BULL. AUSTRAL. MATH. SOC. 17B99, 20D15
VOL. 19 (1978), 11-28.

On the Lie ring of a group of prime exponent II

G.E. Wall

Let p be a prime number. The Lie ring of the largest finite group of exponent p and nilpotency class $3p - 3$ is determined under certain assumptions (which are conjectured always to hold).

1. Introduction

1.1. The present paper, like its predecessor [8], is concerned with the Lie ring $L(G)$ of a finite group G of prime exponent p. Certain results of the earlier paper for degree $2p - 1$ are extended, in part, up to degree $3p - 3$.

We first recall some of the background. Let $L(n)$ denote the free Lie algebra over $\mathbb{F}_p$ on n free generators $x_1, \ldots, x_n$ and let $z_1, z_2, \ldots$ be the basic Lie products in these generators. Let $E_{p-1}(n)$ denote the $(p-1)$th Engel ideal of $L(n)$. Then $E_{p-1}(n)$ is spanned by the elements

$$(1.1) \qquad \langle u_1, \ldots, u_p \rangle ,$$

where $u_1, \ldots, u_p \in L(n)$ ([8], §§3.1, 3.4). Further, since (1.1) is a symmetric, multilinear function which vanishes when its p arguments are all equal, $E_{p-1}(n)$ is even spanned by the elements

$$(1.2) \quad \langle m_1z_1, m_2z_2, \ldots \rangle = (m_1!m_2! \ldots)^{-1}\langle \underbrace{z_1, \ldots, z_1}_{m_1 \text{ terms}}, \underbrace{z_2, \ldots, z_2}_{m_2 \text{ terms}}, \ldots \rangle ,$$

Received 11 May 1978. The financial support of the Australian Research Grants Committee is gratefully acknowledged.

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

where

(1.3) $$0 \le m_i < p \quad (i = 1, 2, \ldots) \ , \quad \sum m_i = p \ .$$

It is conjectured that, for $p \le d \le 2p-2$, those elements (1.2) which have total degree d in $x_1, \ldots, x_n$ are linearly independent[1]; and this has been confirmed[2] in the case where $n = 2$ and $d \le p+4$.

The quotient algebra

$$\Lambda(n) = L(n)/E_{p-1}(n)$$

has properties broadly analogous to those of $\Lambda(n)$. Let $\xi_1, \ldots, \xi_n$ and $\zeta_1, \zeta_2, \ldots$ denote the images of $x_1, \ldots, x_n$ and $z_1, z_2, \ldots$ in $\Lambda(n)$. Consider the elements

(1.4) $$\langle\langle \omega_1, \ldots, \omega_{2p-1} \rangle\rangle \ ,$$

where $\omega_1, \ldots, \omega_{2p-1} \in \Lambda(n)$ ([8], §3.3). The expression (1.4) is a symmetric, multilinear function of its arguments which vanishes when any p of them are equal. Thus, the subspace spanned by the elements (1.4) is already spanned by the elements

(1.5) $$\langle\langle m_1\zeta_1, m_2\zeta_2, \ldots \rangle\rangle = \left(m_1!m_2! \ldots\right)^{-1} \langle\langle \underbrace{\zeta_1, \ldots, \zeta_1}_{m_1 \text{ terms}}, \underbrace{\zeta_2, \ldots, \zeta_2}_{m_2 \text{ terms}}, \ldots \rangle\rangle \ ,$$

where

(1.6) $$0 \le m_i < p \quad (i = 1, 2, \ldots) \ , \quad \sum m_i = 2p - 1 \ .$$

Now, if $B(n)$ denotes the n-generator free group of the variety of all groups of exponent dividing p, there is an isomorphism of graded Lie $\mathbf{F}_p$-algebras of the form

[1] Holenweg ([3], Satz 3.13, and [4], Hauptsatz 9) claims to prove an equivalent group-theoretical result, but the proof seems incomplete. For example, the definition of the mapping σ on p. 193 of [3] is quite unclear.

[2] Kostrikin [5], Theorem 5. As Kostrikin shows, the elements (1.2) of degree greater than $2p - 2$ are linearly *dependent*.

$$(1.7) \qquad L(B(n)) \cong \Lambda(n)/\Sigma(n)$$

([8], §1). Let $\Sigma_r(n)$ denote the homogeneous component of $\Sigma(n)$ of degree r. By Theorem A of [8], §4.1, $\Sigma_{2p-1}(n)$ is spanned by those elements (1.5) of total degree $2p-1$ in $\xi_1, \ldots, \xi_n$. It then follows from Proposition 7 of [8] that *all* elements (1.5) are in $\Sigma(n)$. I shall prove the following result.

THEOREM 1. *Let d be an integer such that $2p-1 \le d \le 3p-3$. Assume that those elements (1.2) which have total degree $d-p+1$ in $x_1, \ldots, x_n$ are linearly independent. Then $\Sigma_d(n)$ is spanned by elements (1.5).*

As an application of Theorem 1, we determine, in §4, a set of ideal generators of $\Sigma(n)$ in the special case $n = 2$, $p = 5$. This provides one way of verifying that the largest 2-generator finite group of exponent 5 has order 5^{34} (Havas, Wall, and Wamsley [2]).

1.2. The method of proof of Theorem 1 in fact yields a rather stronger, but less simply stated, result, which we now proceed to explain.

Let us consider an n-fold multi-index, that is, a row $\underline{\underline{m}} = (m_1, \ldots, m_n)$ of n non-negative integers. The *height* of $\underline{\underline{m}}$ is $|\underline{\underline{m}}| = m_1 + \ldots + m_n$. The *monomial function* associated with $\underline{\underline{m}}$ is the mapping $f_{\underline{\underline{m}}} : \mathbf{F}_p^n \to \mathbf{F}_p$ defined by $f_{\underline{\underline{m}}}(\lambda_1, \ldots, \lambda_n) = \lambda_1^{m_1} \ldots \lambda_n^{m_n}$. Write

$$\theta(\underline{\underline{m}}) = \{\underline{\underline{m}}' : |\underline{\underline{m}}'| = |\underline{\underline{m}}| \text{ and } f_{\underline{\underline{m}}'} = f_{\underline{\underline{m}}}\} .$$

We denote by $L(n)^{\underline{\underline{m}}}$ the subspace of $L(n)$ spanned by those monomials in $x_1, \ldots, x_n$ which have respective partial degrees $m_1, \ldots, m_n$ in these generators. We extend this notation to subspaces, U, and quotients of subspaces, U/V, by defining

$$U^{\underline{\underline{m}}} = U \cap L(n)^{\underline{\underline{m}}} , \quad (U/V)^{\underline{\underline{m}}} = (U^{\underline{\underline{m}}}+V)/V .$$

Finally, we write

$$(U/V)^{\theta(\underline{\underline{m}})} = \sum_{\underline{\underline{r}} \in \theta(\underline{\underline{m}})} (U/V)^{\underline{\underline{r}}} .$$

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

THEOREM 2. *Let* $\underline{\underline{m}}$ *be an* n*-fold multi-index such that* $2p-1 \le |\underline{\underline{m}}| \le 3p-3$. *Assume that, for each multi-index* $\underline{\underline{m}}'$ *satisfying* $f_{\underline{\underline{m}}'} = f_{\underline{\underline{m}}}$ *and* $|\underline{\underline{m}}'| = |\underline{\underline{m}}| - p + 1$ *, those elements* (1.2) *which lie in* $L(n)^{\underline{\underline{m}}'}$ *are linearly independent. Then* $\Sigma(n)^{\theta(\underline{\underline{m}})}$ *is spanned by elements* (1.5).

It is obvious that Theorem 2 implies Theorem 1. We note one case in which Theorem 2 takes a particularly simple form.

COROLLARY. *If* $\underline{\underline{m}}$ *is an* n*-fold multi-index which satisfies* $2p-1 \le |\underline{\underline{m}}| \le 3p-3$ *and* $m_i < p$ $(i = 1, 2, \ldots)$ *then* $\Sigma^{\underline{\underline{m}}}$ *is spanned by elements* (1.5).

(Let $\underline{\underline{m}}$ be as in the corollary and let $\underline{\underline{r}}$ be an arbitrary n-fold multi-index. It is easily seen that $f_{\underline{\underline{r}}} = f_{\underline{\underline{m}}}$ implies $r_i \ge m_i$ $(i = 1, 2, \ldots)$. Thus there are *no* $\underline{\underline{m}}'$ which satisfy the conditions in Theorem 2 and the set $\theta(\underline{\underline{m}})$ consists solely of the element $\underline{\underline{m}}$.)

We comment briefly on the term $\Sigma(n)^{\theta(\underline{\underline{m}})}$ in the enunciation of Theorem 2.

The n-fold multi-indices form a semigroup, Γ , under the usual addition of rows. Furthermore, the family

$$\left(L(n)^{\underline{\underline{m}}}\right)_{\underline{\underline{m}}\in\Gamma}$$

provides a Γ-grading of $L(n)$ in the sense that

$$L(n) = \bigoplus_{\underline{\underline{m}}\in\Gamma} L(n)^{\underline{\underline{m}}} ,$$

$$L(n)^{\underline{\underline{m}}} L(n)^{\underline{\underline{m}}'} \subseteq L(n)^{\underline{\underline{m}}+\underline{\underline{m}}'} \quad \text{for all } \underline{\underline{m}}, \underline{\underline{m}}' \in \Gamma .$$

We may call this the *formal* grading.

It can be verified that the equivalence classes $\theta(\underline{\underline{m}})$ form a quotient semigroup, Δ , of Γ and that the family

$$\left(L(n)^{\theta(\underline{\underline{m}})}\right)_{\theta(\underline{\underline{m}})\in\Delta}$$

defines a Δ-grading of $L(n)$. We shall call this the *functional* grading.

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

Now it can be shown that

$$\Lambda(n)/\Sigma(n) = \bigoplus_{\theta(\underline{\underline{m}})\in\Delta} \left(\Lambda(n)/\Sigma(n)\right)^{\theta(\underline{\underline{m}})} ,$$

that is $\Lambda(n)/\Sigma(n)$ *inherits the functional grading*; this is a fairly easy consequence of Proposition 6 of [8][3]. On the other hand, it is not known whether $\Lambda(n)/\Sigma(n)$ inherits the formal grading.

The proof of Theorem 2 occupies §§2 and 3. It is the same, in principle, as that of Theorem A in [8]. Because of this, our general policy will be to refer the reader to [8] for the basic ideas and procedures, merely indicating, for the most part, what modifications are necessary. This means, in particular, that we shall continue to use the same notation as in [8], often without specific comment.

2. Preparations

We are concerned in the present section with $A(n, c; \mathbb{Q})$ and its subring $A\left(n, c; \mathbb{Q}^0\right)$, where $\mathbb{Q}$ is the rational field and $\mathbb{Q}^0$ the ring of rational p-integers (see §2.1 of [8] for the relevant general definitions). We shall follow the special notation used in §§3.1-3.3 of [8], namely,

$$A = A(n, c; \mathbb{Q}) \ , \quad \underline{\underline{a}} = \underline{\underline{a}}(n, c; \mathbb{Q}) \ , \quad L = L(n, c; \mathbb{Q}) \ ,$$

$$A^0 = A\left(n, c; \mathbb{Q}^0\right) \ , \quad \underline{\underline{a}}^0 = \underline{\underline{a}}\left(n, c; \mathbb{Q}^0\right) \ , \quad L^0 = L\left(n, c; \mathbb{Q}^0\right) \ .$$

We express the Baker-Campbell-Hausdorff formula within A in the general form

$$e^{x_1} \ldots e^{x_n} = e^H , \tag{2.1}$$

where $H = H\left(x_1, \ldots, x_n\right) \in L$. The part played in [8] by the truncated exponential function $\sum_0^{p-1} x^m/m!$ is here taken by the *Artin-Hasse exponential function*

[3] More generally, in the notation of that proposition, if N is a fully invariant subgroup of F, then ${}_pL(F/N)$ inherits the functional grading.

$$(2.2) \qquad E(x) = \exp\left(\sum_0^\infty x^{p^i}/p^i\right) .$$

Since the coefficients in the power series expansion of $E(x)$ are in $\mathbb{Q}^0$ (see Dieudonné [1]), it follows that its general functional equation takes the form

$$(2.3) \qquad E(x_1) \ldots E(x_n) = E(V) ,$$

where

$$V = V(x_1, \ldots, x_n) \in A^0 .$$

The main result of the present section is Proposition 1, in which the terms of V of degree up to $2p - 2$ are determined. Its corollary expresses the same results in a form suitable for subsequent specialization to $A(n, c; \mathbb{F}_p)$.

2.1. LEMMAS

DEFINITION. Let δ denote the derivation of A such that $x_i\delta = x_i^p/p$ $(i = 1, \ldots, n)$.

LEMMA 1. $\left(L^0 \cap \underline{\underline{a}}^2\right)\delta \subseteq A^0 + L$.

The lemma is easily proved by induction, using the formula

$$\begin{aligned}\left[a^p, b\right] &= \langle (p-1)a, [a, b]\rangle \\ &= p!\left[(p-1)a, [a, b]\right] + [a, b, \underbrace{a, \ldots, a}_{p-1 \text{ terms}}] .\end{aligned}$$

DEFINITION. Let Δ denote a $\mathbb{Q}^0$-linear mapping of $L^0 \cap \underline{\underline{a}}^2$ into A^0 such that $\left(L^0 \cap \underline{\underline{a}}^2\right)(\delta-\Delta) \subseteq L$.

The existence of such a Δ is guaranteed by the lemma. If Δ' is another candidate, then

$$\left(L^0 \cap \underline{\underline{a}}^2\right)(\Delta'-\Delta) \subseteq A^0 \cap L = L^0 .$$

LEMMA 2. *Suppose* $p > 2$ *and let* ϕ *be an endomorphism of* A *which maps the set*

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

$$\{x_1, -x_1, \ldots, x_n, -x_n\}$$

into itself. Then

$$\left(L^0 \cap \underline{\underline{a}}^2\right)(\phi\Delta-\Delta\phi) \subseteq L^0 .$$

Proof. Let $u \in L^0 \cap \underline{\underline{a}}^2$. Since $\left(L^0 \cap \underline{\underline{a}}^2\right)\phi \subseteq L^0 \cap \underline{\underline{a}}^2$, it follows that $u\phi\Delta$ is defined and

(2.4) $$u(\phi\delta-\phi\Delta) \in L .$$

Also, since $L\phi \subseteq L$, we have

(2.5) $$u(\delta\phi-\Delta\phi) \in L .$$

A simple computation (using the assumption that $p > 2$) shows that $\phi\delta = \delta\phi$. Therefore (2.4) and (2.5) give

$$u(\phi\Delta-\Delta\phi) \in L .$$

Clearly, $u(\phi\Delta-\Delta\phi) \in A^0$, whence $u(\phi\Delta-\Delta\phi) \in A^0 \cap L = L^0$, as required.

We require a simple formal property of the function R defined in Lemma 2 of [8].

LEMMA 3. *If* $a_1, \ldots, a_s, b_1, \ldots, b_t, \ldots \in L^0$, *then*

$$R\left(a_1, \ldots, a_s, b_1, \ldots, b_t, \ldots\right) - R\left(\sum_1^s a_i, \sum_1^t b_i, \ldots\right)$$
$$\equiv R\left(a_1, \ldots, a_s\right) + R\left(b_1, \ldots, b_t\right) + \ldots \left(\operatorname{mod} L^0\right) .$$

We omit the easy proof.

2.2. FUNCTIONAL EQUATION FOR $E(x)$

In view of (2.1) and (2.2), the functional equation (2.3) for $E(x)$ is equivalent to

(2.6) $$\sum_0^\infty V^{p^i}/p^i = H\left(\sum_0^\infty x_1^{p^i}/p^i, \ldots, \sum_0^\infty x_n^{p^i}/p^i\right) .$$

Let $H_r = H_r\left(x_1, \ldots, x_n\right)$ and $V_r = V_r\left(x_1, \ldots, x_n\right)$ denote the homogeneous components of H and V of degree r. Comparing terms of like degree in (2.6), we get

(2.7) $$V_r = H_r \in A^0 \cap L = L^0 \quad (1 \le r \le p-1) .$$

PROPOSITION 1. *If* $c = 2p - 2$, *then*

$$V \equiv W \quad \left(\bmod L^0 \cap \underline{\underline{a}}^p\right) ,$$

where

$$W = H_1 + \left\{\sum_2^{p-1} H_r\right\}(1+\Delta) - (p-1)!R\left\{x_1, \ldots, x_n, \sum_2^{p-1} H_r\right\} .$$

Proof. Both V and W are in A^0 and, by (2.7), $V \equiv W \quad \left(\bmod \underline{\underline{a}}^p\right)$. It is therefore sufficient to prove that

(2.8) $$V \equiv W \quad (\bmod L) .$$

Now, since $c < 2p$, (2.6) becomes

(2.9) $$V + V^p/p = H\left\{x_1+x_1^p/p, \ldots, x_n+x_n^p/p\right\}$$
$$= H + H\delta .$$

Let $\equiv$ denote congruence modulo L and write $K = \sum_2^{p-1} H_r$. Then

(2.10) $$V^p = \left\{\sum_1^{p-1} V_r\right\}^p \quad (\text{since } c = 2p - 2)$$
$$= \left\{\sum_1^{p-1} H_r\right\}^p \quad \left(\text{by } (2.7)\right)$$
$$= \left\{\sum_1^n x_i+K\right\}^p$$
$$\equiv \sum_1^n x_i^p + K^p + p!R\left(x_1, \ldots, x_n, K\right) \quad (\text{by definition of } R)$$
$$= \sum_1^n x_i^p + p!R\left(x_1, \ldots, x_n, K\right) \quad (\text{since } c = 2p - 2).$$

Therefore

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

$$\begin{aligned} V &= H + H\delta - V^p/p \quad \{\text{by } (2.9)\} \\ &= H + \left\{\sum_1^{p-1} H_r\right\}\delta - V^p/p \quad (\text{as } c = 2p-2) \\ &\equiv K\Delta - \frac{1}{p}\left\{V^p - \sum_1^n x_i^p\right\} \\ &\equiv K\Delta - (p-1)!R(x_1, \ldots, x_n, K) \quad \{\text{by } (2.10)\} \\ &\equiv W . \end{aligned}$$

This proves (2.8) and the proposition.

COROLLARY. *Suppose $c = 2p - 2$. Let G denote the group generated by $E(x_1), \ldots, E(x_n)$. If $E(u) \in G$, then u has the form*

$$u = \sum_1^n \left\{\lambda_i x_i + \mu_i x_i^p\right\} + v(1+\Delta) - (p-1)!R(\lambda_1 x_1, \ldots, \lambda_n x_n, v) ,$$

where

$$\lambda_i, \mu_i \in \mathbb{Q}^0 \quad (1 \le i \le n) , \quad v \in L^0 \cap \underline{\underline{a}}^2 .$$

Proof. It will be sufficient to prove that u is congruent modulo $L^0 \cap \underline{\underline{a}}^p$ to an expression ψ of the given form. For, if $\omega \in L^0 \cap \underline{\underline{a}}^p$, then $\omega = \omega(1+\Delta)$ because $c = 2p - 2$; therefore $\psi + \omega$ again has the same form as ψ.

The corollary is easily verified when $p = 2$ and we shall assume henceforth that $p > 2$. Then $E(x)^{-1} = E(-x)$, so that $E(u)$ is expressible in the form

$$E(u) = E(y_1) \ldots E(y_r) \tag{2.11}$$

with

$$\{y_1, \ldots, y_r\} \subseteq \{x_1, -x_1, \ldots, x_n, -x_n\} .$$

After adding extra redundant factors $E(x_i)E(-x_i)$ if necessary, we may assume that $r \ge n$. Then (2.11) follows from the equation

$$E(V') = E(x_1) \ldots E(x_r) \tag{2.12}$$

in $A(r, c; \mathbb{Q})$ by applying the endomorphism η defined by

$$x_i\eta = y_i \quad (i = 1, \ldots, r) .$$

The form of V' is given by Proposition 1. (We may define Δ in $A(r, c; \mathbb{Q})$ in such a way as to extend Δ in $A(n, c; \mathbb{Q})$; however, this is not really necessary because, in any case, images under Δ are uniquely determined modulo $L^0 \cap \underline{\underline{a}}^p$.) Applying η to (2.12) and using Lemma 2, we conclude that

$$u \equiv \sum_1^r y_j + v(1+\Delta) - (p-1)!R(y_1, \ldots, y_r, v) \pmod{L^0 \cap \underline{\underline{a}}^p} ,$$

where $v \in L^0 \cap \underline{\underline{a}}^2$.

For $i = 1, \ldots, n$, let λ_i' of $y_1, \ldots, y_r$ be equal to x_i and λ_i'' equal to $-x_i$. Then

$$\sum_1^r y_j = \sum_1^n \lambda_i x_i ,$$

where $\lambda_i = \lambda_i' - \lambda_i''$. Further, since $R(\cdot)$ is a symmetric function modulo $L^0 \cap \underline{\underline{a}}^p$, we have

$$R(y_1, \ldots, y_r, v)$$
$$\equiv R(\underbrace{x_1, \ldots, x_1}_{\lambda_1' \text{ terms}}, \underbrace{-x_1, \ldots, -x_1}_{\lambda_1'' \text{ terms}}, x_2, \ldots, v) \pmod{L^0 \cap \underline{\underline{a}}^p} .$$

Now,

$$R(\underbrace{x, \ldots, x}_{\lambda' \text{ terms}}, \underbrace{-x, \ldots, -x}_{\lambda'' \text{ terms}}) = \left\{\frac{\lambda^p-\lambda}{p!}\right\}x^p ,$$

where $\lambda = \lambda' - \lambda''$. Therefore, by Lemma 3,

$$R(y_1, \ldots, y_r, v) \equiv R(\lambda_1 x_1, \ldots, \lambda_n x_n, v) + \sum_1^n \mu_i x_i^p \pmod{L^0 \cap \underline{\underline{a}}^p} ,$$

where

$$\mu_i = \left\{\lambda_i^p - \lambda_i\right\}/p! \in \mathbb{Q}^0 \quad (1 \le i \le n) .$$

Putting these results together, we get the corollary.

3. Proofs

From now on, we shall work exclusively in the algebra $A(n, c; \mathbb{F}_p)$, writing $A = A(n, c; \mathbb{F}_p)$, $L = L(n, c; \mathbb{F}_p)$, and so on. We recall that P denotes the Lie p-algebra generated by $x_1, \ldots, x_n$ and that, if $S \subseteq A$, gr S denotes the (graded) subspace spanned by the leading terms of the elements of S . The common principles behind the proofs of both Theorem 2 and Theorem A of [8] are set out in some detail in §§2.4, 3.4 of [8].

Let $\tilde{F}$ denote the multiplicative subgroup of A generated by the elements $E(x_1), \ldots, E(x_n)$. If $T \subseteq \tilde{F}$, define

$$l(T) = \{u : E(u) \in T\} .$$

The proof of Theorem 2 is based on the Lie ring isomorphism[4]

$$L(\beta(n, c)) \cong P/\mathrm{gr}\left(l\left(\tilde{F}^p\right)\right) ,$$

where $\beta(n, c)$ denotes the largest nilpotent quotient group of $B(n)$ of class less than or equal to c . This is essentially the same as the isomorphism used in [8]; for, since u and $E(u) - 1$ have the same leading term, it follows that $\mathrm{gr}(T-1) = \mathrm{gr}(l(T))$ for every subset T of $\tilde{F}$.

The first step in the proof is to determine $l(\tilde{F})$ when $c = 2p - 2$ (Proposition 2). This is hardly more than a characteristic p transcription of the corollary to Proposition 1. The next step is to determine $l\left(\tilde{F}^p\right)$ when $c = 3p - 3$ (Lemma 4, Corollary). It is shown, in fact, that $l\left(\tilde{F}^p\right)$ is the subspace spanned by the pth powers of the elements of $l(\tilde{F})$. The final step is almost the same as for the proof of Theorem A in §4.2 of [8].

3.1. THE GROUP $\tilde{F}$

We assume in the present subsection that $c = 2p - 2$.

NOTATION. Let $z_1, \ldots, z_t$ be a basis of P satisfying the

[4] The notation $\beta(n, c)$ replaces the (unfortunate) notation $B(n, c)$ of [8].

following conditions:

(a) each z_i is either a homogeneous element of L or a power x_j^p ;

(b) the z_i are arranged in order of increasing degree;

(c) $z_i = x_i$ for $i = 1, \ldots, n$.

Define $z_1^*, \ldots, z_t^*$ as follows:

$$z_i^* = z_i + z_i\Delta \text{ (see §2.1), if } z_i \in L \cap \underline{\underline{a}}^2 ;$$

$$z_i^* = z_i \text{ otherwise.}$$

PROPOSITION 2. *Let* $c = 2p - 2$. *Write*

$$l(\tilde{F}) = \{u : E(u) \in \tilde{F}\} .$$

Then $u \in l(\tilde{F})$ *if, and only if,* u *has the form*

$$u = \sum_1^t \lambda_i z_i^* + R(\lambda_1 z_1, \ldots, \lambda_t z_t) \quad (\lambda_1, \ldots, \lambda_t \in \mathbf{F}_p) .$$

Proof. Since $c = 2p - 2$, we have

$$R(\lambda_1 z_1, \ldots, \lambda_t z_t) = R\left(\lambda_1 x_1, \ldots, \lambda_n x_n, \sum_{n+1}^s \lambda_i z_i\right)$$

and

$$z_i^* = z_i \quad \text{for } i > s ,$$

where $z_1, \ldots, z_s$ are those z_i of degree less than p . Therefore, by the corollary to Proposition 1, every $u \in l(\tilde{F})$ has the specified form. On the other hand, the number of elements of this form is $p^t = |P|$, which equals $|\tilde{F}| = |l(\tilde{F})|$ because $P \cong_p L(\tilde{F})$. This clearly implies the proposition.

3.2. THE SUBGROUP $\tilde{F}^p$

NOTATION. If $M \subseteq \underline{\underline{a}}$, then

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

$$E(M) = \{E(u) : u \in M\} ,$$

$$\text{Lie } M = \text{Lie subalgebra generated by } M .$$

If $N \subseteq 1 + \underline{\underline{a}}$, then

$$l(N) = \{u : E(u) \in N\} ,$$

$$\text{gp } N = \text{multiplicative subgroup generated by } N .$$

LEMMA 4. *If* $M \subseteq \underline{\underline{a}}^r$, *where* $rp > c$, *then*

$$\text{gp } E(M) = E(\text{Lie } M) .$$

Proof. Let $*$ denote the binary operation on A defined by the first $p - 1$ terms of the Baker-Campbell-Hausdorff formula:

$$a * b = \sum_{1}^{p-1} H_r(a, b) .$$

Now, since $rp > c$, we have $\left(\underline{\underline{a}}^r\right)^p = 0$. Therefore, by Theorem (4.6) of Lazard [7], $\underline{\underline{a}}^r$ is a group under $*$ and the subgroup generated by the subset M is the Lie subalgebra generated by M :

(3.1) $$\text{gp}_* M = \text{Lie } M .$$

On the other hand, if $u, v \in \underline{\underline{a}}^r$, then, by (2.7), $E(u)E(v) = E(u * v)$. Hence

(3.2) $$\text{gp } E(M) = E(\text{gp}_* M) .$$

The lemma follows immediately from (3.1) and (3.2).

COROLLARY. *If* $c < p^2$, *then*

$$l\left(\tilde{F}^p\right) = \text{Lie}\left\{u^p : u \in l(\tilde{F})\right\} .$$

Proof. Taking $M = \left\{u^p : u \in l(\tilde{F})\right\}$, we have $E(M) = \tilde{F}^p$ by the formula $E\left(u^p\right) = E(u)^p$. The corollary now follows directly from the lemma.

REMARK. We shall see in §3.3 that, when $c = 3p - 3$, $l\left(\tilde{F}^p\right)$ is actually the subspace spanned by $\left\{u^p : u \in l(\tilde{F})\right\}$.

3.3. CONCLUSION OF PROOF

We assume here that $c = 3p - 3$. Consider an element u^p , where

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

$u \in l(\tilde{F})$. In calculating u^p , it is legitimate to take the form of u derived in Proposition 2 for class $2p - 2$. Write

$$X = \sum_1^t \lambda_i z_i \ , \quad X^* = \sum_1^t \lambda_i z_i^* \ , \quad R = R\left(\lambda_1 z_1, \ldots, \lambda_t z_t\right) .$$

Then

$$\begin{aligned} u^p &= (X^*+R)^p \\ &= (X^*)^p + \langle (p-1)X^*, R\rangle \\ &= (X^*)^p + [R, \underbrace{X^*, \ldots, X^*}_{p-1 \text{ terms}}] \quad \left(\text{by formula } (3.12) \text{ of } [8]\right) \\ &= (X^*)^p + [R, \underbrace{X, \ldots, X}_{p-1 \text{ terms}}] \quad (\text{since } c = 3p - 3) \\ &= (X^*)^p + \left[R \,|\, X^{p-1}\right] \quad \left(\text{by } (2.2) \text{ and } (3.13) \text{ of } [8]\right). \end{aligned}$$

Let M denote the subspace spanned by $\{u^p : u \in l(\tilde{F})\}$. By Lemma 4, Corollary,

$$l\left(\tilde{F}^p\right) = \text{Lie } M .$$

Furthermore, by the same argument as in the proof of Theorem A in §4.2 of [8], we conclude that M is spanned by the following elements:

(3.3) $\quad z_i^p \quad \left(\text{with } z_i \text{ of degree } 1 \text{ or } 2\right)$;

(3.4) $\quad \langle a_1 z_1, a_2 z_2, \ldots\rangle^* = \langle a_1 z_1, a_2 z_2, \ldots\rangle + \ldots$

with $0 \le a_i < p \quad (i = 1, 2, \ldots)$, $\sum a_i = p$, and where, if $\langle a_1 z_1, a_2 z_2, \ldots\rangle \in L(n)^{\underline{\underline{r}}}$, the unwritten terms are in components $L(n)^{\underline{\underline{m}}}$ with $|\underline{\underline{m}}| = |\underline{\underline{r}}| + p - 1$ and $f_{\underline{\underline{m}}} = f_{\underline{\underline{r}}}$;

(3.5) $\quad \langle\langle a_1 z_1, a_2 z_2, \ldots\rangle\rangle$

with $0 \le a_i < p \quad (i = 1, 2, \ldots)$, $\sum a_i = 2p - 1$.

From this, we deduce first that

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

$$[M, M] \subseteq [P, P] \subseteq E_{p-1} \cap \underline{\underline{a}}^{2p} ,$$

$$E_{p-1} \cap \underline{\underline{a}}^{2p-1} \subseteq M ,$$

whence M is a Lie subalgebra. Therefore

$$l(\tilde{F}^p) = M .$$

Now let $\underline{\underline{m}}$ be a multi-index satisfying the conditions of Theorem 2. In view of the Lie algebra isomorphism

$$P/P^{[p]} \cong L/E_{p-1}$$

(see (2.9) of [8]), what we have to show is that

$$(\mathrm{gr}\ M)^{\theta(\underline{\underline{m}})} \subseteq P^{[p]} + W ,$$

where W is the subspace spanned by the elements of the form $\langle\langle b_1z_1, b_2z_2, \ldots\rangle\rangle$ with the b_i integral.

It is evident from the form of the elements which span M that $\mathrm{gr}\ M$ is spanned by elements (3.3), elements (3.5), elements $\langle a_1z_1, a_2z_2, \ldots\rangle$, and finally certain linear combinations

(3.6) $$\sum r_{a_1,a_2,\ldots}\langle a_1z_1, a_2z_2, \ldots\rangle^* ,$$

where

(3.7) $$\sum r_{a_1,a_2,\ldots}\langle a_1z_1, a_2z_2, \ldots\rangle = 0$$

and the sum is taken over a's such that $\langle a_1z_1, a_2z_2, \ldots\rangle$ has total degree less than or equal to $2p - 2$ in $x_1, \ldots, x_n$.

Thus, an element v of $(\mathrm{gr}\ M)^{\theta(\underline{\underline{m}})}$ will be congruent modulo $P^{[p]} + W$ to an element (3.6) with each of the corresponding terms $\langle a_1z_1, a_2z_2, \ldots\rangle$ in a component $L^{\underline{\underline{m}}'}$ with $|\underline{\underline{m}}'| = |\underline{\underline{m}}| - p + 1$ and $f_{\underline{\underline{m}}'} = f_{\underline{\underline{m}}}$. By the hypothesis of the theorem, (3.7) implies that all $r_{a_1,a_2,\ldots}$ are 0. Hence $v \in P^{[p]} + W$, which proves the theorem.

4. Application

We now take

$$p = 5 \ , \quad n = 2 \ .$$

If $\overline{B}(5, 2)$ denotes the largest 2-generator finite group of exponent 5, then

$$L(\overline{B}(5, 2)) \cong \Lambda(2)/\Sigma(2) \ .$$

It is known[5] that $\Lambda(2)$ has dimension 34 and nilpotency class 12. We shall determine a set of generators for the ideal $\Sigma(2)$. A further computation establishes that all these generators are zero, so that

$$\Sigma(2) = \{0\}$$

(see Havas, Wall, and Wamsley [2]). Hence $\overline{B}(5, 2)$ has order 5^{34} and nilpotency class 12.

Now, the class of $\Lambda(2)$ is $3p - 3 = 12$. Moreover, by the result of Kostrikin cited in §1, the elements (1.2) of total degree less than or equal to $2p - 2 = 8$ are linearly independent[6]. Therefore, by Theorem 1, $\Sigma(2)$ is spanned by the elements (1.5).

We shall use the following notation for the 2 generators ξ_1, ξ_2, and their basic products of degree less than or equal to 4:

Degree 1: $\xi = \xi_1 \ , \quad \eta = \xi_2 \ ;$

Degree 2: $\zeta = \eta\xi \ ;$

Degree 3: $\zeta_1 = \zeta\xi \ , \quad \zeta_2 = \zeta\eta \ ;$

Degree[7] 4: $\zeta_{11} = \zeta_1\xi \ , \quad \zeta_{12} = \zeta_1\eta \ , \quad \zeta_{22} = \zeta_2\eta \ .$

We shall also use the simplified notation $(\xi^l\eta^m\zeta^n \ldots)$ instead of $\langle\langle l\xi, m\eta, n\zeta, \ldots\rangle\rangle$.

We now list all the elements (1.5) according to total degree:

---

[5] These results have been proved by Krause and Weston [6] and checked by Havas, Wall, and Wamsley [2]. (Krause and Weston *say* the nilpotency class is 13 while at the same time *proving* it is 12.)

[6] It is not difficult to check this directly.

[7] The product $\zeta_{21} = \zeta_2\xi$ is equal to ζ_{12} by the Jacobi identity.

https://doi.org/10.1017/S0004972700008406 Published online by Cambridge University Press

Degree 10: $(\xi^4\eta^4\zeta)$;

Degree 11: $\{\xi^4\eta^4\zeta_i\}$ $(i = 1, 2)$;

$(\xi^r\eta^{7-r}\zeta^2)$ $(r = 3, 4)$;

Degree 12: $\{\xi^4\eta^4\zeta_{ij}\}$ $\{(i, j) = (1, 1), (1, 2), (2, 2)\}$;

$\{\xi^r\eta^{7-r}\zeta\zeta_i\}$ $(r = 3, 4; i = 1, 2)$;

$(\xi^s\eta^{6-s}\zeta^3)$ $(s = 2, 3, 4)$.

Using the identity

$$\langle\langle u_1, \ldots, u_{2p-1}\rangle\rangle v = \sum_{i=1}^{2p-1} \langle\langle u_1, \ldots, u_i v, \ldots, u_{2p-1}\rangle\rangle ,$$

we find that $\Sigma(2)$ is generated as an ideal by the elements

$$(\xi^4\eta^4\omega) \quad (\omega = \zeta, \zeta_1, \zeta_2, \zeta_{11}, \zeta_{12}, \zeta_{22}) .$$

Further, these elements span an $SL(2, 5)$-module[8], which is generated by the 3 elements corresponding to $\omega = \zeta, \zeta_1, \zeta_{12}$. Thus, in order to prove that $\Sigma(2)$ is zero it suffices to prove that these 3 elements are zero. This computation was carried out by Havas, Wall, and Wamsley ([2]).

References

[1] Jean Dieudonné, "On the Artin-Hasse exponential series", *Proc. Amer. Math. Soc.* 8 (1957), 210-214.

[2] George Havas, G.E. Wall, and J.W. Wamsley, "The two generator restricted Burnside group of exponent five", *Bull. Austral. Math. Soc.* 10 (1974), 459-470.

[3] W. Holenweg, "Die Dimensionsdefekte der Burnside-Gruppen mit zwei Erzeugenden", *Comment. Math. Helv.* 35 (1961), 169-200.

[8] See the final paragraph of §2.4 in [8].

[4] W. Holenweg, "Über die Ordnung von Burnside-Gruppen mit endlich vielen Erzeugenden", *Comment. Math. Helv.* **36** (1962), 83-90.

[5] А.И. Кострикин [A.I. Kostrikin], "О связи между периодическими группами и кольцами Ли." [On the connection between periodic groups and Lie rings], *Izv. Akad. Nauk SSSR Ser. Math.* **21** (1957), 289-310; English Translation: *Amer. Math. Soc. Transl.* (2) **45** (1965), 165-189.

[6] Eugene F. Krause and Kenneth W. Weston, "On the Lie algebra of a Burnside group of exponent 5 ", *Proc. Amer. Math. Soc.* **27** (1971), 463-470.

[7] M. Lazard, "Sur les groupes nilpotents et les anneaux de Lie", *Ann. Sci. École Norm. Sup.* (3) **71** (1954), 101-190.

[8] G.E. Wall, "On the Lie ring of a group of prime exponent", *Proc. Second Internat. Conf. Theory of Groups*, Canberra, 1973, 667-690 (Lecture Notes in Mathematics, **372**. Springer-Verlag, Berlin, Heidelberg, New York, 1974).

Department of Pure Mathematics,
University of Sydney,
Sydney,
New South Wales.