Functional Analysis and Its Applications, Vol. 36, No. 2, pp. 140–144, 2002
Translated from Funktsional′nyi Analiz i Ego Prilozheniya, Vol. 36, No. 2, pp. 69–74, 2002

On the Restricted Lie Algebra Structure of the Witt Lie Algebra in Finite Characteristic

T. J. Evans and D. B. Fuchs

Received November 29, 2001

ABSTRACT. The article contains an explicit formula for the restricted Lie algebra structure in the Witt Lie algebra over a field of finite characteristic. Some combinatorial lemmas can be of independent interest.

KEY WORDS: restricted Lie algebra, Witt algebra.

1. Introduction. Let p be a prime, let $\mathbb{F}$ be a field of characteristic p, and let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$. Set $A = \mathbb{F}[x]/(x^p - 1)$. Note that $\mathbb{F}[x]/(x^p - 1) \cong \mathbb{F}[x]/(x^p)$, and an isomorphism can be established by the formula $x \leftrightarrow x - 1$. We also note that

$$\frac{d}{dx}(x^p - 1) \subset (x^p - 1) \quad \text{and} \quad \frac{d}{dx}(x^p) \subset (x^p),$$

and hence the operator d/dx is defined on A; the above isomorphism commutes with d/dx. Below, we abbreviate the notation d/dx to ∂.

The Lie algebra $W = \operatorname{Der} A$ is called the *Witt algebra*. It consists of the "vector fields" $f\partial$, $f \in A$. In particular, $\dim_{\mathbb{F}} W = \dim_{\mathbb{F}} A = p$.

Since W is a Lie algebra of derivations of a commutative algebra over $\mathbb{F}$, it follows that W has the canonical structure of a restricted Lie algebra. Recall that a Lie algebra over $\mathbb{F}$ is said to be *restricted* if it is endowed with an additional (nonlinear in general) unary operation $g \mapsto g^{[p]}$ for which

$$(\lambda g)^{[p]} = \lambda^p g^{[p]} \quad (\lambda \in \mathbb{F}), \qquad \operatorname{ad}(g^{[p]}) = (\operatorname{ad} g)^p,$$

$$(g + h)^{[p]} = g^{[p]} + h^{[p]} + \sum_{i=1}^{p-1} s_i(g, h),$$

where $is_i(g, h)$ is the coefficient of λ^{i-1} in $(\operatorname{ad}(\lambda g + h))^{p-1}(h)$ modulo p; in particular, $[g^{[p]}, g] = 0$ for any g (for details, see [1]). In $\operatorname{Der} A$ we have $g^{[p]} = g^p$ (obviously, if $g \in \operatorname{Der} A$, then $g^p = g \circ \cdots \circ g \in \operatorname{Der} A$.)

Although the operation $g \mapsto g^{[p]}$ need not be linear, it is completely determined by its values on any basis of the Lie algebra. In particular, in W we have

$$(x\partial)^{[p]} = x\partial, \quad (x^k\partial)^{[p]} = 0 \quad \text{for } k = 0, 2, 3, \ldots, p - 1$$

(these formulas hold if A is regarded either as $\mathbb{F}[x]/(x^p - 1)$ or as $\mathbb{F}[x]/(x^p)$; the same is true for Theorem 1 below). However, we can give a more detailed description of the operation $g \mapsto g^{[p]}$ in W.

Theorem 1. (a) $(f\partial)^{[p]} = C(f)f\partial$ *for any* $f \in A$, *where* $C(f)$ *is a constant* (*depending on* f).

(b) *The expression* $\partial(f\partial(\ldots(f\partial f)\ldots))$ *with* $p - 1$ *letters* ∂ (*and* $p - 1$ *letter* f) *is a constant for any* $f \in A$, *and this constant is equal to* $C(f)$.

(c) $\partial^{p-1} f^{p-1}$ *is a constant for any* $f \in A$, *and this constant is equal to* $-C(f)$.

Since parts (a) and (b) of Theorem 1 are very simple (see Sec. 2), the main result of the paper is part (c), or rather the equivalence between (b) and (c). Moreover, this result is majorated by three (actually equivalent) combinatorial theorems. We state these theorems in Sec. 3 and prove them in Sec. 4.

 0016–2663/02/3602–0140 $27.00

2. Proof of parts (a) and (b) of Theorem 1. The Lie algebra W is of rank one, which means that there exists a nonempty Zariski open subset $U \subset W$ such that $h \in \mathbb{F}g$ if $g \in U$ and $[h, g] = 0$. Since $[g^{[p]}, g] = 0$, it follows that $g^{[p]} \in \mathbb{F}g$, at least for $g \in U$. However, since the mapping $g \mapsto g^{[p]}$ is algebraic, this implies that $g^{[p]} \in \mathbb{F}g$ for any $g \in W$. (Strictly speaking, this holds if $\mathbb{F}$ is infinite, but we can extend $\mathbb{F}$ to $\overline{\mathbb{F}}$ and take U in the extended W if necessary.) This proves (a), namely, $(f\partial)^{[p]} = C(f)f\partial$ for some algebraic function $C\colon W \to \mathbb{F}$. To prove (b), apply this relation to $x \in A$. This gives $f\partial(f\partial(\dots(f\partial f)\dots)) = C(f)f$, which shows that $\partial(f\partial(\dots(f\partial f)\dots)) = C(f)$, at least if $f \in A$ is not a zero divisor. Hence, the last relation holds for any f in a nonempty Zariski open subset of A (for example, if $\tilde{f} \in \mathbb{F}[x]$ has a nonzero constant term, then the image of $\tilde{f}$ under the projection $\mathbb{F}[x] \to \mathbb{F}[x]/(x^p) = A$ is not a zero divisor in A). Since the set of elements $f \in A$ for which our relation fails is also open, it is empty because any two nonempty Zariski open subsets of an affine space over an infinite field nontrivially overlap, and the field $\overline{\mathbb{F}}$ is infinite (even if $\mathbb{F}$ is finite). Thus, the relation holds for any $f \in A$, which proves statement (b).

3. Three combinatorial theorems. In this section, we state Theorems 2, 3, and 4 and show that each of them implies Theorem 1(c) and that Theorems 2 and 3 are equivalent to each other and imply Theorem 4.

First, we consider arbitrary finite words in a two-letter alphabet (∂, f) ending with f. (We do not specify the nature of f and ∂; for example, f can be a C^∞ function in one variable and ∂ the derivative.) By virtue of the standard differentiation rules, such a word can be represented as an integral linear combination of differential monomials $f^{(k_1)} \cdots f^{(k_m)}$. For example, $\partial f \partial\partial f = (ff'')' = f'f'' + ff'''$.

Theorem 2.

$$(\partial f)^{p-1} \equiv -\partial^{p-1} f^{p-1} \bmod p$$

for any prime p.

Example.

$$(\partial f)^4 = \partial f\partial f\partial f\partial f = (f')^4 + 11f(f')^2f'' + 4f^2(f'')^2 + 7f^2f'f''' + f^3f^{(4)},$$
$$\partial^4 f^4 = 24(f')^4 + 144f(f')^2f'' + 36f^2(f'')^2 + 48f^2f'f''' + 4f^3f^{(4)}.$$

We see that $(\partial f)^4 \equiv -\partial^4 f^4 \bmod 5$, as stated in the theorem.

Theorem 2 (together with Theorems 1(a), (b)) implies Theorem 1(c). Indeed, take $f \in \mathbb{F}[x]$ and $\partial = d/dx$ and project the relation $(\partial f)^{p-1} = -\partial^{p-1} f^{p-1}$ (which holds if $\operatorname{char}\mathbb{F} = p$) to A.

Theorem 2 can be restated in the form of a congruence for symmetric polynomials as follows.

Theorem 3. *In $\mathbb{Z}[t_1, \dots, t_{p-1}]$ we have*

$$\sum_{\sigma \in S_{p-1}} t_{\sigma(1)}(t_{\sigma(1)} + t_{\sigma(2)}) \cdots (t_{\sigma(1)} + \cdots + t_{\sigma(p-1)}) \equiv (t_1 + \cdots + t_{p-1})^{p-1} \bmod p,$$

where p is a prime as usual.

(There is no minus sign in this congruence, this is not a misprint!)

Obviously, if

$$t_1(t_1 + t_2) \cdots (t_1 + \cdots + t_{p-1}) = \sum n_{k_1 \dots k_{p-1}} t_1^{k_1} \cdots t_{p-1}^{k_{p-1}},$$

then

$$\partial f_{p-1} \partial f_{p-2} \cdots \partial f_1 = \sum n_{k_1 \dots k_{p-1}} f_1^{(k_1)} \cdots f_{p-1}^{(k_{p-1})}.$$

Similarly, if

$$(t_1 + \cdots + t_{p-1})^{p-1} = \sum m_{k_1 \dots k_{p-1}} t_1^{k_1} \cdots t_{p-1}^{k_{p-1}},$$

then

$$\partial^{p-1}(f_1 \cdots f_{p-1}) = \sum m_{k_1 \dots k_{p-1}} f_1^{(k_1)} \cdots f_{p-1}^{(k_{p-1})}.$$

Hence, the congruence in Theorem 3 is equivalent to

$$\sum_{\sigma\in S_{p-1}} \partial f_{\sigma(p-1)}\partial f_{\sigma(p-2)}\cdots\partial f_{\sigma(1)} \equiv \partial^{p-1}(f_1\cdots f_{p-1}) \bmod p.$$

After substituting $f_1 = \cdots = f_{p-1} = f$, this becomes

$$(p-1)!\,(\partial f)^{p-1} \equiv \partial^{p-1} f^{p-1} \bmod p$$

(the last two congruences are in fact equivalent). Since $(p-1)! \equiv -1 \bmod p$, the last congruence follows from Theorem 2. Thus, Theorems 2 and 3 are equivalent.

Our last combinatorial theorem concerns a certain function on Young diagrams. To avoid drawing, we use the term *Young diagram* for a finite sequence $(j_1,\dots,j_m)$ of integers with $j_1 \geqslant \cdots \geqslant j_m > 0$. The sequence can be empty ($m = 0$). For a Young diagram $J = (j_1,\dots,j_m)$, we set $N(J) = j_1 + \cdots + j_m$, $m(J) = m$, and $n_k(J) = \#\{s \mid j_s = k\}$. Define the function d on the Young diagrams recursively: $d(\varnothing) = 1$, and, if $J = (j_1,\dots,j_m)$, $N(J) = N$, and the values $d(K)$ are already defined for all Young diagrams K with $N(K) = N-1$, then

$$d(J) = \sum_{s, j_s > j_{s+1}} (N - j_s + 1) n_{j_s}(J) d(j_1,\dots,j_{s-1}, j_s - 1, j_{s+1},\dots,j_m).$$

(Here we set $j_{m+1} = 0$, and if $s = m$ and $j_s = 1$, then $j_s - 1$ is zero, and we simply delete this zero.)

Theorem 4. *If $N(J) = p-1$ (where p is a prime), then*

$$d(J) \equiv 1 \bmod p.$$

Examples.

$$\begin{aligned}
d(\varnothing) &= 1;\\
d(1) &= 1\cdot 1\cdot d(\varnothing) = 1;\\
d(1,1) &= 2\cdot 2\cdot d(1) = 4, \quad d(2) = 1\cdot 1\cdot d(1) = 1;\\
d(1,1,1) &= 3\cdot 3\cdot d(1,1) = 36, \quad d(2,1) = 2\cdot 1\cdot d(1,1) + 3\cdot 1\cdot d(2) = 11,\\
&\quad d(3) = 1\cdot 1\cdot d(2) = 1;\\
d(1,1,1,1) &= 4\cdot 4\cdot d(1,1,1) = 576, \quad d(2,1,1) = 3\cdot 1\cdot d(1,1,1) + 4\cdot 2\cdot d(2,1) = 196,\\
&\quad d(2,2) = 3\cdot 2\cdot d(2,1) = 66, \quad d(3,1) = 2\cdot 1\cdot d(2,1) + 4\cdot 1\cdot d(3) = 26,\\
&\quad d(4) = 1\cdot 1\cdot d(3) = 1.
\end{aligned}$$

We see that, if $N(J) = 2$, then $d(J) = 4, 1 \equiv 1 \bmod 3$, and if $N(J) = 4$, then $d(J) = 576, 196, 66, 26, 1 \equiv 1 \bmod 5$.

Theorem 4 is equivalent to Theorem 2 restricted to the case in which f is a monic polynomial of degree $p-1$ (this special case of Theorem 2 is sufficient to prove Theorem 1(c)).

Indeed, let $f(x) = (x-\alpha_1)\cdots(x-\alpha_{p-1})$ (where $\alpha_1,\dots,\alpha_{p-1} \in \overline{\mathbb{F}}$). We set $x - \alpha_i = u_i$; thus, $f = u_1\cdots u_{p-1}$ and $\partial u_i = 1$. Let $n \leqslant p-1$. Then $(\partial f)^n = \partial f \partial f \cdots \partial f$ is a symmetric polynomial in $u_1,\dots,u_{p-1}$ of total degree $n(p-2)$ and of degree $\leqslant p-1$ with respect to each variable u_i. Let $J = (j_1,\dots,j_m)$ be a Young diagram with $N(J) = n$. Then an obvious induction based on the relation $(\partial f)^n = \partial(u_1\cdots u_{p-1}(\partial f)^{n-1})$ shows that the coefficient at

$$u_1^{n-j_1}\cdots u_m^{n-j_m} u_{m+1}^n \cdots u_{p-1}^n$$

in the polynomial $(\partial f)^n$ is $d(J)$.

On the other hand, the coefficient at the same monomial in the polynomial $\partial^n(f^n)$ is

$$\frac{n!}{j_1!\cdots j_m!}\prod_{i=1}^{m} n(n-1)\cdots(n-j_i+1) = \frac{n!}{j_1!\cdots j_m!}\,\frac{n!}{(n-j_1)!}\cdots\frac{n!}{(n-j_m)!} = n!\binom{n}{j_1}\cdots\binom{n}{j_m}.$$

Since $(p-1)! \equiv -1 \bmod p$ and $\binom{p-1}{j} \equiv (-1)^j \bmod p$, the last quantity for $n = p-1$ is equal to

$$(p-1)!\binom{p-1}{j_1}\cdots\binom{p-1}{j_m} \equiv (-1)\cdot(-1)^{j_1}\cdots(-1)^{j_m} \bmod p,$$

and $(-1)\cdot(-1)^{j_1}\cdots(-1)^{j_m} = (-1)^p = -1$ (if p is odd; if $p = 2$, then $-1 \equiv 1 \bmod p$). Thus, Theorem 2 for $f = u_i \cdots u_{p-1}$ is equivalent to Theorem 4.

We conclude this section with three remarks concerning Theorem 4. First, we do not mention this theorem below; certainly, it follows from the other theorems of this section, but we have no direct proof of it. Nevertheless, we think that it deserves to be stated as one of the results of the paper. Second, this theorem can have some meaning in the representation theory of symmetric groups, but this meaning evades us. Third, it is not hard to derive from Theorem 4 that the congruence $d(J) \equiv 1 \bmod p$ holds for $N(J) = p-2$ as well (one can proof this fact for $p = 3$ and 5 by using the example after the statement of Theorem 4).

4. Proofs. Let us now prove Theorem 3 (by using its relationships to propositions similar to Theorems 1 and 2). As we know, this will imply the other theorems of the paper.

Let $\widetilde{W} = \operatorname{Der}\mathbb{F}[x]$. This is an infinite-dimensional restricted Lie algebra. The elements of $\widetilde{W}$ are "vector fields" $f\partial$, $f \in \mathbb{F}[x]$. The pth power of a derivation $f\partial$ is also a derivation, $(f\partial)^p = F\partial$, $F \in \mathbb{F}[x]$. Raising $f\partial$ to the power p, we obtain

$$F_1\partial + F_2\partial^2 + \cdots + F_p\partial^p = F\partial$$

(where $F_1 = f\cdot(\partial(f\partial(\cdots(f\partial f)\cdots)))$ and $F_p = f^p$). Applying this relation to $(x-a)^k$, where $1 < k < p$ and $a \in \overline{\mathbb{F}}$, and then setting $x = a$, we obtain

$$F_k(a)\cdot k! = 0,$$

which shows that $F_2 = \cdots = F_{p-1} = 0$. Since $\partial^p = 0$ on $\mathbb{F}[x]$, we see that

$$F = F_1 = fg, \qquad g = (\partial f)^{p-1} = \partial f \partial f \cdots \partial f.$$

But $[(f\partial)^{[p]}, f\partial] = 0$; hence, $[fg\partial, f\partial] = (fgf' - ff'g - f^2g')\partial = -f^2g'\partial = 0$, i.e., $g' = 0$ (for $f \neq 0$, and therefore for any f). (Actually, this means that g is a polynomial in x^p, but we do not need this fact.)

Consider the differential expression

$$g(f) = \partial\partial f \partial f \cdots \partial f \quad (p\ \partial\text{'s},\ p-1\ f\text{'s}).$$

Polarize the restriction of the form $f \mapsto (g(f))(a)$, $a \in \overline{\mathbb{F}}$, of degree $p-1$ to the vector space of polynomials of degree $< p$. We obtain a symmetric $(p-1)$-linear form

$$G(f_1, \ldots, f_{p-1}) = \sum_{\sigma\in S_{p-1}} (\partial\partial f_{\sigma(1)}\partial f_{\sigma(2)}\cdots\partial f_{\sigma(p-1)})(a),$$

which is equal to 0, since $g'(f) = 0$. The right-hand side of the last relation, regarded as a differential expression, is a linear combination of monomials $f_1^{(j_1)}f_2^{(j_2)}\cdots f_{p-1}^{(j_{p-1})}(a)$ with $j_1 + \cdots + j_{p-1} = p$. However, setting $f_1 = (x-a)^{i_1}, \ldots, f_{p-1} = (x-a)^{i_{p-1}}$ for any $i_1, \ldots, i_{p-1}$ between 0 and $p-1$ and equating the results to 0, we see that the monomials with $j_1 < p, \ldots, j_{p-1} < p$ have zero coefficients in $\mathbb{F}$ (i.e., they are 0 modulo p). Since the coefficient at $f_1 \ldots f_{s-1}f_s^{(p)}f_{s+1}\ldots f_{p-1}$ is obviously equal to $(p-2)! \equiv 1 \bmod p$, we arrive at the following conclusion:

$$\sum_{\sigma\in S_{p-1}} \partial\partial f_{\sigma(1)}\cdots\partial f_{\sigma(p-1)} \equiv \sum_{s=1}^{p-1} f_1\cdots f_{s-1}f_s^{(p)}f_{s+1}\cdots f_{p-1} \bmod p,$$

which can be rewritten as

$$\sum_{\sigma\in S_{p-1}} t_{\sigma(1)}(t_{\sigma(1)} + t_{\sigma(2)})\cdots(t_{\sigma(1)} + \cdots + t_{\sigma(p-1)})(t_1 + \cdots + t_{p-1}) \equiv t_1^p + \cdots + t_{p-1}^p \bmod p$$

(the last factor on the left-hand side of the last formula comes from the first ∂ on the left-hand side of the previous formula). However, $t_1^p+\cdots+t_{p-1}^p \equiv (t_1+\cdots+t_{p-1})^p \bmod p$. Canceling $t_1+\cdots+t_{p-1}$, we obtain the congruence of Theorem 3.

References

1. N. Jacobson, Lie Algebras, Dover Publications, Inc., New York, 1979.

Humboldt State University, Arcata, USA
e-mail: te8@humboldt.edu
University of California, Davis, USA
e-mail: fuchs@math.ucdavis.edu

Translated by T. J. Evans and D. B. Fuchs