THE STRUCTURE OF LIE ALGEBRAS WITH A DERIVATION SATISFYING A POLYNOMIAL IDENTITY

DIETRICH BURDE AND WOLFGANG ALEXANDER MOENS

Abstract. We prove nilpotency results for Lie algebras over an arbitrary field admitting a derivation, which satisfies a given polynomial identity $r(t) = 0$. In the special case of the polynomial $r = t^n - 1$ we obtain a uniform bound on the nilpotency class of Lie algebras admitting a periodic derivation of order n. We even find an optimal bound on the nilpotency class in characteristic p if p does not divide a certain invariant ρ_n.

1. Introduction

Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over an arbitrary field K. A derivation D of $\mathfrak{g}$ is said to be *nonsingular* if it is bijective as a linear transformation. It is called *periodic of order* n, if $D^n = \mathrm{id}$ and $D^k \neq \mathrm{id}$ for all $0 < k < n$. The interest in nonsingular or periodic derivations comes in part from the coclass theory for groups and Lie algebras, with the proof of the coclass conjectures by Shalev. In many cases the existence of a nonsingular or periodic derivation has a strong impact on the structure of the Lie algebra. For example, by a result of Jacobson [4], a Lie algebra over a field of characteristic zero admitting a nonsingular derivation is *nilpotent*. Furthermore, by a result of Kostrikin and Kuznetsov [6], a Lie algebra over a field of characteristic zero admitting a periodic derivation of order n such that 6 does not divide n is *abelian*. In prime characteristic $p > 0$ however, the situation is more complicated. There exist even simple modular Lie algebras admitting a periodic derivation. Shalev asked in his Problem 1 in [13], which positive integers n arise as the order of a periodic derivation for a non-nilpotent Lie algebra in characteristic p. The set of such integers was denoted $\mathcal{N}_p$ by Mattarei, who showed in [10] that $\mathcal{N}_p$ coincides with the set of all positive integers n such that there exists an element $\alpha \in \overline{\mathbb{F}}_p$ with $(\alpha + \lambda)^n = 1$ for all $\lambda \in \mathbb{F}_p$. In [8, 9, 10] Mattarei has made a detailed study of the set $\mathcal{N}_p$, using interesting number theoretical methods. We refer to the introduction of [9] for a nice overview.

In this article we study not only Lie algebras admitting periodic derivations, but more generally Lie algebras over a field K admitting a derivation D, which satisfies an *arbitrary* polynomial identity $r(D) = 0$ given by a polynomial $r \in K[t]$. We obtain a general result on the nilpotency by applying recent work of [11] as follows, see Theorem 3.10 and Remark 3.11.

Theorem *Let K be a field of characteristic $p \geq 0$, $r \in K[t]$ be a polynomial of degree $n \geq 0$ and $X = \{\alpha \in \overline{K} \mid r(a) = 0\}$ be the set of roots in $\overline{K}$. If X is an arithmetically-free subset of $(\overline{K}, +)$, then every Lie algebra $\mathfrak{g}$ over K admitting a derivation D, which satisfies $r(D) = 0$, is nilpotent of class $c(\mathfrak{g}) \leq H(n)$. If X is not an arithmetically-free subset of $(\overline{K}, +)$, then there*

Date: April 19, 2022.

2000 *Mathematics Subject Classification.* Primary 17B40, 17B50.

Key words and phrases. Nonsingular Derivation, polynomial identity.

exists some non-nilpotent Lie algebra over $\overline{K}$ *of dimension* $n+1$ *admitting a derivation* D*, which satisfies* $r(D)=0$*.*

Here $H(n)$ is the generalized Higman map, see section 3. In characteristic zero the root set X is arithmetically-free if and only if $r(0)\neq 0$. In characteristic $p>0$ this is much harder to describe. But if we specify to the case $r=t^n-1\in\mathbb{F}_p[t]$, i.e., to periodic derivations of order dividing n, we can show that $X=X_{n,p}=\{\alpha\in\overline{\mathbb{F}}_p \mid \alpha^n=1\}$ is not an arithmetically-free subset of $(\overline{\mathbb{F}}_p,+)$ if and only if $n\in\mathcal{B}_p$, where

$$\mathcal{B}_p=\mathbb{N}\cdot\{\mathrm{per}(h(t^p-t)) \mid h\in\mathbb{F}_p[t] \text{ with } h(0)\neq 0, \deg(h)\geq 1\}.$$

Here $\mathrm{per}(r)$ denotes the *period* of $r\in\mathbb{F}_p[t]$, which is the minimal positive integer m such that r divides t^m-1 in $\mathbb{F}_p[t]$, if such an m exists. In fact, we prove the following result, see Proposition 3.18.

Proposition *Let* $n\in\mathbb{N}$ *and* p *be a prime number. If* $n\notin\mathcal{B}_p$*, then every Lie algebra* $\mathfrak{g}$ *over a field of characteristic* $p>0$ *admitting a periodic derivation of order* n *is nilpotent of class* $c(\mathfrak{g})\leq H(n)$*. If* $n\in\mathcal{B}_p$ *then there exists some non-nilpotent Lie algebra in characteristic* $p>0$ *admitting a periodic derivation of order* n*.*

In particular we see that the set $\mathcal{N}_p$ considered by Shalev and Mattarei coincides with our set $\mathcal{B}_p$. Any $h\in\mathbb{F}_p[t]$ with $h(0)\neq 0$ and $\deg(h)\geq 1$ will produce an element of $\mathcal{B}_p=\mathcal{N}_p$ by computing the period of $h(t^p-t)$. For example, looking at irreducible polynomials $h\in\mathbb{F}_2[t]$ of low degree we see that $3,7,31,73,85,127$ are the first few primitive elements of $\mathcal{N}_2$, see Example 3.16. However, most importantly we obtain a uniform upper bound $H(n)$ for the nilpotency class in case that $n\notin\mathcal{B}_p$. In addition, we can improve this bound significantly by excluding finitely many prime characteristics $p>0$. In Theorem 3.6 we show the following.

Theorem *Let* $\mathfrak{g}$ *be a Lie algebra over a field* K *of arbitrary characteristic* $p\geq 0$*. Suppose that* $\mathfrak{g}$ *admits a periodic derivation* D *of order* n *such that* p *does not divide* ρ_n*. Then* $\mathfrak{g}$ *is nilpotent of class* $c(\mathfrak{g})\leq 1$ *if* n *is not divisible by* 6 *and of class* $c(\mathfrak{g})\leq 2$ *if* $6\mid n$*.*

The invariant ρ_n is defined by the resultant of the polynomials t^n-1 and $(t+1)^n-1$ if n is not divisible by 6, and by the resultant of $\frac{t^n-1}{\Phi_3}$ and $\frac{(t+1)^n-1}{\Phi_3}$ if $6\mid n$, where Φ_3 is the third cyclotomic polynomial in $\mathbb{Z}[t]$. It is known that ρ_n in the first case is given by the Wendt determinant of a circulant matrix with first row the binomial coefficients. This was first studied by Wendt in [15] in connection with Fermat's last theorem. For our result, the prime divisors of ρ_n are of interest. We show some properties of ρ_n in section 2. In case of $p\mid\rho_n$ the conclusion of Theorem 3.6 may or may not hold. Moreover for many primes p dividing ρ_n the set $X_{n,p}$ is in fact still arithmetically-free, so that $\mathfrak{g}$ is nilpotent.

Finally, we consider a new integer valued invariant $\sigma(r)$ for $r\in\mathbb{Z}[t]$, which we study in section 2. For the specific example of $r=t^n-1$ this invariant is given by $\sigma(r)=(-\rho_n)^n$ if n is not divisible by 6, and by $\sigma(r)=\left(\frac{n^2\rho_n}{3}\right)^n$ if $6\mid n$.

2. Arithmetic Invariants

Let S be a commutative ring and $f,g\in S[t]$ be two polynomials. Denote by $R(f,g)$ the resultant of f and g over S, given by the determinant of the Sylvester matrix with columns

given by the coefficients of f and g, see for example [1, 14]. Recall that the resultant of two polynomials with coefficients in an integral domain is zero if and only if they have a common divisor of positive degree.

Lemma 2.1. *Let $n \geq 1$. The greatest common divisor of $f = t^n - 1, g = (t+1)^n - 1 \in \mathbb{Z}[t]$ is given by*

$$\gcd(f,g) = \begin{cases} 1 & \text{if } n \not\equiv 0 \bmod 6, \\ t^2 + t + 1 & \text{if } n \equiv 0 \bmod 6. \end{cases}$$

Here $\Phi_3 = t^2 + t + 1 \in \mathbb{Z}[t]$ is the third cyclotomic polynomial.

Proof. Let $h = \gcd(f,g)$. Since the discriminant of $t^n - 1$ is nonzero in characteristic zero, every irreducible factor of h has multiplicity one. For the first case let $n \not\equiv 0 \bmod 6$ and assume that $h \neq 1$. Then f and g have a common root γ, so that $\gamma^n = (\gamma+1)^n = 1$. By Lemma 2.2 of [3] with $\alpha = 1$ and $\beta = \gamma$ it follows that $\gamma = \omega$ is a primitive third root of unity, and hence $\gamma + 1$ is a primitive sixth root of unity. Because of $(\gamma+1)^n = 1$ we obtain $6 \mid n$, which is a contradiction. Hence $h = 1$ in this case.
In the second case we assume that $6 \mid n$. Let ω be a primitive third root of unity. Then ω is a root of $t^n - 1$ and of $(t+1)^n - 1$, since $1 + \omega$ is a primitive sixth root of unity. So we have $\Phi_3 \mid h$. By Lemma 2.2 of [3] every root of h is also a root of Φ_3. Since h has only simple roots it follows that $h = \Phi_3$. □

The following definition yields a nonzero integer, because the polynomials are coprime in each case by the above lemma.

Definition 2.2. For $n \geq 1$ define a nonzero integer ρ_n by

$$\rho_n = \begin{cases} R(t^n - 1, (t+1)^n - 1) & \text{if } n \not\equiv 0 \bmod 6, \\ R\left(\frac{t^n-1}{\Phi_3}, \frac{(t+1)^n-1}{\Phi_3}\right) & \text{if } n \equiv 0 \bmod 6. \end{cases}$$

The resultant of $t^n - 1$ and $(t+1)^n - 1$ has been studied among other things in number theory, see for example [7, 15].

Proposition 2.3. *For $n \not\equiv 0 \bmod 6$ the invariant ρ_n is given by the Wendt determinant $\det(C(n))$, where $C(n) \in M_n(\mathbb{Z})$ is the following circulant matrix:*

$$C(n) = \begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{n-1} \\ \binom{n}{n-1} & 1 & \binom{n}{1} & \cdots & \binom{n}{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \cdots & 1 \end{pmatrix}$$

We have $\det(C(n)) = 0$ if and only if $n \equiv 0 \bmod 6$.

Proof. The circulant matrix $C(n)$ with in its first row the binomial coefficients was introduced by E. Wendt in [15] in connection with Fermat's last theorem. Wendt showed that its determinant equals the resultant of the polynomials $t^n - 1$ and $(t+1)^n - 1$. E. Lehmer proved in [7] that $\det(C(n)) = 0$ if and only if $n \equiv 0 \bmod 6$. □

For $n \not\equiv 0 \bmod 6$ the above ρ_n coincides with the invariant Δ_n introduced by Kostrikin and Kuznetsov in [6]. The Wendt determinant is listed at OEIS (On-Line Encyclopedia of Integer Sequences), as sequence $A048954$. The first ten numbers and their prime factorization are given as follows.

n	ρ_n	prime factors
1	1	1
2	-3	-3
3	28	$2^2 \cdot 7$
4	-375	$-3 \cdot 5^3$
5	3751	$11^2 \cdot 31$
7	6835648	$2^6 \cdot 29^2 \cdot 127$
8	-1343091375	$-3^7 \cdot 5^3 \cdot 17^3$
9	364668913756	$2^2 \cdot 7 \cdot 19^4 \cdot 37^2 \cdot 73$
10	-210736858987743	$-3 \cdot 11^9 \cdot 31^3$
11	101832157445630503	$23^5 \cdot 67^2 \cdot 89 \cdot 199^2$

For the case $n \equiv 0 \bmod 6$ there is no sequence available. We list a few numbers with their prime decomposition, which we have computed using Definition 2.2.

n	ρ_n
6	$-2^2 \cdot 3 \cdot 7^3$
12	$-2^{10} \cdot 3 \cdot 5^3 \cdot 7^3 \cdot 13^9$
18	$-2^2 \cdot 3^{12} \cdot 7^3 \cdot 19^{15} \cdot 37^6 \cdot 73^3$
24	$-2^{30} \cdot 3^{31} \cdot 5^{21} \cdot 7^9 \cdot 13^9 \cdot 17^3 \cdot 73^6 \cdot 241^3$
30	$-2^{50} \cdot 3^1 \cdot 5^8 \cdot 7^3 \cdot 11^9 \cdot 31^{27} \cdot 61^{12} \cdot 151^3 \cdot 271^6 \cdot 331^3$
36	$-2^{10} \cdot 3^{12} \cdot 5^3 \cdot 7^3 \cdot 13^9 \cdot 17^6 \cdot 19^{15} \cdot 37^{33} \cdot 73^{15} \cdot 109^9 \cdot 181^6 \cdot 757^6$

The integers ρ_n satisfy the following divisibility property.

Lemma 2.4. *Let $m, n \geq 1$ with $m \mid n$. Then $\rho_m \mid \rho_n$ in $\mathbb{Z}$.*

Proof. The proof is a case-by-case verification. Suppose first that 6 does not divide n. Then 6 also does not divide m. We have $(t^m - 1) \mid (t^n - 1)$ in $\mathbb{Z}[t]$ because of $m \mid n$ in $\mathbb{Z}$. Then we obtain $((t+1)^m - 1) \mid ((t+1)^n - 1)$, and by the multiplicative property of resultants we have

$$\rho_m = R(t^m - 1, (t+1)^m - 1) \mid R(t^n - 1, (t+1)^n - 1) = \rho_n.$$

Now suppose that $6 \mid n$ and $6 \mid m$. Then $\frac{t^m-1}{\Phi_3} \mid \frac{t^n-1}{\Phi_3}$ and $\frac{(t+1)^m-1}{\Phi_3} \mid \frac{(t+1)^n-1}{\Phi_3}$ in $\mathbb{Z}[t]$, so that again $\rho_m \mid \rho_n$. For the last case assume that $6 \mid n$ but 6 does not divide m. Then Φ_3 does not divide $t^m - 1$ and not $(t+1)^m - 1$, but it does divide $t^n - 1$ and $(t+1)^n - 1$. So $t^m - 1$ divides $\frac{t^n-1}{\Phi_3}$ and $(t+1)^m - 1$ divides $\frac{(t+1)^n-1}{\Phi_3}$, so that $\rho_m \mid \rho_n$. □

We also need the following lemma.

Lemma 2.5. *Let K be a field of arbitrary characteristic $p \geq 0$. Suppose that $\alpha \in K$ is a common root of $t^n - 1$ and $(t+1)^n - 1$. If 6 does not divide n then $p \mid \rho_n$. If $6 \mid n$ then $p \mid \rho_n$ or $\Phi_3(\alpha) = 0$.*

Proof. Assume that 6 does not divide n. There exist $u, v \in \mathbb{Z}[t]$ such that

$$\rho_n = u \cdot (t^n - 1) + v \cdot ((t+1)^n - 1).$$

By evaluating in α we obtain $\rho_n \cdot \alpha = 0$ in K and hence $p \mid \rho_n$. Suppose now that $6 \mid n$. Then there exist $u, v \in \mathbb{Z}[t]$ such that $\rho_n \cdot \Phi_3 = u \cdot (t^n - 1) + v \cdot ((t+1)^n - 1)$ and evaluating in α yields $\rho_n \cdot \Phi_3(\alpha) = 0$ in K and therefore $p \mid \rho_n$ or $\varphi_3(\alpha) = 0$. □

The following integer valued invariant for polynomials has been defined in [12], Definition 1.3.3. We do not need it here in this paper, but it is an interesting invariant in this connection.

Definition 2.6. Let $r \in \mathbb{Z}[t]$ be a nonzero polynomial of degree d and leading coefficient $a \in \mathbb{Z}$. Define an invariant $\delta(r)$ by $\delta(r) = r$ for $d = 0$ and by

$$\delta(r) = a^{1+2d^2} \cdot (m-1)! \cdot \prod_{\substack{1 \le i,j \le \ell \\ i \ne j}} (\lambda_i - \lambda_j)^m$$

for $d \ge 1$, where $\lambda_1, \cdots, \lambda_\ell$ are the distinct roots of r in $\overline{\mathbb{Q}}$ with corresponding multiplicities $m_1, \ldots, m_\ell$ and $m := \max\{m_1, \ldots, m_\ell\}$.

Example 2.7. *Let $r = t^n - 1$. Then $\delta(r)$ coincides with the usual discriminant of r. We have*

$$\begin{aligned} \delta(r) &= \operatorname{disc}(t^n - 1) \\ &= \prod_{1 \le i < j \le n} (\zeta^i - \zeta^j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \cdot (-1)^{n-1} \cdot n^n, \end{aligned}$$

where ζ is a primitive n-th root of unity.

This also leads to define another integer valued invariant for polynomials here as follows.

Definition 2.8. Let $r \in \mathbb{Z}[t]$ be a nonzero polynomial of degree d and leading coefficient $a \in \mathbb{Z}$. Define an invariant $\sigma(r)$ by $\sigma(r) = 1$ for $d = 0$ and by

$$\begin{aligned} \sigma(r) &= a^{2d^3} \cdot \prod_{\substack{1 \le i,j \le \ell \\ r(\lambda_i + \lambda_j) \ne 0}} r(\lambda_i + \lambda_j) \\ &= a^{2d^3} \cdot \prod_{\substack{1 \le i,j,k \le \ell \\ r(\lambda_i + \lambda_j) \ne 0}} a \cdot (\lambda_i + \lambda_j - \lambda_k)^{m_k} \end{aligned}$$

for $d \ge 1$, where $\lambda_1, \cdots, \lambda_\ell$ are the distinct roots of r in $\overline{\mathbb{Q}}$ with corresponding multiplicities $m_1, \ldots, m_\ell$.

It is clear from the definition that $\sigma(r)$ is nonzero. Again it can be shown that $\sigma(r)$ is always an integer, see [12], but we only need this for the special case of $r = t^n - 1$. Here we show it in the following proposition.

Proposition 2.9. *Let $r = t^n - 1$. Then $\sigma(r)$ is an integer, which is given by*

$$\sigma(r) = \begin{cases} (-\rho_n)^n & \text{if } n \not\equiv 0 \bmod 6, \\ \left(\dfrac{n^2 \rho_n}{3}\right)^n & \text{if } n \equiv 0 \bmod 6. \end{cases}$$

Proof. Suppose first that 6 does not divide n. Then the sum of two n-th roots is never an n-th root. Thus we have

$$\begin{aligned}\sigma(r) &= \prod_{0\le i,j\le n-1} ((\zeta^i+\zeta^j)^n-1)\\ &= \prod_{0\le i,j\le n-1} ((\zeta^{i-j}+1)^n-1)\\ &= \prod_{0\le k\le n-1} ((\zeta^k+1)^n-1)^n\\ &= (R((t+1)^n-1,t^n-1))^n\\ &= (-\rho_n)^n.\end{aligned}$$

If $6 \mid n$ then the sum of two n-th roots is an n-th root if and only if the ratio is a primitive third root of unity. So we have

$$\begin{aligned}\sigma(r) &= \prod_{\substack{0\le k\le n-1\\ (\zeta^k+1)^n\neq 1}} ((\zeta^k+1)^n-1)^n\\ &= \prod_{\substack{0\le k\le n-1\\ \Phi_3(\zeta^k)\neq 0}} ((\zeta^k+1)^n-1)^n\\ &= \left(R\left((t+1)^n-1,\frac{t^n-1}{\Phi_3}\right)\right)^n\\ &= (-\rho_n)^n\cdot\left(R\left(\Phi_3,\frac{t^n-1}{\Phi_3}\right)\right)^n\\ &= (-\rho_n)^n\cdot\prod_{\substack{d\mid n\\ d\neq 3}} R(\Phi_3,\Phi_d)^n.\end{aligned}$$

Now in [1] it is shown that for integers $n\ge m\ge 1$ we have

$$R(\Phi_m,\Phi_n)=\begin{cases}p^{\varphi(m)} & \text{if } \frac{n}{m} \text{ is a power of a prime } p,\\ 1 & \text{otherwise.}\end{cases}$$

It is easy to see that this implies that

$$\prod_{\substack{d\mid n\\ d\neq 3}} R(\Phi_3,\Phi_d)=-\frac{n^2}{3}\in\mathbb{Z}.$$

□

3. Lie algebra derivations satisfying a polynomial identity

Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over an arbitrary field K of characteristic $p\ge 0$. Denote by $c(\mathfrak{g})$ its nilpotency class and by $\mathrm{Der}(\mathfrak{g})$ its derivation algebra.

Definition 3.1. Let $r\in K[t]$ be a polynomial. We say that a derivation $D\in\mathrm{Der}(\mathfrak{g})$ satisfies a *polynomial identity* given by r if $r(D)=0$.

An important example for such a polynomial identity is given by $r = t^n - 1$. Then D satisfies the polynomial identity given by r if and only if D is a periodic derivation with $D^n = \mathrm{id}$. Note that a periodic derivation is nonsingular. The existence of a nonsingular derivation already has a strong implication on the structure of the Lie algebra.

Let us first assume that K has characteristic zero. Jacobson showed in [4] the following result.

Theorem 3.2 (Jacobson)**.** *Let $\mathfrak{g}$ be a Lie algebra over a field of characteristic zero admitting a nonsingular derivation. Then $\mathfrak{g}$ is nilpotent.*

In case the derivation is even periodic, one can hope to find in addition an effective bound for the nilpotency class. Indeed, in Kostrikin and Kuznetsov [6] showed the following result.

Theorem 3.3. *Let $\mathfrak{g}$ be a Lie algebra over a field of characteristic zero admitting a periodic derivation of order n such that n is not divisible by 6. Then $\mathfrak{g}$ is abelian.*

There is no conclusion here for the case that $6 \mid n$. To fill the gap, we proved in [3] the following result over $\mathbb{C}$.

Proposition 3.4. *Let $\mathfrak{g}$ be a complex Lie algebra admitting a periodic derivation. Then $\mathfrak{g}$ is nilpotent of class $c(\mathfrak{g}) \leq 2$.*

In characteristic $p > 0$ the situation is much more complicated. Jacobson's result is no longer true and even simple modular Lie algebras may admit a periodic derivation for any prime characteristic. We summarize the following classification result by Benkart, Kostrikin and Kuznetsov [2, 5].

Theorem 3.5. *Let $\mathfrak{g}$ be a simple modular Lie algebra over an algebraically closed field of characteristic $p > 7$. Then the following statements are equivalent.*

1. *$\mathfrak{g}$ admits a periodic derivation.*
2. *$\mathfrak{g}$ admits a nonsingular derivation.*
3. *$\mathfrak{g}$ is either a special Lie algebra $S(m; \mathbf{n}, \omega_2)$, or a Hamiltonian Lie algebra $H(m; \mathbf{n}, \omega_2)$ as specified in* [2].

So we cannot conclude in general that a Lie algebra admitting a periodic derivation is nilpotent. On the other hand we might be able to enforce nilpotency by adding further assumptions. Indeed, Kostrikin and Kuznetsov [6] showed that a modular Lie algebra of characteristic $p > 0$ admitting a periodic derivation of order n must be abelian provided that $6 \nmid n$ and that p does not divide ρ_n. We generalize this result for Lie algebras in arbitrary characteristic, including the case $6 \mid n$.

Theorem 3.6. *Let $\mathfrak{g}$ be a Lie algebra over a field K of arbitrary characteristic $p \geq 0$. Suppose that $\mathfrak{g}$ admits a periodic derivation D of order n such that p does not divide ρ_n. Then $\mathfrak{g}$ is nilpotent of class*

$$c(\mathfrak{g}) \leq \begin{cases} 1 & \text{if } n \not\equiv 0 \bmod 6, \\ 2 & \text{if } n \equiv 0 \bmod 6, \end{cases}$$

Proof. We may assume that K is algebraically closed since the nilpotency class is preserved under extensions of scalars. Furthermore there exists a semisimple derivation M. For $p = 0$ we may take $M = D$. If $p > 0$ then there exists an integer $k \geq 0$ such that $p^k \mid n$ and $\gcd(p, m) = 1$ with $m = \frac{n}{p^k}$. Let $M := D^{p^k}$. Then M is a periodic derivation of order m dividing n. Since the

order m of M is coprime to p, the derivation M is semisimple. Since K is algebraically closed we can find an eigenbasis for $\mathfrak{g}$ with respect to M. Note that all eigenvalues λ satisfy $\lambda^m = 1$.

Case 1: $6 \nmid m$. Assume that $\mathfrak{g}$ is not abelian. Then there exists eigenvectors $x, y \in \mathfrak{g}$ with respective eigenvalues α, β such that $[x, y] \neq 0$. It is easy to verify that $[x, y]$ is an eigenvector with eigenvalue $\alpha + \beta$. Hence we have $\alpha^m = \beta^m = (\alpha + \beta)^m = 1$, so that the ratio $\frac{\alpha}{\beta}$ is a common root of the polynomials $t^m - 1$ and $(t + 1)^m - 1$. By Lemma 2.5 we have $p \mid \rho_m$ and by Lemma 2.4 we obtain $p \mid \rho_m \mid \rho_n$ since $m \mid n$. This contradicts the assumption. Hence $\mathfrak{g}$ is abelian.

Case 2: $6 \mid m$. Then $\rho_2 = 3$ and $\rho_3 = 2^2 \cdot 7$ divide ρ_m by Lemma 2.5, so that $6 \mid \rho_m$. Hence $p > 3$ by our assumptions. Assume that $[[\mathfrak{g}, \mathfrak{g}], \mathfrak{g}] \neq 0$. Then there exist eigenvectors x, y, z with respective eigenvalues α, β, γ such that $[[x, y], z] \neq 0$. We note that $[x, y]$ and $[[x, y], z]$ are also eigenvectors with respective eigenvalues $\alpha + \beta$ and $\alpha + \beta + \gamma$. By using the Jacobi identity we may further assume that $[z, x]$ is an eigenvector with corresponding eigenvalues $\alpha + \gamma$. But then the ratios $\frac{\alpha}{\beta}$, $\frac{\alpha}{\gamma}$ and $\frac{\alpha+\beta}{\gamma}$ are all common roots of the polynomials $t^m - 1$ and $(t + 1)^m - 1$. By 2.5 these ratios are roots of the polynomial Φ_3, so that they have order 1 or 3. Since $p > 3$, the order is always equal to 3. Let $\omega \in K$ be an element of order 3. Then there exists $1 \leq i, j, k \leq 2$ such that $\beta = \alpha\omega^i$, $\gamma = \alpha\omega^j$ and $\alpha + \beta = \gamma\omega^k$. By substitution we obtain that $1 + \omega^i - \omega^{j+k} = 0$, so that ω is a common root of $1 + t + t^2$ and $1 + t^i - t^{j+k}$. This implies that the resultant is zero in K, so that p divides $R(t^2 + t + 1, t^i - t^{j+k} + 1)$, which is 1 for all i, j, k except for $(i, j, k) = (1, 1, 1), (2, 2, 2)$, where it is 4. It follows that $p = 2$, which is a contradiction. Hence $c(\mathfrak{g}) \leq 2$.

If $6 \nmid n$ then also $6 \nmid m$, so that we obtain the better bound $c(\mathfrak{g}) \leq 1$ by Case 1. □

Remark 3.7. For $p = 0$ the assumption that $p \nmid \rho_n$ in the theorem is always satisfied since ρ_n is nonzero. Hence the result generalizes Proposition 3.4 from complex numbers to an arbitrary field of characteristic zero. For $p > 0$ there is no conclusion from the theorem for $p \mid \rho_n$. There exist both nilpotent and non-nilpotent Lie algebras admitting a periodic derivation of order n with $p \mid \rho_n$ for some n and some p, see the two examples below.

Example 3.8. *Let $\mathfrak{g} = W(1; m)$ be the Zassenhaus Lie algebra of dimension $2^m - 1$ over $\mathbb{F}_2$ in characteristic $p = 2$. It admits a periodic derivation of order $n = 2^m - 1$, see* [2]. *For all $m \geq 2$ we have $2 \mid \rho_{2^m-1}$, so that there is no conclusion from Theorem* 3.6. *And in fact $\mathfrak{g}$ is simple and hence non-nilpotent.*

Example 3.9. *Let $\mathfrak{g}$ be the free-nilpotent Lie algebra over $\mathbb{F}_3$ with* 3 *generators of nilpotency class* 2. *It has a periodic derivation of order* 6. *Since $3 \mid \rho_6$ we cannot apply Theorem* 3.6, *but nevertheless the conclusion holds. Indeed, $\mathfrak{g}$ is* 2*-step nilpotent.*

We will now generalize Theorem 3.6 from periodic derivations to derivations satisfying an arbitrary polynomial identity. For this we use the methods and results from [11, 12]. Recall that a subset X of an additive group $(G, +)$ is called *arithmetically-free* if X does not contain any arithmetic progression of the form $\alpha, \alpha + \beta, \alpha + 2\beta, \ldots$, with $\alpha, \beta \in X$. Let $H \colon \mathbb{N} \to \mathbb{N}$ be the generalized Higman map, as defined in [11].

Theorem 3.10. *Let K be a field of characteristic $p \geq 0$, $r \in K[t]$ be a polynomial of degree $n \geq 0$ and $X = \{\alpha \in \overline{K} \mid r(a) = 0\}$ be the set of roots in $\overline{K}$. If X is an arithmetically-free*

subset of $(\overline{K},+)$, then every Lie algebra $\mathfrak{g}$ over K admitting a derivation D, which satisfies $r(D)=0$, is nilpotent of class $c(\mathfrak{g})\leq H(n)$.

Proof. Let $\mathfrak{h}=\overline{K}\otimes_K\mathfrak{g}$ and consider the derivation $M=\mathrm{id}\otimes D$ of $\mathfrak{h}$. Then $r(M)=0$ in $\overline{K}$ and the eigenspace decomposition of $\mathfrak{h}$ with respect to M is a grading by $(\overline{K},+)$, whose support is contained in X. So we can apply Theorem 3.14 of [11] to conclude that $\mathfrak{h}$, and hence $\mathfrak{g}$ is nilpotent of class $c(\mathfrak{g})\leq H(|X|)\leq H(n)$. □

Remark 3.11. If X is *not* an arithmetically-free subset of $(\overline{K},+)$ in the above theorem, then there exists some non-nilpotent Lie algebra over $\overline{K}$ of dimension $n+1$ admitting a derivation D, which satisfies $r(D)=0$. This follows immediately from Proposition 3.8 of [11]. Moreover we can construct then a filiform nilpotent Lie algebra of arbitrarily high class admitting a derivation D that satisfies $r(D)=0$, see Corollary 3.9 in [11].

How can we decide for a given polynomial $r\in K[t]$ whether or not X is arithmetically-free?

For $p=0$ the answer is easy. X is arithmetically-free if and only if $r(0)\neq 0$ in K. So we obtain the following corollary.

Corollary 3.12. *Let K be a field of characteristic zero, $r\in K[t]$ be a polynomial of degree $n\geq 0$ such that $r(0)\neq 0$. Then every Lie algebra $\mathfrak{g}$ over K admitting a derivation D, which satisfies $r(D)=0$, is nilpotent of class $c(\mathfrak{g})\leq H(n)$.*

Proof. Assume that $r(0)\neq 0$ and let $\alpha,\beta\in X$. Since the group $(\overline{K},+)$ is torsion-free, the arithmetic progression $\alpha,\alpha+1\cdot\beta,1+2\cdot\beta,\cdots$ contains infinitely many elements, so that it is not contained in the finite set X. Hence X is arithmetically-free. Conversely, let X be arithmetically-free and assume that $r(0)=0$. Then the arithmetic progression $0,0+1\cdot 0,0+2\cdot 0,\cdots$ is contained in X, so that X is not an arithmetically-free subset of $(\overline{K},+)$. This is a contraction, so that $r(0)\neq 0$. □

Remark 3.13. It is interesting to note that the corollary immediately implies Jacobson's result, Theorem 3.2. Indeed, let D be a nonsingular derivation. Then by Cayley-Hamilton the characteristic polynomial $r=\chi_D$ of D satisfies $r(D)=0$ with $r(0)\neq 0$ since $\det(D)\neq 0$. Hence the result follows.

How can we decide for given r whether or not X is arithmetically-free in characteristic $p>0$? This is much harder to answer for $p>0$ than for $p=0$. We will prove a result for $r=t^n-1\in\mathbb{F}_p[t]$.

Definition 3.14. Let $r\in K[t]$ be a polynomial. The *period of r* is the minimal positive integer $m=\mathrm{per}(r)$ such that r divides t^m-1 in $K[t]$, if such an m exists. For $K=\mathbb{F}_p$ we define sets $\mathcal{P}_p$ and $\mathcal{B}_p$ by

$$\mathcal{P}_p=\{\mathrm{per}(h(t^p-t))\mid h\in\mathbb{F}_p[t]\text{ with }h(0)\neq 0,\deg(h)\geq 1\},$$

$$\mathcal{B}_p=\mathbb{N}\cdot\mathcal{P}_p.$$

Note that a polynomial $r\in\mathbb{F}_p[t]$ has a period if and only if $r(0)\neq 0$.

Example 3.15. *We have $p^k-1\in\mathcal{P}_p$ for all primes p and for all $k\geq 2$.*

To see this, let

$$h=1+t^{p-1}+t^{p^2-1}+t^{p^3-1}+\cdots+t^{p^{k-1}-1}\in\mathbb{F}_p[t].$$

Using

$$(t^p - t)^{p^\ell - 1} = (t(t^{p-1} - 1))^{p^\ell - 1} = t^{p^\ell - 1} \cdot \frac{t^{p^\ell (p-1)} - 1}{t^{p-1} - 1}$$

we obtain

$$h(t^p - t) = 1 + t^{p-1} + t^{2(p-1)} + t^{3(p-1)} + \cdots + t^{p^k - p} = \frac{t^{p^k - 1} - 1}{t^{p-1} - 1}.$$

It is now easy to verify that $\mathrm{per}(h(t^p - t)) = p^k - 1$, which is contained in $\mathcal{P}_p$.

By computing the periods of $h(t^p - t)$ for a list of irreducible polynomials $h \in \mathbb{F}_p[t]$ of low degree we obtain several elements in $\mathcal{P}_p$.

Example 3.16. *We have* $3, 7, 31, 73, 85, 127 \in \mathcal{P}_2$.

This follows from the table below, for $p = 2$.

h	$\mathrm{per}(h(t^2 - t))$
$t + 1$	3
$t^3 + t + 1$	7
$t^4 + t^3 + t^2 + t + 1$	85
$t^5 + t^2 + 1$	31
$t^7 + t + 1$	127
$t^9 + t^4 + t^2 + t + 1$	73

We have the following result concerning the root set for $r = t^n - 1 \in \mathbb{F}_p[t]$. Note that this is implicitly stated in [9], section 4. We state it here in an explicit form including a proof for the convenience of the reader.

Proposition 3.17. *Let n be a positive integer and p be a prime. Then the following assertions are equivalent.*

(1) *The set $X_{n,p} = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^n = 1\}$ is an arithmetically-free subset of $(\overline{\mathbb{F}}_p, +)$.*
(2) *We have $h_{n,p} = \gcd(t^n - 1, (t+1)^n - 1, \ldots, (t+p-1)^n - 1) = 1$ in $\mathbb{F}_p[t]$.*
(3) *We have $n \notin \mathcal{B}_p$.*

Proof. (2) $\Longrightarrow$ (1) : Suppose that $X_{n,p}$ is not arithmetically-free. Then there exist $\alpha, \beta \in X_{n,p}$ such that $\alpha^n = (\alpha + \beta)^n = \cdots = (\alpha + (p-1)\beta)^n = 1$. For $\gamma := \frac{\alpha}{\beta}$ we have $\gamma^n = 1$ and $\gamma \in X_{n,p}$. But then also $\gamma^n = (\gamma + 1)^n = \cdots = (\alpha + (p-1))^n = 1$, so that γ is a common root of $t^n - 1, (t+1)^n - 1, \ldots, (t + (p-1))^n - 1$ and therefore of $h_{n,p}$. So $h_{n,p} \neq 1$, a contradiction. It follows that (1) holds.

(1) $\Longrightarrow$ (2) : Suppose that $h_{n,p} \neq 1$. Let γ be a root of it and let $\alpha = \beta = 1$. Then $\alpha, \alpha + \beta, \ldots, \alpha + (p-1)\beta \in X_{n,p}$. Hence $X_{n,p}$ is not arithmetically-free.

(2) $\Longrightarrow$ (3) : Suppose that $n \in \mathcal{B}_p$. Then we can choose an $h \in \mathbb{F}_p[t]$ with $h(0) \neq 0$ and $\deg(h) \geq 1$ such that $m = \mathrm{per}(h(t^p - t))$ divides n. Hence $h(t^p - t)$ divides $t^n - 1$. Using Fermat's little theorem we see that $h(t^p - t) = h((t + \ell)^p - (t + \ell))$, so that $h(t^p - t)$ divides $t^n - 1, (t+1)^n - 1, \ldots, t + p - 1)^n - 1$ and therefore also $h_{n,p}$. it follows that $h_{n,p} \neq 1$.

(3) $\Longrightarrow$ (2) : Suppose that $h_{n,p} \neq 1$. Define polynomials $H_i \in \mathbb{F}_p[t]$ by $H_0 = t^n - 1$ and

$$H_i = \gcd(H_{i-1}(t), H_{i-1}(t+1))$$

for $i \geq 1$. Then for all $k \in \mathbb{F}_p$ we have $H_i(t+k) = \gcd(H_{i-1}(t+k), H_{i-1}(t+k+1))$. Hence we have for all $i \geq 0$ that

$$\begin{aligned} h_{n,p} &= \gcd(H_i(t), H_i(t+1), \ldots, H_i(t+p-1)) \\ &= \gcd(H_{i+1}(t), H_{i+1}(t+1), \ldots, H_{i+1}(t+p-1)). \end{aligned}$$

Furthermore, $\deg(H_i) \geq \deg(H_{i+1})$ for all $i \geq 0$ so that there exists an $\ell \geq 1$ such that $\deg(H_\ell) = \deg(H_{\ell+1})$. Since $H_\ell(t)$ and $H_\ell(t+1)$ are monic polynomials of the same degree as their greatest common divisor, we conclude that $H_\ell(t) = H_{\ell+1}(t) = H_\ell(t+1)$ and therefore $H_\ell(t) = H_\ell(t+1) = \cdots = H_\ell(t+p-1)$, so that $h_{n,p}(t) = h_{n,p}(t+1) = \cdots = h_{n,p}(t+p-1)$. Thus $h_{n,p}$ is of the form $h(t^p - t)$ for some $h \in \mathbb{F}_p[t]$. Since $h_{n,p}$ divides $t^n - 1$, we have $h_{n,p}(0) \neq 0$ and therefore $h(0) \neq 0$. We have assumed that $h_{n,p} \neq 1$, so that h is non-constant. So $\mathrm{per}(h(t^p - t))$ divides n and $n \in \mathcal{B}_p$. □

Theorem 3.10, Remark 3.11 and Proposition 3.17 together yield the following result. Note that if $\mathfrak{g}$ admits a periodic derivation of order dividing n then $\mathfrak{g} \oplus K^n$ admits a periodic derivation of order exactly n.

Proposition 3.18. *Let $n \in \mathbb{N}$ and p be a prime number. If $n \notin \mathcal{B}_p$, then every Lie algebra $\mathfrak{g}$ over a field of characteristic $p > 0$ admitting a periodic derivation of order n is nilpotent of class $c(\mathfrak{g}) \leq H(n)$. If $n \in \mathcal{B}_p$ then there exists some non-nilpotent Lie algebra in characteristic $p > 0$ admitting a periodic derivation of order n.*

Remark 3.19. The proposition shows that our set $\mathcal{B}_p$ coincides with the set $\mathcal{N}_p$ introduced by Shalev [13] and studied further by Mattarei [8, 9, 10]. Shalev asked in his Problem 1 in [13] for the possible orders n of nonsingular derivations of non-nilpotent Lie algebras in characteristic $p > 0$. Mattarei denoted by $\mathcal{N}_p$ the set of such positive integers n and showed in [9], Theorem 2.1 that $\mathcal{N}_p$ can be described in purely arithmetic terms, namely by

$$\mathcal{N}_p = \{n \in \mathbb{N} \mid \text{ there exists an element } \alpha \in \overline{\mathbb{F}}_p \text{ such that } (\alpha + \lambda)^n = 1 \text{ for all } \lambda \in \mathbb{F}_p\}.$$

Shalev already had shown that the n arising as orders of periodic derivations of non-nilpotent Lie algebras in characteristic $p > 0$ belong to this set. Mattarei showed also the converse.

Proposition 3.18 allows us to obtain examples of n lying in $\mathcal{B}_p$. Any $h \in \mathbb{F}_p[t]$ with $h(0) \neq 0$ and $\deg(h) \geq 1$ will produce an element of $\mathcal{B}_p = \mathcal{N}_p$ by computing the period of $h(t^p - t)$. For example, we can show that $3, 7, 31, 73, 85, 127, \ldots$, are elements of $\mathcal{N}_2$, see Example 3.16. These calculations have also been done in section 3.3 of [10], where an efficicient algorithm is used to test whether or not a given $n \in \mathbb{N}$ belongs to $\mathcal{B}_p$.

Example 3.20. *Fix a positive integer $n \leq 12$. For such small n we can decide for which primes p we have $n \in \mathcal{B}_p$. In fact, $n \in \mathcal{B}_p \Longrightarrow p \mid \rho_n$ by Theorem* 3.16*, so that we only need to consider the prime divisors p of ρ_n from the tables in section* 2*. Using further results from* [13] *we see that*

$$n \in \mathcal{B}_p \Longleftrightarrow (n,p) \in \{(3,2), (6,2), (7,2), (8,3), (9,2), (12,2)\}.$$

Hence we know, for example, that every modular Lie algebra of any prime characteristic $p > 0$ admitting a periodic derivation of order $2, 4, 5, 10, 11$ is nilpotent. The "bad" primes for orders $n = 3, 6, 7, 8, 9, 12$ are $p = 2, 3$, where the Lie algebra over characteristic $p > 0$ admitting a derivation of order n need not be nilpotent.

For $p = 2$ we can even describe the set $\mathcal{B}_2$ totally in terms of ρ_n.

Example 3.21. *We have* $n \in \mathcal{B}_2 \iff 2 \mid \rho_n$. *In fact, much more is true. The simple Lie algebra* $W(1;2)$ *of dimension* 3 *in characteristic* 2 *admits a derivation* D *with* $D^n = \mathrm{id}$ *for all* n *with* $2 \mid \rho_n$.

Let (x_1, x_2, x_3) be a basis of $W(1;2)$ with $[x_1, x_2] = x_3$, $[x_1, x_3] = x_2$ and $[x_2, x_3] = x_1$. Assume that $2 \mid \rho_n$. Then there exists a $\lambda \in \overline{\mathbb{F}}_2$ such that $\lambda^n = (1+\lambda)^n = 1$. Define $D = \mathrm{diag}(1, \lambda, 1+\lambda)$. Then D is a derivation of $W(1;2)$ satisfying $D^n = \mathrm{id}$. Since $W(1;2)$ is not nilpotent, it follows that $n \in \mathcal{B}_2$. Conversely, $n \in \mathcal{B}_2$ implies $2 \mid \rho_n$ as above.

Remark 3.22. It would be also interesting to ask about the possible orders n of nonsingular derivations of *non-solvable* Lie algebras in characteristic $p > 0$. The set of such positive integers n would be contained in the set $\mathcal{B}_p$ and potentially be a proper subset.

Acknowledgments

Dietrich Burde is supported by the Austrian Science Foundation FWF, grant I3248 and P33811. Wolfgang A. Moens acknowledges support by the Austrian Science Foundation FWF, grant P30842.

References

[1] T. Apostol: *Resultants of cyclotomic polynomials.* Proc. Amer. Math. Soc. **24** (1970), 457–462.
[2] G. Benkart, A. I. Kostrikin, and M. I. Kuznetsov: *Finite-dimensional simple Lie algebras with a nonsingular derivation.* J. Algebra **171** (1995), no. 3, 894–916.
[3] D. Burde, W. A. Moens: *Periodic derivations and prederivations of Lie algebras.* Journal of Algebra, Vol. **357** (2012), 208–221.
[4] N. Jacobson: *A note on automorphisms and derivations of Lie algebras.* Proc. Amer. Math. Soc. **6** (1955), 281–283.
[5] A. I. Kostrikin, M. I. Kuznetsov: *Lie algebras with a nonsingular derivation.* Algebra and analysis (Kazan, 1994) (de Gruyter, Berlin, 1996) pp. 81–90.
[6] A. I. Kostrikin, M. I. Kuznetsov: *Two remarks on Lie algebras with a nonsingular derivation.* Proceedings of the Steklov Institute of Mathematics **208** (1995), 166-171.
[7] E. Lehmer: *On a resultant connected with Fermat's last theorem.* Bull. Amer. Math. Soc. **41** (1935), 864–867.
[8] S. Mattarei: *The orders of nonsingular derivations of modular Lie algebras.* Israel J. Math. **132** (2002), 265–275.
[9] S. Mattarei: *The orders of nonsingular derivations of Lie algebras of characteristic two.* Israel J. Math. **160** (2007), 23–40.
[10] S. Mattarei: *A sufficient condition for a number to be the order of a nonsingular derivation of a Lie algebra.* Israel J. Math. **171** (2009), 1–14.
[11] W. A. Moens: *Arithmetically-free group-gradings of Lie algebras: II.* Journal of Algebra, Vol. **492** (2017), 457–474.
[12] W. A. Moens: *The nilpotency of finite groups with a fixed-point-free automorphism satisfying an identity.* arXiv:1810.04965v4 (2020).
[13] A. Shalev: *The orders of nonsingular derivations.* J. Austral. Math. Soc. Ser. A **67** (1999), no. 2, 254–260.
[14] B. L. van der Waerden: *Modern Algebra.* Frederick Ungar Publishing Co., New York, N. Y., 1949. xii+264 pp.
[15] E. Wendt: *Arithmetische Studien über den "letzten" Fermatschen Satz, welcher aussagt, dass die Gleichung* $a^n + b^n = c^n$ *für* $n > 2$ *in ganzen Zahlen nicht auflösbar ist.* (German) J. Reine Angew. Math. **113** (1894), 335–347.

Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, 1090 Wien, Austria

Email address: dietrich.burde@univie.ac.at

Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, 1090 Wien, Austria

Email address: wolfgang.moens@univie.ac.at