\ell], A_m] = \bar{w}^i_{k\ell m}(\boldsymbol{X})A_i$$

hold for all $k, \ell, m = 1, \ldots, n$. (25) and (26) imply

$$U^i_{k\ell m}(\boldsymbol{Y}) = w^j_{k\ell m}(\boldsymbol{Y})\xi^i_j(\boldsymbol{Y}).$$

Combining this with $[[F_k, F_\ell], F_m](\mu^i) = U^i_{k\ell m}(\boldsymbol{\mu})$, we obtain

$$[[F_k, F_\ell], F_m](\mu^i(\boldsymbol{X}, \boldsymbol{Y})) = w^j_{k\ell m}(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}))\xi^i_j(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})). \qquad (27)$$

By $[A_k, E_\ell] = 0$, we have

$$[[F_k, F_\ell], F_m](\mu^i) = \bar{w}^j_{k\ell m}(\boldsymbol{X})A_j(\mu^i) - w^j_{k\ell m}(\boldsymbol{Y})E_j(\mu^i). \qquad (28)$$

Using Lemma 3.3, we get

$$\left.\begin{aligned} A_j(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} &= \chi^s_j(\boldsymbol{0})\frac{\partial \mu^i}{\partial X^s}(\boldsymbol{0}, \boldsymbol{Y}) = 2\xi^i_j(\boldsymbol{Y}), \\ A_j(\varphi^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} &= \chi^s_j(\boldsymbol{0})\frac{\partial \varphi^i}{\partial X^s}(\boldsymbol{0}, \boldsymbol{Y}) = 2\chi^i_j(\boldsymbol{Y}), \\ E_j(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} &= \xi^s_j(\boldsymbol{Y})\frac{\partial \mu^i}{\partial Y^s}(\boldsymbol{0}, \boldsymbol{Y}) = \xi^i_j(\boldsymbol{Y}). \end{aligned}\right\} \qquad (29)$$

(29) can be applied to substitute $\boldsymbol{X} = \boldsymbol{0}$ in (28):

$$\begin{aligned} &[[F_k, F_\ell], F_m](\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} \\ &\qquad = 2\bar{w}^j_{k\ell m}(\boldsymbol{0})\xi^i_j(\boldsymbol{Y}) - w^j_{k\ell m}(\boldsymbol{Y})\xi^i_j(\boldsymbol{Y}). \end{aligned} \qquad (30)$$

Substituting $\boldsymbol{X} = \boldsymbol{0}$ in (27), we obtain

$$[[F_k, F_\ell], F_m](\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} = w^j_{k\ell m}(\boldsymbol{Y})\xi^i_j(\boldsymbol{Y}). \qquad (31)$$

Now, if we compare (30) with (31) and use the invertibility of $(\xi^i_k(\boldsymbol{T}))_{i,k}$, we obtain the final result

$$w^j_{k\ell m}(\boldsymbol{Y}) = \bar{w}^j_{k\ell m}(\boldsymbol{0}) = w^j_{k\ell m}(\boldsymbol{0}) \in \mathsf{K} \qquad (32)$$

for all $k, \ell, m, j = 1, \ldots, n$. □

Lemma 3.5. *Let us use the assumptions and notation of Lemma 3.4. If* $\mathrm{char}(\mathsf{K}) = p > 0$*, then the space* $\mathcal{V}$ *of* L*-derivations is closed under the operation* $A \mapsto A^p$.

Proof. The equation (24) gives by induction, that for any $m > 0$, there exist formal power series $U_k^i(\boldsymbol{\mu})$ such that

$$F_k^m(\mu^i) = U_k^i(\boldsymbol{\mu}) \quad \text{and} \quad E_k^m(Y^i) = U_k^i(\boldsymbol{Y})$$

hold for all $i, k = 1, \dots, n$. Put $m = p$, then E_k^p is a derivation and $E_k^p = U_k^i(\boldsymbol{Y})\frac{\partial}{\partial Y^i}$. Moreover, from Lemma 3.3(iv) follows the existence of power series $w_k^j(\boldsymbol{Y}) \in \mathsf{K}[[\boldsymbol{Y}]]$ with

$$E_k^m = w_k^j(\boldsymbol{Y})E_j.$$

Thus,

$$F_k^m(\mu^i) = w_k^j(\boldsymbol{\mu})\xi_j^i(\boldsymbol{\mu}). \tag{33}$$

Still using Lemma 3.3(iv), we can put $A_k^p = \bar{w}_k^i(\boldsymbol{X})A_k$ for some series $\bar{w}_k^i(\boldsymbol{X}) \in \mathsf{K}[[\boldsymbol{X}]]$. By $[A_k, E_k] = 0$, we have

$$F_k^p(\mu^i) = A_k^p(\mu^i) - E_k^p(\mu^i) = \bar{w}_k^j(\boldsymbol{X})A_j(\mu^i) - w_k^j(\boldsymbol{Y})E_j(\mu^i). \tag{34}$$

Setting $\boldsymbol{X} = \mathbf{0}$ in (33) and (34) and applying (29), we obtain

$$w_k^j(\boldsymbol{Y})\xi_j^i(\boldsymbol{Y}) = 2\bar{w}_k^j(\mathbf{0})\xi_j^i(\boldsymbol{Y}) - w_k^j(\boldsymbol{Y})\xi_j^i(\boldsymbol{Y}),$$

which gives

$$w_k^i(\boldsymbol{Y}) = \bar{w}_k^i(\mathbf{0}) = w_k^i(\mathbf{0}) \in \mathsf{K}$$

for all $i, k = 1, \dots, n$. □

Theorem 3.6. *The space of formally invariant derivations of a formal Bruck loop forms a Lie triple system. Moreover, if the characteristic of the ground field is* $p > 2$*, then the Lie triple system is restricted.*

Proof. Since the space of derivations is an associative algebra, the statements follow immediately from Lemma 3.1, Lemma 3.4 and Lemma 3.5. □

We are now able to formulate our main result on the tangent structure of algebraic Bruck loops.

Theorem 3.7. *Let L be an algebraic Bruck loop over an algebraically closed field* K *with* $\mathrm{char}(\mathsf{K}) \neq 2$. *We define the tangent algebra* $\mathfrak{l}$ *of* L *as the space of derivations* $\{D_\alpha \mid \alpha \in T_e(L)\}$ *of* $\mathsf{K}(L)$. *Then* $\mathfrak{l}$ *is a Lie triple system with respect to the operation* $[[D_\alpha, D_\beta], D_\gamma]$. *Moreover, if* $\mathrm{char}(\mathsf{K}) = p > 0$, *then the map* $D_\alpha \mapsto D_\alpha^p$ *makes* $\mathfrak{l}$ *into a restricted Lie triple system.*

Proof. We keep using the notation of Section 2. By Lemma 2.5, the correspondence $D_\alpha \leftrightarrow a^k E_k$ defines an isomorphism between $\mathfrak{l}$ and the space $\mathcal{V}$ spanned by the E_k's. Hence, Theorem 3.6 implies the theorem. □

3.3. The infinitesimal formal associator

Let us consider a system of power series $\mu^i(\boldsymbol{X}, \boldsymbol{Y})$, $e^i(\boldsymbol{T})$ defining a formal Bruck loop. Let us assume that $e^i(\boldsymbol{T}) = -T^i$ holds. This and the automorphic inverse property together imply that the series μ^i to has the form

$$\mu^i(\boldsymbol{X}, \boldsymbol{Y}) = X^i + Y^i + \mu_3^i(\boldsymbol{X}, \boldsymbol{Y}) + o(5), \tag{35}$$

where $\mu_3^i(\boldsymbol{X}, \boldsymbol{Y})$ is a homogenous polynomial of degree 3 in $X^1, \ldots, Y^n$. Moreover, $\mu_3^i(\boldsymbol{X}, -\boldsymbol{X}) = 0$ and $\mu_3^i(-\boldsymbol{X}, -\boldsymbol{Y}) = -\mu_3^i(\boldsymbol{X}, \boldsymbol{Y})$ hold. We define the *associator series*

$$\alpha^i(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = \mu^i(\boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z}), -\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{Z}))).$$

Now,

$$\alpha^i(\boldsymbol{0}, \boldsymbol{Y}, \boldsymbol{Z}) = \alpha^i(\boldsymbol{X}, \boldsymbol{0}, \boldsymbol{Z}) = \alpha^i(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{0}) = 0$$

forces $\alpha^i(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z})$ to have the form

$$\alpha^i(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = \alpha_3^i(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) + o(5),$$

where α_3^i is a homogenous polynomial

$$\alpha_3^i(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = \sum_{k,\ell,m=1}^{n} \omega_{k\ell m}^i \, X^k Y^\ell Z^m$$

of degree 3. Putting $\langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle = \alpha_3^i(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ for the elements $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathsf{K}^n$, we get a trilinear map $(\mathsf{K}^n)^3 \to \mathsf{K}^n$. We call $\langle . , . , . \rangle$ *the infinitesimal formal associator* of the formal loop; it is clear that this concept is the precise analog of the local analytic construction.

Proposition 3.8. *Let us use the above notation and assumptions for the power series μ^i of a formal Bruck loop. Let us identify the vector spaces K^n and $\mathrm{PDer}(\mathsf{K}[[\boldsymbol{Y}]])$ via the canonical bases*

$$\{\epsilon(i) \mid i = 1, \dots, n\} \quad \text{and} \quad \left\{ \frac{\partial}{\partial T^i}\bigg|_{\boldsymbol{T}=\mathbf{0}} \mid i = 1, \dots, n \right\}.$$

Using this identification, let us define the K-linear map

$$\Phi : \mathsf{K}^n \to \mathfrak{b} \leq \mathrm{Der}(\mathsf{K}[[\boldsymbol{Y}]]), \qquad \boldsymbol{x} \mapsto \widetilde{D}_{\boldsymbol{x}}.$$

Then Φ is an isomorphism between the ternary algebras $(\mathsf{K}^n, \langle . , . , . \rangle)$ and $(\mathfrak{b}, [[. , .], .])$.

Proof. Concerning the infinitesimal algebra $\mathfrak{b}$, we use the notation of Section 3.2. From $\xi^i_k(\mathbf{0}) = \delta^i_k$ follows that Φ maps the canonical basis element $\epsilon(i)$ of K^n onto the basis element E_i of $\mathfrak{b}$. Let us denote by $\omega^i_{k\ell m}$ and $w^i_{k\ell m}$ the structure constants of $(\mathsf{K}^n, \langle . , . , . \rangle)$ and $(\mathfrak{b}, [[. , .], .])$ in this basis, respectively. We will show that

$$w^i_{k\ell m} = -2\omega^i_{k\ell m} \tag{36}$$

holds for all $k, \ell, m, i = 1, \dots, n$. We remark that this fact is in accordance with [MS90, p. 419, (8.6)].

Since we have

$$[[E_k, E_\ell], E_m] = U^i_{k\ell m}(\boldsymbol{Y}) \frac{\partial}{\partial Y^i} = w^i_{k\ell m} E_i,$$

$U^i_{k\ell m}(\boldsymbol{Y}) = w^j_{k\ell m} \xi^i_j(\boldsymbol{Y})$ holds, implying

$$w^i_{k\ell m} = U^i_{k\ell m}(\mathbf{0}) = \frac{\partial^2 \xi^i_k}{\partial Y^\ell \partial Y^m}(\mathbf{0}) - \frac{\partial^2 \xi^i_\ell}{\partial Y^k \partial Y^m}(\mathbf{0}),$$

for $\mu^i(\boldsymbol{X}, \boldsymbol{Y})$ does not contain quadratic terms and $\frac{\partial \xi^i_j}{\partial Y^s}(\mathbf{0}) = 0$ for all $i, j, s = 1, \dots, n$. If we put

$$\mu^i_3(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{1 \leq a < b < c \leq n} g^i_{abc}(X^a, X^b, X^c, Y^a, Y^b, Y^c),$$

then we can write

$$w^i_{k\ell m} = \frac{\partial^3 g^i_{abc}}{\partial X^k \partial Y^\ell \partial Y^m}(\mathbf{0}) - \frac{\partial^3 g^i_{abc}}{\partial X^\ell \partial Y^k \partial Y^m}(\mathbf{0}) \tag{37}$$

for $\{a,b,c\} = \{k,\ell,m\}$.

On the other hand, by (35) we have

$$
\begin{aligned}
\alpha^i(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) &= \mu^i(\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}),\boldsymbol{Z}) - \mu^i(\boldsymbol{X},\boldsymbol{\mu}(\boldsymbol{Y},\boldsymbol{Z})) + \mu_3^i(\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}) \\
&\quad + \boldsymbol{Z} + o(3), -\boldsymbol{X} - \boldsymbol{\mu}(\boldsymbol{Y},\boldsymbol{Z}) + o(3)) + o(5) \\
&= \mu^i(\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}),\boldsymbol{Z}) - \mu^i(\boldsymbol{X},\boldsymbol{\mu}(\boldsymbol{Y},\boldsymbol{Z})) \\
&\quad + \mu_3^i(\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}) + \boldsymbol{Z}, -\boldsymbol{X} - \boldsymbol{\mu}(\boldsymbol{Y},\boldsymbol{Z})) + o(5) \\
&= \mu^i(\boldsymbol{X},\boldsymbol{Y}) + Z^i + \mu_3^i(\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}),\boldsymbol{Z}) - X^i - \mu^i(\boldsymbol{Y},\boldsymbol{Z}) \\
&\quad - \mu_3^i(\boldsymbol{X},\boldsymbol{\mu}(\boldsymbol{Y},\boldsymbol{Z})) + \mu_3^i(\boldsymbol{X}+\boldsymbol{Y}+\boldsymbol{Z}+o(3), \\
&\quad - \boldsymbol{X} - \boldsymbol{Y} - \boldsymbol{Z} + o(3)) + o(5) \\
&= \mu_3^i(\boldsymbol{X},\boldsymbol{Y}) + \mu_3^i(\boldsymbol{X}+\boldsymbol{Y}+o(3),\boldsymbol{Z}) \\
&\quad - \mu_3^i(\boldsymbol{Y},\boldsymbol{Z}) - \mu_3^i(\boldsymbol{X},\boldsymbol{Y}+\boldsymbol{Z}+o(3)) + o(5) \\
&= (d\mu_3^i)(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) + o(5),
\end{aligned} \tag{38}
$$

where the operator d associates the function

$$(df)(X,Y,Z) = f(X+Y,Z) + f(X,Y) - f(X,Y+Z) - f(Y,Z)$$

to a function $f(X,Y)$. Thus, we obtain

$$\alpha_3^i(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) = (d\mu_3^i)(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) = \sum_{1\le a<b<c\le n} (dg_{abc}^i)(X^a,\dots,Z^c). \tag{39}$$

Now, by (37) and (39), all we have to show is the following statement:

($*$) *For all a,b,c with $1 \le a < b < c \le n$, the coefficient of $X^kY^\ell Z^m$ in dg_{abc}^i is*

$$-\frac{1}{2}\left(\frac{\partial^3 g_{abc}^i}{\partial X^k \partial Y^\ell \partial Y^m}(\mathbf{0}) - \frac{\partial^3 g_{abc}^i}{\partial X^\ell \partial Y^k \partial Y^m}(\mathbf{0})\right)$$

for all k,ℓ,m with $\{k,\ell,m\} = \{a,b,c\}$.

However, we should not forget that the series μ^i defines a formal Bruck loop. With the help of calculations of type (38), we get

$$(d'\mu_3^i)(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) = 0 \tag{40}$$

from the formal Bol identity, where the operator d' associates the function

$$\begin{aligned}(d'f)(X,Y,Z) &= f(2X+Y,Z)+f(X,Y+X)+f(Y,X)\\ &\qquad - f(X,Y+X+Z)-f(Y,X+Z)-f(X,Z)\end{aligned}$$

to a function $f(X,Y)$. For any $1 \le a,b,c \le n$, putting $X^j = Y^j = Z^j = 0$ for all $j \notin \{a,b,c\}$, we obtain

$$(d'g^i_{abc})(X^a,X^b,X^c,Y^a,Y^b,Y^c,Z^a,Z^b,Z^c) = 0.$$

Conversely, if $d'g^i_{abc} = 0$ holds for all $1 \le a,b,c \le n$, then (40) is satisfied. Using a short "Maple V" program, one can see that the homogenous polynomial g^i_{abc} satisfies $d'g^i_{abc} = 0$ if and only if it has the form

$$\begin{aligned}
& s_1\,(X^a\,X^b\,Y^a + X^b\,Y^{a2}) + s_2\,(-X^a\,(Y^c)^2 + 2\,X^c\,Y^a\,Y^c + (X^c)^2\,Y^a)\\
&\quad + s_3\,(X^c\,(Y^c)^2 + (X^c)^2\,Y_3) + s_4\,(2\,X^c\,Y^b\,Y^c - X^b\,(Y^c)^2 + (X^c)^2\,Y^b)\\
&\quad + s_5\,(-X^a\,(Y^b)^2 + 2\,X^b\,Y^a\,Y^b + (X^b)^2\,Y^a)\\
&\quad + s_6\,((X^b)^2\,Y^c - X^c\,(Y^b)^2 + 2\,X^b\,Y^b\,Y^c)\\
&\quad + s_7\,((X^b)^2\,Y^b + X^b\,(Y^b)^2) + s_8\,(X^a\,(Y^a)^2 + (X^a)^2\,Y^a)\\
&\quad + s_9\,(-X^c\,(Y^a)^2 + 2\,X^a\,Y^a\,Y^c + (X^a)^2\,Y^c)\\
&\quad + s_1 0\,(X^a\,X^b\,Y^a + (X^a)^2\,Y^b + 2\,X^a\,Y^a\,Y^b)\\
&\quad + s_{11}\,(-X^c\,Y^a\,Y^b + X^a\,X^b\,Y^c + X^a\,Y^b\,Y^c + X^b\,Y^a\,Y^c)\\
&\quad + s_{12}\,(X^a\,X^b\,Y^b + X^a\,(Y_2)^2)\\
&\quad + s_1 3\,(X^a\,X^c\,Y^a + X^c\,(Y^a)^2) + s_{14}\,(X^a\,(Y^c)^2 + X^a\,X^c\,Y^c)\\
&\quad + s_1 5\,(X^a\,X^c\,Y^b + X^c\,Y^a\,Y^b - X^b\,Y^a\,Y^c + X^a\,Y^b\,Y^c)\\
&\quad + s_{16}\,(X^b\,Y^a\,Y^c - X^a\,Y^b\,Y^c + X^c\,Y^a\,Y^b + X^b\,X^c\,Y^a)\\
&\quad + s_{17}\,(X^b\,X^c\,Y^c + X^b\,(Y^c)^2) + s_{18}\,(X^c\,(Y^b)^2 + X^b\,X^c\,Y^b)
\end{aligned}$$

with $s_1, \ldots, s_{18} \in \mathsf{K}$. Some more (symbolic, thus programmable) calculation gives that polynomials of the above form satisfy $(*)$. $\square$

4. The Cartier duality of formal Bruck loops

In this section, we extend the definition given in Section 2 for formal loops. The new definition enables us to prove a functorial equivalence between the category of (restricted) Lie triple systems and a certain subcategory of the category of formal Bruck loops of characteristic 0 and 3. Our construction generalizes an analogous result of P. Cartier [Car62, Théorème 3, 4] on (restricted) Lie algebras and formal groups.

4.1. Generalized formal loops

In Section 2, we defined a formal loop as an n-tuple $\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}) = (\mu^i(\boldsymbol{X},\boldsymbol{Y}))$ of elements of the ring $\mathsf{K}[[\boldsymbol{X},\boldsymbol{Y}]]$ of formal powers in $2n$ variables. In this case, the ring $\mathsf{K}[[\boldsymbol{T}]]$ ($\boldsymbol{T} = (T^1,\ldots,T^n)$) of formal power series in n variables took over the role of the ring of the regular functions of an algebraic loop. For this reason, we will call $\mathsf{K}[[\boldsymbol{T}]]$ the *function ring* of the formal loop $\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y})$.

From now on, the definition of formal loops remains unchanged if the ground field K has characteristic 0. However, if $\mathrm{chr}(\mathsf{K}) = p > 0$, then we allow the ring $\mathsf{K}[[\boldsymbol{T}]]/I$ as formal function ring as well, where the ideal $I \triangleleft \mathsf{K}[[\boldsymbol{T}]]$ is generated by elements of the form $(T^j)^{p^k}$ with $j \in \{1,\ldots,n\}$ and $k \geq 1$. This means that the power series $\mu^i(\boldsymbol{X},\boldsymbol{Y})$ defining the formal product are elements of the ring $\mathsf{K}[[\boldsymbol{X},\boldsymbol{Y}]]/J$, where the ideal J is generated by the elements $(X^j)^{p^k}$, $(Y^j)^{p^k}$ with the above indices j, k.

In the following, the function ring of a formal loop will still be denoted by $\mathsf{K}[[\boldsymbol{T}]]$, where $(T^j)^{p^k} = 0$ is allowed when $\mathrm{chr}(\mathsf{K}) = p > 0$. We will say that *the formal loop has height* h if $(T^i)^{p^{h+1}} = 0$ holds for all $i \in \{1,\ldots,n\}$. If there exists no positive integer h with this property, then we speak of a *formal loop of infinite height* (cf. [Die73, Chapter II]).

Clearly, the concepts of derivation, point derivation, tangent algebra and formal Bruck loop can be taken over to this extended definition without any difficulty. The most important results concerning formal Bruck loops, like the Lemmas 3.4, 3.5, 2.2 and Proposition 3.8, remain true.

There is another, more abstract way to define formal loops in the above sense; this was done for formal groups by P. Cartier [Car62] and J. Dieudonné [Die73]. Their definition is based on the properties of the function ring $A = \mathsf{K}[[\boldsymbol{T}]]$. On the one hand, A is clearly a commutative, associative algebra over the field K. Moreover, A is a local ring with unique maximal ideal $\mathfrak{M} = (T^1, \ldots, T^n)$. Introducing the $\mathfrak{M}$-adic topology on A, it turns out to be a linearly compact vector space with continuous algebra operations. One can deduce from [Car62, Théorème 2] and [Die73, Chapter II] that these properties (linearly compact, commutative, associative local algebra) characterize the rings $\mathsf{K}[[\boldsymbol{T}]]/I$, where $I = 0$ if $\mathrm{chr}(\mathsf{K}) = 0$ and I is as above if $\mathrm{chr}(\mathsf{K}) = p > 0$.

Let us now consider the category $\mathrm{ALC}_{\mathsf{K}}$ of linearly compact, commutative, associative local K-algebras. Morphisms are the continuous algebra homomorphisms, and the sum of the objects A and B can be defined as follows. We endow the vector space $A \otimes B$ with the tensor product topology and construct the *completed tensor product* $A \mathbin{\widehat{\otimes}} B$ as the topological completion of $A \otimes B$ via Cauchy sequences.

Finally, we can put on A the structure of a formal loop using the concept of *comultiplication*, which is a continuous homomorphism

$$c : A \to A \mathbin{\widehat{\otimes}} A$$

and that of *counit* (or *augmentation*), which is a continuous homomorphism

$$\gamma : A \to \mathsf{K},$$

sending both homomorphisms unit to unit.

In the original definition, for $A = \mathsf{K}[[\boldsymbol{T}]]/I$ we have

$$A \mathbin{\widehat{\otimes}} A = \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]/J$$

(I and J defined as above) and the comultiplication is induced by the map $T^i \mapsto \mu^i(\boldsymbol{X}, \boldsymbol{Y})$.

The associativity of the formal loop (i.e., formal groups) translates to the following commutative diagram:

$$\begin{array}{ccc}
A & \xrightarrow{c} & A \mathbin{\widehat{\otimes}} A \\
{\scriptstyle c}\big\downarrow & & \big\downarrow{\scriptstyle c \otimes 1} \\
A \mathbin{\widehat{\otimes}} A & \xrightarrow[1 \otimes c]{} & A \mathbin{\widehat{\otimes}} A \mathbin{\widehat{\otimes}} A
\end{array}$$

Other loop identities can be expressed by diagrams, too. However, even simple looking loop identities produce rather complex diagrams. For example, the loop identity $x(xy) = x^2y$ has diagram

$$\begin{array}{ccccc} A & \xrightarrow{c} & A \mathbin{\widehat{\otimes}} A & \xrightarrow{c\otimes 1} & A \mathbin{\widehat{\otimes}} A \mathbin{\widehat{\otimes}} A \\ {\scriptstyle c}\big\downarrow & & & & \big\downarrow {\scriptstyle \mu\otimes 1} \\ A \mathbin{\widehat{\otimes}} A & \xrightarrow[1\otimes c]{} & A \mathbin{\widehat{\otimes}} A \mathbin{\widehat{\otimes}} A & \xrightarrow[\mu\otimes 1]{} & A \mathbin{\widehat{\otimes}} A \end{array}$$

In the rest of this section, we will use the *naive* concept of formal loops and groups.

4.2. Cartier duality of formal groups

The functorial equivalence between the category of Lie algebras (restricted Lie algebras) and the category of formal groups (formal groups of height 0) goes as follows.

Theorem 4.1 (Cartier)**.** *Let* K *be a field and let us denote the Lie algebra of the formal group* G *by* $\mathcal{L}(G)$*.*

a) *If* $\mathrm{chr}(\mathsf{K}) = 0$*, then* $\mathcal{L}$ *is an equivalence between the category of formal* K*-groups and the category of Lie algebras over* K*.*

b) *If* $\mathrm{chr}(\mathsf{K}) = p > 0$*, then* $\mathcal{L}$ *is an equivalence between the category of formal* K*-groups of height 0 and the category of restricted Lie algebras over* K*.*

Proof. See [Car62, Théorème 3,4]. □

Using the formal Campbell-Hausdorff series of Lie groups, part a) of the theorem can be shown immediately. However, the proof of part b) requires higher algebra. The idea is the following. Let $\mathfrak{g}$ be a restricted Lie algebra over the field K with $\mathrm{chr}(\mathsf{K}) = p > 0$, and let $B = \{b_1, \ldots, b_n\}$ be a basis of $\mathfrak{g}$. Then, the *restricted universal associative algebra* $U_p(\mathfrak{g})$ is a finite dimensional K-space with basis

$$\{b_1^{s_1} \cdots b_n^{s_n} \mid 0 \leq s_1, \ldots, s_n < p\}$$

(see [Sel67, Theorem I.3.2]). One can introduce a cocommutative, coassociative comultiplication on the associative algebra $U_p(\mathfrak{g})$ by extending the map

$$\mathfrak{g} \to \mathfrak{g} \oplus \mathfrak{g}, \qquad x \mapsto x \oplus x$$

into a map $U_p(\mathfrak{g}) \to U_p(\mathfrak{g} \oplus \mathfrak{g}) = U_p(\mathfrak{g}) \otimes U_p(\mathfrak{g})$. Similarly, the trivial map $\mathfrak{g} \to 0$ extends to a counit $U_p(\mathfrak{g}) \to \mathsf{K}$.

Now, if we consider the dual vector space $A = U_p(\mathfrak{g})^*$, A turns out to be a finite dimensional, commutative, associative algebra with unit, coassociative comultiplication and counit. The basis of the dual space A (symbolically) can be written in the form

$$\{(T^1)^{s_1} \cdots (T^n)^{s_n} \mid 0 \leq s_1, \ldots, s_n < p\}.$$

One shows that the commutative algebra structure of A is such that A is isomorphic to the ring $\mathsf{K}[[T^1, \ldots, T^n]]/((T^1)^p, \ldots, (T^n)^p)$ of formal power series of height 0 (cf. [Die73, Chapter II, §1, No. 4]). Finally, the images $\mu^i(\boldsymbol{X}, \boldsymbol{Y})$ of the generating elements T^i under the comultiplication map $A \to A \otimes A = \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]/((X^i)^p, (Y^j)^p)$ define the formal group G we were looking for. The coassociativity of the comultiplication is equivalent to the formal associativity of G.

4.3. The generalization of the Cartier duality

In this section, we generalize Theorem 4.1 for the category of formal Bruck loops. Since our result uses heavily the embeddings of the tangential L.t.s. of the formal Bruck loop (cf. Theorem 3.2), we have to restrict ourselves to the case $\mathrm{chr}(\mathsf{K}) \in \{0, 3\}$. However, a proof of Theorem 3.2 for the case $\mathrm{chr}(\mathsf{K}) > 3$ would immediately imply the full generality of Theorem 4.2.

Let K be a field of characteristic 0 (characteristic 3) and let us denote by $\mathcal{L}(B)$ the tangent (restricted) L.t.s. of the formal Bruck loop B.

Theorem 4.2. a) *If $\mathrm{chr}(\mathsf{K}) = 0$, then $\mathcal{L}$ is an equivalence between the category of formal Bruck loops over K and the category of Lie triple systems over K.*

b) *If $\mathrm{chr}(\mathsf{K}) = 3$, then $\mathcal{L}$ is an equivalence between the category of formal Bruck loops of height 0 over K and the category of restricted Lie triple systems over K.*

Proof. Since the construction of the tangent algebra of a formal Bruck loop B is natural, the non-trivial part of the proof is to obtain the inverse of $\mathcal{L}$, that is, to find the formal loop of a given (restricted) L.t.s.

In [Nag99], we showed the existence of a Campbell–Hausdorff formula of local analytic Bruck loops. This means that if B is a local analytic

Bruck loop with tangent L.t.s. $(\mathfrak{b}, (.\,,.\,,.\,))$, then we have the following: Identifying the unit element of B with 0 we can choose an appropriate coordinate system on B in such a way that in a neighborhood U of the unit element, the local multiplication of B is given by the absolutely convergent series

$$\sum_{k=0}^{\infty} d_{2k+1}(X, Y), \tag{41}$$

where $X, Y \in U$ and $d_{2k+1}(X, Y)$ is a homogenous $(.\,,.\,,.\,)$-polynomial of degree $2k+1$. Moreover, the $(.\,,.\,,.\,)$-polynomials are universal and the coefficients are *rational numbers* not depending on B or $\mathfrak{b}$.

Now, if $\mathrm{chr}(\mathsf{K}) = 0$, then $\mathbb{Q} \subset \mathsf{K}$ and we can take the series (41) as a formal power series over K in $n = \dim \mathfrak{b}$ variables and forget about convergence in order to obtain part a) of the theorem for any field K of characteristic 0. (On local analytic Bruck loops and their expansions see also [MS90], [NS98] and [Fig99].)

Let us now assume $\mathrm{chr}(\mathsf{K}) = 3$ and let $\mathfrak{b}$ be a restricted L.t.s. over K. In Theorem 3.2, we have shown that $\mathfrak{b}$ can be embedded in a restricted Lie algebra $\mathfrak{g}$ of finite dimension. Moreover, we had the vector space decomposition $\mathfrak{g} = \mathfrak{b} \oplus \mathcal{D}$, where $\mathcal{D}$ was a restricted Lie subalgebra of $\mathfrak{g}$, consisting of derivations of $\mathfrak{b}$.

We define the map

$$\sigma : \mathfrak{g} \to \mathfrak{g}, \quad x + \delta \mapsto -x + \delta \qquad (x \in \mathfrak{b}, \delta \in \mathcal{D}).$$

A direct calculation gives that σ is an involutorial automorphism of $\mathfrak{g}$. Then, σ can be lifted to an involutorial automorphism of the restricted universal associative algebra $U_3(\mathfrak{g})$ of $\mathfrak{g}$. We denote this algebra automorphism also by σ. As we explained in the previous section, $U_3(\mathfrak{g})$ is an associative algebra with a cocommutative, coassociative comultiplication and a counit. Clearly, σ is an automorphism with respect to the co-operations, too.

Let us consider the dual algebra $A = (U_3(\mathfrak{g}))^*$ together with the dual (algebra and coalgebra) automorphism σ^*. As before, the commutative, associative algebra A is isomorphic to $\mathsf{K}[[T^1, \dots, T^n]/((T^i)^3)$, the comultiplication, antipodism (=coinverse) and the dual automorphism σ^* are given by the maps

$$T^i \mapsto \mu^i(\boldsymbol{X}, \boldsymbol{Y}), e^i(\boldsymbol{T}), s^i(\boldsymbol{T}),$$

respectively. Clearly, we have $s^i(\boldsymbol{s}(\boldsymbol{T})) = T^i$.

Lemma 4.3. *By an appropriate change of coordinates, the series e^i and s^i can be brought to the form $e^i(\boldsymbol{T}) = -T^i$ and $s^i(\boldsymbol{T}) = \pm T^i$.*

Proof. By Lemma 2.2, we can assume that $\boldsymbol{e}(\boldsymbol{T}) = -T$. Let us define the matrix $D = (d^i_j)$ by $d^i_j = \frac{\partial s^i}{\partial T^j}(\mathbf{0})$, that is,

$$s^i(\boldsymbol{T}) = \sum_j d^i_j T^j + \sum \text{ terms of degree} \geq 2 \text{ w.r.t. } T^i$$

and $D^2 = 1$. We define the system of power series $u^i(\boldsymbol{T})$ by

$$\boldsymbol{u}(\boldsymbol{T}) = \boldsymbol{s}(\boldsymbol{T}) + D\boldsymbol{T}.$$

One gets $\boldsymbol{u}(\boldsymbol{s}(\boldsymbol{T})) = D\boldsymbol{u}(\boldsymbol{T})$ immediately. On the other hand, $\boldsymbol{u}(\boldsymbol{T})$ has non-zero Jacobian. Thus, the map $T^i \mapsto u^i(\boldsymbol{T})$ induces an automorphism of A which is a change of coordinates yielding $\boldsymbol{s}(\boldsymbol{T}) = D\boldsymbol{T}$. Now, by $D^2 = 1$, a linear substitution gives $s^i(\boldsymbol{T}) = \pm T^i$.

Finally, we have to show that the change of coordinates, induced by $T^i \mapsto u^i(\boldsymbol{T})$ does not affect the form of $e^i(\boldsymbol{T}) = -T^i$. Indeed, since $\boldsymbol{s}$ is an automorphism w.r.t. the antipodism $\boldsymbol{e}$, we have

$$\boldsymbol{u}(-\boldsymbol{T}) = \boldsymbol{s}(-\boldsymbol{T}) - D\boldsymbol{T} = -\boldsymbol{s}(\boldsymbol{T}) - D\boldsymbol{T} = -\boldsymbol{u}(\boldsymbol{T}). \qquad \square$$

We suppose now that a formal group $G = (\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$ on A is given such that $e^i(\boldsymbol{T}) = -T^i$ $(i = 1, \dots, n)$, $s^i(\boldsymbol{T}) = -T^i$ $(i = 1, \dots, m)$ and $s^i(\boldsymbol{T}) = T^i$ $(i = m+1, \dots, n)$ hold. It follows from Cartier's Theorem 4.1 that the tangent algebra of G is the restricted Lie algebra $\mathfrak{g}$. Clearly, the automorphism $\sigma^* = \boldsymbol{s}$ of G induces an involutorial automorphism $d\boldsymbol{s}$ of $\mathfrak{g}$ and $\mathfrak{g}$ decomposes into $\mathfrak{g} = \mathfrak{g}^- \oplus \mathfrak{g}^+$. Moreover, since the induced Lie algebra automorphism $d\boldsymbol{s}$ is the original σ, we have $\mathfrak{g}^- = \mathfrak{b}$ and $m = \dim \mathfrak{b}$.

Following Glauberman [Gla64], to any 2-divisible group one can associate a 2-divisible Bruck loop with operation

$$x \circ y = x^{\frac{1}{2}} \cdot y x^{\frac{1}{2}}.$$

In the next lemma, we copy this trick for the formal case.

Lemma 4.4. *Let the series $(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$ define a formal group G with formal square root operation $(\nu^i(\boldsymbol{T}))$ and tangent (restricted) Lie algeba $\mathfrak{g}$. Then the series*

$$\widehat{\mu}^i(\boldsymbol{X}, \boldsymbol{Y}) = \mu^i(\boldsymbol{\nu}(\boldsymbol{X}), \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{\nu}(\boldsymbol{X})))$$

defines a formal Bruck loop $\widehat{G}$ *such that*

a) *the inversion* $\boldsymbol{e}$ *and any automorphism of* G *are automorphisms of* $\widehat{G}$.

b) *the tangent L.t.s.* $\widehat{\mathfrak{g}}$ *of* $\widehat{G}$ *is isomorphic to* $(\mathfrak{g}, [[.\,,.\,],.\,])$.

c) *If* $\operatorname{chr} \mathsf{K} > 0$, *then* $\widehat{\mathfrak{g}}$ *and* $(\mathfrak{g}, [[.\,,.\,],.\,])$ *are isomorphic as restricted Lie triple systems.*

Proof. The fact that $(\widehat{\mu}^i(\boldsymbol{X}, \boldsymbol{Y}))$ is a formal Bruck loop can be shown by the same steps that one uses to check the properties of the operation $x \circ y = x^{\frac{1}{2}} \cdot yx^{\frac{1}{2}}$, cf. [Gla64], [MS90] or [NS02]. Part a) follows immediately.

The tangent (restricted) Lie algebra $\mathfrak{g}$ of G is spanned by the derivations

$$E_k = \xi_k^i(\boldsymbol{Y}) \frac{\partial}{\partial Y^i}, \qquad \xi_k^i(\boldsymbol{Y}) = \frac{\partial \mu^i}{\partial X^j}(\boldsymbol{0}, \boldsymbol{Y}),$$

which is clearly a (restricted) L.t.s. with respect to the operation $[[A, B], C]$.

The tangent algebra of $\widehat{G}$ is spanned by the derivations

$$\widehat{E}_k = \widehat{\xi}_k^i(\boldsymbol{Y}) \frac{\partial}{\partial Y^i}, \quad \widehat{\xi}_k^i(\boldsymbol{Y}) = \frac{\partial \widehat{\mu}^i}{\partial X^j}(\boldsymbol{0}, \boldsymbol{Y}).$$

Following the notation of Section 3.2, we have

$$\varphi^i(\boldsymbol{X}, \boldsymbol{Y}) = \mu^i(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{X})),$$

$$\chi_k^i(\boldsymbol{Y}) = \frac{\partial \varphi^i}{\partial X^j}(\boldsymbol{0}, \boldsymbol{Y}), \quad A_k = \chi_k^i(\boldsymbol{X}) \frac{\partial}{\partial X^i}.$$

Moreover, since G satisfies the formal Bol identity (3), the proof of Lemma 3.4 shows that the spaces of derivations spanned by $\{E_k\}$ and $\{A_k\}$ are isomorphic with respect to the operation $[[A, B], C]$ (cf. (26) and (32)).

On the other hand $\widehat{\boldsymbol{\mu}}(\boldsymbol{X}, \boldsymbol{Y}) = \boldsymbol{\varphi}(\boldsymbol{\nu}(\boldsymbol{X}), \boldsymbol{Y})$, thus, by $\boldsymbol{\nu}(\boldsymbol{T}) = \frac{1}{2}\boldsymbol{T} + \dots$

$$\widehat{\xi}_k^i(\boldsymbol{Y}) = \frac{1}{2} \chi_k^i(\boldsymbol{Y})$$

holds. Hence, the map

$$g^i(\boldsymbol{Y}) \frac{\partial}{\partial Y^i} \mapsto 2 g^i(\boldsymbol{X}) \frac{\partial}{\partial X^i}$$

is an isomorphism between $\widehat{\mathfrak{g}}$ and the space spanned by $\{A_k\}$. Hence $\widehat{\mathfrak{g}}$ and $(\mathfrak{g}, [[.\,,.],.])$ are isomorphic too, which proves b).

We can argue similarly to see that the [3]-maps are isomorphic, too. $\square$

Using this lemma, we define the formal Bruck loop $\widehat{G} = (\widehat{\mu}^i(\boldsymbol{X}, \boldsymbol{Y}))$ of G. All we have to show is that $\widehat{G}$ has a *formal subloop* whose tangent space is the subspace $\mathfrak{b} = \mathfrak{g}^-$. The theory of formal subloops is rather well elaborated and we do not intend to go into details, the problem can, however, be solved very easily.

Lemma 4.5. *The equations $T^{m+1} = \cdots = T^n = 0$ define a formal subloop of $\widehat{G}$ whose tangent algebra is $\mathfrak{b}$.*

Proof. All we have to show is that the "space" $T^{m+1} = \cdots = T^n = 0$ is closed under $\widehat{\boldsymbol{\mu}}$. Let us put $\boldsymbol{X}_0 = (X^1, \dots, X^m, 0, \dots, 0)$ and $\boldsymbol{Y}_0 = (Y^1, \dots, Y^m, 0, \dots, 0)$ and show

$$\widehat{\mu}^t(\boldsymbol{X}_0, \boldsymbol{Y}_0) = 0, \qquad t = m+1, \dots, n.$$

Indeed, since $\boldsymbol{e}$ and $\boldsymbol{s}$ are automorphisms of $\widehat{G}$, we have

$$\begin{aligned} -\widehat{\mu}^t(\boldsymbol{X}_0, \boldsymbol{Y}_0) &= e^t(\widehat{\boldsymbol{\mu}}(\boldsymbol{X}_0, \boldsymbol{Y}_0) \\ &= \widehat{\mu}^t(-\boldsymbol{X}_0, -\boldsymbol{Y}_0) = \widehat{\mu}^t(\boldsymbol{s}(\boldsymbol{X}_0), \boldsymbol{s}(\boldsymbol{Y}_0)) \\ &= s^t(\widehat{\boldsymbol{\mu}}(\boldsymbol{X}_0, \boldsymbol{Y}_0)) = \widehat{\boldsymbol{\mu}}(\boldsymbol{X}_0, \boldsymbol{Y}_0) \end{aligned}$$

for any $t \in \{m+1, \dots, n\}$, which implies $\widehat{\mu}^t(\boldsymbol{X}_0, \boldsymbol{Y}_0) = 0$. $\square$

This finishes the proof of Theorem 4.2.

Remark. Obviously, a generalization of Theorem 3.2 together with the above proof would imply the proof of the preceding theorem for general characteristic $p > 0$.

4.4. An interesting example

The method explained so far can be applied to calculate the formal Bruck loop of height 0 of a given restricted L.t.s. Now we do the calculation for an example which has some interest if one consider a special class of algebraic Bruck loops, namely the algebraic commutative Moufang loops.

The tangent L.t.s. of such loops satisfy an infinite set of equations, which also imply the nilpotency of the systems. The simplest of these identities is $(X, Y, Y) = 0$, which is equivalent with saying that the ternary operation (X, Y, Z) alternates. If $\operatorname{chr} \mathsf{K} \neq 3$, then by (13) the L.t.s. is trivial.

However, there are non-nilpotent alternating Lie triple systems: Let K be a field of characteristic 3, and let us define the structure constants

$$w^3_{123} = -w^3_{132} = w^3_{231} = -w^3_{213} = w^3_{312} = -w^3_{321} = 1$$

and $w^i_{k\ell m} = 0$ for all other $k, \ell, m, i \in \{1, 2, 3\}$. Let $\{e_1, e_2, e_3\}$ be a basis of a vector space $\mathfrak{l}$ over K and let us define the trilinear operation by

$$(e_k, e_\ell, e_m) = w^i_{k\ell m} e_i.$$

With the trivial [3]-map, $\mathfrak{l}$ becomes an alternating restricted L.t.s., which is solvable but not nilpotent. (And hence, it is not the tangent algebra of a formal commutative Moufang loop.)

The following formal Bruck loop of height 0 has $\mathfrak{l}$ as its tangent L.t.s. We constructed this example by using the method of the proof of 4.2. The calculations were done with the computer algebra program GAP4 [Gro98].

$$\begin{pmatrix} X_1 + Y_1 \\ X_2 + Y_2 \\ X_3 + Y_3 + (X_1 - Y_1)(X_2 Y_3 - X_3 Y_2) + \mu_5(\boldsymbol{X}, \boldsymbol{Y}) + \mu_7(\boldsymbol{X}, \boldsymbol{Y}) \end{pmatrix}$$

$$\begin{aligned} \mu_5(\boldsymbol{X}, \boldsymbol{Y}) = {} & -X_1^2 X_2^2 Y_3 + X_1^2 X_2 X_3 Y_2 + X_1 X_2^2 X_3 Y_1 - X_1 X_2^2 Y_1 Y_3 \\ & + X_1 X_2 X_3 Y_1 Y_2 + X_2^2 X_3 Y_1^2 - X_2^2 Y_1^2 Y_3 + X_2 X_3 Y_1^2 Y_2 \end{aligned}$$

$$\mu_7(\boldsymbol{X}, \boldsymbol{Y}) = -X_1^2 X_2^2 X_3 Y_1 Y_2.$$

References

[Bou50] N. Bourbaki, Eléments de Mathématique: Algèbre, chap. IV–V, *Number 1102 in Actualités Sci. Ind. Hermann, Paris*, 1950.

[Bou89] N. Bourbaki, Lie Groups and Lie Algebras, Chapters 1-3, *Springer–Verlag, Berlin–Heidelberg–New York*, 1989.

[Car62] P. Cartier, Groups algébriques et groupes formels, in: Colloque sur la Théorie des Groupes Algébriques, *Librairie Gauthier–Villars*, 1962, 87–111.

[Die57] J. Dieudonné., Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (vi), *Amer. J. Math.* **79** (1957), 331–288.

[Die73] J. Dieudonné., Introduction to the theory of formal groups, Pure and Applied Mathematics, *Marcel Dekker, Inc.*, *New York*, 1973.

[Fig99] Á. Figula, Geodesic loops, *J. Lie Theory* (1999) (*to appear*).

[Gla64] G. Glauberman, On loops of odd order I, *J. Alg.* **1** (1964), 374–396.

[Gro98] The GAP Group, Gap – groups, algorithms, and programming, *University of St Andrews and RWTH Aachen*, 1998, Version 45b5.

[Hod00] T. L. Hodge, Restricted Lie triple systems and algebraic groups, 2000, (*to appear*).

[Hum75] J. E. Humphreys, Linear Algebraic Groups, *Springer-Verlag*, *Berlin–Heidelberg–New York*, 1975.

[Jac51] N. Jacobson, General representation theory of Jordan algebras, *Trans. Amer. Math. Soc.* **70** (1951), 509–530.

[KK95] E. Kolb and A. Kreuzer, Geometry of kinematic K-loops, *Abh. Math. Sem. Univ. Hamburg* **65** (1995), 189–197.

[Loo69] O. Loos, Symmetric Spaces, vol. 1, 2, *Benjamin*, *New York*, 1969.

[MS90] P. O. Miheev and L. V. Sabinin, Quasigroups and differential geometry, Quasigroups and Loops: Theory and Applications (O. Chein et al., eds.), number 8, Sigma Series in Pure Mathematics, *Heldermann Verlag*, *Berlin*, 1990, 357–430.

[Nag99] G. P. Nagy, On the Hausdorff series of local analytic Bruck loops, 1999, (*submitted*).

[Nôn61] T. Nôno, Sur les familles triples locales de transformations locales de Lie, *J. Sci. Hiroshima Univ. Ser. A-I* **25** (1961), 357–366.

[NS98] P. T. Nagy and K. Strambach, Loops, their cores and symmetric spaces, *Israel J. Math.* **105** (1998), 285–322.

[NS02] P. T. Nagy and K. Strambach, Loops in Group and Lie Theory, *Walter De Gruyter*, *Berlin, New York*, 2002.

[Sel67] G. B. Seligman, Modular Lie Algebras, *Springer–Verlag*, *Berlin–Heidelberg-New York*, 1967.

GÁBOR P. NAGY
MATHEMATISCHES INSTITUT
DER UNIVERSITÄT ERLANGEN–NÜRNBERG
BISMARKSTR. 1 1/2
D–91054 ERLANGEN
GERMANY
AND
SZTE BOLYAI INSTITUTE
ARADI VÉRTANÚK TERE 1
H–6720 SZEGED
HUNGARY

E-mail: nagyg@math.u-szeged.hu

(Received April 3, 2001; revised February 4, 2002)