LAGUERRE POLYNOMIALS OF DERIVATIONS

MARINA AVITABILE AND SANDRO MATTAREI

Abstract. We introduce a *grading switching* for arbitrary non-associative algebras of prime characteristic p, aimed at producing a new grading of an algebra from a given one. We take inspiration from a fundamental tool in the classification theory of modular Lie algebras known as *toral switching,* which relies on a delicate adaptation of the exponential of a derivation. Our grading switching is achieved by evaluating certain generalized Laguerre polynomials of degree $p-1$, which play the role of generalized exponentials, on a derivation of the algebra. A crucial part of our argument is establishing a congruence for them which is an appropriate analogue of the functional equation $e^x \cdot e^y = e^{x+y}$ for the classical exponential. Besides having a wider scope, our treatment provides a more transparent explanation of some aspects of the original toral switching, which can be recovered as a special case.

1. Introduction

The exponential function is certainly one of the most important mathematical functions. The main reason, sometimes disguised in other forms, such as its differential formulation $(d/dx)e^x = e^x$, is that it interconnects additive and multiplicative structures, because of the fundamental identity $e^x \cdot e^y = e^{x+y}$. In particular, one of the important classical applications is the local reconstruction of a Lie group from its Lie algebra. This Lie-theoretic use of the exponential function can be formulated in more general terms as a device which turns derivations of a *non-associative* (in the standard meaning of *not necessarily associative*) algebra into automorphisms. The basic algebraic fact is already visible in the special case of nilpotent derivations, where convergence matters play no role: if D is a nilpotent derivation of a non-associative algebra A over a field of characteristic zero, then the finite sum $\exp(D) = \sum_{i=0}^{\infty} D^i/i!$ defines an automorphism of A.

This nice property breaks down over fields of positive characteristic p. The condition $D^p = 0$, which seems the minimum requirement for $\exp(D)$ to make sense in this context, does not guarantee that $\exp(D)$ is an automorphism. In fact, only the stronger assumption $D^{(p+1)/2} = 0$ does, for p odd. In the absence of the assumption $D^p = 0$ one can use the *truncated*

2000 *Mathematics Subject Classification.* Primary 17A36; secondary 33C52, 17B50, 17B65.

Key words and phrases. Non-associative algebra; grading; derivation; Laguerre polynomial; restricted Lie algebra; toral switching.

exponential $E(X) = \sum_{i=0}^{p-1} X^i/i!$ as some kind of substitute for the exponential series, of course dropping any expectation that evaluating it on D may yield an automorphism.

In the theory of modular Lie algebras the apparent shortcoming of $\exp(D)$ not necessarily being an automorphism when it is defined is turned into an advantage with the technique of *toral switching.* This is a fundamental tool which originated in [Win69], but has undergone substantial generalizations in [BW82] and finally [Pre86], where maps similar to exponentials of derivations are used to produce a new torus from a given one. The very fact that the map need not be an automorphism allows the new torus to have rather different properties than the original one, which are more suited to classification purposes.

A crucial function of tori in modular Lie algebras is to produce gradings, as the corresponding eigenspace decompositions with respect to the adjoint action (a *(generalized) root space decomposition*). One naturally wonders whether some kind of exponential could be used to pass from a grading to another without reference to the grading arising as the root space decomposition with respect to some torus. Besides effectively extending the applicability of the technique from the realm of Lie algebras to the wider one of non-associative algebras, such *grading switching* does have applications within Lie algebra theory, where not all gradings of interest are directly related to tori. A special instance of such grading switching was described in [Mat05], in terms of *Artin-Hasse exponentials.* The strong limitation of [Mat05] was that the derivation D had to be nilpotent, but that special version was already sufficient for an application to certain Lie algebra gradings in [AM05].

The main goal of the present work is to describe how grading switching, in the spirit of [Mat05], can be done in full generality, for arbitrary derivations of non-associative algebras (with respect to compatible gradings). We will show how this extends the classical toral switching in a natural way. The role of the exponential series is taken by certain (generalized) *Laguerre polynomials*, which suggest the title of this paper.

We only sketch the essence of our main result in this introduction and refer the reader to Section 5 for a precise formulation. Let $A = \bigoplus A_k$ be a non-associative algebra over a field $\mathbb{F}$ of prime characteristic p, graded over the integers modulo m, and let D be a graded derivation of A, whose degree d satisfies $m \mid pd$. Assume $\mathbb{F}$ algebraically closed and A finite-dimensional for simplicity, but much weaker assumptions are sufficient and will be specified later. Then we construct a linear map $\mathcal{L}_D : A \to A$ such that $A = \bigoplus_k \mathcal{L}_D(A_k)$ is a new grading over the integers modulo m. In the special case where D is nilpotent the map $\mathcal{L}_D$ coincides with $E_p(D)$, which denotes the Artin-Hasse exponential series evaluated on D and was investigated in [Mat05].

In Section 4 we prove a special case of our result, where the main argument is stripped of the distraction of some additional technicalities of the general case.

Both the special case and the general case depend on a congruence for certain Laguerre polynomials, which we prove in Section 3 and which might well be of interest outside the area of non-associative algebras. It is a polynomial congruence analogue of the functional equation $\exp(X)\exp(Y) = \exp(X+Y)$ for the classical exponential.

Section 2 contains a review of definitions and known properties of Laguerre polynomials, and also a modular property which might be new.

In the concluding Section 6 we explain how our main result specializes to the setting of toral switching in finite-dimensional modular Lie algebras.

Our preprint [AM] contains a result on certain modular Lie algebras whose proof depends on a grading switching as described here.

2. Laguerre polynomials and some of their properties

The classical (generalized) Laguerre polynomial of degree $n \geq 0$ is defined as

$$L_n^{(\alpha)}(X) = \sum_{k=0}^{n} \binom{\alpha+n}{n-k} \frac{(-X)^k}{k!},$$

where α is a parameter, usually taken in the complex numbers. However, we may also view $L_n^{(\alpha)}(X)$ as a polynomial with rational coefficients in the two indeterminates α and X. It is well known and easy to check that the Laguerre polynomials satisfy the identities

$$L_n^{(\gamma)}(X) = L_n^{(\gamma+1)}(X) - L_{n-1}^{(\gamma+1)}(X), \tag{1}$$

$$nL_n^{(\gamma+1)}(X) = (n-X)L_{n-1}^{(\gamma+1)}(X) + (n+\gamma)L_{n-1}^{(\gamma)}(X). \tag{2}$$

The derivative of $L_n^{(\gamma)}(X)$ with respect to X equals $-L_{n-1}^{(\gamma+1)}(X)$, which according to Equation (1) can be written as

$$\frac{d}{dX}L_n^{(\gamma)}(X) = L_n^{(\gamma)}(X) - L_n^{(\gamma+1)}(X), \tag{3}$$

Now fix a prime p. We are essentially interested only in the polynomial $L_{p-1}^{(\alpha)}(X)$. The reason is that, viewed in characteristic p, it may be thought of as a generalization of the truncated exponential $E(X) = \sum_{k=0}^{p-1} X^k/k!$ which we mentioned in the introduction. In fact, we have $L_{p-1}^{(0)}(X) \equiv E(X) \pmod{p}$ because $\binom{p-1}{k} \equiv \binom{-1}{k} = (-1)^k$ for $k \geq 0$, and the full sense of this generalization should be conveyed by the congruence

$$L_{p-1}^{(\alpha)}(X) \equiv (1-\alpha^{p-1}) \sum_{k=0}^{p-1} \frac{X^k}{(\alpha+k)(\alpha+k-1)\cdots(\alpha+1)} \pmod{p}, \tag{4}$$

which holds because $(\alpha+p-1)\cdots(\alpha+1) \equiv \alpha^{p-1}-1 \pmod{p}$.

In this preparatory section we collect some properties of $L_{p-1}^{(\alpha)}(X) \pmod p$, starting with some easy ones. Equation (2) with $n = p$ yields

$$pL_p^{(\gamma+1)}(X) = (p - X)L_{p-1}^{(\gamma+1)}(X) + (p + \gamma)L_{p-1}^{(\gamma)}(X).$$

Because

$$pL_p^{(\gamma+1)}(X) = p\sum_{k=0}^{p} \binom{\gamma+1+p}{p-k} \frac{(-X)^k}{k!} \equiv X^p - (\gamma^p - \gamma) \pmod p,$$

we deduce the congruence

$$X^p - (\gamma^p - \gamma) \equiv -XL_{p-1}^{(\gamma+1)}(X) + \gamma L_{p-1}^{(\gamma)}(X) \pmod p. \tag{5}$$

Equation (5) allows one to give Equation (3) for the derivative of $L_{p-1}^{(\gamma)}(X)$ a variant in congruence form which we will use later, namely,

$$X \cdot \frac{d}{dX} L_{p-1}^{(\gamma)}(X) \equiv (X - \gamma) \cdot L_{p-1}^{(\gamma)}(X) + X^p - (\gamma^p - \gamma) \pmod p. \tag{6}$$

In the special case where $\gamma = 0$ this reads

$$XE'(X) \equiv XE(X) + X^p \pmod p \tag{7}$$

in terms of the truncated exponential $E(X)$. Because of this analogy with the defining differential equation $\exp'(X) = \exp(X)$ for the classical exponential, Equation (6) plays a key role in the proof of our Proposition 2, which, in turn, is crucial for our main result. Note in passing that further differentiation of Equation (7) leads to $XE''(X) + (1 - X)E'(X) - E(X) \equiv 0 \pmod p$. This is a special case modulo p of the second-order differential equation $XY'' + (\alpha + 1 - X)Y' + nY = 0$, which is often used to define the Laguerre polynomials $Y = L_n^{(\alpha)}(X)$.

Now we present a property of $L_{p-1}^{(\alpha)}(X) \pmod p$ which appears more hidden, and might well be of more general interest. To avoid constant use of the 'mod p' notation, in the remainder of the paper the Laguerre polynomial $L_{p-1}^{(\alpha)}(X)$ will always be viewed as having coefficients in $\mathbb{F}_p$, the field with p elements. The polynomial $L_{p-1}^{(Z^p)}(Z^p - Z)$ will play a special role in the sequel. Equation (4) shows at once that it vanishes on $\mathbb{F}_p^*$, but what we will actually need later is that it has no further roots in the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. This is a consequence of the following result.

Lemma 1. *We have* $L_{p-1}^{(Z^p)}(Z^p - Z) = \prod_{i=1}^{p-1}(1 + Z/i)^i$ *in* $\mathbb{F}_p[Z]$.

This can also be stated in the equivalent form

$$L_{p-1}^{(Z^p)}(Z^p - Z) = (-1)^{p(p-1)/2} \prod_{j=1}^{p-1} \binom{Z-1}{j}$$

in $\mathbb{F}_p[Z]$. In fact, the right-hand sides of the two equations are polynomials with the same roots in $\overline{\mathbb{F}}_p$, with corresponding multiplicities, and the same constant term 1 because $\prod_{j=1}^{p-1}\binom{-1}{j} = \prod_{j=1}^{p-1}(-1)^j = (-1)^{p(p-1)/2}$. A non-trivial consequence of Lemma 1 is the fact that $L_{p-1}^{(Z^p)}(Z^p - Z)$ has degree $p(p-1)/2$. Another noteworthy consequence is the identity

$$L_{p-1}^{(Z^p)}(Z^p - Z) \cdot L_{p-1}^{(-Z^p)}(-Z^p + Z) = 1 - Z^{p(p-1)}.$$

in $\mathbb{F}_p[Z]$, to be compared with the familiar $\exp(X)\exp(-X) = 1$, after noting that $L_{p-1}^{(Z^p)}(Z^p - Z) \equiv L_{p-1}^{(0)}(-Z) = E(-Z) \pmod{Z^p}$.

Proof of Lemma 1. Equation (5) yields

$$(Z^p - Z) \cdot L_{p-1}^{(Z^p+1)}(Z^p - Z) = Z^p \cdot L_{p-1}^{(Z^p)}(Z^p - Z) \tag{8}$$

in $\mathbb{F}_p[Z]$. Note that $L_{p-1}^{(0)}(0) = 1$ and write $L_{p-1}^{(Z^p)}(Z^p - Z) = \prod_{i=1}^{s}(1 - Z/\alpha_i)$ in $\overline{\mathbb{F}}_p[Z]$. Then Equation (8) says that

$$\prod_{j=1}^{p-1}(Z - j) \cdot \prod_{i=1}^{s}\bigl(Z - (\alpha_i - 1)\bigr) = Z^{p-1} \cdot \prod_{i=1}^{s}(Z - \alpha_i).$$

We infer that if some $\alpha \in \overline{\mathbb{F}}_p$ is a root of $L_{p-1}^{(Z^p)}(Z^p - Z)$ with multiplicity m, where we allow m to be zero, then $\alpha + 1$ is a root with multiplicity $m + p - 1$ if $\alpha = 0$, $m - 1$ if $\alpha \in \mathbb{F}_p^*$, and m otherwise. In particular, because 0 is not a root, each element of $\mathbb{F}_p$ is a root of $L_{p-1}^{(Z^p)}(Z^p - Z)$ with the multiplicity claimed in Lemma 1.

Because $L_{p-1}^{(Z^p)}(Z^p - Z)$ has constant term 1, in order to conclude the proof it remains to show that it has no further roots in $\overline{\mathbb{F}}_p$. To prove the latter it suffices to show that the polynomial has degree at most $p(p-1)/2$. Note that direct expansion only shows us that it has degree at most $p(p-1)$, which is twice as high as our goal. One way to proceed is noting that according to Equation (8) the product

$$Z^p \cdot L_{p-1}^{(Z^p)}(Z^p - Z) \cdot L_{p-1}^{(-Z^p)}(-Z^p + Z) \tag{9}$$

is invariant under the substitution $Z \mapsto Z + 1$, and hence can be expressed as a polynomial in $Z^p - Z$. However, because its derivative is zero, as we prove in the next paragraph, it can also be expressed as a polynomial in Z^p. These conditions together imply that it can be expressed as a polynomial in $Z^{p^2} - Z^p$. Because we know that its degree cannot exceed $2p^2 - p$ we infer that it cannot exceed p^2, whence $L_{p-1}^{(Z^p)}(Z^p - Z)$ has degree at most $p(p-1)/2$, as desired.

Now we prove our claim about the polynomial of Equation (9) having zero derivative. According to Equation (3) we have

$$\frac{d}{dZ} L_{p-1}^{(Z^p)}(Z^p - Z) = -L_{p-1}^{(Z^p)}(Z^p - Z) + L_{p-1}^{(Z^p+1)}(Z^p - Z),$$

and hence the derivative of that polynomial equals the product of Z^p and

$$\begin{aligned}
&\frac{d}{dZ}\bigl(L_{p-1}^{(Z^p)}(Z^p-Z)\cdot L_{p-1}^{(-Z^p)}(-Z^p+Z)\bigr)\\
&\quad = L_{p-1}^{(Z^p+1)}(Z^p-Z)\cdot L_{p-1}^{(-Z^p)}(-Z^p+Z) - L_{p-1}^{(Z^p)}(Z^p-Z)\cdot L_{p-1}^{(-Z^p+1)}(-Z^p+Z)\\
&\quad = \left(\frac{Z^p}{Z^p-Z}-\frac{(-Z)^p}{(-Z)^p-(-Z)}\right)\cdot L_{p-1}^{(Z^p)}(Z^p-Z)\cdot L_{p-1}^{(-Z^p)}(-Z^p+Z)=0,
\end{aligned}$$

where in the last step we have used Equation (8) twice, with $-Z$ in place of Z in the latter case. □

3. An exponential-like property of $L_{p-1}^{(\alpha)}(X)$

In this section we use the differential equation modulo p for $L_{p-1}^{(\alpha)}(X)$ which we stated in Equation (6) to prove a congruence similar to the functional equation $\exp(X)\exp(Y)=\exp(X+Y)$ satisfied by the classical exponential.

Proposition 2. *Consider the subring $R=\mathbb{F}_p\bigl[\alpha,\beta,\bigl((\alpha+\beta)^{p-1}-1\bigr)^{-1}\bigr]$ of the ring $\mathbb{F}_p(\alpha,\beta)$ of rational expressions in the indeterminates α and β, and let X and Y be further indeterminates. There exist rational expressions $c_i(\alpha,\beta)\in R$, such that*

$$L_{p-1}^{(\alpha)}(X)L_{p-1}^{(\beta)}(Y)\equiv L_{p-1}^{(\alpha+\beta)}(X+Y)\Bigl(c_0(\alpha,\beta)+\sum_{i=1}^{p-1}c_i(\alpha,\beta)X^iY^{p-i}\Bigr)$$

in $R[X,Y]$, modulo the ideal generated by $X^p-(\alpha^p-\alpha)$ and $Y^p-(\beta^p-\beta)$.

The crucial point for our applications of Proposition 2 is that the polynomial $c_0(\alpha,\beta)+\sum_{i=1}^{p-1}c_i(\alpha,\beta)X^iY^{p-i}$ has only terms of total degree a multiple of p. A simplified but weaker form of Proposition 2 is that the stated congruence holds in $\mathbb{F}_p(\alpha,\beta)[X,Y]$, modulo the ideal generated by the stated elements. This weaker statement would suffice for the proof of Theorem 3, but not for that of Theorem 4.

Proof. Let $\mathcal{I}$ denote the ideal of the polynomial ring $R[X,Y]$ generated by $X^p-(\alpha^p-\alpha)$ and $Y^p-(\beta^p-\beta)$. According to Lemma 1 we have

$$\begin{aligned}
\bigl(L_{p-1}^{(\alpha+\beta)}(X+Y)\bigr)^p &= L_{p-1}^{((\alpha+\beta)^p)}((X+Y)^p)\\
&\equiv L_{p-1}^{((\alpha+\beta)^p)}((\alpha+\beta)^p-(\alpha+\beta)) \pmod{\mathcal{I}}\\
&= \prod_{i=1}^{p-1}\Bigl(1+\frac{\alpha+\beta}{i}\Bigr)^i,
\end{aligned}\tag{10}$$

a non-zero element of R. In particular, the image of $L_{p-1}^{(\alpha+\beta)}(X+Y)$ in the quotient ring $R[X,Y]/\mathcal{I}$ is invertible. Reading congruences as equalities in the corresponding quotient ring, we have

$$\frac{L_{p-1}^{(\alpha)}(X)L_{p-1}^{(\beta)}(Y)}{L_{p-1}^{(\alpha+\beta)}(X+Y)} \equiv \sum_{i,j=0}^{p-1} c'_{ij}(\alpha,\beta)X^iY^j \pmod{\mathcal{I}}, \tag{11}$$

for certain (uniquely determined) $c'_{ij}(\alpha,\beta) \in R$. Our goal is proving that $c'_{ij}(\alpha,\beta)$ vanishes when p does not divide $i+j$.

Following [Mat06] we introduce a further indeterminate T and consider the polynomial ring $R[X,Y,T]$ and its ideal $\mathcal{I}_T$ generated by $(TX)^p-(\alpha^p-\alpha)$ and $(TY)^p-(\beta^p-\beta)$. The epimorphism $R[X,Y,T]=R[X,Y][T]$ onto $R[X,Y]$ given by evaluation at $T=1$ maps $\mathcal{I}_T$ onto $\mathcal{I}$, and hence induces an epimorphism of $R[X,Y,T]/\mathcal{I}_T$ onto $R[X,Y]/\mathcal{I}$. Substituting TX for X and TY for Y in Equation (11) yields

$$\frac{L_{p-1}^{(\alpha)}(TX)L_{p-1}^{(\beta)}(TY)}{L_{p-1}^{(\alpha+\beta)}(TX+TY)} \equiv \sum_{i,j=0}^{p-1} c'_{ij}(\alpha,\beta)T^{i+j}X^iY^j \pmod{\mathcal{I}_T}.$$

Because the differential operator d/dT on $R[X,Y,T]$, with kernel $R[X,Y,T^p]$, maps the ideal $\mathcal{I}_T$ into itself, it induces a derivation of the quotient ring $R[X,Y,T]/\mathcal{I}_T$. Hence proving that $c'_{ij}(\alpha,\beta)$ vanishes when p does not divide $i+j$ is equivalent to proving that

$$\frac{d}{dT}\frac{L_{p-1}^{(\alpha)}(TX)L_{p-1}^{(\beta)}(TY)}{L_{p-1}^{(\alpha+\beta)}(TX+TY)} \equiv 0 \pmod{\mathcal{I}_T} \tag{12}$$

in $R[X,Y,T]$. After expanding via Leibniz's rule and evaluating at $T=1$ (which can be reversed by substituting TX for X and TY for Y) we see that Equation (12) is equivalent to

$$\begin{aligned} XL_{p-1}^{(\alpha)}(X)'\cdot L_{p-1}^{(\beta)}(Y) + L_{p-1}^{(\alpha)}(X)\cdot YL_{p-1}^{(\beta)}(Y)' \\ \equiv (X+Y)\frac{L_{p-1}^{(\alpha+\beta)}(X+Y)'}{L_{p-1}^{(\alpha+\beta)}(X+Y)}\cdot L_{p-1}^{(\alpha)}(X)\cdot L_{p-1}^{(\beta)}(Y) \pmod{\mathcal{I}} \end{aligned} \tag{13}$$

where we have used the shorthand $L_n^{(\gamma)}(Z)'=(d/dZ)L_n^{(\gamma)}(Z)$. According to Equation (6) we have

$$ZL_{p-1}^{(\gamma)}(Z)' = (Z-\gamma)L_{p-1}^{(\gamma)}(Z) + Z^p - (\gamma^p-\gamma).$$

Taking, in turn, $Z=X$, $Z=Y$, and $Z=X+Y$, shows that Equation (13) holds. In conclusion, we have proved that

$$\frac{L_{p-1}^{(\alpha)}(X)L_{p-1}^{(\beta)}(Y)}{L_{p-1}^{(\alpha+\beta)}(X+Y)} \equiv c_0(\alpha,\beta) + \sum_{i=1}^{p-1} c_i(\alpha,\beta)X^iY^{p-i} \pmod{\mathcal{I}} \tag{14}$$

with $c_0(\alpha,\beta) := c'_{0,0}(\alpha,\beta)$, and $c_i(\alpha,\beta) := c'_{i,p-i}(\alpha,\beta)$ for $0<i<p$. □

The specialization of Proposition 2 to $\alpha=\beta=0$, where $L_{p-1}^{(0)}(X)$ equals the *truncated exponential* $E(X)=\sum_{i=0}^{p-1}X^i/i!$, takes the more precise form

$$E(X)\cdot E(Y)\equiv E(X+Y)\Big(1+\sum_{i=1}^{p-1}(-1)^iX^iY^{p-i}/i\Big)$$

in $\mathbb{F}_p[X,Y]$, modulo the ideal generated by X^p and Y^p, see [Mat05, Lemma 2.1]. This can be viewed as a truncated version of a corresponding property of (the reduction modulo p of) the Artin-Hasse exponential series, which is defined as

$$E_p(X):=\exp\Big(\sum_{i=0}^{\infty}X^{p^i}/p^i\Big)=\prod_{i=0}^{\infty}\exp(X^{p^i}/p^i).$$

In fact, as shown in the proof of [Mat05, Theorem 2.2], we have

$$E_p(X)\cdot E_p(Y)=E_p(X+Y)\Big(1+\sum_{i,j=1}^{\infty}a_{ij}X^iY^j\Big)$$

in $\mathbb{F}_p[[X,Y]]$, for certain coefficients $a_{ij}\in\mathbb{F}_p$ which vanish unless $p\mid i+j$. It was proved in [Mat06] that this property essentially characterizes the reduction modulo p of the Artin-Hasse series, up to some natural variations.

4. A model special case

In order to avoid that too many technical details may obscure our main argument, we first present an application of Proposition 2 to a special situation, and postpone consideration of a more general setting to the next section.

Theorem 3. *Let $A=\bigoplus_k A_k$ be a non-associative algebra over the field $\mathbb{F}$ of characteristic $p>0$, graded over the integers modulo m. Suppose that A has a graded derivation D of degree d such that $D^{p^2}=D^p$, with $m\mid pd$. Suppose that $\mathbb{F}$ contains the field of p^p elements, and choose $\gamma\in\mathbb{F}$ with $\gamma^p-\gamma=1$. Let $A=\bigoplus_{a\in\mathbb{F}_p}A^{(a)}$ be the decomposition of A into a direct sum of generalized eigenspaces for D, and let $\mathcal{L}_D:A\to A$ be the linear map whose restriction to $A^{(a)}$coincides with $L_{p-1}^{(a\gamma)}(D)$. Then $A=\bigoplus_k\mathcal{L}_D(A_k)$ is also a grading of A over the integers modulo m.*

Proof. In this special case the eigenvalues of D^p are elements of the prime field $\mathbb{F}_p$, hence of the form $\alpha^p-\alpha$, with $\alpha=a\gamma$ for some $a\in\mathbb{F}_p$.

The linear map $\mathcal{L}_D$ is bijective. In fact, $(\mathcal{L}_D)^p$ acts on the eigenspace $A^{(a)}$ of D^p as multiplication by the scalar

$$\big(L_{p-1}^{(a\gamma)}(a)\big)^p=L_{p-1}^{((a\gamma)^p)}\big((a\gamma)^p-a\gamma\big),$$

which is non-zero according to Lemma 1. Hence we have the direct sum decomposition $A=\bigoplus_k\mathcal{L}_D(A_k)$.

In order to prove that this is a grading we need to prepare the ground for an application of Proposition 2, in a similar way as was done in the proof of [Mat05, Theorem 2.2] in case of the Artin-Hasse exponential. If $m : A \otimes A \to A$ denotes the map given by the multiplication in A, the fact that D is a derivation means that $D(m(x \otimes y)) = m(Dx \otimes y) + m(x \otimes Dy)$ for any $x, y \in A$. This property can be more concisely written as $D \circ m = m \circ (D \otimes \mathrm{id} + \mathrm{id} \otimes D)$, where $\mathrm{id} : A \to A$ is the identity map. In particular, we have $L_{p-1}^{(\theta)}(D) \circ m = m \circ L_{p-1}^{(\theta)}(D \otimes \mathrm{id} + \mathrm{id} \otimes D)$ for any $\theta \in \mathbb{F}$. The multiplication map m restricts to a map $A^{(a)} \otimes A^{(b)} \to A^{(a+b)}$, for any $a, b \in \mathbb{F}_p$, and all the components involved are invariant under D. Viewing the commuting linear operators $D \otimes \mathrm{id}$ and $\mathrm{id} \otimes D$ as restricted to $A^{(a)} \otimes A^{(b)}$, the congruence of Proposition 2 can be evaluated on $D \otimes \mathrm{id}$ and $\mathrm{id} \otimes D$ for X and Y, with $a\gamma$ and $b\gamma$ for α and β. This is because D^p acts as multiplication by $a^p = a = (a\gamma)^p - a\gamma$ on $A^{(a)}$, and similarly for $A^{(b)}$. Also note that the rational expressions $c_i(\alpha, \beta)$ can be evaluated on $a\gamma$ and $b\gamma$ because $(a+b)\gamma \notin \mathbb{F}_p^*$, which is equivalent to $\big((a+b)\gamma\big)^{p-1} \neq 1$. The result of this evaluation, followed by composition with the multiplication map m, is that the restriction of $m \circ \big(L_{p-1}^{(a\gamma)}(D) \otimes L_{p-1}^{(b\gamma)}(D)\big)$ to $A^{(a)} \otimes A^{(b)}$ coincides with the restriction of

$$L_{p-1}^{(a\gamma+b\gamma)}(D) \circ m \circ \Big(c_0(a\gamma, b\gamma) + \sum_{i=1}^{p-1} c_i(a\gamma, b\gamma)(D^i \otimes D^{p-i})\Big).$$

This means that

$$L_{p-1}^{(a\gamma)}(D)x \cdot L_{p-1}^{(b\gamma)}(D)y = L_{p-1}^{(a\gamma+b\gamma)}(D)\Big(c_0(a\gamma, b\gamma)xy + \sum_{i=1}^{p-1} c_i(a\gamma, b\gamma)D^i x \cdot D^{p-i} y\Big)$$

for $x \in A^{(a)}$ and $y \in A^{(b)}$, which we can also write as

$$\mathcal{L}_D(x) \cdot \mathcal{L}_D(y) = \mathcal{L}_D\Big(c_0(a\gamma, b\gamma)xy + \sum_{i=1}^{p-1} c_i(a\gamma, b\gamma)D^i x \cdot D^{p-i} y\Big). \tag{15}$$

Because D^p is a graded derivation of degree zero, it maps each component A_k of the grading into itself, and hence $A_k = \bigoplus_{a \in \mathbb{F}_p} A_k \cap A^{(a)}$. Because $m \mid pd$, the term $D^i x \cdot D^{p-i} y$ in Equation (15), for $x \in A_k \cap A^{(a)}$ and $y \in A_\ell \cap A^{(b)}$, belongs to $A_{k+\ell}$ as well as the term xy. Hence Equation (15) implies that $\mathcal{L}_D(x) \cdot \mathcal{L}_D(y) \in \mathcal{L}_D\big(A_{k+\ell} \cap A^{(a+b)}\big)$. In particular, we conclude that $\mathcal{L}_D(A_k) \cdot \mathcal{L}_D(A_\ell) \subseteq \mathcal{L}_D(A_{k+\ell})$, and so $A = \bigoplus_k \mathcal{L}_D(A_k)$ is a grading of A over the integers modulo m. □

5. The general case

In this section we prove our main result, which extends Theorem 3 to the general case where D is a derivation of a non-associative algebra A over a field $\mathbb{F}$ of characteristic p, which we assume as large as we need in this paragraph, under the sole assumption on D that D^{p^r} is semisimple with finitely many eigenvalues, for some r. In fact, in that case D satisfies an equation

$$D^{p^n}+a_{n-1}D^{p^{n-1}}+\cdots+a_rD^{p^r}=0, \tag{16}$$

with $a_r\neq 0$. It is then not hard to see, as in [Str04, Section 1.5], or see our Remark 6 below, that there is a p-polynomial $g(t)=\sum_{i=r}^{n-1}b_iT^{p^i}$ such that $g(D)^p-g(D)=D^{p^r}$.

Theorem 4. *Let $A=\bigoplus A_k$ be a non-associative algebra over the perfect field $\mathbb{F}$ of prime characteristic p, graded over the integers modulo m. Suppose that A has a graded derivation D of degree d with $m\mid pd$, such that D^{p^r} is diagonalizable over $\mathbb{F}$. Suppose that there exists a p-polynomial $g(T)\in\mathbb{F}[T]$ such that $g(D)^p-g(D)=D^{p^r}$. Set $h(T)=\sum_{i=1}^{r-1}T^{p^i}\in\mathbb{F}_p[T]$.*

Let $A=\bigoplus_{\rho\in\mathbb{F}}A^{(\rho)}$ be the decomposition of A into a direct sum of generalized eigenspaces for D (with $A^{(\rho)}$ corresponding to the eigenvalue ρ). Let $\mathcal{L}_D:A\to A$ be the linear map whose restriction to $A^{(\rho)}$ coincides with $L_{p-1}^{(g(\rho)-h(D))}(D)$. Then $A=\bigoplus_k\mathcal{L}_D(A_k)$ is also a grading of A over the integers modulo m.

Proof. We adapt the proof of Theorem 3 to the present more general setting. Note that $h(T^p-T)=h(T)^p-h(T)=T^{p^r}-T^p$, and that in the special case of Theorem 3 we had $h(T)=0$ and $g(T)=\gamma T^p$, where $\gamma^p-\gamma-1=0$.

The linear map $\mathcal{L}_D$ is bijective. In fact, because $g(\rho)^p-g(\rho)=\rho^{p^r}$ for any eigenvalue of D, on the generalized eigenspace $A^{(\rho)}$ of D the linear map $\bigl(g(\rho)-h(D)\bigr)^{p^r}=g(\rho)^{p^r}-h(D^{p^r})$ acts as multiplication by the scalar

$$g(\rho)^{p^r}-h(\rho^{p^r})=g(\rho)^{p^r}-h\bigl(g(\rho)^p-g(\rho)\bigr)=g(\rho)^p,$$

and hence $(\mathcal{L}_D)^{p^r}$ acts on $A^{(\rho)}$ as multiplication by the scalar

$$\bigl(L_{p-1}^{(g(\rho)-h(\rho))}(\rho)\bigr)^{p^r}=L_{p-1}^{(g(\rho)^{p^r}-h(\rho^{p^r}))}(\rho^{p^r})=L_{p-1}^{(g(\rho)^p)}\bigl(g(\rho)^p-g(\rho)\bigr),$$

which is non-zero according to Lemma 1. Hence we have the direct sum decomposition $A=\bigoplus_k\mathcal{L}_D(A_k)$.

As in the proof of Theorem 3 we consider the multiplication map $m:A\otimes A\to A$, and note that because D is a derivation, and hence $D\circ m=m\circ(D\otimes\mathrm{id}+\mathrm{id}\otimes D)$, we have

$$L_{p-1}^{(\theta(D))}(D)\circ m=m\circ L_{p-1}^{(\theta(D\otimes\mathrm{id}+\mathrm{id}\otimes D))}(D\otimes\mathrm{id}+\mathrm{id}\otimes D)$$

for any polynomial $\theta(t)\in\mathbb{F}[t]$. Fix eigenvalues $\rho,\sigma\in\mathbb{F}$ for D, view m as restricted to a map $A^{(\rho)}\otimes A^{(\sigma)}\to A^{(\rho+\sigma)}$, and view the commuting linear operators $D\otimes\mathrm{id}$ and $\mathrm{id}\otimes D$ as restricted to $A^{(\rho)}\otimes A^{(\sigma)}$.

We intend to evaluate the congruence of Proposition 2 on $D\otimes\mathrm{id}$ and $\mathrm{id}\otimes D$ for X and Y, with $g(\rho)-h(D\otimes\mathrm{id})$ and $g(\sigma)-h(\mathrm{id}\otimes D)$ for α and β. To see that this makes sense we first need to check that the denominators of the rational expressions $c_i(\alpha,\beta)$ appearing in the congruence of Proposition 2 evaluate to invertible linear maps on $A^{(\rho)}\otimes A^{(\sigma)}$. In fact, α^{p^r} evaluates to $\big(g(\rho)-h(D)\big)^{p^r}\otimes\mathrm{id}$, which, from what we saw earlier in the proof, acts on $A^{(\rho)}\otimes A^{(\sigma)}$ as scalar multiplication by $g(\rho)^p$. Together with the analogous fact about β^{p^r}, this shows that both $(\alpha+\beta)^{p^r}$ and $\big((\alpha+\beta)^p-(\alpha+\beta)\big)^{p^r}=\big((\alpha+\beta)^{p-1}-1\big)^{p^r}(\alpha+\beta)^{p^r}$ evaluate to linear maps acting scalarly on $A^{(\rho)}\otimes A^{(\sigma)}$, by the scalars $g(\rho)^p+g(\sigma)^p$ and $\big(g(\rho)+g(\sigma)\big)^{p^2}-\big(g(\rho)+g(\sigma)\big)^p=(\rho+\sigma)^{p^{r+1}}$, respectively. Whether $\rho+\sigma$ vanishes or not, it follows that $(\alpha+\beta)^{p-1}-1$ evaluates to an invertible linear map on $A^{(\rho)}\otimes A^{(\sigma)}$, in the former case because $\alpha+\beta$ evaluates to a nilpotent map.

All this can be stated more formally by saying that evaluating both sides of the congruence of Proposition 2 amounts to apply a ring homomorphism from $\mathbb{F}_p\big[\alpha,\beta,\big((\alpha+\beta)^{p-1}-1\big)^{-1},X,Y\big]$ to $\mathbb{F}[D]$, the subring of the ring $\mathrm{End}_{\mathbb{F}}(A^{(\rho)}\otimes A^{(\sigma)})$ of linear endomorphisms generated by $\mathbb{F}$ and D. To ensure that such a homomorphism exists we have just checked that $(\alpha+\beta)^{p-1}-1$ is mapped to an invertible element of $\mathbb{F}[D]$. In conclusion, both sides of the congruence of Proposition 2 can be evaluated as described. However, to draw any conclusion from this evaluation we need to make sure that the ideal of the ring $\mathbb{F}_p\big[\alpha,\beta,\big((\alpha+\beta)^{p-1}-1\big)^{-1},X,Y\big]$ generated by $X^p-(\alpha^p-\alpha)$ and $Y^p-(\beta^p-\beta)$ evaluates to zero. This is so because both generators evaluate to zero. In fact, the former evaluates to

$$\begin{aligned}(D\otimes\mathrm{id})^p&-\Big(\big(g(\rho)-h(D\otimes\mathrm{id})\big)^p-\big(g(\rho)-h(D\otimes\mathrm{id})\big)\Big)\\&=(D\otimes\mathrm{id})^{p^r}-\big(g(\rho)^p-g(\rho)\big)=\Big(D^{p^r}-\big(g(\rho)^p-g(\rho)\big)\Big)\otimes\mathrm{id},\end{aligned}$$

which acts as zero on $A^{(\rho)}\otimes A^{(\sigma)}$.

The result of evaluating the congruence of Proposition 2 as described, followed by composition with the multiplication map m, is that the restriction of

$$m\circ L_{p-1}^{(g(\rho)-h(D\otimes\mathrm{id}))}(D\otimes\mathrm{id})\circ L_{p-1}^{(g(\sigma)-h(\mathrm{id}\otimes D))}(\mathrm{id}\otimes D)=m\circ\big(\mathcal{L}_D\otimes\mathcal{L}_D\big)$$

to $A^{(\rho)}\otimes A^{(\sigma)}$ coincides with the restriction of

$$L_{p-1}^{(g(\rho)+g(\sigma)-h(D))}(D)\circ m\circ\left(c_0(\alpha_0,\beta_0)+\sum_{i=1}^{p-1}c_i(\alpha_0,\beta_0)(D^i\otimes D^{p-i})\right),$$

where we have set $\alpha_0=g(\rho)-h(D\otimes\mathrm{id})$ and $\beta_0=g(\sigma)-h(\mathrm{id}\otimes D)$ for the sake of readability. This means that

(17)
$$\begin{aligned}\mathcal{L}_D(x)\cdot\mathcal{L}_D(y)=\mathcal{L}_D\bigg(&c_0\big(g(\rho)-h(D),g(\sigma)-h(D)\big)xy\\&+\sum_{i=1}^{p-1}c_i\big(g(\rho)-h(D),g(\sigma)-h(D)\big)D^ix\cdot D^{p-i}y\bigg)\end{aligned}$$

for $x\in A^{(\rho)}$ and $y\in A^{(\sigma)}$.

Because D^p is a graded derivation of degree zero, it maps each component A_k of the grading into itself, and hence $A_k = \bigoplus_{\rho\in\mathbb{F}} A_k \cap A^{(\rho)}$. Because $m \mid pd$, the term $D^i x \cdot D^{p-i} y$ in Equation (17), for $x \in A_k \cap A^{(\rho)}$ and $y \in A_\ell \cap A^{(\sigma)}$, belongs to $A_{k+\ell}$ as well as the term xy. Furthermore, each of the linear maps $c_i\bigl(g(\rho) - h(D), g(\sigma) - h(D)\bigr)$ on the space $A^{(\rho+\sigma)}$, for $0 \le i < p$, can be written as a polynomial map in D^p, and hence sends $A_{k+\ell} \cap A^{(\rho+\sigma)}$ into itself, again because D^p is a derivation of degree zero. Hence Equation (17) tells us that $\mathcal{L}_D(x) \cdot \mathcal{L}_D(y) \in \mathcal{L}_D\bigl(A_{k+\ell} \cap A^{(\rho+\sigma)}\bigr)$. In particular, we conclude that $\mathcal{L}_D(A_k) \cdot \mathcal{L}_D(A_\ell) \subseteq \mathcal{L}_D(A_{k+\ell})$, and so $A = \bigoplus_k \mathcal{L}_D(A_k)$ is a grading of A over the integers modulo m. □

Remark 5. Restricted to the subalgebra $\ker(D^{p^r})$, where $\rho = 0$, the map $\mathcal{L}_D$ coincides with that obtained by applying a variation of the Artin-Hasse exponential, namely, the series $S(X)$ considered in [Mat05, Section 3], to which we refer the reader for details.

Remark 6. Following [Str04, Section 1.5] we sketch the construction of a p-polynomial $g(T) = \sum_{i=r}^{n-1} b_i T^{p^i}$ such that $g(D)^p - g(D) = D^{p^r}$. One way is to introduce a parameter λ and impose that $g(T)^p - g(T) - T^{p^r} = \lambda^p \sum_{i=r}^{n} a_i T^{p^i}$. Starting from $b_{n-1} = \lambda$, the equation recursively determines b_h in terms of λ as $b_h^p = b_{h+1} + \lambda^p a_{h+1}$, for $h = n-2, n-3, \dots, r$, and also forces $-1 - b_r = \lambda^p a_r$. Hence $b_h = -1 - \sum_{k=r}^{h} \lambda^{p^{h+1-r}} a_k^{p^{h-k}}$, for $h = r, \dots, n-1$, where λ is chosen among the roots of the polynomial $1 + T + \sum_{k=r}^{n-1} T^{p^{n-k}} a_k^{p^{n-1-k}}$.

6. Toral switching in restricted Lie algebras

In this final section we discuss the connection with the *toral switching* in modular Lie algebras. Roughly speaking, this technique replaces a torus T of a restricted Lie algebra L with another torus T_x which is more suitable for further study of L. In the simplest and original setting of [Win69] this amounts to applying to T the exponential of the inner derivation $\operatorname{ad} x$, for some root vector $x \in L$ with respect to T. Because $(\operatorname{ad} x)^2 T = 0$ the exponential of $\operatorname{ad} x$ can be taken to be $1 + \operatorname{ad} x$ for this purpose. This is reminiscent of, and certainly motivated by, the classical characteristic zero situation where $\exp(\operatorname{ad} x)$ for some root vector x is used to conjugate a Cartan subalgebra into another. However, in more general settings $(1 + \operatorname{ad} x)T$ fails to be a torus, and hence the construction of T_x is slightly more involved. This technique was originally introduced by Winter in [Win69] and later generalized by Block and Wilson in [BW82]. The most general version was finally produced by Premet in [Pre86]. An exposition of Premet's version can be found in [Str04, Section 1.5].

A crucial step in this process is to keep track of the root space decomposition with respect to the new torus, by constructing linear maps from the root spaces with respect to T onto the root spaces with respect to T_x. Following Strade's exposition in [Str04, Section 1.5] we briefly sketch the construction of the new torus T_x and of a linear map $E(x,\lambda)$ which connects the old and new root spaces. Our goal is to show that $E(x,\lambda)$ coincides with the map $\mathcal{L}_D$ of Theorem 4, where $D = \operatorname{ad} x$. This shows that the toral switching process, if we disregard the strictly Lie-theoretic aspects, can be viewed as a special instance of Theorem 4. We only include enough details and notation to make the specialization of our results to toral switching readable in conjunction with [Str04, Section 1.5], and refer to that source for more.

Let L be a finite-dimensional restricted Lie algebra, over a perfect field $\mathbb{F}$ of positive chacteristic p, with p-mapping $[p]$. Let r be the difference between $\dim(L)$ and the maximum dimension of a torus of L (but any larger integer would do). In particular, $x^{[p^r]}$ is semisimple for each $x \in L$. It is shown in [Str04, Section 1.5] how to associate to each element x of L a certain element $\xi(x,\lambda)$ of L, which also depends on a choice of a certain admissible scalar $\lambda \in \mathbb{F}$, itself depending on x. This is done in a systematic 'polynomial' way whose details we disregard here, except for pointing out that when $D = \operatorname{ad} x$ the map $\operatorname{ad} \xi(x,\lambda)$ plays the role of our $g(D)$ in the previous section. The crucial property of $\xi(x,\lambda)$ is that

$$\xi(x,\lambda)^{[p]} - \xi(x,\lambda) = x^{[p]^r}. \tag{18}$$

Set $q(x) = \sum_{t=1}^{r-1} x^{[p]^t}$. Strade then defines the map $E_{(x,\lambda)}$ as

$$E_{(x,\lambda)} = -\sum_{i=0}^{p-1}\biggl(\prod_{k=i+1}^{p-1} \bigl(\operatorname{ad}\xi(x,\lambda) - \operatorname{ad} q(x) + kId\bigr)\biggr)(\operatorname{ad} x)^i.$$

Now let T be a torus of L of maximal dimension, and let $L = \bigoplus_{\gamma\in\Gamma} L_\gamma$ be the corresponding root space decomposition (where $\Gamma = \Gamma(L,T)$ in [Str04]). Let $x \in L_\beta$ be a root vector (hence with $\beta \neq 0$) such that $x^{[p]^r} \in T$, whence each L_γ is an eigenspace for $\operatorname{ad} x^{[p]^r} = (\operatorname{ad} x)^{p^r}$. It is stated in [Str04, Theorem 1.5.1] that $T_x = \{t - \beta(t)(\sum_{k=0}^{r-1} x^{[p]^k}) : t \in T\}$ is also a torus of L, and that $L = \bigoplus_{\gamma\in\Gamma} E_{(x,\lambda)} L_\gamma$ is the corresponding root space decomposition. Note that $(1 + \operatorname{ad} x)t = t - \beta(t)x$ can be taken as an interpretation of $\exp(\operatorname{ad} x)t$ because $(\operatorname{ad} x)^2 t = 0$; however, the elements used to define T_x above are more complicated than that, in general.

We now show that the map $E_{(x,\lambda)}$ coincides with the map $\mathcal{L}_D$ of our Theorem 4. Setting $D = \operatorname{ad} x$ in the situation of [Str04, Theorem 1.5.1] we have that D^{p^r} is semisimple. The polynomial g of Section 5 was defined in such a way that $g(D) = \operatorname{ad}\xi(x,\lambda)$, and obviously $h(D) = \operatorname{ad} q(x)$. We know that $g(D)$ acts scalarly on any generalized eigenspace for D (which for $\operatorname{ad}\xi(x,\lambda)$ can be deduced from Equation (18)). Now any L_γ (a root space, or L_0) is contained in the generalized eigenspace for D with respect to the eigenvalue ρ, where $\rho \in \mathbb{F}$ is determined by $\gamma(x^{[p^r]}) = \rho^{p^r}$. Then the map

$E_{(x,\lambda)}$ acts on L_γ as

$$E_{(D,\lambda)} = -\sum_{i=0}^{p-1}\Bigl(\prod_{k=i+1}^{p-1}\bigl(g(\rho)-h(D)+k\,\mathrm{id}\bigr)\Bigr)D^i = L_{p-1}^{(g(\rho)-h(D))}(D),$$

and therefore coincides with our $\mathcal{L}_D$.

To conclude our comparison with toral switching we show that part of the information given in [Str04, Theorem 1.5.1], namely, that $\bigoplus_{\gamma\in\Gamma} E_{(x,\lambda)}L_\gamma$ is a grading of L (over $\langle\Gamma\rangle$, the additive group generated by Γ), is a consequence of our Theorem 4. Of course, a crucial part of the toral switching technique is that this grading is actually the root space decomposition of a new torus T_x, but this part loses meaning in our more general setting where A is an arbitrary non-associative algebra.

In loose terms, toral switching modifies the original grading (that is, root space decomposition) in only one direction and does not affect it in suitably complementary directions. Our formulation of Theorem 4 for a cyclic grading means that it focuses on the one 'direction' where the switching takes place, and so we need a little work to isolate that direction before Theorem 4 becomes applicable to the toral switching setting.

Because $\beta(t^{[p]}) = \beta(t)^p$ for $t\in T$ (see [Str04, Equation (1.3.2)]), the maximal subspace $T_0 := \ker(\beta) = \{t\in T : \beta(t)=0\}$ is a p-subalgebra of the torus T, and hence a torus itself. The restriction $\gamma\mapsto\gamma_{|T_0}$ to T_0 gives a surjective $\mathbb{F}$-linear map $T^*\to T_0^*$, with kernel spanned by β. Let Γ_0 be the image of Γ under this restriction map. Note that the subgroup $\langle\Gamma_0\rangle$ generated by Γ_0 has rank one less than the rank of $\langle\Gamma\rangle$. Choose a toral element $t_1\in T$ (hence $t_1^{[p]}=t_1$) with $\beta(t_1)=1$; this can be done because T is spanned by toral elements. We have a group isomorphism of $\langle\Gamma\rangle$ with the direct product $\mathbb{F}_p\times\langle\Gamma_0\rangle$, where to γ there corresponds the pair $\bigl(\gamma(t_1),\gamma_{|T_0}\bigr)$.

For $\gamma_0\in\Gamma_0$ the sum $L_{\gamma_0} := \bigoplus_{\gamma\in\Gamma\colon\,\gamma_{|T_0}=\gamma_0} L_\gamma$ is a root space for the torus T_0. Hence $L=\bigoplus_{\gamma_0\in\Gamma_0} L_{\gamma_0}$ is the root space decomposition of L with respect to T_0. Similarly, $L=\bigoplus_{k\in\mathbb{F}_p} L_k$, where $L_k := \bigoplus_{\gamma\in\Gamma\colon\,\gamma(t_1)=k} L_\gamma$, is the root space decomposition of L with respect to the torus spanned by t_1. The root space decomposition of L with respect to T can be viewed as a grading

$$L = \bigoplus_{(k,\gamma_0)\in\mathbb{F}_p\times\langle\Gamma_0\rangle} L_k\cap L_{\gamma_0}$$

over $\mathbb{F}_p\times\langle\Gamma_0\rangle$. Now our Theorem 4 applies, with $m=p$, to the grading $L=\bigoplus_{k\in\mathbb{F}_p} L_k$, and yields a grading $L=\bigoplus_{k\in\mathbb{F}_p}\mathcal{L}_D(L_k)$. (Following [Str04] one may show that this is the root space decomposition with respect to the torus spanned by $t_1-x-h(x)$, but we may ignore this fact here.)

Because $[T_0,x]=0$, the derivation $D=\operatorname{ad}x$ commutes with $\operatorname{ad}t$ for each $t\in T_0$. Consequently, each L_{γ_0} is invariant under the linear map $\mathcal{L}_D$, because the latter can be expressed as a polynomial in D on L_{γ_0}. Therefore, $\mathcal{L}_D(L_{\gamma_0})=L_{\gamma_0}$ for each $\gamma_0\in\Gamma_0$, being $\mathcal{L}_D$ bijective, and hence

$\mathcal{L}_D(L_k \cap L_{\gamma_0}) = \mathcal{L}_D(L_k) \cap L_{\gamma_0}$ for $(k, \gamma_0) \in \mathbb{F}_p \times \langle \Gamma_0 \rangle$. Because both of $L = \bigoplus_{k \in \mathbb{F}_p} \mathcal{L}_D(L_k)$ and $L = \bigoplus_{\gamma_0 \in \Gamma_0} L_{\gamma_0}$ are gradings (according to Theorem 4 in case of the former), the direct sum decomposition

$$L = \bigoplus_{(k,\gamma_0) \in \mathbb{F}_p \times \langle \Gamma_0 \rangle} \mathcal{L}_D(L_k \cap L_{\gamma_0}) = \bigoplus_{(k,\gamma_0) \in \mathbb{F}_p \times \langle \Gamma_0 \rangle} \mathcal{L}_D(L_k) \cap L_{\gamma_0}$$

is a grading as well. This is equivalent to saying that $\bigoplus_{\gamma \in \Gamma} \mathcal{L}_D(L_\gamma)$ is a grading of L, as we wanted to prove.

References

[AM] M. Avitabile and S. Mattarei, *Nottingham Lie algebras with diamonds of finite and infinite type*, preprint, arXiv:1211.4436.

[AM05] ———, *Thin Lie algebras with diamonds of finite and infinite type*, J. Algebra **293** (2005), no. 1, 34–64. MR 2173965 (2006f:17018)

[BW82] Richard E. Block and Robert Lee Wilson, *The simple Lie p-algebras of rank two*, Ann. of Math. (2) **115** (1982), no. 1, 93–168. MR 644017 (83j:17008)

[Mat05] S. Mattarei, *Artin-Hasse exponentials of derivations*, J. Algebra **294** (2005), no. 1, 1–18. MR 2171626

[Mat06] ———, *Exponential functions in prime characteristic*, Aequationes Math. **71** (2006), no. 3, 311–317. MR 2236408 (2007b:39056)

[Pre86] A. A. Premet, *Cartan subalgebras of Lie p-algebras*, Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), no. 4, 788–800, 878–879. MR 88d:17012

[Str04] Helmut Strade, *Simple Lie algebras over fields of positive characteristic. I, Structure theory*, de Gruyter Expositions in Mathematics, vol. 38, Walter de Gruyter & Co., Berlin, 2004. MR 2059133 (2005c:17025)

[Win69] David J. Winter, *On the toral structure of Lie p-algebras*, Acta Math. **123** (1969), 69–81. MR 0251095 (40 #4326)

E-mail address: marina.avitabile@unimib.it

Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano - Bicocca, via Cozzi 53, I-20125 Milano, Italy

E-mail address: mattarei@science.unitn.it

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38050 Povo (Trento), Italy