BULLETIN

OF THE

AUSTRALIAN MATHEMATICAL SOCIETY

Volume 72, Number 1
August, 2005

(MathReviews) (Zentralblatt)

The Australian Mathematical Publishing Assoc. Inc.
Australian National University, ACT 0200, Australia
Printed in Australia by Pirion Printing
Print Post approved - PP229219/00095

ISSN 0004-9727

Information for Authors

The Bulletin of the Australian Mathematical Society aims at quick publication of original research in all branches of mathematics. The Editors receive more than three times as much material as can be published in the BULLETIN; many meritorious papers can, therefore, not be accepted. Authors are asked to avoid, as far as possible the use of mathematical symbols in the title. Manuscripts are accepted for review with the understanding that the same work is not concurrently submitted elsewhere.

To ensure speedy publication, editorial decisions on acceptance or otherwise are taken quickly, normally within a month of receipt of the paper. Papers are accepted only after a careful evaluation by the Editor and an Associate Editor or other expert in the field. As even minor revisions are generally not permitted, authors should read carefully all the details listed below. For a paper to be acceptable for publication, not only should it contain new and interesting results but also

(i) the exposition should be clear and attractive;
(ii) the manuscript should be in publishable form, without revision.

Authors should submit three clean, high quality copies to

The Editorial Office, Bulletin of the Australian Mathematical Society,
Department of Mathematics, The University of Queensland,
Queensland 4072, Australia.

Unless requested at the time, material submitted to the BULLETIN will usually not be returned.

Editorial Policy

1. References. Arrange references alphabetically (by surname of the first author) and cite them numerically in the text. Ensure the accuracy of the references: authors' names should appear as in the work quoted. Include in the list of references only those works cited, and avoid citing works which are "in preparation" or "submitted". Where the work cited is not readily accessible (for example, a preprint) a photocopy of the title page and relevant sections of the copy that you have used should be included with your submission.

2. Abstracts.

1. Each paper must include an abstract of not more than 200 words, which should contain a brief but informative summary of the contents of the paper, but no inessential details.
2. The abstract should be self-contained, but may refer to the title.
3. Specific references (by number) to a section, proposition, equation or bibliographical item should be avoided.

3. Subject Classification. Authors should include in their papers one or more classification numbers, following the 2000 Mathematics Subject Classification. Details of this scheme can be found in each Annual Index of Mathematical Reviews or on the web at http://www.ams.org/msc .

4. Abstracts of Ph.D. Theses. The Bulletin endeavours to publish abstracts of all accepted Australasian Ph.D. theses in mathematics. One restriction, however, is that the abstract must be received by the Editor within 6 months of the degree being approved.

5. Electronic Manuscripts. The Bulletin is produced using $\mathcal{AMS}$-TEX. Authors who are able to do so are invited to prepare their manuscripts using TEX. (We accept Plain TEX, $\mathcal{AMS}$-TEX or LATEX.) Hard copy only should be submitted for assessment, but if the paper is accepted the author will be asked to send the text on an IBM PC compatible diskette or via e-mail to ams@maths.uq.edu.au. [Typed manuscripts are, of course, still acceptable.]

Bulletin of the Australian Mathematical Society

Volume 72 Number 1 **August 2005**

Bull. Austral. Math. Soc.
Vol. 72 (2005) [147–156]

17B01, 17B50

SUBALGEBRAS OF FREE RESTRICTED LIE ALGEBRAS

R.M. Bryant, L.G. Kovács and Ralph Stöhr

A theorem independently due to A.I. Shirshov and E. Witt asserts that every subalgebra of a free Lie algebra (over a field) is free. The main step in Shirshov's proof is a little known but rather remarkable result: if a set of homogeneous elements in a free Lie algebra has the property that no element of it is contained in the subalgebra generated by the other elements, then this subset is a free generating set for the subalgebra it generates. Witt also proved that every subalgebra of a free restricted Lie algebra is free. Later G.P. Kukin gave a proof of this theorem in which he adapted Shirshov's argument. The main step is similar, but it has come to light that its proof contains substantial gaps. Here we give a corrected proof of this main step in order to justify its applications elsewhere.

1. Introduction

The Shirshov–Witt Theorem [9, 11] asserts that every subalgebra of a free Lie algebra (over a field) is free. Witt [11] also gave a similar result for restricted Lie algebras (over fields of positive characteristic), and of course there are some even better known results of the same kind in other branches of algebra, particularly for free groups and free Abelian groups. Shirshov's proof in [9] started with an easy application of a method of Kurosh to show that each subalgebra of a free Lie algebra has a generating set S which is *reduced* in the following sense: for each $s \in S$ the leading term of s (that is, the highest degree homogeneous component of s) does not belong to the subalgebra generated by the leading terms of the other elements of S. The second and main step of the proof was to show that *every reduced subset of a free Lie algebra is independent* in the sense that it is a free generating set for the subalgebra it generates. This step was not proclaimed as a lemma or theorem in its own right and has not become well-known like the Shirshov–Witt Theorem, but it is a remarkable result with, as far as we are aware, no non-trivial parallels in other branches of algebra. It may have contributed to this lack of recognition that [9] is still only available in the original Russian and that books presenting the Shirshov-Witt Theorem have chosen proofs which do not involve this step.

One might try to modify the definition of a reduced set to say that a set S is *irredundant* if no element of S belongs to the subalgebra generated by the other elements.

Received 18th April, 2005

Shirshov's main step yields that every irredundant set of homogeneous elements is independent. However, the homogeneity condition cannot be removed. For example, in the Lie algebra L freely generated by x and y, let

$$S = \Big\{x,\ x + [y,x],\ y + \big[[y,x],x\big]\Big\}.$$

Then it is not difficult to verify that S is irredundant; but S is not independent (because S generates L). It should also be noted that independent sets need not be reduced: consider, for example, the set $\{x, y, z + [y,x]\}$ in the Lie algebra freely generated by x, y and z.

Kukin [7] adapted Shirshov's argument to give a proof of Witt's result for free restricted Lie algebras. This adaptation contained an analogue of Shirshov's main step, this time proclaimed as a lemma. With definitions of reduced and independent as before, except that subalgebra now means restricted Lie subalgebra, Kukin's Lemma (Lemma 2 in [7]) states that *every reduced subset of a free restricted Lie algebra is independent.*

In that paper, and later also in Bakhturin's book [1], this result was used not only in the proof of Witt's Theorem, but (for instance) also in proving Kukin's formula for the free rank of a subalgebra of finite codimension in a free restricted Lie algebra (the analogue of Schreier's formula so well known in group theory). We have found it an indispensable tool in [2, 3, 6], and have little doubt that it will find many further applications.

However, we have been aware for some time that both of its proofs in print, the original in [7] and the one given in [1], contain substantial gaps (see the *Remarks* in the last section of this note). Our confidence in the result was sustained by possible alternative approaches, but recently we found that Kukin's proof may be corrected by extending and modifying his argument. The main purpose of this note is to provide firm foundations for the applications of the result by making available our corrected proof. A consolidated exposition seems preferable to a list of corrigenda, and then it is only one short step to complete Kukin's proof of Witt's Theorem: we include that to make the readers' labour more rewarding.

The focus here is on free restricted Lie algebras, but only minor modifications are needed to deal with the case of free Lie algebras, as considered by Shirshov. We hope that our exposition will bring wider attention to the powerful and rather striking results of Shirshov and Kukin that have been described above.

2. Free restricted Lie algebras

Let K be a field of prime characteristic p. When considering Lie algebras over K we write the Lie product of elements u and v as $[u,v]$, and $[u_1, u_2, \dots, u_n]$ denotes the left-normed product $\Big[\cdots\big[[u_1,u_2],\dots\big],u_n\Big]$.

A restricted Lie algebra R over K is a Lie algebra over K with an additional unary "p-powering" operation, in which the image of each element u of R is written as a formal

power u^p. The properties of this operation are $(\alpha u)^p = \alpha^p u^p$ for all $\alpha \in K$, $u \in R$, where α^p denotes the usual pth power,

$$[u, v^p] = [u, \underbrace{v, \ldots, v}_{p}]$$

for all $u, v \in R$, and $(u+v)^p = u^p + v^p + l(u, v)$, for all $u, v \in R$, where $l(u, v)$ is a certain linear combination of Lie products (see [5, Definition V.4] or [8, Section 2.5.2] for the precise form).

Free restricted Lie algebras may be defined by means of a universal property. However, they arise in a concrete way from free associative algebras, as now described. For many purposes this is the easiest way of thinking about them.

Let A be a free associative algebra over K with a free generating set X. Then A may be regarded as a restricted Lie algebra with Lie multiplication given by $[u, v] = uv - vu$ and p-powering given by

$$u \mapsto u^p = \underbrace{u \cdots u}_{p}.$$

The restricted Lie subalgebra R of A generated by X is a free restricted Lie algebra with free generating set X (see, for example, [8, Section 5.2]). If $|X| = r$ then R is said to have rank r.

For each positive integer n let A_n be the subspace of A spanned by all products of the form $u_1 u_2 \cdots u_n$ with $u_1, \ldots, u_n \in X$, and write $R_n = R \cap A_n$. It is easily proved that R_n is spanned by all monomials that have the form u^{p^k} where $k \geqslant 0$, $p^k \mid n$, and u is the Lie product, with some bracketing, of n/p^k not necessarily distinct elements of X.

As a vector space, R has the decomposition $R = \bigoplus_n R_n$. Furthermore, R is graded as an algebra: if $u \in R_m$ and $v \in R_n$ then $[u, v] \in R_{m+n}$ and $u^p \in R_{pm}$. An element u of R is said to be *homogeneous* if $u \in R_n$ for some n. Each element u of R may be written uniquely in the form $u = \sum_n u_n$, where $u_n \in R_n$ for all n and only finitely many of the u_n are non-zero. If $u \neq 0$ we write $\deg u$ for the largest value of n for which $u_n \neq 0$. This is called the *degree* of u. The corresponding term u_n is called the *leading term* of u and denoted by $\overline{u}$. For $u = 0$ we define $\deg u = 0$ and $\overline{u} = 0$. Furthermore, if S is a finite subset of R we write

$$\deg S = \sum_{u \in S} \deg u.$$

This is called the *degree sum* of S.

By a subalgebra of R we always mean a restricted Lie subalgebra, and the subalgebra generated by a set S is denoted by $\langle S \rangle$. A subset S is said to be *independent* if S is a free generating set for $\langle S \rangle$, and S is said to be *reduced* if, for all $u \in S$,

$$\overline{u} \notin \langle \overline{w} : w \in S \backslash \{u\} \rangle.$$

The concepts of homogeneous element, degree, leading term and reduced subset are defined in terms of the grading of R given by the free generating set X. Unless otherwise specified this grading is taken as fixed.

In [7], Kukin used the alternative terminology of Lie p-algebras, instead of restricted Lie algebras. He referred to p-subalgebras, p-reduced subsets and p-independent subsets, presumably in order to avoid any confusion with the corresponding concepts for Lie algebras discussed in Shirshov's paper [9]. Since we concentrate on restricted Lie algebras there should be no confusion here.

Then [7, Lemma 4] may be paraphrased as follows.

LEMMA 2.1. *Let R be a free restricted Lie algebra with free generating set $\{x_1, \dots, x_r\}$, where r is a positive integer. Then the ideal I of R generated by $x_1^p, x_2, \dots, x_r$ is a free subalgebra of R with a free generating set Y consisting of x_1^p and the elements*

$$[x_i, \underbrace{x_1, \dots, x_1}_{c}]$$

for $i = 2, \dots, r$ and $c = 0, \dots, p-1$.

We have no reservations about the proof of this lemma in [7] or in Bakhturin's book [1, Section 2.7, proof of Witt's Theorem], so we give no proof here. This lemma, in the terminology of [10], is called "restricted elimination". There was a corresponding result for free Lie algebras in [9] and that was the simplest special case of what has since become known as "elimination" or "Lazard elimination" (see, for example, [4, Proposition 10 in Section 2.9, Chapter 2] or [8, Section 0.3]).

The subalgebra I of R described in Lemma 2.1 has a grading determined by its free generating set Y. For elements and subsets of I it is sometimes necessary to distinguish between the concepts homogeneous, degree, leading term and reduced defined in terms of X and the same concepts defined in terms of Y. When necessary we make this explicit. For example, we write $\deg_X u$ and $\deg_Y u$ for the degrees of an element u of I with respect to X and Y, respectively.

Our main object here is to give a corrected proof of [7, Lemma 2], namely the following result.

LEMMA 2.2. (Kukin's Lemma) *Let S be a reduced subset of a free restricted Lie algebra R. Then S is independent.*

Once the machinery for the proof of Lemma 2.2 has been set up it is rather easy to prove the following result, [7, Lemma 1].

LEMMA 2.3. *Let Q be a subalgebra of a free restricted Lie algebra R. Then Q has a reduced generating set.*

We include a proof of this result partly because Kukin suppressed some of the details but mainly because Lemmas 2.2 and 2.3 immediately give Witt's Theorem.

THEOREM 2.4. (Witt [11]) *Let Q be a subalgebra of a free restricted Lie algebra R. Then Q is free.*

3. Preliminary results

Throughout this section we take K to be a field of prime characteristic p and R to be a free restricted Lie algebra over K.

Let ϕ or $\phi(y_1, \dots, y_m)$ be a monomial in a free restricted Lie algebra over K with free generating set $\{y_1, \dots, y_m\}$ and let $u_1, \dots, u_m$ be homogeneous elements of R. Then either $\phi(u_1, \dots, u_m) = 0$ or $\phi(u_1, \dots, u_m)$ has degree $\sum_j d_j \deg u_j$, where d_j is the degree of y_j in ϕ. We call the number $\sum_j d_j \deg u_j$ the *formal degree* of $\phi(u_1, \dots, u_m)$ and denote it by $\operatorname{Deg} \phi(u_1, \dots, u_m)$.

LEMMA 3.1. *Let S be a finite subset of R which is not independent. If the leading terms of distinct elements of S are distinct then the set of these leading terms is not independent.*

PROOF: Let $S = \{s_1, \dots, s_m\}$. Clearly we may assume that each s_i is non-zero. Since S is not independent there exists a non-zero element ϕ in a free restricted Lie algebra of rank m such that $\phi(s_1, \dots, s_m) = 0$. We can write $\phi = \sum_{j=1}^{l} \alpha_j \phi_j$ where the α_j are non-zero elements of K and the ϕ_j are linearly independent monomials.

Let n be the maximum of the formal degrees $\operatorname{Deg} \phi_j(\overline{s}_1, \dots, \overline{s}_m)$. We can renumber the ϕ_j so that, for some $k > 0$, $\operatorname{Deg} \phi_j(\overline{s}_1, \dots, \overline{s}_m) = n$ for $j \leqslant k$ and $\operatorname{Deg} \phi_j(\overline{s}_1, \dots, \overline{s}_m) < n$ for $j > k$.

For $j \leqslant k$ we have

$$\phi_j(s_1, \dots, s_m) = \phi_j(\overline{s}_1, \dots, \overline{s}_m) + v_j$$

where $\deg v_j < n$. Also, for $j > k$, we have $\deg \phi_j(s_1, \dots, s_m) < n$. Write $\phi^* = \sum_{j=1}^{k} \alpha_j \phi_j$. Then $\phi^* \neq 0$ and

$$0 = \phi(s_1, \dots, s_m) = \phi^*(\overline{s}_1, \dots, \overline{s}_m) + v$$

where $\phi^*(\overline{s}_1, \dots, \overline{s}_m) \in R_n$ and $\deg v < n$. Thus $\phi^*(\overline{s}_1, \dots, \overline{s}_m) = 0$. Hence $\{\overline{s}_1, \dots, \overline{s}_m\}$ is not independent. □

LEMMA 3.2. *Let S be a finite set of non-zero elements of R and suppose that S is not reduced. Then, for some $u \in S$, there exists $w \in \langle S \backslash \{u\} \rangle$ such that $\deg(u - w) < \deg u$. Furthermore we may take w in the form $w = w_1 + w_2$, where w_1 is a linear combination of elements of $S \backslash \{u\}$ of degree equal to $\deg u$ and w_2 belongs to the subalgebra of R generated by the elements of $S \backslash \{u\}$ of degree smaller than $\deg u$.*

PROOF: By assumption there exists $u \in S$ such that

$$\overline{u} \in \langle \overline{v} : v \in S \backslash \{u\} \rangle.$$

Write $S\backslash\{u\} = \{s_1, \ldots, s_m\}$. There exists an element ϕ in a free restricted Lie algebra of rank m such that $\overline{u} = \phi(\overline{s}_1, \ldots, \overline{s}_m)$. Write $\phi = \sum_{j=1}^{l} \alpha_j \phi_j$ where the α_j belong to K and the ϕ_j are monomials. Let $n = \deg u = \deg \overline{u}$. We consider the formal degrees $\operatorname{Deg} \phi_j(\overline{s}_1, \ldots, \overline{s}_m)$ and renumber the ϕ_j so that, for some k, $\operatorname{Deg} \phi_j(\overline{s}_1, \ldots, \overline{s}_m) = n$ for $j \leqslant k$ and $\operatorname{Deg} \phi_j(\overline{s}_1, \ldots, \overline{s}_m) \neq n$ for $j > k$. Write $\phi^* = \sum_{j=1}^{k} \alpha_j \phi_j$. Then $\overline{u} = \phi^*(\overline{s}_1, \ldots, \overline{s}_m)$. Let $w = \phi^*(s_1, \ldots, s_m)$. For $j = 1, \ldots, k$ we have

$$\phi_j(s_1, \ldots, s_m) = \phi_j(\overline{s}_1, \ldots, \overline{s}_m) + v_j$$

where $\deg v_j < n$. Thus

$$w = \phi^*(s_1, \ldots, s_m) = \phi^*(\overline{s}_1, \ldots, \overline{s}_m) + v = \overline{u} + v,$$

where $\deg v < n$. Hence $\deg(u - w) < n$.

We may renumber $\phi_1, \ldots, \phi_k$ so that, for some t, $\deg \phi_j = 1$ for $j \leqslant t$ and $\deg \phi_j > 1$ for $j > t$. Then $w = w_1 + w_2$ where

$$w_1 = \sum_{j=1}^{t} \alpha_j \phi_j(s_1, \ldots, s_m) \quad \text{and} \quad w_2 = \sum_{j=t+1}^{k} \alpha_j \phi_j(s_1, \ldots, s_m).$$

Since $\operatorname{Deg} \phi_j(\overline{s}_1, \ldots, \overline{s}_m) = n$ for $j = 1, \ldots, k$, the elements w_1 and w_2 have the required properties. ∎

LEMMA 3.3. *Let S be a reduced set of homogeneous elements of R. Then no set of cardinality smaller than $|S|$ can generate $\langle S \rangle$.*

PROOF: Let $Q = \langle S \rangle$. Write Q' for the ideal of Q generated by all elements of the forms u^p and $[u, v]$ where $u, v \in Q$. Then any generating set of the restricted Lie algebra Q/Q' spans it as a vector space. If W is any generating set of Q it follows that W spans Q modulo Q'. Hence $|W| \geqslant \dim Q/Q'$. Thus it suffices to show that the elements of S are linearly independent modulo Q'.

Suppose that this is not the case. Then for some $u \in S$ there exist elements $u_1, \ldots, u_m \in S\backslash\{u\}$, $\alpha_1, \ldots, \alpha_m \in K$ and $v \in Q'$ such that

$$u = v + \sum_{j=1}^{m} \alpha_j u_j.$$

Let Ω be the subset of Q consisting of the elements s^{p^k} where $s \in S$ and $k \geqslant 1$ and the elements w^{p^k} where w is a Lie product (with arbitrary bracket arrangement) of two

or more (not necessarily distinct) elements of S and $k \geqslant 0$. Thus each element of Ω is homogeneous. It is straightforward to verify that Q' is spanned by Ω. Thus v is a linear combination of elements of Ω.

Write $n = \deg u$. We may renumber $u_1, \dots, u_m$ so that, for some k, $\deg u_j = n$ for $j \leqslant k$ and $\deg u_j \neq n$ for $j > k$. Then, by comparing terms of degree n in the equation $u = v + \sum \alpha_j u_j$ we obtain a relation

$$u = v' + \sum_{j=1}^{k} \alpha_j u_j$$

where v' is a linear combination of elements of Ω of degree n.

By the definition of Ω, every element of Ω of degree n is formed from elements of S of degree smaller than n. Thus $v' \in \langle S \backslash \{u\} \rangle$ and we obtain $u \in \langle S \backslash \{u\} \rangle$. This contradicts the fact that S is reduced and completes the proof. □

LEMMA 3.4. *Let S be a subset of R. Let $u \in S$ and $w \in \langle S \backslash \{u\} \rangle$, and write $S^* = \big(S \backslash \{u\}\big) \cup \{u - w\}$. If $u - w \notin S \backslash \{u\}$ and S^* is independent then S is independent.*

PROOF: Clearly $\langle S^* \rangle = \langle S \rangle$. Suppose that $u - w \notin S \backslash \{u\}$ and S^* is independent. Then there are endomorphisms σ and τ of $\langle S^* \rangle$ given by

$$\begin{aligned} s\sigma &= s \quad \text{for} \quad s \in S \backslash \{u\}, \quad (u - w)\sigma = u, \\ s\tau &= s \quad \text{for} \quad s \in S \backslash \{u\}, \quad (u - w)\tau = u - 2w. \end{aligned}$$

It is easily proved that σ and τ are mutually inverse. Thus σ is an automorphism. Since $S = S^*\sigma$, it follows that S is independent. □

4. Kukin's proof of Witt's Theorem

In this section we prove Lemmas 2.2 and 2.3. As already remarked, they immediately yield Witt's Theorem, Theorem 2.4. Since the main purpose of our work is the correction of Kukin's proof in [7] and the account of it in [1] we follow the proof of Lemma 2.2 with a brief indication of the problems with the original proofs.

PROOF OF LEMMA 2.2: It is clearly sufficient to prove the result in the case where S is finite and R has finite rank. We assume that there is a counterexample, that is, a pair (S, R) where S is a finite and reduced, but not independent, subset of R, and R has finite rank. We shall obtain a contradiction.

We choose n as small as possible such that there exists a counterexample (S, R) where S has degree sum n, that is, $\deg S = n$. We then choose r as small as possible such that there exists a counterexample (S, R) with $\deg S = n$ and R of rank r. Let X be a free generating set of R, where $X = \{x_1, \dots, x_r\}$.

Since S is reduced, distinct elements of S have distinct leading terms. Let H be the set of these leading terms. Note that the elements of H are non-zero and homogeneous and H is reduced. By Lemma 3.1 H is not independent. Also, $\deg H = n$.

Suppose that the elements of H of degree 1 are $z_1, \dots, z_s$. Since H is reduced, $\{z_1, \dots, z_s\}$ is a linearly independent subset of R_1. If $s = r$ then $\{z_1, \dots, z_s\}$ is a free generating set for R and, since H is reduced, we get $H = \{z_1, \dots, z_s\}$, contrary to the fact that H is not independent. Hence $s < r$. It follows that there is an automorphism θ of R which maps R_1 to R_1 and maps $\{z_1, \dots, z_s\}$ to a subset of $\{x_2, \dots, x_r\}$. Then $H\theta$ has all the properties of H. Thus without loss of generality we may assume that the elements of H of degree 1 all belong to $\{x_2, \dots, x_r\}$.

Let I be the ideal of R generated by $x_1^p, x_2, \dots, x_r$. All monomials of R of degree greater than 1 belong to I. Therefore $H \subseteq I$. Let Y be the free generating set for I given by Lemma 2.1. When the elements of H are written with respect to Y they need not be homogeneous. However, for $h \in H$, we may write $h = h_1 + h_2$ where $h_1 \in \langle x_2, \dots, x_r \rangle$ and either $h_1 = 0$ or $\deg_Y h_1 = \deg_X h$ and where $\deg_Y h_2 < \deg_X h$. Thus $\deg_Y H \leqslant \deg_X H = n$ and if $\deg_Y H = \deg_X H$ then the leading terms of the elements of H with respect to Y all belong to $\langle x_2, \dots, x_r \rangle$.

The definition of independence for a set involves only the subalgebra it generates. Hence H is not independent when considered with respect to Y.

Suppose that H is reduced with respect to Y. Then the minimality of n gives $\deg_Y H = n$. Since H is reduced, the leading terms of distinct elements of H are distinct. Let $\overline{H}$ be the set of these. Clearly $\overline{H}$ is reduced (with respect to Y) and $\deg_Y \overline{H} = n$. By Lemma 3.1, $\overline{H}$ is not independent. However, as observed above, $\overline{H} \subseteq \langle x_2, \dots, x_r \rangle$. This contradicts the minimality of r. Hence H is not reduced with respect to Y.

Consider the subsets N of $\langle H \rangle$ satisfying $\langle N \rangle = \langle H \rangle$, $|N| = |H|$, $0 \notin N$, N is not independent, N is not reduced with respect to Y, and $\deg_Y N \leqslant n$. For example, we can take $N = H$. Among these sets, choose N so that $\deg_Y N$ is as small as possible. By Lemma 3.2, there exist $u \in N$ and $w \in \langle N \backslash \{u\} \rangle$ such that $\deg_Y(u - w) < \deg_Y u$. Write $N^* = \big(N \backslash \{u\}\big) \cup \{u - w\}$. Clearly $\langle N^* \rangle = \langle N \rangle = \langle H \rangle$. Since H is reduced and consists of homogeneous elements with respect to X, it follows by Lemma 3.3 that $u - w \notin \langle N \backslash \{u\} \rangle$. Thus $|N^*| = |N| = |H|$ and the elements of N^* are non-zero. Also, by Lemma 3.4, N^* is not independent. Clearly $\deg_Y N^* < \deg_Y N \leqslant n$. Thus, by the minimality of n, N^* is not reduced. This contradicts the choice of N and completes the proof of the lemma. □

Remarks 1. The last two paragraphs of our proof of Lemma 2.2 should be compared with the last paragraph of Kukin's proof of his Lemma 2. In terms of the notation used here, Kukin claims that $\deg_Y H < \deg_X H$. This does not hold, for example, if H is the set

$$\big\{x_2,\ [x_3, x_2] + [x_2, x_1]\big\}.$$

We have had to treat the case $\deg_Y H = \deg_X H$ by observing that $\overline{H} \subseteq \langle x_2, \dots, x_r \rangle$

and using Lemma 3.1. Kukin's use of "elementary transformations" is essentially the passage from N to N^* in our proof. However, Kukin does not consider the possibility that $u - w = 0$. To show that this case does not arise we have had to introduce Lemma 3.3.

In the version of the proof given in [1, Section 2.7, proof of Witt's Theorem] it seems that the assumption is made that H remains homogeneous and reduced when written with respect to Y. However, neither property is preserved, for example, if $p > 3$ and H is the set

$$\Big\{\big[[x_2, x_1], [x_3, x_1]\big] + [x_2, x_1, x_1, x_1],\ [x_2, x_1],\ [x_3, x_1]\Big\}.$$

Proof of Lemma 2.3: For each non-negative integer n, let Q_n be the subspace of Q consisting of all elements u of Q such that $\deg u \leqslant n$. (In particular, $Q_0 = \{0\}$.) For each $n \geqslant 1$, let V_n be a subspace of Q_n such that

$$Q_n = \big(\langle Q_{n-1}\rangle \cap Q_n\big) \oplus V_n$$

and let S_n be a basis of V_n. Define $S = \bigcup_n S_n$. It follows by induction that $\langle Q_n\rangle = \langle S_1 \cup \cdots \cup S_n\rangle$ for all n. Hence $Q = \langle S\rangle$. It remains to prove that S is reduced.

Suppose otherwise. Note that, by construction, every element of S is non-zero. Since S is not reduced it contains a finite subset which is not reduced. Thus we can apply Lemma 3.2. There exist $u \in S$ and $w \in \langle S\backslash\{u\}\rangle$ such that $\deg(u-w) < \deg u$ and $w = w_1 + w_2$, where w_1 and w_2 are as in Lemma 3.2. Let $n = \deg u$. Thus $u \in S_n$, w_1 is a linear combination of elements of $S_n\backslash\{u\}$ and $w_2 \in \langle Q_{n-1}\rangle$. By the choice of S_n, $u - w_1$ is a non-zero element of V_n. However, since $\deg(u - w) < n$, we have $u - w \in Q_{n-1}$. Hence

$$u - w_1 = (u - w) + w_2 \in \langle Q_{n-1}\rangle.$$

Thus $u - w_1$ is a non-zero element of $\langle Q_{n-1}\rangle \cap V_n$. However,

$$\langle Q_{n-1}\rangle \cap V_n = \big(\langle Q_{n-1}\rangle \cap Q_n\big) \cap V_n = \{0\}.$$

This is a contradiction, completing the proof of the lemma. □

References

[1] Yu. A. Bakhturin, *Identical relations in Lie algebras*, (Russian) (Nauka, Moscow, 1985). English translation: (VNU Science Press, Utrecht, 1987).

[2] R.M. Bryant and R. Stöhr, 'On the module structure of free Lie algebras', *Trans. Amer. Math. Soc.* **352** (2000), 901–934.

[3] R.M. Bryant, L.G. Kovács and R. Stöhr, 'Lie powers of modules for groups of prime order', *Proc. London Math. Soc. (3)* **84** (2002), 343–374.

[4] N. Bourbaki, *Lie groups and Lie algebras*, (Part I: Chapters 1–3) (Hermann, Paris, 1975).

[5] N. Jacobson, *Lie algebras* (Interscience, New York, 1962).

[6] L.G. Kovács and R. Stöhr, 'Lie powers of the natural module for $GL(2)$', *J. Algebra* **229** (2000), 435–462.

[7] G.P. Kukin, 'Subalgebras of free Lie p-algebras', (Russian), *Algebra i Logika* **11** (1972), 535–550. English translation: *Algebra Logic* **11** (1972), 294–303.

[8] C. Reutenauer, *Free Lie algebras* (Clarendon Press, Oxford, 1993).

[9] A.I. Shirshov, 'Subalgebras of free Lie algebras', (Russian), *Mat. Sbornik N. S.* **33** (1953), 441–452.

[10] R. Stöhr, 'Restricted Lazard elimination and modular Lie powers', *J. Austral. Math. Soc.* **71** (2001), 259–277.

[11] E. Witt, 'Die Unterringe der freien Lieschen Ringe', *Math. Z.* **64** (1956), 195–216.

School of Mathematics
University of Manchester
PO Box 88
Manchester M60 1QD
United Kingdom
e-mail: roger.bryant@manchester.ac.uk
ralph.stohr@manchester.ac.uk

Australian National University
Canberra ACT 0200
Australia
e-mail: kovacs@maths.anu.edu.au