TORSION IN ENGEL MODULES¹

ROBERT L. DAVIS

The original motive for studying Lie rings with Engel condition stemmed from Burnside's problem. The restricted Burnside hypothesis (that any group of exponent p on q generators has finite lower central series [8]) could be established for prime p by showing that any Lie nil ring of a certain kind on q generators is actually nilpotent. It is not known whether this sufficient condition is also necessary; nevertheless, there are advantages in treating the problem within the context of Lie rings.

Transition from the group problem to the Lie-ring problem is set up by the Magnus representation. This maps the q group generators into the q generators of the Lie ring, while the significance in the Lie ring of the group's having exponent p appears in two known ways. One is that, since the Magnus representation takes products into sums, the Lie ring must have $pf=0$ for every element f . The other lies deeper, and requires for the Lie ring that if f and g are any elements of L then $[f, g^{p-1}] = [\dots [[f, g], g], \dots, g] = 0$ (the bracket denotes Lie multiplication; there are $p-1$ g 's on the right). Because Engel's theorem (for Lie *algebras*) begins with such an assumption, a condition like this is called an *Engel condition of exponent p* (though some writers prefer "exponent $p-1$ ").

In actual computations it is not enough to know that each $[f, g^{p-1}] = 0$. The information needed is that all of what will here be called S_μ 's, the "strongly homogeneous parts" of the polynomials $[f, g^{p-1}]$, are also zero. Over a field, as in computations directly bearing on Burnside's problem, a standard Vandermonde determinant argument shows that indeed, if all $[f, g^{p-1}] = 0$, then also all such $S_\mu = 0$. When the scalars may not admit division this is no longer necessarily so.

The important role of the Engel condition in such computations has led to creation of an independent area of study in groups and rings subjected to an Engel condition (see, e.g., [4; 6]). To study the condition by itself, apart from the other consequence ($pf=0$) of assuming exponent p in the Burnside group, one may begin with a

Presented to the Society, December 29, 1956 under the title *Torsion structure in Engel modules of arbitrary exponent*; received by the editors January 14, 1959.

¹ This paper is taken from Chapter III of my doctoral dissertation, University of Michigan, 1956. I wish to again thank Professors R. M. Thrall and R. C. Lyndon for their generous counsel and many valuable suggestions. In some of this work I was supported by a National Science Foundation grant, NSF-G2371.

free Lie Z -module (Z the rational integers) and "divide out" all the terms annihilated by the Engel condition. I will later call the quotient thus attained an *Engel module of exponent p* (dropping the restriction that p be prime). Before then we must determine just what ideal we should divide out in order to get the Engel module.

One approach here is to take the ideal generated by all $[f, g^{p-1}]$ and then to adduce such hypotheses, ad hoc, as will give the needed conclusion that all $S_\mu = 0$. This is essentially the path followed by P. J. Higgins [6] in a very interesting paper whose first part lies close to the subject of this one. Higgins assumed that the "characteristic" of the Lie ring was "prime to" $(p-2)!$.

The work reported in this paper was stimulated by direct computations over the rational integers based on assuming all $S_\mu = 0$. For the special case $p=5$, $q=2$, the Engel condition alone (in this strong form: all $S_\mu = 0$) guarantees most of the 5-torsion: for forms of degree seven or higher, $5f=0$ for all f [1; 3]. Thus for my own concept of Engel module I was led to divide out all S_μ from the start.

This paper investigates torsion in Engel modules of exponent m (not necessarily prime) and shows that whenever $m=p^s$ is a prime power there is necessarily some p -torsion. Thus in any such case there is at least some resemblance, in torsion, to the special case $p=5$, $q=2$, where the Engel condition alone is enough to guarantee the ultimate nilpotency.

1. Preliminaries. Let L be the free Lie Z -module generated by $x_1, \dots, x_q$, with multiplication written $[,]$. All relations in L are consequences of the defining properties of Lie rings:

- (1) $[f, g] + [g, f] = 0$ (skew commutativity);
- (2) $[[f, g], h] + [[g, h], f] + [[h, f], g] = 0$ (Jacobi identity).

Whenever possible we will deal in *normed forms*. These are built up by multiplying by generators on the right, so that in ordinary notation all the left-hand brackets would appear at the beginning. A standard notation for these sets

$$[x_{i_1} x_{i_2} x_{i_3} \cdots x_{i_r}] = [\cdots [[x_{i_1}, x_{i_2}], x_{i_3}], \cdots, x_{i_r}].$$

In cases where Lie forms are not given in normed form we will use commas and brackets to prevent misunderstanding.

Now if the ideal generated by all elements $[f, g^{m-1}]$, for some fixed m , were what has been called strongly homogeneous [9] we could define "Engel module" very simply as the quotient of a Lie ring by such an ideal. Since it is not, the definition will take two steps.

DEFINITION A. Let L be the free Lie Z -module on noncommutative generators $x_1, \dots, x_q$, and let $s > 2$ be an integer. A *strongly*

homogeneous Engel polynomial of exponent s is any polynomial $S_\mu(z; y_1, \dots, y_r)$ which is the sum of all formally distinct normed forms beginning with z and of degrees $\mu_1, \dots, \mu_r$ in $y_1, \dots, y_r$; (μ) is any solution in non-negative integers of the equation $\mu_1 + \mu_2 + \dots + \mu_r = s - 1$. Thus any S_μ can be picked out as the polynomial whose coefficient is $c_1^{\mu_1} c_2^{\mu_2} \dots c_r^{\mu_r}$ in the formal expansion

$$[z, (c_1 y_1 + \dots + c_r y_r)^{s-1}] = \sum_{(\mu)} c_1^{\mu_1} \dots c_r^{\mu_r} S_\mu(z; y_1, \dots, y_r).$$

Two strongly homogeneous Engel polynomials of exponent 5, for example, are $S_{(31)}(z; x, y) = [zx^3y] + [zx^2yx] + [zxyx^2] + [zyx^3]$, and $S_{(1^5)}(z; y_1, \dots, y_5)$ which is a sum of $5!$ terms of the form

$$[zy_1 y_2 y_3 y_4 y_5].$$

DEFINITION B. Let L be any free Lie Z -module. The *Engel ideal*, I , of exponent m in L is the ideal generated by all Lie elements $S_\mu(f; g_1, \dots, g_r)$ derived by substituting Lie forms $f, g_1, \dots, g_r$ for $z, y_1, \dots, y_r$ in any strongly homogeneous Engel polynomial of exponent $s = m$. The *Engel Z -module $E(m, q)$ of exponent m on q generators* is then the quotient module L/I .

Because I is strongly homogeneous we can not only write L and E as direct sums $L = L_1 \oplus L_2 \oplus \dots$ and $E = E_1 \oplus E_2 \oplus \dots$ of submodules L_n and E_n of homogeneous polynomials of degree n , but can further split each of these into direct sums of submodules homogeneous in each of the generators. There is thus a submodule $L_{(\nu)}$ or $E_{(\nu)}$ for each ordered partition of any integer n into q non-negative parts. The rank of each $L_{(\nu)}$ is known from Witt's formulas [10]. In principle one could write down a basis for any $L_{(\nu)}$ (using the process given by Marshall Hall [5], for instance) and then cut down to $E_{(\nu)}$ by using what may be called the " I -identities"; that is, all consequences of dividing out the ideal I . There are, of course, very few cases in which such a detailed procedure is practicable.

The special results which led me to suspect the general existence of torsion in these modules were these.

FACT [1; 3]. In the Engel Z -module $E = E(5, 2)$ of exponent 5 on 2 generators the submodule E_6 is free, E_8 is mixed, and $5E_7 = 0$. Hence for any f of degree seven or higher in $E(5, 2)$, $5f = 0$, and in fact Kostrikin's computations [7] for $L(5, 2)$ with Engel condition over Z_5 can be used to show $E_{13} = 0$.

FACT [2; 3]. In any Engel module $E(4, q)$ of exponent 4 all submodules of type $E_{(2^2)}$ are additively isomorphic to Z_2 , all of type $E_{(21^2)}$ to $Z_2 \oplus Z$, and all of type $E_{(1^4)}$ to $Z_2 \oplus Z_2 \oplus Z \oplus Z \oplus Z$.

The computations which establish these facts cover some ten pages of my dissertation with equations: I will not include them here. Among the mathematicians I informed of this result the only one who seems to have considered the possibility of torsion in such modules before was Michel Lazard. He wrote back to say that he had discovered torsion in submodules of forms of degree p equal to the exponent of the module. Although I am not certain how he defined his modules, I would suppose this (unpublished) result of his to be given by the following.

FACT (LAZARD). In any $E = E(p, q)$ with prime exponent and $q \geq 3$ there is some p -torsion in the submodule E_p .

I will establish a generalization of this in the theorem below.

2. Two numerical lemmas. The following p -modular properties of certain binomial coefficients are conclusive in settling several questions about torsion in modules $E(m, q)$. I do not know of a statement of either one in the literature.

LEMMA 1. *Let $n > 2$ be an integer and p any prime. If $(-1)^k C_{n-1, k} \equiv 1 \pmod{p}$ for each k with $1 \leq k \leq n-2$, then n must be a power of p .*

PROOF. Write $n = p^r q > 2$ with $r \geq 0$, $p \nmid q$. We will show that supposing $q > 1$ leads to a contradiction.

First we see that we must have $r > 0$. For when $k = 1$ the hypothesis requires $-C_{n-1, 1} \equiv 1 \pmod{p}$, so that $p \mid n$.

Now if $q > 1$ then $1 < p^r < n-1$. Hence both p^r and $(p^r - 1)$ will in this case be among the values of k limited by the hypothesis, so that both:

$$(-1)^{p^r} C_{n-1, p^r} \equiv 1 \pmod{p}, \quad (-1)^{p^r-1} C_{n-1, p^r-1} \equiv 1 \pmod{p}.$$

But since

$$(-1)^{p^r} C_{n-1, p^r} = (-1) [(-1)^{p^r-1} C_{n-1, p^r-1}] \frac{n - p^r}{p^r}$$

we see from $n = p^r q$ that $-(n - p^r)/p^r = -(q - 1) \equiv 1 \pmod{p}$. In that event, $p \mid q$; this contradicts the assumption on q .

LEMMA 2. *If $n = p^r > 1$ for any prime p , then for each k with $1 \leq k \leq n-2$: $(-1)^k C_{n-1, k} \equiv 1 \pmod{p}$. On the other hand, there is a k in this range with $(-1)^k C_{n/1, k} \not\equiv 1 \pmod{p^2}$.*

PROOF. First, write the binomial coefficient as a product: $C_{n-1, k} = \prod (n-t)/t$. For each t here we have $n-t \equiv -t \pmod{p^r}$. Now write $n-t = n_s p^s$ with $(n_s, p) = 1$, and $t = t_u p^u$ with $(t_u, p) = 1$. The

congruence mod p^r of $n-t$ and $-t$ then shows that $s=u$ and furthermore that $n_s \equiv -t_s \pmod{p^{r-s}}$.

Since $r-s \geq 1$ for all t this shows that each of the k quotients in the product expression for the binomial coefficient is congruent mod p to -1 . Thus multiplying by $(-1)^k$ makes it congruent to $1 \pmod{p}$.

As for the further conclusion, observe that for $k \leq p^{r-1} - 1$ we have $r-s \geq 2$ for each $t \leq k$. Hence when $k = p^{r-1} - 1$ we may even conclude that $n_s \equiv -t_s \pmod{p^2}$, so that for this k , $(-1)^k C_{n-1,k} \equiv 1 \pmod{p^2}$. But for the next following coefficient we have

$$(-1)^{k+1} C_{n-1,k+1} = (-1)[(-1)^k C_{n-1,k}] \frac{n - (k+1)}{k+1}.$$

Since the term inside the large bracket is congruent mod p^2 to 1 this yields

$$\frac{n - (k+1)}{k+1} = \frac{p^r - p^{r-1}}{p^{r-1}} = p - 1 \not\equiv -1 \pmod{p^2},$$

and so we see that $(-1)^{k+1} C_{n-1,k+1} \not\equiv 1 \pmod{p^2}$ when $k+1 = p^{r-1} < n-2$.

3. Structure of $E_{(n-2,1^2)}$. Consider the submodule E_n of forms of degree n in a module of exponent n ($m=n$), and suppose $q > 2$. We look for torsion in those submodules of E_n in which all forms have degree $n-2$ in one generator (say x) and degree 1 in each of two others (say y and z).

The dimension of $L_{(n-2,1^2)}$ is $n-1$, and this free Lie submodule has a set of independent generators:

$$P_k = [yx^kzx^{r-k}], \quad 0 \leq k \leq r = n-2.$$

(It will be convenient to write r for $n-2$ now.) Naturally, these forms also generate $E_{(r,1^2)}$, although they are no longer independent there. We will also want special names for the forms symmetric to these:

$$Q_k = [zx^k yx^{r-k}], \quad 0 \leq k \leq r.$$

To see what I -identities may hold here we first observe that because of the degree restriction the only Lie elements we can use for the f , $g_1, \dots, g_r$ of Definition B are the generators themselves. The further restriction to degree-type $(r, 1^2)$ means that once we have chosen which generator to use for f we have completely determined all the others.

Thus there are only three I -identities available here. We can say

that $E_{(r,1^2)}$ has generators $P_0, \dots, P_r$ and defining relations given by (the Lie-Jacobi identities and)

$$(3) \quad S_{(r,1)}(y; x, z) = \sum_{k=0}^r P_k \equiv 0 \pmod{I};$$

$$(4) \quad S_{(r,1)}(z; x, y) = \sum_{k=0}^r Q_k \equiv 0 \pmod{I};$$

$$(5) \quad S_{(r-1,1^2)}(x; x, y, z) \equiv 0 \pmod{I}.$$

LEMMA 3. $S_{(r-1,1^2)}(x; x, y, z) = -[\sum_0^r P_k + \sum_0^r Q_k]$ in the Lie ring. Hence, taken with (3) and (4), (5) is redundant.

PROOF. The left side of (5) is a sum of normed forms beginning with x . Hence its only nonzero terms are those in which the second entry is y or z . For such terms we observe that

$$[xyz^kzx^{r-1-k}] = -[yx^{k+1}zx^{r-1-k}] = -P_{k+1},$$

and likewise $[xzx^kyx^{r-1-k}] = -Q_{k+1}$. Furthermore, all the P 's and Q 's except P_0 and Q_0 appear on the left side of (5) so that the equation of the lemma would hold if we added $P_0 + Q_0$ to the right side. But since $P_0 = -Q_0$ this establishes that equation itself.

Now to make the most economical use of the identities (3) and (4) we first express the sum of the Q 's in terms of the P 's. The equation here was established by Higgins [6] (and see also [3]).

$$(6) \quad \sum_{k=0}^r Q_k = \sum_{i=0}^r (-1)^{i+1} C_{r+1,i+1} P_i.$$

We also use (3) to eliminate P_r , leaving the $r=n-2$ generators $P_0, \dots, P_{r-1}$. The only possible remaining relation is that given by (4), which we now rewrite as

$$(7) \quad \sum_{i=0}^{r-1} [(-1)^{i+1} C_{r+1,i+1} + (-1)^n] P_i \equiv 0 \pmod{I}.$$

This comes from (6) using the fact that the coefficient of P_r there is $(-1)^{r+1} = (-1)^{n-1}$; thus after solving for P_r the contribution from P_r to the coefficient of any P_i is $(-1)(-1)^{n-1}$.

With this we have all that is needed to establish the following.

THEOREM. Let $E = E(n, q)$, $q > 2$. (i) If $n = p^s$ is a prime power then each submodule of type $(n-2, 1^2)$ has the additive structure of $Z_p \oplus Z \oplus \dots \oplus Z$, with $n-3$ copies of Z . (ii) If n has two or more distinct prime factors then the additive structure of any $E_{(n-2,1^2)}$ is that of the free abelian group of rank $n-3$.

PROOF. If we write a_i for the coefficient of P_i in (7) it follows that $E_{(n-2,1^2)}$ has type $Z_a \oplus Z \oplus \cdots \oplus Z$ ($n-3$ copies of Z) where a is the greatest common divisor of the a_i .

If $n = p^s$, Lemma 1 tells us first that there is no prime factor q of a other than p , so that the greatest common divisor a must be p^t for some t . But since Lemma 2 tells us that $p^2 \nmid a$ we must have $a = p$.

If $n \neq p^s$ for any p or s then $a = 1$. For if any $q \mid a$ Lemma 1 tells us that $n = q^s$ is a prime power. In this case the module has type $0 \oplus Z \oplus \cdots \oplus Z$ ($n-3$ Z 's).

REFERENCES

1. R. L. Davis, *Torsion in Engel modules*, Bull. Amer. Math. Soc. Abstract 62-6-605.
2. ———, *Torsion structure in Engel modules of arbitrary exponent*, Bull. Amer. Math. Soc. Abstract 63-2-158.
3. ———, *Lie and Engel modules and their relation to Burnside's problem*, Doctoral Dissertation, University of Michigan, 1956.
4. K. W. Gruenberg, *Two theorems on Engel groups*, Proc. Cambridge Philos. Soc. vol. 49 (1953) pp. 377-380.
5. Marshall Hall, *A basis for free Lie rings and higher commutators in free groups*, Proc. Amer. Math. Soc. vol. 1 (1950) pp. 575-581.
6. P. J. Higgins, *Lie rings satisfying the Engel condition*, Proc. Cambridge Philos. Soc. vol. 50 (1954) pp. 8-15.
7. A. L. Kostrikin, *Solution of the restricted Burnside problem for the exponent 5*, Izv. Akad. Nauk USSR vol. 19 (1955) pp. 233-244 (in Russian).
8. R. C. Lyndon, *On Burnside's problem I*, Trans. Amer. Math. Soc. vol. 77 (1954) pp. 202-215.
9. R. M. Thrall, *On symmetrized Kronecker powers and the structure of the free Lie ring*, Amer. J. Math. vol. 64 (1942) pp. 371-388.
10. E. Witt, *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. vol. 177 (1937) pp. 152-160.

UNIVERSITY OF MICHIGAN AND
UNIVERSITY OF VIRGINIA