J. Austral. Math. Soc. (*Series A*) **67** (1999), 254–260

THE ORDERS OF NONSINGULAR DERIVATIONS

ANER SHALEV

Dedicated to M. F. (Mike) Newman on the occasion of his 65th birthday

(Received 24 March 1999; revised 3 May 1999)

Communicated by E. A. O'Brien

Abstract

Nonsingular derivations of modular Lie algebras which have finite multiplicative order play a role in the coclass theory for pro-p groups and Lie algebras. We study the orders of nonsingular derivations of finite-dimensional non-nilpotent Lie algebras of characteristic $p > 0$. The methods are essentially number-theoretic.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 17B50; secondary 12E20.

1. Introduction

Let L be a Lie algebra over a field F. A derivation d of L is said to be *nonsingular* if it is injective as a linear transformation. The notion of nonsingular derivations is in a way analogous to that of regular automorphisms. There is a rich theory of Lie algebras and groups admitting regular automorphisms, in which the order of the automorphism plays a significant role. For example, Lie algebras admitting a regular automorphism of prime order are nilpotent, and those admitting a regular automorphism of finite order are soluble. See for instance [Kh] and the references therein.

What can be said about Lie algebras L which admit nonsingular derivations? By a result of Jacobson [J1], if L is finite-dimensional and the ground field F has characteristic zero (or L is restricted) then L must be nilpotent. However, some non-nilpotent finite-dimensional Lie algebras in positive characteristic have nonsingular derivations.

Supported by the Bi-National Science Foundation United States – Israel, Grant No. 96-00101.

A systematic study of simple Lie algebras of Cartan type which admit a nonsingular derivation is carried out by Benkart, Kostrikin and Kuznetsov in [BKK]. In [KK] Kostrikin and Kuznetsov show that if a simple Lie algebra over an algebraically closed field of characteristic $p > 7$ has a nonsingular derivation, then it has a nonsingular derivation of order $p^k - 1$ for some $k \geq 2$.

The recent interest in nonsingular derivations seems to stem in part from the coclass theory for groups and Lie algebras. The proof in [ShZ] and [Sh1] of the coclass conjectures of Leedham-Green and Newman [LGN] eventually boils down to the fact that finite-dimensional Lie algebras in characteristic $p > 0$ which admit a nonsingular derivation d satisfying $d^{p-1} = 1$ are nilpotent. Moreover, the existence of simple Lie algebras in characteristic p with a nonsingular derivation of order $p^k - 1$ $(k \geq 2)$ was instrumental in the construction, in [Sh2], of non-soluble modular graded Lie algebras of maximal class. Roughly speaking, these infinite-dimensional algebras are constructed from the positive part of a loop algebra associated with certain simple Lie algebras discovered by Albert and Frank [AF] by adding the nonsingular derivation to the first homogeneous component. The resulting Lie algebras of maximal class are generated in degree one, namely, they are generated by their first homogeneous component.

A systematic study of graded Lie algebras of maximal class which are generated in degree one was carried out by Caranti, Mattarei and Newman [CMN] and then by Caranti and Newman [CN]. The latter paper classifies the non-soluble graded Lie algebras of maximal class in odd characteristic generated in degree one, and shows that they all arise from algebras constructed in [Sh2] via repeated process of inflation, introduced in [CMN]. We may say that these Lie algebras owe their existence to nonsingular derivations of certain finite-dimensional simple Lie algebras.

The purpose of this note is to explore conditions on the order of a nonsingular derivation of a Lie algebra L which imply the nilpotency of L. Our main result is as follows.

THEOREM 1.1. *Let L be a finite-dimensional Lie algebra in characteristic $p > 0$ which admits a nonsingular derivation of order n. Write $n = p^s m$ where m is prime to p. Suppose $m < p^2 - 1$. Then L is nilpotent.*

The bound on m is best possible, since the (p^2-1)-dimensional simple Lie algebras of Albert and Frank have a nonsingular derivation of order $p^2 - 1$. More generally, we propose the following.

PROBLEM 1. Study the possible orders n of nonsingular derivations of finite-dimensional non-nilpotent Lie algebras in characteristic p.

Note that if L has a derivation d of order n, and m is any multiple of n, then

$L \otimes_F F[x]/(x^m - 1)$ has a derivation of order m (obtained by multiplying d by the image of x, considered as scalar). Now, for each $k \geq 2$ there is a simple Albert-Frank Lie algebra over the field F_p with p elements which admits a nonsingular derivation of order $p^k - 1$. Therefore, each multiple of $p^k - 1$ ($k \geq 2$) is the order of some finite-dimensional non-nilpotent Lie algebra over F_p. It remains to be seen whether additional numbers n are obtained as orders of such derivations. The problem is easily reduced to the study of numbers n which are prime to p. Indeed, if d is a derivation of order $n = p^s m$, then d^{p^s} is a derivation of order m.

The proof of Theorem 1.1 does not apply [BKK] and the recent classification of finite-dimensional simple Lie algebras in characteristic p (see [St] and the references therein). Indeed, this classification is obtained over algebraically closed fields of characteristic $p \geq 11$, while we do not make such assumptions on the ground field. Instead, our arguments have some number-theoretic flavour. Let $\bar{F}_p$ denote the algebraic closure of F_p. We shall show that Problem 1 is related to the following.

PROBLEM 2. For which numbers n is there an element $\alpha \in \bar{F}_p$ such that $(\alpha + \lambda)^n = 1$ for all $\lambda \in F_p$?

Examples of such numbers are $p^k - 1$ ($k \geq 2$) and their multiples. Some additional examples will be constructed below. It will be shown that if a number n which is prime to p satisfies the condition in Problem 1, then it satisfies the condition in Problem 2. It is unlikely that the converse also holds, and it would be nice to find examples to that effect.

While it is hoped that further progress could be made in these directions, it seems that Problem 2 is rather difficult, being related to characterizing periods of polynomials of the form $x^k - x - c$ over finite fields.

2. Proofs

Let p be a fixed prime. For a Lie algebra L and elements $x, y \in L$ we write $[x,_n y] = [x, y, \dots, y]$ where y occurs n times, and the long Lie product is interpreted using the left normed convention.

We start with the following variation of Jacobson on Engel's theorem (see [J2]).

LEMMA 2.1. *Let L be a finite-dimensional Lie algebra graded by some Abelian group. Suppose L satisfies the Engel condition $[x,_n y] = 0$ for all homogeneous elements $x, y \in L$. Then L is nilpotent.*

We can now deduce the following.

LEMMA 2.2. *Let L be a finite-dimensional Lie algebra in characteristic p which admits a nonsingular derivation d whose order n is prime to p. Suppose L is not nilpotent. Then there exists $\alpha \in \bar{F}_p$ satisfying $(\alpha + \lambda)^n = 1$ for all $\lambda \in F_p$.*

PROOF. Let $R = \{\alpha \in \bar{F}_p : \alpha^n = 1\}$. By extending scalars if needed we may assume that R is contained in the ground field F of L. Since the order of d is prime to p, d is a semisimple element of $\mathrm{End}(L)$; its eigenvalues lie in $R \subseteq F$, so we may write

$$L = \oplus_{\alpha \in R} L_\alpha,$$

where d acts on L_α as multiplication by α. Since d is a derivation we have $[L_\alpha, L_\beta] \leq L_{\alpha+\beta}$, where we define $L_\gamma = 0$ for $\gamma \in F \setminus R$. This turns L into a Lie algebra which is graded by the additive group of F.

We claim that there exist $\alpha, \beta \in R$ such $\alpha + i\beta \in R$ for all $i = 0, 1, \dots, p-1$. Suppose otherwise, then for every $\alpha, \beta \in R$ there is $i \leq p-1$ such that $[L_\alpha,_i L_\beta] \leq L_{\alpha+i\beta} = 0$, and it follows that $[L_\alpha,_{p-1} L_\beta] = 0$ for all $\alpha, \beta \in R$. By Lemma 2.1 this implies that L is nilpotent, a contradiction.

Having proved the claim we deduce that $\alpha\beta^{-1} + \lambda \in R$ for all $\lambda \in F_p$. The result follows. □

COROLLARY 2.3. *Let L, d, n be as above. Then there exists an element $c \in \bar{F}_p$ such that $x^p - x - c$ divides $x^n - 1$ as elements of the polynomial ring $\bar{F}_p[x]$.*

PROOF. We have $x^n - 1 = \prod_{\alpha \in R}(x - \alpha)$. Let α be as in the conclusion of Lemma 2.2. Then we see that $\prod_{\lambda \in F_p}(x - \alpha - \lambda)$ divides $x^n - 1$. But

$$\prod_{\lambda \in F_p}(x - \alpha - \lambda) = (x - \alpha)^p - (x - \alpha) = x^p - x - c,$$

where $c = \alpha^p - \alpha$. The result follows. □

Clearly the element c above is non-zero.

LEMMA 2.4. *Let L, d, n be as above. Then $n \geq p^2 - 1$.*

PROOF. Suppose $n < p^2 - 1$ and write $n = a + bp$ where $0 \leq a, b \leq p - 1$. Then $a + b \leq 2p - 3$. Let c be as in Corollary 2.3 and let $g(x) = x^p - x - c$. Then x^n is congruent to 1 modulo g. Working modulo g we may write

$$x^n = x^a(x^p)^b \equiv x^a(x + c)^b.$$

This yields

$$x^n \equiv x^{a+b} + bcx^{a+b-1} + \cdots + \binom{b}{i} c^i x^{a+b-i} + \cdots + c^b x^a.$$

If $a+b<p$ then the above polynomial is not congruent to 1 modulo g. We therefore have $a+b \geq p$. Write $a+b = p+e$ where $0 \leq e \leq p-3$. Then

$$x^n \equiv x^p A + B \equiv (x+c)A + B,$$

where

$$A = x^e + bcx^{e-1} + \cdots + \binom{b}{e} c^e,$$

and

$$B = \binom{b}{e+1} c^{e+1} x^{p-1} + \cdots + c^b x^a.$$

Note that the polynomial $(x+c)A$ has degree at most $p-2$. On the other hand, $\binom{b}{e+1} c^{e+1} \neq 0$ (since $c \neq 0$ and $e+1 \leq b < p$), so B has degree $p-1$. Therefore the polynomial $(x+c)A + B$ has degree $p-1$, and is the residue of x^n modulo g. We see that $x^n \not\equiv 1$ modulo g, a contradiction. □

PROOF OF THEOREM 1.1. The derivation d has order $n = p^s m$ where m is prime to p. Now, d^{p^s} is also a derivation of L, and its order is m. The inequality $m \geq p^2 - 1$ now follows from Lemma 2.4. □

We conclude with some number-theoretic remarks regarding Problem 2 mentioned in the introduction. It is trivial that for $n = p^k - 1$ ($k \geq 2$), any primitive nth root of unity $\alpha \in \bar{F}_p$ satisfies $(\alpha + \lambda)^n = 1$ for all $\lambda \in F_p$. It turns out that there are other numbers with this property. Recall that the *period* of a polynomial $f(x) \in F[x]$ is the minimal positive integer n such that $f(x)$ divides $x^n - 1$ (if there is such an integer). Clearly, if f has period n then all its roots are nth roots of unity.

EXAMPLE 2.5. Let $p = 2$ and let $f(x) = x^9 + x + 1 \in F_2[x]$. It is known that f is irreducible in $F_2[x]$ and that its period is 73. See for instance [LN, p. 378]. Let α be a root of f. Then $\alpha \in F_{512}$ has order 73. Moreover, since $\alpha + 1 = \alpha^9$, $\alpha + 1$ too has order 73.

EXAMPLE 2.6. Let $p > 2$ and let $\alpha \in \bar{F}_p$ be a root of the polynomial $x^p - x - 1$. Then we easily see that

$$\alpha^{p^i} = \alpha + i \quad \text{for } i = 0, 1, \ldots, p-1.$$

In particular $\alpha^{p^p} = \alpha$ so $\alpha \in F_{p^p}$.

Let $n = (p^p - 1)/(p - 1) = \sum_{i=0}^{p-1} p^i$. We claim that $(\alpha + \lambda)^n = 1$ for all $\lambda \in F_p$. Indeed we have

$$\alpha^n = \prod_{i=0}^{p-1} \alpha^{p^i} = \prod_{i=0}^{p-1} (\alpha + i) = \alpha^p - \alpha = 1.$$

Let $\lambda \in F_p$. Then $\alpha + \lambda$ is a power of α, and so it follows that $(\alpha + \lambda)^n = 1$. Note that n is not divisible by numbers of the form $p^k - 1$ ($k \geq 2$).

It is unclear whether the examples above correspond to some Lie algebras. In particular, is there a finite-dimensional non-nilpotent Lie algebra L in characteristic 2 with a nonsingular derivation d satisfying $d^{73} = 1$?

Acknowledgment

Part of this work was carried out while the author visited the University of Trento. He wishes to thank Andrea Caranti and the University of Trento for their support and hospitality.

References

[AF] A. A. Albert and M. S. Frank, 'Simple Lie algebras of characteristic p', *Rend. Torino* **14** (1954/5), 117–139.

[BKK] G. Benkart, A. I. Kostrikin and M. I. Kuznetsov, 'Finite-dimensional Lie algebras with a nonsingular derivation', *J. Algebra* **171** (1995), 894–916.

[CMN] A. Caranti, S. Mattarei and M. F. Newman, 'Graded Lie algebras of maximal class', *Trans. Amer. Math. Soc.* **349** (1997), 4021–4051.

[CN] A. Caranti and M. F. Newman, 'Graded Lie algebras of maximal class. II', preprint, 1998.

[J1] N. Jacobson, 'A note on automorphisms and derivations of Lie algebras', *Proc. Amer. Math. Soc.* **6** (1955), 281–283.

[J2] ———, *Lie algebras* (Wiley-Interscience, New York, 1962).

[Kh] E. I. Khukhro, *Nilpotent groups and their automorphisms* (de Gruyter, Berlin, 1993).

[KK] A. I. Kostrikin and M. I. Kuznetsov, 'Lie algebras with a nonsingular derivation', in: *Algebra and analysis (Kazan, 1994)* (de Gruyter, Berlin, 1996) pp. 81–90.

[LGN] C. R. Leedham-Green and M. F. Newman, 'Space groups and groups of prime power order I', *Arch. Math.* **35** (1980), 193–202.

[LN] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications* (Cambridge Univ. Press, Cambridge, 1986).

[Sh1] A. Shalev, 'The structure of finite p-groups: effective proof of the coclass conjectures', *Invent. Math.* **115** (1994), 315–345.

[Sh2] ———, 'Simple Lie algebras and Lie algebras of maximal class', *Arch. Math.* **63** (1994), 297–301.

[ShZ] A. Shalev and E. I. Zelmanov, 'Pro-p groups of finite coclass', *Math. Proc. Cambridge Philos. Soc.* **111** (1992), 417–421.

[St] H. Strade, 'The classification of the simple modular Lie algebras. VI. Solving the final case', *Trans. Amer. Math. Soc.* **350** (1998), 2553–2628.

Institute of Mathematics
The Hebrew University
Jerusalem 91904
Israel
e-mail: shalev@math.huji.ac.il