Algebraische kommutative Moufang-Loops

Den Naturwissenschaftlichen Fakultäten
der Friedrich-Alexander-Universität Erlangen-Nürnberg
zur
Erlangung des Doktorgrades

vorgelegt von
Gábor P. Nagy
aus Szeged (Ungarn)

Als Dissertation genehmigt von den Naturwissenschaftlichen
Fakultäten der Universität Erlangen-Nürnberg

Tag der mündlichen Prüfung:

Vorsitzender der Promotionskommission:	Professor Dr. W. Buggisch
Erstberichterstatter:	Professor Dr. K. Strambach
Zweitberichterstatter:	Professor Dr. O. Kegel

Contents

Introduction

The first impulse to study non-associative structures came in the first decades of this century from the foundations of geometry, in particular from the investigation of coordinate systems of non-Desarguesian planes. The interest of W. Blaschke in the systematic treatment of loops and quasigroups was motivated by topological questions of differential gemetry (1938). R. Baer (1939), A.A. Albert (1943, 1944) and R.H. Bruck (1958) established the theory of quasigroups and loops as an independent algebraic theory.

Beside the theory of abstract loops, in view of the deepness of the methods and result, the most developed part of the theory of loops is certainly the theory of topological and differentiable loops. This field gained importance originally by the work of M.A. Akivis, V.V. Goldberg, K.H. Hofmann, H. Salzmann and K. Strambach, the usefulness of analytic methods is shown in the work of L.V. Sabinin, for a collected documentation see [CPS90]. Very recent contributions to this field are the monographs [NS99] of P.T. Nagy and K. Strambach (under preparation) and [Sab99] by L.V. Sabinin.

The main object of this dissertation is the category of *algebraic commutative Moufang loops*. The adjective *algebraic* is used in the sense it is used in the theory of algebraic groups: The underlying set of the loop under consideration is an (affine) algebraic variety over an algebraically closed field K and the loop operations are morphisms of algebraic varieties.

On the one hand, the richness of the analytic theory enables us to speak of the *Lie theory* of some special loop classes (Moufang, Bruck, local Bol). On the other hand, the theory of algebraic groups, built up along the same lines as the theory of Lie groups in some sense, is one of the main branches of group theory. This makes the fact that *algebraic loops and quasigroups* were so far only sporadically investigated ([Ene94], [NS99, Section 11]) surprising. The main aim of this dissertation is to start filling out this gap and to create the foundations of the theory of algebraic loops. The first large obstacle is the absence of properly formulated definitions and problem settings. For this reason, we decided to restrict ourselves to the class of *commutative Moufang loops;* an abstractly defined class with many useful properties and a rather transparent structure.

In **Chapter 1**, we recall the basic definitions and properties of the theory of abstract commutative Moufang loops and give some important expamles.

In **Chapter 2**, we first define the concept of an algebraic commutative Moufang loop. After giving the (easy) generalizations of properties of algebraic groups we prove that *any algebraic commutative Moufang loop is nilpotent* (Theorem 2.1.6). This result determines the guide line of our investigations. Its immediate consequences are: the characteristic 3 of the ground field K, the existence of algebraic factor loops (Corollaries 2.1.7 and 2.1.8) and the description of the algebraic structure of the underlying variety of the loop (Theorem 2.1.10). Later on, the study of central extensions of algebraic commutative Moufang loops leads to the complete classification of the 2-dimensional connected species of them (Theorem 2.3.4). Finally we prove the main result of this chapter by showing that *the multiplication group of an algebraic commutative Moufang loop has a unique structure of an algebraic transformation group, acting on the loop* (Theorem 2.4.2).

Our next aim is to give a meaningful definition for the tangent algebra of a commutative Moufang loop. The fact that the most important classes of commutative topological Moufang loops are associative (cf. [HS90]) makes this question more exciting. The solution is the idea of looking at commutative Moufang loops as special cases of *Bruck loops* (instead of *Moufang loops*).

In **Chapter 3**, we first consider the concept of *restricted Lie triple systems* and prove a result concerning their embeddability in restricted Lie algebras (Theorem 3.1.2). In the next step, we define the category of *formal Bol loops* analogously to the theory of formal groups which was originally derived in a natural way from the theory of classical Lie groups by S. Borchner. Our approach to this field is the *naive* one in Dieudonné's terminolgy ([Die73]). Using methods of the theory of local analytic Bol loops we show that the space of L- derivations of a formal Bol loop forms a (restricted if char $\mathsf{K} = 3$) Lie triple system (Proposition 3.3.4). At the end of the chapter, we relate the infinitesimal Lie triple system of a formal Bruck loop with its formal associator (Proposition 3.4.1); also this relation is motivated by methods of local analytic Bruck loops.

In **Chapter 4**, we explain the *localization process* for algebraic Bol loops. This process allows us to apply the results of the previous chapter in order to obtain properties of the structure of the tangent algebra of an algebraic commutative Moufang loop (Theorem 4.3.1). We also give a method of recovering the tangent L.t.s. of an algebraic commutative Moufang loop in the tangent Lie algebra of its multiplication group (Proposition 4.2.3). Using this method, we obtain an algebraic homomorphism of the group of inner mappings of the loop in the (linear) group of automorphisms of the tangent L.t.s. (Theorem 4.3.7). This homomorphism implies well expected results on tangent spaces of closed normal and associator subloops (Propositions 4.3.8

and 4.3.9).

After these results, it is natural to ask to what extent one can invert the above functorial map from the category of algebraic commutative Moufang loops to the category of restricted Lie triple systems. However, knowing the complexity of analogous problem for algebraic groups, one cannot expect a simple answer. Indeed, on the one hand, the "variety" of connected algebraic commutative Moufang loops of dimension 2 is "infinite dimensional" (cannot be parametrized with finitely many parameters), but any such has a trivial tangent algebra of dimension 2.

On the other hand, Theorem 4.3.1 contains an infinite family of necessary conditions for a restricted Lie triple system to be the tangent algebra of an algebraic commutative Moufang loop. The first of these conditions says that the ternary L.t.s. operation must *alternate*; an example on page 49 shows that this property is not sufficient. It is not difficult to generalize this example to show that no finite part of the family implies the rest.

In **Chapter 5**, we consider a modification of the aforementioned "inverting problem". The modification relies on the fact that in characteristic 0, the classical Hausdorff-Campbell formula produces a 1-1 correspondence between the category of formal groups and the category of Lie algebras. P. Cartier [Car62] proved an analogous correspondence between the category of formal groups *of height 0* and the category of restricted Lie algebras in characteristic $p > 0$. We generalize this last result by proving a *functorial equivalence* between the *category of formal Bruck loops of height 0* and the *category of restricted Lie triple systems* in characteristic 3 (Theorem 5.3.1).

In **Chapter 6**, we consider a special class of algebraic commutative Moufang loops, namely the loop of units of a commutative alternative algebra. Starting with a finite commutative Moufang loop, we construct a finite dimensional commutative alternative algebra as a factor of the loop ring. In this way, we represent every finite commutative Moufang loop L modulo its second associator subloop L'' linearly (Theorem 6.3.5).

The most commonly used notations of this dissertations are:

$L, \dots$	loops
$G, \dots$	groups
λ_x	left translation
$\lambda_{x,y}$	inner mapping
(x,y,z), $\alpha(x,y,z)$	associator of loop elements
L'	associator subloop of L
$Z(L)$	center of L
$G(L)$	left translation group of L
$N \ltimes H$	semidirect product of the groups N and H
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
$\mathfrak{g},\dots$	Lie algebras of the groups $G,\dots$
$\mathfrak{l},\dots$	tangent algebras of the loops $L,\dots$
(x,y,z)	ternary operation in Lie triple systems
A^*	loop of units of the alternative algebra A
$[x,y]$, $[x,y,z]$	commutator and associator brackets of algebra elements
$\mathsf{K}L$	loop ring of L over the field K

Acknowledgments

I would like to express my deepest thanks to my supervisor Professor Dr. Karl Strambach for this excellent subject, for his permanent support and for the many valuable suggestions he gave me during the writing of this dissertation.

I have been helped in the last correction of this dissertation by Michael Kinyon (IUSB); I thank him very much.

I am also grateful for the hospitality of the Mathematical Institut of the University Erlangen-Nürnberg and for the financial support of the Hungarian Ministry of Education ("Eötvös Fellowship" and grant nr. FKFP-0152/1997) and the Hungarian National Scientific and Research Foundation (grants nos. F030737, F029849).

Chapter 1

Loop theoretical backgrounds

In this chapter, we recall those definitions and basic properties of the theory of loops, which play an important rôle in our investigations. The abstract class of *commutative Moufang loops* is the intersection of two larger loop classes of great importance: the *Moufang loops* and the *Bruck loops*. Both of these are subclasses of the classes of *Bol loops*. For introductory literature on loops and on commutative Moufang loops see [Pfl90] and [Bru58].

The following principle is valid for the whole dissertation: It is not our aim to work out all definitions and results in full generality, the basic objects of our investigation are *algebraic commutative Moufang loops*. However, in many cases the general formulation of the results was so evident and the extra work with the definitions were so little that we gave way to the temptation.

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 $x = 1 \cdot x = x \cdot 1$ 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 $x = a\backslash b$ and $y = d/c$. The property of the unique solvability can be equivalently expressed by the identities

$$x \cdot (x\backslash y) = y, \qquad (x/y) \cdot y = x, \qquad x\backslash(x \cdot y) = x, \qquad (x \cdot y)/y = x. \tag{1.1}$$

As one sees from the definition, loops are in some sense the non-associative generalizations of groups. However, in general, interesting loop classes always bear some weak form of associativity. The widest class of interest to us is the class of *Bol loops*, defined by the identity

$$x \cdot (y \cdot xz) = (x \cdot yx) \cdot z. \tag{1.2}$$

It is known that this identity implies $1/x = x\backslash 1 = x^{-1}$ and then the identity $x^{-1} \cdot xy = y$ holds. In the following technical lemma we prove a kind of converse of these facts.

Lemma 1.0.1. *Let $L = (L, \cdot, (.)^{-1}, 1)$ be a set, endowed with a binary, a unary and a nullary operation, satisfying the identities*

$$x \cdot 1 = x = 1 \cdot x, \quad x^{-1} \cdot xy = y \quad \text{and} \quad x \cdot (y \cdot xz) = (x \cdot yx) \cdot z.$$

Then, L is a Bol loop.

Proof. We only have to show that L is a loop. Let us define the operations

$$x\backslash y = x^{-1}y \quad \text{and} \quad x/y = y^{-1}(yx \cdot y^{-1})$$

and show that they satisfy the identities (1.1). Clearly, $x^{-1}x = x^{-1} \cdot x1 = 1$. Let us now assume first that $xy = xz$ for some elements $x, y, z \in L$. Then, $y = x^{-1} \cdot xy = x^{-1} \cdot xz = z$. Therefore,

$$x^{-1} \cdot (x \cdot x^{-1}y) = (x^{-1} \cdot xx^{-1}) \cdot y = x^{-1}y$$

implies the identity $x \cdot x^{-1}y = y$. This proves $x \cdot (x\backslash y) = y$ and $x\backslash(x \cdot y) = x$. Moreover, using the Bol identity, we have

$$\begin{aligned} x/y \cdot y &= (y^{-1}(yx \cdot y^{-1})) \cdot y \\ &= y^{-1} \cdot (yx \cdot y^{-1}y) \\ &= y^{-1} \cdot yx = x \end{aligned}$$

and

$$\begin{aligned} (xy)/y &= y^{-1} \cdot ((y \cdot xy) \cdot y^{-1}) \\ &= y^{-1} \cdot (y \cdot x1) = x, \end{aligned}$$

which finishes the proof of the lemma. □

An important subclass of Bol loops is defined by the so called *automorphic inverse property*

$$(xy)^{-1} = x^{-1}y^{-1}. \tag{1.3}$$

The most common name of this class is *Bruck loops* (cf. [NS99]). For Bruck loops, it can be 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 [NS99].

Let L be an abstract Bruck loop. For any element $x, y \in L$, we define

$$\text{the } \textit{(left) translation map } \lambda_x(y) = xy,$$

and

$$\text{the } \textit{inner mapping } \lambda_{x,y}(z) = (xy)^{-1}(x \cdot yz)$$

and the groups

$$\begin{aligned} G = G(L) = \langle \lambda_x : x \in L \rangle, \\ H = H(L) = \langle \lambda_{x,y} : x, y \in L \rangle \end{aligned}$$

generated by these maps. Clearly, the *left translation group* $G(L)$ acts transitively on L, $H \leq G(L)$ is the stabilizer subgroup of the unit element $1 \in L$ and the set

$$\{\lambda_x : x \in L\}$$

is a system of (left and right) coset representatives to H.

Now, we come to the definition of the loop class which will be the most deeply investigated in this dissertation.

Definition. *The loop* $(L, \cdot)$ *is said to be an abstract* commutative Moufang loop *(abbreviated CML), if for all* $x, y, z \in L$,

$$(xy)(xz) = x^2(yz) \tag{1.4}$$

holds.

It is not completely immediate to see that these loops are commutative, but one can show it rather quickly, using similar tricks as in the proof of Lemma 1.0.1. Moreover, due to the commutativity, one has $x/y = xy^{-1}$ and $x\backslash y = x^{-1}y$. This means that CML's can be axiomatized in the same way as groups, but taking (1.4) instead of associativity.

In the rest of this chapter, L will denote an (abstract) commutative Moufang loop.

Let us denote by $\mathcal{F}_{x,y}$ the set of elements which are left fixed by $\lambda_{x,y}$. The intersection of all these sets is the *center* of L, that is, the set

$$Z(L) = \{z \in L | x \cdot yz = xy \cdot z \ \forall x, y \in L\}.$$

In a CML, for an element $z \in Z(L)$ the identities $x \cdot zy = xz \cdot y$ and $z \cdot xy = zx \cdot y$ also hold for any $x, y \in L$. Clearly, $Z(L)$ is a normal subgroup of L, having many similarities to the center of a group. For example, we can speak of lower central series of L.

Let us now define the *associator map* of a CML:

$$(x, y, z) = (x \cdot yz)^{-1} \cdot (xy \cdot z).$$

For the subsets A, B, C of L, (A, B, C) denotes the subloop generated by all the elements (a, b, c) with $a \in A$, $b \in B$ and $c \in C$. The *associator subloop* $L' = (L, L, L)$ is the smallest normal subloop of L such that L/L' is an Abelian group. Now, we also can speak about the upper cental series of L: $L_0 = L$ and $L_{i+1} = (L, L, L_i)$ for $i > 0$. L is *nilpotent*, if $L_i = 1$ for some i. Just like for groups, the lengths of upper and lower central series of a nilpotent loop coincide (cf. [Bru58, Chapter VI]).

We enumerate the most important properties of abstract CML's (see [Bru58]).

(L1) For all $x \in L$, $x^3 \in Z(L)$.

(L2) The associator map alternates in the sense that $(y, x, z) = (x, y, z)^{-1}$, $(x, z, y) = (x, y, z)^{-1}$ and $(x^n, y, z) = (x, y, z)^n$ for $n \in \mathbb{Z}$.

(L3) The *inner mapping*

$$\lambda_{x,y} : z \mapsto (xy)^{-1} \cdot (x \cdot yz)$$

is an automorphism of L.

(L4) The loops L' and $L/Z(L)$ have exponent 3.

(L5) (Theorem of Bruck and Slaby.) Let L be an abstract CML which is generated by n elements. Then L is nilpotent of class at most $n - 1$.

Item (L1) and (L4) imply that "interesting" CML's have exponent 3, they are therefore 2-divisible (Bruck loops, of course).

Item (L5) implies that finite CML's are nilpotent. However, as the following example due to Bruck shows, there exist infinite CML's with trivial center.

Examples

Our first example is due to Bruck [Bru58]. Let K be a field of characteristic 3. Let let us take the set $S = \{x_0, x_1, \ldots\}$ and let $\tilde{S}$ be the semigroup generated by S, with neutral element x_0. Let R be a vector space over K with basis $\tilde{S}$. Define a multiplication on R by using the associative and distributive laws to extend the following multiplication of elements of S:

$$x_0 x_i = x_i = x_i x_0, \qquad x_i x_j = \begin{cases} x_i x_j & \text{if } i < j \\ 0 & \text{if } i = j \\ -x_j x_i & \text{if } i > j \end{cases}.$$

Let V be the subspace of R with basis $S = \{x_1, x_2, \ldots\}$ and let R be the *exterior algebra* of V over K. Define $\cdot$ on $L = V \times R$ by

$$(a, x) \cdot (b, y) = (a + b, x + y + (x - y)ab).$$

Then, $(L, \cdot)$ is a CML. A direct calculation gives the inverse $(a, x)^{-1} = (-a, -x)$ and the associator

$$((a, x), (b, y), (c, z)) = (0, xbc + yca + zab).$$

This shows that $L' = (0, RV^2)$ is an Abelian group and L has solvability class 2.

If $|S| = n$ then the nilpotence class of L is $\lfloor n/2 \rfloor$, see [Bru58, Chapter VIII.1]. If S is infinite, then $Z(L) = \{(0, 0)\}$. Indeed, taking an arbitrary element $(a, x) \in V \times R$, a is a finite linear combination of elements $x_{i_1} \ldots x_{i_m}$.

Choosing $x_r, x_s \in S$ such that $i_k < r < s$ holds for all i_k occurring in x, one has

$$((a,x),(x_r,0),(x_s,0)) = (0, xx_rx_s) \neq (0,0).$$

The second example is due to Zassenhaus. Let K be a field of characteristic 3 and define "$\circ$" on $L = \mathsf{K}^4$ by

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \circ \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_0 + y_0 + (x_1 - y_1)(x_2y_3 - x_3y_2) \\ x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix}$$

Then, $(L, \circ)$ is an (algebraic) commutative Moufang loop. If K is algebraically closed, then

$$\{(x_0, x_1, x_1^3, x_1^9) : x_1, x_2 \in \mathsf{K}\}$$

is a proper closed, connected subloop of dimension 2 which has dimension two.

Our final example ([Nag99a]) is an algebraic proper (not Bruck and not Moufang) Bol loop of exponent 3. Let K be again a field of characteristic 3 and let us define the following loop operation on K^4:

$$\begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 + x_1y_2 - x_2y_1 \\ x_4 + y_4 + (x_1y_2 - x_2y_1)(x_3 - y_3 + x_1y_2 - x_2y_1) \end{pmatrix}.$$

Then, $(\mathsf{K}^4, \circ, -(.))$ is a proper Bol loop of exponent 3.

Chapter 2

Algebraic commutative Moufang loops

2.1 Algebraic CML's

Definition. *Let L be an algebraic variety over the algebraically closed field* K *and an abstract loop $L = (L, \cdot, /, \backslash)$. We say that L is an* algebraic loop *if the $L \times L \to L$ maps*

$$(x, y) \mapsto x \cdot y, x/y, x\backslash y$$

are morphisms of algebraic varieties.

One can say that the above definition defines algebraic loops *in a wide sense.* A more restricted definition of algebraic quasigroups was given in [Ene94], where one requires the right multiplication group of an algebraic quasigroup Q to be an algebraic transformation group on Q. For the class of algebraic loop we are investigating, we prove this property in Theorem 2.4.2.

The most general class of loops we are dealing with are *Bol loops.* Due to Lemma 1.0.1, the category of algebraic Bol loops can be defined in the same way than algebraic groups.

Definition. *Let L be an algebraic variety over the algebraically closed field* K *and an abstract Bol loop $(L, \cdot, (.)^{-1})$ in the sense of Lemma 1.0.1. We say that L is an* algebraic Bol loop *if the map*

$$\begin{cases} L \times L \to L \\ (x, y) \mapsto xy^{-1} \end{cases}$$

is a morphism of algebraic varieties.

Clearly, for any subclass of Bol loop which is defined by identities in the two loop operations we can define the corresponding class of algebraic loop. Thus, we are able to speak of *algebraic Bruck loops, algebraic Moufang loops* or *algebraic commutative Moufang loops.* In contrast, the proper definition of *algebraic 2-divisible Bruck loops* remains open.[1]

Now, subloops and homomorphisms of algebraic loops are defined in a very obvious way: algebraic subloops are Zariski closed subvarieties, closed under product and inverting and homomorphisms of algebraic loops are supposed to be homomorphisms of loops and morphisms of algebraic varieties. It is also clear that the kernel of an algebraic homomorphism is a closed normal subloop, but the converse, namely that any closed normal subloop occurs as kernel of an algebraic homomorphism, is not so obvious at all. We will get around this difficulty in a way which can only be applied for *centrally nilpotent* algebraic loops (Lemma 2.1.2).

In the sequel, L will always denote an algebraic CML (ACML for short) over the algebraically closed field K. Many properties of algebraic groups can be easily generalized for ACML's. For example, the identity component L^0 of L is a normal subloop such that L/L^0 is finite. And, since the theory of finite CML's is rather elaborate, we will restrict ourselves to the case when $L = L^0$ is connected. Another property is that the center $Z(L)$ is a closed subgroup of L. Both of these properties follow from the fact that the map

$$\begin{cases} L \times L \times L \to L \\ (x, y, z) \mapsto \lambda_{x,y}(z) \end{cases}$$

is a morphism of varieties.

By definition, an algebraic group G is *affine* if the algebraic variety G is affine, and is an *Abelian variety* if G is projective and irreducible. It is well know that an Abelian variety is always an Abelian group (cf. [Sha94, Chap. III, 4.3, Theorem 2.]). We have to modify slightly the proof to obtain the same result for algebraic (commutative Moufang) loops.

Proposition 2.1.1. *Let L be an algebraic commutative Moufang (Bol) loop whose algebraic variety is projective and irreducible. Then L is an algebraic Abelian group.*

Proof. Consider the family of maps $u_z(x, y) = \lambda_{x,y}(z)$ from $L \times L$ to L with base L. Obviously if e is the unit element we have $u_e(x, y) = e$ for all $(x, y) \in L \times L$, and hence by [Sha94, Chap. III, 4.3, Lemma], $u_z(L \times L)$ is a point for every $z \in L$. Hence $u_z(x, y) = u_z(e, e) = z$, and this means that L is an Abelian group. □

Remark. This proof, combined with the proof of [Sha94, Chap. III, 4.3, Theorem 2.] imply the above result for *any algebraic loop.*

From now on, in the whole dissertation, without mentioning it, we will consider only *affine algebraic Bol loops.*

[1] The reason for this is that to require the 2-division map $x \mapsto x^{\frac{1}{2}}$ to be morphical seems to be too strong.

Lemma 2.1.2. *Let L be an algebraic (commutative Moufang) loop let N be a closed subgroup of the center $Z(L)$ of L. Then, the factor variety L/N exists and the factor loop has a uniquely defined structure of an algebraic (commutative Moufang) loop.*

Proof. The factor variety exists and is uniquely defined by [Ros56, Theorem 2]. □

Some theorems on subgroups of algebraic groups are easy to generalize for Moufang loops. Lemmas 2.1.3 and 2.1.4 and Proposition 2.1.5 are analogons of [Hum75, Lemma 7.4, Proposition 7.5 and Proposition 17.2], to obtain their proofs only small modifications were needed.

Lemma 2.1.3. *Let U, V be two dense open subsets of an algebraic CML L. Then $L = U \cdot V$.*

Proof. Since inversion is an isomorphism of varieties, V^{-1} is again a dense open set. So is its translate xV^{-1} (for any given $x \in L$). Therefore, U must meet xV^{-1}, $u = xv^{-1}$ holds for some $u \in U$ and $v \in V$. This forces $x = u \cdot v \in U \cdot V$. □

For each positive integer n, we define a set M_n of mappings $L^n \to L$ inductively. For $n = 1$, M_1 consists only of the identity map $L \to L$. For $n > 1$, we take M_n to be the union of the sets $M_p \times M_{n-p}$ where $p = 1, \ldots, n-1$; we write $(w, w') = w.w'$ for $(w, w') \in M_p \times M_{n-p}$. The map $w.w' : L^n \to L$ will be defined by $(w.w')(x_1, \ldots, x_n) = w(x_1, \ldots, x_p) \cdot w'(x_{p+1}, \ldots, x_n)$. The element $w \in M_n$ is said to be of length $l(w) = n$. If $M_1, \ldots, M_n$ are subsets of L, then $w(M_1, \ldots, M_n)$ means the set of elements $w(x_1, \ldots, x_n)$ with $x_1 \in M_1, \ldots, x_n \in M_n$.

Given an arbitrary subset M of L, let us denote by $\mathcal{A}(M)$ the intersection of all closed subloops of L containing M. This is the smallest closed subloop of G containing M; we call it the *loop closure* of M.

Lemma 2.1.4. *Let L be an ACML, I an index set, $f_i : X_i \to L$ $(i \in I)$ a family of morphisms from irreducible varieties X_i, such that $1 \in Y_i = f_i(X_i)$ for each $i \in I$. Set $M = \cup_{i \in I} Y_i$. Then:*

(i) *$\mathcal{A}(M)$ is a connected subloop of L.*

(ii) *For some positive integer n and an element $w \in M_n$, $k(i) \in I$ and $e(i) = \pm 1$ $(i = 1, \ldots, n)$, we have $\mathcal{A}(M) = w(Y_{k(1)}^{e(1)}, \ldots, Y_{k(n)}^{e(n)})$.*

Proof. Enlarge I such that the morphisms $x \mapsto f_i(x)^{-1}$ also occur. Define the set

$$S = \{(w, k(1), \ldots, k(n)) : w \in \cup_{n \in \mathbb{N}} M_n, n = l(w), (k(1), \ldots, k(n)) \in I^n\}.$$

For an element $a = (w, k(1), \ldots, k(n)) \in S$, set $Y_a = w(Y_{k(1)}, \ldots, Y_{k(n)})$. As the image of the irreducible variety $X_{k(1)} \times \cdots \times X_{k(n)}$ under the morphism $f_{k(1)} \times \cdots \times f_{k(n)}$ composed with μ_w, Y_a is constructible (cf. [Hum75, (4.4)]), and $\bar{Y}_a$ is an irreducible variety passing through e. Using the maximal condition on irreducible closed subsets of L^0, we can therefore find an element $a \in S$ for which $\bar{Y}_a$ is maximal. Given any two elements $b = (w, k(1), \ldots, k(n)), c = (w', k'(1), \ldots, k'(n)) \in S$, we define

$$(b, c) = (w.w', k(1), \ldots, k(n), k'(1), \ldots, k'(n)) \in S.$$

We claim that

$$(*) \qquad \bar{Y}_b \bar{Y}_c \subseteq \bar{Y}_{(b,c)}.$$

The proof is in two steps. For $x \in Y_c$, the (continuous) map $y \mapsto yx$ sends Y_b into $Y_{(b,c)}$, hence $\bar{Y}_b$ into $\bar{Y}_{(b,c)}$, i.e., $\bar{Y}_b Y_c \subseteq \bar{Y}_{(b,c)}$. In turn, $x \in \bar{Y}_b$ sends Y_c into $\bar{Y}_{(b,c)}$, hence $\bar{Y}_c$ as well.

Because $\bar{Y}_a$ is maximal, and e lies in each $\bar{Y}_b$, $(*)$ implies that

$$\bar{Y}_a \subseteq \bar{Y}_a \bar{Y}_b \subseteq \bar{Y}_{(a,b)} = \bar{Y}_a$$

for any $b \in S$. Setting $b = a$, we have $\bar{Y}_a$ stable under multiplication. Choosing b such that $Y_b = Y_a^{-1}$ (cf. first sentence of the proof), we also have $\bar{Y}_a$ stable under inversion. Conclusion: $\bar{Y}_a$ is a closed *subloop* of G containing all Y_i $(i \in I)$, so $\bar{Y}_a = \mathcal{A}(M)$, proving (i). Moreover, since Y_a is constructible, Lemma 2.1.3 shows that $\bar{Y}_a = Y_a \cdot Y_a = Y_{(a,a)}$, so the tuple $(a, a) = (w, k(1), \ldots, k(n))$ satisfies (ii). □

Proposition 2.1.5. *Let A, B, C closed subloops of an ACML L.*

(i) If A is connected, then (A, B, C) is closed and connected.

(ii) If A, B and C are normal in L, then (A, B, C) is closed (and normal in L). In particular, (L, L, L) is always closed.

Proof. (i) Associate with each $y \in B, z \in C$ the morphism $\varphi_{y,z} : A \to L$ defined by $\varphi_{y,z}(x) = x^{-1}\lambda_{y,z}(x) = (x, y, z)$. Since A is connected and $\varphi_{y,z}(1) = 1$, Lemma 2.1.4 shows that the group generated by all $\varphi_{y,z}(A)$ $(y \in B, u \in C)$ is closed and connected; but this is by definition (A, B, C).

(ii) It follows from part (i) that (A^0, B, C), (A, B^0, C) and (A, B, C^0) are closed, connected (as well as normal) subloops of G, so their product D has the same properties. To show that (A, B, C) is closed, it therefore suffices to show that D has finite index in (A, B, C), which is a purely loop-theoretical question. In the abstract CML L/D, the image of A^0 (resp. B^0, C^0) centralizes the image of BC (resp. AC, AB). Since $|A : A^0|, |B : B^0|, |C : C^0| < \infty$, this implies that the set $S = \{(x, y, z) \pmod{D}; x \in A, y \in B, z \in C\}$ is finite. Moreover, elements of S have order 3, therefore they generate a CML of exponent 3 modulo D, which is finite by [Bru58, Theorem VIII.11.2]. This means that $(A, B, C)/D$ is finite. □

The proposition implies that the elements of the upper central series of a loop are closed, and connected as well if L is connected. We can now prove the main result of this section.

Theorem 2.1.6. *Let L be a connected ACML of positive dimension. Then $Z(L)$ has positive dimension. In particular, any ACML is nilpotent.*

Proof. Suppose the statement is not true and let L be a connected counterexample of minimal dimension. $\dim Z(L) = 0$, hence $|Z(L)| < \infty$. Define $Z_2(L)$ with the property $Z_2(L)/Z(L) = Z(L/Z(L))$. If $\dim Z_2(L) > 0$, then $L/Z_2(L)$ has a finite lower central series, therefore its upper central series $L = L_0, L_1, \dots$ is finite, too. Let n be the greatest index for which $L_i \neq \{1\}$, then $L_n \leq Z(L)$ closed and connected, a contradiction. This means that $\dim Z_2(L) = 0$ and $|Z_2(L)| < \infty$. But for a fixed $a \in L$, the map $L \times L \to L$, $(x, y) \mapsto \lambda_{x,y}(a)$ is morphical, thus the "conjugacy class" $\{\lambda_{x,y}(a) : (x, y) \in L \times L\}$ is connected if L is connected. Therefore, a finite normal subloop of a connected loop lies in the center, and we have $Z_2(L) = Z(L)$. Hence, $L/Z(L)$ has trivial center and by Lemma 2.1.2, we can assume that the algebraic CML L has trivial center.

By definition, $Z(L) = \cap_{x,y \in L} \mathcal{F}_{x,y}$, where $\mathcal{F}_{x,y}$ are closed subsets of L. Thus, there exist a finite set $S = \{x_1, y_1, \dots, x_n, y_n\}$ such that

$$\{1\} = \bigcap_{i=1}^{n} \mathcal{F}_{x_i,y_i}.$$

On the other hand, the subloop M generated by S is nilpotent by the theorem of Bruck-Slaby (L5), so it contains an element $1 \neq z \in Z(M)$. This element is left fixed by all the λ_{x_i,y_i}'s, therefore $z \in \mathcal{F}_{x_i,y_i}$ for all $i = 1, \dots, n$, a contradiction. □

Remark. The above proof is based on the important CML property of *local nilpotence.*

Corollary 2.1.7. *Let N be a closed normal subloop of the algebraic CML L. Then, there exists an algebraic CML $\bar{L}$ and a surjective algebraic homomorphism $\varphi : L \to \bar{L}$ whose kernel is N. The loop $\bar{L}$ is uniquely defined up to isomorphisms of algebraic loops.*

Proof. Let us first assume that N is connected and let us define the normal subloops $N_0 = N$ and $N_{i+1} = (L, L, N_i)$. By Proposition 2.1.5, the subloops N_i are connected and by the nilpotence of L, we have $N_k = \{1\}$ for some $k > 0$. Let k be the largest index for which $N_k \neq \{1\}$, then $(L, L, N_k) = \{1\}$ and $N_k \leq Z(L)$. By Lemma 2.1.2, the algebraic factor loop L/N_k is well defined, and we can apply induction on $\dim L$ since $\dim N_k > 0$.

If N is not connected, then we first factorize with its connected component N^0. Since N/N^0 is finite, it is central in L/N^0, thus the factor $L/N = (L/N^0)/(N/N^0)$ is well defined, too. □

In the rest of this dissertation, the uniquely defined algebraic loop $\bar{L}$ will be denoted by $\bar{L} = L/N$ and will be called the *algebraic factor loop* without referring to the previous corollary.

Corollary 2.1.8. *Let L be a connected proper ACML over the field K. Then* $\mathrm{char}\mathsf{K} = 3$.

Proof. Let n be the greatest index for which $L_n \neq \{1\}$, then L_n is a closed, connected, Abelian algebraic group of positive dimension. Moreover, since $n > 0$, any element of L_n has order 3 (cf. property (L4)) and L_n is unipotent. This implies $\mathrm{char}\,\mathsf{K} = 3$ and L_n is a K-vector group. □

In this chapter, we always assume K to have characteristic 3, even if L is not connected or proper.

We call an element x of an ACML *unipotent*, if its order is a power of 3. A subloop of L is *unipotent*, if it contains only unipotent elements.

Proposition 2.1.9. *Let L be an ACML. Then $L = U \times S$, where U is a unipotent subloop and S is the subgroup of all semisimple elements of $Z(L)$.*

Proof. $Z(L)$ and L/L' are Abelian algebraic groups over K, they are therefore the direct product of a unipotent and a semisimple subgroup; $Z(L) = Z_1 \times S$ and $L/L' = \bar{U} \times \bar{S}$. Let $U \leq L$ be the subloop of L such that $U/L' = \bar{U}$. The orders of the elements of $\bar{U}$ are 3-powers, and L' has exponent 3, thus U is a unipotent subloop of L. Conversely, since $L/U \cong \bar{S}$ is a group consisting of semisimple elements, all unipotent loop elements are contained in U. We will show that $L = US$.

Take an arbitrary element $x \in L$ and consider the loop closure $M = \mathcal{A}(x)$ of x. Since the associator map is trivial on $\langle x \rangle$, M is associative. More precisely, it is an Abelian algebraic group over K. Using its decomposition $M = M_u \times M_s$ (cf. [Hum75, Proposition 19.2]), we find unipotent $u \in M_u$ and semisimple $s \in M_s$ elements of L with $x = us$. On the one hand, u has 3-power order, $u \in U$. On the other hand, the connected component M_s^0 is a torus and M_s/M_s^0 is finite with order prime to 3 (cf. [Hum75, Theorem 16.2]). Thus, the map $x \mapsto x^3$ is bijective on M_s and an element r exists with $r^3 = s$. This implies $s \in Z(L)$ and $s \in S$. □

Of course, we are more interested in the subloop U of L. The following theorem describes its structure as algebraic variety.

Theorem 2.1.10. *Let L be a connected ACML of dimension n and suppose that L consists of unipotent elements only. Then, L is isomorphic to the affine space K^n as variety.*

Proof. Let k be the greatest index for which $L_k \neq \{1\}$ and consider the connected Abelian algebraic group L_k of exponent 3; it is isomorphic to K^m as an algebraic group ($m = \dim L_k$). By induction we assume that $\bar{L} = L/L_k$ is birationally isomorphic to K^{n-m}. Moreover, L_k operates regularly and morphically on the variety L. Let us denote by $\tau : L \to \bar{L}$ the natural rational homomorphism. By [Ros56, Theorem 10], there exists a cross section

$\sigma : \bar{L} \to L$, defined over K, with $\tau \circ \sigma = id_{\bar{L}}$. We claim that the morphisms

$$A : \left\{ \begin{array}{l} \bar{L} \times L_k \to L \\ (\bar{x}, c) \mapsto \sigma(\bar{x}) \cdot c \end{array} \right. \qquad B : \left\{ \begin{array}{l} L \to \bar{L} \times L_k \\ x \mapsto (\tau(x), x \cdot \sigma(\tau(x))^{-1}) \end{array} \right.$$

are each other's inverses. Indeed, one has

$$\begin{array}{rcl} B(\sigma(\bar{x})c) & = & (\tau(\sigma(\bar{x})), \sigma(\bar{x})c \cdot (\sigma(\tau(\sigma(\bar{x})c))^{-1}) \\ & = & (\bar{x}, \sigma(\bar{x})c \cdot \sigma(\bar{x})^{-1}) = (\bar{x}, c); \\ A((\tau(x), x \cdot \sigma(\tau(x))^{-1})) & = & \sigma(\tau(x)) \cdot (x \cdot \sigma(\tau(x))^{-1} = x. \end{array}$$

Thus, L is isomorphic to $\bar{L} \times L_k \cong \mathsf{K}^n$ as a variety. □

Corollary 2.1.11. *Let L be a unipotent ACML. Then L has a finite exponent of the form 3^e. The map $x \mapsto x^2$ is a bijective morphism of L with inverse $x \mapsto x^{(3^e+1)/2}$.*

Proof. Let us first suppose that L is connected. We claim that $x^{3^d} = 1$ for all $x \in L$ where $d = \dim L$. If $d = 1$, then L is isomorphic to K^+ and has exponent 3. If $d > 1$, then L has a connected normal subloop M of codimension 1, we can assume by induction that $y^{3^{d-1}} = 1$ for all $y \in M$. Furthermore, L/M is a connected unipotent Abelian algebraic group of dimension 1, thus $x^3 \in M$ holds for all $x \in L$. This implies $x^{3^d} = 1$.

If L is not connected, then L/L^0 is a finite CML of 3-power order. Hence $x^{3^f} \in L^0$ and $x^{3^{f+d}} = 1$ for all $x \in L$. The last statement follows immediately. □

The inverse of the map $x \mapsto x^2$ will be denoted by $x \mapsto x^{\frac{1}{2}}$.

2.2 Central extensions

Theorem 2.1.10 makes possible to consider the theory of central extensions of algebraic commutative Moufang loops via the second cohomology groups.

Let $(E, \cdot)$ be a connected unipotent ACML, M be a connected subgroup of $Z(E)$ and $L = E/M$. We use additive terminology for L and M: the loop operations are going to be "$\oplus$" and "$+$", resp. The inverse of x is $-x$ and the unit element will be denoted by 0, in all cases.

Let σ_1 be a cross section $\sigma_1 : L \to E$ over K. Define the morphism $\sigma : L \to E$ by

$$\sigma(x) = (\sigma_1(x) \cdot (-\sigma_1(-x)))^{\frac{1}{2}}, \qquad x \in L.$$

Then, σ is a cross section as well, with the further property

$$\sigma(-x) = -\sigma(x). \tag{2.1}$$

The morphism

$$f : \begin{cases} L \times L \to M \\ (x, y) \mapsto (-\sigma(x \oplus y)) \cdot (\sigma(x) \cdot \sigma(y)) \end{cases}$$

has the following properties:

(C1) $f(x, y) = f(y, x)$ for all $x, y \in L$.

(C2) $f(x, 0) = f(0, y) = f(x, -x) = 0$ for all $x \in L$.

(C3) $d'f(x, y, z) = 0$ for all $x, y, z \in L$, where

$$\begin{aligned} d'f(x, y, z) &= f(x \oplus y, x \oplus z) + f(x, y) + f(x, z) \\ &\quad - f(x \oplus x, y \oplus z) - f(x, x) - f(y, z). \end{aligned}$$

The property $f(x, -x) = 0$ follows from (2.1); it is not essential but makes computations easier. Property (C3) follows from the commutative Moufang identity (1.4).

We call d' the *modified boundary operator*. Let us recall the definition of the usual boundary operators. For the morphisms $\varphi : L \to M$ and $f : L \times L \to M$ we have

$$d\varphi : \begin{cases} L \times L \to M \\ (x, y) \mapsto \varphi(x \oplus y) - \varphi(x) - \varphi(y) \end{cases}$$

and

$$df : \begin{cases} L \times L \times L \to M \\ (x, y, z) \mapsto f(x \oplus y, z) + f(x, y) - f(x, y \oplus z) - f(y, z). \end{cases}$$

Definition. *Let $(L, \oplus)$ be an algebraic CML and M be a vector group over K. We define the following sets of morphism.*

$$\begin{aligned} B^2(L, M) &= \{f : L^2 \to M : f = d\varphi \text{ for some morphism } \varphi : L \to M\}, \\ Z^2_\ell(L, M) &= \{f : L^2 \to M : f \text{ satisfies (C1), (C2) and (C3)}\}, \\ Z^2(L, M) &= \{f : L^2 \to M : f \text{ satisfies (C1), (C2) and } df = 0\}, \\ Z^2_{3e}(L, M) &= \{f \in Z^2_\ell(L, M) : f(x, x) = 0 \text{ identically}\}. \end{aligned}$$

On any of these sets, a natural (additive) group structure is defined as well. We call the elements of $B^2(L, M)$ and $Z^2_\ell(L, M)$ 2-coboundaries *and* loop 2-cocycles*, respectively.*

Lemma 2.2.1. *We have $B^2(L, M), Z^2(L, M) \leq Z^2_\ell(L, M)$ in general. If L is associative, then even $B^2(L, M) \leq Z^2(L, M)$ holds.*

Proof. Simple calculation shows $d'd\varphi = 0$ and

$$dd\varphi(x, y, z) = \varphi((x \oplus y) \oplus z) - \varphi(x \oplus (y \oplus z))$$

for any map $\varphi : L \to M$. This proves the first and the third assertions. To show $Z^2(L, M) \leq Z^2_\ell(L, M)$, take an arbitrary element $f \in Z^2(L, M)$. Then

$$\begin{array}{rcl} d'f(x,y,z) & = & f(x \oplus y, x \oplus z) + f(x,y) + f(x,z) \\ & & \quad -f(x \oplus x, y \oplus z) - f(x,x) - f(y,z) \\ & = & f(2x \oplus y, z) + f(x \oplus y, x) + f(x,y) \\ & & \quad -f(2x \oplus y, z) - f(2x, y) - f(x,x) \\ & = & f(y, 2x) + f(x,x) - f(2x,y) - f(x,x) \\ & = & 0, \end{array}$$

where $2x$ denotes $x \oplus x$. □

Definition. *Let* L *be an algebraic CML and* M *be a vector group. We define the following* cohomology groups

$$\begin{array}{c} H^2_\ell(L,M) = Z^2_\ell(L,M)/B^2(L,M), \\ H^2_{3e}(L,M) = Z^2_{3e}(L,M)/B^2(L,M). \end{array}$$

If L *is associative, then we put*

$$H^2(L,M) = Z^2(L,M)/B^2(L,M).$$

Clearly, $H^2_{3e}(L,M), H^2(L,M) \leq H^2_\ell(L,M)$ holds.

Proposition 2.2.2. *The elements of the factor group*

$$H^2_\ell(L,M) = Z^2_\ell(L,M)/B^2(L,M)$$

are in 1-1 relation with the isomorphism classes of ACML extensions of L *by* M*.*

Proof. Let us consider an algebraic CML extension

$$0 \to M \to E \to L \to 0.$$

It follows from the proof of Theorem 2.1.10 that $E = L \times M$ can be assumed without loss of generality. Moreover, the embedding $M \to E$ is simply $a \mapsto (0, a)$.

Given such an extension, we define the map $f : L^2 \to M$ as at the beginning of this section. We saw that $f \in Z^2_\ell(L, M)$. Conversely, any morphism $f \in Z^2_\ell(L, M)$ defines an algebraic CML structure on $E = L \times M$ by

$$(x, a) \cdot (y, b) = (x \oplus y, a + b + f(x, y)). \tag{2.2}$$

Choosing the section $\sigma(x) = (x, 0)$, we get back the original $f : L^2 \to M$. In general, any section belonging to this extension has the form $\sigma(x) = (x, \varphi(x))$ with morphism $\varphi : L \to M$. The factor set $\tilde{f}$ defined by this σ is $\tilde{f} = f - d\varphi$.

Let us suppose that $f_1, f_2 \in Z^2_\ell(L, M)$ belong to isomorphic extensions E_1, E_2. Then, the isomorphism $E_1 \to E_2$ has the form $(x, a) \mapsto (x, a + \varphi(x))$ and a simple calculation gives $f_2 - f_1 = d\varphi$. This proves the 1-1 relation between extension and elements of the group $Z^2_\ell(L, M)/B^2(L, M)$. □

We close this section with a simple remark.

Lemma 2.2.3. *Let an algebraic CML structure be defined on $L = \mathsf{K}^n$. Then, a coordinatization of L can be chosen in such a way, that $X^{-1} = -X$ holds identically on L.*

Proof. We use induction on n. If $n = 1$, then there is nothing to prove. If $n > 1$, then L can be seen as a central extension of a loop of smaller dimension. Let f be the factor set belonging to this extension. By property $f(x, -x) = 0$ (cf. (C2)), we have

$$(x, a) \cdot (-x, -a) = (0, 0),$$

and $(x, a)^{-1} = (-x, -a) = -(x, a)$. □

2.3 Classification of 2-dimensional algebraic CML's

At the end of Chapter 1, we saw an example for a proper algebraic commutative Moufang loop of dimension 2. In this section, we give a complete classification of two dimensional algebraic commutative Moufang loops.

By an easy calculation we obtain the identities

$$\begin{aligned} (x, a)^3 &= (3x, 3a + f(2x, x) + f(x, x)), \\ ((x, a), (y, b), (z, c)) &= ((x, y, z), df(x, y, z)). \end{aligned}$$

where we write $2x, 3x, \ldots$ for $x \oplus x, x \oplus x \oplus x, \ldots$.

If L is a vector group, then these equalities become $(x, a)^3 = (0, f(x, x))$ and $((x, a), (y, b), (z, c)) = (0, df(x, y, z))$, respectively. Thus, in this case, the elements of $H^2(L, M)$ and $H^2_{3e}(L, M)$ describe precisely the associative and exponent 3 extensions of L, respectively.

Lemma 2.3.1. *Let L and M be vector groups over the field K of characteristic 3. Then, $H^2_\ell(L, M) = H^2(L, M) \times H^2_{3e}(L, M)$.*

Proof. Let us take an arbitrary element $f \in Z^2_\ell(L, M)$ with vector groups L, M over K and consider the extension (2.2). Since the map $\tilde{x} \mapsto 3\tilde{x} = (0, f(x, x))$ is a loop homomorphism from E to M containing M in its kernel, we obtain that the map $L \to M$, $x \mapsto f(x, x)$ is a homomorphism. Put $L = \mathsf{K}^n$, $M = \mathsf{K}^m$ and $\varphi(x) = f(x, x)$. We have

$$\varphi^k(X) = \sum_{i,j} a^k_{ij} X_i^{3^j}, \qquad a^{(k)}_{ij} \in \mathsf{K}.$$

By (C2), f contains no linear term, thus $j \geq 1$ in the above sum. This makes possible to define the rational map $f_2 : \mathsf{K}^n \times \mathsf{K}^n \to \mathsf{K}^m$ by

$$f_2^k(X,Y) = -\sum_{i,j} a_{ij}^k (X_i^2 Y_i + X_i Y_i^2)^{3^{j-1}}.$$

An easy calculation gives $\varphi(X) = f_2(X,X)$ and $df_2 = 0$. Thus, $f_2 \in Z^2(L,M)$. Putting $f_1 = f - f_2$, we obtain $f_1 \in Z_\ell^2(L,M)$ with $f_1(X,X) = 0$, hence $f_1 \in Z_{3e}^2$. This proves $Z_\ell^2(L,M) = Z_{3e}^2(L,M) + Z^2(L,M)$.

Let us now take an element $f \in Z_{3e}^2(L,M) \cap Z^2(L,M)$. Then f defines an extension E which is an Abelian group of exponent 3, that is, E is a vector group as well. Hence, the extension splits and $f \in B^2(L,M)$ (cf. [Hum75, Corollary 20.4.]). □

The following lemma can be shown by straightforward calculation.

Lemma 2.3.2. *Define the function $f : \mathsf{K}^3 \to \mathsf{K}$ by*

$$f(X_1, X_2, X_3, Y_1, Y_2, Y_3) = (X_1 - Y_1)(X_2 Y_3 - X_3 Y_2).$$

Then we have

$$(d'f)(X_i, Y_i, Z_i) = 0 \text{ and } (df)(X_i, Y_i, Z_i) = -\begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix},$$

where d and d' are defined with respect to $(\mathsf{K}, +)$. □

Lemma 2.3.3. *a) Any element of $H^2(\mathsf{K},\mathsf{K})$ can be uniquely represented by a polynomial $f \in \mathsf{K}[X,Y]$ with $f(X,Y) = \sum_{j\geq 1} a_j (X^2Y + XY^2)^{3^j}$.*

b) Any element of $H_{3e}^2(\mathsf{K},\mathsf{K})$ can be uniquely represented by a polynomial $f \in \mathsf{K}[X,Y]$ with

$$f(X,Y) = \sum_{i<j<k} c_{ijk} (X^{3^i} - Y^{3^i})(X^{3^j} Y^{3^k} - X^{3^k} Y^{3^j}).$$

Proof. Part a) follows immediately from the proof of Lemma 2.3.1. For part b), we fix an element $f \in Z_{3e}^2(\mathsf{K},\mathsf{K})$. As we saw at the beginning of this section, $((x,a),(y,b),(z,c)) = (0,(df)(x,y,z))$ holds for the associator map on the extension defined by f.

Since $\mathsf{K} = M \leq Z(E)$, the properties of the associator map imply the induced polynomial $u = df \in \mathsf{K}[X,Y,Z]$ to be additive and alternating in the sense of (L2). (The additivity relies on the fact that the loop L has nilpotency class 2.) Thus, u has the form

$$u(X,Y,Z) = \sum_{i<j<k} c_{ijk} \begin{vmatrix} X^{3^i} & Y^{3^i} & Z^{3^i} \\ X^{3^j} & Y^{3^j} & Z^{3^j} \\ X^{3^k} & Y^{3^k} & Z^{3^k} \end{vmatrix}. \qquad (2.3)$$

Let us define the polynomial

$$f_0(X,Y,Z) = -\sum_{i<j<k} c_{ijk}(X^{3^i} - Y^{3^i})(X^{3^j}Y^{3^k} - X^{3^k}Y^{3^j}),$$

with coefficients c_{ijk} taken from (2.3). Then, by Lemma 2.3.2, $d'f_0 = 0$ and $df_0 = df$. Moreover, $f(X,X) = 0$ and $f_0(X,X) = 0$ by definition, thus $f - f_0 \in Z^2_{3e}(\mathsf{K},\mathsf{K}) \cap Z^2(\mathsf{K},\mathsf{K}) = B^2(\mathsf{K},\mathsf{K})$ (see Lemma 2.3.1), and f_0 represents f. Clearly, the coefficients c_{ijk} of u determine the coefficients of f_0 uniquely. □

Lemma 2.3.1 and 2.3.3 imply the complete classification of 2-dimensional algebraic commutative Moufang loops.

Theorem 2.3.4. *Let K be an arbitrary algebraically closed field of characteristic 3. Choose arbitrary coefficients $\{a_j\}_{1\le j\le n}$ and $\{c_{ijk}\}_{0\le i<j<k\le m}$ and define the polynomial $f \in \mathsf{K}[X,Y]$ by*

$$\begin{aligned} f(X,Y) \;=\; & \sum_{0\le i<j<k\le m} c_{ijk}(X^{3^i} - Y^{3^i})(X^{3^j}Y^{3^k} - X^{3^k}Y^{3^j}) \\ & + \sum_{1\le j\le n} a_j(X^2Y + XY^2)^{3^j}. \end{aligned}$$

Then, the operation

$$(x,a)\cdot(y,b) = (x+y, a+b+f(x,y))$$

defines an algebraic commutative Moufang loop on K^2. Moreover, any connected 2-dimensional algebraic CML is isomorphic to precisely one of these loops. □

2.4 Group of automorphisms and the multiplication group

In this section, we consider the central algebraic CML extension

$$0 \to (M,+) \to (\tilde{L},\cdot) \to (L,\oplus) \to 0,$$

where $(L,\oplus)$ is a connected unipotent algebraic CML over K; M is a 1-dimensional connected central subgroup of $\tilde{L}$, identified with K^+.

Let us consider an algebraic automorphism $\tilde{\alpha}$ of $\tilde{L}$ which leaves the elements of M fixed. (Like any element of the group of inner mappings does.) Then we have

$$\tilde{\alpha}(z,c) = \tilde{\alpha}(z,0)\cdot\tilde{\alpha}(0,c) = (\alpha(z), c + h(z)), \tag{2.4}$$

where $\alpha : L \to L$ is the induced automorphism on $L = \tilde{L}/M$ and $h : L \to M$ is a morphism. Let us observe that the set of $L \to M$ regular morphisms can be identified with $\mathsf{K}[L]$ and any morphism $\alpha : L \to L$ acts on $\mathsf{K}[L]$ in a natural way: For $h \in \mathsf{K}[L]$ we have

$$\tau_\alpha(h) = \alpha^*(h) = h \circ \alpha.$$

If $\tilde{\alpha} = (\alpha, h)$ and $\tilde{\beta} = (\beta, k)$ are automorphisms of $\tilde{L}$ fixing M, then their product is

$$\tilde{\alpha}\tilde{\beta} = (\alpha\beta, \tau_\beta(h) + k). \tag{2.5}$$

The fact that $\tilde{\alpha}$ is an automorphism implies that

$$\tilde{\alpha}((z, c) \cdot (z', c')) = (\alpha(z \oplus z'), c + c' + f(z, z') + h(z \oplus z'))$$

and

$$\tilde{\alpha}(z, c) \cdot \tilde{\alpha}(z', c') = (\alpha(z) \oplus \alpha(z')), c + c' + h(z) + h(z') + f(\alpha(z), \alpha(z')))$$

are equal. This happens if and only if α and h satisfy the equations

$$\begin{cases} \alpha(z \oplus z') = \alpha(z) \oplus \alpha(z') \\ f(z, z') + h(z \oplus z') = h(z) + h(z') + f(\alpha(z), \alpha(z')) \end{cases} \tag{2.6}$$

for all $z, z' \in L$.

Let now $\tilde{\alpha}$ be the inner map $\tilde{\lambda}_{(x,a),(y,b)}$ of $\tilde{L}$. This map does not depend on a, b, we will write $\tilde{\lambda}_{x,y}$. A simple calculation shows that the morphism $L \to M$ belonging to $\tilde{\lambda}_{x,y}$ is

$$\begin{aligned} h_{x,y}(z) &= h(x, y, z) \\ &= f(-x \oplus y, x \oplus (y \oplus z)) - f(x, y) + f(x, y \oplus z) + f(y, z). \end{aligned}$$

Using this notation, we prove:

Lemma 2.4.1. *Let $\tilde{L}$ be a connected ACML. Then, the inner mappings $\tilde{\lambda}_{\tilde{x},\tilde{y}}$ of $\tilde{L}$ are contained in an algebraic transformation group $\tilde{H}$ of $\tilde{L}$ consisting of automorphisms of $\tilde{L}$. Moreover, the map $\tilde{L} \times \tilde{L} \to \tilde{H}$, $(\tilde{x}, \tilde{y}) \mapsto \tilde{\lambda}_{\tilde{x},\tilde{y}}$ is a morphism.*

Proof. If $\dim \tilde{L} \leq 1$ then $\tilde{L}$ is associative and there is nothing to prove. Suppose that $\dim \tilde{L} > 1$ and choose $M \leq Z(L)$ to be connected of dimension 1. We identify M with K, so, for any K-variety X, a regular morphism $X \to M$ is simply an element of $\mathsf{K}[X]$. We use induction on $\dim \tilde{L}$ and assume that H is an algebraic transformation group of L, it consists of automorphisms of L, and it contains all inner mappings of L.

For the morphism $h \in \mathsf{K}[L \times L \times L] = \mathsf{K}[L] \otimes \mathsf{K}[L] \otimes \mathsf{K}[L]$, one has

$$h(x, y, z) = \sum g_i^{(1)}(x) g_i^{(2)}(y) g_i^{(3)}(z),$$

where $g_i^{(j)} \in \mathsf{K}[L]$ $(j = 1, 2, 3; i = 1, \dots t)$. Let W_1 be the vector space spanned by the functions $g_i^{(3)}$. H acts locally finitely on $\mathsf{K}[L]$ via the action τ_β for $\beta \in H$. Thus, W_1 is contained in a finite dimensional H-stable vector space $W \leq \mathsf{K}[L]$. Since the action of H on W by τ is morphical and, for $h, k \in W$, we have $k, \tau_\beta(h), k + \tau_\beta(h) \in W$, equation (2.5) introduces the algebraic semidirect product $H \ltimes W$. The morphism

$$\varphi : \begin{cases} H \ltimes W \times \tilde{L} \to \tilde{L} \\ ((\alpha, h), (z, c)) \mapsto (\alpha(z), h(c)) \end{cases}$$

defines an algebraic action of $H \ltimes W$ on $\tilde{L}$.

We define the subset $\tilde{H}$ of $H \ltimes W$ by

$$\tilde{H} = \{(\alpha, h) \in H \ltimes W | \alpha \text{ and } h \text{ satisfy (2.6)}\}.$$

We claim that for fixed elements $z, z' \in L$, (2.6) is an algebraic equation for α and h. Indeed, the map

$$\begin{cases} H \ltimes W \times L \times L \to M \\ (\alpha, h, z, z') \mapsto f(z, z') + h(z \oplus z') - h(z) - h(z') - f(\alpha(z), \alpha(z')) \end{cases}$$

is a morphism. With fixed $z, z' \in L$, this is a $H \times W \to M$ morphism, and the pre-image of $\{0\}$ is closed. This means that $\tilde{H}$ is a closed subvariety of $H \ltimes W$. Moreover, $\tilde{H}$ is a subgroup $H \ltimes W$, it consists precisely of automorphisms of $\tilde{L}$ contained in $H \ltimes W$. Let us fix arbitrary elements $x, y \in L$ and consider the inner mapping $\tilde{\lambda}_{x,y} = (\lambda_{x,y}, h_{x,y})$ of $\tilde{L}$. By the definition of H and W, $\lambda_{x,y} \in H$ and $h_{x,y} = \sum g_i^{(1)}(x) g_i^{(2)}(y) g_i^{(3)} \in W$, thus $\tilde{\lambda}_{x,y} \in \tilde{H}$. Hence, $\tilde{H}$ is the algebraic group we were looking for.

By induction, the map $(x, y) \mapsto \lambda_{x,y}$ is rational for $x, y \in L$. The map $(x, y) \mapsto h_{x,y} = \sum g_i^{(1)}(x) g_i^{(2)}(y) g_i^{(3)}$ is rational as well. Therefore, for elements $\tilde{x} = (x, a), \tilde{y} = (y, b) \in \tilde{L} = L \times M$, we have the rational map

$$\begin{cases} \tilde{L} \times \tilde{L} \to \tilde{H} \\ (\tilde{x}, \tilde{y}) \mapsto (\lambda_{x,y}, h_{x,y}) = \tilde{\lambda}_{\tilde{x},\tilde{y}}. \end{cases} \qquad \square$$

The main result of this section is

Theorem 2.4.2. *Let L be a connected ACML. Then the multiplication group $G(L)$ can be uniquely given the structure of a connected algebraic group acting morphically on L.*

Proof. By Lemma 2.4.1, there exists an algebraic transformation group H of automorphisms of L, which contains all inner mapping $\lambda_{x,y}$ of L. Define the variety $\hat{G}$ by $\hat{G} = L \times H$ and introduce the operation

$$(x, \alpha) \circ (y, \beta) = (x \cdot \alpha(y), \lambda_{x,\alpha(y)} \alpha\beta)$$

on $\hat{G}$. By [Kik75, Theorem 2.1] (or, in a more general context, [MS90, Section XII.6.]), $(\hat{G}, \circ)$ is a group. We claim that $(\hat{G}, \circ)$ is an algebraic group, acting rationally on L via

$$\varphi : \begin{cases} \hat{G} \times L \to L \\ ((x, \alpha), z) \mapsto x \cdot \alpha(z). \end{cases}$$

Clearly, φ is a morphism, so we only have to show that the map

$$\begin{cases} L \times H \times L \to L \\ (x, \alpha, y) \mapsto \lambda_{x,\alpha(y)} \end{cases}$$

is rational. Indeed, this is the composition of the rational mappings

$$(x, \alpha, y) \mapsto (x, \alpha(y)) \quad \text{and} \quad (x, z) \mapsto \lambda_{x,z},$$

both being rational by Lemma 2.4.1. Finally, for $x \in L$, the action of (x, id) equals to λ_x and the map $x \mapsto (x, id)$ is rational.

We identify the elements λ_x and $(x, id) \in \hat{G}$. Then, the set

$$S(L) = \{\lambda_x : x \in L\}$$

is an irreducible subvariety of $\hat{G}$. Then by [Hum75, Proposition 7.5], there exists a finite number n such that the group closure of $S(L)$ in $\hat{G}$ is $G(L) = S(L)^n$. This implies $G(L)$ to be a closed subgroup of $\hat{G}$. The uniqueness of the algebraic structure of $G(L)$ follows from [Ram64]. □

An analogue of this theorem yields for analytic Bruck loops. Namely, Kikkawa [Kik75] showed that for an analytic Bruck loop L, the group $G(L)$ is a Lie transformation group on L. Moreover, it follows from [MS90, p. 424] that $\dim G(L) \le n + \binom{n}{2}$ with $n = \dim L$. In the rest of this chapter we construct an example to show that in the algebraic case, no limitation on $\dim G(L)$ can be expected.

Let $m = 2n$ be an arbitrary positive even number. Let us define the "structure constants"

$$c_{012} = c_{034} = \ldots = c_{0,m-1,m} = 1,\ c_{ijk} = 0 \text{ otherwise}, 0 \le i < j < k \le m,$$

and

$$c_{\sigma(i)\sigma(j)\sigma(k)} = \operatorname{sgn}(\sigma) \cdot c_{ijk}, \qquad 0 \le i < j < k \le m, \sigma \in S_3.$$

Put

$$f(X, Y) = \sum_{0 \le i < j < k \le m} c_{ijk}(X^{3^i} - Y^{3^i})(X^{3^j} Y^{3^k} - X^{3^k} Y^{3^j}),$$

and consider the 2-dimensional algebraic CML $L = \mathsf{K}^2$ with the operation

$$(x, a) \cdot (y, b) = (x + y, a + b + f(x, y)).$$

We have

$$\lambda_{(x,a),(y,b)}(z,c) = (z, c + h_{x,y}(z)),$$

that is,

$$\begin{array}{rcl} (0, h_{x,y}(z)) & = & \lambda_{(x,a),(y,b)}(z,c) \cdot (z,c)^{-1} \\ & = & ((x,a),(y,b),(z,c)) \\ & = & (0, df(x,y,z)), \end{array}$$

where the second equality follows from [Bru58, (5.16), p. 124]. Hence,

$$h_{x,y}(Z) = -\sum_{0 \le i<j<k \le m} c_{ijk} \begin{vmatrix} x^{3^i} & y^{3^i} & Z^{3^i} \\ x^{3^j} & y^{3^j} & Z^{3^j} \\ x^{3^k} & y^{3^k} & Z^{3^k} \end{vmatrix},$$

and the coefficient of Z^{3^k} in $h_{x,y}$ is

$$a_k(x,y) = -\sum_{0 \le i,j \le m} c_{ijk} x^{3^i} y^{3^j}.$$

We have

$$a_0(X,Y) = -\sum_{i=1}^{n} (X^{3^{2i-1}} Y^{3^{2i}} - X^{3^{2i}} Y^{3^{2i-1}}) = \sum_{i=1}^{n} (X^3Y - XY^3)^{3^{2i-1}}$$

and

$$\begin{array}{ll} a_1(X,Y) = XY^{3^2} - X^{3^2}Y, & a_2(X,Y) = -XY^3 + X^3Y, \\ \vdots & \\ a_{m-1}(X,Y) = XY^{3^{m-1}} - X^{3^{m-1}}Y, & a_m(X,Y) = -XY^{3^{m-2}} + X^{3^{m-2}}Y. \end{array}$$

Since the polynomials X^{3^i} and Y^{3^j} are linear independent, the polynomials $X^{3^i}Y^{3^j} - X^{3^j}Y^{3^i}$ are linear independent as well. Thus, the only 3-polynomial relation between $a_0(X,Y), \ldots, a_m(X,Y)$ is

$$a_0 - \sum a_2^{3^{2i-1}} = 0.$$

This means that the set

$$\{(a_0(x,y), \ldots, a_m(x,y) : x, y \in \mathsf{K}\}$$

is contained in a unique 1-codimensional additive subgroup of K^{m+1}; with other words, it generates an m-dimensional additive subgroup A of K^{m+1}. On the other hand, the product of two automorphism of form (id, g_1), (id, g_2) of L is $(id, g_1 + g_2)$, thus the automorphism group generated by $\lambda_{(x,a),(y,b)}$ is isomorphic to the additive subgroup of $\mathsf{K}[L]$ generated by the set $\{h_{x,y} : x, y \in \mathsf{K}\}$, which is clearly isomorphic to A. We therefore have proved

$$\dim H = m, \ \dim G(L) = m + 2.$$

Chapter 3

Formal Bol loops and their tangent algebras

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 this chapter, introduce and investigate the concept of formal Bol loops and especially their tangent algebras. Therefore, we first consider the ternary algebra of Lie triple systems; by the motivation of the theory of local analytic Bol loops they are hopeful candidates as tangential objects of formal Bol loops.

The treatment of formal loops in this chapter will be the *naive* one (direct calculations with formal power series, terminology by Dieudonné), in Chapter 5, we will use a slightly more general definition.

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 object 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* $x, y, z, u, v \in \mathfrak{b}$,

$$(x, x, y) = 0 \tag{3.1}$$

$$(x, y, z) + (y, z, x) + (z, x, y) = 0 \tag{3.2}$$

$$(u, v, (x, y, z)) = ((u, v, x), y, z) + (x, (u, v, y), z) + (x, y, (u, v, z)) \tag{3.3}$$

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

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

and $\Delta_x = \Delta_{x,x}$.

Any Lie algebra $(\mathfrak{g}, [.,.])$ can be made into a 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 on M 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 a 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 a 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:*

$$\begin{aligned} [x, y^{[p]}] &= [[x, \underbrace{y] \ldots, y}_{p}]; && (3.4) \\ (\alpha z)^{[p]} &= \alpha^p z^{[p]}; && (3.5) \\ (y+z)^{[p]} &= y^{[p]} + z^{[p]} + \Lambda_p(x,y); && (3.6) \end{aligned}$$

This definition motivates the following.

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

$$\begin{aligned} (x, y^{[p]}, z) &= (((x, \underbrace{y, y), \ldots y, y), y}_{p}, z); && (3.7) \\ (\alpha z)^{[p]} &= \alpha^p z^{[p]}; && (3.8) \\ (y+z)^{[p]} &= y^{[p]} + z^{[p]} + \Lambda_p(x, y); && (3.9) \end{aligned}$$

The identities (3.4) and (3.7) 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 3.1.1. *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 (3.7), all the defining properties of a L.t.s. can be checked easily. For (3.7), we have

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

Theorem 3.1.2. *Let* $\mathfrak{b}$ *be restricted L.t.s. over a field of characteristic 3. Then,* $\mathfrak{b}$ *can be embedded in a restricted Lie algebra* $\mathfrak{g}$. *Moreover, if* $\dim \mathfrak{b} = n < \infty$, *then* $\dim \mathfrak{g} \leq n + n^2$.

Proof. Let us suppose that $\mathfrak{b}$ is a 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

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

First we show that $\mathcal{D}$ is a restricted Lie algebra such that $D_{x,y} \in \mathcal{D}$. By (3.1), (3.2) and (3.7), 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

$$((x, y, z), z, z) = ((x, z, z), z, y) - ((y, z, z), z, x). \tag{3.10}$$

We claim that (3.10) yields 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 $\mathcal{F}$, (3.10) 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

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

and

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

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

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

(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 a 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 $\dim \mathcal{D} \leq \dim(\mathrm{Der}(\mathfrak{b})) \leq n^2$. □

Remark. In [Hod00], the result of the above theorem is obtained for general prime $p > 2$ but under the assumption $\mathfrak{z}(\mathfrak{b}) = \{0\}$. (Cf. page 54.)

3.2 Formal loops

For the rest of this dissertation, X^i, Y^i, Z^i, T^i will denote indeterminates over the field K with $n \in \mathbb{N}$ and $i, j, k = 1, \ldots, n$. We also put $\boldsymbol{X} = (X^1, \ldots, X^n)$,

$\boldsymbol{Y} = (Y^1, \dots, Y^n)$, $\boldsymbol{Z} = (Z^1, \dots, Z^n)$, $\boldsymbol{T} = (T^1, \dots, T^n)$. 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

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

By Lemma 1.0.1 we know that requiring the correct axioms, (abstract) Bol loops can be defined by two operation. This motivates the following definition.

Definition. *A* formal Bol 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*

$$\boldsymbol{\mu}(\boldsymbol{0}, \boldsymbol{Y}) = \boldsymbol{Y}, \quad \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{0}) = \boldsymbol{0}, \tag{3.11}$$

$$\boldsymbol{\mu}(\boldsymbol{e}(\boldsymbol{X}), \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})) = \boldsymbol{X} \tag{3.12}$$

$$\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Z})))) = \boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{X})), \boldsymbol{Z}) \tag{3.13}$$

hold.

The next lemma shows that the existence of the formal inverting is not really important for formal Bol loops. Moreover, if char(K) $\neq 2$, then the 2-divisibility is automatically given, as well.

Lemma 3.2.1. *Let the system of formal series $\mu^i(\boldsymbol{X}, \boldsymbol{Y}), \dots, \mu^i(\boldsymbol{X}, \boldsymbol{Y}) \in \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ over the field K satisfy the identities* (3.11)*.*

a) There exist formal power series $e^1(\boldsymbol{T}), \dots, e^n(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ satisfying (3.12)*.*

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

Proof. From condition (3.11) 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, prop. 10 and p.59, prop. 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 (3.12) holds. For b), if char(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

$$\boldsymbol{\nu}(\boldsymbol{\mu}(\boldsymbol{\nu}(\boldsymbol{T}), \boldsymbol{\nu}(\boldsymbol{T}))) = \boldsymbol{\nu}(\boldsymbol{T}). \tag{3.14}$$

On the other hand, let $\mathfrak{M}$ be the unique maximal ideal of $\mathsf{K}[[\boldsymbol{T}]]$, generated by $\{T^1, \ldots, T^n\}$. 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 (3.14) is equivalent with

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

and the lemma is proved. □

It is well know 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 *change 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 3.2.2. *Let the series $e^i(\boldsymbol{T}) \in \mathsf{K}[[\boldsymbol{T}]]$ $(i = 1, \ldots, n)$ be given such that*

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

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

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

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

$$u^i(\boldsymbol{e}(\boldsymbol{Y})) = e^i(\boldsymbol{e}(\boldsymbol{Y})) - e^i(\boldsymbol{Y}) = Y^i - e^i(\boldsymbol{Y}) = -u^i(\boldsymbol{Y}). \tag{3.15}$$

However, we have $\dfrac{\partial u^i}{\partial T^j}(\mathbf{0}) = -2\delta^i_j$, 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 (3.15), we get $u^i(\boldsymbol{e}(\boldsymbol{v}(\boldsymbol{T}))) = -T^i$. □

As 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 derivations* 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 $T^1, \ldots, T^n$ (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 Bol loop be given with formal product $(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$ and cosider 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

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

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

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

Lemma 3.2.3. *The map $\tilde{D} : \alpha \mapsto \tilde{D}_\alpha$ is a K-linear embedding*

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

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

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

Remark. We call the derivations $\tilde{D}_\alpha$ 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 calculte the formula for $\tilde{D}_\alpha$. By definition, we have

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

Hence,

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

3.3 Infinitesimal algebras of formal Bol loops

In contrast to the previous section, we now start using the Bol property of our formal loops heavily. The basis of the applied calculation methods relies on [Nôn61].

For $i = 1, \dots, n$, we introduce the power series

$$e^i(\boldsymbol{T}) = \nu_1^i(\boldsymbol{T}, \boldsymbol{0}) \text{ and } \varphi^i(\boldsymbol{X}, \boldsymbol{Y}) = \mu^i(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{X})).$$

Lemma 3.3.1. *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 notation $\chi^i_k(\boldsymbol{T}) = \dfrac{\partial \varphi^i}{\partial X^k}(\boldsymbol{0}, \boldsymbol{T})$ *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

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

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

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

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, put $\boldsymbol{Y} = \boldsymbol{0}$ and use (ii). Then we have

$$\frac{\partial \varphi^i}{\partial X^j}(\boldsymbol{X}, \boldsymbol{0}) = 2\frac{\partial \mu^i}{\partial X^j}(\boldsymbol{X}, \boldsymbol{X}), \tag{3.16}$$

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 3.3.2. *Let us consider the formal Bol loop B with formal product $(\mu^i(\boldsymbol{X},\boldsymbol{Y}))$ and assume* $\operatorname{char}(\mathsf{K}) \neq 2$. *Let us define the elements*

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

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 very last statement only. In any Bol loop, the identity $t \cdot yx = (t \cdot xt) \cdot t^{-1}y$ holds. 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 it by T^k and putting $\boldsymbol{T} = \boldsymbol{0}$ results

$$\frac{\partial \mu^i}{\partial X^k}(\boldsymbol{0},\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y})) = \frac{\partial \mu^i}{\partial X^j}(\boldsymbol{X},\boldsymbol{Y})\frac{\partial \varphi^j}{\partial X^k}(\boldsymbol{0},\boldsymbol{X}) - \frac{\partial \mu^i}{\partial Y^j}(\boldsymbol{X},\boldsymbol{Y})\frac{\partial \mu^j}{\partial X^k}(\boldsymbol{0},\boldsymbol{Y}). \tag{3.17}$$

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

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

and put $F_k = A_k - E_k$. Then, (3.17) can be equivalently written as

$$F_k(\mu^i(\boldsymbol{X},\boldsymbol{Y})) = \xi^i_k(\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y})). \tag{3.18}$$

Applying (3.18) several times, we get

$$\begin{aligned}
[[F_k,F_\ell],F_m](\mu^i) &= (F_kF_\ell F_m - F_\ell F_k F_m - F_m F_k F_\ell + F_m F_\ell F_k)(\mu^i) \\
&= F_kF_\ell(\xi^i_m(\boldsymbol{\mu})) - F_\ell F_k(\xi^i_m(\boldsymbol{\mu})) \\
&\quad -F_mF_k(\xi^i_\ell(\boldsymbol{\mu})) + F_mF_\ell(\xi^i_k(\boldsymbol{\mu})) \\
&= F_k\left(\frac{\partial \xi^i_m}{\partial Y^r}(\boldsymbol{\mu})\xi^r_\ell(\boldsymbol{\mu})\right) - F_\ell\left(\frac{\partial \xi^i_m}{\partial Y^r}(\boldsymbol{\mu})\xi^r_k(\boldsymbol{\mu})\right) \\
&\quad -F_m\left(\frac{\partial \xi^i_\ell}{\partial Y^r}(\boldsymbol{\mu})\xi^r_k(\boldsymbol{\mu})\right) + F_m\left(\frac{\partial \xi^i_k}{\partial Y^r}(\boldsymbol{\mu})\xi^r_\ell(\boldsymbol{\mu})\right) \\
&= U^i_{k\ell m}(\boldsymbol{\mu}),
\end{aligned}$$

where

$$\begin{aligned}
U^i_{k\ell m}(\boldsymbol{T}) &= \frac{\partial \xi^i_m}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi^r_\ell}{\partial Y^s}(\boldsymbol{T})\xi^s_k(\boldsymbol{T}) - \frac{\partial \xi^i_m}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi^r_k}{\partial Y^s}(\boldsymbol{T})\xi^s_\ell(\boldsymbol{T}) \\
&\quad -\frac{\partial \xi^i_\ell}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi^r_k}{\partial Y^s}(\boldsymbol{T})\xi^s_m(\boldsymbol{T}) + \frac{\partial \xi^i_k}{\partial Y^r}(\boldsymbol{T})\frac{\partial \xi^r_\ell}{\partial Y^s}(\boldsymbol{T})\xi^s_m(\boldsymbol{T}) \\
&\quad -\frac{\partial^2 \xi^i_\ell}{\partial Y^r \partial Y^s}(\boldsymbol{T})\xi^s_m(\boldsymbol{T})\xi^r_k(\boldsymbol{T}) + \frac{\partial^2 \xi^i_k}{\partial Y^r \partial Y^s}(\boldsymbol{T})\xi^s_m(\boldsymbol{T})\xi^r_\ell(\boldsymbol{T}) \\
&\in \mathsf{K}[[\boldsymbol{T}]].
\end{aligned}$$

On the other hand, straightforward calculation gives

$$[[E_k, E_\ell], E_m] = U^i_{k\ell m}(\boldsymbol{Y}) \frac{\partial}{\partial Y^i}, \tag{3.19}$$

for the series $U^i_{k\ell m}(\boldsymbol{Y})$ with $k, \ell, m = 1, \ldots, n$. Moreover, the invertibility of the matrices $(\chi^i_k(\boldsymbol{T}))_{i,k}$ and $(\xi^i_k(\boldsymbol{T}))_{i,k}$ 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

$$\begin{aligned} [[E_k, E_\ell], E_m] &= w^i_{k\ell m}(\boldsymbol{Y}) E_i, \\ [[A_k, A_\ell], A_m] &= \bar{w}^i_{k\ell m}(\boldsymbol{X}) A_i \end{aligned} \tag{3.20}$$

hold for all $k, \ell, m = 1, \ldots, n$. (3.19) and (3.20) 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

$$[[F_k, F_\ell], F_m](\mu^i(\boldsymbol{X}, \boldsymbol{Y})) = w^j_{k\ell m}(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})) \xi^i_j(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})). \tag{3.21}$$

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

$$[[F_k, F_\ell], F_m](\mu^i) = \bar{w}^j_{k\ell m}(\boldsymbol{X}) A_j(\mu^i) - w^j_{k\ell m}(\boldsymbol{Y}) E_j(\mu^i). \tag{3.22}$$

Using Lemma 3.3.1, we get

$$\left.\begin{aligned} A_j(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} &= \chi^s_j(\boldsymbol{0}) \frac{\partial \mu^i}{\partial X^s}(\boldsymbol{0}, \boldsymbol{Y}) = 2\xi^i_j(\boldsymbol{Y}), \\ A_j(\varphi^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} &= \chi^s_j(\boldsymbol{0}) \frac{\partial \varphi^i}{\partial X^s}(\boldsymbol{0}, \boldsymbol{Y}) = 2\chi^i_j(\boldsymbol{Y}), \\ E_j(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} &= \xi^s_j(\boldsymbol{Y}) \frac{\partial \mu^i}{\partial Y^s}(\boldsymbol{0}, \boldsymbol{Y}) = \xi^i_j(\boldsymbol{Y}). \end{aligned}\right\} \tag{3.23}$$

(3.23) can be applied to substitute $\boldsymbol{X} = \boldsymbol{0}$ in (3.22):

$$[[F_k, F_\ell], F_m](\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} = 2\bar{w}^j_{k\ell m}(\boldsymbol{0}) \xi^i_j(\boldsymbol{Y}) - w^j_{k\ell m}(\boldsymbol{Y}) \xi^i_j(\boldsymbol{Y}). \tag{3.24}$$

Substituting $\boldsymbol{X} = \boldsymbol{0}$ in (3.21), we obtain

$$[[F_k, F_\ell], F_m](\mu^i(\boldsymbol{X}, \boldsymbol{Y}))|_{\boldsymbol{X}=\boldsymbol{0}} = w^j_{k\ell m}(\boldsymbol{Y}) \xi^i_j(\boldsymbol{Y}). \tag{3.25}$$

Now, if we compare (3.24) with (3.25) and use the invertibility of $(\xi^i_k(\boldsymbol{T}))_{i,k}$, we obtain the final result

$$w^j_{k\ell m}(\boldsymbol{Y}) = \bar{w}^j_{k\ell m}(\boldsymbol{0}) = w^j_{k\ell m}(\boldsymbol{0}) \in \mathsf{K} \tag{3.26}$$

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

Lemma 3.3.3. *Let us use the notation of Lemma 3.3.2. If* $\mathrm{char}(\mathsf{K}) = 3$, *then the space* $\mathcal{V}$ *of L-derivations is closed under the operation* $A \mapsto A^3$.

Proof. We start with applying (3.18) several times to obtain

$$\begin{aligned} F_k^3(\mu^i) &= F_k^2(\xi_k^i(\boldsymbol{\mu})) = F_k\left(\frac{\partial \xi_k^i}{\partial Y^r}(\boldsymbol{\mu})\xi_k^r(\boldsymbol{\mu})\right) \\ &= \frac{\partial^2 \xi_k^i}{\partial Y^s \partial Y^r}(\boldsymbol{\mu})\xi_k^s(\boldsymbol{\mu})\xi_k^r(\boldsymbol{\mu}) + \frac{\partial \xi_k^i}{\partial Y^r}(\boldsymbol{\mu})\frac{\partial \xi_k^r}{\partial Y^s}(\boldsymbol{\mu})\xi_k^s(\boldsymbol{\mu}) \\ &= U_k^i(\boldsymbol{\mu}). \end{aligned}$$

At the same time, straightforward calculation gives

$$E_k^3 = U_k^i(\boldsymbol{Y})\frac{\partial}{\partial Y^i} = w_k^j(\boldsymbol{Y})E_j,$$

where the existence of the power series $w_k^j(\boldsymbol{Y}) \in \mathsf{K}[[\boldsymbol{Y}]]$ follows from Lemma 3.3.1(iv). Thus,

$$F_k^3(\mu^i) = w_k^j(\boldsymbol{\mu})\xi_j^i(\boldsymbol{\mu}). \tag{3.27}$$

On the other hand, still using Lemma 3.3.1(iv), we can put $A_k^3 = \bar{w}_k^i(\boldsymbol{X})A_k$ for some series $\bar{w}_k^i(\boldsymbol{X}) \in \mathsf{K}[[\boldsymbol{X}]]$. By $[A_k, E_k] = 0$, we have

$$F_k^3(\mu^i) = A_k^3(\mu^i) - E_k^3(\mu^i) = \bar{w}_k^j(\boldsymbol{X})A_j(\mu^i) - w_k^j(\boldsymbol{Y})E_j(\mu^i). \tag{3.28}$$

Setting $\boldsymbol{X} = \boldsymbol{0}$ in (3.27) and (3.28) and applying (3.23), we obtain

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

which gives

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

for all $i, k = 1, \ldots, n$. □

Proposition 3.3.4. *The space of formally invariant derivations of a formal Bol loop forms a Lie triple system. Moreover, if the characteristic of the ground field is 3, then the Lie triple system is restricted.*

Proof. Since the space of derivations is an associative algebra, the statements follow immediately from Lemma 3.1.1, Lemma 3.3.2 and Lemma 3.3.3. □

3.4 The infinitesimal formal associator

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

$$\mu^i(\boldsymbol{X}, \boldsymbol{Y}) = X^i + Y^i + \mu_3^i(\boldsymbol{X}, \boldsymbol{Y}) + o(5), \tag{3.29}$$

where $\mu_3^i(\boldsymbol{X},\boldsymbol{Y})$ is a homogenous polynomial of degree 3 in $X^1,\dots,Y^n$. 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*

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

On the one hand,

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

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

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

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 3.4.1. *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*

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

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

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

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 3.3. From $\xi_k^i(\boldsymbol{0})=\delta_k^i$ follows that Φ maps the canonical basis element $\epsilon(i)$ of K^n to the basis element E_i of $\mathfrak{b}$. Let us denote by $\omega_{k\ell m}^i$ and $w_{k\ell m}^i$ the structure constants of $(\mathsf{K}^n,\langle.,.,.\rangle)$ and $(\mathfrak{b},[[.,.],.])$ in these basis, respectively. We will show that

$$w_{k\ell m}^i=-2\omega_{k\ell m}^i\tag{3.30}$$

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 $\dfrac{\partial \xi^i_j}{\partial Y^s}(\mathbf{0}) = 0$ for all $i, j, s = 1, \dots, n$. If we put

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

then we can write

$$w^i_{k\ell m} = \frac{\partial^3 g^i_{abc}}{\partial X^k \partial Y^\ell \partial Y^m}(\mathbf{0}) - \frac{\partial^3 g^i_{abc}}{\partial X^\ell \partial Y^k \partial Y^m}(\mathbf{0}) \tag{3.31}$$

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

On the other hand, by (3.29) we have

$$\begin{aligned}
\alpha^i(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) &= \mu^i(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z}) - \mu^i(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{Z})) \\
&\quad + \mu^i_3(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}) + \boldsymbol{Z} + o(3), -\boldsymbol{X} - \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{Z}) + o(3)) \\
&\quad + o(5) \\
&= \mu^i(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z}) - \mu^i(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{Z})) \\
&\quad + \mu^i_3(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}) + \boldsymbol{Z}, -\boldsymbol{X} - \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{Z})) + o(5) \\
&= \mu^i(\boldsymbol{X}, \boldsymbol{Y}) + Z^i + \mu^i_3(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z}) \\
&\quad - X^i - \mu^i(\boldsymbol{Y}, \boldsymbol{Z}) - \mu^i_3(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{Z})) \\
&\quad + \mu^i_3(\boldsymbol{X} + \boldsymbol{Y} + \boldsymbol{Z} + o(3), -\boldsymbol{X} - \boldsymbol{Y} - \boldsymbol{Z} + o(3)) + o(5) \\
&= \mu^i_3(\boldsymbol{X}, \boldsymbol{Y}) + \mu^i_3(\boldsymbol{X} + \boldsymbol{Y} + o(3), \boldsymbol{Z}) \\
&\quad - \mu^i_3(\boldsymbol{Y}, \boldsymbol{Z}) - \mu^i_3(\boldsymbol{X}, \boldsymbol{Y} + \boldsymbol{Z} + o(3)) + o(5) \\
&= (d\mu^i_3)(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) + o(5),
\end{aligned} \tag{3.32}$$

where the operator d associate 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

$$\alpha^i_3(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = (d\mu^i_3)(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = \sum_{1 \le a < b < c \le n} (dg^i_{abc})(X^a, \dots, Z^c). \tag{3.33}$$

Now, by (3.31) and (3.33), all we have to show is the following statement:

(*) *For all a, b, c with $1 \leq a < b < c \leq n$, the coefficient of $X^k Y^\ell Z^m$ in dg^i_{abc} is precisely*

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

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

However, we should not forget that the series μ^i define a formal Bol loop. With help of calculations of type (3.32), we get

$$(d'\mu^i_3)(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = 0 \tag{3.34}$$

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

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

to a function $f(X, Y)$. For any $1 \leq a, b, c \leq n$, 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 $1 \leq a, b, c \leq n$, then (3.34) 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

$$\begin{aligned} & s_1\,(X^a\,X^b\,Y^a + X^b\,Y^{a2}) + s_2\,(-X^a\,(Y^c)^2 + 2\,X^c\,Y^a\,Y^c + (X^c)^2\,Y^a) \\ &\quad + s_3\,(X^c\,(Y^c)^2 + (X^c)^2\,Y_3) + s_4\,(2\,X^c\,Y^b\,Y^c - X^b\,(Y^c)^2 + (X^c)^2\,Y^b) \\ &\quad + s_5\,(-X^a\,(Y^b)^2 + 2\,X^b\,Y^a\,Y^b + (X^b)^2\,Y^a) \\ &\quad + s_6\,((X^b)^2\,Y^c - X^c\,(Y^b)^2 + 2\,X^b\,Y^b\,Y^c) \\ &\quad + s_7\,((X^b)^2\,Y^b + X^b\,(Y^b)^2) + s_8\,(X^a\,(Y^a)^2 + (X^a)^2\,Y^a) \\ &\quad + s_9\,(-X^c\,(Y^a)^2 + 2\,X^a\,Y^a\,Y^c + (X^a)^2\,Y^c) \\ &\quad + s_{10}\,(X^a\,X^b\,Y^a + (X^a)^2\,Y^b + 2\,X^a\,Y^a\,Y^b) \\ &\quad + s_{11}\,(-X^c\,Y^a\,Y^b + X^a\,X^b\,Y^c + X^a\,Y^b\,Y^c + X^b\,Y^a\,Y^c) \\ &\quad + s_{12}\,(X^a\,X^b\,Y^b + X^a\,(Y_2)^2) \\ &\quad + s_{13}\,(X^a\,X^c\,Y^a + X^c\,(Y^a)^2) + s_{14}\,(X^a\,(Y^c)^2 + X^a\,X^c\,Y^c) \\ &\quad + s_{15}\,(X^a\,X^c\,Y^b + X^c\,Y^a\,Y^b - X^b\,Y^a\,Y^c + X^a\,Y^b\,Y^c) \\ &\quad + s_{16}\,(X^b\,Y^a\,Y^c - X^a\,Y^b\,Y^c + X^c\,Y^a\,Y^b + X^b\,X^c\,Y^a) \\ &\quad + s_{17}\,(X^b\,X^c\,Y^c + X^b\,(Y^c)^2) + s_{18}\,(X^c\,(Y^b)^2 + X^b\,X^c\,Y^b) \end{aligned}$$

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

Chapter 4

Tangent algebras of algebraic CML's

4.1 Localization of algebraic loops

It is known that via the *localization process*, any algebraic group determines a formal group (see [Die57, Sel67]). In this section, we explain this method for the class of algebraic Bol loops and use it to describe the tangent algebra of an algebraic Bol loop abstractly.

Let L be a Bol 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 $\mathsf{K}[L] = \cap_{x\in L}\mathfrak{o}_x(L)$ 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, $\mathfrak{O}_x(L)$ can be identified with the ring of power series $\mathsf{K}[[\boldsymbol{T}]] = \mathsf{K}[[T^1, \ldots, T^n]]$ 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 $L \times L$ to 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 coproduct* on $\mathsf{K}[[\boldsymbol{T}]]$. Now, for each $i = 1, \ldots, n$, we define the power series $\mu^i(\boldsymbol{X}, \boldsymbol{Y}) = \Delta(T^i)$.

We do the same for the inverting map $x \mapsto x^{-1}$ 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 3.2.1, it suffices to consider the series $\mu^i(\boldsymbol{X}, \boldsymbol{Y})$.

Lemma 4.1.1. *The formal power series $\mu^i(\boldsymbol{X}, \boldsymbol{Y})$ $(i = 1, \ldots, n)$ determine a formal Bol loop in n variables.*

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

$$\begin{aligned}
&u_1 : (x_1, x_2, x_3, x_4) \mapsto x_1(x_2 \cdot x_3x_4),\\
&u_2 : (x_1, x_2, x_3, x_4) \mapsto (x_1 \cdot x_2x_3)x_4,\\
&v : (x_1, x_2, x_3) \mapsto (x_1, x_2, x_1, x_3).
\end{aligned}$$

We have

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

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. □

A *point derivation* δ in $x \in L$ is a linear map $\mathfrak{o}_x(L) \to \mathsf{K}$ such that the Leibnitz 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 Leibnitz rule can be uniquely extended 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 on [Hum75, p. 66 and 68] to show that $D : \alpha \mapsto$

D_α is an 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 coproduct $\mathsf{K}[L] \to \mathsf{K}[L] \otimes \mathsf{K}[L]$.

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 results 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 3.2.3.

Lemma 4.1.2. *For the maps $D : \alpha \mapsto D_\alpha$, $\tilde{D} : \alpha \mapsto \tilde{D}_\alpha$ we have $\tilde{D}_\alpha \in \mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]])$ and the diagram*

$$\begin{tikzcd}
T_eL \arrow[r, "D"] \arrow[d, "natural"'] & \mathrm{Der}(\mathsf{K}[L]) \arrow[d, "extensions"] \\
\mathrm{PDer}(\mathsf{K}[[\boldsymbol{T}]]) \arrow[r, "\tilde{D}"'] & \mathrm{Der}(\mathsf{K}[[\boldsymbol{T}]])
\end{tikzcd}$$

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

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

Proof. The mappings of the diagram are well well defined and the formula for $\tilde{D}_\alpha$ holds by Lemma 3.2.3. Let α be a point derivations pf $\mathsf{K}[L]$ with completion $\tilde{\alpha} \in \mathrm{PDer}(\mathsf{K}[[\boldsymbol{T}]])$. The derivations $D_\alpha = (\alpha \otimes 1) \circ \mu^*$ and $\tilde{D}_{\tilde{\alpha}} = (\tilde{\alpha} \hat{\otimes} 1) \circ \Delta$ are compatible since the formal coproduct $\Delta : \mathsf{K}[[\boldsymbol{T}]] \to \mathsf{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ is the completion of the coproduct $\mu^* : \mathsf{K}[L] \to \mathsf{K}[L] \otimes \mathsf{K}[L]$ by definition. □

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

Theorem 4.1.3. *Let L be an algebraic Bol 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 $\{D_\alpha | \alpha \in T_e(L)\}$ 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 $\mathrm{char}(\mathsf{K}) = 3$, then the map $D_\alpha \mapsto D_\alpha^3$ makes $\mathfrak{l}$ into a restricted Lie triple system.*

Proof. We keep using the notation of Chapter 3. By Lemma 4.1.2, 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, Proposition 3.3.4 imply the theorem. □

Remark. Clearly, any algebraic group G is an algebraic Bol loop. From now on, in the sense of the above proposition, beside the tangent Lie algebra of G we can speak of the tangent L.t.s. of G, as well.

4.2 Loops as sections in algebraic groups

The method of considering loops as sections in their translation groups is originally due to A.A. Albert ([Alb43], [Alb44]), for a very recent and excessive reference see [NS99]. This method is extremely useful in the investigation of Bruck and in particular commutative Moufang loops.

It is not the aim of this section to explain the method in details, but we use it in order to *recover the tangent algebra of an algebraic CML in the Lie algebra of its multiplication group.*

From now on, we consider the connected unipotent algebraic CML L. We denote by H the group generated by the inner maps $\lambda_{x,y}$ $(x, y \in L)$ and by G the multiplication group of L. From the proof of Theorem 2.4.2 we know that G is isomorphic to $L \times H$ as a variety. Hence, we have the morphisms

$$\psi : G \to L \ \text{ and } \ i : L \to G$$

such that $i(x) = \lambda_x$ and $\psi(\lambda_x h) = x$ for all $x \in L$ and $h \in H$. Moreover, for any $x \in L$ and $g \in G$, the K-homomorphisms $\tau_x : \mathsf{K}[L] \to \mathsf{K}[L]$ and $\bar\tau_g : \mathsf{K}[G] \to \mathsf{K}[G]$ are defined by

$$(\tau_x f)(x') = f(x'x) \ \text{ and } \ (\bar\tau_g p)(g') = p(g'g)$$

for all $x' \in L$, $f \in \mathsf{K}[L]$ and $g' \in G$ and $p \in \mathsf{K}[G]$.

Lemma 4.2.1. *For all $x \in L$ and $h \in H$, the following diagram commutes:*

$$\begin{tikzcd}
\mathsf{K}[L] \arrow[r, "\tau_x"] \arrow[d, "\psi^*"'] & \mathsf{K}[L] \\
\mathsf{K}[G] \arrow[r, "\bar\tau_{\lambda_x h}"'] & \mathsf{K}[G] \arrow[u, "i^*"']
\end{tikzcd}$$

Proof. With $h' = \lambda_{yx}\lambda_y\lambda_x h \in H$, we have

$$\begin{aligned}
(i^*\bar\tau_{\lambda_x h}\psi^* f)(y) &= (\bar\tau_{\lambda_x h}\psi^* f)(\lambda_y) \\
&= (\psi^* f)(\lambda_y\lambda_x h) = (\psi^* f)(\lambda_{yx}h') \\
&= f(yx) = (\tau_x f)(y)
\end{aligned}$$

for all $y \in L$ and $f \in \mathsf{K}[L]$. □

Let us denote by $\mathfrak{g}$ the Lie algebra of G. Recall that the elements of $\mathfrak{g}$ are the (right) invariant derivations of $\mathsf{K}[G]$; these are precisely the derivations of the form D_α with point derivation $\alpha \in T_eG$ (cf. [Hum75, Chapter III]); by definition:

$$(D_\alpha f)(g) = \alpha(\bar\tau_g f), \qquad g \in G.$$

Since $i(e) = e$, the morphism i defines a K-linear map $di : T_eL \to T_eG$.

Lemma 4.2.2. *For any $\alpha \in T_eL$, the following diagram commutes:*

$$\begin{tikzcd}
\mathsf{K}[L] \arrow[r, "D_\alpha"] \arrow[d, "\psi^*"'] & \mathsf{K}[L] \arrow[d, "\psi^*"] \\
\mathsf{K}[G] \arrow[r, "D_{di(\alpha)}"'] & \mathsf{K}[G]
\end{tikzcd}$$

Proof. On the one hand, $(\psi^* D_\alpha f)(\lambda_x h) = (D_\alpha f)(x) = \alpha(\tau_x f)$ holds for all $f \in \mathsf{K}[L]$, $x \in L$ and $h \in H$. On the other hand, we have

$$\begin{aligned}
(D_{di(\alpha)}\psi^* f)(\lambda_x h) &= di(\alpha)(\bar{\tau}_{\lambda_x h}\psi^* f) \\
&= \alpha(i^*\bar{\tau}_{\lambda_x h}\psi^* f) \\
&= \alpha(\tau_x f)
\end{aligned}$$

by Lemma 4.2.1. □

We define the automorphism σ of G by $\sigma(\lambda_x h) = \lambda_x^{-1} h$. It is clear that σ is an involutive morphism of G (cf. [Bru58]), in the terminology of [NS99, Section 11], $G\langle\sigma\rangle$ is an algebraic reflection group with respect to the conjugacy class of σ.

Since $\sigma(e) = e$, the map $d\sigma : \alpha \mapsto \alpha \circ \sigma^*$ is an involutive automorphism of T_eG. Using the definitions given so far, we obtain

$$\begin{aligned}
((\sigma^* D_{d\sigma(\alpha)})f)(g) &= (D_{d\sigma(\alpha)}f)(\sigma(g)) = d\sigma(\alpha)(\bar{\tau}_{\sigma(g)}f) \\
&= \alpha(\sigma^*\bar{\tau}_{\sigma(g)}f) = \alpha(\bar{\tau}_g\sigma^* f) \\
&= ((D_\alpha\sigma^*)f)(g)
\end{aligned}$$

for all $f \in \mathsf{K}[G]$ and $g \in G$, whence $D_{d\sigma(\alpha)} = \sigma^* D_\alpha \sigma^*$. With other words, the action of $d\sigma$ on T_eG is compatible the action $\delta \mapsto \sigma^*\delta\sigma^*$ of σ^* on $\mathfrak{g}$. We denote by $(T_eG)^-$ and $\mathfrak{g}^-$ the nontrivial eigenspace of $d\sigma$ and σ^*, respectively. Clearly, $\mathfrak{g}^-$ is closed under $[[.,.],.]$.

Proposition 4.2.3. *Let L be an algebraic CML with tangent algebra $\mathfrak{l}$. Let G be the multiplication group of L with Lie algebra $\mathfrak{g}$. Then, the map $D_\alpha \mapsto D_{di(\alpha)}$ ($\alpha \in T_eL$) defines an isomorphism between the Lie triple systems $(\mathfrak{l}, [[.,.],.])$ and $(\mathfrak{g}^-, [[.,.],.])$.*

Proof. Clearly, the map $\Theta : D_\alpha \mapsto D_{di(\alpha)}$ ($\alpha \in T_eL$) is injective. Moreover, since $\mathrm{char}(\mathsf{K}) \neq 2$, σ is a semisimple element, and by [Hum75, Proposition 18.1], $\mathfrak{g}^-$ is the tangent space of

$$\{g^{-1}\sigma(g) | g \in G\} = \{\lambda_x | x \in L\},$$

which is isomorphic to L. Thus, $\dim \mathfrak{l} = \dim \mathfrak{g}^-$. We still have to show $di(\alpha) \in (T_eG)^-$ in order to see that Θ is a linear isomorphism between $\mathfrak{l}$

and $\mathfrak{g}^-$. And indeed, the composition $L \xrightarrow{(i,\sigma i)} G \times G \xrightarrow{\mu} G$ maps x to e, its differential $d\mu \circ (di, d\sigma di)$ is therefore 0. This means $di(\alpha) + d\sigma(di(\alpha)) = 0$ for all $\alpha \in T_eL$ (cf. [Hum75, Proposition 10.1]), and implies $\sigma^* D_{di(\alpha)}\sigma^* = -D_{di(\alpha)}$ by the calculation above.

Finally, Lemma 4.2.2 implies $\psi^* D_\alpha D_\beta D_\gamma = D_{di(\alpha)} D_{di(\beta)} D_{di(\gamma)} \psi^*$ for all $\alpha, \beta, \gamma \in T_eL$, whence $\psi^*[[D_\alpha, D_\beta], D_\gamma] = [[D_{di(\alpha)}, D_{di(\beta)}], D_{di(\gamma)}]\psi^*$.

Let us now choose a basis $\alpha_1, \ldots, \alpha_n$ for T_eL and consider the structure constants $w^j_{k\ell m}$, $\bar{w}^j_{k\ell m}$ of $\mathfrak{l}$ and $\mathfrak{g}^-$, with respect to the basis $D_{\alpha_1}, \ldots, D_{\alpha_n}$ and $D_{di(\alpha_1)}, \ldots, D_{di(\alpha_n)}$, respectively. As we just have seen,

$$\psi^*(w^j_{k\ell m} D_{\alpha_j}) = (\bar{w}^j_{k\ell m} D_{di(\alpha_j)})\psi^* = \psi^*(\bar{w}^j_{k\ell m} D_{\alpha_j}).$$

Substituting $\beta = (w^j_{k\ell m} - \bar{w}^j_{k\ell m})\alpha_j \in T_eL$, we obtain $\psi^* D_\beta = 0$. This implies

$$(D_\beta f)(x) = (\psi^* D_\beta f)(\lambda_x) = 0$$

for all $f \in \mathsf{K}[L]$ and $x \in L$, thus $\beta = 0$ and $w^j_{k\ell m} = \bar{w}^j_{k\ell m}$ holds for all $k, \ell, m, j = 1, \ldots, n$. □

4.3 Tangent algebras of algebraic CML's

Theorem 4.1.3 shows that the tangent space of an algebraic Bol loop can be endowed with a structure of a Lie triple system. In this section, we show that for an algebraic commutative Moufang loop, the tangent algebra defined in this way plays exactly the same role that Lie algebras do in the case of algebraic groups.

In this section, we denote by $\alpha(x, y, z)$ the associator map $(x{\cdot}yz)^{-1}{\cdot}(xy{\cdot}z)$ of a CML. For any non-negative integer i, Bruck [Bru58] defines the functions f_i on the commutative Moufang loop L by

$$\begin{aligned} f_0(x, y, z) &= \alpha(x, y, z), \\ f_{i+1}(x, y, z; a_1, \ldots, a_i, u) &= \alpha(f_i(x, y, u; a_1, \ldots, a_i), u, z). \end{aligned}$$

Let $(\mathfrak{b}, (.,.,.))$ be a Lie triple system over a field K. For each non-negative integer i, we define a function F_i on $\mathfrak{b}$ by

$$\begin{aligned} F_0(x, y, z) &= (x, y, z), \\ F_{i+1}(x, y, z; a_1, \ldots, a_i, u) &= (F_i(x, y, u; a_1, \ldots, a_i), u, z). \end{aligned}$$

Theorem 4.3.1. *Let L be an algebraic commutative Moufang loop with tangent algebra $\mathfrak{l}$. Then, $\mathfrak{l}$ is a restricted Lie triple system w.r.t. the operations $(D_\alpha, D_\beta, D_\gamma) = [[D_\alpha, D_\beta], D_\gamma]$ and $D^{[3]}_\alpha = D^3_\alpha$ ($\alpha, \beta, \gamma \in T_eL$). Moreover, for each non-negative integer i, the functions $F_i = F_i(x, y, z; a_1, \ldots, a_i)$ are symmetric in $a_1, \ldots, a_n$ and skew-symmetric in x, y, z.*

Proof. We assume L to be connected w.l.o.g. and proper in order to avoid trivialities. By Corollary 2.1.8, the base field has to have characteristic 3, thus, by Theorem 4.1.3, $(\mathfrak{l}, (.,.,.))$ is a restricted L.t.s. By Proposition 2.1.9, L has a Jordan decomposition $L = U \times S$ with $S \leq Z(L)$. It is very easy to see that this induces a decomposition $\mathfrak{l} = \mathfrak{u} \oplus \mathfrak{s}$, where $\mathfrak{u}, \mathfrak{s} \triangleleft \mathfrak{l}$ are the tangent subalgebras of U and S, respectively, and the L.t.s. $\mathfrak{s}$ is trivial. This means that we may suppose $L = U$ when considering non-trivial properties of the tangent L.t.s. $\mathfrak{l}$.

By Theorem 2.1.10 and Lemma 2.2.3, L can be supposed to be identical with K^n ($n = \dim L$) such that $X^{-1} = -X$ holds. Then, $\mathsf{K}[L] = \mathsf{K}[\boldsymbol{T}]$ and we can identify T_eL with K^n by

$$(a_1, \ldots, a_n) \longleftrightarrow a^i \left.\frac{\partial}{\partial T^i}\right|_{\boldsymbol{T}=\boldsymbol{0}}.$$

Let us define the L.t.s. operation $(.,.,.)$ on K^n by

$$D_{(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})} = [[D_{\boldsymbol{x}}, D_{\boldsymbol{y}}], D_{\boldsymbol{z}}],$$

clearly $(\mathsf{K}^n, (.,.,.)) \cong \mathfrak{l}$ holds. Furthermore, by Proposition 3.4.1, we have

$$\alpha(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = (\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) + o(5).$$

This implies

$$f_i(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}; \boldsymbol{a}_1, \ldots, \boldsymbol{a}_i) = F_i(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}; \boldsymbol{a}_1, \ldots, \boldsymbol{a}_i) + o(2i + 5)$$

immediately. The properties of the functions f_i given in [Bru58, Lemma VIII.7.2.] imply the second part of the theorem. □

Remark. One of the most important property of the tangent algebra of an algebraic CML is that the L.t.s. operation *alternates*, i.e.,

$$(x, y, z) = -(y, x, z) \quad \text{and} \quad (x, y, z) = (y, z, x)$$

hold. Much to our regrets, this property is far not sufficient: If K is a field of characteristic 3, then we can construct an L.t.s. on K^3 with 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, ℓ, m, i. We define the [3]-map to be the trivial map $x \mapsto 0$. The resulting ternary algebra is an "alternating" restricted L.t.s., which does not happen to be the tangent algebra of a CML since $F_1(x, y, y; a) = 0$ is not satisfied.

On page 62, we will present an example for a proper formal Bruck loop (in a generalized sense), whose tangent algebra is precisely the one just explained. Similarly, one can show that now finite subset of the identities describing the properties of the functions F_i characterizes the tangent algebras of algebraic CML's.

Proposition 4.3.2. *Let L and M be algebraic CML's over the algebraically closed field K and let $u : L \to M$ be a morphism of algebraic loops over K. Then, the map $\Psi : D_\alpha \to D_{du(\alpha)}$ ($\alpha \in T_eL$) defines a homomorphism between the Lie triple systems $\mathfrak{l}$ and $\mathfrak{m}$ of L and M, respectively.*

Proof. First we show that the diagram

$$\begin{tikzcd} \mathsf{K}[M] \arrow[r, "D_{du(\alpha)}"] \arrow[d, "u^*"'] & \mathsf{K}[M] \arrow[d, "u^*"] \\ \mathsf{K}[L] \arrow[r, "D_\alpha"'] & \mathsf{K}[L] \end{tikzcd} \tag{4.1}$$

commutes. Indeed, for any $f \in \mathsf{K}[M]$ and $x, y \in L$, we have $(\tau_x u^* f)(y) = f(u(yx))$ and $(u^*\tau_{u(x)} f)(y) = f(u(y)u(x))$, hence $\tau_x u^* f = u^*\tau_{u(x)} f$. Therefore,

$$(D_\alpha u^* f)(x) = \alpha(\tau_x u^* f) = \alpha(u^*\tau_{u(x)} f) = du(\alpha)(\tau_{u(x)}f) = (u^* D_{du(\alpha)} f)(x).$$

The diagram implies $D_\alpha D_\beta D_\gamma u^* = u^* D_{du(\alpha)} D_{du(\beta)} D_{du(\gamma)}$ as well, hence

$$[[D_\alpha, D_\beta], D_\gamma]u^* = u^*[[D_{du(\alpha)}, D_{du(\beta)}], D_{du(\gamma)}]$$

holds for all $\alpha, \beta, \gamma \in T_eL$. Let us put

$$D_\delta = [[D_\alpha, D_\beta], D_\gamma] \text{ and } D_\epsilon = [[D_{du(\alpha)}, D_{du(\beta)}], D_{du(\gamma)}]$$

with $\delta \in T_eL$ and $\epsilon \in T_eM$. All we have to show is $\epsilon = du(\delta)$. However, we have $D_\delta u^* = u^* D_\epsilon$, thus $u^* D_\varphi = 0$ with $\varphi = du(\delta) - \epsilon$. This means that

$$0 = (u^* D_\varphi f)(e) = (D_\varphi f)(u(e)) = \varphi(f)$$

holds for all $f \in \mathsf{K}[L]$, whence $\varphi = 0$ and $du(\delta) = \epsilon$. □

The following property of $\mathfrak{l}$ is analog to the ones of Lie algebras given in [Hum75, Lemma 8.5. and Lemma 9.4.].

Let H be a closed subloop of the algebraic CML L. The inclusion $u : H \to L$ is an isomorphism onto a closed subloop, u^* maps $\mathsf{K}[L]$ onto $\mathsf{K}[H] = \mathsf{K}[L]/I$ (I the ideal vanishing on H). Therefore, du identifies T_eH with a subspace of T_eG consisting of those α for which $\alpha(I) = 0$. But u is also a morphism of algebraic loops, so $du : \mathfrak{h} \to \mathfrak{l}$ is a L.t.s. homomorphism, which allows us to view $\mathfrak{h}$ as a Lie triples subsystem of $\mathfrak{l}$ (see Proposition 4.3.2).

Proposition 4.3.3. *Let H be a closed subloop of the algebraic CML L, I the ideal of $\mathsf{K}[L]$ vanishing on H. Then $H = \{x \in L | \tau_x(I) \subseteq I\}$ and $\mathfrak{h} = \{D_\alpha | \alpha \in T_eL,\ D_\alpha(I) \subseteq I\}$.*

Proof. See the proofs of [Hum75, Lemma 8.5. and Lemma 9.4.]. □

We have the following elementary formulas (cf. [Hum75, Proposition 10.1]).

Proposition 4.3.4. *Let L be an algebraic CML with multiplication $\mu(x, y) = xy$ and inverse mapping $\iota : x \mapsto x^{-1}$. Then, for all $\alpha, \beta \in T_eL$:*

(i) $d\mu(\alpha, \beta) = \alpha + \beta$.

(ii) $d\iota(\alpha) = -\alpha$.

(iii) $(dg_{x,y})(\alpha) = (1 - d\lambda_{x,y})(\alpha)$, *where* $g_{x,y}(z) = (x, y, z)$, $(x, y, z \in L)$.

Proof. For (i) and (ii), see the proof of [Hum75, Proposition 10.1]. Since by [Bru58, Lemma VIII.5.4.] we have $g_{x,y}(z) = (x, y, z) = z\lambda_{x,y}(z^{-1})$, hence $g_{x,y}$ is the composition $\mu \circ (id, \lambda_{x,y}) \circ (id, \iota)$. If $\alpha \in T_eL$, then by (i) and (ii), $dg_{x,y}(\alpha) = d\mu(\alpha, d\lambda_{x,y}(-\alpha)) = (1 - d\lambda_{x,y})(\alpha)$. □

Let us take an algebraic automorphism h of L. By diagram (4.1), we have the action

$$D_{dh(\alpha)} = (h^{-1})^* D_\alpha h^* \tag{4.2}$$

of dh on $\mathfrak{l}$. In particular, for any $x, y \in L$, we have the algebraic automorphism $\lambda_{x,y}$ of L; we denote by $\mathrm{Ad}_{x,y}$ the action (4.2) on $\mathfrak{l}$. For any $x \in L$, we have thus a map $u_x : L \to \hom(\mathfrak{l}, \mathfrak{l})$, mapping y to $\mathrm{Ad}_{x,y}$. $\hom(\mathfrak{l}, \mathfrak{l})$ has a natural structure of a variety. If u_x is a morphism, then the map $u : L \to \hom(\mathfrak{l}, \hom(\mathfrak{l}, \mathfrak{l}))$, $x \mapsto du_x$ is well defined. We will show that for all $x \in L$, the maps u_x and v are morphisms, and $(dv)(\alpha)(\beta)(\gamma) = \frac{1}{2}(\alpha, \beta, \gamma)$ holds. This fact is in analogy with [Hum75, Theorem 10.4].

Lemma 4.3.5. *Let G be a 2-divisible algebraic group, that is, we assume that the map $x \to x^2$ is a automorphism of the variety G. Let us denote by $\nu : x \mapsto x^{\frac{1}{2}}$ the inverse of $x \mapsto x^2$. For any $x, y \in G$, we define the map $t_{x,y} : G \to G$ by*

$$t_{x,y}(z) = (x^{-\frac{1}{2}}y^{-1}x^{\frac{1}{2}}y)z(x^{-\frac{1}{2}}y^{-1}x^{\frac{1}{2}}y)^{-1}.$$

Then, for all $x, y \in G$, $t_{x,y}$ is a morphism. For any $x \in G$, let us define the map $u_x : G \to \hom(\mathfrak{g}, \mathfrak{g})$ by $u_x(y) = dt_{x,y}$. Then, for all $x \in G$, u_x is a morphism. Finally, we define the map $v : G \mapsto \hom(\mathfrak{g}, \hom(\mathfrak{g}, \mathfrak{g}))$ by $v(x) = du_x$. Then, v is a morphism and

$$(dv)(\alpha)(\beta)(\gamma) = \frac{1}{2}[[\alpha, \beta], \gamma]$$

holds for all $\alpha, \beta, \gamma \in \mathfrak{g}$.

Proof. For any $x \in L$, we define the $G \to G$ morphisms $\mathrm{Int}(x)\,(y) = xyx^{-1}$ and $\psi(x)\,(y) = x^{-1}y^{-1}xy$. Then, $t_{x,y} = \mathrm{Int}(x^{-\frac{1}{2}}y^{-1}x^{\frac{1}{2}}y)$ and

$$dt_{x,y} = \mathrm{Ad}(x^{-\frac{1}{2}}y^{-1}x^{\frac{1}{2}}y) = (\mathrm{Ad} \circ \psi(x^{\frac{1}{2}}))(y)$$

in the notation of [Hum75]. Since for any $x \in L$, $\psi(x^{\frac{1}{2}}) : G \to G$ is a morphism and $\mathrm{Ad} : G \to \hom(\mathfrak{g}, \mathfrak{g})$ is a morphism by [Hum75, Proposition 10.3], v_x is a morphism, as well. Moreover, $d\,\mathrm{Ad} = \mathrm{ad}$ and $d\psi(x) = 1 - \mathrm{Ad}(x^{-1})$ by [Hum75, Proposition 10.1 and Theorem 10.4], thus, $du_x = \mathrm{ad} \circ (1 - \mathrm{Ad}(x^{-\frac{1}{2}}))$. $\mathrm{ad} : \mathfrak{g} \to \hom(\mathfrak{g}, \mathfrak{g})$ is linear map and Ad and $x \mapsto x^{-\frac{1}{2}}$ are morphisms, thus $v : x \mapsto du_x$ is a morphism with differential

$$dv = \frac{1}{2}\,\mathrm{ad} \circ \mathrm{ad} : \mathfrak{g} \to \hom(\mathfrak{g}, \hom(\mathfrak{g}, \mathfrak{g})).$$

This finishes the proof of the lemma. □

Let X_1, X_2, Y_1, Y_2 be (abstract) sets. We say that the maps $f_1 : X_1 \to Y_1$ and $f_2 : X_2 \to Y_2$ are *(φ, ψ)-equivalent*, if the maps $\varphi : X_1 \to X_2$ and $\psi : Y_1 \to Y_2$ are bijections and $f_1 \circ \psi = \varphi \circ f_2$ holds. We express this fact with the diagram

$$\begin{tikzcd}
X_1 \arrow[r, "f_1"] \arrow[d, "\varphi"'] & Y_1 \arrow[d, "\psi"] \\
X_2 \arrow[r, "f_2"'] & Y_2
\end{tikzcd} .$$

If $Y_1 = Y_2$ and $\varphi = \psi$, we simply speak of φ-equivalence. Clearly, if X_1, X_2, Y_1, Y_2 are varieties with morphism f_1 and automorphisms φ, ψ of varieties, then f_2 is a morphism, as well.

Let V_1, V_2 be vector spaces, then $\hom(V_1, V_2) \cong V_1^* \otimes V_2$ in a natural way. Now, if $f_1 : V_1 \to W_1$ and $f_2 : V_2 \to W_2$ are linear isomorphisms, then they induce a $\hom(V_1, V_2) \to \hom(W_1, W_2)$ isomorphism, which we denote by $(f_1^{-1})^* \otimes f_2$.

Lemma 4.3.6. *The map $L \times L \to \hom(\mathfrak{l}, \mathfrak{l})$, $(x, y) \mapsto d\lambda_{x,y}$ is a morphism of algebraic varieties.*

Proof. An element $h \in H$ is an algebraic automorphism of L, normalizing the set $S = S(L)$. Moreover, h acts on L in the same way as it does on S by conjugation. This is easy to show abstractly, and it follows from the construction in the proof of Theorem 2.4.2 that the two actions are i-equivalent. Thus, by Proposition 4.2.3, the linear action of dh on T_eL is di-equivalent to the linear action of Ad_h on $\mathfrak{g}^- \leq \mathfrak{g}$. By [Hum75, Proposition 10.3], the map $H \to \hom(\mathfrak{g}^-, \mathfrak{g}^-)$, $h \mapsto \mathrm{Ad}_h$ is a morphism. On the other hand, the map $(x, y) \mapsto \mathrm{Ad}_{x,y}$ is precisely the composition of the morphisms

$$\begin{cases} L \times L \to H \\ (x, y) \mapsto \lambda_{x,y} \end{cases}, \qquad \begin{cases} H \to GL(\mathfrak{g}^-) \\ h \mapsto \mathrm{Ad}_h |_{\mathfrak{g}^-} \end{cases}$$

and $(di)^{-1} \otimes (di)^{-1} : \hom(\mathfrak{g}^-, \mathfrak{g}^-) \to \hom(\mathfrak{l}, \mathfrak{l})$. This gives us the diagrams

$$\begin{tikzcd} L \arrow[r, "\lambda_{x,y}"] \arrow[d, "i"'] & L \arrow[d, "i"] \\ S(L) \arrow[r, "t_{i(x),i(y)}"'] & S(L) \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} \mathfrak{l} \arrow[r, "d\lambda_{x,y}"] \arrow[d, "di"'] & \mathfrak{l} \arrow[d, "di"] \\ \mathfrak{g}^- \arrow[r, "dt_{i(x),i(y)}"'] & \mathfrak{g}^- \end{tikzcd} . \qquad \square$$

We make two remarks for the next theorem. Due to the Jordan decomposition $L = U \times S$, we can assume L to be a connected, unipotent and proper algebraic CML. Let us denote by G and H the translation group and the group generated by the inner mappings of L. Let $S(L)$ be the set of left translations λ_x of L. Then $G = S(L) \times H \cong L \times H$ as variety. We denote by i the automorphism $x \mapsto \lambda_x$ between the varieties L and $S(L)$.

By Corollary 2.1.11, L has finite exponent of the form 3^e, hence by [Bru58, Lemma VIII.11.5.], G has finite exponent of the form 3^f, thus, the group G is 2-divisible.

Theorem 4.3.7. *Let L be an algebraic CML with tangent L.t.s. $(\mathfrak{l}, (.,.,.))$. The map $\mathrm{Ad} : L \times L \to GL(\mathfrak{l})$, defined by $(x, y) \mapsto \mathrm{Ad}_{x,y}$ is a morphism of algebraic varieties. The map $U_x : L \to \hom(\mathfrak{l}, \mathfrak{l})$ defined by $U_x(y) = \mathrm{Ad}_{x,y}$ is a morphism. Finally, the map $V : L \to \hom(\mathfrak{l}, \hom(\mathfrak{l}, \mathfrak{l}))$ defined by $V(x) = dU_x$ is a morphism with differential*

$$(dV)(\alpha)(\beta)(\gamma) = \frac{1}{2}(\alpha, \beta, \gamma).$$

Proof. Applying the definition of morphically equivalent actions, we get first the diagrams

$$\begin{tikzcd} L \arrow[r, "U_x"] \arrow[d, "i"'] & \hom(\mathfrak{l}, \mathfrak{l}) \arrow[d, "(di^{-1})^* \otimes di"] \\ S(L) \arrow[r, "u_{i(x)}"'] & \hom(\mathfrak{g}^-, \mathfrak{g}^-) \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} \mathfrak{l} \arrow[r, "dU_x"] \arrow[d, "di"'] & \hom(\mathfrak{l}, \mathfrak{l}) \arrow[d, "(di^{-1})^* \otimes di"] \\ \mathfrak{g}^- \arrow[r, "du_{i(x)}"'] & \hom(\mathfrak{g}^-, \mathfrak{g}^-) \end{tikzcd} ,$$

explaining us the equivalences of the mappings dU_x and $du_{i(x)}$ for all $x \in L$. Using the same thing once more, we get

$$\left.\begin{tikzcd} L \arrow[r, "V"] \arrow[d, "i"'] & \hom(\mathfrak{l}, \hom(\mathfrak{l}, \mathfrak{l})) \arrow[d, "(di^{-1})^* \otimes (di^{-1})^* \otimes di"] \\ S(L) \arrow[r, "v"'] & \hom(\mathfrak{g}^-, \hom(\mathfrak{g}^-, \mathfrak{g}^-)) \\ \mathfrak{l} \arrow[r, "dV"] \arrow[d, "di"'] & \hom(\mathfrak{l}, \hom(\mathfrak{l}, \mathfrak{l})) \arrow[d, "(di^{-1})^* \otimes (di^{-1})^* \otimes di"] \\ \mathfrak{g}^- \arrow[r, "dv"'] & \hom(\mathfrak{g}^-, \hom(\mathfrak{g}^-, \mathfrak{g}^-)) \end{tikzcd}\right\} \tag{4.3}$$

representing the equivalences of the mappings V and v. Using Lemma 4.3.5, we obtain that all maps mentioned in the proposition are morphism, and by Proposition 4.2.3, the diagrams (4.3) give precisely

$$(dV)(\alpha)(\beta)(\gamma) = \frac{1}{2}(\alpha, \beta, \gamma). \quad \square$$

An *ideal* (see [Lis52]) of a L.t.s. $\mathfrak{b}$ is a subspace $\mathfrak{h}$ such that for

$$(x, y, \mathfrak{h}), (x, \mathfrak{h}, y), (\mathfrak{h}, x, y) \leq \mathfrak{h}$$

holds all $x, y \in \mathfrak{b}$. The *center* $\mathfrak{z}(\mathfrak{b})$ of $\mathfrak{b}$ is the subspace consisting of the elements $z \in \mathfrak{b}$ such that

$$(z, \mathfrak{b}, \mathfrak{b}) = (\mathfrak{b}, z, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{b}, z) = 0.$$

Proposition 4.3.8. *Let K be a closed normal subloop of the algebraic CML L. Then, the tangent L.t.s. $\mathfrak{k}$ of K is an ideal in $\mathfrak{l}$.*

Proof. To say that K is normal is to say that all $\lambda_{x,y}$ $(x, y \in L)$ stabilize K; hence $\mathrm{Ad}_{x,y}$ $(x, y \in L)$ stabilize $\mathfrak{k}$. Thus, in an appropriate basis, $\mathrm{Ad}_{x,y}$ has the form

$$\left(\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right). \tag{4.4}$$

Let us denote by $\mathfrak{M}$ the subspace of $\hom(\mathfrak{l}, \mathfrak{l})$, consisting of matrices of the form (4.4). Then, U_x maps L to $\mathfrak{M}$ and $V(x) = dU_x \in \hom(\mathfrak{l}, \mathfrak{M})$. Since $\hom(\mathfrak{l}, \mathfrak{M})$ is a linear subspace of $\hom(\mathfrak{l}, \hom(\mathfrak{l}, \mathfrak{l}))$, we have $(dV)(\alpha) \in \hom(\mathfrak{l}, \mathfrak{M})$ for all $\alpha \in \mathfrak{l}$. This means that $(dV)(\alpha)(\beta)$ has the form (4.4) for all $\alpha, \beta \in \mathfrak{l}$, hence

$$(dV)(\alpha)(\beta)(\gamma) = \frac{1}{2}(\alpha, \beta, \gamma) \in \mathfrak{k}$$

for all $\gamma \in \mathfrak{k}$. By the alternation property of $\mathfrak{l}$, this suffices to have $\mathfrak{k} \lhd \mathfrak{l}$. $\square$

Proposition 4.3.9. *Let A, B and C closed subloops of the algebraic CML L with tangent algebras $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, respectively. Let D be the subloop (A, B, C), generated by the associators. Then, the tangent algebra $\mathfrak{d}$ of D contains all elements*

$$\begin{gathered} \gamma - \mathrm{Ad}_{x,y}(\gamma), \beta - \mathrm{Ad}_{x,z}(\beta), \alpha - \mathrm{Ad}_{y,z}(\alpha), \\ V(x)(\beta)(\gamma), V(y)(\alpha)(\gamma), V(z)(\alpha)(\beta) \ \ \textit{and} \ \ (\alpha, \beta, \gamma) \end{gathered}$$

($x \in A, y \in B, z \in C$, $\alpha \in \mathfrak{a}, \beta \in \mathfrak{b}, \gamma \in \mathfrak{c}$).

Proof. All concepts of the statement are well defined, since by Proposition 2.1.5, D is a closed subloop of L. We use the notation of Proposition 4.3.4. For $x \in A$, $y \in B$, $g_{x,y}$ maps $C \to D$, so the differential $1 - \mathrm{Ad}_{x,y}$ maps $\mathfrak{c} \to \mathfrak{d}$.

This yields the elements of the first type listed, similarly for the second and third type.

For fixed $x \in A$ and $\gamma \in \mathfrak{c}$, consider the morphism $B \to \mathfrak{d}$, $y \mapsto \gamma - \mathrm{Ad}_{x,y}(\gamma) = \gamma - U_x(y)(\gamma)$. Since it maps e to 0, we can compute its derivative $\mathfrak{b} \to \mathfrak{d}$, mapping β to $V(x)(\beta)(\gamma) \in \mathfrak{d}$ (since $V(x) = dU_x$). This works for elements of the 4th, 5th and 6th types.

Finally, for fixed $\beta \in \mathfrak{b}$ and $\gamma \in \mathfrak{c}$, we have the $A \to \mathfrak{d}$ morphism $x \mapsto V(x)(\beta)(\gamma)$, its derivative maps an element $\alpha \in \mathfrak{a}$ to the element

$$(dV)(\alpha)(\beta)(\gamma) = \frac{1}{2}(\alpha, \beta, \gamma)$$

of $\mathfrak{d}$, showing $(\alpha, \beta, \gamma) \in \mathfrak{d}$. □

Corollary 4.3.10. *Let L be an algebraic CML with associator subloop $L' = (L, L, L)$. Then, the tangent L.t.s. $\mathfrak{l}'$ of L' includes $(\mathfrak{l}, \mathfrak{l}, \mathfrak{l})$ (= the set of all linear combinations of elements (α, β, γ), $\alpha, \beta, \gamma \in \mathfrak{l}$).* □

Chapter 5

The Cartier duality of formal Bruck loops

In this chapter, we extend the definition given in Chapter 3 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 in characteristic 0 and 3. Our construction generalizes an analogous result of P. Cartier [Car62, Théorème 3, 4] on (restricted) Lie algebras and formal groups.

5.1 Generalized formal loops

In Chapter 3, 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 $\mathsf{K}[[\boldsymbol{T}]]$ ($\boldsymbol{T} = (T^1,\dots,T^n)$) of formal power series in n variables "imitated" 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 $\operatorname{char}(\mathsf{K}) = p > 0$, then we allow the ring $\mathsf{K}[[\boldsymbol{T}]]/I$ as formal function ring, as well, where the ideal $I \lhd \mathsf{K}[[\boldsymbol{T}]]$ is generated by elements of the form $(T^j)^{p^k}$ with $j \in \{1,\dots,n\}$ 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 be still denoted by $\mathsf{K}[[\boldsymbol{T}]]$, where $(T^j)^{p^k} = 0$ is allowed when $\operatorname{char}(\mathsf{K}) = p > 0$. We will say that *the formal loop has height h* if $(T^i)^{p^{h+1}} = 0$ holds for all $i \in \{1,\dots,n\}$. 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 concept of derivations, point derivations, tangent algebras, formal Bol loops and formal Bruck loops can be taken over to this extended definition without any difficulty. The most important results concerning formal Bol loops, like the Lemmas 3.3.2, 3.3.3, 3.2.2 and Proposition 3.4.1, 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 $\mathrm{char}(\mathsf{K}) = 0$ and I is as above if $\mathrm{char}(\mathsf{K}) = p > 0$.

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* $A \hat{\otimes} B$ 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 a *coproduct*, which is a continuous homomorphism

$$c : A \to A \hat{\otimes} A$$

and a *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

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

(I and J defined as above) and the coproduct 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:

$$\begin{tikzcd}
A \arrow[r, "c"] \arrow[d, "c"'] & A \hat{\otimes} A \arrow[d, "c \otimes 1"] \\
A \hat{\otimes} A \arrow[r, "1 \otimes c"'] & A \hat{\otimes} A \hat{\otimes} A
\end{tikzcd}$$

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

$$\begin{tikzcd}
A \arrow[r, "c"] \arrow[d, "c"'] & A\hat{\otimes}A \arrow[r, "c\otimes 1"] & A\hat{\otimes}A\hat{\otimes}A \arrow[d, "\mu\otimes 1"] \\
A\hat{\otimes}A \arrow[r, "1\otimes c"'] & A\hat{\otimes}A\hat{\otimes}A \arrow[r, "\mu\otimes 1"'] & A\hat{\otimes}A
\end{tikzcd}$$

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

5.2 Cartier duality of formal groups

In this section, we explain the functorial equivalence between the category of Lie algebras (restricted Lie algebras) and the category of formal groups (formal groups of height 0).

Theorem 5.2.1 (Cartier)**.** *Let* K *be a field and let us denote the Lie algebra of the formal group* G *by* $\mathfrak{L}(G)$*.*

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

b) If $\mathrm{char}(\mathsf{K}) = p > 0$*, then* $\mathfrak{L}$ *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) needs some higher algebra. The idea is the following. Let $\mathfrak{g}$ be a restricted Lie algebra over the field K with $\mathrm{char}(\mathsf{K}) = p > 0$, 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

$$\{b_1^{s_1} \cdots b_n^{s_n} | 0 \le s_1, \ldots, s_n < p\}$$

(see [Sel67, Theorem I.3.2]). One can introduce a cocommutative, coassociative coproduct 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 one, coassociative coproduct and counit. The basis of the dual space A can be (symbolically) written in the form

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

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. Finally, the images $\mu^i(\boldsymbol{X},\boldsymbol{Y})$ of the generating elements T^i under the coproduct 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 coproduct is equivalent to the formal associativity of G.

5.3 The generalization of the Cartier duality

In this section, we generalize Theorem 5.2.1 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 3.1.2), we have to restrict ourselves to the case $\mathrm{char}(\mathsf{K})\in\{0,3\}$. However, a proof of Theorem 3.1.2 for the case $\mathrm{char}(\mathsf{K})>3$ would immediately imply the full generality of the Theorem 5.3.1.

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

Theorem 5.3.1. *a) If* $\mathrm{char}(\mathsf{K})=0$*, then* $\mathfrak{L}$ *is an equivalence between the category of formal Bruck loops over* K *and the category of Lie triple systems over* K*.*

b) If $\mathrm{char}(\mathsf{K})=3$*, then* $\mathfrak{L}$ *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 $\mathfrak{L}$, that is, to find the formal loop of a given (restricted) L.t.s.

In [Nag99b], 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

$$\sum_{k=0}^{\infty}d_{2k+1}(X,Y),\tag{5.1}$$

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 $\mathrm{char}(\mathsf{K}) = 0$, then $\mathbb{Q} \subset \mathsf{K}$ and we can take the series (5.1) as a formal power series over K in $n = \dim \mathfrak{b}$ variables and forget about the 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 $\mathrm{char}(\mathsf{K}) = 3$ and let $\mathfrak{b}$ be a restricted L.t.s. over K. In Theorem 3.1.2, 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 $\mathfrak{g} = \mathfrak{b} \oplus \mathfrak{D}$, where $\mathfrak{D}$ was a restricted Lie subalgebra of $\mathfrak{g}$, consisting of derivations of $\mathfrak{b}$.

We define the map

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

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 by σ, as well. As we explained in the previous section, $U_3(\mathfrak{g})$ is an associative algebra with a cocommutative, coassociative coproduct 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 $\mathsf{K}[[T^1, \ldots, T^n]]/((T^i)^3)$, the coproduct, 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 5.3.2. *With 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 3.2.2, 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 resulting $\boldsymbol{s}(\boldsymbol{T}) = D\boldsymbol{T}$. 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

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

We suppose now that the formal group $G = (\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$ on A is given such that $e^i(\boldsymbol{T}) = -T^i$ $(i = 1, \ldots, n)$, $s^i(\boldsymbol{T}) = -T^i$ $(i = 1, \ldots, m)$ and $s^i(\boldsymbol{T}) = T^i$ $(i = m+1, \ldots, n)$ hold. It follows from Cartier's Theorem 5.2.1 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 Bol loop one can associate a 2-divisible Bruck loop with operation

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

In the next lemma, we copy this trick on formal Bol loops and use it for the formal group G later on.

Lemma 5.3.3. *Let the series $(\mu^i(\boldsymbol{X}, \boldsymbol{Y}))$ define a formal Bol loop L with with formal square root operation $(\nu^i(\boldsymbol{T}))$ and tangent L.t.s. $\mathfrak{l}$. Then, the series*

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

define a formal Bruck loop $\hat{L}$ such that

a) the inverting $\boldsymbol{e}$ and any automorphism of L are automorphisms of $\hat{L}$.

b) the tangent L.t.s. $\hat{\mathfrak{l}}$ of $\hat{L}$ is isomorphic to $\mathfrak{l}$.

Proof. The fact that $(\hat{\mu}^i(\boldsymbol{X}, \boldsymbol{Y}))$ is a formal Bruck loop can be shown in 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 [NS99]. Part a) follows immediately.

Let us now consider the tangent algebras $\mathfrak{l}$ and $\hat{\mathfrak{l}}$ and use the notation of Section 3.3. The tangent algebras are spanned by the derivations $\{E_k\}$ and $\{\hat{A}_k\}$ with

$$E_k = \xi_k^i(\boldsymbol{Y})\frac{\partial}{\partial Y^i},\ \hat{E}_k = \hat{\xi}_k^i(\boldsymbol{Y})\frac{\partial}{\partial Y^i}$$

and

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

Let us now recall the notation

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

Clearly, $\hat{\boldsymbol{\mu}}(\boldsymbol{X},\boldsymbol{Y}) = \boldsymbol{\varphi}(\boldsymbol{\nu}(\boldsymbol{X}),\boldsymbol{Y})$, thus, by $\boldsymbol{\nu}(\boldsymbol{T}) = \frac{1}{2}\boldsymbol{T} + \ldots$

$$\hat{\xi}^i_k(\boldsymbol{Y}) = \frac{1}{2}\chi^i_k(\boldsymbol{Y})$$

holds. Hence, $\{\hat{E}_k\}$ and $\{A_k\}$ span isomorphic algebras. In particular, $\{A_k\}$ spans an restricted Lie triple, say $\mathfrak{l}'$. If we denote the structure constants of $\mathfrak{l}$ and $\mathfrak{l}'$ by $w^i_{k\ell m}$ and $\bar{w}^i_{k\ell m}$, respectively, then the equations (3.20) and (3.26) give $w^i_{k\ell m} = \bar{w}^i_{k\ell m}$.

This shows that $\mathfrak{l}$ and $\mathfrak{l}'$ are isomorphic Lie triple systems. We can similarly argue to see that the [3]-maps are isomorphic, too. □

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

Lemma 5.3.4. *The equations $T^{m+1} = \ldots = T^n = 0$ define a formal subloop of $\hat{G}$ whose tangent algebra is $\mathfrak{b}$.*

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

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

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

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

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

This finishes the proof of Theorem 5.3.1. □

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. We did the calculation for the example given on page 49. Thus, the following formal Bruck loop of height 0 has an "alternating" tangent L.t.s. but it is not a formal CML. (Actually, it has trivial center, it is solvable but not nilpotent.)

$$\begin{pmatrix} X_1 + Y_1 \\ X_2 + Y_2 \\ X_3 + Y_3 + (X_1 - Y_1)(X_2Y_3 - X_3Y_2) + \mu_5(\boldsymbol{X}, \boldsymbol{Y}) + \mu_7(\boldsymbol{X}, \boldsymbol{Y}) \end{pmatrix}$$

$$\begin{aligned} \mu_5(\boldsymbol{X}, \boldsymbol{Y}) &= -X_1^2\, X_2^2\, Y_3 + X_1^2\, X_2\, X_3\, Y_2 + X_1\, X_2^2\, X_3\, Y_1 - X_1\, X_2^2\, Y_1\, Y_3 \\ &\quad +X_1\, X_2\, X_3\, Y_1\, Y_2 + X_2^2\, X_3\, Y_1^2 - X_2^2\, Y_1^2\, Y_3 + X_2\, X_3\, Y_1^2\, Y_2 \\ \mu_7(\boldsymbol{X}, \boldsymbol{Y}) &= -X_1^2\, X_2^2\, X_3\, Y_1\, Y_2 \end{aligned}$$

For obtaining this example and for checking its correctness, we used the computer algebra program GAP4 [Gro98].

Chapter 6

Commutative alternative algebras

In this chapter, we consider a special class of algebraic commutative Moufang loops, namely the loop of units of a commutative alternative algebra. More precisely, starting with a finite commutative Moufang loop L and a field K of characteristic 3 we constract a finite dimensional commutative alternative algebra as a factor of the loop ring $\mathsf{K}L$.

6.1 Alternative algebras and bimodules

An *algebra* A over the field K is a finite dimensional vector space over K which is at the same time a distributive ring. In this chapter, we don't require neither the multiplication to be associative nor the existence of a multiplicative unit. Subalgebras and ideals of a non-associative algebra can be defined in the obvious way.

For the algebra A we define the *commutator* and *associator brackets*:

$$[x, y] = xy - yx, \qquad\qquad [x, y, z] = xy \cdot z - x \cdot yz.$$

Both maps are linear in every variable, and the commutator bracket is anticommutative. The commutator and associator brackets are linked with the following identities.

$$\left\{\begin{array}{rcl} [xy, z] + [yz, x] + [zx, y] & = & [x, y, z] + [y, z, x] + [z, x, y] \\ [[x, y], z] + [[y, z], x] + [[z, x], y] & = & [x, y, z] - [y, x, z] + [y, z, x] \\ & & -[z, y, x] + [z, x, y] - [x, z, y] \end{array}\right. \tag{6.1}$$

The algebra A is an *alternative algebra* when

$$x(xy) = x^2y, \qquad x(yx) = (xy)x, \qquad (xy)y = xy^2$$

holds for all $x, y \in A$. These equations can be expressed with the associator bracket: $[x, x, y] = [x, y, x] = [x, y, y] = 0$. By polarization, the associator bracket turns out to be an alternating map from $A \times A \times A$ to A. Conversely, the alternating property for the associator bracket implies A to be an alternative algebra. For alternative algebras, the identities (6.1) become

$$\begin{cases} 3[x,y,z] = [xy,z] + [yz,x] + [zx,y], \\ 6[x,y,z] = [[x,y],z] + [[y,z],x] + [[z,x],y]. \end{cases} \tag{6.2}$$

That is, if $\mathrm{char}(\mathsf{K}) \neq 2, 3$, the commutator map determines the associator. Furthermore, if $\mathrm{char}(\mathsf{K}) \neq 3$, a commutative alternative algebra is associative.

Let us now suppose that $\mathrm{char}(\mathsf{K}) = 3$ and A be a commutative algebra. Then, $[x, y, z] = -[z, y, x]$ holds for all x, y, z; thus, for A to be alternative, it suffices to have $[x, y, z] = -[y, x, z]$, which is equivalent to

$$xy \cdot z + yz \cdot x + zx \cdot y = 0. \tag{6.3}$$

Proposition 6.1.1. *The set A^* of the units of a commutative alternative algebra A form an algebraic commutative Moufang loop.*

Proof. To see that A^* is a CML, we take an element $x \in A^*$; this means that there is an element $x^{-1} \in A$ such that $x^{-1}x = 1$. We have to show that $x^{-1} \cdot xy = y$ holds for all $y \in A$. Let us first suppose $xy = 0$. By (6.3), we have

$$xy \cdot x^{-1} + yx^{-1} \cdot x + x^{-1}x \cdot y = 0,$$

thus, $y = -x \cdot x^{-1}y$. By [Sch66, p. 28.], alternative algebras satisfy the left Bol identity (1.2), hence

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

and $x^{-1}y = 0 = -x \cdot x^{-1}y = y$. Let us now suppose $y \neq 0$, then $xy \neq 0$, and because of $xy = x(x^{-1} \cdot xy)$, one has $x(x^{-1} \cdot xy - y) = 0$. This gives us $x^{-1} \cdot xy = y = yx \cdot x^{-1}$ and A^* is a loop.

On the other hand, the algebra multiplication is bilinear, hence given by quadratic polynomials over K. The set A^* is isomorphic to the Zariski closed subset $\{x \oplus y \in A \oplus A | xy = 1\}$ of $A \oplus A$. □

6.2 Bimodules and loop representations

For an associative K-algebra A and a K-vector space M, we use the concepts of A-modules and A-bimodules in the usual sense.

Let now A be an alternative K-algebra. Following [Sch66, p. 65.], the K-vector space M is said to be an *A-bimodule* , when the actions $(a, m) \mapsto a.m$ and $(m, a) \mapsto m.a$ are given on both sides such that

$$a.(a.m) = a^2.m \qquad a.(m.a) = (a.m).a \qquad (m.a).a = m.a^2$$
$$(a.m).b - a.(m.b) = -a.(b.m) + ab.m = -(m.a).b + m.ab.$$

Analogously to the associative case, this implies that the semidirect product defined by

$$(a, m)(b, n) = (ab, a \cdot n + m \cdot b)$$

is an alternative algebra $B = A + M$ with subalgebra A and nilideal M. If A is commutative, then it suffices to define the action on one side and to require the analogue of (6.3)

$$ab.m + a.(b.m) + b.(a.m) = 0. \tag{6.4}$$

An easy non-associative example for a commutative bimodule is the following. Let K be an arbitrary field of characteristic 3, $A = \mathsf{K}^2$ a nilalgebra and $M = \mathsf{K}^4$ a vector space. Let us define the action of $a = (x, y)$ on $\mathbf{v} \in M$ by

$$a.\mathbf{v} = \left(\begin{array}{cccc} 0 & x & y & 0 \\ & & & y \\ & \mathbf{0} & & -x \\ & & & 0 \end{array} \right) \cdot \mathbf{v}.$$

Since $a.(a.\mathbf{v}) = \mathbf{0} = a^2.\mathbf{v}$, we have $a.(b.\mathbf{v}) + b.(a.\mathbf{v}) = 0$ by polarization, which is enough because of $ab = 0$. Moreover, with $a = (x, y)$ and $a' = (x', y')$,

$$a.(a'.\mathbf{v}) = \left(\begin{array}{cccc} 0 & 0 & 0 & xy' - x'y \\ & & & 0 \\ & \mathbf{0} & & 0 \\ & & & 0 \end{array} \right) \cdot \mathbf{v}$$

is not zero in general, hence the semidirct sum $B = A + M$ is a proper commutative alternative algebra.

Let $(L, \cdot)$ be a 2-divisible CML, M a K-space, $\mathrm{char}(\mathsf{K}) = 3$. The mapping $\rho : L \longrightarrow \mathrm{GL}(M)$ is by definition a *representation of* L if

$$\rho(x^{-1}) = \rho(x)^{-1} \quad \text{and} \quad \rho(xy) = \frac{1}{2}(\rho(x)\rho(y) + \rho(y)\rho(x)) \tag{6.5}$$

for all $x, y \in L$. If L is finite, then the condition $\rho(x^{-1}) = \rho(x)^{-1}$ can be replaced by $\rho(1) = 1$. Furthermore, $\rho(xyx) = \rho(x)\rho(y)\rho(x)$ follows from the definition immediately.

A representation ρ of L is called *linear* , if for all $x_1, x_2, x_3 \in L$ holds

$$\sum_{\{i,j,k\}=\{1,2,3\}} \rho(x_i)\rho(x_j)\rho(x_k) = 0 \tag{6.6}$$

Let us define the kernel $\ker \rho = \{x \in L; \rho(x) = 1\}$. We claim that $\rho(x) = \rho(y)$ if and only if $xy^{-1} \in \ker \rho$; the "if" part being trivial. Conversely,

$\rho(x) = \rho(xa)$ implies $\rho(x^{\frac{1}{2}})^2 = \rho(x^{\frac{1}{2}})\rho(a)\rho(x^{\frac{1}{2}})$ and $\rho(a) = 1$. For any $n, m \in \ker\rho$ and $x, y \in L$ we have

$$\begin{array}{rcl}\rho(xn \cdot ym) & = & \frac{1}{2}(\rho(xn)\rho(ym) + \rho(ym)\rho(xn)) \\ & = & \frac{1}{2}(\rho(x)\rho(y) + \rho(y)\rho(x)) \\ & = & \rho(xy),\end{array}$$

which means that $\ker\rho$ is a normal subloop of L and $\bar{\rho}(x \cdot \ker\rho) = \rho(x)$ is a faithful representation of $L/\ker\rho$. A representation with trivial kernel is called *faithful*.

Equation (6.3) implies that $A^* \longrightarrow \mathrm{GL}(A)$, $x \mapsto L_x$ is a representation. ($\frac{1}{2} = -1 \pmod 3$). We remark, that $A^* \neq \emptyset$ if and only if A has a multiplicative unit. In this case, this representation is faithful and linear, as we shall show now.

For a representation ρ, the loop identity $x \cdot xy = x^2y$ implies

$$\rho(x)^2\rho(y) + \rho(x)\rho(y)\rho(x) + \rho(y)\rho(x)^2 = 0. \qquad (6.7)$$

This gives the condition (6.6) after "polarization". Of course, in general, $\rho(x) + \rho(y) \neq \rho(z)$. But in A^*, we have $L_x + L_y = L_{x+y}$, thus the polarization method works, and the representation turns out to be linear. This proves the following lemma.

Lemma 6.2.1. *Let A be a commutative alternative algebra with unit* 1*. Then the loop of units A^* of A is not empty, and the map $x \mapsto L_x$ ($x \in A^*$) is a faithful linear representation of A^*.*

The next proposition shows that for a CML linear representations correspond precisely to embeddings in commutative alternative algebras; this is the reason for our choice of terminology.

Proposition 6.2.2. *Let L be a finite CML. A homomorphism of L in the loop of units of a commutative alternative algebra defines a linear representation of L. Conversely, a linear representation of L defines a homomorphism $L \longrightarrow A^*$ for some commutative alternative algebra A.*

Proof. Lemma 6.2.1 proves the first statement. Let us now take a linear representation $\rho : L \longrightarrow \mathrm{GL}(M)$ and put $\mathcal{M} = \rho(L)$. On the one hand, $\mathcal{M}$ is closed under the commutative, bilinear operation $a \circ b = \frac{1}{2}(ab + ba)$, hence so does the linear span $A = \langle\mathcal{M}\rangle$, as well. In order to check the alternativity of the commutative K-algebra $(A, \circ)$ it suffices to show $[a_1, a_2, a_3]^\circ = -[a_2, a_1, a_3]^\circ$ for the generating elements $a_i = \rho(x_i) \in \mathcal{M}$ ($x_i \in L, i = 1, 2, 3$). But ρ is linear and

$$[a_1, a_2, a_3]^\circ + [a_2, a_1, a_3]^\circ = \frac{1}{2} \sum_{\{i,j,k\}=\{1,2,3\}} a_i a_j a_k = 0$$

holds by (6.6). Hence, $(A, \circ)$ is s commutative alternative algebra and $\rho : L \longrightarrow (A^*, \circ)$ is a loop homomorphism. □

6.3 Commutative Moufang loop rings

Let T be a finite CML of odd order and K an arbitrary field of characteristic 3. We define the linear space $V = \mathsf{K}T$, and its subspaces

$$V_0 = \langle x - y; x, y \in T\rangle, \qquad W_0 = \langle x + y + (xy)^{-1}; x, y \in T\rangle.$$

Obviously, V_0 is just a hyperplane (sum of the coefficients is 0), and $W_0 \leq V_0$. A question arises naturally: "How big is W_0 in V_0?". In Lemma 6.3.2, we completely answer this question. We first prove a lemma.

Lemma 6.3.1.

(i) *Let* $T = \mathbb{Z}_3$ *be the group of order 3. Then,* $\dim V = 3$*,* $\dim V_0 = 2$*,* $\dim W_0 = 1$ *and* $x - y \in \tilde{W}_0$ *if and only if* $x = y$*.*

(ii) *For the elements* $x, y \in T$*,* $x - y \in W_0$ *if and only if* $1 - xy^{-1} \in W_0$*.*

(iii) *Let* W_1 *some fixed subspace* $W_0 \leq W_1 \leq V_0$*. Then,* $S = \{z \in T; 1 - z \in W_1\}$ *is a subloop of* L*.*

Proof. The (i) is trivial. (ii) follows from the congruence

$$1 - xy^{-1} = (1 + x + x^{-1}) - (x^{-1} + y + xy^{-1}) + y - x \equiv y - x \pmod{W_0}.$$

To show (iii), take two elements $a, b \in S$. Then, $1 - ab^{-1} \equiv a - b = 1 - b - (1 - a) \in W_1$, thus S is a subloop. □

Lemma 6.3.2.

(i) $\mathrm{codim}_{V_0} W_0 = \mathrm{rank}(T)$*, where* $\mathrm{rank}(T)$ *is the minimal number of generators of* T*.*

(ii) $x - y \in W_0$ *if and only if* $xy^{-1} \in T'$*.*

Proof. Let $m = \mathrm{rank}(T)$ and choose a minimal generating set $\{x_1, \dots, x_m\}$ for T. Put $W_1 = \langle W_0, 1 - x_i; i = 1, \dots, m\rangle$. Then the subloop S associated to W_1 as in Lemma 6.3.1(ii) is equal to T, thus $W_1 = V_0$, and

$$\mathrm{codim}_{V_0} W_0 \leq m = \mathrm{rank}(T)$$

follows.

Let us now suppose that $\mathrm{codim}_{V_0} W_0 < m$, that is,

$$V_0 = \langle W_0, 1 - x_i; i = 1, \dots, m - 1\rangle.$$

Let S be a maximal subloop of T, containing $x_1, \dots, x_{m-1}$. Clearly, $x_m \notin S$ and it is known that S is a normal subloop of index 3 in T (see [Bru58]). The map $\alpha : T \to T/S$ induces a surjective linear map $A : V \to \tilde{V}$, which maps V_0 to $\tilde{V}_0$ and W_0 to $\tilde{W}_0$ surjectively. Since for all $i = 1, \dots, m - 1$,

$\alpha(1) = \alpha(x_i)$, we have $A(1 - x_i) = 0$, thus $A(V_0) = A(W_0)$, which implies $\tilde{V}_0 = \tilde{W}_0$, a contradiction to Lemma 6.3.1(i). This proves (i).

To show (ii), we define the surjective homomorphism $\beta : T \to \bar{T} = T/T'$ and its induced $B : V \to \bar{V}$, which is surjective as well. As before, one has $B(V_0) = \bar{V}_0$ and $B(W_0) = \bar{W}_0$, which gives a surjective map $V_0/W_0 \to \bar{V}_0/\bar{W}_0$. On the other hand, $\operatorname{rank}(T) = \operatorname{rank}(\bar{T})$, thus, by (i), we get

$$\dim V_0/W_0 = \operatorname{codim}_{V_0} W_0 = \operatorname{codim}_{\bar{V}_0} \bar{W}_0 = \dim \bar{V}_0/\bar{W}_0.$$

This means that the map $V_0/W_0 \to \bar{V}_0/\bar{W}_0$ is an isomorphism, and $\ker B \leq W_0$. This proves one direction of (ii), since for $z \in T'$, $B(1 - z) = \beta(1) - \beta(z) = 0$, $1 - z \in \ker B \leq W_0$.

If $z \notin T'$, then there is a maximal normal subgroup of T not containing z, and using the factorization trick, it follows from Lemma 6.3.1(i) that $1 - z \notin W_0$. □

Let L be a CML and K be a field of characteristic 3. Let R be a system of representatives of the cosets L/L' with $1 \in R$. We define the following K-spaces.

$$\begin{aligned} B &= \mathsf{K}L, \\ W &= \langle a + b + (ab)^{-1}; a, b \in L' \rangle, \\ I &= \langle rw; w \in W, r \in R \rangle. \end{aligned}$$

One calls $B = \mathsf{K}L$ the *loop ring* of L (cf. [JGM96]).

Clearly, the associator subloop L' of L is invariant under the inner mapping $\lambda_{x,y}$. For $a, b \in L'$, this implies

$$x \cdot y(a + b + (ab)^{-1}) = xy \cdot (a' + b' + (a'b')) \tag{6.8}$$

with $a', b' \in L'$. Recall also that by the property (L4) of commutative Moufang loops, L' has exponent 3.

Proposition 6.3.3.

(i) *B is a commutative, distributive K-algebra.*

(ii) *I is a (two sided) ideal of B.*

(iii) *$A = B/I$ is a commutative alternative K-algebra.*

Proof. (i) is trivial. To show (ii), choose elements $x \in L$, $r_1 \in R$ and

$a_1, b_1 \in L'$. One has

$$\begin{aligned} x\cdot r_1(a_1+b_1+(a_1b_1)^{-1}) &= xr_1\cdot(a_2+b_2+(a_2b_2)^{-1}) \\ &\qquad (a_2,b_2\in L', \text{ by } (6.8)) \\ &= r_2c\cdot(a_2+b_2+(a_2b_2)^{-1}) \\ &\qquad (r_2\in R, c\in L', r_2c=xr_1) \\ &= r_2\cdot c(a_3+b_3+(a_3b_3)^{-1}) \\ &\qquad (a_3,b_3\in L') \\ &= r_2\cdot(ca_3+cb_3+((ca_3)(cb_3))^{-1}) \\ &\qquad (\text{yields for CML's of exp. 3}) \\ &= r_2\cdot(a_4+b_4+(a_4b_4)^{-1})\in I \\ &\qquad (a_4,b_4\in L'), \end{aligned}$$

which gives $xI \subseteq I$, proving (ii) by distributivity. For (iii) one only has to show that $\bar{x}\bar{y}\cdot\bar{z}+\bar{y}\bar{z}\cdot\bar{x}+\bar{z}\bar{x}\cdot\bar{y}=0$ holds for every $\bar{x},\bar{y},\bar{z}\in B/I$. This is equivalent to $xy\cdot z+yz\cdot x+zx\cdot y\in I$ for all $x,y,z\in B$. However,

$$xy\cdot z+yz\cdot x+zx\cdot y=(xy\cdot z)(1+(x,y,z)+(z,x,y)^{-1}),$$

where $(x,y,z)=(xy\cdot z)^{-1}(x\cdot yz)$. By [Bru58, VII. Lemma 5.5.], $(x,y,z)=(z,x,y)$. Therefore,

$$xy\cdot z+yz\cdot x+zx\cdot y=rb\cdot(1+a+a^{-1})=r\cdot(b+ba_1+(b\cdot ba_1)^{-1})\in I,$$

with $xy\cdot z=rb$, $(x,y,z)=a$ and $rb\cdot a=r\cdot ba_1$ ($r\in R$, $a,b,a_1\in L'$). □

It turns out from this proof that the construction works also if we take

$$W'=\langle 1+(x,y,z)+(x,y,z)^{-1}; x,y,z\in L\rangle$$

instead of W and put $I'=BW'$. Moreover, I' is the smallest ideal of B such that B/I' is an alternative algebra. It is not clear whether there are cases when I' is properly contained in I. However, an advantage of choosing W and I as we did is that in this case, we are able to compute the kernel of the map $L\to A^*$.

Lemma 6.3.4. *Let L be a finite CML and A be the alternative algebra constructed in Proposition 6.3.3. Then, $\rho(x)=\bar{x}$, $(x\in L)$ is a homomorphism of L (e.i., it is a linear representation) in A^* and* $\ker\rho=L''$.

Proof. The element $z\in L$ belongs to $\ker\rho$ if and only if $\bar{z}\bar{a}=\bar{a}$ for all $\bar{a}\in A$, that is, $(1-z)a\in I$ for all $a\in B$, and this is equivalent to $1-z\in I$. Let us write $R^{\#}=R\setminus\{1\}$. Then

$$A=\mathsf{K}L'\dot{+}\mathsf{K}(R^{\#}L') \text{ and } I=W\dot{+}R^{\#}W.$$

If $z\notin L'$ and $1-z\in I=W\dot{+}R^{\#}W$, then $1\in W$ and $z\in R^{\#}W$. But $1\in W$ is impossible.

Let us suppose $z \in L'$. Then, $1 - z \in I = W \dot{+} R^{\#}W$ if and only if $1 - z \in W$. Looking at the definition of W, one sees that deciding whether $1 - z \in W$ is exactly the problem solved in Lemma 6.3.2 b), where one replaces T by L' and W_0 by W. Thus, $1 - z \in W$ if and only if $z \in L''$. □

As a corollary, we have the main result of this chapter.

Theorem 6.3.5. *Any finite commutative Moufang loop $(L, \cdot)$ of odd order has a linear representation modulo L''.*

Proof. See Proposition 6.3.3 and Lemma 6.3.4. □

Corollary 6.3.6. *Any 2-divisible commutative Moufang loop L with solvability class 2 can be embedded in the loop of units of a commutative alternative algebra.* □

Remark. The class of 2-divisible CML's with solvability class 2 is quite rich. A series of examples is given on page 11; they also show that the bound on the solvability class does not restrict the nilpotency class of L.

Bibliography

[Alb43] A.A. Albert. Quasigroups I. *Trans. Amer. Math. Soc.*, 54:507–519, 1943.

[Alb44] A.A. Albert. Quasigroups II. *Trans. Amer. Math. Soc.*, 55:401–419, 1944.

[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.

[Bru58] R.H. Bruck. *A Survey of Binary Systems.* Springer-Verlag, Berlin, 1958.

[Car62] P. Cartier. Groups algébrique et groupes formels. In *Colloque sur la Théorie des Groupes Algébrique*, pages 87–111. Librairie Gauthier-Villars, 1962.

[CPS90] O. Chein, H.O. Pflugfelder, and J.D.H. Smith, editors. *Quasigroups and Loops: Theory and Applications*, volume 8 of *Sigma Series in Pure Mathematics.* Heldermann Verlag, Berlin, 1990.

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

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

[Ene94] M.R. Enea. Right distributive quasigroups on algebraic varieties. *Geom. Dedicata*, 51:257–286, 1994.

[Fig99] Á. Figula. Geodesic loops. To appear in *J. Lie Theory*, 1999.

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

[Gro98] The GAP Group. Gap — groups, algorithms, and programming. University of St Andrews and RWTH Aachen, 1998. Version 4b5.

[Hod00] T.L. Hodge. Restricted Lie triple systems and algebraic groups. To appear, 2000.

[HS90] K.H. Hofmann and K. Strambach. Topological and analytical loops. In O. Chein et al., editor, *Quasigroups and Loops: Theory and Applications*, number 8 in Sigma Series in Pure Mathematics, pages 205–262. Heldermann Verlag, Berlin, 1990.

[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.*, 70:509–530, 1951.

[JGM96] E. Jespers, E.G. Goodair, and C. Polcino Milies. *Alternative loop rings.* Number 184 in North-Holland Mathematics Studies. North-Holland, Amsterdam, 1996.

[Kik75] M. Kikkawa. Geometry of homogenous Lie loops. *Hiroshima Math. J.*, 5:141–179, 1975.

[Lis52] W.G. Lister. A structure theory of Lie triple systems. *Trans. Amer. Math. Soc.*, 72:217–242, 1952.

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

[Nag99a] G.P. Nagy. On the Burnside problems for Moufang and Bol loops. Submitted, 1999.

[Nag99b] G.P. Nagy. On the Hausdorff series of local analytic Bruck loops. Submitted, 1999.

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

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

[NS99] P.T. Nagy and K. Strambach. Sharply transitive sections in Lie groups: A Lie theory of smooth loops. Manuscript, Debrecen-Erlangen, 1999.

[Pfl90] H.O. Pflugfelder. *Quasigroups and loops: Introduction.* Number 7 in Sigma Series in Pure Mathematics. Heldermann Verlag, Berlin, 1990.

[Ram64] C.P. Ramanujam. A note on automorphism groups of algebraic varieties. *Math. Annalen*, 156:25–33, 1964.

[Ros56] M. Rosenlicht. Some basic theorems on algebraic groups. *Amer. J. Math.*, 78:401–443, 1956.

[Sab99] L.V. Sabinin. *Smooth Quasigroups and Groups*. Number 492 in Mathematics and its applications. Kluwer Academic Publisher, Dordrecht, 1999.

[Sch66] R.D. Schafer. *An Introduction to nonassociative Algebras*. Academic Press, New York and London, 1966.

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

[Sha94] I.R. Shafarevich. *Basic Algebraic Geometry*. Springer, Berlin, etc., 1994.

LEBENSLAUF

Gábor Nagy

16. Aug. 1972	Geboren in Szeged (Ungarn) als zweites Kind von Dr. Péter Nagy (Dipl.-Math.) und seiner Ehefrau Éva Kovács (Lehrerin)
Sept. 1978–Juni 1986	Besuch der Grundschule ,,Ságvári Endre” in Szeged
Sept. 1986–Juni 1990	Besuch des Ságvári-Endre-Gymnasiums in Szeged
Juni 1990	Abitur
Sept. 1990–Juni 1995	Studium der Mathematik fürs Diplom an der Attila-József-Universität Szeged (Ungarn)
Okt. 1992–Juni 1993	Studium der Mathematik an der Rijksuniversiteit Gent (Belgium), gefördert durch das TEMPUS-Programm der Europäischen Gemeinschaften
Juni 1995	Diplom Mathematik
Sept. 1995–Aug. 1996	Wissenschaflicher Mitarbeiter am Mathematischen Institut der Universität Erlangen-Nürnberg
Aug. 1996	Eheschlieung mit Krisztina Frauhammer (Lehrerin)
Sept. 1996–Aug. 1998	Wissenschaflicher Mitarbeiter am Mathematischen Institut der Attila-József-Universität Szeged
Sept. 1998–Febr. 2000	Wissenschaflicher Mitarbeiter am Mathematischen Institut der Universität Erlangen-Nürnberg
ab März 2000	Wissenschaflicher Mitarbeiter am Mathematischen Institut der Universität Szeged (Ungarn)

Erlangen, im Mai 2000